IEWB-RS-VOL2 Lab 17

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	3
IPv4	19
IPv6	0
MPLS VPN	0
Multicast	7
Security	22
Network Services	17
QoS	11

GOOD LUCK!

1. Layer 2 Technologies

Layer 2 settings have been configured to match the diagram supplied with the lab. Refer to the switches configuration for more information.

1.1 Fault Tolerance

- The Serial link between R4 and R5 will be used as a backup of the Frame Relay circuit between them.
- Configure the network in such a way that this link is activated if the Frame Relay circuit between these devices goes down at any point throughout the provider cloud.

3 Points

2. IPv4

2.1 OSPF

- Configure OSPF area 137 on VLAN 137 between R1, R3, and SW1.
- R1 connects to VLAN 137 with a FastEthernet interface, while R3 connects to VLAN 137 with a regular Ethernet interface. Configure the network so that SW1 takes this factor into account when it is computing the OSPF cost to reach destinations through these neighbors.

2 Points

2.2 OSPF

- Configure OSPF area 23 on VLAN 23 between R2, R3, & SW2, and VLAN 8 on SW2.
- Advertise the Loopback 0 interfaces of SW1 and SW2 into the OSPF domain, but do not use the **`network`** statement under the OSPF process to accomplish this.

2 Points

2.3 IGP Redistribution

- Redistribute between OSPF and EIGRP on R5.
- In order to ensure optimal routing within the OSPF domain configure your network so that routes redistributed in from EIGRP have a cumulative metric throughout the OSPF domain.

2 Points

2.4 IGP Redistribution

- Redistribute between OSPF and RIP on SW1.
- To minimize the amount of prefixes in the routing table configure your network so that all devices except SW1 see only one route for the prefixes learned from BB3 via RIP.
- This route should be as specific as possible and not unnecessarily overlap any address space.

2 Points

2.5 OSPF

- Since SW2 has no choice to reach external parts of the network other than to go through R2 or R3 it does not need specific reachability information about these external prefixes. However since R2 and R3 have various connections to the rest of the internal network it is advisable for SW2 to have reachability information about the internal OSPF network.
- Additionally since R2 only has the single low speed Frame Relay circuit that connects to the rest of the network SW2 should send all traffic to R3 that is destined for prefixes outside of the OSPF domain.
- Configure your network to reflect this specification.

3 Points

2.6 BGP Filtering

BGP has been pre-configured according to the following description:

- *Autonomous systems assigned per the diagram.*
- *Fully meshed iBGP peerings within AS 100.*
- *Fully meshed iBGP peerings within AS 200.*
- *eBGP peering session between SW1 and BB3.*
- *eBGP peering sessions between R1 and R5, R2 and R5*
- *eBGP peering session between R5 and BB2.*

- Configure AS 100 so that it cannot be used as a transit AS for customers in AS 54 to reach AS 200, and vice versa.
- Do not use access-list, prefix-list, or AS-Path access-list filtering to accomplish this.

3 Points

2.7 BGP Peering

- In order to avoid transiting the already congested Frame Relay circuit between R2 and R5 configure AS 100 so that it sends all traffic destined to AS 254 out the Frame Relay connection between R1 and R5.
- This configuration should be done on R2.
- Do not use local-preference to accomplish this.

3 Points

2.8 BGP Timers

- Tune BGP timers in R5 to run the BGP scanner three times more often than by default.
- Ensure that R5 waits for no more that 12 seconds before sending the initial BGP update.

2 Points

3. IPv6

No scenarios in this section.

4. MPLS VPN

No scenarios in this section.

5. IP Multicast

5.1 PIM

- Users on VLAN 46 want to join the multicast group 227.69.53.7 that is going to be streamed into your network from BB3. However since these are the only users in the network that you want to receive multicast feeds you do not want to enable multicast routing everywhere in your network.
- Configure your network to accommodate these users without affecting any other devices in the transit path.
- Do not use any RP assignments to accomplish this.

2 Points

5.2 Multicast Testing

- To ensure that this setup will work before the multicast stream is injected, configure your network so that R4 will respond to ICMP echo requests sent from SW1's interface Fa0/24 to the group 227.69.53.7.

2 Points

5.3 Multicast Filtering

- Your design team does not want any multicast streams to be delivered to hosts on VLAN 46 other than the 227.69.53.7 group coming from behind BB3.
- Configure SW1 to reflect this policy.
- Do not use the **`ip multicast boundary`** command to accomplish this.

3 Points

6. Security

6.1 Traffic Filtering

- Recent traffic monitoring of your network has indicated that various hosts from behind BB1 are performing port scans on your network. Configure R6 so that these hosts are denied entry into your network. The IP addresses of these hosts are as follows:

    - 200.0.1.2
    - 200.0.3.2
    - 200.0.3.10
    - 200.0.1.18
    - 200.0.3.26
    - 200.0.1.10
    - 200.0.3.18
    - 200.0.1.26

- Use the minimum amount of lines necessary to complete this task.
- Do not deny traffic from any other hosts.

2 Points

6.2 Attack Mitigation

- Recently monitoring of your web server on VLAN 5 has shown an inordinate amount of half open TCP sessions, possibly indicating a DoS attack. In order to reduce the load on the server while the possibility of attack is investigated configure R5 to that TCP requests sent to this server are limited to a maximum of 500Kbps.

2 Points

6.3 Traffic Filtering

- Hosts on VLAN44 of R4 are running Cisco Trust Agent. Configure R4 so that traffic from these hosts is only allowed into the network if they have authenticated to your RADIUS server using EAP over UDP.
- The RADIUS server's IP address is 173.X.137.252.
- The RADIUS server will be expecting the request to be sourced from R4's Loopback0 and use the password of CISCO.
- Ensure that if additional RADIUS servers are configured that they will automatically use the password of CISCO.

2 Points

6.4 Authentication

- Configure PPP on the Serial links between R1 & R3 and R2 & R3.
- R3 should challenge R1 and R2 to authenticate via CHAP.
- Use the minimum amount of **`username`** commands on R3 to accomplish this.

3 Points

6.5 Traffic Filtering

- Ports Fa0/10 and Fa0/11 of SW1 connect to your web and mail servers respectively. Since they are in the same VLAN, your security administrators are concerned about one server being compromised and an attack being launched on the other from inside your network.
- In order to prevent this configure SW1 so that these servers cannot pass traffic between each other.

2 Points

6.6 Traffic Filtering

- As an additional protective measure configure SW1 so that an attacker who has compromised your servers can not circumvent your security by sending frames to random unicast and multicast MAC addresses.

2 Points

6.7 Traffic Filtering

- Ports Fa0/22 and Fa0/23 on SW2 connect to the legacy shared portion of your network. Recently you have been getting complaints from users in VLAN 137 about slow network response time. After further investigation you have determined that too many users are connecting to the hubs attached to SW2. In order to help alleviate this congestion while additional connections are added to your switch block a new policy has been implemented which states that maximum of 5 hosts can be connected to either of these ports at the same time.
- Configure SW2 to reflect this policy.
- Traffic received from excess hosts should be dropped.
- In order to ensure that inactive hosts do not unnecessarily take up one of these spots ensure that their MAC addresses are flushed out of the CAM table if they have been inactive for over 5 minutes.

3 Points

6.8 Trusts

- The security administrator decided that R4 has trust issues for security. VLAN 4 needs to be protected.
- Web traffic from VLAN 4 should be allowed out either WAN Serial interface as well as VLAN46. FTP traffic destined for R5's loopback should only be allowed to go out the WAN-Serial zone.
- Any web traffic that is destined to go out the Fa0/0 interface should be subject to a deeper inspection that will disallow URL fields greater than 222 characters.
- You do not need to modify any routing for this task.

3 Points

6.9 Pass-Through Trust

- Any IP traffic between the WAN-Serial Zone and the WAN-Ethernet Zone should be allowed unhindered.

3 Points

7. Network Services

7.1 Logging

- After applying this configuration the server administrator has reported that R4 is overwhelming the syslog server when debugging is turned on.
- Configure R4 to limit the number of syslog messages to 10 per second.

2 Points

7.2 Telnet Logging

- Your network security team has expressed interest in tracking login attempts going to SW1 from outside your network.
- Configure SW1 so that all attempts to login to the command line via telnet are logged locally, except those coming from your internal network.
- Ensure that these log message remain in the case that the switch crashes.

3 Points

7.3 Address Translation

- For the purposes of security you do not want devices beyond BB2 to have specific reachability information about your network. Configure your network so that BB2 only has access to your network when hosts from inside initiate the connection.
- When BB2 receives this traffic it should all appear to have originated from the 192.10.X.5 address.
- Do not allow traffic originated from outside of your internal network to use this translation.

3 Points

7.4 Address Translation

- After configuring the above address translation you have been receiving reports from various users that they are not receiving any e-mail. In addition to this it appears as though users on the Internet cannot get access to your company's web server. Apparently while configuring address translation you forgot to account for these servers which are located on VLAN 5. In response to this your server administrators have updated the A records for your web server and the MX records in your DNS to point to the public address 192.10.X.5.
- Configure R5 so that users from behind BB2 can access both of these services.
- Your web server located on VLAN 5 has the IP address 173.X.5.100.
- Users will be accessing this server via normal TCP port 80 as well as SSL.
- Your e-mail server located on VLAN 5 has the IP address 173.X.5.100.
- Users will be accessing this server via both SMTP and POP3.

3 Points

7.5 Secure Shell

- Configure R1 so that an outside use may access the device connected to R1's AUX port via SSH.
- The outside user should be able to SSH into the port 2002 and authenticate itself with the username CISCO and the password of CISCO.

3 Points

7.6 Traffic Export

- A Traffic Analysis Module has been placed on VLAN 5. It can be reached at 173.X.5.100 and MAC 0010.1731.5100
- Sample one out of every 10 packets from each of the three WAN interfaces (either direction) and forward them to the device for analysis.

3 Points

8. QoS

8.1 Application Auditing

- Recently your network administrators have been getting complaints from users in VLAN 5 about a general network slowdown. During the investigation into this issue one of your administrators seems to recall overhearing some users in the lunch room talking about downloading mp3 files at work. You now suspect that peer-to-peer file sharing programs are the cause of this network slowdown. Since you are not sure that this is the case you still need to collect more information regarding the issue.
- Configure R5 to detect whether this peer-to-peer file sharing traffic is transiting the Ethernet segment of VLAN 5 and the Ethernet segment connecting to BB2.

2 Points

8.2 Application Filtering

- After applying the previous configuration you have in fact confirmed that an exorbitant amount of your bandwidth is being consumed by peer-to-peer file sharing applications. Also, it seems that users are running a wide range of these applications including Morpheus, LimeWire, Napster, and KaZaA version 2.
- In order to alleviate the congestion caused by these applications configure R5 to neither accept nor send traffic for these applications on the Ethernet segment to VLANs 5 and BB2.

3 Points

8.3 Traffic Policing

- You agreed to provide transit services between AS 54 and AS 254.
- In order to optimize network usage, you decided to implement bandwidth oversubscription in your network.
- The traffic contract with AS254 specifies the CIR of 512Kbps and the EIR of 384Kbps
- Implement traffic policing on R5's connection to BB2 using two-rate MQC policer.
- Mark the exceeding traffic with the DSCP value of CS0 and drop packets violating the traffic contract.
- The measurement interval in the contract is set to 30ms.

3 Points

8.4 Congestion Management

- The customer in AS 254 marks VoIP packets with DSCP value of EF.
- Configure R5's physical Frame-Relay interface so that the VoIP. packets are given priority treatment but limited to 256Kbps.
- Do not allow the customer to use more than 512Kbps of the interface bandwidth.
- All other traffic should be scheduled using flow-based fair queuing and have DE-bit set in Frame-Relay frames.
- Make sure that your configuration only affects the DLCIs connecting R5 to R1
- Implement your solution using MQC syntax only.

3 Points