

# 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 5

### Troubleshooting Section

---

---

COPYRIGHT 2013, CISCO SYSTEMS, INC. ALL RIGHTS RESERVED. ALL CONTENT AND MATERIALS, INCLUDING WITHOUT LIMITATION, RECORDINGS, COURSE MATERIALS, HANDOUTS AND PRESENTATIONS AVAILABLE ON THIS PAGE, ARE PROTECTED BY COPYRIGHT LAWS. THESE MATERIALS ARE LICENSED EXCLUSIVELY TO REGISTERED STUDENTS FOR THEIR INDIVIDUAL PARTICIPATION IN THE SUBJECT COURSE. DOWNLOADING THESE MATERIALS SIGNIFIES YOUR AGREEMENT TO THE FOLLOWING: (1) YOU ARE PERMITTED TO PRINT THESE MATERIALS ONLY ONCE, AND OTHERWISE MAY NOT REPRODUCE THESE MATERIALS IN ANY FORM, OR BY ANY MEANS, WITHOUT PRIOR WRITTEN PERMISSION FROM CISCO; AND (2) YOU ARE NOT PERMITTED TO SAVE ON ANY SYSTEM, MODIFY, DISTRIBUTE, REBROADCAST, PUBLISH, TRANSMIT, SHARE OR CREATE DERIVATIVE WORKS ANY OF THESE MATERIALS. IF YOU ARE NOT A REGISTERED STUDENT THAT HAS ACCEPTED THESE AND OTHER TERMS OUTLINED IN THE STUDENT AGREEMENT OR OTHERWISE AUTHORIZED BY CISCO, YOU ARE NOT AUTHORIZED TO ACCESS THESE MATERIALS.

---

# Table of Contents

<b>Cisco 360 CCIE R&amp;S Exercise Workbook Lab 5 Troubleshooting Section .....</b>	<b>2</b>
Activity Objectives .....	4
General Lab Instructions .....	4
Difficulty Levels.....	5
<b>Exercise Workbook Lab 5 Troubleshooting Section .....</b>	<b>6</b>
Grading and Duration .....	6
Difficulty Level .....	6
Restrictions and Goals .....	6
1. Switched Network Troubleshooting Section (Total: 3 points) .....	11
1.1. Troubleshooting Ticket.....	11
1.2. Description of the Topology .....	11
1.3. Expected Behavior and Network Policies .....	11
1.4. Special Goals and Restrictions .....	11
2. IPv4 OSPF Troubleshooting Section (Total: 3 points) .....	11
2.1. Troubleshooting Ticket.....	11
2.2. Description of the Topology .....	11
2.3. Expected Behavior and Network Policies .....	12
3. EIGRP Troubleshooting Section (Total: 3 points) .....	12
3.1. Troubleshooting Ticket.....	12
3.2. Description of the Topology .....	12
3.3. Expected Behavior and Network Policies .....	12
3.4. Special Goals and Restrictions .....	12
4. IPv4 RIP Troubleshooting Section (Total: 2 points) .....	12
4.1. Troubleshooting Ticket.....	12
4.2. Description of the Topology .....	12
4.3. Expected Behavior and Network Policies .....	12
4.4. Special Goals and Restrictions .....	12
5. BGP Troubleshooting Section (Total: 3 points) .....	13
5.1. Troubleshooting Ticket.....	13
5.2. Description of the Topology .....	13
5.3. Expected Behavior and Network Policies .....	13
6. IPv4 Redistribution Troubleshooting Section (Total: 2 points) .....	13
6.1. Troubleshooting Ticket.....	13
6.2. Description of the Topology .....	13
6.3. Expected Behavior and Network Policies .....	13
6.4. Special Goals and Restrictions .....	14
7. MPLS Section (Total: 3 points) .....	14
7.1. Troubleshooting Ticket.....	14
7.2. Description of the Topology .....	14
7.3. Expected Behavior and Network Policies .....	14
7.4. Special Goals and Restrictions .....	14
8. Multicast Section (Total: 3 points) .....	14
8.1. Troubleshooting Ticket.....	14
8.2. Description of the Topology .....	14
8.3. Expected Behavior and Network Policies .....	15
8.4. Special Goals and Restrictions .....	15
9. Gateway Redundancy Section (Total: 2 points) .....	15
9.1. Troubleshooting Ticket.....	15
9.2. Description of the Topology .....	15
9.3. Expected Behavior and Network Policies .....	15
9.4. Special Goals and Restrictions .....	15

# 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 5

## 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

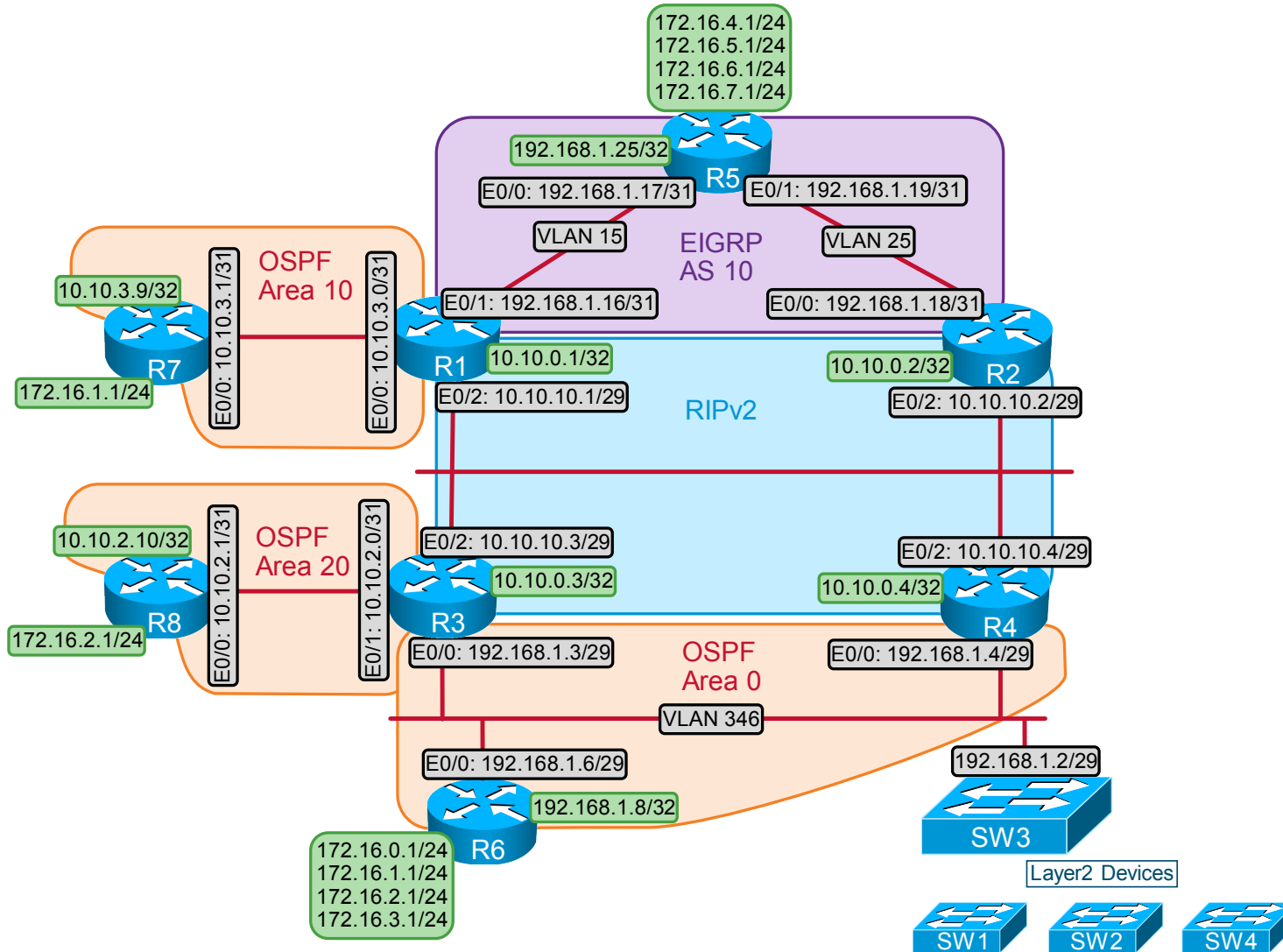
---

**Note** Read this section carefully.

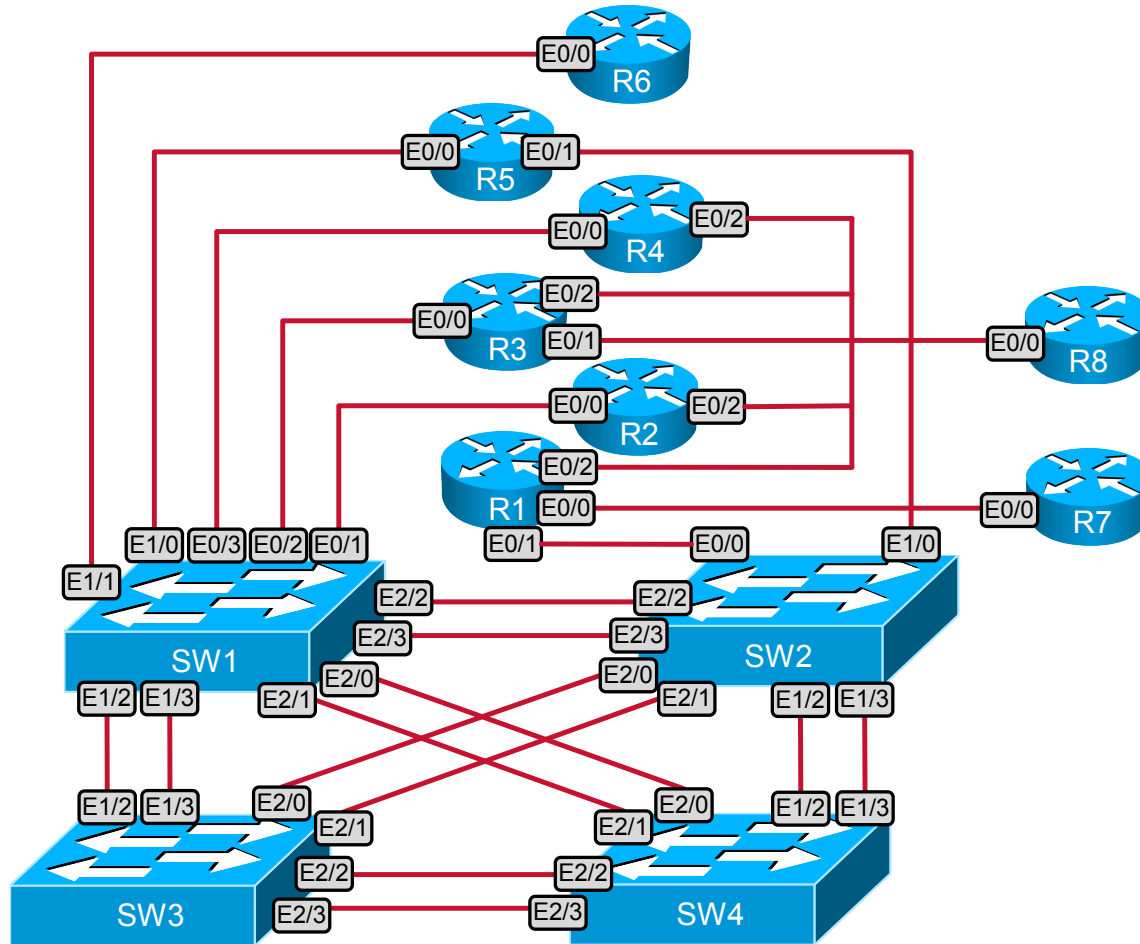
---

- 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.
- Use the IPv4 subnets that are displayed in the "Lab IPv4 IGP" diagram. *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Advertise loopback interfaces with their original masks.
- 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.

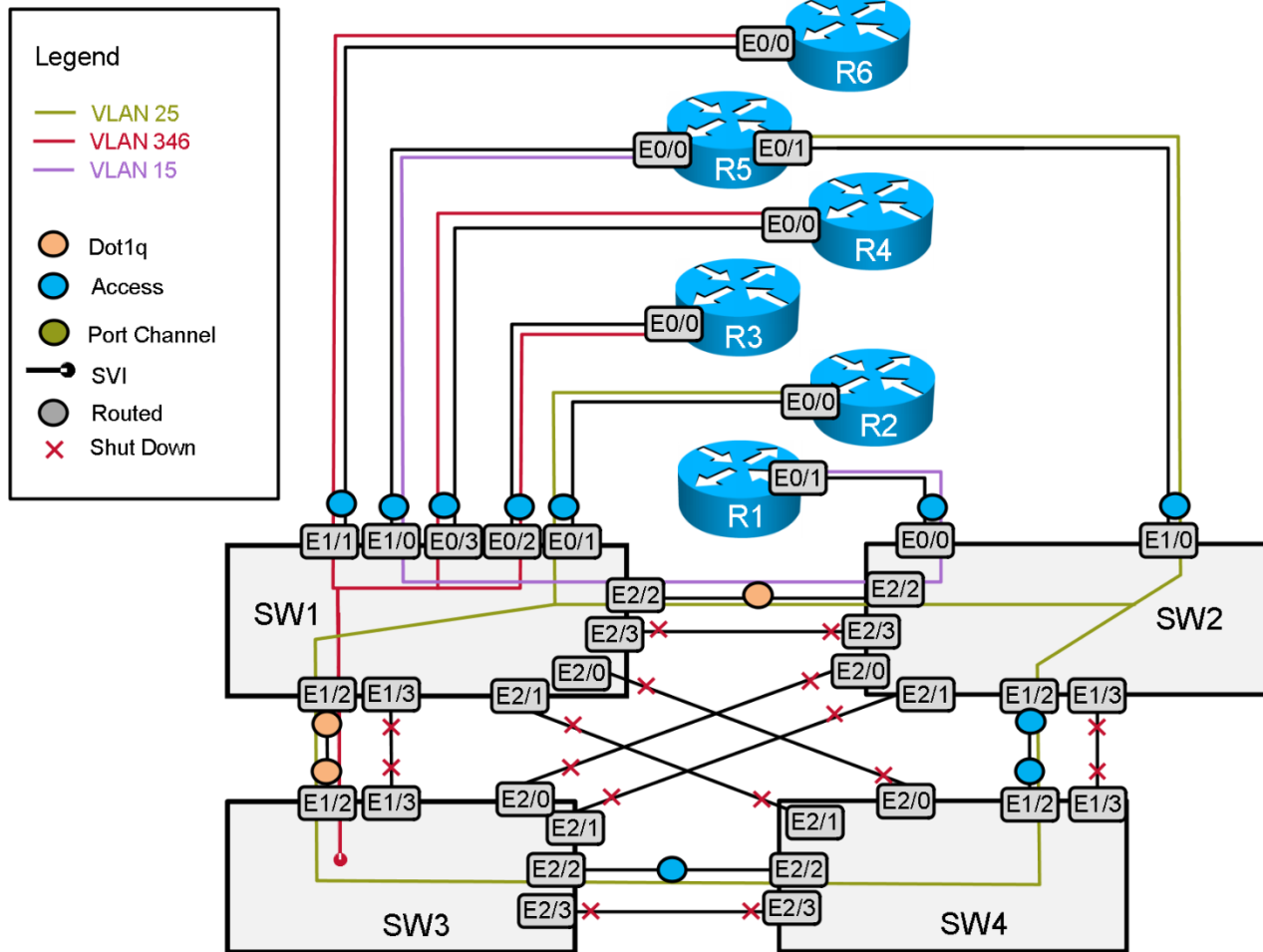
# Lab IPv4 IGP



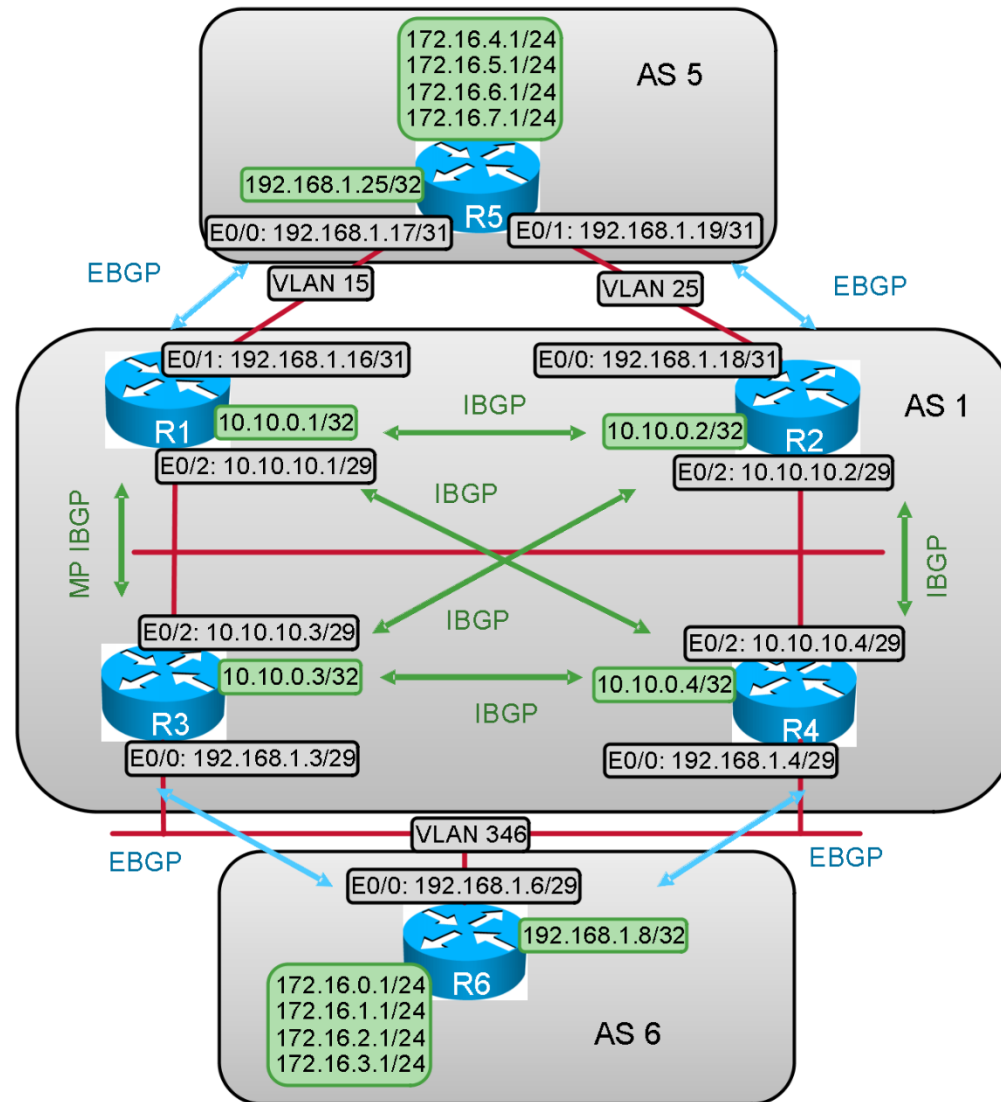
## Ethernet Cabling Topology



## Lab VLANs Topology



## Lab BGP



## 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 that are provided in the “Switched Network Troubleshooting” section. There is no reachability to SW3. Also users detected that VLANs were incorrectly set up on SW1, SW3, and SW4.
- 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 the VLANs that are listed in the supplied “Lab IPv4 IGP” and “Lab Ethernet Topology” diagrams. Make sure that all VLANs are configured and that all port designations are fulfilled according to these diagrams.
- Interfaces should be shut down as indicated on the diagram.

### 1.3. Expected Behavior and Network Policies

- The trunks between SW1 and SW2 and between SW1 and SW3 should permit only the required VLANs.
- All switches are in VTP mode transparent.

### 1.4. Special Goals and Restrictions

- Create only the necessary VLANs.
- Configure VLANs and Ethernet links to precisely match the diagram.

## 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 in the “IPv4 OSPF Troubleshooting” section. The network monitoring application does not show all necessary OSPF neighbor relationships in the OSPF Area 0 and Area 10.
- While resolving this ticket, refer to the “Description of the Topology” and the “Expected Behavior and Network Policies” subsections to determine if your solution is appropriate.

### 2.2. Description of the Topology

- All subnets that would be included in a 192.168.1.0/28 summary should be in OSPF process 1 and Area 0, except for the IP addresses on SW3.
- All subnets that would be included in a 10.10.3.0/24 summary should be in OSPF process 10 and Area 10.
- All subnets that would be included in a 10.10.2.0/24 summary should be in OSPF process 20 and Area 20.

### 2.3. Expected Behavior and Network Policies

- Redistribute subnet 172.16.1.0/24 into OSPF on R7.

- Redistribute subnet 172.16.2.0/24 into OSPF on R8.

### **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 necessary 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.

#### **3.2. Description of the Topology**

- EIGRP is preconfigured on the routers.

#### **3.3. Expected Behavior and Network Policies**

- All subnets that would be included in a 192.168.1.16/28 summary should be in EIGRP AS 10.

#### **3.4. Special Goals and Restrictions**

- No other prefixes should be included as internal EIGRP networks.

### **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. Extra RIP prefixes are leaked to R4.
- 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**

- RIPv2 is preconfigured on the routers.

#### **4.3. Expected Behavior and Network Policies**

- All subnets of 10.0.0.0/8 that are part of the default VRF instance should be included in RIPv2.
- R1 and R2 should advertise only a single best, longest match summary for the routes in the EIGRP domain.
- R3 and R4 should advertise only a single best, longest match summary for the routes in the OSPF process 1 domain.
- A discovery process must be used to determine which routers are running RIPv2.

#### **4.4. Special Goals and Restrictions**

- Ensure that as many interfaces as possible on RIP-speaking routers are made passive.

### **5. BGP Troubleshooting Section (Total: 3 points)**

#### **5.1. Troubleshooting Ticket**

- Users reported that the IPv4 BGP routing domain does not operate according to the requirements that are provided in the “BGP Troubleshooting” section.

- While resolving this ticket, refer to the “Description of the Topology” and the “Expected Behavior and Network Policies” subsections to determine if your solution is appropriate.

## 5.2. Description of the Topology

- In AS 1, a full mesh of IBGP speakers is maintained among R1, R2, R3, and R4. All IBGP peering within AS 1 should use IP addresses that are assigned to loopback interfaces.
- R5 resides in AS 5, and it is peered with R1 and R2 using IP addresses on common subnets.
- R6 resides in AS 6, and it is peered with R3 and R4 using IP addresses on the 192.168.1.0/29 subnet.

## 5.3. Expected Behavior and Network Policies

- BGP AS 1 and BGP AS 6 should not see specific prefixes from BGP AS 5, only the summary prefix.
- R5 should load-share its traffic to the prefix that is advertised on R6.
- R6 should prefer the path through R3 to the prefix that is advertised by R5.

# 6. IPv4 Redistribution Troubleshooting Section (Total: 2 points)

## 6.1. Troubleshooting Ticket

- Users reported that the IPv4 IGP routing domain does not operate according to the requirements that are provided in the “IPv4 Redistribution Troubleshooting” section. RIP routers do not meet the requirement for the internal forwarding path preference.
- 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

- A set of route redistribution commands has been configured to provide universal connectivity among all routers in this scenario:
  - RIP and EIGRP are mutually redistributed on R1 and R2.
  - RIP and OSPF process ID 1 are redistributed on R3 and R4.

## 6.3. 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.
- All routers should prefer internal paths over external paths.

## 6.4. Special Goals and Restrictions

- Do not configure any static or default route to attain universal connectivity.

# 7. MPLS Troubleshooting Section (Total: 3 points)

## 7.1. Troubleshooting Ticket

- Users reported that the MPLS network does not operate according to the requirements that are provided in the “MPLS Troubleshooting” section. R7 can not communicate with the MPLS network.
- 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

- An MPLS Layer 3 VPN is deployed between R1 and R3.

## 7.3. Expected Behavior and Network Policies

- Use MPLS Layer 3 VPNs to provide reachability between the VPN1 subnets that are specified below.

## 7.4. Special Goals and Restrictions

- R7 should have subnets 10.10.2.0/31 and 10.10.2.10/32 as OSPF inter-area routes and subnet 172.16.2.0/24 as an OSPF external route.
- R8 should have subnets 10.10.3.0/31 and 10.10.3.9/32 as OSPF inter-area routes and subnet 172.16.1.0/24 as an OSPF external route.

## 8. Multicast Troubleshooting Section (Total: 3 points)

### 8.1. Troubleshooting Ticket

- Users reported that the multicast network does not operate according to the requirements that are provided in the “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.

### 8.2. Description of the Topology

- R1 and R2 are redundant RP candidates and BSR candidates with the default priorities.
- R5 should respond when R6 sources a ping from E0/0 to any of these eight IP multicast IP addresses:  
239.255.1.0  
239.255.1.1  
239.255.1.2  
239.255.1.3  
239.255.1.4  
239.255.1.5  
239.255.1.6  
239.255.1.7

### 8.3. Expected Behavior and Network Policies

- Use the PIMv2 hash-length parameter to enable RP 10.10.0.1 to be the primary RP for half of these groups and RP 10.10.0.2 to be the primary RP for the other four groups.

### 8.4. Special Goals and Restrictions

- Do not change routing tables, create static mroutes, move the RPs, or add PIM to any interface to meet these requirements.

## 9. Gateway Redundancy Troubleshooting Section Total: 2 points

### 9.1. Troubleshooting Ticket

- Users reported that the gateway redundancy does not operate according to the requirements that are provided in the “Gateway Redundancy 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

- VRRP is configured between R3 and R4 on VLAN 346.

### 9.3. Expected Behavior and Network Policies

- SW3 must use the VRRP address as its default gateway.

### 9.4. Special Goals and Restrictions

- R4 should be the master and R3 should be backup.
- If R4 E0/2 goes down, R3 should take over as master.