IEWB-RS-VOL2 Lab 12

Difficulty Rating (10 highest): 7

Lab Overview:

The following scenario is a practice lab exam designed to test your skills at configuring Cisco networking devices. Specifically, this scenario is designed to assist you in your preparation for Cisco Systems' CCIE Routing & Switching Lab exam. However, remember that in addition to being designed as a simulation of the actual CCIE lab exam, this practice lab should be used as a learning tool. Instead of rushing through the lab in order to complete all the configuration steps, take the time to research the networking technology in question and gain a deeper understanding of the principles behind its operation.

Lab Instructions:

Prior to starting, ensure that the initial configuration scripts for this lab have been applied. For a current copy of these scripts, see the Internetwork Expert members' site at http://members.INE.com. If you have any questions related to the scenario solutions, visit our CCIE support forum at http://IEOC.com.

Refer to the attached diagrams for interface and protocol assignments. Any reference to X in an IP address refers to your rack number, while any reference to Y in an IP address refers to your router number.

Upon completion, all devices should have full IP reachability to all networks in the routing domain, including any networks generated by the backbone routers unless explicitly specified.

Lab Do's and Don'ts:

- Do not change or add any IP addresses from the initial configuration unless otherwise specified or required for troubleshooting
- If additional IP addresses are needed but not specifically permitted by the task use IP unnumbered
- Do not change any interface encapsulations unless otherwise specified
- Do not change the console, AUX, and VTY passwords or access methods unless otherwise specified
- Do not use any static routes, default routes, default networks, or policy routing unless otherwise specified
- Save your configurations often

Grading:

This practice lab consists of various sections totaling 79 points. A score of 64 points is required to pass the exam. A section must work 100% with the requirements given in order to be awarded the points for that section. No partial credit is awarded. If a section has multiple possible solutions, choose the solution that best meets the requirements.

Point Values:

The point values for each section are as follows:

Section	Point Value
L2 Technologies	9
IPv4	22
IPv6	10
MPLS VPN	8
Multicast	6
Security	5
Network Services	10
QoS	9

GOOD LUCK!

1. L2 Technologies

1.1 MAC Filtering

- SW1's interfaces Fa0/7 and Fa0/8 are connected to the company's public meeting room. Your corporate policy dictates that these ports should not be connected to a hub or switch to split the connection, however, your users have not been cooperating.
- In order to limit the number of PCs that can connect to the network through these ports, configure SW1 to shutdown an interface connected to the meeting room for 60 seconds if it learns more than two MAC addresses on it.
- Additionally, you have suspicions that a sales engineer has plans to circumvent the two MAC address limitation in the meeting room by connecting a router to one of the RJ-45 jacks in the room.
- Configure SW1 to stop this router which has the MAC address of 0030.1369.87a0 from communicating if it is connected to either interface Fa0/7 or Fa0/8.

3 Points

1.2 QoS

- Your company has purchased a 3Mbps service contract to the Internet using the Ethernet connection between R2 and BB2. The provider for this Ethernet service does not limit your bandwidth to 3Mbps, but instead charges your company for any unicast traffic received by BB2 over this amount.
- Configure SW2 to ensure that R2 confirms to the 3Mbps rate.
- Do not use policing to accomplish this task.

2 Points

1.3 Traffic Filtering

- The company has experienced recent security issues with PCs in VLAN 17 trying to connect to each other using Windows file and print sharing. After attempting to get the IS department to disable file and print sharing on the PCs without success, you have been tasked with ensuring that PCs in VLAN 17 cannot talk directly with each other but still can communicate with other ports or interfaces in VLAN 17.
- Use the minimum configuration needed to complete this task.

2 Points

1.4 Keepalives

- Due to limitations with the Frame Relay service provider, the switches in the cloud do not inform each other when one of their local DLCIs changes status. Therefore, if one side of the Frame Relay connection goes down the other side's local Frame Relay switch will not be informed about the status change of the remote DLCI. This, in turn, will cause the DLCI on the remote end to remain active.
- To help protect against this problem, ensure that a Frame Relay failure can be detected by having R4 and R5 poll each other to ensure that the other side's Frame Relay interface is up and reachable every 15 seconds.

2 Points

2. IPv4

Note: Do not redistribute between IGPs for this lab.

2.1 OSPF

- Configure SW4 to match exactly the output below and nothing more:

```
Rack1SW4#show ip ospf database | include Net Link States \(Area 34\)
                Summary Net Link States (Area 34)
Rack1SW4#
```

2 Points

2.2 BGP Route Reflection

Routers are configured in BGP Autonomous Systems per the diagram. The following BGP peering sessions are pre-configured for you:

Device 1	Device 2
R2	BB2
R2	R3
R2	R4
R3	R1
R1	R4
R1	SW1
SW1	SW2
SW2	BB3
SW2	R5
R5	R4
R4	R6
R6	BB1

- R4 and R5 should be configured as route-reflectors in AS 100; These devices should treat each other as non-clients.
- R1 and R3 should be designated as route-reflectors in AS 200; These devices should treat each other as non-clients.

2 Points

2.3 BGP Origination

- Advertise VLANs 3, 17, and 33 into BGP on R1 and R3.
- Advertise VLANs 45, 46, and 58 into BGP on R4 and SW2.

2 Points

2.4 BGP Bestpath Selection

- Configure AS 200 so that all traffic destined for VLAN 3 uses the Ethernet segment between SW1 and SW2.
- All traffic destined for VLAN 33 should use the Frame Relay segment between R1 and R4.
- In the case that either of these links is down, traffic should be able to be rerouted out the other link.
- The Frame Relay circuit between R2 and R4 should not be used as transit to either of these destinations.

3 Points

2.5 BGP Filtering

- In order to avoid unnecessarily transiting additional devices in the path to AS 254, the BGP policy of AS 200 states that the only link that can be used to reach AS 254 is the Frame Relay circuit between R2 and R4.
- Under no circumstance should AS 100 be allowed to use its other connections to AS 200 as transit to AS 254, regardless if the Frame Relay circuit between R2 and R4 is down.
- This configuration should be done in AS 200.

2 Points

2.6 BGP Default Routing

- Due to the memory limitations of SW1, AS 100 has agreed to send AS 200 default information. However, since AS 200 still has additional connections to AS 100, it wants to make a better routing decision based on longer prefixes. Unfortunately, AS 100 has refused to maintain a complex filtering policy for AS 200. Therefore, they have decided to send AS 200 a full view along with a default out each BGP connection.
- Configure AS 100 to reflect this policy.

2 Points

2.7 BGP Default Routing

- Since SW1 does not have the memory capacity to take a full view of the BGP table, AS 200's BGP policy dictates that the only prefix it should take from AS 100 is the default.
- Additionally, ensure that SW1 is the most preferred exit point out of AS 200 for a prefix that no other device in AS 100 has a longer match for.
- Configure SW1 to reflect this policy.

2 Points

2.8 BGP Bestpath Selection

- Since AS 100 is already using a large portion of the bandwidth on the Frame Relay circuit between R2 and R4, AS 200 does not want to send traffic for a large amount of prefixes out this link.
- Configure AS 200 so that it will only send traffic out this link that is destined for AS 100 and its directly connected customers.
- Configure this filtering in such a way that it can account for an arbitrary amount of new customers that may be connected to AS 100 in the future.
- This link should still be able to be used to send traffic out to AS 100 if there are no other longer matches throughout the BGP domain, but should only be preferred as a default exit point if SW1's connection to AS 100 is down.

2 Points

2.9 BGP Bestpath Selection

- Since R1 does have the memory capacity to take a full view of the BGP table, AS 200's BGP policy dictates that the Frame Relay circuit between R1 and R4 should be used for all prefixes that the other BGP speaking devices do not have a longer match for.
- This exit point may be used as a default connection, but only if both the Ethernet connection between SW1 and SW2 and the Frame Relay circuit between R2 and R4 is down.

2 Points

2.10 BGP Aggregation

- To ensure that your upstream peers (AS 54 and AS 254) have full IP reachability to your network, configure your border routers to advertise an aggregate block of your internal address space to these neighbors.
- In order to prevent unnecessary forwarding within your network, configure these border routers so that no other devices within your network see this aggregate address block.

3 Points

3. IPv6

3.1 IPv6 Addressing

- Enable IPv6 routing on R1, R2, R3, R4, and R6.
- Use the address 2001:CC1E:X:1::Y/64 for R1's Ethernet interface.
- Use the address 2001:CC1E:X:3::Y/64 for R3's Ethernet interface.
- Use the addresses 2001:CC1E:X:46::Y/64 for the Ethernet segment between R4 and R6.
- Use the addresses 2001:CC1E:X:23::Y/64 for the Serial connection between R2 and R3.

2 Points

3.2 IPv6 over Frame Relay

- Enable IPv6 on the Frame Relay segment between R1, R2, and R4 using the addresses 2001:CC1E:X:124::Y/64.
- Use link-local addresses in the format FE80::Y on these devices.

2 Points

3.3 EIGRP

- Configure EIGRP for the Ethernet link between R4 and R6.
- Create and advertise into EIGRP three additional Loopback interfaces on R6 with the following IPv6 addresses:
  - 2001:205:90:31::1/48
  - 2001:220:20:3::1/64
  - 2001:222:22:2::1/80
- Ensure that R4 does not advertise to R1 or R2 any IPv6 prefixes that originated in EIGRP and have a prefix length longer than 64, even if other networks are added in the future.

2 Points

3.4 OSPFv3

- Configure OSPFv3 area 0 on the Frame Relay segment between R1, R2, and R4, the FastEthernet interfaces of R1, and R3, and the serial line between R2 and R3.

2 points

3.5 IPv6 Redistribution

- Redistribute between OSPFv3 and EIGRP on R4.
- Ensure full reachability through the IPv6 enabled network, without using any default routes.

2 Points

4. MPLS VPN

4.1 VRF

R6 is preconfigured for a VRF named VPNB on the Fa0/1 interface. R5 is preconfigured for a VRF named VPNA.

- Configure SW4 for a VRF named TEST, and add interface Fa0/6 to this VRF as a Layer 3 port, using the address 10.0.0.10/24.
- Configure an OSPF process for this VRF, using the process id of 129 and area 0.

3 Points

4.2 MPLS

- Configure the connections between R4 and R5 and between R4 and R6 for MPLS, using LDP as the label protocol.

2 Points

4.3 VPNv4

- Configure BGP for a VPNv4 peering between R5 and R6. Redistribute as needed on R5 and R6 for the VRFs. Verify that SW4 can ping the VPNA loopbacks on R5.

3 Points

5. IP Multicast

PIM dense-mode is pre-configured on the following interfaces:

Device	Interface
R1	Fa0/0
R1	S0/1
R3	S1/2
R2	S0/1
R2	Fa0/0

PIM sparse-mode should be used on the following interfaces:

Device	Interfaces
SW2	VL58
R5	Fa0/0, Fa0/1
R4	Fa0/0, Fa0/1
R6	Fa0/0

5.1 Multicast Distribution

- There is a Windows Media Server located on VLAN 17 that is streaming a video feed into your network. This feed is using the multicast group address 225.25.25.25 and the UDP port 31337. Users in VLAN 22 have been complaining that they are unable to receive traffic for this group.

After looking into the problem further, it seems that R3 is having issues with sending multicast packets out the PPP link to R2, but can send unicast and broadcast packets. Since you have been unable to determine why this is happening, you have opened a case with TAC, however, hosts in VLAN 22 need access to this group immediately.

- Configure your network so that these hosts can receive traffic from this group.
- Do not enable PIM on any additional interfaces to accomplish this.

3 Points

5.2 Static RP

- Create Loopback1 on R4 and R5 using the IP address 150.X.0.255/32.
- Advertise these interfaces into OSPF area 0 on R4 and R5.
- Configure R6 and SW2 to use R4 150.X.0.255 as the RP for all multicast groups.
- R4 and R5 should exchange information on active multicast sources with each other.

3 Points

6. Security

6.1 Traffic Filtering

- Recent security monitoring of your network has indicated that various unauthorized devices have been attempting to telnet to R6 and gain access to the CLI. The only legitimate device in your network that should be allowed to telnet to R6 is the NMS located at 129.X.46.100.
- In order to detect these unauthorized attempts as they occur, configure R6 to deny and log all attempts to access it via telnet.
- Ensure that your NMS can still access R6 via telnet.

2 Points

6.2 Router Hardening

- Your security manager is worried about frequent hacker attacks trying to bruteforce the access password for R2.
- In order to minimize the effectiveness of bruteforce attacks, configure R2 to block any login attempts for 5 minutes after 10 unsuccessful attempts in a minute.
- Ensure that users connecting from your internal network 129.X.0.0/16 are not affected by this configuration

3 Points

7. IP and IOS Features

7.1 Logging

- After telnet logging had been configured on R6, it had been determined that there are too many devices attempting to access it to keep track of just by looking at the console output. In order to store and parse these log messages at a later date, the syslog service has been enabled on the NMS. NMS is located at 2001:CC1E:X:1::100, where X is your rack number.
- Configure R6 to send its logged access-list hits to this device.
- A log message should only be generated once 10 access-list hits have been accumulated.

2 Points

7.2 NTP

- Configure NTP on all of your devices throughout the network in order to accomplish this.
    - R3 and R6 should be the NTP servers.
    - R1, R2, and SW1 should get their time from R4.
    - R4, R5, and SW2 should get their time from R6.
    - All devices in BGP AS 100 are physically located in Chicago, IL (CST -6), while all devices in BGP AS 200 are physically located in Reno, NV (PST -8).
- Configure these devices to reflect the appropriate time zone and daylight savings time configuration.
- Configure SW3 and SW4 in such a way that they will display the exact time and date of the last restart using the **`show version`** command.

3 Points

7.3 DNS

- As your network has grown, it has become increasingly difficult to keep track of all the IP addresses of your network devices.
- In order to ease your device management and identification, configure R3 to provide hostname to IP address mappings for your network devices.
- Configure R1, R2, and SW1 to use R3 as the DNS server.
- Add three "A" records to the DNS database, namely Rack**X**R1, Rack**X**R2, and Rack**X**SW1, pointing to the respective devices Loopback0 IP addresses.

2 Points

7.4 Default Gateway Redundancy

- Configure R4 and R5 to represent a virtual gateway on VLAN45 with the IP address of 129.X.45.6
- R5 is the least loaded of the two routers, so it must receive about 70% of clients' traffic.
- R4 should respond to ARP requests sent by clients on VLAN45.

3 Points

8. QoS

8.1 Frame Relay Traffic Shaping

- VoIP users on VLAN 46 and behind BB2 have been complaining about intermittent voice cutouts when making phone calls. After further investigation, you have determined that the utilization of the Frame Relay circuit between R2 and R4 is well within normal parameters. However, it seems that the VoIP traffic is getting delayed behind larger data packets. To partly resolve this issue, your design team has asked you to configure Frame Relay Traffic Shaping to minimize the amount of delay that this VoIP traffic must endure.
- The Frame Relay circuit between R2 and R4 has been provisioned at 512Kbps; ensure that neither of these devices sends traffic beyond this rate on this circuit.

- Additional VCs on R4 should equally share the remaining bandwidth of its T1 interface to the Frame Relay cloud.
- In order to allow VoIP traffic to be interleaved between larger data conversations, ensure that the maximum time it takes to transmit a packet across the Frame Relay network is 10ms.

3 Points

8.2 Priority Queueing

- Now that the Frame Relay network is configured to conform to its provisioned rate, configure your network so that all VoIP traffic (UDP 16384 – 32767) for VLAN 46 that traverses the Frame Relay circuit between R4 and R2 gets priority over data traffic.
- VoIP should be allocated a maximum of 192Kbps during periods of congestion on this link.

3 Points

8.3 Traffic Marking

- There is a server in VLAN58 that hosts HTTP and STMP applications.
- Configure SW3 to mark HTTP responses entering on the port connected to R5 using DSCP value of AF21.
- At the same time, STMP reply traffic should be marked with DSCP value of AF23.
- In addition to that, limit the cumulative rate of HTTP and SMTP traffic to 2Mbps.

3 Points

