360RSW05-WKB-TA06

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 6 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.
- 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 6 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

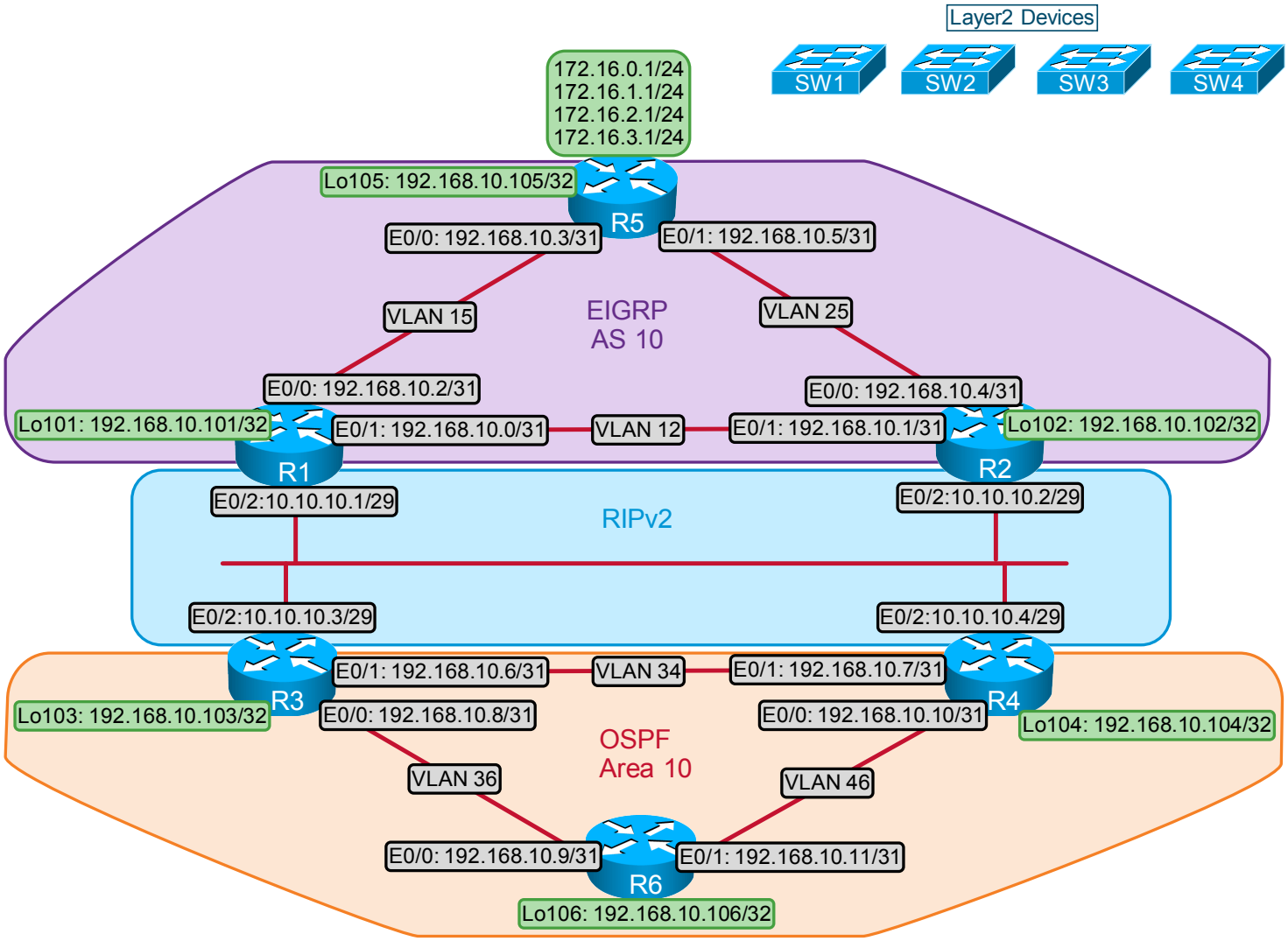
- Difficulty: Intermediate

Restrictions and Goals

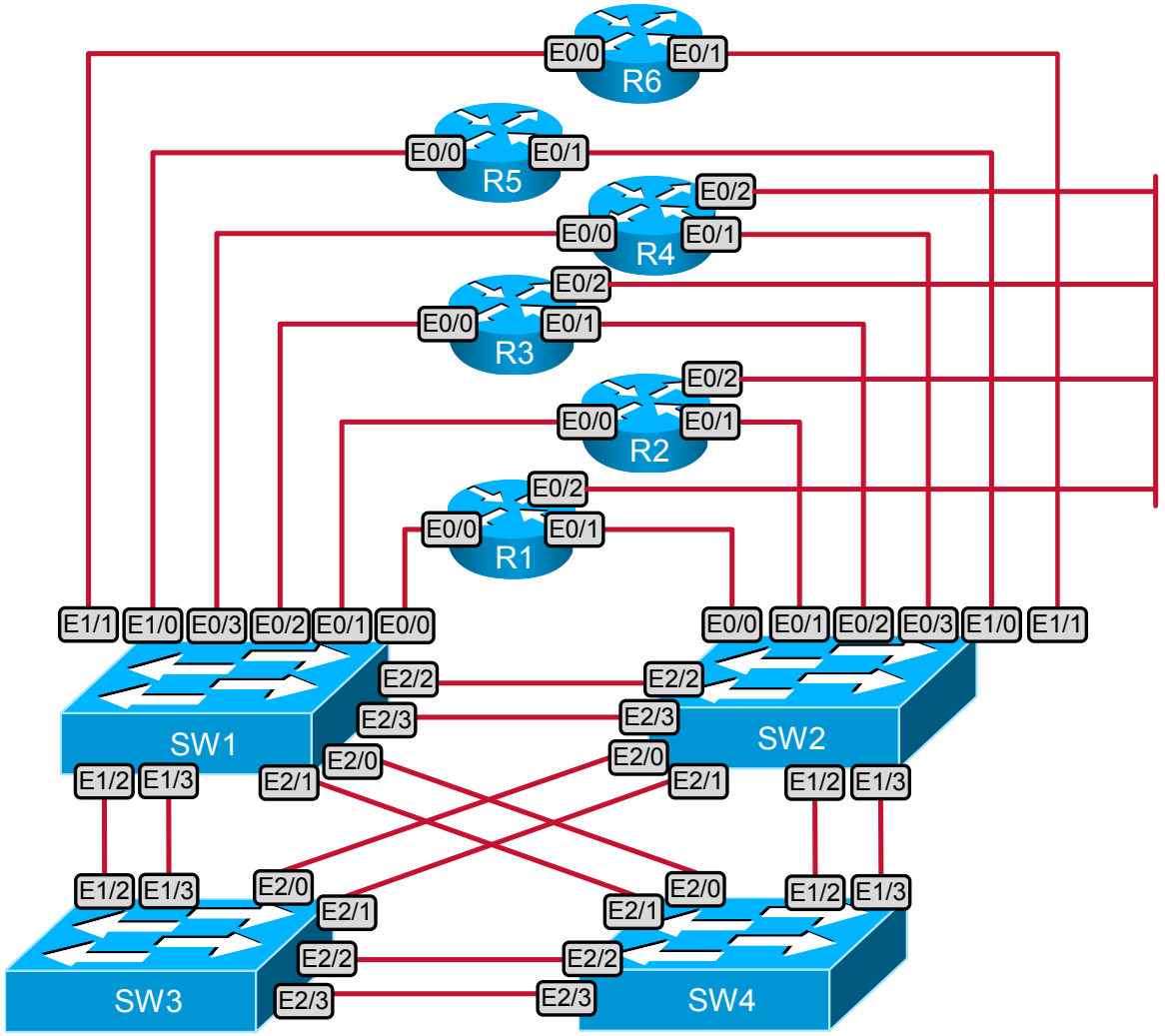
Note Read this section carefully.

- 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 displayed in the IPv4 IGP diagram are /24 networks of 192.168.0.0, except for CustomerA VRF, which is 172.16.0.0.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Advertise loopback interfaces with their original masks.
- All IP addresses 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 the instructions specify 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.

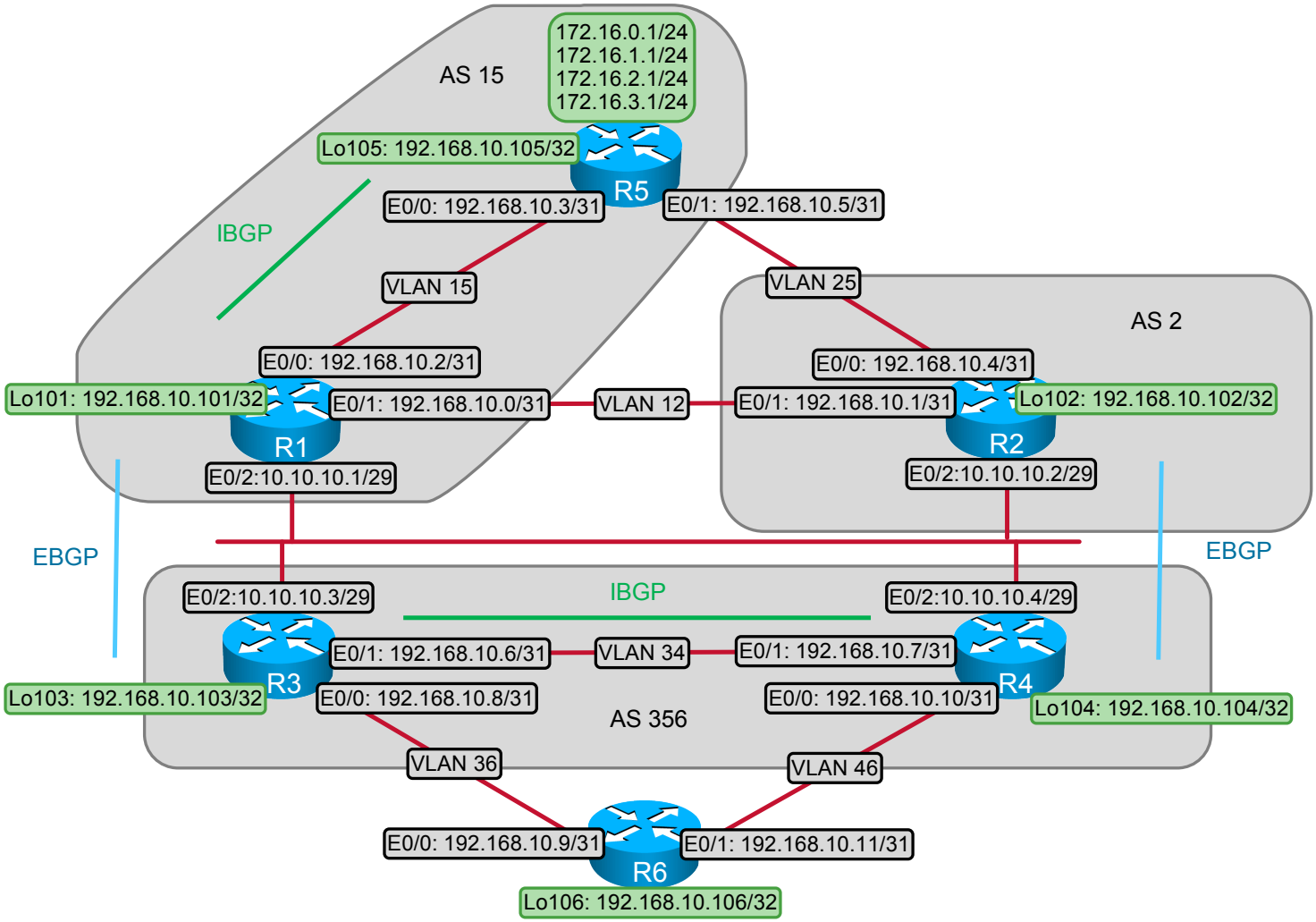
IPv4 IGP Diagram



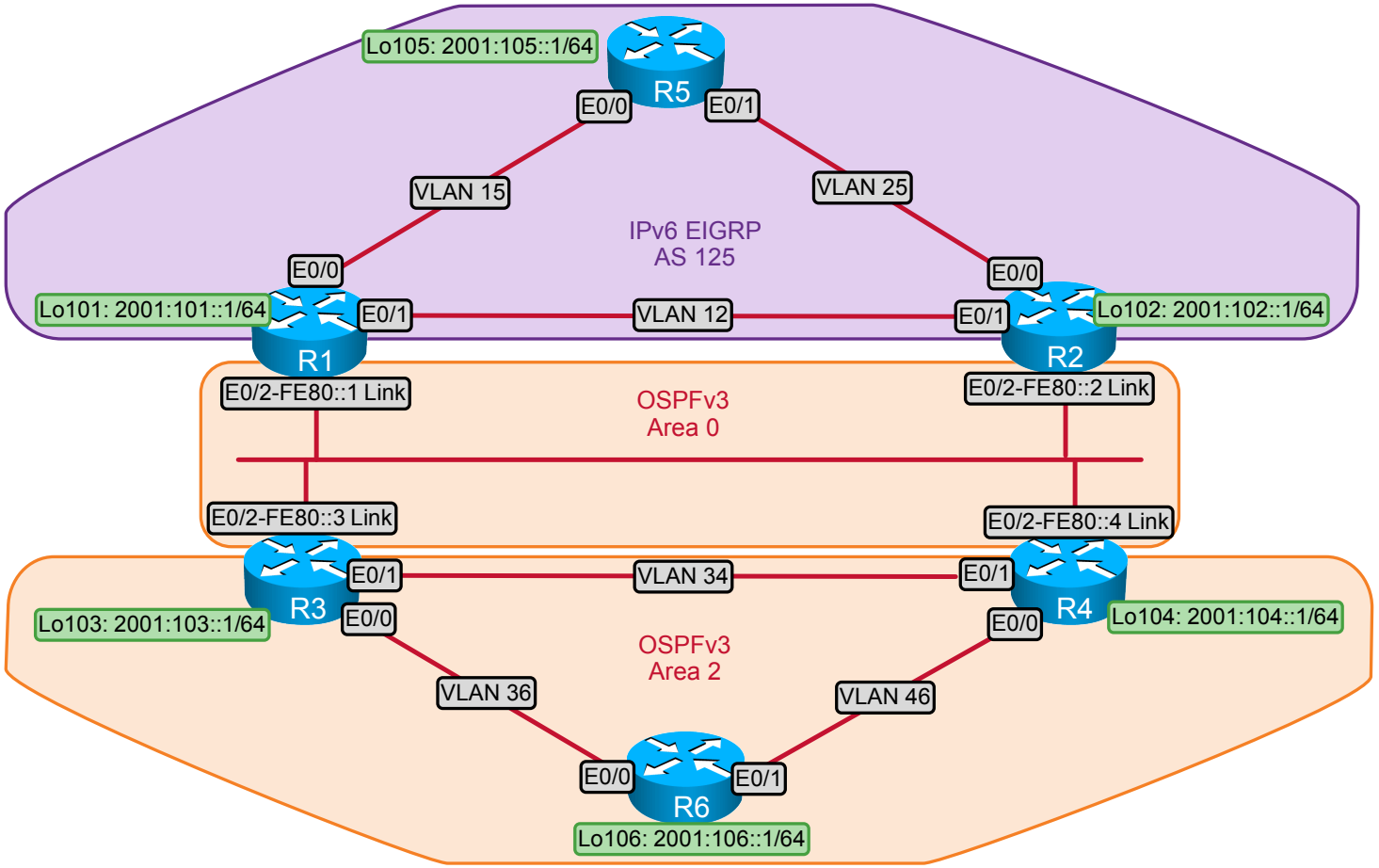
Ethernet Switched Cabling Topology



IPv4 BGP Diagram



IPv6 IGP Diagram



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. Link reachability is broken on R5 and R6. Also, the monitoring system sends notifications about unnecessary VLANs and links detected in the topology.
- 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

- All router-to-switch links are access ports.
- Make sure that the following switch-to-switch configuration links conform to the table below. No additional interswitch links may be active.

VLAN 25	SW1-SW4 E2/0	Dot1q trunk
VLAN 25	SW2-SW4 E1/2	Access
VLAN 46	SW1-SW3 E1/2	Access
VLAN 46	SW2-SW3 E2/0	Access

1.3. Expected Behavior and Network Policies

- Only the interswitch links listed in the "Description of the Topology" subsection should be active.

1.4. Special Goals and Restrictions

- In addition to default VLAN 1, only the necessary VLANs should be created on each switch.

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

- Configure the OSPF area in the diagram.

2.3. Expected Behavior and Network Policies

- OSPF must provide stable reachability between all internal subnets and neighbors.

2.4. Special Goals and Restrictions

- Do not change the originally configured OSPF network types.

3. IPv4 EIGRP Troubleshooting Section (Total: 3 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 10 should operate over VLANs 12, 15, and 25.
- As indicated in the IPv4 IGP diagram, the EIGRP routing domain possesses redundant paths for external routes learned within the domain.

3.3. Expected Behavior and Network Policies

- Authenticate all EIGRP neighbor relationships with the password "san-fran."

3.4. Special Goals and Restrictions

- Redistribute between EIGRP and RIP on routers R1 and R2.

4. IPv4 RIP Troubleshooting Section (Total: 3 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 all routers attached to the 10.10.10.0/29 subnet.

4.3. Expected Behavior and Network Policies

- RIP routes must be exchanged and autosummarized between R1, R2, R3, and R4.

5. IPv4 Redistribution Troubleshooting Section (Total: 3 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

- A set of route redistribution commands has been configured to provide universal connectivity among all routers in this scenario.

5.3. Expected Behavior and Network Policies

- Ensure that there is universal connectivity among all routers in all routing domains.
- Make sure that all external routes are stable in all routing domains.

5.4. Special Goals and Restrictions

- The OSPF domain must see only a /24 summary of the EIGRP domain routes, and the EIGRP domain must see only a /24 summary of the OSPF domain routes.
- Do not configure any static or default route to attain universal connectivity.

6. BGP Troubleshooting Section (Total: 3 points)

6.1. Troubleshooting Ticket

- Users reported that the IPv4 BGP routing domain 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.

6.2. Description of the Topology

- BGP is preconfigured according to the supplied diagram.

6.3. Expected Behavior and Network Policies

- Make sure that the specified BGP updates in the diagram are propagated to all devices displayed on the IPv4 BGP diagram.

6.4. Special Goals and Restrictions

- Use the synchronization method on BGP AS 356.

7. IPv6 Troubleshooting Section (Total: 3 points)

7.1. Troubleshooting Ticket

- Users reported that the IPv6 routing domain does not operate according to the requirements provided in the "IPv6 Troubleshooting" section. OSPFv3 Area 0 restrictions are violated. IPv6 connectivity is broken.

- 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

- Verify that IPv6 is configured according to the supplied diagram.

7.3. Expected Behavior and Network Policies

- Provide full IPv6 connectivity among routable addresses.

7.4. Special Goals and Restrictions

- Do not explicitly configure global IPv6 addresses on any Ethernet links or change configured IPv6 addresses.
- Do not elect a designated router (DR) or a backup designated router (BDR) on the link that connects R1, R2, R3, and R4. No IPv6 multicast traffic is allowed between R1, R2, R3, and R4 for security reasons.

8. IP 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

- QoS configuration is preconfigured on R2 and R5.

8.3. Expected Behavior and Network Policies

- All ICMP traffic leaving R2 port E0/0 must be marked with the IP flash precedence.
- All ICMP traffic arriving on R5 port E0/1 that is marked with the IP flash precedence must be assigned a DSCP of 45.

8.4. Special Goals and Restrictions

- Verify that the pings originating from the R2 Loopback 102 interface and destined to IP address 192.168.10.101 arrive at router R1 with packets marked with a DSCP value of 45.

