360RSW05-WKB-CA02

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 2 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 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 Cisco Catalyst 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 2 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

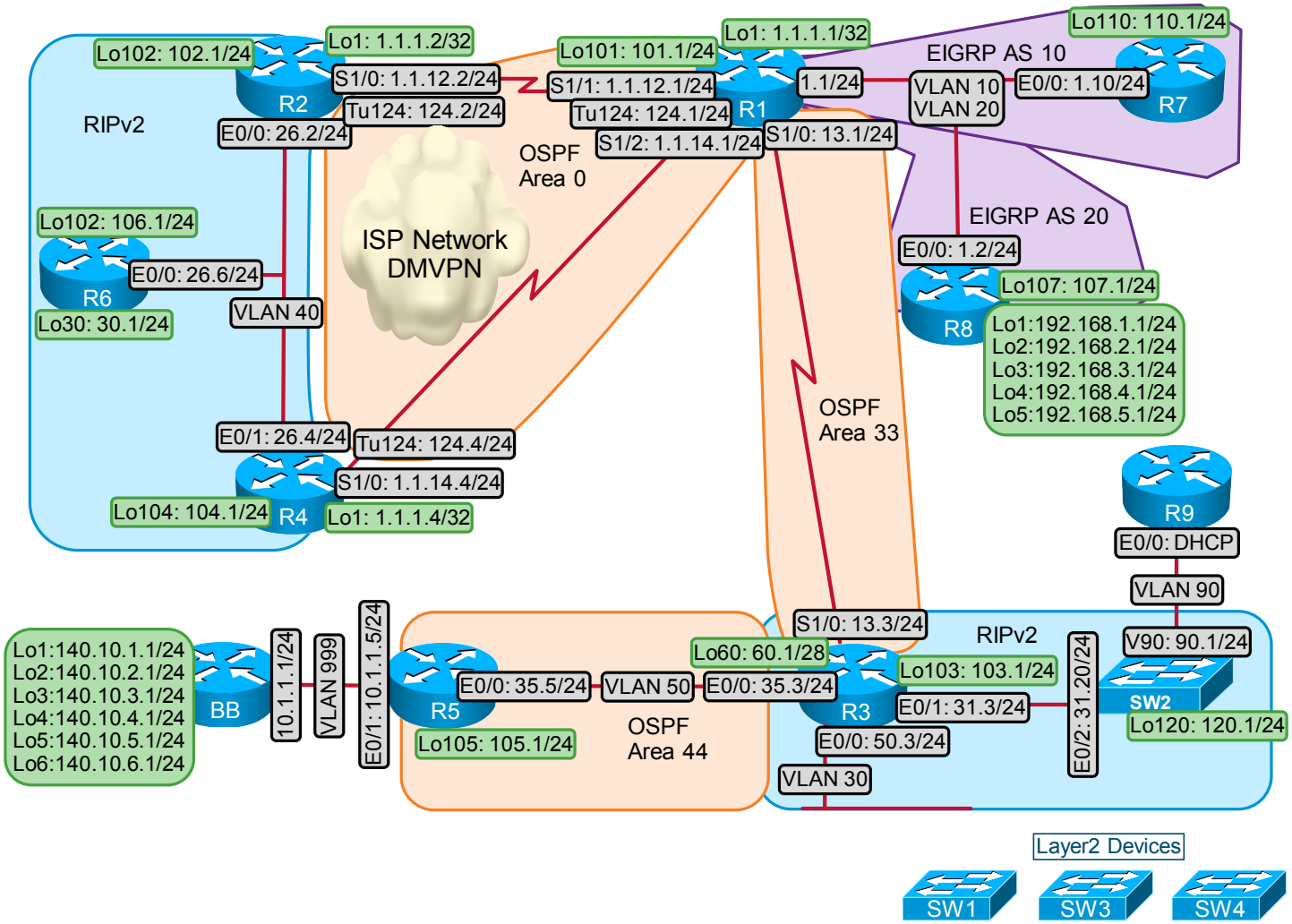
Restrictions and Goals

Note Read this section carefully.

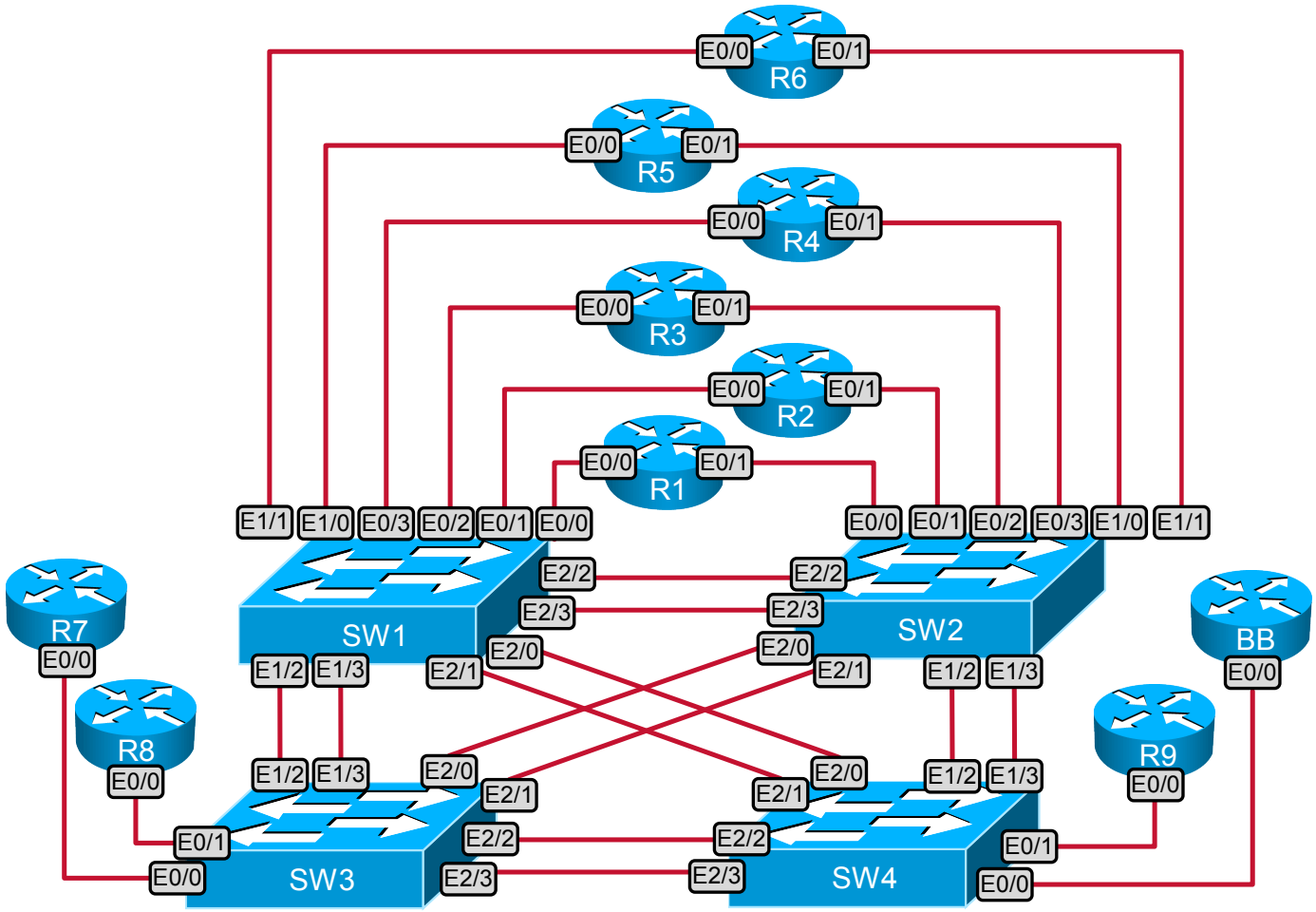
- To receive credit for a subsection, you must fully complete the subsection as the requirements. You will *not* receive partial credit for partially completed subsections.
- IPv4 subnets that are displayed in the scenario diagram belong to network 172.16.0.0/16.
- *Points will be deducted from multiple sections for failing to assign correct IPv4 addresses.*
- Do not use any static routes.
- Advertise loopback interfaces with their original masks.
- Network 0.0.0.0/0 should not appear in any routing table (**show ip route**).
- Do not use the **ip default-network** command.
- All IP addresses from the 172.16.0.0/16 range that are involved in this scenario must be reachable, unless explicitly specified otherwise.
- The OSPF PID 1111 network is initialized for DMVPN configuration. Subnets that are routing via OSPF PID 1111 on R1, R2, and R4 are excluded from the universal reachability requirement.
- In this exercise, R8 is used for backbone router simulation. IP packets from R8 do not need to be delivered to the destinations beyond 172.16.1.0/24. However, unless explicitly specified otherwise, the routes advertised by R8 need to be present in the routing tables of other routers, and traffic from other routers needs to be able to reach R8.
- Unless explicitly specified otherwise, addresses and networks that are advertised in the BGP section must be reachable by all BGP routers, but do not have to be reachable by routers that use only IGP.

- Do not create new interfaces to fulfill IGP requirements, and do not summarize unless you are explicitly asked to do so.
- Do not introduce any new IPv4 addresses.
- Use conventional routing algorithms only.
- 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



1. DMVPN Communications Section (Total: 5 points)

1.1. Configure mGRE Tunnel Interfaces (Basic: 3 points)

- Connectivity between the loopback1 interfaces of R1, R2, and R4 is provided via OSPF routing during the lab initialization. The OSPF process ID is 1111.
- Configure the mGRE Tunnel124 interfaces on R1, R2, and R4.
- Use the Loopback1 interfaces on R1, R2, and R4 for the Tunnel124 source.
- Supply IPv4 addresses on all required tunnel interfaces according to the "IPv4 IGP" diagram.

1.2. Configure DMVPN and Verify Layer 3 Connectivity in DMVPN (Basic: 2 points)

- Configure R1 as an NHS for the NHRP spokes R2 and R4.
- Supply the NHRP NHS mapping on R2 and R4. Do not configure any NHRP mapping on R1.
- Make sure that R1, R2, and R4 can ping all attached, same-subnet Tunnel124 IPv4 interfaces.

2. Switch Configuration Section (Total: 11 points)

2.1. Configure VLANs (Basic: 2 points)

- On SW1, SW2, SW3, and SW4 create the VLANs that are listed in the following table:

VLANs

VLAN	VLAN Name
10	
20	
30	
40	
50	
90	
999	

2.2. Configure Switch-to-Router Ports (Basic: 3 points)

- Configure the following switch-to-router connections:

Switch-to-Router Connections

Switch	Router	VLAN
SW2	R1	VLAN 10, LAN 20
SW1	R2	VLAN 40
SW1	R3	VLAN 30, VLAN 50
SW2	R3	Layer 3
SW2	R4	VLAN 40
SW1	R5	VLAN 50
SW2	R5	VLAN 999
SW1	R6	VLAN 40
SW3	R7	VLAN 10
SW3	R8	VLAN 20
SW4	R9	VLAN 90

- Configure switch port as access whenever possible. Otherwise use trunks.
- For switch-to-router trunking, use IEEE 802.1Q. Limit VLANs on the switch-to-router trunks to what is required in this scenario.
- Create the necessary switch virtual interface (SVI) interfaces on the switches and assign the IP addresses specified in the diagram.
- Create the necessary Ethernet logical subinterfaces on the routers and assign the IP addresses specified in the diagram.

2.3. Configure VTP (Basic: 2 points)

- Use a VLAN Trunking Protocol (VTP) mode that does not propagate VLAN information over the trunks.
- On all switches, use the VTP domain name "ccie**"**.

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

- 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.

Shutdown Ports

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

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

- Configure switch ports on switch-to-switch links as 802.1Q trunks.
- Do not use EtherChannel.
- Only VLANs that need to carry traffic should be allowed on the trunks.

2.5. Configure Spanning Tree (Intermediate: 2 points)

- Configure switch rapid convergence based on the IEEE 802.1w standard with minimal extra configuration.
- Each VLAN on the switch-to-switch links between switches should run its own spanning-tree instance.

3. IP Addresses Configuration Section (Total: 4 points)

3.1. Assign IP Addresses (Intermediate: 2 points)

- Configure SW2 to supply the IP addresses on subnet 172.16.90.0/24 to devices on VLAN 90.
- Assign only IP addresses 172.16.90.3, 172.16.90.5, and 172.16.90.7.
- Devices on VLAN 90 should use 172.16.90.1 as the default router.
- Ensure that R9 has an IP address assignment.

3.2. Configure R1 – R7 - R8 Connectivity (Intermediate: 2 points)

- Assign IP addresses 172.16.1.1/24 to R1, 172.16.1.10/24 to R7, and 172.16.1.2/24 to R8.
- Make sure that all three routers can ping each other.

4. IPv4 OSPF Section (Total: 8 points)

Note	All OSPF routers except of the routers that are connected to DMVPN 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.

4.1. Create OSPF Areas (Basic: 2 points)

- Configure OSPF area 0 on DMVPN subnet 172.16.124.0/24 between R1, R2, and R4.
- Configure OSPF area 33 on subnet 172.16.13.0/24 between R1 and R3.
- Configure OSPF area 44 on subnet 172.16.35.0/24 between R3 and R5.

4.2. Advertise Networks into OSPF (Basic: 3 points)

- Advertise loopback subnet 172.16.101.1/24 in area 0.
- Advertise loopback subnets 172.16.60.1/28 and 172.16.105.0/24 in area 44.
- On R3, have the VLAN 30 subnet advertised via OSPF without including it as one of your OSPF networks. Make sure that it is viewed as a type 1 route by OSPF and that the network can be reached from everywhere.
- Make any other external OSPF routes type 2.

4.3. Establish OSPF Adjacencies (Intermediate: 2 points)

- Make R3 the designated router for the link between R1 and R3.
- Use the OSPF network type nonbroadcast for 172.16.124.0/24 and 172.16.13.0 subnets.

4.4. Verify Connectivity (Basic: 1 point)

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

5. IPv4 RIP Section (Total: 6 points)

5.1. Enable RIP (Basic: 2 points)

- Configure RIPv2 between R3 and SW2.
- Configure RIPv2 between the routers R2, R4, and R6.
- Configure RIPv2 routing only for the subnets from the 172.16.0.0/16 range on all RIP routers.

5.2. Control RIP Updates (Intermediate: 2 points)

- Send RIP updates on VLAN 40, but for security reasons do not use broadcast or multicast RIP updates.
- Send RIP updates on the link between R3 and SW2.
- Do not send any other RIP updates.

5.3. Control RIP Routing (Intermediate: 2 point)

- Routers R2 and R4 should prefer the RIP path when transmitting traffic between their respective loopback interfaces.

6. IPv4 EIGRP Section (Total: 9 points)

6.1. Enable EIGRP (Basic: 2 points)

- Configure the EIGRP AS 10 subnet 172.16.1.0/24 between R1 and R7.
- Configure the EIGRP AS 20 subnet 172.16.1.0/24 between R1 and R8.

6.2. Advertise Networks into EIGRP (Basic: 3 points)

- Advertise the loopback network 172.16.110.0/24 in EIGRP AS 10.
- Advertise the loopback network 172.16.107.0/24 in EIGRP AS 20.
- Advertise the loopback networks 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24, and 192.168.5.0/24 in EIGRP AS 20 as external networks.

6.3. Control EIGRP Routing Updates (Intermediate: 2 points)

- R1 should not send EIGRP updates within EIGRP 20.
- Do not use any filtering techniques.

6.4. Control EIGRP Routing (Advanced: 2 points)

- Using a minimal number of configuration lines, configure R1 to accept only the following routes from R8:
  - 172.16.107.0/24

- 192.168.2.0/24,
- 192.168.3.0/24

7. IPv4 Route Redistribution Section (Total: 8 points)

7.1. Obtain Universal Connectivity (Advanced: 3 points)

- Perform mutual redistribution between RIP and OSPF on R2.
- Perform mutual redistribution between RIP and OSPF on R4.
- Perform mutual redistribution between RIP and OSPF on R3.
- Perform mutual redistribution between EIGRP 10 and OSPF on R1.
- Perform redistribution from EIGRP 20 into EIGRP 10 and OSPF on R1.
- Do not perform any other redistribution, except as required in the EIGRP section.

7.2. Complete Redistribution Tuning (Intermediate: 2 points)

- Use the minimal nonzero metric in redistribution on R2 and R4.

7.3. Complete Filtering During Redistribution (Intermediate: 2 points)

- When configuring redistribution from RIP into OSPF on R2 and R4, permit only the following networks:
  - 172.16.26.0/24
  - 172.16.30.0/24
  - 172.16.102.0/24
  - 172.16.104.0/24
  - 172.16.106.0/24
- When configuring redistribution from OSPF into RIP on R2 and R4, deny the networks listed in the previous bullet. Use a single standard ACL on each router.

7.4. Verify Connectivity (Advanced: 1 point)

- Verify that all IPv4 IGP prefixes that are specified in the "Lab IPv4 IGP" diagram can be reached from all devices. See the "Restrictions and Goals" section.

8. BGP Section (Total: 9 points)

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

- Configure BGP AS 100 on R1, R3, and R4.
- Configure BGP AS 500 on R5.
- Configure BGP peer relationships within AS 100 using peers R1-R3 and R1-R4.
- Configure BGP peer relationships between AS 100 and AS 500 using peers R3 and R5.
- Configure BGP peer relationships between R5 and BB in AS 500.

8.2. Advertise BGP Prefixes (Intermediate: 3 points)

- Advertise the following networks in AS 100 from R3:
  - 172.16.50.0/24
- R5 should learn the following networks in AS 500 from BB:
  - 140.10.1.0/24
  - 140.10.2.0/24
  - 140.10.3.0/24
  - 140.10.4.0/24
  - 140.10.5.0/24
  - 140.10.6.0/24
- Configure R5 to advertise all the 140.10 listed prefixes to R3.

8.3. Control BGP Routing (Intermediate: 3 points)

- Configure R3 to advertise only 172.0.0.0/8.
- Configure R3 to accept only the following networks from AS 500:
  - 140.10.2.0/24
  - 140.10.3.0/24
  - 140.10.4.0/24
  - 140.10.5.0/24
- Use the ACL with no more than two lines. Filtering should remain accurate even if additional networks are advertised by AS 500.
- The networks learned by R3 from AS 500 should be present in the BGP tables of R1 and R4.
- R4 should have only a single BGP route 140.10.2.0/24 in its IPv4 routing table; no other BGP routes are allowed on R4. Do not introduce modifications in the R4 BGP table to meet this requirement.
- R1 and R3 should be able to ping destinations on four networks learned from AS 500, and R4 should be able to ping destinations on one network learned from AS 500.

9. Router Maintenance Section (Total: 11 points)

9.1. Configure Router Provisioning (Intermediate: 3 points)

- Configure R4 to supply configuration information to a new router that will be connected to VLAN 40.
  - The new router will use interface Ethernet0/1 with the MAC address 0010.7be8.131d, and the Ethernet0/1 interface should be assigned the IP address 172.16.26.100/24.
- The new router should receive its configuration from the TFTP server 172.16.50.100 located on the VLAN 30 and should send the request for the configuration R100.cfg via R2.

9.2. Complete Private Network Connectivity (Intermediate: 2 points)

- Configure the 7.7.7.3/24 address on the R3 Ethernet0/1 interface without changing any pre-existing IP addresses.
- Do not advertise subnet 7.7.7.0/24 into any routing protocol.
- Ensure that workstations on the 7.7.7.0/24 private address space can reach the rest of the network using a portion of the address space of the R3 172.16.31.0/24 subnet.

9.3. Configure Administrator Access to R7 (Basic: 2 points)

- Ensure that the administrator can access only R7 from R3 interface Lo103, and using only Telnet.
- Apply the configuration on R7.

9.4. Monitor Network Forwarding (Intermediate: 2 points)

- Simulate traffic every 2 minutes by sending 100 test packets and monitor the jitter of this simulated traffic from R5 to R1. Provide a minimal configuration on R1.
- Provide two separate sets of simulated traffic from R5 to R1 with one set of traffic marked as precedence 4 and the second set of traffic marked as precedence 3.
- For any type of IP service that needs to be configured for the task, make sure that R1 is the server of any supporting service.

9.5. Monitor Network Traffic (Basic: 2 points)

- Provide a mechanism that can be used on R1 to count the number of packets received on the S1/0 interface.
- Packet counts should be classified by the precedence setting of the received packets.
- Do not use any access lists to fulfill this requirement.
- R5 should obtain the network time from R1 for accurate monitoring.

10. Security Section (Total: 5 points)

10.1. Configure Router Security Part 1 (Intermediate: 2 points)

- The network administrator needs to secure the following parts of the network:
  - The administrator does not want any packet to be routed in the network based on the routing path carried in the IP packet.
  - Do not allow DHCP services.
  - Ensure that abnormally terminated TCP sessions are removed.
- Develop a sample configuration that achieves these requirements and apply it on R5; apply interface-specific commands to the FastEthernet0/0 interface.

10.2. Configure Router Security Part 2 (Intermediate: 1 point)

- R4 should ignore and not reply to Bootstrap Protocol request packets received.

10.3. Configure VLAN 90 Security (Intermediate: 2 points)

- SW2 is connected to the test environment network 172.16.90.0/24. SW2 will be providing security separation between the test segment and the rest of your network.
- Provide a solution to allow traffic sourced on the network 172.16.90.0/24 only from the selected hosts addresses (.1, .3, .5, .7 in the fourth octet) to be permitted onto your network.
- Apply the solution on SW2 interface in subnet 172.16.31.0/24.
- Do not use filtering techniques based on Layer 2 filtering. Use a minimal number of statements for this task.

11. Multicast Section (Total: 3 points)

11.1. Configure Protocol Independent Multicast (PIM) (Advanced: 2 points)

- Configure multicast routing on R1, R2, R3, R4, and R6 using R1 as the shared root.
- Announce the shared root without use of any dense groups or static configurations.
- Join management loopback interfaces of R1, R2, R3, R4, and R6 to group 239.10.10.10.

11.2. Verify Multicast Connectivity (Advanced: 1 point)

- Test multicast configuration by pinging group address 239.10.10.10 from SW2.