Cisco Certified Network Associate (CCNA) Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://ciscoccna.examzify.com

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

Questions

1. **With a subnet mask of 255.255.255.224, which of the following addresses can be assigned to network hosts?**

   A. 15.234.118.63

   B. 92.11.178.93

   C. 134.178.18.56

   D. 192.168.16.87

2. **Which dynamic routing protocol has auto summarization enabled by default?**

   A. OSPF

   B. BGP

   C. EIGRP

   D. RIP

3. **Type 4 LSA is generated by which OSPF component?**

   A. Designated Router (DR)

   B. Area Border Router (ABR)

   C. Autonomous System Boundary Router (ASBR)

   D. Stub Router

4. **Which Cisco proprietary VPN tunneling protocol relies on the tunneled protocol for encryption?**

   A. Point-to-Point Tunneling Protocol

   B. Layer 2 Tunneling Protocol

   C. Layer 2 Forwarding

   D. IPsec

5. **Which protocol uses port number 53?**

   A. FTP

   B. DNS

   C. SMTP

   D. HTTP

6. Which commands are used to configure EIGRP stub routing?

A. router eigrp AS NUMBER enable

B. router eigrp AS NUMBER stub

C. router eigrp AS NUMBER eigrp stub

D. router eigrp AS NUMBER stub enable

7. What type of LSA is responsible for propagating Inter-area routes in OSPF?

A. Type 1 - Router LSA

B. Type 2 - Network LSA

C. Type 3 - Summary LSA

D. Type 4 - ASBR Summary LSA

8. What actions can be completed using the command history feature?

A. Save configurations permanently

B. Recalled commands from the history buffer

C. Display interface status

D. Set static IP addresses

9. To display general VTP information, which command should be used?

A. #show vtp info

B. #show vtp summary

C. #show vtp status

D. #display vtp configuration

10. In an EIGRP network, what does ‘passive’ signify about a network?

A. The network is congested

B. The network is unstable

C. The network is stable and working

D. The network is down

Answers

1. **B**
2. **C**
3. **B**
4. **C**
5. **B**
6. **B**
7. **C**
8. **B**
9. **C**
10. **C**

Explanations

1. With a subnet mask of 255.255.255.224, which of the following addresses can be assigned to network hosts?

A. 15.234.118.63

B. 92.11.178.93

C. 134.178.18.56

D. 192.168.16.87

To determine which IP addresses can be assigned to network hosts with a subnet mask of 255.255.255.224, it is essential to understand the implications of the subnet mask. A subnet mask of 255.255.255.224 indicates that the first 27 bits are used for the network portion, leaving 5 bits for the host portion. This means there are 2^5, or 32, possible addresses in this subnet. However, two addresses are reserved: one for the network address (the first address) and one for the broadcast address (the last address). Consequently, the usable addresses for hosts in a /27 subnet are 30. For a given IP address to be part of a subnet defined by the 255.255.255.224 mask, it must fall within a specific range defined by a base address. Each subnet has a block size of 32 (derived from the 5 bits available for hosts), meaning subnets are defined at every multiple of 32. To analyze the options: - For the first address, 15.234.118.63, it belongs to the subnet calculated using the last octet. However, determining the range entails calculating that the subnet would actually begin

2. Which dynamic routing protocol has auto summarization enabled by default?

A. OSPF

B. BGP

C. EIGRP

D. RIP

The correct answer is that EIGRP has auto summarization enabled by default. EIGRP, or Enhanced Interior Gateway Routing Protocol, is designed to simplify routing table entries by automatically summarizing subnets at network boundaries. This feature reduces the amount of routing information that needs to be processed, which optimizes performance, especially in large or complex networks. In contrast, OSPF (Open Shortest Path First) does not use auto summarization, as it is designed to maintain a link-state database that reflects the state of the entire network. BGP (Border Gateway Protocol) also does not support auto summarization by default since it primarily operates at a more complex internet boundary level, dealing with route advertisements between autonomous systems. RIP (Routing Information Protocol), while it does perform route summarization, does not do so automatically unless explicitly configured. Thus, EIGRP’s default behavior of auto summarization sets it apart among these protocols.

3. Type 4 LSA is generated by which OSPF component?

A. Designated Router (DR)

B. Area Border Router (ABR)

C. Autonomous System Boundary Router (ASBR)

D. Stub Router

Type 4 LSA, or Link-State Advertisement, is specifically generated by an Area Border Router (ABR) in OSPF (Open Shortest Path First) networking. The primary function of the ABR is to connect different OSPF areas and to manage the exchanges of routing information between these areas. When an ABR advertises Type 4 LSAs, it signifies the existence of an Autonomous System Boundary Router (ASBR) that is connected to the OSPF domain. Type 4 LSAs point to the ASBR's location so that routers in other areas can know how to reach the external routes. This is crucial for ensuring that all routers within an OSPF topology have a consistent view of how to route packets to external networks. In the context of OSPF, understanding the role of different router types – such as Designated Routers (DRs) and ASBRs – is essential. While a Designated Router is responsible for generating Type 2 LSAs for multi-access networks and representing the network to other OSPF routers, it does not handle Type 4 LSAs. Similarly, an ASBR is responsible for generating Type 5 LSAs, which represent external routing information. Therefore, the

4. Which Cisco proprietary VPN tunneling protocol relies on the tunneled protocol for encryption?

A. Point-to-Point Tunneling Protocol

B. Layer 2 Tunneling Protocol

C. Layer 2 Forwarding

D. IPsec

The correct choice aligns with the characteristic of the Layer 2 Tunneling Protocol (L2TP), which is a Cisco proprietary VPN tunneling protocol. L2TP does not provide encryption by itself. Instead, it relies on the underlying data link layer protocol and typically uses protocols such as IPsec for encryption when implemented in conjunction with it. Point-to-Point Tunneling Protocol (PPTP) and L2TP are both tunneling protocols but they differ significantly; PPTP does have built-in encryption capabilities although it's often considered less secure than L2TP when paired with IPsec. Layer 2 Forwarding (L2F) is another tunneling protocol but is generally regarded as more of an extension of L2TP and does not inherently provide encryption either. IPsec, while a widely used protocol for securing IP communications, is not a tunneling protocol but rather a suite of protocols that provide encryption and authentication over IP networks. Thus, the correct answer clarifies that L2TP relies on the encryption of the tunneled protocol, which makes it a suitable option for contexts requiring the tunneling of protocols while depending on another for security, emphasizing its operation within the VPN landscape as part of a broader encryption strategy.

5. Which protocol uses port number 53?

A. FTP

B. DNS

C. SMTP

D. HTTP

The protocol that uses port number 53 is DNS, which stands for Domain Name System. DNS is fundamental for the functionality of the internet, as it translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. This translation is necessary because people find it easier to remember names rather than numerical IP addresses. Port 53 is designated for DNS services, both for TCP and UDP protocols. While DNS primarily uses UDP for queries, it also uses TCP for tasks such as zone transfers and when the response data size exceeds the limit of a UDP packet. This specific port assignment allows DNS servers and clients to communicate effectively across the internet, facilitating the resolution of domain names to their corresponding IP addresses swiftly. In contrast, other options like FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and HTTP (Hypertext Transfer Protocol) are associated with different port numbers: FTP uses port 21, SMTP utilizes port 25, and HTTP operates on port 80. Each of these protocols serves distinct functions within network communication, helping to manage file transfers, email delivery, and web traffic, respectively. However, they do not operate on port 53, which is solely allocated for DNS.

6. Which commands are used to configure EIGRP stub routing?

A. router eigrp AS NUMBER enable

B. router eigrp AS NUMBER stub

C. router eigrp AS NUMBER eigrp stub

D. router eigrp AS NUMBER stub enable

The command to configure EIGRP stub routing is indeed the configuration that specifies the router will operate as a stub. By entering "router eigrp AS NUMBER stub," you effectively inform the EIGRP process to treat the router as a stub, which limits the types of routes that are advertised to its neighbors. This is particularly useful in scenarios where a router does not need to receive or advertise all EIGRP routes, such as in branch offices where resource conservation is important. While other options appear to reference commands that may look similar, they do not accurately encapsulate the correct syntax required for configuring a stub routing scenario in EIGRP. This command streamlines the routing protocol's performance and improves network efficiency by reducing unnecessary updates.

7. What type of LSA is responsible for propagating Inter-area routes in OSPF?

A. Type 1 - Router LSA

B. Type 2 - Network LSA

C. Type 3 - Summary LSA

D. Type 4 - ASBR Summary LSA

The type of LSA responsible for propagating inter-area routes in OSPF (Open Shortest Path First) is indeed a Summary LSA, which is classified as Type 3. Summary LSAs are utilized to advertise routes between different OSPF areas, allowing OSPF to provide a streamlined method for sharing routing information efficiently. This is essential in a multi-area OSPF environment, as it helps maintain a compact and manageable routing table by summarizing the routes from one area into another, rather than flooding every route individually across the areas. In the context of OSPF LSAs: - Router LSAs (Type 1) are used by routers to describe the links within their area and do not include inter-area route information. - Network LSAs (Type 2) are generated by the designated router for broadcast and non-broadcast multi-access networks, providing information about the routers connected to the network, but again, they do not propagate inter-area routes. - ASBR Summary LSAs (Type 4) advertise the presence of an Autonomous System Boundary Router (ASBR) and its associated routes, but they serve a different function specifically tied to external route information rather than general inter-area routing. Therefore, Type 3

8. What actions can be completed using the command history feature?

A. Save configurations permanently

B. Recalled commands from the history buffer

C. Display interface status

D. Set static IP addresses

The command history feature allows users to recall commands that have been previously entered into the command-line interface. This capability is particularly useful for network administrators who frequently execute similar commands or need to repeat tasks without retyping command lines. Users can cycle through previous commands using the up and down arrow keys, facilitating efficient management and configuration of network devices. While saving configurations, displaying interface status, and setting static IP addresses are important tasks within network management, they are not functions specifically associated with the command history feature. The command history is solely focused on recalling and revisiting past commands that have been executed during the current session or prior sessions, enabling easier and faster command entry.

9. To display general VTP information, which command should be used?

A. #show vtp info

B. #show vtp summary

C. #show vtp status

D. #display vtp configuration

To display general VTP (VLAN Trunking Protocol) information, the command that should be used is "show vtp status." This command provides a summary of the VTP parameters currently configured on the switch. The output includes important information such as the current VTP configuration revision number, the VTP mode (server, client, or transparent), the VTP domain name, and the number of VLANs known by the switch. Using "show vtp status" is crucial for network administrators to verify the VTP operating parameters and ensure that VTP is functioning correctly across the network. By checking this status, one can diagnose issues related to VLAN propagation and ensure consistency in VLAN configurations in a VTP domain.

10. In an EIGRP network, what does ‘passive’ signify about a network?

A. The network is congested

B. The network is unstable

C. The network is stable and working

D. The network is down

In an EIGRP (Enhanced Interior Gateway Routing Protocol) network, designating a network as 'passive' indicates that the network is stable and operational. A passive interface is one that is configured to not send EIGRP updates but can still receive updates. This is particularly useful in situations where you want to suppress EIGRP traffic on certain networks or interfaces while still allowing the router to learn about and route packets to those networks. By marking a network as passive, it signifies that the EIGRP process will treat that interface as stable—meaning no changes or updates are expected to occur from it, and therefore, it won't actively engage in the EIGRP neighbor discovery process. This is a critical configuration in maintaining efficient routing and resource usage, especially in larger networks.   In contrast, options that imply congestion, instability, or a down state do not align with the meaning of a passive interface in EIGRP, which instead indicates a network being stable and functioning correctly within the routing protocol framework.