360RSW05-WKB-TA10

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 10 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 10 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

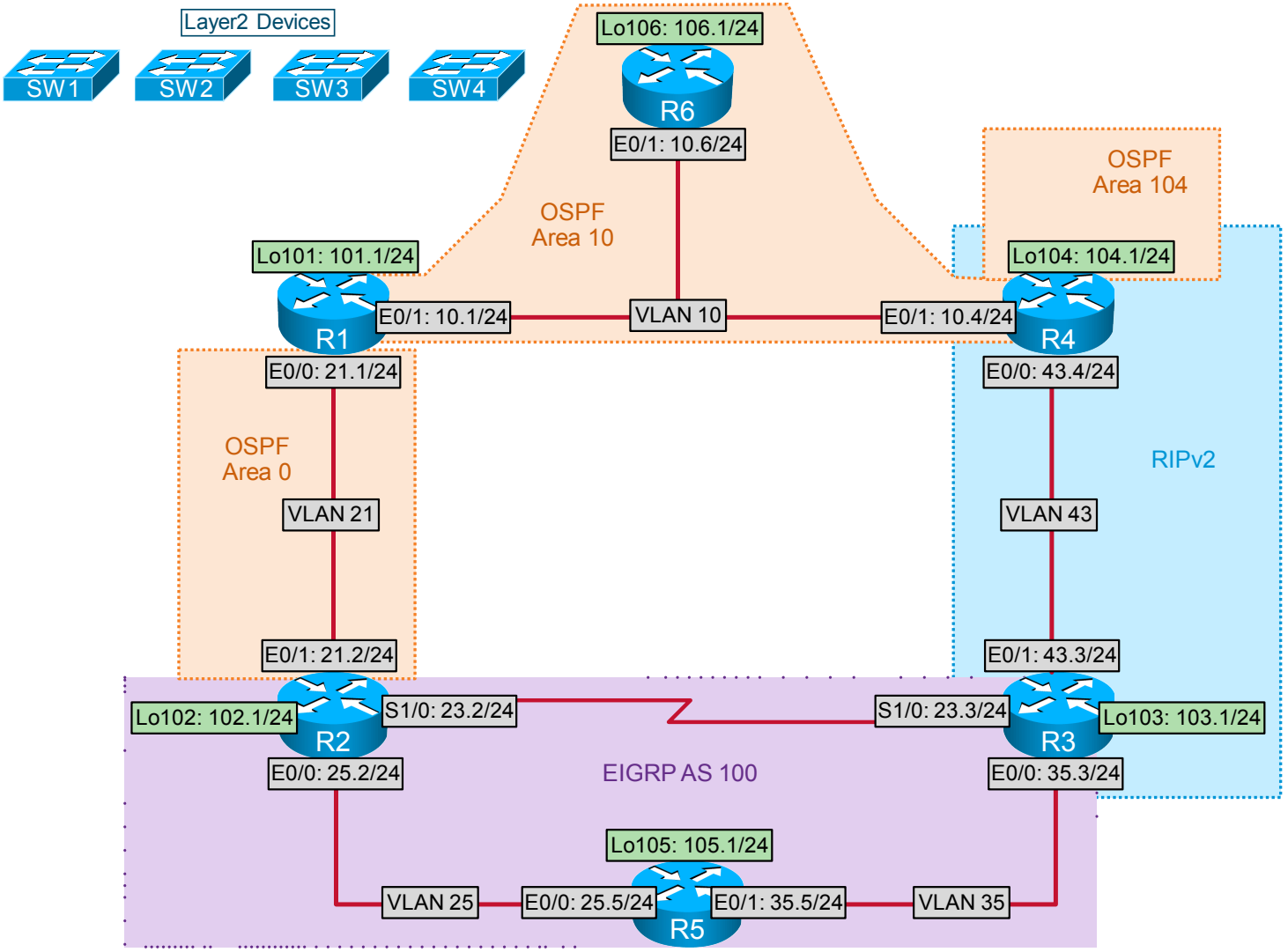
- Difficulty: Intermediate

Restrictions and Goals

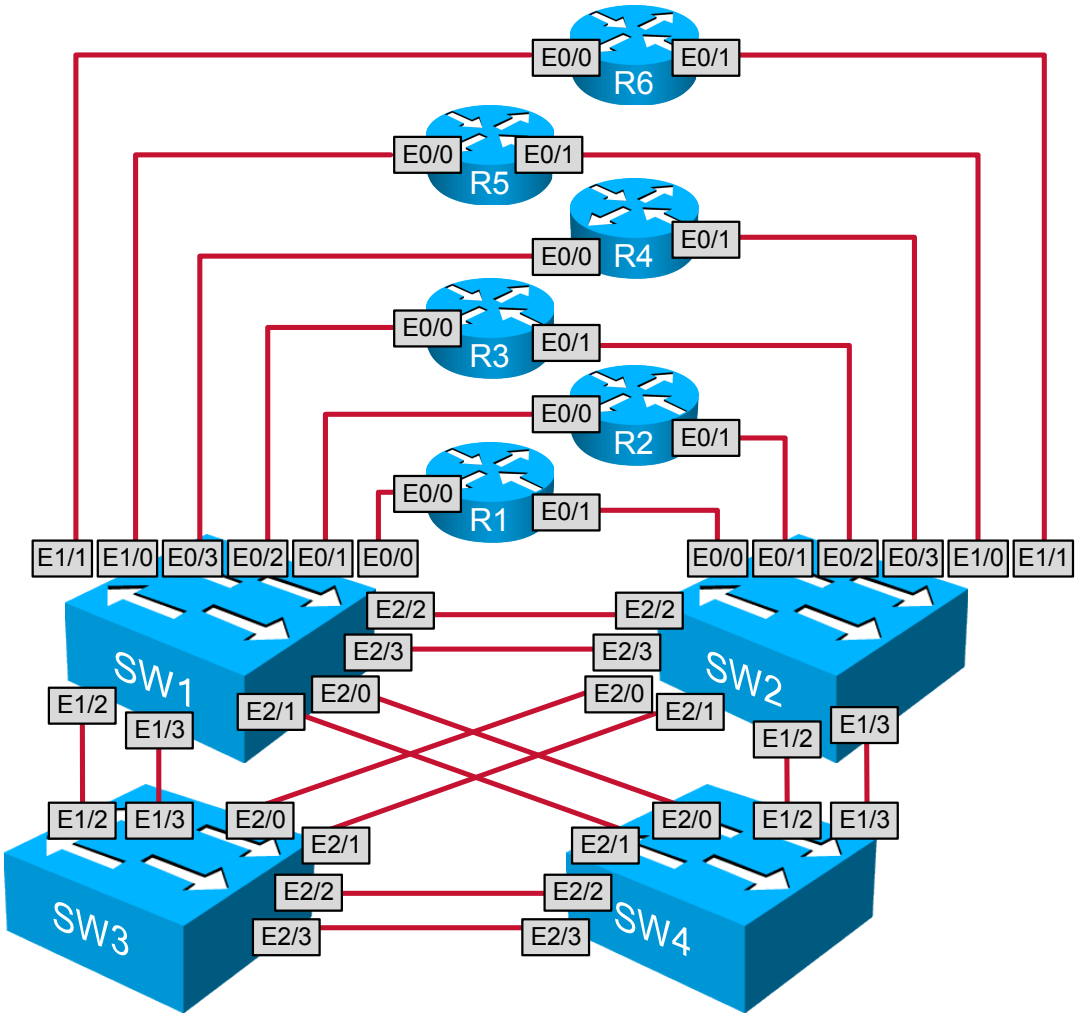
Note Read this section carefully.

- 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**).
- 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.
- Do not create new interfaces to fulfill IGP requirements, and 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



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 that are used for the IP connectivity, as shown in the "IPv4 IGP" diagram. No other VLANs may be used.
- All trunk links connecting two switches are encapsulated with 802.1Q.

1.3. Expected Behavior and Network Policies

- The Ethernet links shown in the "IPv4 IGP" diagram 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.
- All switch ports are access, except the E2/3 link between SW1 and SW2. Only VLANs 35 and 43 are allowed on this trunk.
- SW1 is the root bridge for VLAN 43 and SW2 is the root bridge for VLAN 35.
- If the link between the E2/3 interfaces of SW1 and SW2 becomes unavailable, VLAN 43 packets should be forwarded via SW3 and VLAN 35 packets should be forwarded via SW4.
- All links that are administratively down must remain so.

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 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 as listed below. Only these listed subnets should be internal to OSPF.
  - Area 0 includes subnet 172.16.21.0/24.
  - Area 10 includes subnets 172.16.10.0/24 and 172.16.106.0/24.
  - Area 104 includes subnet 172.16.104.0/24.

2.3. Expected Behavior and Network Policies

- OSPF must provide stable reachability between all internal subnets.

- All OSPF-speaking routers assigned to the backbone must be secured with the most secure level of authentication using the string CISCO.

2.4. Special Goals and Restrictions

- Retain the preconfigured OSPF network types on all nonloopback interfaces on R2.
- Do not remove or alter access list 10 or its associated distribute list on R4.
- Do not change the access list 111 configuration on R1 and R4. This restriction applies to all tickets.

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 100 should operate over the Serial link subnet as well as VLAN 25 and VLAN 35.
- As indicated in the "IPv4 IGP" diagram, the EIGRP routing domain possesses redundant paths for routes learned within the domain.

3.3. Expected Behavior and Network Policies

- Since the EIGRP routing domain possesses redundant paths, make sure that all paths are used and load balancing is maintained on R5 for the 172.16.23.0/23 subnet.

3.4. Special Goals and Restrictions

- No commands related to the EIGRP configuration on R5 can be removed.

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 version 2 operates between routers R3 and R4 on VLAN 43 as shown in the "IPv4 IGP" diagram.

4.3. Expected Behavior and Network Policies

- Both OSPF and EIGRP routes should be redistributed into RIP; however, RIP should not act as a transit routing domain.

4.4. Special Goals and Restrictions

- No access list is allowed within a router RIP configuration mode.
- The use of the **distance** command is not allowed.

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.
- 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 R4.
- EIGRP and RIP are mutually redistributed on R3.
- OSPF and EIGRP are mutually redistributed on R2.

5.3. Expected Behavior and Network Policies

- All devices should be able to reach all subnets.
- Perform **redistribute connected** where required and not restricted by the scenario.

5.4. Special Goals and Restrictions

- All restrictions related to redistribution specified in previous sections must be observed.
- You may not configure any additional dynamic routing protocols on any interface other than those indicated in the "IPv4 IGP" diagram.
- Use the route maps preconfigured with the **redistribute** commands within OSPF. Set the metric to the highest value while still allowing the external OSPF routes to be advertised.

6. Security Troubleshooting Section (Total: 3 points)

6.1. Troubleshooting Ticket

- Users reported that 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

- Configure an inbound extended access list on the E0/1 interface of R6 to permit only traffic generated for ping, Telnet, and any control plane traffic used on R6 for this scenario.

6.3. Expected Behavior and Network Policies

- You should be able to ping R6, R6 should be reachable via Telnet, and all of the routing protocols that use this interface should be fully operational.

6.4. Special Goals and Restrictions

- Limit traffic permitted by this access list to only the traffic specified above.

7. BGP Troubleshooting Section (Total: 3 points)

7.1. Troubleshooting Ticket

- Users reported that the BGP network does not operate according to the requirements provided in 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

- Configure an EBGP neighbor relationship between R2 and R4 using 172.16.102.1 and 172.16.104.1 as the update-source addresses.
- Place R2 in AS 200 and R4 in AS 400.

7.3. Expected Behavior and Network Policies

- Maintain a stable, steady-state BGP neighbor relationship between R2 and R4.
- Have R2 and R4 exchange the routes 172.16.102.0/24 and 172.16.104.0/24 between the two EBGP speakers.

7.4. Special Goals and Restrictions

- Do not use the **distance** command in this configuration.

8. QoS Troubleshooting Section (Total: 3 points)

8.1. Troubleshooting Ticket

- Users reported that router monitoring 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 the Serial interface of R2, an MQC configuration is configured for traffic policing and congestion management purposes.

8.3. Expected Behavior and Network Policies

- Ensure that DSCP EF traffic is policed to the maximum rate of 100,000 b/s.
- The packet size of the EF traffic is 1,000 bytes.

8.4. Special Goals and Restrictions

- Do not change the interface software bandwidth setting on any interface.
- Use minimally sufficient value in your solution.
- No access list is allowed for this section.

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

9.1. Troubleshooting Ticket

- Users reported that the multicast network does not operate according to the requirements provided in the "IP Multicast 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

- R2 IP address 172.16.21.2 is the source of a multicast ping using group 239.255.1.1.
- PIM sparse mode should be configured on the interfaces associated with the following interfaces:
  - 172.16.21.1
  - 172.16.10.1
  - 172.16.101.1
  - 172.16.10.6
  - 172.16.106.1
  - 172.16.10.4
  - 172.16.104.1
- Routers R1, R4, and R6 are statically configured for rendezvous point 172.16.106.1.
- Multicast clients for group 239.255.1.1 are assigned to the loopback interfaces on R1, R4, and R6.

9.3. Expected Behavior and Network Policies

- All multicast clients should reply to the multicast ping generated by R2.

9.4. Special Goals and Restrictions

- Make sure to explicitly specify the source address for the multicast ping traffic.