360RSW05-WKB-CA07

Cisco 360 CCIE R&S Exercise Workbook Introduction

The Cisco 360 CCIE® R&S Version 5 Exercise Workbook contains 20 challenging scenarios at the 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 7 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 diagram.
- 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.
  - 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 7 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

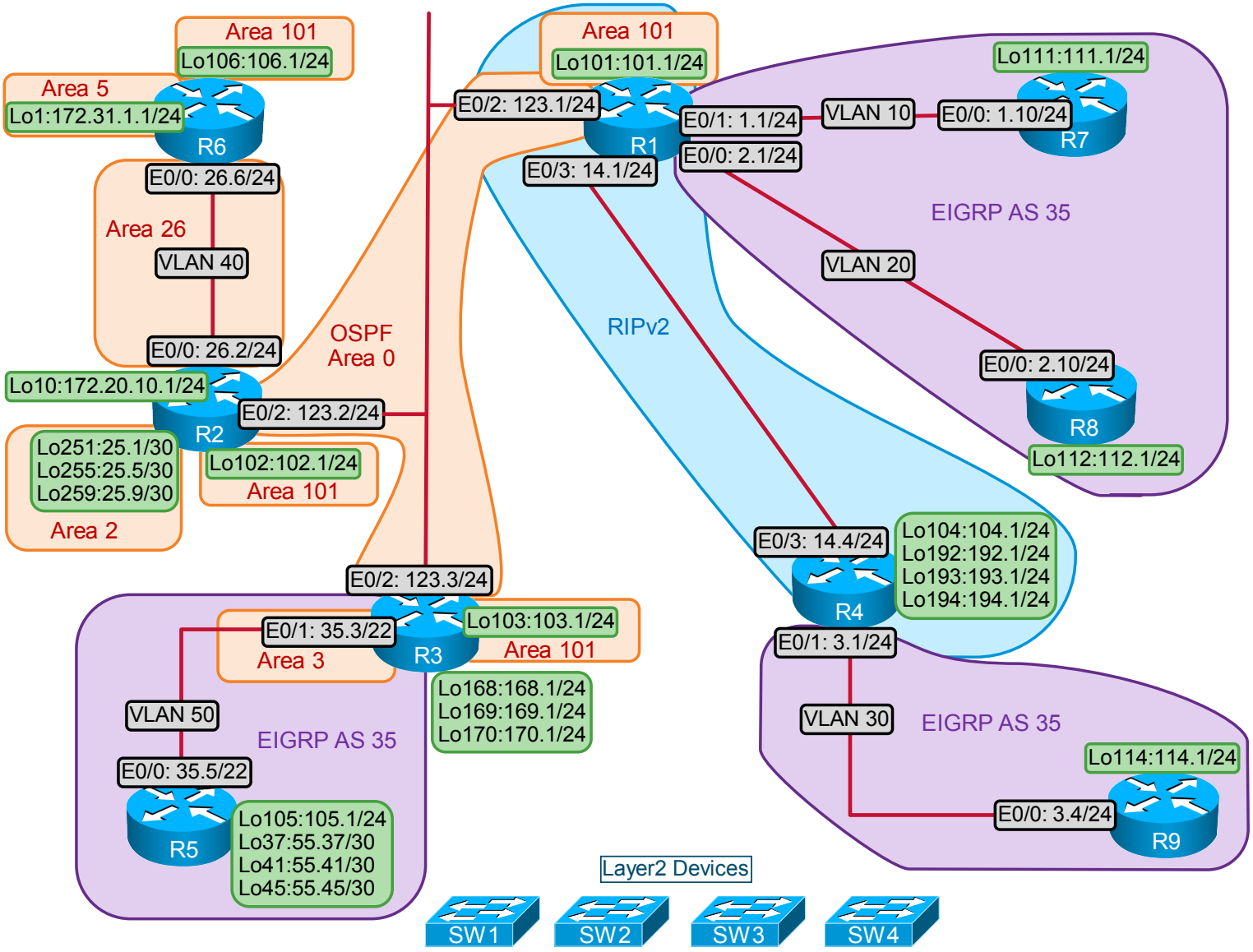
- Difficulty: Intermediate to Advanced

Restrictions and Goals

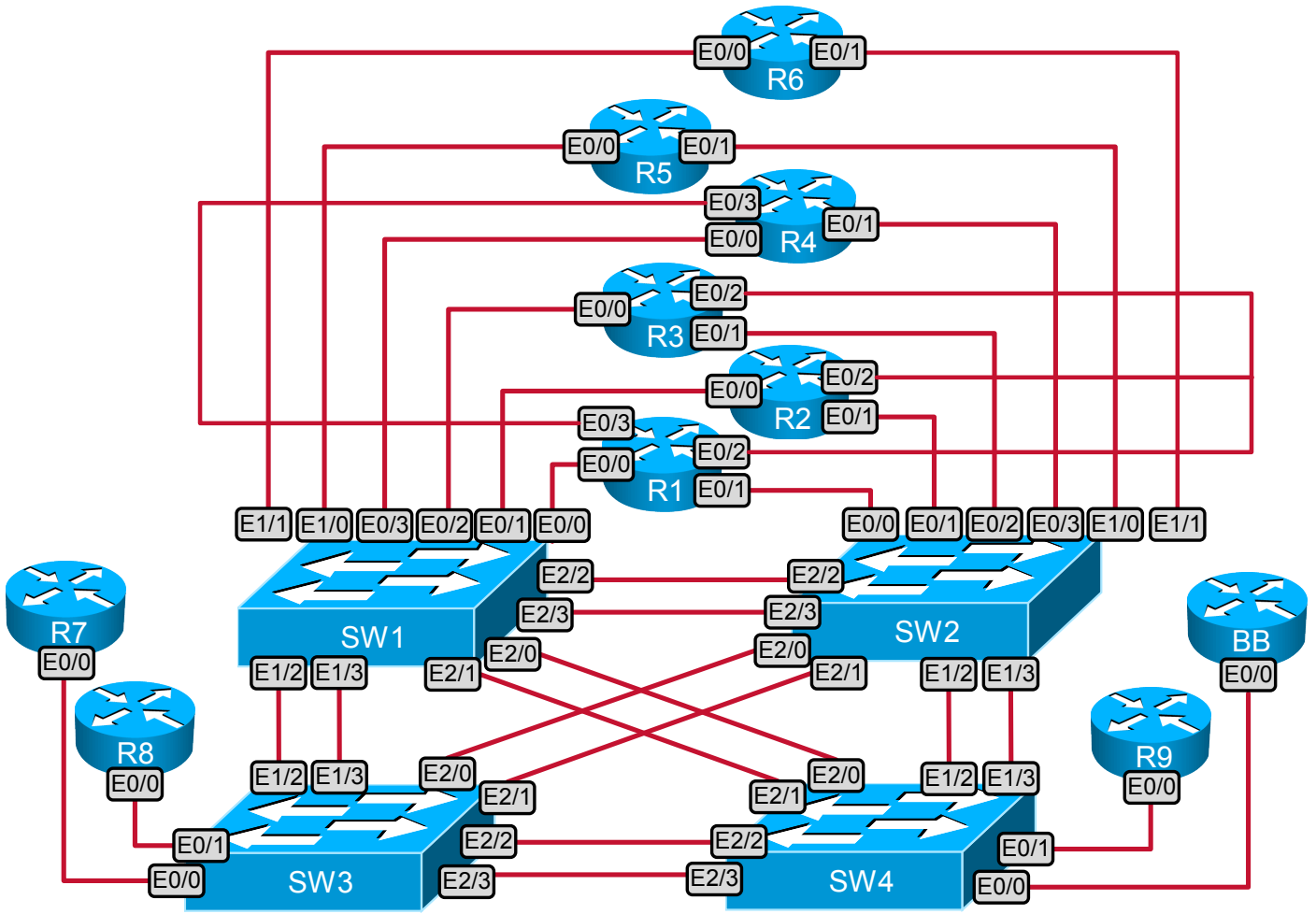
> **Note** Read this section carefully.

- 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 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 for IPv4 protocol.
- Do not use the **ip default-network** or **ip default-gateway** commands.
- All IP addresses that are involved in the same virtual routing and forwarding (VRF) instance must be reachable, unless an explicitly stated filtering requirement restricts reachability.
- Do not introduce any new IPv4 addresses, unless the instructions specifically require it.
- Networks do not have to be reachable outside of their VRF.
- Use conventional routing algorithms only, unless the instructions 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 Diagram



Ethernet Switched Cabling Topology



1. Switch Configuration Section (Total: 10 points)

1.1. Configure VLANs (Basic: 2 points)

- On SW1, SW2, SW3, and SW4, create the VLANs that are referenced in the VLAN table.

VLANs

Device	VLAN	VLAN Name
SW1	10	VLAN10
	20	VLAN20
	40	VLAN40
	50	VLAN50
SW2	10	VLAN10
	20	VLAN20
	30	VLAN30
	50	VLAN50
SW3	10	VLAN10
	20	VLAN20
	30	VLAN30
SW4	30	VLAN30

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

- Configure the following switch-to-router connections. Enable trunking on the necessary ports to fulfill connectivity requirements.

Switch-to-Router Connections

Switch	Router	VLAN
SW1	R1	VLAN 20
SW2	R1	VLAN 10
SW1	R2	VLAN 40
SW2	R3	VLAN 50
SW2	R4	VLAN 30
SW1	R5	VLAN 50
SW1	R6	VLAN 40
SW3	R7	VLAN 10
SW3	R8	VLAN 20
SW4	R9	VLAN 30

- Supply IP addresses for all specified router interfaces in the diagram.

1.3. VTP Configuration (Basic: 2 points)

- Do not advertise VLAN database information between switches, but allow VLAN information forwarding on the trunks.

1.4. Control Interswitch Links (Basic: 2 points)

- Swtich ports listed in the following table must be administratively shut down. Verify and make sure they remain in the shutdown state.

Switch Ports Shut Down

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

Switch	Port
SW3	1/2
	1/3
SW4	1/2
	1/3
	2/0
	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
SW3	2/0 2/1	SW2	2/0 2/1	Trunk dot1Q Trunk dot1Q
SW4	2/2 2/3	SW3	2/2 2/3	Trunk dot1Q Trunk dot1Q

- Configure a link between SW1 and SW2 with the aggregate bandwidth 20 Mb/s. Use ports 2/2 and 2/3 to accomplish this task.

1.5. Control VLAN Propagation (Basic: 2 points)

- For all trunks, ensure that only the necessary subsets of VLANs are allowed to pass over the trunk. Do not use VTP pruning.

2. IPv4 OSPF Section (Total: 12 points)

Note All OSPF routers must be configured with only one OSPF PID. *Points will be deducted from multiple sections for failing to assign one and only one OSPF PID on each specified router.* Use the IPv4 IGP diagram to help guide your configuration.

2.1. Create OSPF Areas on R1, R2, and R3 (Basic: 2 points)

- Configure an OSPF backbone area between routers R1, R2, and R3.
- On R2, create the following three loopback interfaces with 30-bit address masks and place them into OSPF Area 2:
    - 172.16.25.1/30
    - 172.16.25.5/30
    - 172.16.25.9/30

  Summarize the subnets with a 27-bit mask.

2.2. Control OSPF Adjacency Formation (Intermediate: 2 points)

- Do not use an OSPF network type that uses a DR/BDR on the 172.16.123.0/24 link.

2.3. Create OSPF Areas on R2, R3, and R6 (Basic: 2 points)

- Configure VLAN 40 in OSPF Area 26. Place the Loopback1 interface with the address of 172.31.1.1/24 into OSPF Area 5. Place Et0/1 on R3 into Area 3.

2.4. Control OSPF Advertisements (Advanced: 2 points)

- Advertise the following loopback subnets in OSPF Area 101:
    - 172.16.101.0/24
    - 172.16.102.0/24
    - 172.16.103.0/24
    - 172.16.106.0/24

- Assign the IP address 172.20.10.1/24 to a loopback interface on R2 and add it into the OSPF routing process as an external major network.

2.5. Configure OSPF Authentication (Advanced: 2 points)

- Authenticate the OSPF backbone area. Do not use a cleartext password. Use the password **test**.

2.6. Verify Connectivity (Basic: 2 points)

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

3. IPv4 RIP Section (Total: 8 points)

3.1. RIP Configuration (Basic: 3 points)

- Configure RIP version 2 over the connection between R1 and R4.
- Make sure that RIP advertises only over the necessary interfaces.

3.2. RIP Tuning (Intermediate: 3 points)

- Configure R1 to send two routes to R4 using RIP. One route will provide reachability to all possible IPv4 prefixes. Choose the other route to support MPLS reachability. Do not use summarization.
- Summarize these prefixes when they are redistributed into OSPF:
    - 172.16.192.0/24
    - 172.16.193.0/24
    - 172.16.194.0/24

3.3. Verify Connectivity (Basic: 2 points)

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

4. IPv4 EIGRP Section (Total: 8 points)

4.1. EIGRP Configuration (Basic: 2 points)

- Configure EIGRP AS 35 on the VLAN between R3 and R5.
- Make sure that EIGRP AS 35 advertises only over the specified interfaces.
- Configure EIGRP AS 35 on the VLAN between R4 and R9.
- Configure EIGRP AS 35 on the VLANs between R1, R7, and R8.

4.2. EIGRP Route Advertisement (Basic: 4 points)

- Advertise the following three loopback interfaces on R5 with the addresses displayed below in EIGRP AS 35:

    - 172.16.55.37/30
    - 172.16.55.41/30
    - 172.16.55.45/30

  Make sure that R3 has only a summary of these routes in its routing table.

- Advertise loopback subnet 172.16.105.0/24 in EIGRP AS 35.
- Restrict the bandwidth utilization to half of the default value for EIGRP traffic between R3 and R5.
- Advertise the minimal number of prefixes to router R5. However, make sure that R5 is able to reach all IP addresses within your pod. Do not use a 0.0.0.0/0 route.

4.3. Verify Connectivity (Basic: 2 points)

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

5. Redistribution Section (Total: 6 points)

5.1. Obtain Universal Connectivity (Intermediate: 3 points)

- Perform a mutual redistribution of dynamic interior gateway protocols:
    - Between RIP and OSPF on router R1
    - Between OSPF and EIGRP on R3
- Do not perform any other redistribution in this scenario.
- Use the **redistribute connected** command where required and not restricted by the scenario.

5.2. Verify Connectivity (Intermediate: 3 points)

- Verify that all IPv4 IGP prefixes specified on the IPv4 IGP diagram can be reached from all devices.

6. MPLS Layer 3 VPNs Section (Total: 7 points)

6.1. Configure Provider Edge Routers (Basic: 3 points)

- Configure Multiprotocol BGP between R1 and R4 using AS number 14. Peer to loopbacks 101 and 104.
- Enable the link between R1 and R4 to support VPN labels.
- Create a VPN named CustomerA on R1 and R4. Use the value 14:100 as the route distinguisher and route-target values.
- On R1, place interfaces Et0/0 and Et0/1 into the CustomerA VPN. On R4, place interface Et0/1 into this VPN.

6.2. Enable EIGRP for PE-to-CE Routing and Verify Connectivity (Intermediate: 4 points)

- Enable EIGRP AS 1 within the CustomerA VPN. Configure EIGRP AS numbers at each site to ensure that all learned VPN prefixes are EIGRP internal routes.
- Verify that IP addresses within the CustomerA VPN are fully reachable.

7. Router Maintenance Section (Total: 4 points)

7.1. Time Management Service (Basic: 2 points)

- R3 should return the system date and time to the other routers when they connect via Telnet to R3 to port 13.
- R3 should return the time in the EST zone, offset -5 hours.

7.2. Cisco IOS Features Configuration (Basic: 2 points)

- Sometimes, while switching between reverse Telnet sessions, users enter the X28 inline editor. Apply a solution to disable this editor on router R1.

8. Security Section (Total: 3 points)

8.1. Network Security (Basic: 3 points)

- The network administrator is planning to secure the network by implementing the following steps:
    - Stop sending and receiving ICMP redirects on Ethernet networks.
    - Lower the risk of being an amplifier network for any smurf attacks.
    - Prevent a quick port scan of UDP ports. A port scan is used by the attacker to find out what services are available on your network.
- Develop a sample configuration and apply it on the R9 interface associated with IP address 172.16.3.4.

9. QoS Section (Total: 5 points)

9.1. Bandwidth Allocation Configuration (Advanced: 5 points)

- On R2, limit all traffic originating from the 172.16.26.0/24 network from consuming more than 32,000 b/s of the bandwidth.
- Also, limit this same classification of traffic from the same network from consuming more than 16,000 b/s of bandwidth for a subset of this traffic that possesses a precedence setting of no higher than 2.
- Finally, limit this same classification of traffic from the same network from consuming more than 8,000 b/s of bandwidth for an additional subset of this traffic that possesses a precedence setting of 2.
- Allow for a 750-ms burst for all traffic originating from the 172.16.26.0/24 network and for a 1-second burst of the traffic of other described classes.
- Apply your QoS solution on the Ethernet0/2 interface of R2.

10. Switch Specialties Section (Total: 4 points)

10.1. Network Access Control Configuration (Intermediate: 4 points)

- Port 0/3 on SW1 is patched to the visitor room to provide connectivity to different visitors. Allow continuous access to the network for two workstations and allow either workstation to be replaced by another after 5 minutes.

11. Multicast Section (Total: 5 points)

11.1. Multicast Network Configuration (Basic: 5 points)

- Configure PIM sparse-dense mode multicast routing on routers R1, R3, and R4.
- Encapsulate the PIM and multicast data packets into GRE packets using the Ethernet0/2 interfaces between R1 and R3. Do not enable PIM on the Ethernet0/2 interface on R3.
- Enable PIM on the Ethernet0/3 interfaces between R1 and R4.
- Generate multicast traffic destined to 229.13.13.13 from the Ethernet0/2 interface of R2.
- Simulate a member of the multicast group 229.13.13.13 on routers R1, R3, and R4. Use one of the loopback interfaces.
- Simulate a member of the 229.13.13.13 multicast group on R5 using the Ethernet interface of R5.

12. Gateway Redundancy Section (Total: 4 points)

12.1. Router Selection Configuration (Intermediate: 4 points)

- On VLAN 40, configure a first-hop router selection solution that uses UDP port 3222 for end systems. The technique selection must represent multiple routers via a single IP address. The existence of the multiple routers must be completely transparent to the end systems.
- Make R2 the router that coordinates the allocation of MAC addresses in ARP responses. Make R6 its backup router.

  To fulfill the requirements of this section, limit the participation to only routers R2 and R6. Fulfill this requirement by not using any global configuration commands.

