IEWB-RS-VOL2 Lab 16

Difficulty Rating (10 highest): 8

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
Layer 2 Technologies	14
IPv4	24
IPv6	9
MPLS VPN	0
Multicast	6
Security	5
Network Services	11
QoS	10

GOOD LUCK!

1. Layer 2 Technologies

1.1 Pruning

- Some time ago a new switch was installed in your network that had a high configuration revision number and it erroneously overwrote your entire VTP domain.
- In order to protect against this type of misconfiguration in the future your new corporate policy dictates that all switches must run in VTP transparent mode. However since SW1, SW2, SW3, and SW4 are not advertising VLAN information to each other they cannot participate in VTP pruning. This has resulted in a large amount of unnecessary broadcast traffic being sent over your trunk links.
- In order to solve this problem manually configure your network to behave as though VTP pruning has been enabled.
- Trunk only the necessary VLANs on SW2's trunk to R6.

3 Points

1.2 Metro Ethernet

- SW1 and SW2 have been preconfigured to provide transparent layer 2 transit for VLAN 45 between SW3 and SW4 using the metro tags of 100 and 200.
- Configure interfaces Fa0/13 - 14 on SW3 and interfaces Fa0/16 - 17 on SW4 as access links that forward traffic for VLAN 45.
- SW3 and SW4 should see each other via CDP on these interfaces.

3 Points

1.3 Bridging over Frame Relay

- Users on VLAN 16 and VLAN 22 are running a legacy application that only supports broadcast transmission. In order to support this application your design team has decided to bridge these two segments together. Configure your network to that traffic between these two segments can be bridged.
- Ensure that the rest of the routing domain can still communicate with these segments.

3 Points

1.4 L2 Protocol Tunneling

- Provide a protection against multicast packet flooding for the metro Ethernet connection between SW3 and SW4.
- Provider-Edge interfaces should drop STP packets once their rate exceeds 100 per second.
- Ensure that your configuration does not affect CDP or VTP packets.

3 Points

1.5 MPLS

- After reading some articles on the benefits of label switching, your CTO has decided to start a pilot project of MPLS on the network.
- Configure MPLS to run on R4 and R5
- Specifically the Ethernet link between R4 and R5 should be utilized for this transport.
- Do not use the “implicit-null” label in your network.
- R4 and R5 must originate label bindings for their own loopback addresses

2 Points

2. IPv4

The customer is currently running OSPF Area 0 throughout their network. Some changes are necessary.

2.1 OSPF

- Configure OSPF area 3457 on VLAN 45 between R4 & R5 and on VLAN 47 between R4 & SW1.
- Configure OSPF area 3457 on the Frame Relay network between R3, R4, and R5.

- The Frame Relay circuit between R3 and R4 has a provisioned rate of 1024Kbps, while the circuit between R3 and R5 is only provisioned at 512Kbps. Ensure that R3 takes this into account when computing OSPF metrics on this segment.
- Advertise the Loopback 0 addresses of these devices into area 3457.

3 Points

2.2 OSPF

- Configure OSPF area 51 on the 192.10.X.0/24 subnet between R1, R2, R6, and BB2.
- Advertise the Loopback 0 addresses of R1, R2, and R6 into OSPF area 51.
- In order to reduce the amount of prefixes necessary in the IGP tables throughout the routing domain, configure your network so that OSPF enabled devices outside of area 51 only see one route to R1 and R2's Loopback 0 networks. This route should be as specific as possible and not unnecessarily overlap any address space.

3 Points

2.3 OSPF

- Configure OSPF area 38 on VLAN 38 between R3 and SW2.
- Advertise the Loopback 0 address of SW2 into OSPF area 38.
- OSPF area 3457 connects to public areas of your network infrastructure. Since services offered in OSPF area 38 are of a business confidential nature your corporate policy dictates that devices in area 3457 should not have access to the resources of area 38.
- Configure R3 to reflect this policy.

3 Points

2.4 OSPF

- You have noticed very high CPU utilization on R3. After further investigation it appears that many consecutive changes in the OSPF topology are causing R3 to constantly run its SPF algorithm over and over. In order to help deal with this issue until the topology changes are diagnosed configure R3 so that it waits 4 seconds after receiving a link state update packet before running SPF.
- Additionally configure R3 so that it waits at least 10 seconds between consecutively running the SPF algorithm.

3 Points

2.5 BGP Communities

- To ease in the identification and traffic engineering of prefixes learned from their upstream peer, AS 100 has implemented a clearly defined routing policy based on community values. This policy states that prefixes learned from AS 54 should be tagged with community values as follows:

    - Prefixes originated in AS 54 and learned from BB1 should be tagged with the community *54:1*
    - Prefixes originated in AS 54 and learned from BB3 should be tagged with the community *54:3*
    - Prefixes not originated in AS 54 and learned from BB1 should be tagged with the community *X:1*, where X is the originating autonomous system.
    - Prefixes not originated in AS 54 and learned from BB3 should be tagged with the community *X:3*, where X is the originating autonomous system.

- Configure R6 to reflect this policy.

3 Points

2.6 BGP Bestpath Selection

- Configure your network so that R6 prefers to use the PPPoFR link for prefixes in the community *54:1*.
- Configure your network so that R6 prefers to use the Ethernet link to BB3 for prefixes in the community *X:3*.
- Do not use local-preference to accomplish this.

3 Points

2.7 BGP Bestpath Selection

- Configure AS 200 so that all traffic destined for prefixes in the *54:1* community come in the Serial link between R1 and R3.
- Configure AS 200 so that all traffic destined for prefixes in the *X:3* community come in the Serial link between R2 and R3.
- Do not use MED to accomplish this.

3 Points

2.8 BGP Bestpath Selection

- Configure AS 300 so that all traffic destined for VLAN 5 comes in the PPP link between R3 and R1.
- Traffic should be rerouted to the other PPP link in the case that the first fails.
- Do not use AS-Path prepending to accomplish this.

3 Points

3. IPv6

3.1 IPv6 Tunneling

- Configure an IPv6IP tunnel between R5 and R6 to connect their IPv6 segments.
- These tunnels should be sourced from their respective Loopback0 networks.
- Use the addressing format 2001:CC1E:X:56::Y/64.

3 Points

3.2 IPv6 Traffic Engineering

- Configure the network so that R4 sends IPv6 traffic from R6 destined for R5 directly to R5.
- Traffic from R5 back to R6 should go via R4.
- Do not modify any OSPF cost values to accomplish this.

3 Points

3.3 EIGRPv6

- Enable EIGRPv6 on all interfaces running IPv6.
- R6 should advertise the minimum amount of EIGRPv6 routes to R5 necessary for it to reach all of R6’s prefixes.
- R6 should not advertise any address space that it does not have a more specific route for.

3 Points

4. MPLS VPN

No scenarios in this section.

5. Multicast

5.1 RP Assignment

- Multicast servers are located on VLANs 45 and 63 in your network.
- The servers in VLAN 45 are sending to groups in the range of 224.0.0.0/5.
- The servers in VLAN 64 are sending to groups in the range of 232.0.0.0/5, with the exception of the administratively scoped range.
- Configure R3 to assign R4 as the RP for the servers in VLAN 45 and R6 as the RP for the servers in VLAN 63.
- In the case that R4 is unreachable R5 should be the RP for the servers in VLAN 45.
- Groups in the administratively scoped multicast range should not be distributed throughout the multicast domain in either a sparse or dense fashion.

3 Points

5.2 RP Security

- Your network security team is concerned with your RP information leaking outside of your internal network. To prevent this configure R6 so that your RP information is not advertised out to devices in VLAN 63.

3 Points

6. Security

6.1 Source Verification

- Your security team has expressed concerns with the possibility of traffic sent from spoofed IP addresses being received inbound on R2's connection to BB2.

- In order to protect against this vulnerability configure R2 to drop any packets without a verifiable source IP address that are received from BB2.

2 Points

6.2 Traffic Filtering

- Your security team has informed you that a large amount of traffic coming in from R6’s connection to BB1 is being sourced from RFC 1918 address space.
- Configure R6 to drop this traffic when it is received.

3 Points

7. Network Services

7.1 Authentication Failure Message

- Recently your security team has reported that someone is attempting a brute force attack on various devices throughout your network. Apparently this person seems to know that routers which display a “% Login invalid” message do not have AAA enabled and is specifically targeting these devices. In order to help discourage these attacks in the future the security team has requested that your border routers be configured to display a custom authentication failed message.
- Users who fail to authenticate should be given the message below:

```
"Authentication Failed. Username or Password was Incorrect"
```

- As an additional measure to thwart these attacks on your network in the future, configure these devices to disconnect a session after one failed login attempt.

3 Points

7.2 Authentication Prompt

- The security team has also recommended that when users telnet into the border routers they should be presented with the username prompt of “Login Name: “ and the password prompt of “Passcode: “.

- Configure the border routers to reflect this.

2 Points

7.3 Port Redirection

- Further monitoring of R6 has shown that most of the brute force attacks are going to the IP addresses of the interfaces connected to BB1 and BB3. In order to distract hackers and analyze their attack techniques your security team has installed a VMware honeypot terminal in VLAN 16 with a blank root password.
- Configure R6 so that all telnet and SSH requests sent to its outside interfaces are redirected to the honeypot.
- This machine’s IP address is 192.10.X.112.

3 Points

7.4 Address Manipulation

- Configure a new Loopback interface on R4 using the 154.X.44.0/24 subnet.
- Configure R4 to automatically source all telnet sessions off this new Loopback interface.
- Without advertising this Loopback, ensure that users on R4 can successfully telnet to all devices in your network.

3 Points

8. QoS

8.1. Frame Relay Traffic Shaping

- The Frame Relay interfaces of R3, R4, and R5 all physically support a speed of T1, however the Frame Relay circuits are not provisioned in this way. The circuit between R3 and R5 is provisioned at 512Kbps while the circuit between R4 and R5 is provisioned at 1024Kbps.

- Configure FRTS so that all end points of the network conform to the provisioned rate.
- Both spokes should be allowed to burst up to their access-rate if they have accumulated credit.

3 Points

8.2 Application Filtering

- Administrators of your network have been having Quake 3 tournaments during lunch. Your management has expressed that this is not a problem as long as they're not playing Quake during normal business hours.
- Configure R5 so that these administrators can only play Quake 3 before business hours, during their lunch break, and after hours.
- Work starts at 9am, ends at 5pm, and the lunch hour is noon to 1pm.
- The Quake 3 server is located on VLAN 5 with the IP address of 154.X.5.100 and is sending Quake 3 traffic out using UDP port 27960.
- The administrators that are playing are on located on VLANs 47 and 3003.
- Do not apply an access-group to any interface to accomplish this.

3 Points

8.3 Prioritization

- The administrators on VLAN 3003 have been complaining that they are getting 0wned while playing Quake due to high ping times. Since they are only playing during off hours you have decided to help them out and decrease the latency of their packets. Configure your network so that the Quake 3 traffic coming from the server is prioritized on its way to VLAN 3003.
- This traffic should be allotted as much bandwidth as necessary.

2 Points

8.4 Link Efficiency

- Due to slow speed of the Serial links connecting R1 and R2 with R3, you have been tasked to come with a solution that improves bandwidth usage.

- Use the Lempel-Ziv based algorithm that is more CPU intensive but requires less memory usage.

2 Points