IEWB-RS-VOL2 Lab 18

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
Layer 2 Technologies	0
IPv4	21
IPv6	3
MPLS VPN	0
Multicast	7
Security	9
Network Services	20
QoS	19

GOOD LUCK!

1. Layer 2 Technologies

Note: All Layer2 information has been pre-configured in this lab. SW3 and SW4 only require IPv4 reachability to each other.

2. IPv4

2.1 EIGRP

- Enable EIGRP 10 on R6's Frame Relay connection to BB1.
- Authenticate the adjacency between these devices with an MD5 hash value that represents the password CISCO.
- Use key 1 for this authentication.
- Redistribute between EIGRP processes.

3 Points

2.2 EIGRP

- Configure the network so that hosts in VLAN 8 use VLAN 18 to reach all hosts with an even number in the third octet, while VLAN 58 is used to reach all hosts with an odd number in the third octet.
- Ensure that traffic is rerouted within 5 seconds if SW2 loses connectivity to either R1 or R5.

3 Points

2.3 EIGRP

- Network monitoring has reported congestion on the Frame Relay circuits between R1, R3, and R5. After further investigation it appears that constant changes in the routing topology are causing EIGRP to consume half of the link bandwidth on the Frame Relay circuits.
- In order to help deal with this problem until the cause of the topology changes is tracked down configure your network so that EIGRP cannot use more that 10% of the bandwidth on these Frame Relay circuits.

2 Points

2.4 EIGRP

- Engineers in your network operations center have recently noticed that the %DUAL-3-SIA message has been periodically appearing in your syslog server logs. After further investigation you have determined that the constant changes in the EIGRP topology have been overwhelming R3's CPU, which in turn is delaying its replies to EIGRP query messages.
- In order to help manage this problem while the source of the topology changes is found configure routers in the EIGRP domain to wait up to 5 minutes for a response to an EIGRP query message.

2 Points

2.5 On-Demand Routing

- R4's only connection to the rest of the routing domain is through R5. Therefore it does not need specific reachability information about the rest of your network.
- Configure R5 so that it can learn about R4's stub networks via CDP.
- Ensure that hosts on VLANs 4 and 44 have connectivity to the rest of your network.

2 Points

3.1 BGP Peering

- After attempting in vain to establish the BGP peering session between R5 and BB2 you have called AS 254 to see what the problem is. After hours of escalation you have come to realize that the administrators of BB2 mistakenly configured your remote-as number as 200, and have failed to tell you that their BGP peering sessions require MD5 authentication. Luckily they have told you that the password for authentication is CISCO. However their remote-as configuration statement cannot be changed until the next maintenance window which is not scheduled for another few months.
- Configure R5 to peer with BB2 and support their configuration in the meantime.

3 Points

3.2 NLRI Advertisement

- To ensure that your upstream peers have full IP reachability to your internal network advertise all of your IGP learned networks into BGP.
- Do not use the **`network`** statement under BGP to accomplish this.

3 Points

3.3 BGP Reachability

- In order to reduce the memory utilization throughout your network your design team has opted not to run BGP on any device besides R5 and R6.
- Configure the network in such a way that these routers still have reachability to all BGP learned prefixes, but do not need to carry a full view of the Internet routing table.
- Ensure that this configuration does not withdraw any previously learned IGP information.

3 Points

3. IPv6

2.6 NAT-PT

- The network administrator has requested that R3 provide communication so that a host running only IPv6 can communicate with one of your servers running only IPv4.
- The IPv6 host's address is 2001:CC1E:X:3::100.
- The IPv4 server's address is 156.X.8.100.
- The IPv6 host should see the IPv4 server as 2001:CC1E:FFFF::100.
- The IPv4 server should see the IPv6 host as 156.X.8.50.
- Configure R3 to reflect this request.

3 Points

4. MPLS VPN

No scenarios in this section.

5. IP Multicast

5.1 RP Assignments

- Configure R1 and R5 as candidate RPs for your multicast network via Auto-RP.
- Configure SW2 as the mapping agent for these RPs.
- R1 should service the multicast groups 224.0.0.0 – 231.255.255.255.
- R5 should service the multicast groups 232.0.0.0 – 239.255.255.255.

3 Points

5.2 Multicast Testing

- There will be a multicast media server installed in VLAN 8 in the near future. In order to facilitate in testing your multicast routing before this server is installed, configure R3's interface Fa0/0 to join multicast groups 224.24.24.24 and 232.32.32.32.
- Ensure that R3 responds to ICMP echo requests sent from SW2's interface VLAN 8 destined for these two groups.

2 Points

5.3 Multicast Filtering

- After implementing the above configuration you have been getting complaints from users on VLAN 3 trying to access the multicast feed originated by the server in VLAN 8. After further investigation, you have determined that a device inside of AS 54 is mistakenly being used as the RP for this group. In order to prevent this problem from occurring in the future, configure your network so that the Auto-RP announce and discovery messages cannot be sent to or received from BB3.

2 Points

6. Security

7.1 SSH

- Your security team has informed you that they are concerned about clear text telnet traffic being used to manage your Catalyst switches.
- Configure SW1 and SW2 so that they can be access remotely in a secure manner.
- The domain name used to generate RSA keys on SW1 and SW2 should be InternetworkExpert.com.
- For maximum security configure SW1 and SW2 with a key length of 2048 bits.
- Ensure that SW1 and SW2 can no longer be accessed via regular text telnet.

3 Points

7.2 Traffic Filtering

- Your security team has asked you to implement a filtering policy for hosts located on VLANs 4 and 44. Configure R4 to conform to this policy as follows:
    - Hosts in VLANs 4 and 44 should be able to initiate VoIP calls to any destination using the H.323 codec.
    - Hosts in VLANs 4 and 44 should be able to browse the web at ports 80, 443, and 8080.
    - The FTP server located at 156.X.4.40 should be allowed to accept active FTP sessions.
    - Traffic between VLANs 4 and 44 should be unfiltered.
- All other traffic from these segments should be dropped.

3 Points

7.3 PPP Authentication

- PPP is configured on the link between R4 and R5.
- R5 should authenticate R4 across this link, but R4 should not authenticate R5.
- Configure R5 to request CHAP authentication
- If CHAP authentication is rejected by R4, R5 should offer PAP authentication.
- Configure R4 to refuse CHAP authentication offered during the LCP negotiation.
- R4 should send the username of ROUTER4 and the password of CISCO for PAP authentication.

3 Points

7. Network Services

4.1 Syslog

- You have been tasked with configuring R2 to log all critical and below messages to a syslog server at IP address 156.X.8.100.
- In order to organize these messages the syslog server will be expecting R2 to use the facility local2.
- You suspect that someone may be tampering with R2's syslog messages on the syslog server itself. You believe that certain messages relating to configuration changes on R2 are being deleted by a NOC engineer in an attempt to circumvent your change control policy.
- Configure R2 to send its syslog messages in such a way that you can determine if any of R2's syslog messages have been deleted from the server.

2 Points

4.2 Logging

- After reviewing your syslog logs it seems that someone is in fact deleting messages from the server. In order to determine what type of messages are being deleted configure R2 to track the number and type of log messages being generated and store this information locally.

2 Points

4.3 DNS

- Recently your internal DNS server failed and your network administrators have asked you to configure R6 as a DNS server while your normal server undergoes repair.
- Configure R6 in such a way that when you issue the command **`ping host`** from any of your devices, where *host* is the hostname of any of your routers 1 through 6 or Switches 1 through 4, R6 receives requests for **`host.ine.com`** and resolves.

3 Points

4.4 Traceroute

- Recently administrators in your NOC have been complaining that it is too hard to decode the output from a traceroute going through your network. Apparently every time they traceroute they have to look at the IP addressing table to see which device has which IP address. They have requested that all devices in the network simply reply to a traceroute from their Loopback 0 interfaces. Although the other engineers on your team have told the NOC engineers that this is not possible, you know that it can be done. In order to show off your skills to your coworkers, configure R1 so that it always replies to a traceroute from its Loopback 0 interface.

4 Points

4.5 EEM

- If the transmit load value on R6's Frame-Relay interface goes over 1,000 Bytes per second, averaged over 4 seconds, EIGRP should be reconfigured to utilize "load" as part of the metrics.
- Use a chassis-id of RackX-R6 where 'X' is your rack number.

4 Points

4.6 Logging

- Other routers should detect the change to EIGRP and add "load" to their EIGRP processes as well

2 Points

7.4 Layer 2 Filtering

- Configure SW2 so that only PPPoE connections are allowed on VLAN8.
- You solution should account for any future ports added to VLAN 8.

3 Points

8. QoS

6.1 Traffic Limiting

- Recently an Ethernet drop has been installed in your network as a new connection to the Internet. This link terminates at a public peering point, and is used to connect to both BB2 and BB3. Although the interface that R5 is using to connect to these upstream peers is a 10Mbps Ethernet connection, the provisioned rates for these circuits are much lower. BB2 will only allow R5 to send traffic across this link at a maximum of 2.5Mbps. BB3 will only allow R5 to send traffic into its network at a maximum rate of 3Mbps.
- Configure R5 to conform to these provisioned rates.

3 Points

6.2 Priority Queueing

- VoIP users connected to VLAN 4 have been complaining about poor voice quality when calling other users behind BB2.
- In order to help improve voice quality configure your network so that 64Kbps of bidirectional VoIP traffic is guaranteed to be dequeued first over the Serial link between R4 and R5.
- Additionally, to ensure that this VoIP traffic does not endure additional delay when sent out to BB2, configure R5 so that 64Kbps of this VoIP traffic is guaranteed to be dequeued first out the Ethernet link.

3 Points

6.3 Traffic Limiting

- As preventative maintenance against DoS attacks being launched from your network your security team has requested that you limit all ICMP traffic to a maximum of 16Kbps when implementing your QoS policy out to BB2 and BB3.
- Configure R5 to reflect this policy.

3 Points

6.4 DSCP Marking

- Lastly to try to fool BB2 and BB3 into providing your data traffic with expedited forwarding configure R5 so that all traffic sent out to both BB2 and BB3 is marked with a DSCP value of 101110.

3 Points

6.5 Policing

- Hosts attached to ports Fa0/10 and Fa0/11 on SW1 have been sending an inordinate amount of traffic into the network. Most of this traffic is specifically being set with DSCP values of EF and CS5.
- Configure SW1 to limit the reception of this traffic from these ports to 1Mbps.
- Traffic above this rate should be dropped.

3 Points

6.6 Per-Port Per-VLAN Policing

- Configure QoS marking in SW1 per the following requirements:
    - Set IP precedence to 3 for ICMP packets on VLAN52 and limit it the input rate to 256Kbps.
    - Set IP precedence to 4 for TCP packets on VLAN53 and limit the input rate to 512Kbps.
    - Remark the exceeding TCP packets on VLAN53 with DSCP value of CS1.
- Packets enter the trunk link marked with DSCP value of CS0.
- Do not use the interface-level policing to accomplish this task.

4 Points

