360RSW05-WKB-CA05

Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Version 5 Exercise Workbook contains 20 challenging scenarios at the Cisco CCIE level that can be used for rigorous self-paced practice. The Exercise Workbook scenarios include both a troubleshooting section and a configuration section.

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 Configuration 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, and 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 Switched Cabling Topology" diagram and the IPv4 and IPv6 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 tasks 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 Configuration Section

Grading and Duration

- Configuration lab duration: 6 hours
- Configuration lab maximum score: 76 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

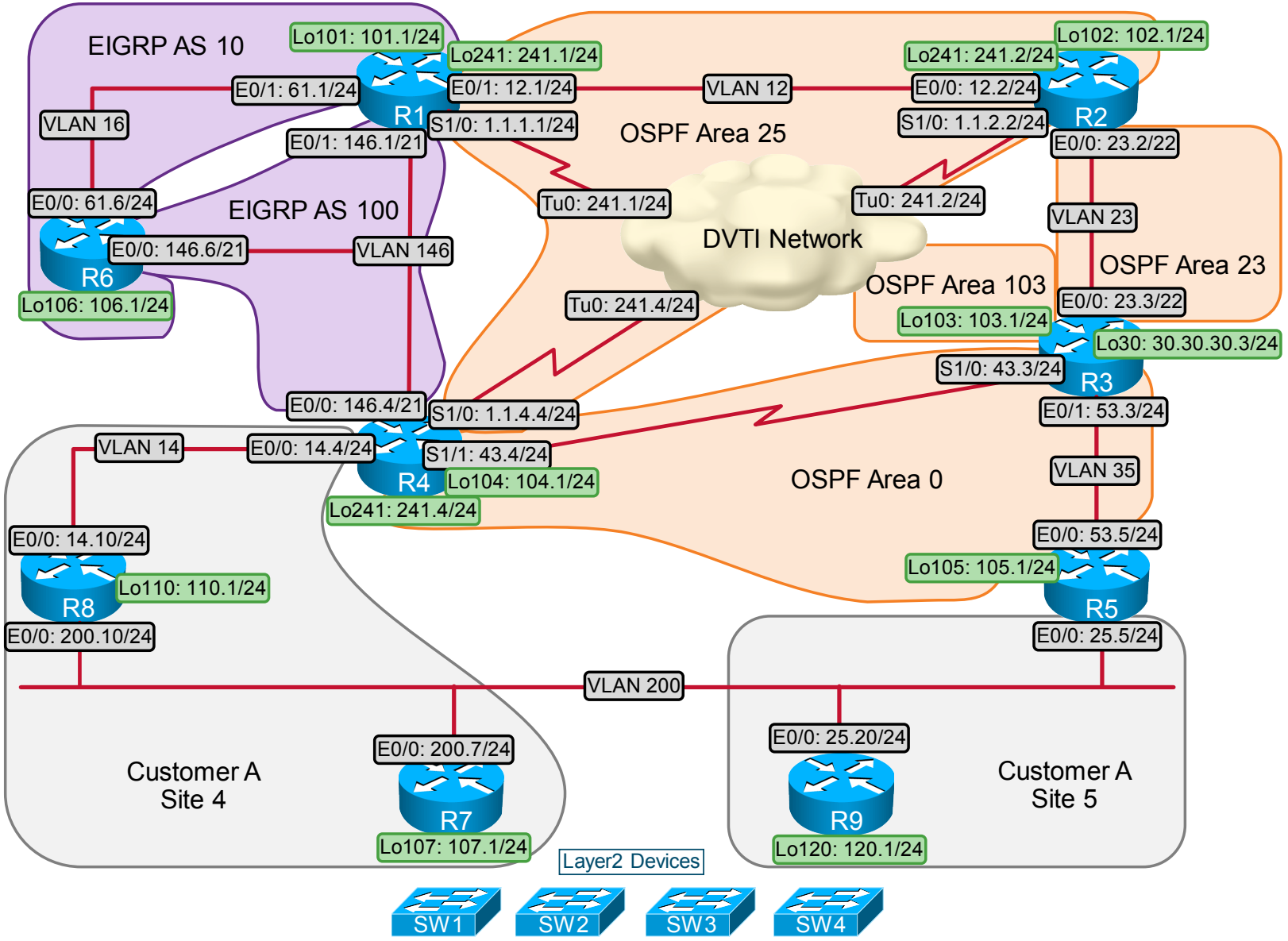
- Difficulty: Intermediate

Restrictions and Goals

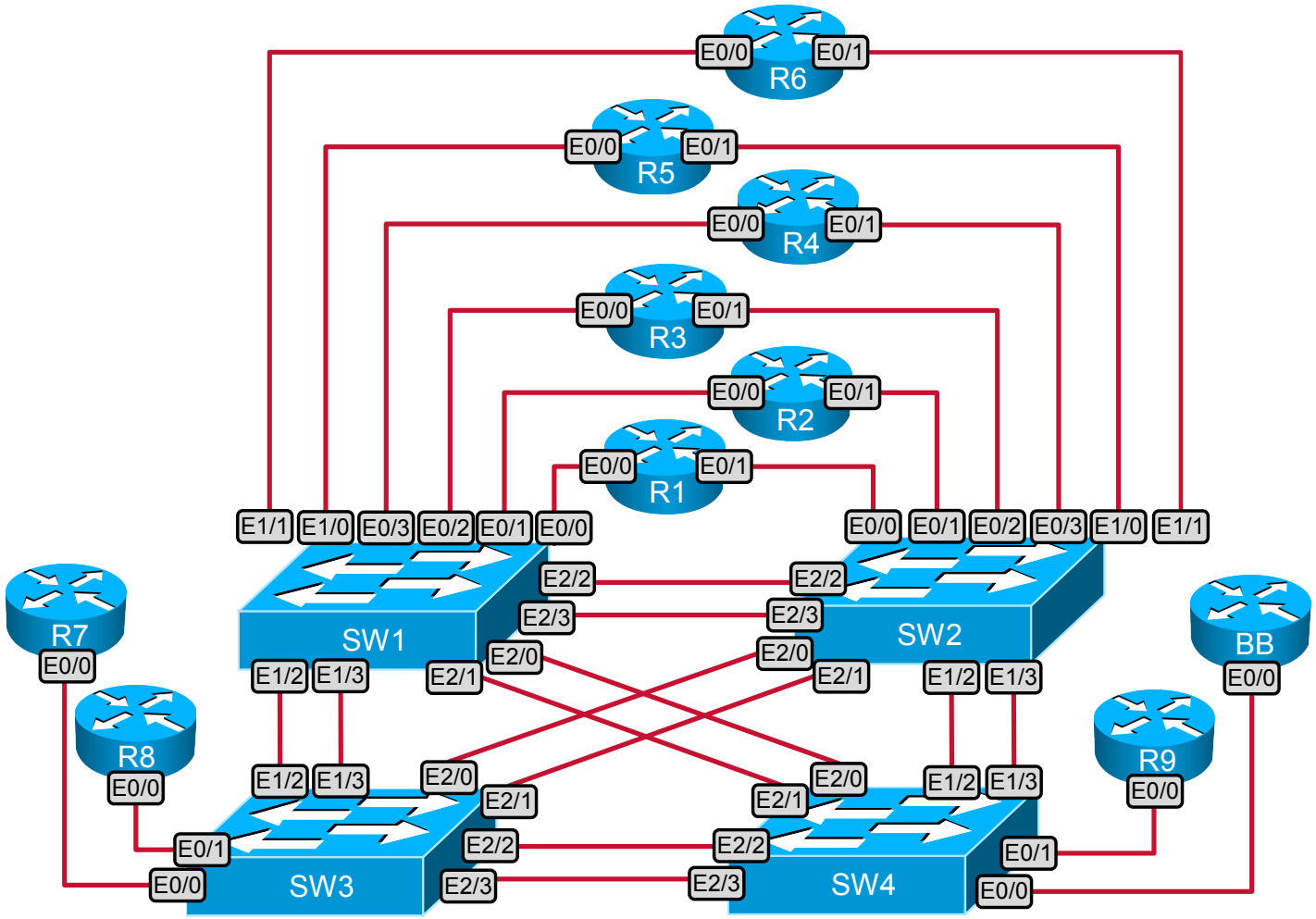
Note Read this section carefully.

- To receive any credit for a subsection, you must fully complete the subsection as per the requirements. You will not receive partial credit for partially completed sections.
- IP subnets displayed in the scenario diagram belong to network 172.16.0.0/16.
- Do not configure any static routes. Do not modify any preconifugred static routes.
- Make sure all IP version 4 (IPv4) and IP version 6 (IPv6) loopback interfaces are advertised with their original masks unless otherwise specified. The DVTI loopback interfaces are excluded from this requirent.
- Make sure all IPv4 interfaces in the diagram are reachable within this internetwork. The 1.1.0.0./16 range is excluded from this requirement.
- IP subnets in the CustomerA VPN do not have to be reachable from outside the VPN.

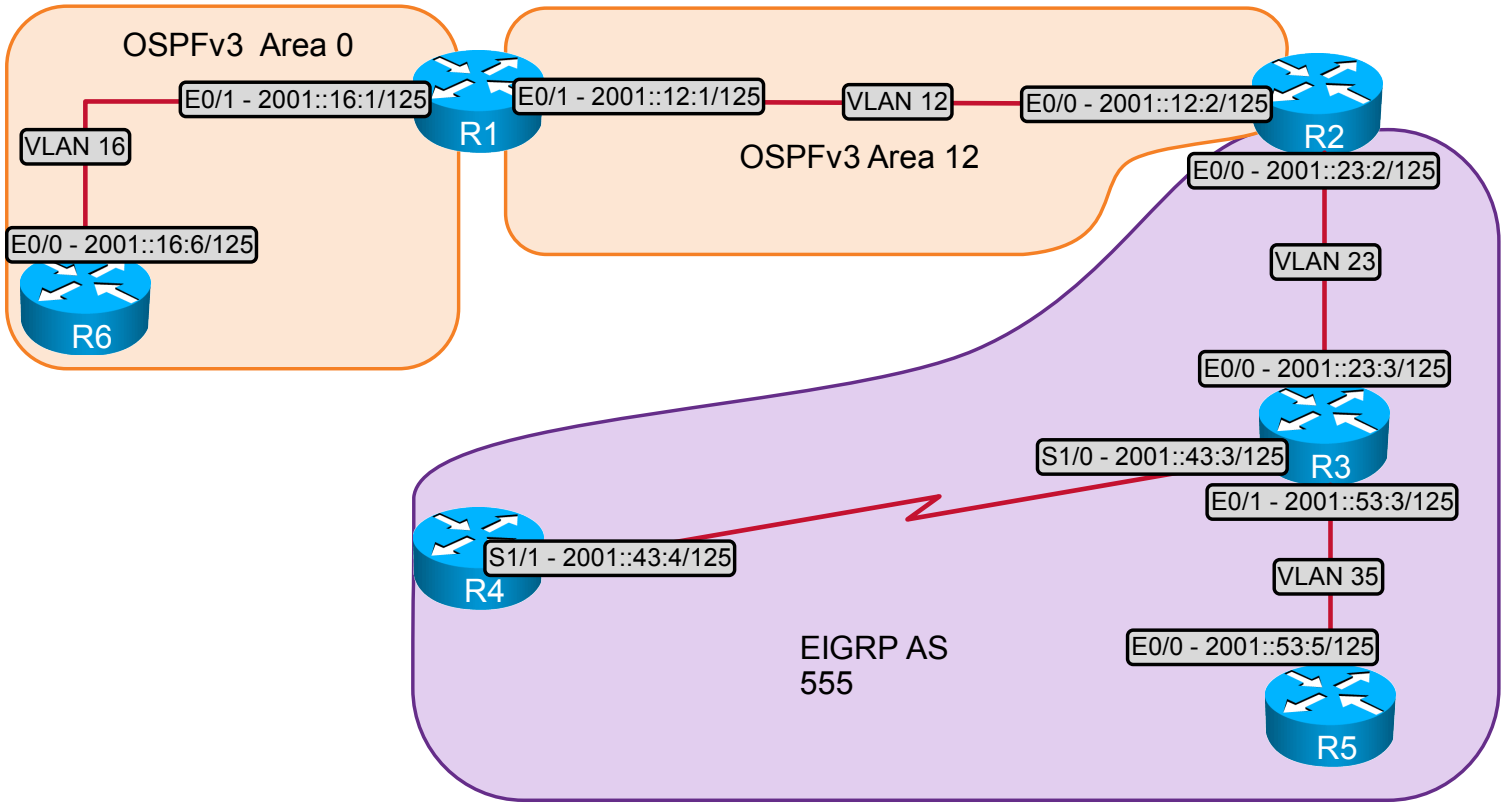
IPv4 IGP Diagram



Ethernet Switched Cabling Topology



IPv6 IGP Diagram



1. Switch Configuration Section (Total: 12 points)

1.1. Configure VLANs (Basic: 2 points)

- On SW1 and SW2, create the VLANs that are referenced in the following table.

SW1 and SW2 VLANs

VLAN	VLAN Name
VLAN 12	-
VLAN 14	-
VLAN 16	-
VLAN 23	-
VLAN 35	-
VLAN 146	-
VLAN 200	-

- On SW3 and SW4, create the VLANs that are referenced in the following table.

SW3 and SW4 VLANs

VLAN	VLAN Name	Switch
VLAN 14	-	SW3
VLAN 110	-	
VLAN 120	-	
VLAN 200	-	
VLAN 999	-	
VLAN 110	-	SW4
VLAN 120	-	
VLAN 200	-	
VLAN 999	-	

- Configure the switch-to-router connections in the following table. Use dot1q trunk links where necessary; otherwise, configure an access VLAN.

Switch-to-Router Connections

Switch	Router	VLAN
SW1	R2	VLAN 12, VLAN 23
SW1	R3	VLAN 23
SW1	R4	VLAN 14, VLAN 146
SW1	R5	VLAN 35, VLAN 200
SW1	R6	VLAN 16, VLAN 146
SW2	R1	VLAN 12, VLAN 16, VLAN 146
SW2	R3	VLAN 35
SW3	R7	VLAN 200
SW3	R8	VLAN 14, VLAN 200
SW4	R9	VLAN 200

- VLAN Trunking Protocol (VTP) mode should be transparent on all switches.

1.2. Tune Switch-to-Router Links (Basic: 2 points)

- Allow only the necessary VLANs on the switch-to-router trunks.

1.3. Control Switch-to-Switch Links (Basic: 2 points)

- The ports that are listed in the following table must be administratively shut down. Verify that they remain in the shutdown state.

Ports to Be Shut Down

Switch	Port
SW1	1/3 2/1
SW2	1/3 2/0 2/1
SW3	1/3 2/0 2/1
SW4	1/3 2/1

- Configure interfaces on active interswitch links according to the following table:

Switch-to-Switch Connections

Switch	Port	Switch	Port	Mode
SW1	2/2 2/3	SW2	2/2 2/3	trunk dot1q trunk dot1q
SW1	1/2	SW3	1/2	trunk dot1q
SW1	2/0	SW4	2/0	VLAN 200
SW2	1/2	SW4	1/2	VLAN 200

1.4. Spanning Tree Manipulation (Advanced: 3 points)

- Configure VLAN 200 bridge priority 4096 on SW4, and bridge priority 8192 on SW2. Leave the VLAN 200 bridge priority at the default value on SW1.
- Make sure that the forwarding on VLAN 200 is done between SW1 and SW2 and between SW1 and SW4.

1.5. Configure EtherChannel (Advanced: 3 points)

- Configure an aggregated trunk link with a bandwidth of 20 Mb/s between SW3 and SW4. Use the Link Aggregation Control Protocol (LACP) and SW3 should initiate EtherChannel initialization procedures. Configure the dot1q trunk on the EtherChannel link. Allow only VLAN 110, VLAN 120, and VLAN 999 on the trunk between SW3 and SW4.
- Verify that the packets that are coming from the same IP source to multiple IP destinations are distributed across the ports of the EtherChannel group, but the packets from different IP sources to the same destination are forwarded via the same switch port in the group.

2. Secure DVTI Communications Section (Total: 6 points)

2.1. Configure VTI Tunnel Interfaces (Intermediate: 3 points)

- Connectivity between the Serial1/0 interfaces of R1, R2, and R4 is provided via static routing during the lab initialization.
  - Configure the static VTI Tunnel241 interfaces on the spokes R1 and R4.
- Use the Serial1/0 interfaces on R1 and R4 for the Tunnel241 source.
- Configure the unnumbered IPv4 addresses on the Tunnel241 interfaces on R1 and R4 according to the "IPv4 IGP" diagram. Use the Loopback241 interface for this task.
- Configure the dynamic VTI Virtual-Template124 interface on the hub R2.
- Link the IP address of the VTI interface to the Loopback241 interface on R2

2.2. Configure IPsec DVTI Communications Between R1, R2, and R4 (Intermediate: 3 points)

- Configure IPSec ISAKMP policy on R1, R2, and R4 according to the following specifications:

ISAKMP

Parameter	Value
pre-share key	sharedpswd
encryption	3DES
hash	MD5
IPsec transform name	vti_transform
IPsec transform algorithm	esp-3des esp-md5-hmac
IPsec profile name	vti_profile
ISAKMP profile	vti_isakmp_profile

- Apply the IPsec profile on the DVTI interface on R2.
- Apply the IPsec profile on the static VTI interfaces on R1 and R4.

3. IPv4 OSPF Section (Total: 11 points)

3.1. Create OSPF Areas (Basic: 3 points)

- Configure Open Shortest Path First (OSPF) Area 0 on subnets 172.16.43.0/24, 172.16.53.0/24, 172.16.104.0/24, and 172.16.105.0/24.
- Configure OSPF Area 25 on subnets 172.16.241.0/24, 172.16.12.0/24, and 172.16.102.0/24.
- Configure OSPF Area 23 on subnet 172.16.23.0/22.
- Advertise network 172.16.103.0/24 in OSPF Area 103.

3.2. Tune OSPF Adjacency (Advanced: 3 points)

- Elect a designated router (DR) on R3 for all subnets in Area 0. Configure the network type that uses multicast to transmit the OSPF packets.
- Do not elect a DR on subnet 172.16.23.0/22.

3.3. Modify OSPF Areas (Advanced: 3 points)

- Do not allow external routing information into Areas 23 and 25 on the redistribution from EIGRP to OSPF. However, allow that information to transit *through* Areas 23 and 25 when such external information is originated by the routers within the areas.

- Make sure that R2 can still forward packets to all routers. Use the R4 address 172.16.241.4 as the next hop of last resort.

3.4. Verify Connectivity (Intermediate: 2 points)

- Verify that all OSPF prefixes that are specified in this section can be reached from all devices in the OSPF domain.

4. IPv4 EIGRP Section (Total: 7 points)

4.1. Configure Autonomous Systems (AS) (Basic: 2 points)

- Configure EIGRP AS 100 on the subnet between R1, R4, and R6.
- Configure EIGRP AS 10 on the VLAN 16 links between R1 and R6.
- Advertise the loopback networks 172.16.101.0/24 and 172.16.106.0/24 into EIGRP AS 10.

4.2. Secure Routing Updates (Intermediate: 3 points)

- Authenticate EIGRP AS 100 adjacencies with the string "cisco." This key should be used from midnight, January 1, 2013, to midnight, January 1, 2030.

4.3. Verify Connectivity (Intermediate: 2 points)

- Perform redistribution of EIGRP AS 10 to AS 100 on R6.
- Verify that all EIGRP prefixes that are specified in this section can be reached from all devices in the EIGRP domain.

5. Redistribution Section (Total: 5 points)

5.1. Establish Universal Connectivity (Intermediate: 2 points)

- Perform mutual redistribution between EIGRP AS 100 and OSPF on R4.
- Do not perform any other redistribution, except in cases where connections are required and not restricted by the scenario.

5.2. Verify Connectivity (Advanced: 3 points)

- Verify that all IPv4 IGP prefixes that are specified in the "IPv4 IGP" diagram can be reached from all devices, as specified in the "Restrictions and Goals" section. Network 30.30.30.0/24 should be reachable after the completion of later sections.

6. BGP Section (Total: 8 points)

6.1. Configure Processes and Peers (Basic: 3 points)

- Peer R1 in BGP AS 1 and R4 in BGP AS 4 using IP addresses 172.16.146.1 and 172.16.146.4.

- Peer R4 and R5 in BGP AS 4 using IP addresses 172.16.104.1 and 172.16.105.1.
- Configure AS 2 on R2 and AS 3 on R3. Peer R2 and R3 using IP addresses on the 172.16.23.0/22 subnet.
- Peer R1 and R2 using addresses on the 172.16.12.0/24 subnet.
- Peer R3 and R4 using addresses on the 172.16.43.0/24 subnet.

6.2. BGP Advertisements (Basic: 2 points)

- On R3, advertise the Loopback 30 subnet into BGP as a classful prefix. Do not use aggregation.

6.3. Next-Hop Availability (Advanced: 3 points)

- On router R2, configure BGP to track next-hop changes and report these changes directly to BGP. Increase the default delay for next-hop changes by 1 second.

7. MPLS Layer 3 VPN Section (Total: 8 points)

7.1. Configure VRFs on R4 and R5 (Basic: 2 points)

- Configure a VRF called CustomerA on R4 and R5. Use route distinguisher value 4:100. Assign interface E0/0.14 on R4 and interface E0/0.200 on R5 to this VRF.

7.2. Configure BGP to Carry VPN Routes Between R4 and R5 (Basic: 3 points)

- Enable the exchange of VPNv4 addresses between R4 and R5. Enable the Label Distribution Protocol (LDP) between R3 and R4 and between R3 and R5.

7.3. Configure BGP for Provider Edge to Customer Edge Routing (Basic: 3 points)

- Configure R7 and R8 as peers in BGP AS 100. Peer R8 with R4. Configure R9 in BGP AS 100 and peer it with R5.
- Redistribute connected routes into BGP on the customer routers and verify reachability between 172.16.107.0/24 and 172.16.120.0/24 within AS 100.

8. IPv6 Routing Section (Total: 11 points)

8.1. Configure IPv6 Addresses (Basic: 2 points)

- Configure IPv6 addresses on the devices. Use the following table to accomplish this task, and consult the “IPv6 IGP” diagram:

IPv6 Address Configuration

Router	Interface with IPv4 Address	IPv6 Address
R1	172.16.12.1	2001::12:1/125
R1	172.16.61.1	2001::16:1/125
R2	172.16.12.2	2001::12:2/125
R2	172.16.23.2	2001::23:2/125
R3	172.16.23.3	2001::23:3/125
R3	172.16.43.3	2001::43:3/125

Router	Interface with IPv4 Address	IPv6 Address
R3	172.16.53.3	2001::53:3/125
R4	172.16.43.4	2001::43:4/125
R5	172.16.53.5	2001::53:5/125
R6	172.16.61.6	2001::16:6/125

8.2. Configure IPv6 OSPF (Intermediate: 3 points)

- Configure OSPF Area 0 on VLAN 16 between R1 and R6.
- Configure OSPF Area 12 on VLAN 12. Do not send link-state advertisement (LSA) type 5 into Area 12; however, R1 and R6 must have external prefixes received from Area 12.

8.3. Configure IPv6 EIGRP AS 555 (Intermediate: 3 points)

- Configure the EIGRP AS 555 process on R2, R3, R4, and R5.
- Summarize 2001::43:0/125 and 2001::53:0/125 on R3 using the best possible mask.

8.4. Verify IPv6 Connectivity (Advanced: 3 points)

- Perform mutual redistribution between IPv6 EIGRP AS 555 and IPv6 OSPF on R2.
- Verify that all IPv6 IGP prefixes that are specified in the "IPv6 IGP" diagram can be reached from all devices. See the "Restrictions and Goals" section.

9. Cisco IOS Features Section (Total: 3 points)

9.1. SNMP (Advanced: 3 points)

- Configure R1 to report EIGRP notifications to the Simple Network Management Protocol (SNMP) server with the address 172.16.12.10 (imaginary). Send this information using traps, and use SNMPv2c and the community string SNMPSERVER. Allow remote access to this router with the community string EIGRPR1.

10. QoS Section (Total: 5 points)

10.1. Policy Maps (Advanced: 5 points)

- There is a flood attack, R1 receives an excessive amount of IPv6 packets with random protocol, sources, and destination addresses and ports, but the length is equal to 110.
- Packets are coming to R1 via an Ethernet interface, probably from R6. It has been confirmed that the packets that are transferred via R2 are not part of the attack. Block that traffic on R1. Make sure that packets of size 110 coming from R2 are not affected. The R2 MAC address is 0004.c18e.0bc0.