

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

Configuration 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 OF 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

Cisco 360 CCIE R&S Exercise Workbook Lab 10 Configuration Section	2
Activity Objectives	4
General Lab Instructions	4
Difficulty Levels.....	5
Exercise Workbook Lab 10 Configuration Section	6
Grading and Duration	6
Difficulty Level	6
Restrictions and Goals	6
1. Switch Configuration Section (Total: 8 points)	11
1.1. Configure VLANs (Basic: 1 point)	11
1.2. Switch-to-Router Port Configuration (Basic: 3 points)	11
1.3. Control Switch-to-Switch Links (Basic: 2 point)	11
1.4. Configure Spanning Tree (Intermediate: 2 points).....	12
2. IP Address Configuration Section (Total: 6 points).....	12
2.1. Assign IP Addresses (Intermediate: 2 points).....	12
2.2. Configure IP Address Assignment Security (Intermediate: 2 points).....	12
2.3. Configure the Interface (Basic: 2 points).....	12
3. IPv4 OSPF Section (Total: 8 points).....	12
3.1. Create OSPF Areas (Basic: 2 points)	13
3.2. Advertise Networks into OSPF (Basic: 2 points).....	13
3.3. Complete OSPF Tuning (Intermediate: 2 points).....	13
3.4. Verify Connectivity (Basic: 2 points)	13
4. IPv4 RIP Section (Total: 3 points).....	13
4.1. Enable RIP (Basic: 1 point).....	13
4.2. Control RIP Routing (Intermediate: 2 points).....	13
5. IPv4 EIGRP Section (Total: 6 points)	13
5.1. Enable Enhanced Interior Gateway Routing Protocol (EIGRP) (Basic: 1 point)	13
5.2. Control EIGRP Adjacencies (Basic: 2 points).....	13
5.3. Control EIGRP Routing (Advanced: 2 points).....	14
5.4. Verify Connectivity (Intermediate: 1 point).....	14
6. IPv4 Route Redistribution Section (Total: 9 points)	14
6.1. Obtain Universal Connectivity (Advanced: 1 point).....	14
6.2. Complete Redistribution Tuning (Intermediate: 2 points).....	14
6.3. Verify Traffic Forwarding Path (Intermediate: 1 point)	14
6.4. Check Filtering During Redistribution (Intermediate: 2 points)	15
6.5. Ensure Redistribution High Availability (Intermediate: 2 points)	15
6.6. Verify Connectivity (Advanced: 1 point).....	15
7. Border Gateway Protocol Section (Total: 6 points).....	15
7.1. Configure Processes and Peers (Intermediate: 3 points)	15
7.2. Advertise BGP Prefixes (Intermediate: 3 points)	15
8. Router Maintenance Section (Total: 4 points)	15
8.1. Monitor Traffic (Intermediate: 2 points)	15
8.2. Complete Policy-Based Routing (Intermediate: 2 points)	15
9. IPv6 Routing Section (Total: 10 points)	16
9.1. Configure IPv6 Interfaces and Link-Local Addresses (Basic: 1 point)	16
9.2. Configure IPv6 Addresses (Intermediate: 1 point).....	16
9.3. Configure IPv6 OSPF ((Intermediate: 2 points)	16
9.4. Complete IPv6 OSPF Tuning (Advanced: 2 points).....	16
9.5. Configure IPv6 EIGRP (Basic: 2 points)	17
9.6. Complete IPv6 Route Redistribution and Static Routing (Intermediate: 2 points)	17
10. Security Section (Total: 6 points).....	17
10.1. Configure IPv4 Inbound Access List on R5 (Intermediate: 3 points)	17
10.2. Configure IPv6 Inbound Access List on R4 (Intermediate: 3 points)	17
11. Quality of Service Section (Total: 5 points).....	17
11.1. Complete Traffic Marking (Intermediate: 5 points).....	17
12. Multicast Section (Total: 5 points).....	17
12.1. Configure Protocol Independent Multicast (PIM) (Advanced: 5 points)	17

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 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 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 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 10

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

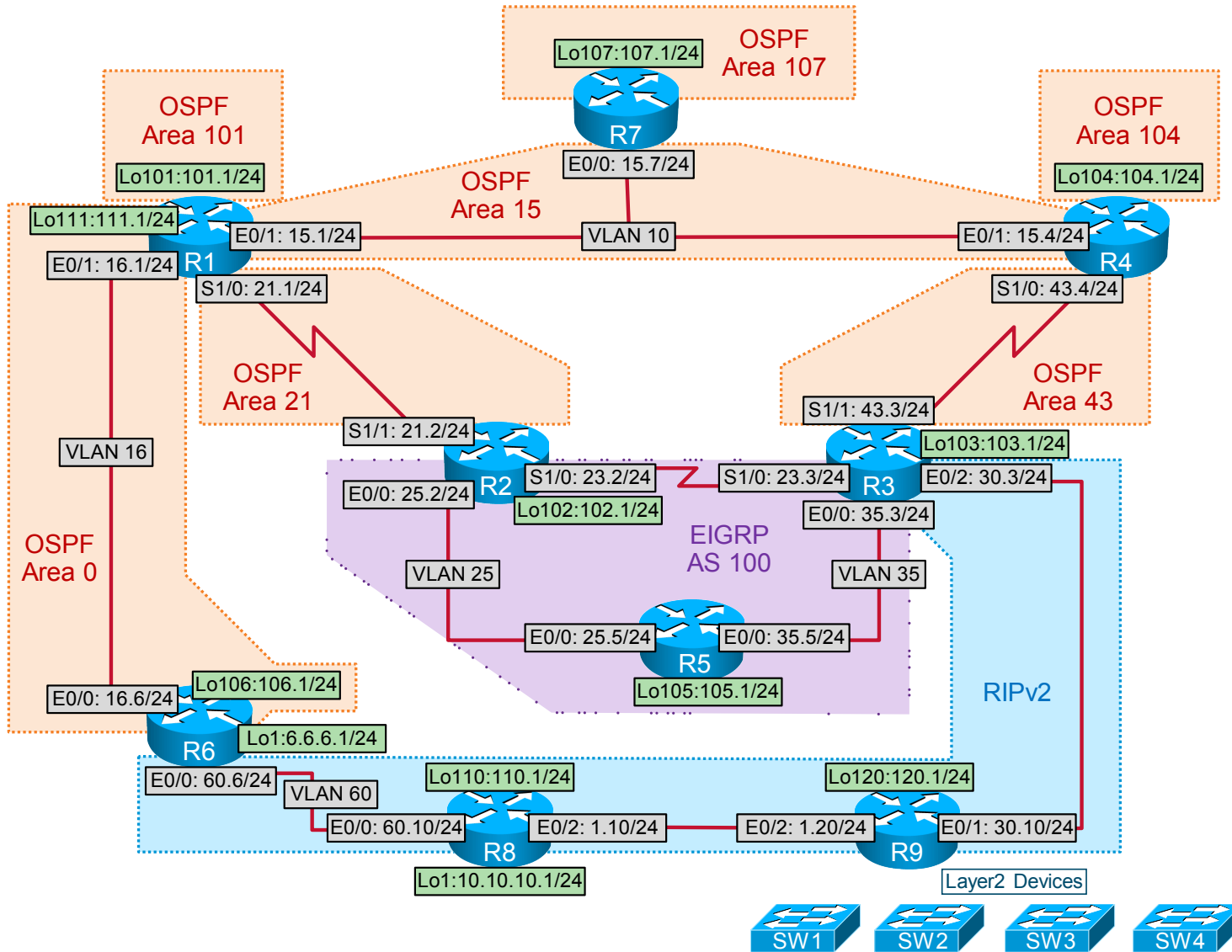
Restrictions and Goals

Note Read this section carefully.

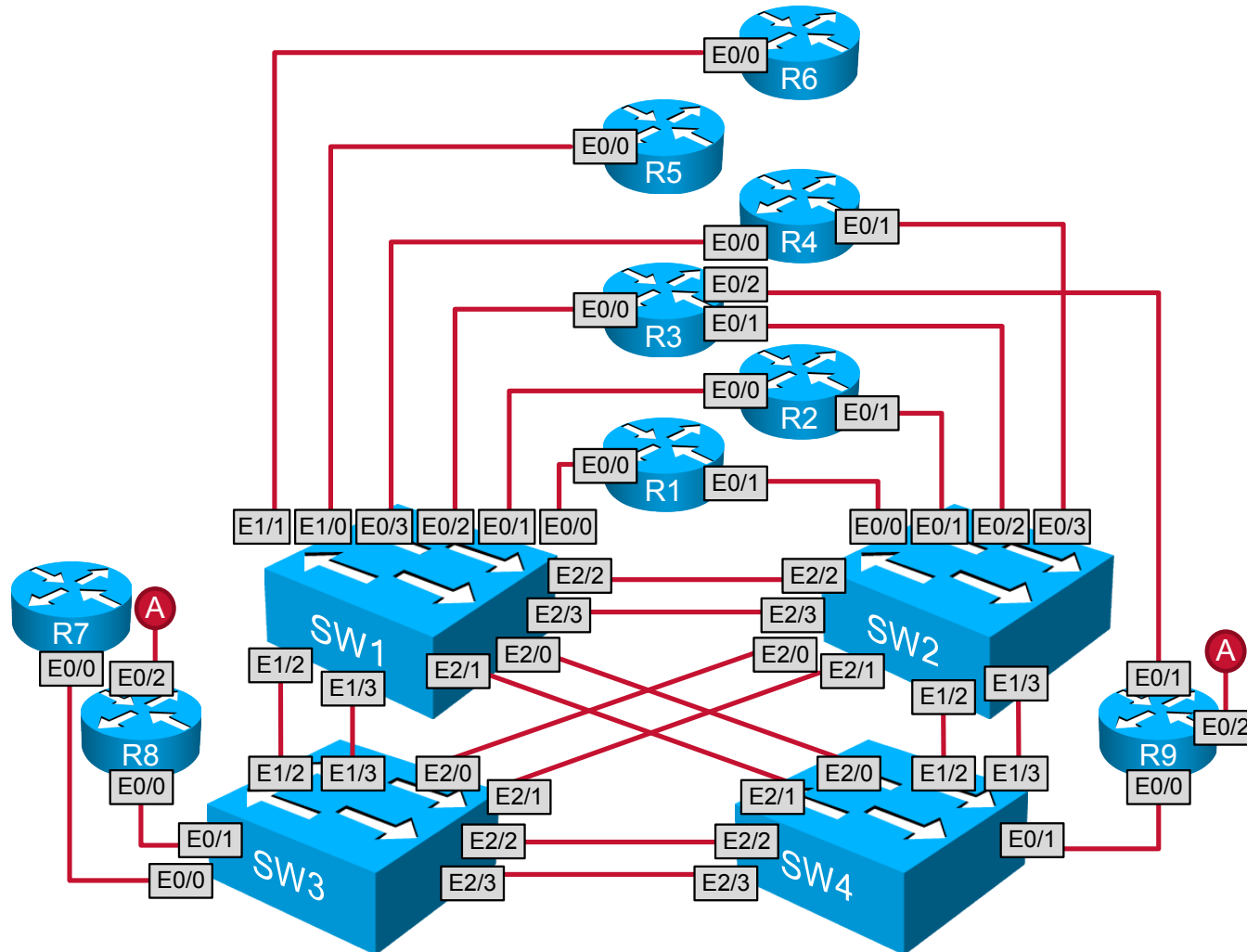
- To receive any credit for a subsection, you must fully complete the subsection as per requirements. You will *not* receive partial credit for partially completed subsections.
- IP version 4 (IPv4) subnets displayed in the scenario diagram belong to network 151.10.0.0/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Do not use any static routes.
- Advertise loopback interfaces with their original masks for IPv4 and IPv6 protocols.
- Network 0.0.0.0/0 should not appear in any routing table (**show ip route**) except on R8.
- Do not use the **ip default-network** commands.
- 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 interior gateway protocol (IGP)-only routers.
- Do not create new interfaces to fulfill IGP requirements, and do not create any summaries, unless the summary is required to meet explicitly stated scenario requirements.
- Do not introduce any new IPv4 or IPv6 addresses unless the instructions explicitly specify otherwise.
- 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.

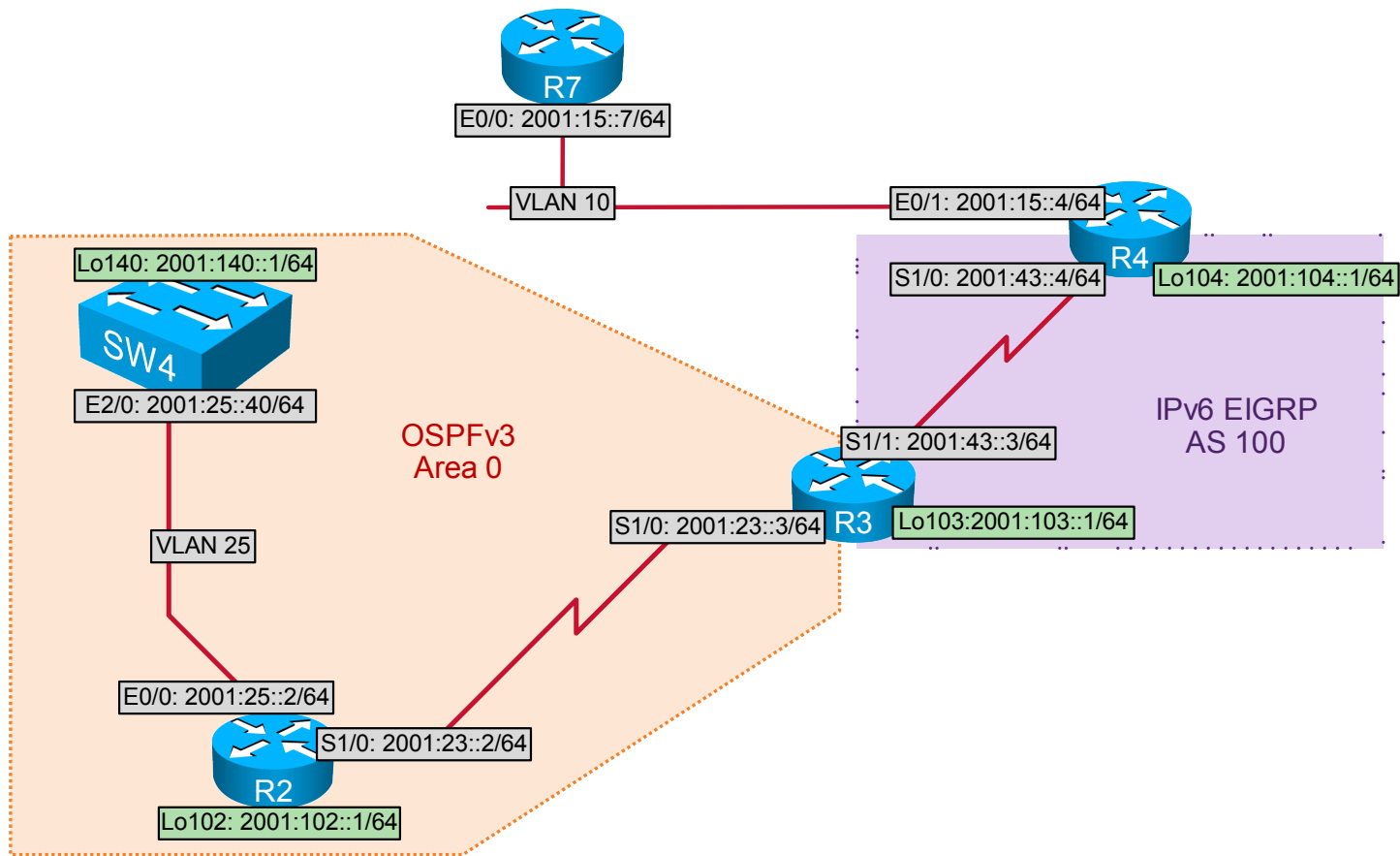
IPv4 IGP



Ethernet Switched Cabling Topology



IPv6 IGP



1. Switch Configuration Section (Total: 8 points)

1.1. Configure VLANs (Basic: 1 point)

- On SW1, SW2, SW3, and SW4, create the VLANs referenced in the following table:

VLAN	VLAN Name
10	
16	
25	
35	
60	

- Only create VLANs on the switch or switches where VLANs are used.

1.2. Switch-to-Router Port Configuration (Basic: 3 points)

- Configure the following switch-to-router connections.

Switch	Router	VLAN
SW2	R1	VLAN 10, VLAN 16
SW1	R2	VLAN 25
SW1	R3	VLAN 35
SW2	R4	VLAN 10
SW1	R5	VLAN 25, VLAN 35
SW1	R6	VLAN 16, VLAN 60
SW3	R7	VLAN 10
SW3	R8	VLAN 60

- Ports listed in the following table must be configured as routed ports.

Switch	Port
SW4	2/0

- Configure switch ports as access VLAN ports whenever possible. Otherwise, use trunks.
- For switch-to-router trunking, use 802.1q. Limit VLANs on the switch-to-router trunks to what is required in this scenario.
- Create the necessary Ethernet logical subinterfaces on the routers and assign the IP addresses specified in the diagram.
- Use a VLAN Trunking Protocol (VTP) transparent mode.

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

- Ports listed in the following table must be administratively shut down. Verify that they are shut down and make sure that they remain in a shutdown state.

Switch Shutdown Ports

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

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

Switch-to-Switch Connections

Switch	Port	Switch	Port	Mode
SW1	2/2	SW2	2/2	TBD
SW2	1/3	SW4	1/3	TBD
SW1	1/2	SW3	1/2	TBD
SW3	2/2	SW4	2/2	TBD

- Configure switch ports on switch-to-switch connections as access VLAN ports whenever possible. Otherwise, use 802.1q trunking on switch-to-switch connections. Limit VLANs on the on switch-to-switch trunks to what is required in this scenario.

1.4. Configure Spanning Tree (Intermediate: 2 points)

- Configure ports on the switches SW1 and SW2 connected to routers R1, R2, R3, R4, R5, and R6 to change the spanning-tree state directly from blocking to forwarding.

2. IP Address Configuration Section (Total: 6 points)

2.1. Assign IP Addresses (Intermediate: 2 points)

- Configure R6 to supply the IP address 151.10.16.1 to R1 via DHCP. Do not use any MAC address-based identification. Ensure that R6 only leases 151.10.16.1 to R1.

2.2. Configure IP Address Assignment Security (Intermediate: 2 points)

- Configure a switch feature that will permit only R6 to be a DHCP server in VLAN 16.

2.3. Configure the Interface (Basic: 2 points)

- Configure all VLAN 25 and VLAN 35 interfaces for a bandwidth of 100 Mb/s.
- Configure all VLAN 25 interfaces for a delay of 100 microseconds.
- Configure the R2 and R3 interfaces on subnet 151.10.23.0/24 to have the same bandwidth and delay as the R2 interface on subnet 151.10.25.0/24.

3. IPv4 OSPF Section (Total: 8 points)

Note All OSPF routers must be configured with only one OSPF PID. Points will be deducted from multiple sections for failing to assign only one OSPF PID on each specified router. Use your IGP diagram to help guide configuration.

3.1. Create OSPF Areas (Basic: 2 points)

- Configure OSPF Area 0 on subnet 151.10.16.0/24.
- Configure OSPF Area 15 on subnet 151.10.15.0/24.
- Configure OSPF Area 21 on subnet 151.10.21.0/24.
- Configure OSPF Area 43 on subnet 151.10.43.0/24.

3.2. Advertise Networks into OSPF (Basic: 2 points)

- Advertise loopback subnets 151.10.106.0/24 and 151.10.111.0/24 in Area 0.
- Advertise loopback subnet 151.10.101.0/24 in Area 101.
- Advertise loopback subnet 151.10.104.0/24 in Area 104.
- Advertise loopback subnet 151.10.107.0/24 in Area 107.

3.3. Complete OSPF Tuning (Intermediate: 2 points)

- Do not form an OSPF neighbor relationship between R1 and R4 in OSPF Area 15. Host routes should be generated for the interfaces that are connected to OSPF Area 15.
- Make sure that host routes are not advertised to other areas.

3.4. Verify Connectivity (Basic: 2 points)

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

4. IPv4 RIP Section (Total: 3 points)

4.1. Enable RIP (Basic: 1 point)

- Configure RIP version 2 (RIPv2) between routing devices R3, R6, R8, and R9.
- RIP updates must be sent only on the segments between these routers.

4.2. Control RIP Routing (Intermediate: 2 points)

- R6 should have no RIP-learned routes in its routing table. Do not use passive interface, route filtering, or administrative distance manipulation to accomplish this.
- R8 and R9 should have the single smallest route in the routing tables to reach destinations outside of the RIP routing domain via R3.

5. IPv4 EIGRP Section (Total: 6 points)

5.1. Enable Enhanced Interior Gateway Routing Protocol (EIGRP) (Basic: 1 point)

- Configure EIGRP autonomous system (AS) 100 subnet 151.10.23.0/24 between R2 and R3.
- Configure EIGRP AS 100 subnet 151.10.25.0/24 between R2 and R5.
- Configure EIGRP AS 100 subnet 151.10.35.0/24 between R3 and R5.
- Advertise the Loopback network 172.16.105.0/24 in EIGRP AS 100.

5.2. Control EIGRP Adjacencies (Basic: 2 points)

- Authenticate the EIGRP adjacency over the 151.10.23.0/24 subnet using key **rs?ccie**.

5.3. Control EIGRP Routing (Advanced: 2 points)

- On R5, traffic to native OSPF domain prefixes should be load-balanced using a 6:1 ratio favoring R2.
- R5 should prefer the direct path across VLAN 35 to the RIP domain routes.
- Influence the routing decisions for these prefixes by configuring R5 only.

5.4. Verify Connectivity (Intermediate: 1 point)

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

6. IPv4 Route Redistribution Section (Total: 9 points)

6.1. Obtain Universal Connectivity (Advanced: 1 point)

- Perform mutual redistribution between EIGRP and OSPF on R2.
- Perform mutual redistribution between EIGRP and OSPF on R3.
- Perform redistribution from RIP into OSPF on R3.
- Perform redistribution from RIP into EIGRP on R3.
- Do not perform any other redistribution.

6.2. Complete Redistribution Tuning (Intermediate: 2 points)

- When redistributing OSPF into EIGRP, use the following metrics:
 - Bandwidth 10,000
 - Delay 100
 - Reliability 255
 - Load 1
 - MTU 1500
- When redistributing RIP into EIGRP, use the following metrics:
 - Bandwidth 10,000
 - Delay 100
 - Reliability 255
 - Load 1
 - MTU 1500

6.3. Verify Traffic Forwarding Path (Intermediate: 1 point)

- Except as required by the “Multicast” section, routers in the OSPF domain should prefer to reach RIP destinations via R3.
- Routers in the OSPF domain should prefer to reach EIGRP destinations via R2.
- R2 should prefer to reach RIP destinations via the EIGRP path toward R3.
- OSPF routers should prefer to reach OSPF destinations via OSPF links.
- EIGRP routers should prefer to reach EIGRP destinations via EIGRP links.

6.4. Check Filtering During Redistribution (Intermediate: 2 points)

- When redistributing from RIP into OSPF and EIGRP, limit redistribution to the following networks; do not use access control lists (ACLs):
 - 151.10.1.0/24
 - 151.10.60.0/24
 - 151.10.110.0/24
 - 151.10.120.0/24
 - Connected routes on R3 that are part of the RIP routing domain

6.5. Ensure Redistribution High Availability (Intermediate: 2 points)

- Allow for full reachability (except for failed links) if either R2 or R3 loses its connection to the Serial links.

6.6. Verify Connectivity (Advanced: 1 point)

- Verify that all IPv4 IGP prefixes specified on the “IPv4 IGP” diagram can be reached from all devices. See the “Restrictions and Goals” section.

7. Border Gateway Protocol Section (Total: 6 points)

7.1. Configure Processes and Peers (Intermediate: 3 points)

- Configure BGP AS 600 on R6.
- Configure BGP AS 1000 on R8 and R9.
- Configure BGP peer relationships between AS 600 and AS 1000 using peers R6 and R8. Use the Loopback interface 151.10.110.1 of R8 for this peering.

7.2. Advertise BGP Prefixes (Intermediate: 3 points)

- Advertise the following networks in AS 600 from R6:
 - 6.6.6.0/24
- Advertise the following networks in AS 1000 from R8:
 - 10.10.10.0/24
- Ensure reachability of the preceding addresses from all BGP routers.

8. Router Maintenance Section (Total: 4 points)

8.1. Monitor Traffic (Intermediate: 2 points)

- Capture data on IP flows arriving on the E0/0.16 interface of R6.
- Send the flow statistics to a management workstation on 151.10.60.100, port 9992.
- For Internet Control Message Protocol (ICMP) packets, sample just one ICMP packet out of every one hundred.

8.2. Complete Policy-Based Routing (Intermediate: 2 points)

- All packets originating from 151.10.111.1 and destined to 151.10.105.1 must be forwarded to R6.

- On R6, all traffic coming from 151.10.111.1 and destined to 151.10.105.1 must be forwarded to R8 with the type of service (ToS) field set to Network Control.

9. IPv6 Routing Section (Total: 10 points)

9.1. Configure IPv6 Interfaces and Link-Local Addresses (Basic: 1 point)

- Configure the IPv6 link-local addresses for interfaces on subnet 151.10.23.0/24 and 151.10.43.0/24 according to the following table:

IPv6 Link-Local Address Assignment

Router	Link	IPv6 Link-Local Address
R2	R2 - R3	FE80::2
R3	R2 - R3	FE80::3
R3	R3 - R4	FE80::3
R4	R3 - R4	FE80::4

- Verify connectivity using configured IPv6 link-local addresses.

9.2. Configure IPv6 Addresses (Intermediate: 1 point)

- Configure IPv6 addresses according to the following table:

IPv6 Address Assignment

Router	Link	IPv6 Address
R2	Lo102	2001:102::1/64
	R2 - R3	2001:23::2/64
	R2 - SW4	2001:25::2/64
R3	Lo103	2001:103::1/64
	R3 - R2	2001:23::3/64
	R3 - R4	2001:43::3/64
R4	Lo104	2001:104::1/64
	R4 - R3	2001:43::4/64
	R4 - R7	2001:15::4/64
R7	R7 - R4	2001:15::7/64
SW4	Lo140	2001:140::1/64
	R2 - SW4	2001:25::40/64

9.3. Configure IPv6 OSPF ((Intermediate: 2 points)

- Configure OSPFv3 Area 0 on the network between R2 and R3.
- Configure OSPFv3 Area 0 on the network between R2 and SW4.
- Introduce the IPv6 address of the loopback interface of R2 into OSPFv3 Area 0.
- Introduce the IPv6 address of the loopback interface of SW4 into OSPFv3 Area 0.

9.4. Complete IPv6 OSPF Tuning (Advanced: 2 points)

- Use the same OSPF network type on all interfaces.
- Use Secure Hash Algorithm (SHA) to authenticate OSPFv3 packets between R2 and R3. Use a key constructed as a repeating pattern of 204 (decimal).

9.5. Configure IPv6 EIGRP (Basic: 2 points)

- Configure the IPv6 EIGRP AS 100 between routers R3 and R4.
- Introduce the IPv6 addresses of the loopback interface of R3 and R4 into IPv6 EIGRP AS 100.

9.6. Complete IPv6 Route Redistribution and Static Routing (Intermediate: 2 points)

- Perform mutual redistribution between IPv6 EIGRP AS 100 and OSPFv3 on R3.
- Redistribute the VLAN 10 IPv6 network into IPv6 EIGRP AS 100 as connected.
- Configure the static IPv6 default route on R7.

10. Security Section (Total: 6 points)

10.1. Configure IPv4 Inbound Access List on R5 (Intermediate: 3 points)

- For monitoring purposes, permit the following types of traffic in the extended numbered access list on R5:
 - Any IP packets that are marked with the IP precedence **network**
 - Any IP packets that are marked with the IP precedence **critical**
 - Any IP packets that are marked with differentiated services code point (DSCP) 25
 - Any IP packets that are marked with DSCP 20
- Apply your access list on all Ethernet interfaces on R5.
- Your solution should not disturb any other IPv4 traffic.

10.2. Configure IPv6 Inbound Access List on R4 (Intermediate: 3 points)

- Permit the following types of traffic in the extended named access list on R4:
 - Telnet packets from the Loopback102 IPv6 address of R2 to the Loopback104 IPv6 address of R4
- All other Telnet traffic to R4 should be dropped.
- Your solution should not disturb any other IPv6 traffic.

11. Quality of Service Section (Total: 5 points)

11.1. Complete Traffic Marking (Intermediate: 5 points)

- Ingress traffic with IP precedence 7 arriving from R6 should be marked with DSCP 25 on R8.
- Ingress traffic with DSCP 25 arriving from R8 to R9 should be marked with DSCP 20 on R9.
- Ingress traffic arriving from R9 and marked as DSCP 20 should be marked as IP precedence **critical** on R3.

12. Multicast Section (Total: 5 points)

12.1. Configure Protocol Independent Multicast (PIM) (Advanced: 5 points)

- Configure PIM neighbors between multicast routing devices R1, R2, R3, R7, and R9 using the following table:

PIM Interfaces

Router	Link
R1	151.10.15.0/24
	151.10.21.0/24
R2	151.10.21.0/24
	151.10.23.0/24
R3	151.10.23.0/24
	151.10.30.0/24
R7	151.10.15.0/24
R9	151.10.30.0/24
	151.10.1.0/24

- Statically configure Loopback103 on R3 as the root of the shared tree.
- Join one of the loopback interfaces of each multicast router to group 225.12.12.12.
- From R8, source a ping to address 225.12.12.12, and make sure that all routers with clients respond.
- You are not permitted to use static mroute entries.