360RSW05-WKB-TA03

Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Exercise Workbook contains 20 challenging scenarios at the Cisco 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 3 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 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 through 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 Domain Name System (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 Cisco Catalyst switches.
    - Verify that all the routers and switches recognize 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 3 Troubleshooting Section

Grading and Duration

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

Note The self-paced labs found in this workbook are assessed using the basic grading rules. Points that are assigned to sections and tasks should be used for self-assessment. Consider taking the full Assessment Labs to assess your readiness level.

Difficulty Level

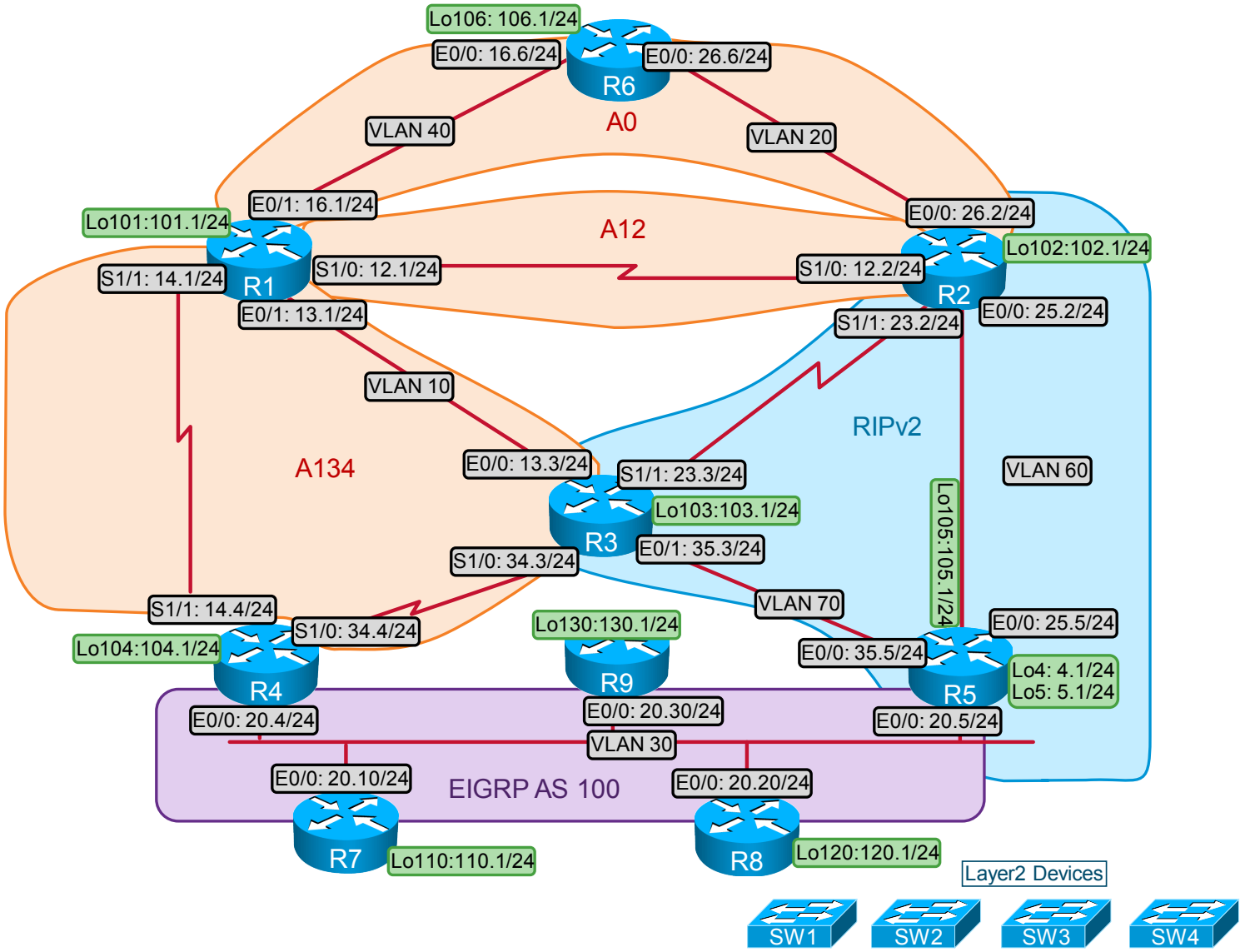
- Difficulty: Intermediate

Restrictions and Goals

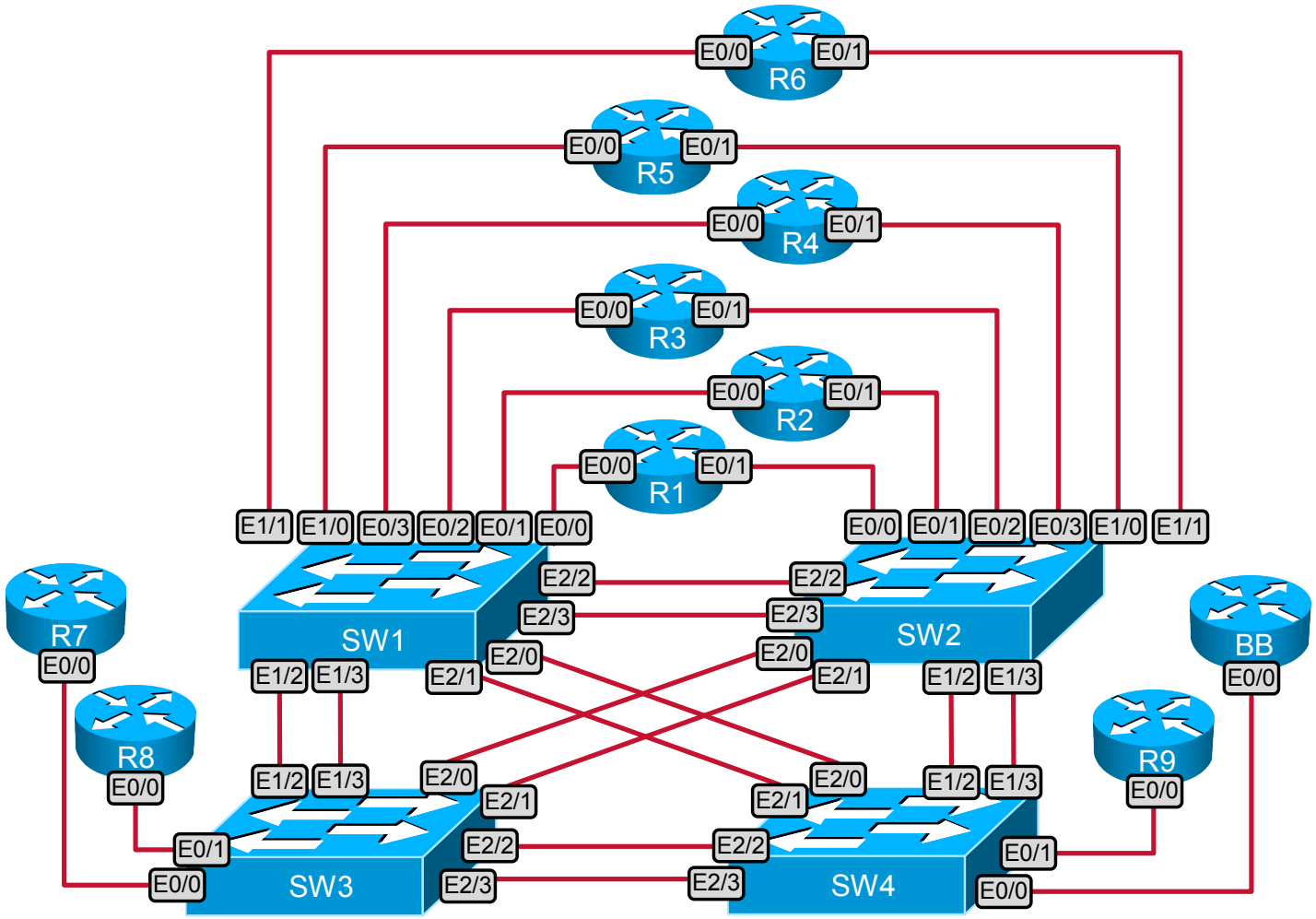
Note Read this section carefully.

- To receive credit for a subsection, you must fully complete the subsection as per requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets displayed in the scenario diagram belong to network 135.15.0.0/16. *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 Border Gateway Protocol (BGP) section need to be reachable by all BGP routers but do not have to be reachable by routers that use only interior gateway protocol (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.

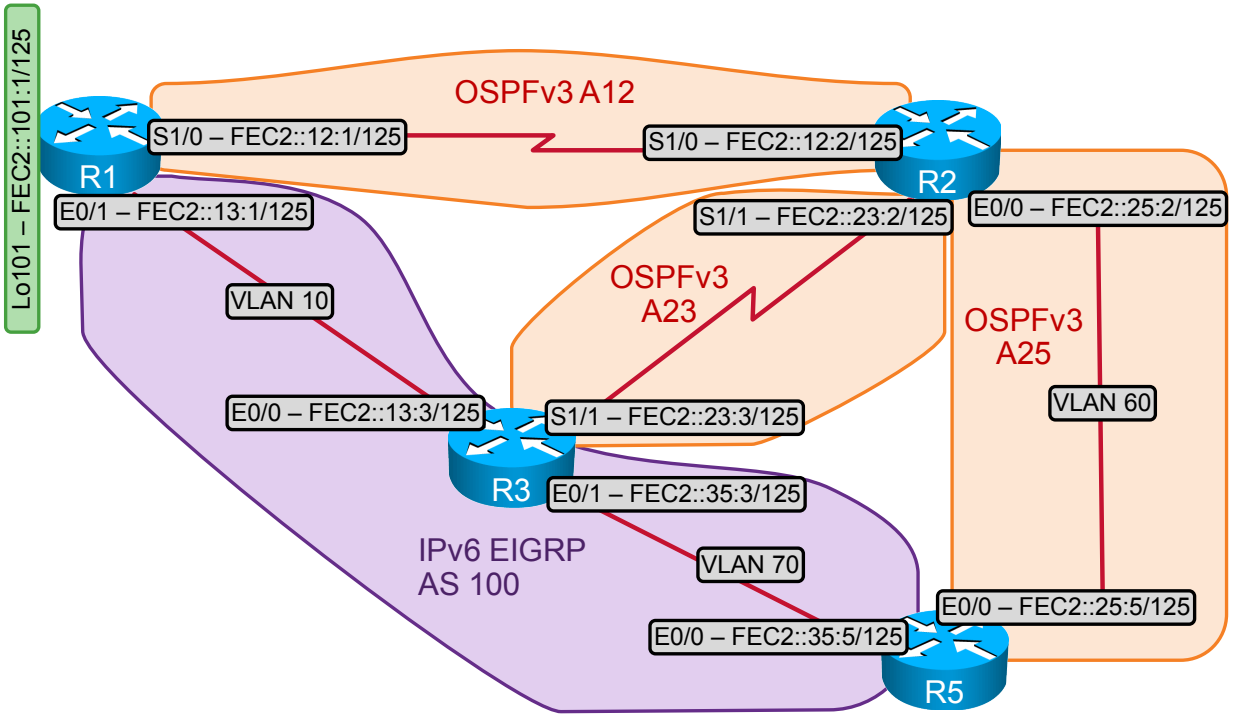
Lab IPv4 IGP



Ethernet Cabling Topology



Lab 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. There is no connectivity from R9 to R7 and R8. The link between SW3 and SW4 does not utilize the 20 Mb/s bandwidth and inactive MAC entries are not processed correctly.
- 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 six VLANs, as shown in the "Lab IPv4 IGP" diagram. No additional VLANs may be configured or used.
- All trunk links are encapsulated with 802.1Q.

1.3. Expected Behavior and Network Policies

- The Ethernet links that are shown in the "Lab IPv4 IGP" diagram must support same-subnet reachability and the routing protocols that are shown.
- All VLANs should be configured only on SW4.

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.
- SW4 should be the root switch for VLAN 30.
- Using a standard protocol, bundle interfaces E2/2 and E2/3 between SW3 and SW4. Only SW3 should actively request negotiation for bundling these interfaces.
- If any switch reboots, it should begin sending VTP updates for the domain CISCO360, hashed by the MD5 password CISCO.
- Activate VTP pruning for all VLANs with the following exception:
  - No pruning is allowed for VLAN 10 between SW1 and SW2.
- For VLAN 30 only, inactive entries in the MAC address table of SW4 should be discarded twice as fast as the default behavior.

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

2.1. Troubleshooting Ticket

- Users reported that the OSPF routing domain does not operate according to the requirements that are provided it the "IPv4 OSPF Troubleshooting" section. The network monitoring application does not show all necessary OSPF neighbor relationships in the OSPF areas. The OSPF cost is not correctly assigned.
- 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 "Lab IPv4 IGP" diagram and listed below. Only these listed subnets should be internal to OSPF:
  - Area 0 includes subnets 135.15.16.0/24 and 135.15.26.0/24.
  - Area 134 includes subnets 135.15.13.0/24, 135.15.14.0/24 and 135.15.34.0/24.
  - Area 12 includes subnet 135.15.12.0/24.

2.3. Expected Behavior and Network Policies

- OSPF must provide stable reachability between all internal subnets.
- On all OSPF devices, OSPF costs should be adapted so that a cost of 1 would be attributed to a 1000-Mb/s link.
- The serial link between R1 and R4 should have an OSPF cost of 65535.
- The following subnets should be redistributed into OSPF:
  - 135.15.101.0/24 on R1 with a metric of 101
  - 135.15.103.0/24 on R3 with a metric of 103
  - 135.15.104.0/24 on R4 with a metric of 104
  - 135.15.106.0/24 on R6 with a metric of 106

2.4. Special Goals and Restrictions

- You may not modify the bandwidth on the Frame Relay link between R1 and R4.
- Only the following subnets should elect a DR or BDR:
  - 135.15.12.0/24
  - 135.15.13.0/24
  - 135.15.16.0/24
- Only the following subnets should automatically discover OSPF neighbors:
  - 135.15.12.0/24
  - 135.15.13.0/24
  - 135.15.14.0/24
- The only interfaces that should remain in the OSPF network type point-to-point are those that are located in subnet 135.15.34.0/24.
- Loopback networks must be advertised with their original masks.

3. EIGRP Troubleshooting Section (Total: 3 points)

3.1. Troubleshooting Ticket

- Users reported that the EIGRP routing domain does not operate according to the requirements that are provided in the "IPv4 EIGRP Troubleshooting" section. The network monitoring application does not show all of the necessary EIGRP neighbor relationships. There is a connectivity issue to the subnet 135.15.110.0/24

- 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.

3.2. Description of the Topology

- As shown in the "Lab IPv4 IGP" diagram, EIGRP AS 100 should operate on VLAN 30.
- Only subnet 135.15.20.0/24 should be internal to EIGRP AS 100.

3.3. Expected Behavior and Network Policies

- The following subnets should be redistributed into EIGRP:
  - 135.15.110.0/24 on R7
  - 135.15.120.0/24 on R8
  - 135.15.130.0/24 on R9
- Devices that are located in EIGRP AS 100 should send hello messages twice as slow as the default behavior.
- Such devices should also authenticate each other using the password CISCO

3.4. Special Goals and Restrictions

- The K1 metric should be equal to 1.
- The K3 metric should be equal to 3.

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 that are provided in the "IPv4 RIP Troubleshooting" section. R2 does not show any RIP prefixes in the routing table.
- 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 version 2 operates between routers R2, R3, and R5, as shown in the "Lab IPv4 IGP" diagram.

4.3. Expected Behavior and Network Policies

- R5 should advertise the best summary address for subnets 135.15.4.0/24 and 135.15.5.0/24.
- RIP updates should be sent only on subnets 135.15.23.0/24, 135.15.35.0/24 and 135.15.25.0/24.
- R2 should have some RIP routes in its routing table.

4.4. Special Goals and Restrictions

- R2 should deny all RIP updates that are received directly from R5.
- R5 should deny all RIP updates that are received directly from R2.
- No access list is allowed.
- No route map is allowed.
- The command **distribute-list prefix-list** is not allowed.
- The configuration should be done on R2 and R5.

5. IPv4 Redistribution Troubleshooting Section (Total: 2 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. The EIGRP AS 100 devices cannot communicate with 135.15.104.1.
- 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 R2 and R3.
- EIGRP and RIP are mutually redistributed on R5 only.

5.3. 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.

5.4. Special Goals and Restrictions

- No redistribution into EIGRP is allowed on R4.
- You may not configure any dynamic protocol on any additional interface from those that are indicated in the "Lab IPv4 IGP" diagram.

6. Security Troubleshooting Section (Total: 3 points)

6.1. Troubleshooting Ticket

- Users reported that network security does not operate according to the requirements that are 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

- Using a reflexive access list, configure R4 so that hosts in the network 135.15.20.0/24 are permitted to reach specific resources.

6.3. Expected Behavior and Network Policies

- The only permitted resources are SSL, HTTP, and Telnet servers.

6.4. Special Goals and Restrictions

- Ensure that hosts located in the network 135.15.20.0/24 can ping any device and reply to pings that are received from any device.

7. IPv6 Troubleshooting Section (Total: 3 points)

7.1. Troubleshooting Ticket

- Users reported that the IPv6 network does not operate according to the requirements that are provided it the "IPv6 Troubleshooting" section. Users complain that they can see the traffic that is forwarded from R5 to the IPv6 application server. Also, R5 does not prefer the route to FEC2::101:0/125 via IPv6 EIGRP, though it should.
- 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 "Lab IPv6 IGP" diagram.
- All routable IPv6 prefixes start with hexadecimals FEC2.
- IPv6 EIGRP AS 100 is configured on VLAN 10 and VLAN 70.
- The Loopback101 IPv6 network is redistributed to IPv6 EIGRP AS 100 on R1.
- OSPFv3 is configured as follows:
  - Area 23 on prefixes FEC2::23:0/125, between routers R2 and R3.
  - Area 12 on prefixes FEC2::12:0/125, between routers R1 and R2.
  - Area 25 on prefixes FEC2::25:0/125, between routers R2 and R5.
- OSPFv3 and IPv6 EIGRP AS 100 are mutually redistributed on R3.

7.3. Expected Behavior and Network Policies

- All routable IPv6 prefixes should be reachable from any other IPv6 interface.
- Ensure that R5 prefers the route to FEC2::101:0/125 via IPv6 EIGRP.

7.4. Special Goals and Restrictions

- All networks must be advertised with only their original masks.
- An IPv6 application server with confidential data is located on VLAN 70, with the IP address FEC2::35:98/125. The IPv6 access list is configured on R5 to ensure that the IPv6 user data traffic is blocked to this server on the Ethernet0/0 interface.

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

- On R1, ensure that traffic that is sent out of serial interface S1/0 is given specific bandwidth in times of congestion according to the following specifications:
  - HTTP traffic should get at least 25 percent of the available bandwidth.
  - SNMP traffic should get at least 20 percent of the available bandwidth.
  - NTP traffic should get at least 5 percent of the available bandwidth.

8.3. Expected Behavior and Network Policies

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

8.4. Special Goals and Restrictions

- Only Modular QoS CLI (MQC) is allowed.
- No access list is allowed for this section.

9. IP Services Troubleshooting Section (Total: 3 points)

9.1. Troubleshooting Ticket

- Users reported that the IP services do not operate according to the requirements that are provided in the "IP Services Troubleshooting" section. The clock on R2 is not synchronized with the NTP server.

- 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 and R6 should be synchronized via NTP.

9.3. Expected Behavior and Network Policies

- R6 should behave as the NTP server for R2.

9.4. Special Goals and Restrictions

- R2 should expect NTP messages to be authenticated.
- Use the MD5 password TIME for authentication purposes.

