360RSW05-WKB-TA02

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 2 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 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 2 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: Intermediate

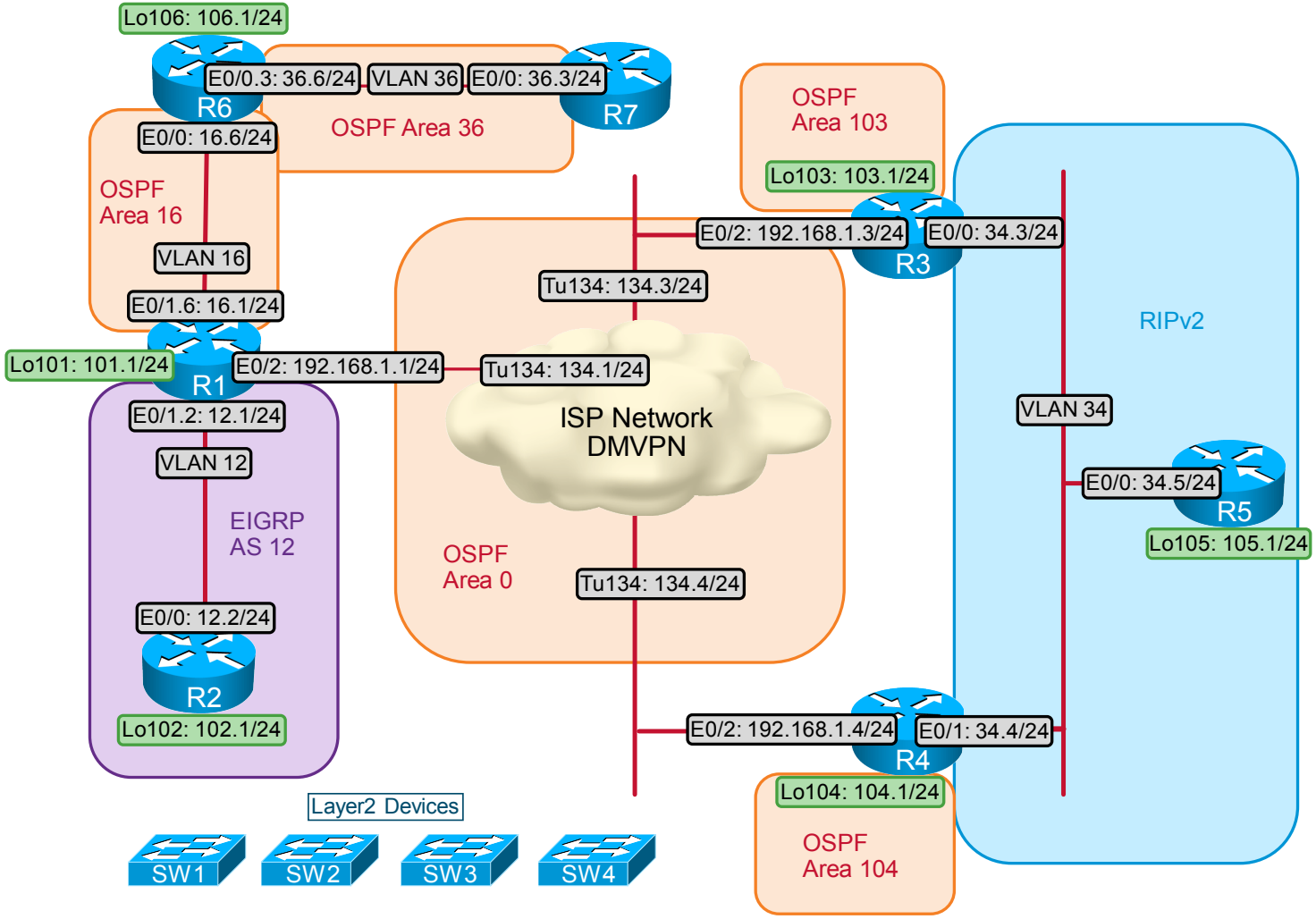
Restrictions and Goals

Note Read this section carefully.

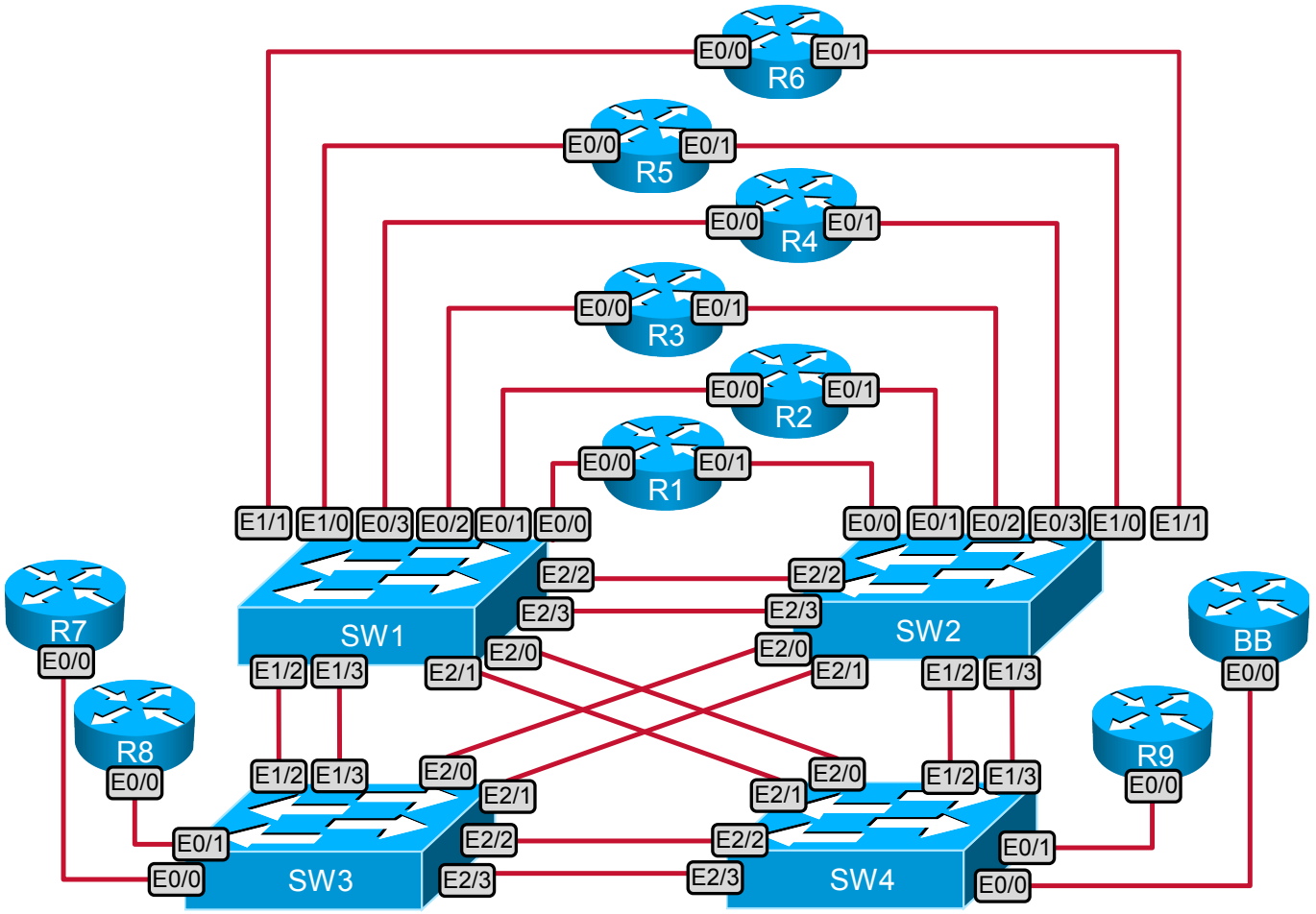
- To receive credit for a subsection, you must fully complete the subsection per requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 172.16.0.0/16.
- *Points will be deducted from multiple 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**), unless explicitly specified otherwise.
- Do not use the **ip default-gateway** or **ip default-network** command.
- 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 must 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; 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.

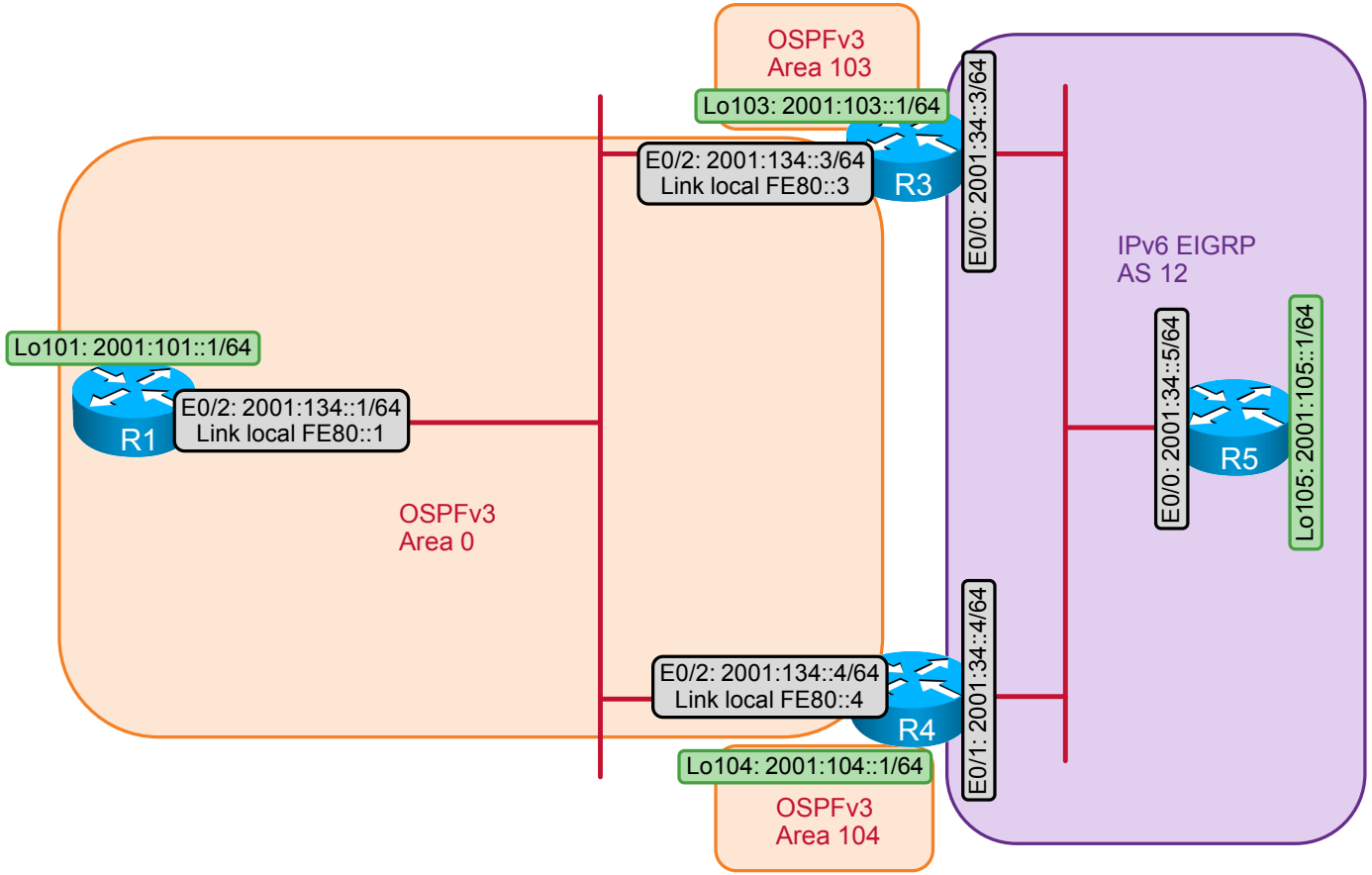
IPv4 IGP Diagram



Ethernet Switched Cabling Topology



IPv6 Topology Diagram



1. DMVPN Troubleshooting Section (Total: 2 points)

1.1. Troubleshooting Ticket

- Users reported that connectivity within the DMVPN is broken. R1 cannot ping R3 and 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 172.16.134.0/24 to exchange the IPv4 traffic as shown on the "IPv4 IGP" diagram:
  - The Ethernet0/2 interfaces on the subnet 192.168.1.1/24 are used for the DMVPN mGRE tunnel source.
  - R1 is the DMVPN hub.
  - R3 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 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. There is no reachability between R1 and R2 on VLAN 12. There is no reachability between R1 and R6 on VLAN 16. R4 cannot reach R3 or R5 on VLAN 34, but R3 and R5 can communicate. R6 cannot reach R7 on VLAN 36.
- 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 in the lab diagrams. No additional VLANs may be configured or used.
- The links E2/2 and E2/3 connecting SW3 and SW4 are bundled to the EtherChannel link.
- The links E2/2 and E2/3 connecting SW1 and SW2 are dot1q trunks. The links to R1 and R6 are dot1q trunks. All other links are access links.
- The links E2/2 and E2/3 connecting SW3 and SW4 are the EtherChannel links.

2.3. Expected Behavior and Network Policies

- The Ethernet links that are shown in the lab diagrams must support same-subnet reachability and the routing protocols that are shown.

2.4. 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 unused links in the Ethernet switching topology that are administratively down must remain so.

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 it 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.

3.2. Description of the Topology

- OSPF for IPv4 is divided into five areas, as shown in the "Lab IPv4 IGP" diagram and listed here. Only these listed subnets should be internal to OSPF:
  - Area 0 includes subnet 172.16.134.0/24.
  - Area 16 includes subnet 172.16.16.0/24.
  - Area 36 includes subnet 172.16.36.0/24.
  - Area 103 includes subnet 172.16.103.0/24.
  - Area 104 includes subnet 172.16.104.0/24.

3.3. Expected Behavior and Network Policies

- OSPF must provide stable reachability between all internal subnets.
- R6 is permitted to advertise only one subnet, 0.0.0.0/0, to R7.

3.4. Special Goals and Restrictions

- You are not permitted to change the OSPF network type on any interface.
- Do not create any distribute lists, filter lists, route maps, or access lists on R6.
- Loopback networks must be advertised with their original masks.

4. 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 it 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.

4.2. Description of the Topology

- EIGRP AS 12 should operate on VLAN 12 between R1 and R2, as shown in the "IPv4 IGP" diagram.
- Subnet 172.16.102.0/24 is included in EIGRP AS 12. No other networks are internal to EIGRP.

4.3. Expected Behavior and Network Policies

- EIGRP must provide reachability between R2 and the rest of the network.

4.4. Special Goals and Restrictions

- No default routes may be advertised or used by EIGRP.
- EIGRP must originate and accept only unicast protocol traffic on subnet 172.16.12.0/24.

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 it 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 version 2 operates on routers R3, R4, and R5, as shown in the "IPv4 IGP" diagram.
- Given the classful nature of the RIP network statement, all the interfaces on these three routers will be included in the RIP process.

5.3. Expected Behavior and Network Policies

- RIP must provide stable reachability between R5 and the rest of the network.
- RIP may send only unicast updates.

5.4. Special Goals and Restrictions

- R3 and R4 may not learn RIP routes directly from each other. All RIP protocol traffic on subnet 172.16.34.0/24 must transit R5.

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 it 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.

6.2. Description of the Topology

- OSPF and RIP are mutually redistributed on R3 and R4.
- EIGRP and OSPF are mutually redistributed on R1.
- Connected networks are redistributed as necessary to provide reachability.

6.3. Expected Behavior and Network Policies

- R1 should have two next hops to networks 172.16.34.0/24 and 172.16.105.0/24.
- If the Ethenet0/2 interface link on R3 or R4 goes down, the remaining link should provide reachability between the remaining interfaces in the OSPF and RIP domains.
- Generally, routers should prefer internal route sources to external route sources.

6.4. Special Goals and Restrictions

- All addresses in this lab must be reachable by all routers.
- All routes must be preferred by their native route sources.

7. BGP Troubleshooting Section (Total: 3 points)

7.1. Troubleshooting Ticket

- Users reported that the IPv4 BGP routing domain does not operate according to the requirements provided it the "BGP 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

- R6 is assigned to AS 600. R1, R4, and R5 are assigned to AS 100.
- AS 100 is configured as a BGP confederation. R1 is assigned to AS 65001. R4 and R5 are assigned to AS 65002.
- R6 is originating the 172.16.106.0/24 prefix into BGP.
- R1 is originating the 172.16.101.0/24 prefix into BGP.

7.3. Expected Behavior and Network Policies

- R5 must learn prefixes that include only the following in their AS path and nothing more: "(65001)".

7.4. Special Goals and Restrictions

- BGP filters may be edited, but they cannot be completely removed.

8. IPv6 Troubleshooting Section (Total: 2 points)

8.1. Troubleshooting Ticket

- Users reported that the IPv6 routing domain does not operate according to the requirements provided it 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.

8.2. Description of the Topology

- The IPv6 topology is shown in the "IPv6 IGP" diagram. All routable IPv6 prefixes start with hexadecimal 2001. All routable subnets use a /64 mask. Link-local addresses are manually configured on the links.
- As shown in the "IPv6 IGP" diagram, IPv6 EIGRP for IPv6 is configured on interfaces with prefix 2001:34::/64. The OSPFv3 subnets are as follows:
  - OSPFv3 Area 0 includes interfaces configured with prefixes 2001:101::/64 and 2001:134::/64.
  - Area 103 includes Loopback 103 with prefix 2001:103::/64.
- OSPFv3 and IPv6 EIGRP are mutually redistributed on R3 and R4.

8.3. Expected Behavior and Network Policies

- All routable IPv6 prefixes should be reachable from any other IPv6 interface.
- While all links are active, R1 must have two routes in its forwarding table to networks in the IPv6 EIGRP domain.

8.4. Special Goals and Restrictions

- All networks must be advertised only with their original masks.
- Existing OSPF network types may not be changed.

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

9.1. Troubleshooting Ticket

- Users reported that QoS does not operate according to the requirements provided it 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

- A router MQC implementation is configured on Ethernet interface E0/1.6 of R1.

9.3. Expected Behavior and Network Policies

- For traffic originating on R6 and transiting the VLAN 16 Ethernet interface of R1, the traffic should adhere to the following policy on R1: All ICMP traffic marked with precedence 0 should be re-marked with the IP precedence 2. All DSCP AF11 traffic should get policed with a CIR of 8000 b/s. All ICMP traffic, excluding AF11 traffic, will be dropped.

9.4. Special Goals and Restrictions

- The MQC service policy configuration cannot be removed from R1.

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

10.1. Troubleshooting Ticket

- Users reported that the IP SLA does not operate according to the requirements provided it the “IP SLA 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

- The IP SLAs process is configured for the jitter service on R2 and R6.

10.3. Expected Behavior and Network Policies

- The IP SLAs traffic will activate every 5 minutes.

10.4. Special Goals and Restrictions

- The IP SLAs process will detect delay variation before phone calls do.

