360RSW05-WKB-CA03

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 3 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 3 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 to Advanced

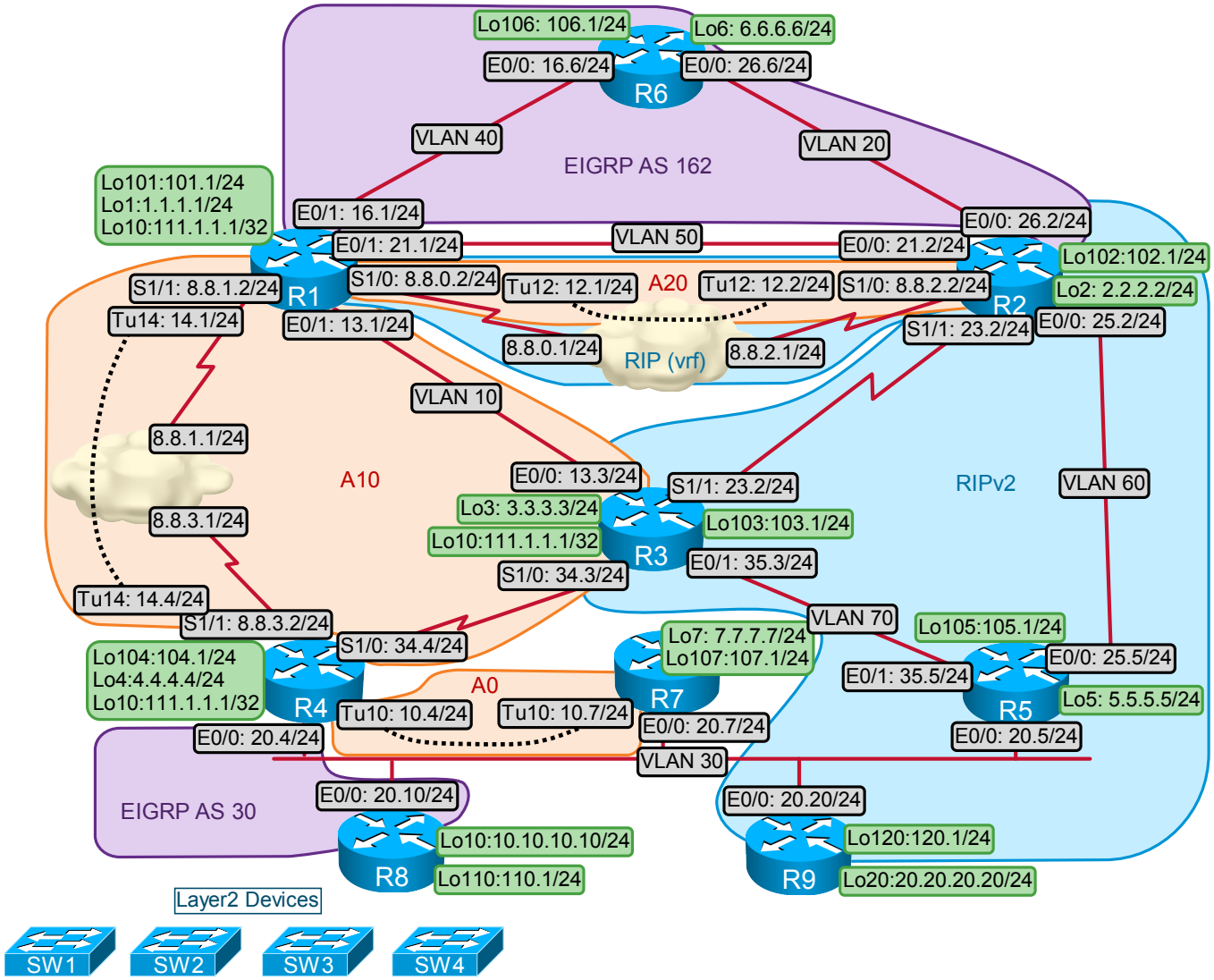
Restrictions and Goals

Note Read this section carefully.

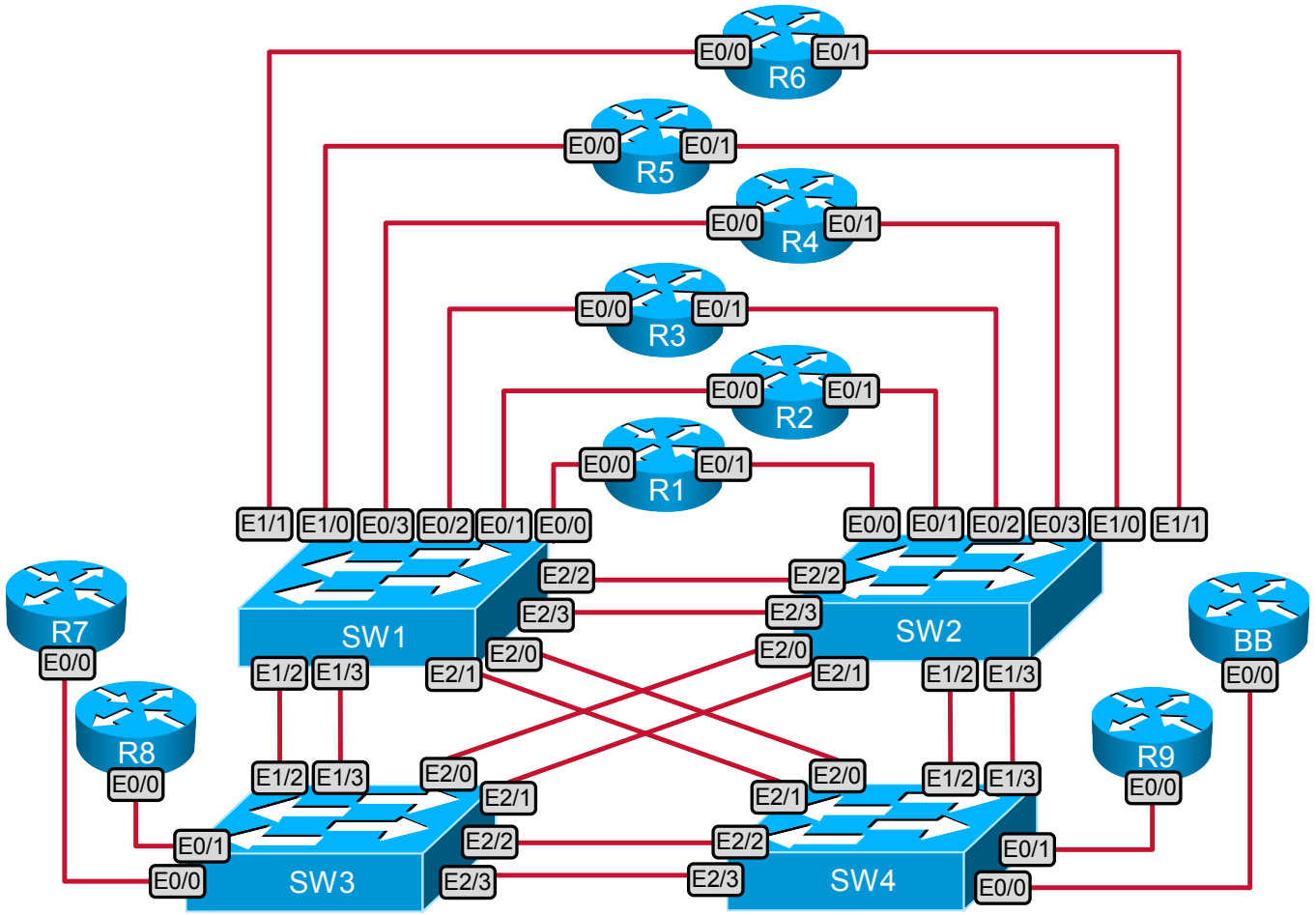
- To receive credit for a subsection, you must fully complete the subsection per the requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 135.15.0.0/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- IPv6 subnets that are displayed in the scenario diagram belong to network FEC2::/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv6 addresses.*
- Do not use any static routes unless explicitly permitted.
- Advertise loopback interfaces with their original masks.
- IPv4 network 0.0.0.0/0 should not appear in any routing table (**show ip route**).
- IPv6 network ::/0 should not appear in any routing table (**show ipv6 route**) except on R5.
- Do not introduce any new IP addresses.
- 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.
- Except in the Traffic Control subsection, 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.

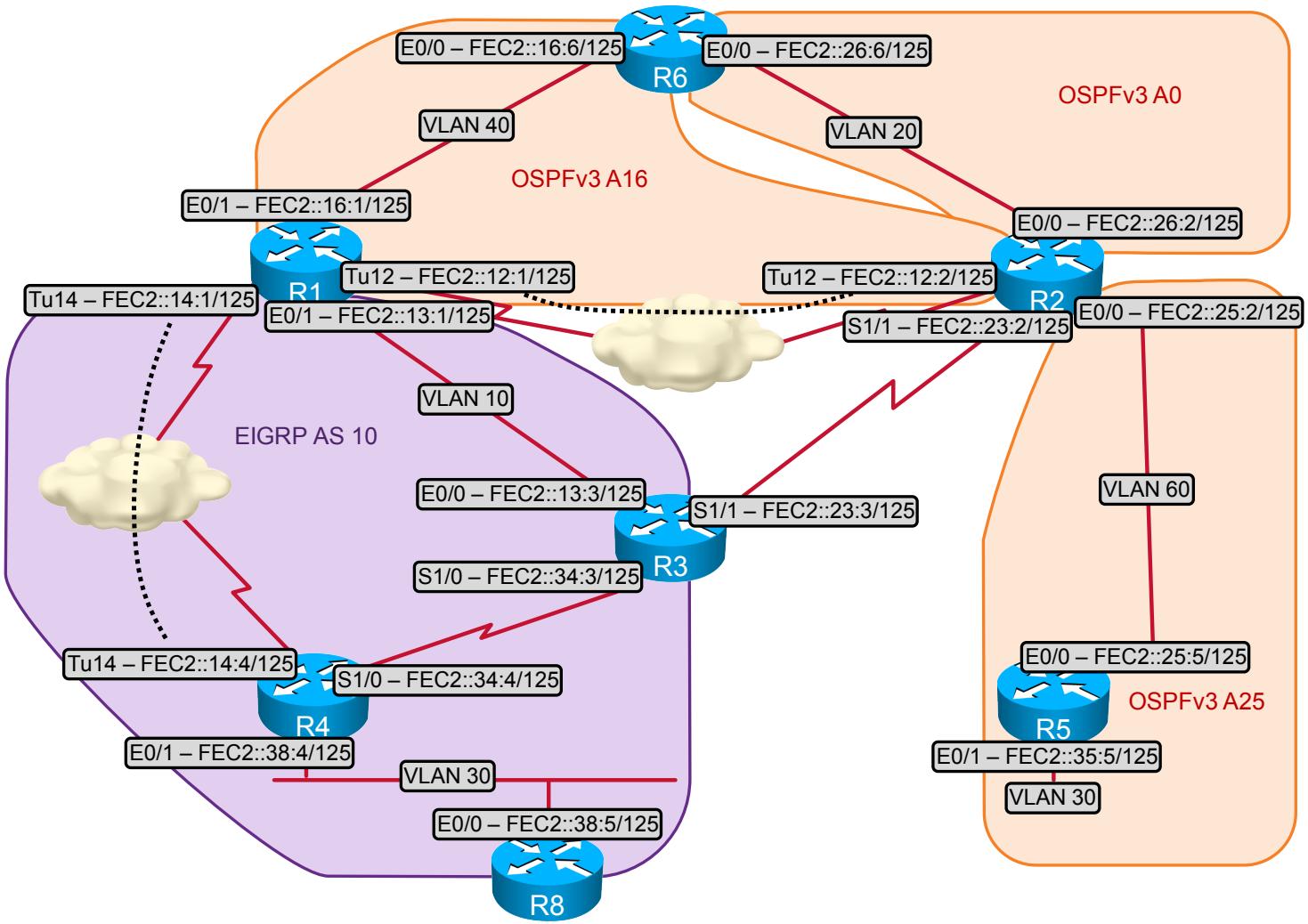
IPv4 IGP Diagram



Ethernet Switched Cabling Topology



IPv6 Topology Diagram



1. Switch Configuration Section (Total: 5 points)

Note Port 0/0 on SW4 is connected to the backbone. Healthy trunk status should be displayed as shown here:

```
Port        Mode         Encapsulation  Status
Et0/0       on           802.1q         trunking
```

Note **Do not change any initially configured link speeds.**

1.1. Configure VLANs (Basic: 2 points)

- Create the VLANs that are listed in the following table:

VLAN Allocation

VLAN	VLAN Name
VLAN 10	CA
VLAN 20	VA
VLAN 30	TX
VLAN 40	MD
VLAN 50	NY
VLAN 60	MI
VLAN 70	DC

- Use the IEEE 802.1Q protocol for trunking.
- Configure only the necessary VLANs on each switch without using any dynamic VLAN advertisement protocol.
- Configure the following switch-to-router connections:

Switch-to-Router Connections

Switch	Router	VLAN	Mode
SW1	R1		Administratively shut down
SW1	R2	20, 50, 60	Trunk
SW1	R3	10	Access
SW1	R4	30	Access
SW1	R5	30, 60	Trunk
SW1	R6	20, 40	Trunk
SW2	R1	10, 40, 50	Trunk
SW2	R2		Administratively shut down
SW2	R3	70	Access
SW2	R4	30	Access
SW2	R5	70	Access
SW2	R6		Administratively shut down
SW3	R7	30	Access
SW3	R8	30	Access
SW4	R9	30	Access

1.2. VTP Configuration (Basic: 1 point)

- Do not configure any switch for the VTP server mode.

1.3. Control Switch-to-Switch Links (Basic: 1 point)

- Configure interfaces on active switch-to-switch links according to the following table, and verify that ports that indicate they are administratively shut down remain in the shutdown state:

Switch-to-Switch Connections

Switch / Port		Switch / Port		Mode
SW1	1/2	SW3	1/2	Trunk dot1q
	1/3		1/3	Trunk dot1q
	2/0	SW4	2/0	Administratively shut down
	2/1		2/1	Administratively shut down
	2/2	SW2	2/2	Trunk dot1q
	2/3		2/3	Trunk dot1q
SW2	1/2	SW4	1/2	Trunk dot1q
	1/3		1/3	Administratively shut down
	2/0	SW3	2/0	Administratively shut down
	2/1		2/1	Administratively shut down
SW3	2/2	SW4	2/2	Trunk dot1q
	2/3		2/3	Trunk dot1q

- Allow only necessary VLANs on trunk links.

1.4. Tune Switch-to-Switch Links (Basic: 1 point)

- Configure EtherChannel between SW1 and SW2, bundling ports 2/2 and 2/3 on both switches.
- The EtherChannel should be built using Cisco aggregation protocol with both switches actively participating in protocol negotiations.

2. Internet Connectivity Section (Total: 4 points)

2.1. Configure Internet Connectivity (Basic: 2 points)

- Assign IP address 8.8.1.2/24 to the Serial1/1 interface of R1.
- Assign IP address 8.8.3.2/24 to the Serial1/1 interface of R4.
- Configure static host routes on R1 and R4 to allow connectivity between 8.8.1.2 and 8.8.3.2. The ISP router uses 8.8.x.1 IP address on each subnet.

2.2. Configure Internet Connectivity (Advanced: 2 points)

- Assign IP address 8.8.0.2/24 to the Serial1/0 interface of R1.
- Assign IP address 8.8.2.2/24 to the Serial1/0 interface of R2.
- The ISP router advertises the default route on subnets 8.8.0.0/24 and 8.8.2.0/24 via RIPv2. Configure routers R1 and R2 to accept the ISP advertised route.
- All IP addresses and subnets described in this subsection will be kept in a separate routing table called "Internet."

3. VPN Communications Section (Total: 5 points)

Note	Use your IGP diagram to help guide configuration.

Note	IP addresses from the 8.8.0.0/16 range are used strictly for Internet connectivity purposes. These IP addresses do not need to be reachable from any other routers, except the routers used for Internet connectivity. These subnets should not show in the routing tables (**show ip route**) of any other routers, except the routers used for Internet connectivity.

3.1. Configure VPN Connectivity Between R1 and R2 (Intermediate: 2 points)

- Create and configure tunnel interface Tunnel12.
- Use IP addresses 135.15.12.1/24 on R1 and 135.15.12.2/24 on R2.

3.2. Configure VPN Connectivity Between R1 and R4 (Basic: 1 point)

- Create and configure tunnel interface Tunnel14.
- Use IP addresses 135.15.14.1/24 on R1 and 135.15.14.4/24 on R4.

3.3. Establish VPN Connectivity Between R4 and R7 (Intermediate: 2 points)

- Create and configure tunnel interface Tunnel10.
- Use IP addresses 135.15.10.4/24 on R4 and 135.15.10.7/24 on R7.
- Use IP addresses on the existing 135.15.20.0/24 subnet for underlying connectivity.
- In the future, additional routers will be added to the 135.15.10.0/24 subnet.
- Do not use dynamic resolution of IP addresses on the VPN network.

4. VPN Security Section (Total: 2 points)

4.1. Protect VPN Between R1 and R4 with Encryption (Intermediate: 2 points)

- Use the preshared key R1-R4-secret. This key will be only used for the IP address of the peer.
- Use 168-bit DES for encryption, MD5 as the hash algorithm, and a 1024-bit group for key exchange.
- Use 168-bit DES for encryption and SHA as the hash algorithm for data protection.
- Do not associate protection configuration with the physical interface.

5. IPv4 OSPF Section (Total: 5 points)

Caution	All Open Shortest Path First (OSPF) routers must be configured with only one OSPF process ID (PID). *Points will be deducted from multiple sections for failing to assign one and only one OSPF PID on each specified router.* Use your IGP diagram to help guide configuration.

5.1. OSPF Area 0 (Intermediate: 1 point)

- Configure OSPF Area 0 between R4 and R7 on the network 135.15.10.0/24.

- On Area 0, use the OSPF network type that elects a designated router (DR) or backup designated router (BDR) and does not use the unicast packet exchange.
- R7 should be configured not to become the DR.

5.2. Create OSPF Area 10 (Basic: 1 point)

- Configure OSPF Area 10 on links 135.15.13.0/24, 135.15.14.0/24, and 135.15.34.0/24.
- The point-to-point OSPF network type should be used on 135.15.13.0/24 and 135.15.14.0/24.
- The broadcast OSPF network type should be used on 135.15.34.0/24, with R4 as the DR.

5.3. Create OSPF Area 20 (Basic: 1 point)

- Configure OSPF Area 20 on the link 135.15.12.0/24, using the nonbroadcast network type.
- Originate OSPF traffic from R1 only on this subnet.

5.4. Authenticate OSPF Area (Intermediate: 2 point)

- The adjacency on the 135.15.14.0/24 link should be authenticated with a cleartext password "clear-do".
- The adjacency on the 135.15.34.0/24 link should be authenticated with MD5 string "md5-test".

6. IPv4 EIGRP Section (Total: 3 points)

6.1. Configure AS 30 (Basic: 1 point)

- Configure Enhanced Interior Gateway Protocol (EIGRP) AS 30 on R4 and R8 interfaces connected to VLAN 30.
- All networks from the range 135.15.0.0/16 should be advertised as external EIGRP networks on R4 and R8.

6.2. Configure AS 162 (Basic: 2 points)

- Configure EIGRP AS 162 on the interfaces connected to VLANs 20 and 40 between the routers R1, R6, and R2, as well as on the Loopback 106 interface of the router R6.

7. IPv4 RIP Section (Total: 2 points)

7.1. Enable RIP (Basic: 2 points)

- Configure Routing Information Protocol (RIP) version 2 between routers R2, R3, R5, and R9.
- Advertise updates only on VLANs 30, 60, and 70, and the R2-R3 Serial link.

8. IPv4 Redistribution Section (Total: 5 points)

8.1. IGP Redistribution (Advanced: 3 points)

- Perform a mutual redistribution of dynamic interior gateway protocols:
  - Between EIGRP 162, and OSPF on R1
  - Between RIP, EIGRP 162, and OSPF on R2
  - Between RIP and OSPF on R3
  - Between OSPF and EIGRP 30 on R4
- Do not perform any other redistribution.
- Restrict redistribution:
  - Only allow the EIGRP 162 native subnet out of EIGRP 162
  - Do not allow the EIGRP 162 native subnet from RIP into EIGRP 162
  - Only allow RIP native subnets into OSPF

8.2. Redistribution of Connected (Intermediate: 2 points)

- Perform the **redistribute connected** command where required and not restricted by the scenario.
- Limit prefixes redistributed with the **redistribute connected** command to the list of subnets required to obtain universal connectivity.

9. Border Gateway Protocol Section (Total: 8 points)

9.1. Configure Processes and Peers (Basic: 2 points)

- Disable Border Gateway Protocol (BGP) synchronization.
- Configure BGP autonomous systems according to the table:

BGP AS Assignment

Device	AS
R8	1000
R9, R3, and R5	235
R7 and R4	47
R1, R2, and R6	126

- Configure EBGP peering between:
  - R8 and R9
  - R8 and R4
  - R7 and R3
  - R1 and R4

9.2. Tune IBGP Peering (Basic: 2 points)

- Do not configure a full mesh and BGP confederations in AS 126 and AS 235.
- Use R6 and R5 to exchange reachability information.

9.3. Advertise Networks (Basic: 2 points)

- Advertise the following loopback networks:
  - 1.1.1.0/24 from R1
  - 2.2.2.0/24 from R2
  - 3.3.3.0/24 from R3
  - 4.4.4.0/24 from R4
  - 5.5.5.0/24 from R5
  - 6.6.6.0/24 from R6
  - 7.7.7.0/24 from R7
  - 10.10.10.0/24 from R8
  - 20.20.20.0/24 from R9

9.4. Tune BGP Routing (Intermediate: 2 points)

- Configure R5 to ensure that R3 has a next hop 135.15.35.5 for subnet 20.20.20.0/24.
- Configure R7 to ensure that R3 has a next hop 135.15.106.1 for subnet 1.1.1.0/24, 2.2.2.0/24, 6.6.6.0/24.
- Configure R4 to ensure that R7 has a next hop 135.15.20.4 for subnet 1.1.1.0/24, 2.2.2.0/24, 6.6.6.0/24.

10. Control Traffic Section (Total: 3 points)

10.1. Configure Traffic Path (Intermediate: 3 points)

- If traffic is originated from the 135.15.103.0/24 subnet and destined to the 135.15.106.0/24 subnet, it must be forwarded to R2 from R3.
- This traffic flow must traverse router R2 twice and R1 once in one direction.
- The term **traverse** is defined as follows: enter the route on one interface and exit the router on a different interface.
- This traffic flow must be symmetric.
- Do not make forwarding decisions based on the precise source and destination match on R1.

11. IPv4 Connectivity Verification Section (Total: 1 point)

11.1. Verify Connectivity (Advanced: 1 point)

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

12. SNMP Security Section (Total: 3 points)

12.1. Create SNMP View (Intermediate: 1 point)

- On R1, create an SNMP view test via SNMP of all objects in the system group except for system 7 objects. Also, add all objects of the Cisco private MIB.

12.2. Secure SNMP (Advanced: 2 points)

- On R1, configure a user **administrato**r in the SNMP group **administratorgrp** to be able to read and write to view test via SNMP, if the user passes SNMP authentication.

- Use Message Digest 5 (MD5) and the password **test**.
- Configure the user **operator** in the SNMP group **operatorgrp** to be able to read the view test via SNMP. No SNMP authentication is required for the user operator.
- Configure read-only access for **operator** from VLAN 20 only.
- Configure read-write access for **administrator** from VLAN 30 only.
- Configure security model **V3** for this task.

13. IPv6 Addressing Section (Total: 2 points)

13.1. Configure IPv6 Addresses (Basic: 2 points)

- Configure IPv6 addresses according to the following table:

IPv6 Address Assignment

Router	IPv4 Interface	Link-Local Addresses	Site-Local Addresses
R1	E0/1.10		FEC2::13:1/125
	E0/1.40		FEC2::16:1/125
	Tu12	FE80::1	FEC2::12:1/125
	Tu14	FE80::1	FEC2::14:1/125
R2	E0/0.20	FE80::2	FEC2::26:2/125
	E0/0.60		FEC2::25:2/125
	S1/1	FE80::2	FEC2::23:2/125
	Tu12	FE80::2	FEC2::12:2/125
R3	E0/0		FEC2::13:3/125
	S1/0	FE80::3	FEC2::34:3/125
	S1/1	FE80::3	FEC2::23:3/125
R4	E0/1	FE80::4	FEC2::38:4/125
	S1/0	FE80::4	FEC2::34:4/125
	Tu14	FE80::4	FEC2::14:4/125
R5	E0/0.60		FEC2::25:5/125
	E0/1		FEC2::35:5/125
R6	E0/0.20	FE80::6	FEC2::26:6/125
	E0/0.40		FEC2::16:6/125
R8	E0/0	FE80::5	FEC2::38:5/125

- Verify connectivity between IPv6 addresses on the Serial, Ethernet, and VPN links.

14. IPv6 Routing Section (Total: 7 points)

14.1. Configure IPv6 OSPF Area 0 (Intermediate: 1 point)

- Configure the OSPFv3 backbone area on VLAN 20.
- R2 must be always the DR and have router ID (RID) 200.200.200.2.
- OSPFv3 hello packets must be unicast.

14.2. Configure IPv6 OSPF Area 25 (Intermediate: 1 point)

- Configure OSPFv3 Area 25 between R2 and R5 over VLAN 60, and on R5 on interface E0/1.
- The OSPF process on R5 must not have knowledge of routing information beyond its area.

14.3. Configure IPv6 OSPF Area 16 (Intermediate: 1 point)

- Configure OSPFv3 Area 16 on the VLAN 40 link between R1 and R6, and over VPN between R1 and R2.
- On VLAN 40, ensure that OSPF announces the other end of link as host route.
- Use OSPF configuration to achieve this.

14.4. Advertise External Route into IPv6 OSPF (Basic: 1 point)

- Subnet 23:0/125 must be external to OSPF.
- Limit redistribution to the 23:0/125 subnet.

14.5. Configure IPv6 EIGRP (Basic: 2 point)

- Configure EIGRP between R1 and R4, R1 and R3, R3 and R4, and R4 and R8.

14.6. Advertise External Route into IPv6 EIGRP (Basic: 1 point)

- Subnet 23:0/125 must be external to EIGRP.
- Apply the configuration on R3.

15. IPv6 Redistribution Section (Total: 4 points)

15.1. Redistribute IPv6 IGP (Intermediate: 1 point)

- Redistribute EIGRP into OSPF on R1 using a minimal nonzero metric.
- Redistribute OSPF into EIGRP on R1.

15.2. Control IPv6 Redistribution (Intermediate: 2 point)

- Restrict redistribution to exclude 23:0/125 subnet.

15.3. Verify IPv6 Connectivity (Intermediate: 1 point)

- Ensure that all global IPv6 addresses specified in the IPv6 routing section are reachable.

16. QoS Section (Total: 3 points)

16.1. Traffic Marking (Intermediate: 2 points)

- Traffic between the networks 135.15.103.0/24 and 135.15.106.0/24 should be marked with IP precedence 2.
- The marking should be retained throughout the network.
- Accomplish this without the use of route maps.

16.2. Traffic Remarking (Intermediate: 1 point)

- Configure R2 and mark IP traffic coming from R3 with flash precedence, unless it is already marked with immediate precedence.

17. Switching Specialties Section (Total: 4 points)

17.1. Configure Port Security (Intermediate: 2 points)

- On SW4, configure ports 0/3, 1/0, and 1/1 in access mode in VLAN 30.
- On each of these three interfaces, only one MAC address is allowed.
- On SW4 port 1/0, when the number of port-secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses should be dropped. The switch should not notify that a security violation has occurred.
- On SW4 port 1/1, when the number of port-secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses should be dropped. An SNMP trap should be sent, a syslog message should be logged, and the violation counter should increment.
- On SW4 port 0/3, the interface should be error-disabled when a violation occurs. An SNMP trap should be sent, a syslog message should be logged, and the violation counter should increment.
- SW4 port 0/3 should be automatically brought out of the error-disabled state after a time-out of 50 seconds.

17.2. Tune Port Security Aging (Intermediate: 2 points)

- For SW4 port 1/0, if the first connected device is inactive for 2 minutes, SW4 should allow another device to use port 1/0.
- For SW4 port 1/1, SW4 should systematically delete the secure address 2 hours after it entered its MAC address table.

18. System Administration Section (Total: 4 points)

18.1. Configure Telnet Access (Intermediate: 2 point)

- The network administrator would like to have the Telnet session to R6 on port 3004 redirected to R2 on port 3007.
- Redirection should occur only if user **admin** with the password **test** is authenticated on both R6 and R2.
- Allow a Telnet session to R6's port 3004 only from the 135.35.101.0/24 network.
- Apply configuration on R2 and R6. You can modify VTY line 4 configurations of these routers to meet requirements of this section.

18.2. Secure Access (Advanced: 1 point)

- The network administrator would like to have ability to execute commands on R5 using remote shell protocol.
- User TESTADMIN from R4 should be able to see the R5's output of any commands, for example the **show run** and **show version** commands.
- User TESTOPERATOR from R4 should be able to see R5's output of nonprivileged commands, for example the **show version** command but not the **show run** command.

18.3. Memory Monitoring (Advanced: 1 point)

- Router R5 should send a notification to indicate that free processor memory has fallen below 80,000 KB.
- Reserve 2500 KB of memory for critical operations such as event logging to continue to function even when router memory is exhausted.

19. Multicast Section (Total: 6 points)

19.1. PIM Configuration (Basic: 2 points)

- Configure Protocol Independent Multicast (PIM) sparse mode (SM) routing on all routers involved in this scenario.
- Add all links in multicast routing, except for the VLAN 50 link.

19.2. Configure Membership (Basic: 1 point)

- Join multicast group 225.22.22.22 on the following loopback interfaces:
  - 1.1.1.0/24 from R1
  - 2.2.2.0/24 from R2
  - 3.3.3.0/24 from R3
  - 4.4.4.0/24 from R4
  - 5.5.5.0/24 from R5
  - 6.6.6.0/24 from R6
  - 7.7.7.0/24 from R7
  - 10.10.10.0/24 from R8
  - 20.20.20.0/24 from R9

19.3. Configure RP (Advanced: 2 points)

- Configure R1, R3, and R4 as redundant rendezvous points (RPs) in the network.
- Use 111.1.1.1/32 as the RP address.
- Configure all three routers to cache source/group pairs to reduce join latency.
- Use a static configuration on all routers and switches that need to access this RP address.

19.4. Verify Multicast Connectivity (Intermediate: 1 point)

- Each router and switch should receive a reply from every router when the address 225.22.22.22 is pinged.