360RSW05-WKB-TA01

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 1 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, 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 Cabling Topology" diagram 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 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 1 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

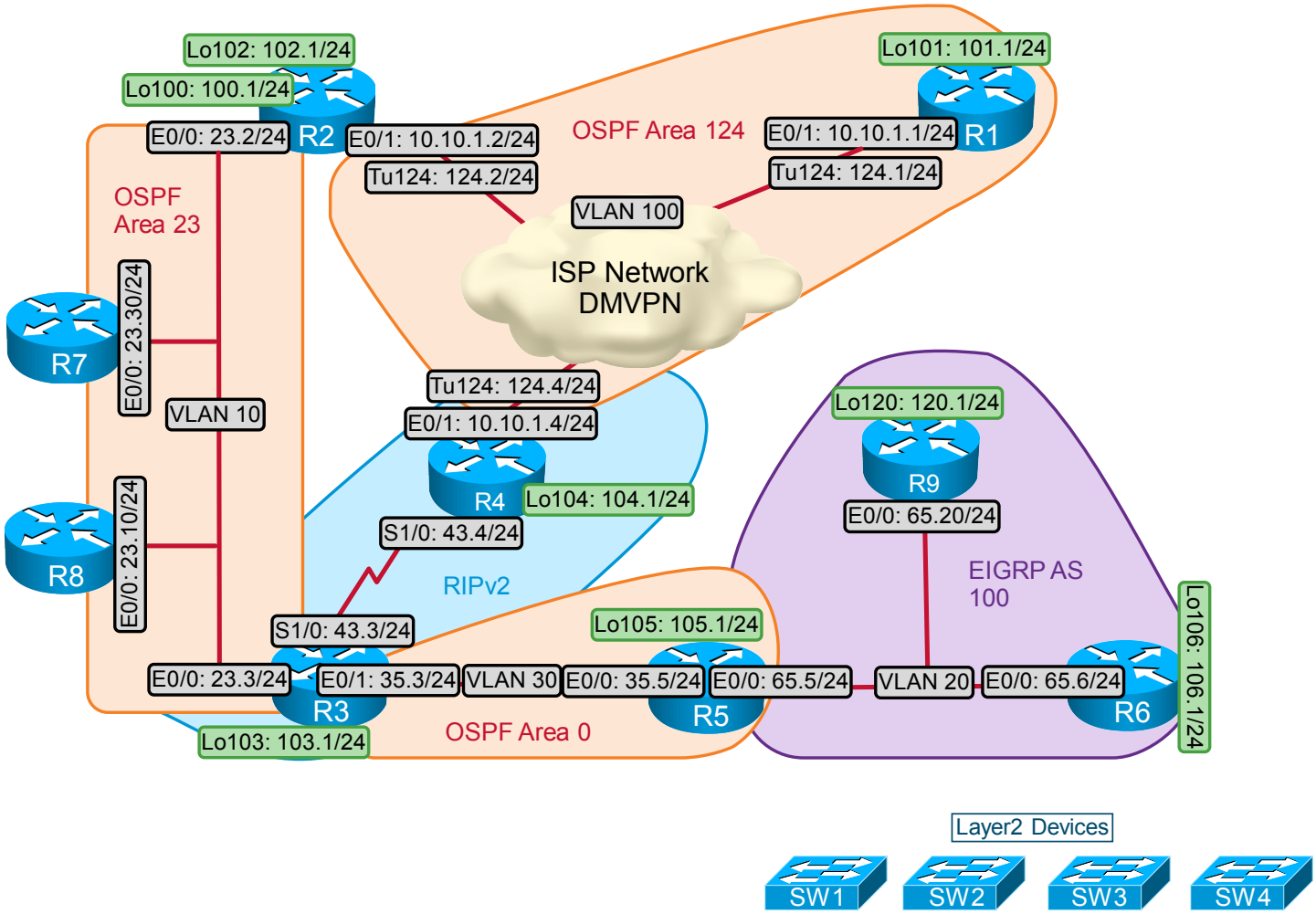
Restrictions and Goals

Note Read this section carefully.

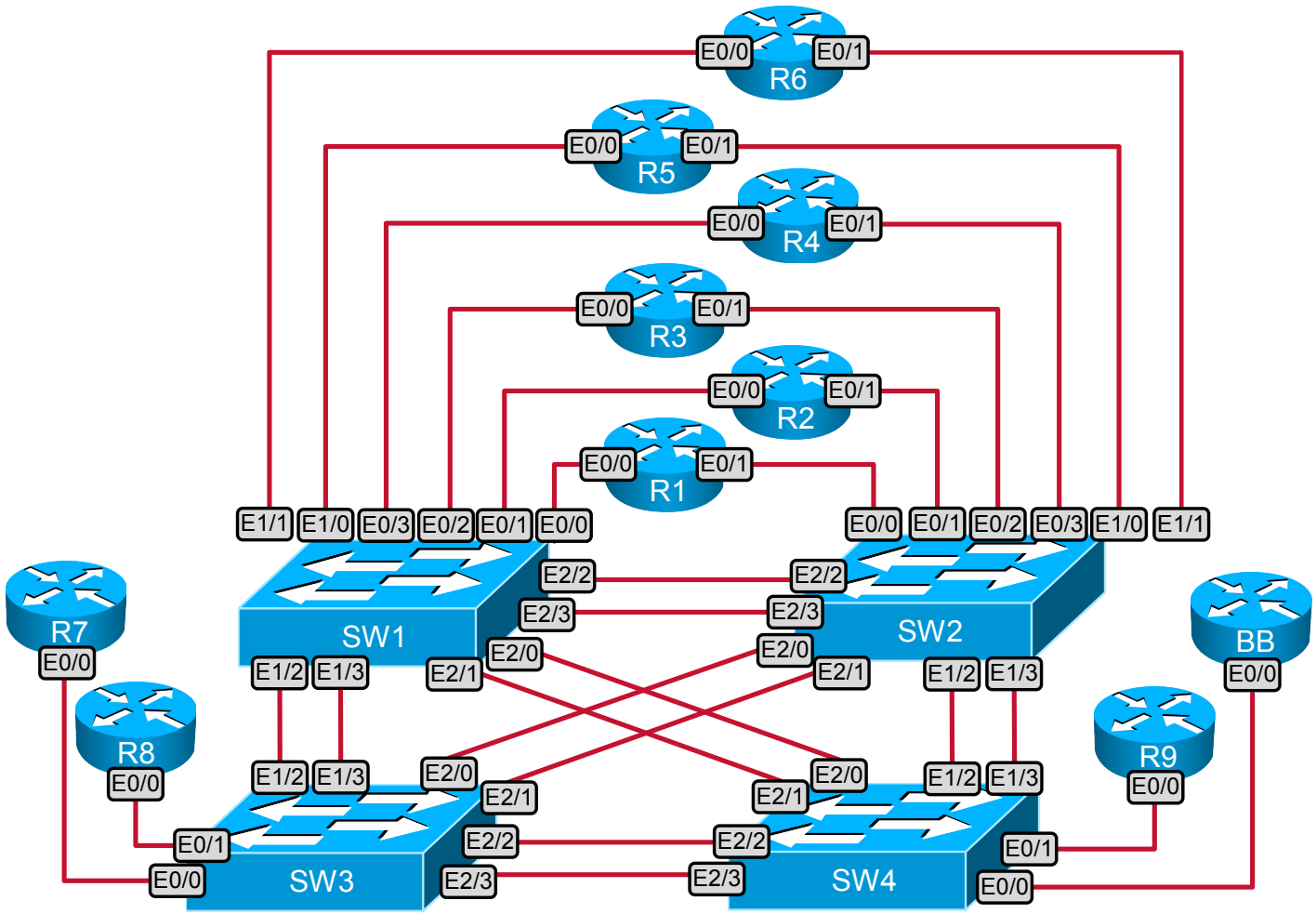
- To receive credit for a subsection, you must fully complete the subsection as per the requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 172.10.0.0/16.
- *Points will be deducted from multiple 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.
- All IP addresses that are involved in this scenario must be reachable, unless explicitly specified otherwise.
- Unless explicitly specified otherwise, addresses and networks that are advertised in the BGP section need to be reachable by all BGP routers, but do not have to be reachable by routers that use only IGP.
- Use conventional routing algorithms only, unless specified otherwise.
- Do not create new interfaces to fulfill IGP requirements, and do not summarize unless you are 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.

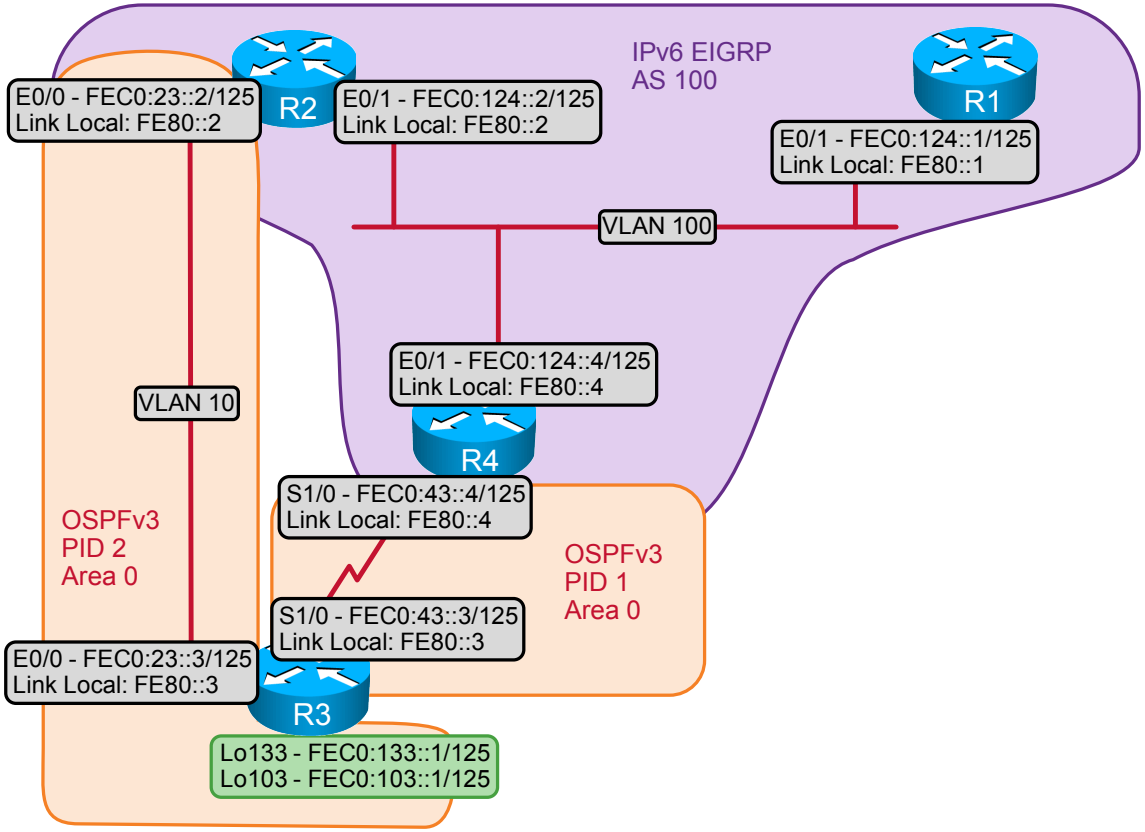
IPv4 IGP Diagram



Ethernet Switched Cabling Topology



IPv6 Topology Diagram



1. DMVPN Troubleshooting Section (Total: 2 points)

1.1. Troubleshooting Ticket

Users reported that the connectivity within the DMVPN is broken. R2 can ping R1, but R2 cannot ping R4 across the DMVPN subnet.

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

R1, R2, and R4 use the DMVPN subnet 172.10.124.0/24 to exchange the IPv4 traffic as shown on the "IPv4 IGP" diagram:

- The Ethernet0/1 interfaces on the subnet 10.10.1.0/24 are used for the DMVPN multipoint Generic Routing Encapsulation (mGRE) tunnel source.
- R1 is the DMVPN hub.
- R2 and R4 are the DMVPN spokes.

1.3. Expected Behavior and Network Policies

All IPv4 same-subnet addresses that are configured on the DMVPN must be reachable without requiring routing protocol support.

1.4. Special Goals and Restrictions

Only IPv4 unicast traffic is forwarding between the DMVPN devices.

R1 is the next-hop server (NHS) for R2 and R4.

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

2.1. 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.

2.2. Description of the Topology

The switched Ethernet topology for this lab consists of four VLANs, as shown on the "IPv4 IGP" diagram and "IPv6 IGP" diagram. No additional VLANs may be configured or used.

All trunk links are encapsulated with 802.1Q.

2.3. Expected Behavior and Network Policies

The Ethernet links that are shown on the "IPv4 IGP" diagram and "IPv6 IGP" diagram must support same-subnet reachability and the routing protocols shown.

All switches should be in the VTP domain CISCO360.

Only one VLAN is allowed on the trunk link between SW1 and SW2.

2.4. Special Goals and Restrictions

No additional Ethernet interfaces should be created in your solution.

All links that are administratively down must remain so.

Ensure that only two spanning trees span over VLANs 10, 20, and 30:

- The first spanning tree should span over both VLANs 10 and 20.
- The second spanning tree should span over VLAN 30.

SW1 should be the root switch for VLAN 10.

SW2 should be the root switch for VLAN 30.

STP should operate according to the following requirements:

- The preferred path between SW1 and SW3 for VLAN 10 should be through the port E1/3.
- The preferred path between SW1 and SW2 for VLAN 30 should be through the port E2/3.
- Do not use the same method to implement these requirements.
- No configuration is allowed on SW1 to implement these requirements.

3. IPv4 OSPF Troubleshooting Section (Total: 3 points)

3.1. Troubleshooting Ticket

Users reported that the OSPF routing domain does not operate according to the requirements provided in the "IPv4 OSPF Troubleshooting" section. OSPF is not stable on the DMVPN. Also R7, R8, and R5 do not see the DMVPN subnet in their respective routing tables.

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

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

- Area 0 includes the subnets 172.10.35.0/24.and 172.10.105.0/24.
- Area 124 includes the subnets 172.10.124.0/24 and 172.10.101.0/24.
- Area 23 includes the subnet 172.10.23.0/24.

3.3. Expected Behavior and Network Policies

OSPF should elect the designated router (DR) and must use IPv4 unicast communications for the control packets on the DMVPN subnet.

OSPF must provide stable reachability between all internal subnets.

All internal OSPF routes should get an administrative distance of 121.

All external OSPF routes should get an administrative distance of 171.

The following subnets should be advertised across the OSPF network but should not belong to any OSPF area:

- subnet 172.10.100.0/24
- subnet 172.10.102.0/24

3.4. Special Goals and Restrictions

OSPF area 23 should be authenticated with the password "CISCO." The password should not be sent in cleartext.

R3 should systematically become the DR.

The subnet 172.10.23.0/24 should not be advertised into area 124 by any OSPF process.

Loopback networks must be advertised with their original masks.

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

4.1. Troubleshooting Ticket

Users reported that the EIGRP routing domain does not operate according to the requirements provided in the "IPv4 EIGRP Troubleshooting" section. R6 does not form any EIGRP neighbor relationships.

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

As shown on the "IPv4 IGP" diagram, EIGRP AS 100 should operate on VLAN 20.

Only the subnets 172.10.65.0/24 and 172.10.120.0/24 should be internal to EIGRP AS 100.

4.3. Expected Behavior and Network Policies

The following subnets should be redistributed into EIGRP:

- subnet 172.10.106.0/24 on R6
- subnet 172.10.105.0/24 on R5

The devices that are located in EIGRP AS 100 should trust only authenticated EIGRP messages:

- The trusted password should be “CISCO1” set from 01/01/2013 and should never expire.
- The password should not be sent in cleartext.

4.4. Special Goals and Restrictions

Ensure that R6 adds the value 1000 to the EIGRP metric received for the subnet 172.10.120.0/24.

All internal EIGRP routes should get an administrative distance of 123.

All external EIGRP routes should get an administrative distance of 169.

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

5.1. 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.

5.2. Description of the Topology

RIP operates between routers R3 and R4 as shown on the “IPv4 IGP” diagram.

R3 should send only RIPv1 updates and listen to only RIPv2 updates.

R4 should send only RIPv2 updates and listen to only RIPv1 updates.

5.3. Expected Behavior and Network Policies

RIP updates should be sent on only the subnet 172.10.43.0/34.

All RIP updates should be sent to only the 255.255.255.255 destination address.

5.4. Special Goals and Restrictions

All RIP routes should get an administrative distance of 119.

RIP version 2 should be configured on R4.

6. IPv4 Redistribution Troubleshooting Section (Total: 3 points)

6.1. Troubleshooting Ticket

Users reported that the IPv4 IGP routing domain does not operate according to the requirements provided in the "IPv4 Redistribution Troubleshooting" section. R6 and R9 cannot communicate with the subnet 172.10.35.0/24, and R1 cannot communicate with the subnet 172.10.23.0/24.

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

OSPF and RIP are mutually redistributed on R3 and R4.

OSPF and EIGRP are mutually redistributed on R5 only.

6.3. Expected Behavior and Network Policies

All devices should be able to reach all subnets.

Use the **redistribute connected** command where required and not restricted by the scenario.

6.4. Special Goals and Restrictions

You may not configure any dynamic protocol on any additional interface from those indicated on the "IPv4 IGP" diagram.

7. Security Troubleshooting Section (Total: 2 points)

7.1. Troubleshooting Ticket

Users reported that IP 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.

7.2. Description of the Topology

Prevent IP address spoofing on both Ethernet interfaces of R3.

Any denied packet should trigger a log on R3.

7.3. Expected Behavior and Network Policies

On E0/0, allow only packets sourced from the subnet 172.10.0.0/16.

Ensure that a PC located in VLAN 10 may communicate with a DHCP server through R3.

The IP address of the DHCP server is 172.10.35.254.

On E0/1, packets from the subnet 10.0.0.0/8 should not be submitted to this spoofing control.

7.4. Special Goals and Restrictions

Do not use the same method on E0/0 and E0/1 to implement this security feature.

On E0/1, ensure that the implemented spoofing method relies on the content of the routing table of R3.

8. IPv6 Troubleshooting Section (Total: 3 points)

8.1. Troubleshooting Ticket

Users reported that the IPv6 routing domain does not operate according to the requirements provided in the "IPv6 Troubleshooting" section. R2 cannot ping the IPv6 subnets FEC0:103::/125, FEC0:133::/125, and FEC0:43::/125.

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

The IPv6 topology is shown on the "IPv6 IGP" diagram.

All routable IPv6 prefixes start with the hexadecimal FEC0.

EIGRP for IPv6 is configured on the subnet FEC0:124::/125. R2 and R4 should form the IPv6 EIGRP neighbor relationship with R1 via unicast communications. R2 and R4 must not form the direct neighbor relationship.

OSPFv3 is configured as follows:

- **Process 1:** Area 0 on prefix FEC0:43::/125, between routers R3 and R4.
- **Process 2:** Area 0 on prefix FEC2:23::/125 between routers R2 and R3, on Loopback 103 and Loopback 133 of R3.

OSPFv3 and EIGRP for IPv6 are mutually redistributed on R2 and R4.

No other redistribution is allowed.

8.3. Expected Behavior and Network Policies

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

No DR should be elected in VLAN 10.

No OSPFv3 multicast packets should be seen in VLAN 10.

8.4. Special Goals and Restrictions

All networks must be advertised with their original masks only.

Ensure that the OSPFv3 PID 2 router id of R4 is 244.244.244.244.

Ensure that the OSPFv3 PID 1 router id of R3 is 233.233.233.233.

9. Quality of Service Troubleshooting Section (Total: 2 points)

9.1. Troubleshooting Ticket

Users reported that QoS does not operate according to the requirements provided in the "Quality of Service 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.

9.2. Description of the Topology

On R2, in times of congestion, ensure that the traffic that is sent out of the E0/0 interface is given a specific bandwidth according to the following specifications:

- HTTP traffic should get at least 20 percent of the available bandwidth.
- SMTP traffic should get at least 20 percent of the available bandwidth.
- DNS traffic should get at least 5 percent of the available bandwidth.
- Telnet traffic should get at least 5 percent of the available bandwidth.

9.3. Expected Behavior and Network Policies

In times of congestion, ensure that voice traffic does not get more than 20 percent of the available traffic.

Voice packets use H.323 signaling.

9.4. Special Goals and Restrictions

Only a Modular QoS CLI (MQC) is allowed.

10. IP Service Troubleshooting Section (Total: 2 points)

10.1. Troubleshooting Ticket

Users reported that the IP services do not operate according to the requirements provided in the "IP Service 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.

10.2. Description of the Topology

Ensure that all configuration changes made on R4 are logged.

10.3. Expected Behavior and Network Policies

Set the maximum number of entries retained in the configuration log as two times larger as the default value.

10.4. Special Goals and Restrictions

Suppress the display of password information in configuration log files.