Advanced Router Tech Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is the highest-metric route to subnet 2 visible in the output of the show ip route eigrp command given R1's route metrics?

A. The feasible successor route (metric 350)

B. The successor route (metric 100)

C. The route with the highest metric (450)

D. The route with the lowest metric (350)

2. Which command will show the routing table for IPv6?

A. show ipv6 routes

B. show running-config ipv6

C. show ipv6 route

D. show ip route

3. What is the difference between an FD and an RD in EIGRP?

A. An FD is reported by a neighbor, while an RD is calculated on the local router

B. An RD is a historical route, while an FD is a fresh route

C. An RD is reported by a neighbor, and an FD is the calculated route on the local EIGRP router

D. There is no difference; both are the same metrics

4. When an Ethernet switch receives a frame with a priority tag, which standard is it using?

A. IEEE 802.1Q

B. IEEE 802.1D

C. IEEE 802.3ad

D. IEEE 802.3

5. Which Cisco IOS command displays the currently configured VTP password?

A. show vtp password

B. display vtp status

C. show vtp status

D. get vtp password

6. What characteristic of a root port is key in determining its functionality in STP?

A. Lowest cost path to the root

B. Highest speed available

C. Configured with trunking

D. Has an active VLAN configuration

7. What is the primary purpose of using neighbor statements in a routing protocol?

A. To define metric values for routes

B. To specify which routes to summarize

C. To establish communication with other routers

D. To control traffic flow on the network

8. Which command displays the status of the default modes of the PortFast and BPDU Guard features?

A. show spanning-tree status

B. show spanning-tree summary

C. show interface status

D. show portfast status

9. What are two AAA protocols commonly used on Cisco devices for local device authentication?

A. RADIUS

B. LDAP

C. TACACS+

D. HTTP

10. Which two timers are used by EIGRP to maintain the status of a neighbor?

A. Update Interval and Hold Timer

B. Hello Interval and Hold Timer

C. Keepalive Interval and Hello Interval

D. Retransmit Timer and Update Interval

Answers

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

Explanations

1. What is the highest-metric route to subnet 2 visible in the output of the show ip route eigrp command given R1's route metrics?

A. The feasible successor route (metric 350)

B. The successor route (metric 100)

C. The route with the highest metric (450)

D. The route with the lowest metric (350)

The highest-metric route to a subnet refers to the route with the greatest EIGRP metric value that is still considered viable for routing. In EIGRP, routes are categorized into successor and feasible successor routes. The successor route is the primary route to the destination and has the lowest metric, while the feasible successor routes are backup routes that can be used if the successor route becomes unavailable. In this context, the feasible successor route with a metric of 350 is the choice that reflects the highest metric among the valid routes to subnet 2. While the successor route has a metric of 100, making it the primary route, the feasible successor, although still significantly lower than the highest possible metric, qualifies as the highest among alternatives when you disregard active pathways. The other choices suggest metrics that do not fall in line with EIGRP's criteria for what defines the highest-metric viable route. Thus, the feasible successor route holds significance as it is available for use within the EIGRP topology, showing that, even though it's not the primary path, it is still a reliable option when needed.

2. Which command will show the routing table for IPv6?

A. show ipv6 routes

B. show running-config ipv6

C. show ipv6 route

D. show ip route

The command that displays the routing table for IPv6 is "show ipv6 route." This command provides a detailed view of the active IPv6 routes that are currently in the routing table. When executed on a router or switch that supports IPv6, it will list not only the next-hop addresses but also the route type, metrics, and the interface through which the routes can be reached. This command is essential for network engineers to analyze and troubleshoot IP routing issues in an IPv6 environment. The other options do not serve this specific purpose. For instance, the command "show ipv6 routes" does not exist; the correct syntax includes the term "route" without an "s." "show running-config ipv6" refers to displaying the current configuration pertaining to IPv6, rather than the actual routing table. The command "show ip route" is meant for displaying the IPv4 routing table, thus it does not provide information on IPv6 routes. Therefore, "show ipv6 route" is the correct command for viewing the routing table specifically for IPv6 addresses.

3. What is the difference between an FD and an RD in EIGRP?

A. An FD is reported by a neighbor, while an RD is calculated on the local router

B. An RD is a historical route, while an FD is a fresh route

C. An RD is reported by a neighbor, and an FD is the calculated route on the local EIGRP router

D. There is no difference; both are the same metrics

In EIGRP (Enhanced Interior Gateway Routing Protocol), the terms FD (Feasible Distance) and RD (Reported Distance) refer to critical components of the routing decision process. The correct answer states that the RD is reported by a neighbor, while the FD represents the calculated route distance on the local EIGRP router. The Feasible Distance is the lowest calculated metric to reach a destination as determined by the local router. This metric takes into account all potential paths to the destination and is used to make routing decisions. It influences the selection of the best route among multiple available paths. On the other hand, the Reported Distance is the distance to the destination reported by a neighboring router. This value indicates how far the neighbor perceives itself to be from the destination and is essential in EIGRP's feasibility condition to determine if a route can be used. Thus, the distinction between these two metrics lies in their origin: the RD comes from a neighbor's perspective, whereas the FD is derived from the local router's calculations. Understanding these differences is crucial for grasping how EIGRP maintains loop-free operation and optimizes routing paths through its advanced metrics.

4. When an Ethernet switch receives a frame with a priority tag, which standard is it using?

A. IEEE 802.1Q

B. IEEE 802.1D

C. IEEE 802.3ad

D. IEEE 802.3

An Ethernet switch that receives a frame with a priority tag is utilizing the IEEE 802.1Q standard. This standard is specifically designed for introducing Virtual LANs (VLANs) and includes the capability for tagging frames with a priority level in what's known as Quality of Service (QoS). When a frame is tagged, it includes a 4-bit priority code point (PCP) that allows for prioritizing certain types of traffic, which is crucial in environments where bandwidth management and ensuring timely delivery of data packets are essential. This capability enables network devices to differentiate between traffic types, such as voice, video, and standard data, ensuring that more sensitive data can be prioritized over less critical transmissions. In contrast, other options focus on different aspects of networking. IEEE 802.1D addresses bridging and spanning tree protocols, IEEE 802.3ad relates to link aggregation for increased bandwidth and redundancy, and IEEE 802.3 covers standards for Ethernet networking without specific provisions for VLAN tagging or QoS. Therefore, the presence of a priority tag aligns specifically with the functions defined in IEEE 802.1Q.

5. Which Cisco IOS command displays the currently configured VTP password?

A. show vtp password

B. display vtp status

C. show vtp status

D. get vtp password

The correct command to display the currently configured VTP (VLAN Trunking Protocol) password in Cisco IOS is "show vtp password." This command specifically retrieves and presents the VTP password that has been set on the VTP domain for the switch. Understanding this command is crucial for network administrators who need to verify VTP configurations and ensure that the correct password is in place for secure VLAN management. The other commands listed may provide useful information regarding VTP, but they either do not display the password itself or are not valid commands for this purpose. For instance, "display vtp status" is not a recognized command in Cisco IOS, while "show vtp status" provides information about the VTP version, domain name, and other VTP settings but does not reveal the password. "Get vtp password" is also not a valid command in Cisco IOS, thus reinforces the importance of knowing the specific command that achieves the desired outcome.

6. What characteristic of a root port is key in determining its functionality in STP?

A. Lowest cost path to the root

B. Highest speed available

C. Configured with trunking

D. Has an active VLAN configuration

The characteristic of a root port that is key to its functionality in Spanning Tree Protocol (STP) is its designation as the lowest cost path to the root bridge. In STP, the root port serves as the port on a switch that has the least cost associated with reaching the root bridge in the network topology. This cost is calculated based on various factors including the speed of the links and the type of interface used. By selecting the path with the lowest cost, STP ensures that data is transmitted efficiently and minimizes loop formation in the network. This is crucial for maintaining a stable and efficient Ethernet network, as loops can lead to broadcast storms and network instability. The other characteristics mentioned, such as speed, trunking configuration, or VLAN setup, do not directly influence the designation of a port as the root port within the context of STP's decision-making process. Thus, the emphasis on the lowest cost path to the root bridge is what ultimately defines the functionality of the root port in maintaining the integrity of the network topology.

7. What is the primary purpose of using neighbor statements in a routing protocol?

A. To define metric values for routes

B. To specify which routes to summarize

C. To establish communication with other routers

D. To control traffic flow on the network

The primary purpose of using neighbor statements in a routing protocol is to establish communication with other routers. In routing protocols such as OSPF and EIGRP, neighbor statements explicitly define which routers are to be considered neighbors, allowing them to exchange routing information and coordinate their activities. This communication is critical for updating routing tables and ensuring that all routers have accurate and consistent information about the network topology. By identifying neighbors, routers can initiate sessions and share updates for link-state or distance-vector routing, facilitating real-time adjustments to routing decisions as network conditions change. This process helps maintain the efficiency and reliability of the routing decisions made across the network. Other options like defining metric values, specifying route summarization, or controlling traffic flow involve different aspects of routing protocol configuration and operations but are not the primary function of neighbor statements. They relate to how routes are managed more than the essential act of establishing communication with adjacent routers, which is fundamental to the operation of any dynamic routing protocol.

8. Which command displays the status of the default modes of the PortFast and BPDU Guard features?

A. show spanning-tree status

B. show spanning-tree summary

C. show interface status

D. show portfast status

The command that displays the status of the default modes of the PortFast and BPDU Guard features is "show spanning-tree summary." This command provides a consolidated view of the spanning tree configuration across the entire switch, highlighting various settings and statuses of features such as PortFast and BPDU Guard. When you use this command, it reveals important information, including whether PortFast is enabled on ports and the configuration for BPDU Guard. This is valuable for network administrators to ensure that these features are correctly set up to enhance network stability and prevent loops. Understanding the status helps in troubleshooting and optimizing the network. The other commands listed do not provide the same comprehensive overview of the PortFast and BPDU Guard settings. For example, while "show spanning-tree status" might display information about the spanning tree operations, it does not include the specific details related to PortFast and BPDU Guard. Similarly, "show interface status" focuses on the physical interface status, and "show portfast status" typically pertains to individual PortFast configurations rather than the broader spanning tree status.

9. What are two AAA protocols commonly used on Cisco devices for local device authentication?

A. RADIUS

B. LDAP

C. TACACS+

D. HTTP

The correct answer includes RADIUS and TACACS+. Both of these are widely used AAA (Authentication, Authorization, and Accounting) protocols on Cisco devices for local device authentication. RADIUS, which stands for Remote Authentication Dial-In User Service, is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service. It is particularly useful for authenticating users trying to access a network via remote connections. TACACS+, or Terminal Access Controller Access-Control System Plus, is another protocol that provides similar functionalities but is often preferred in environments needing enhanced security features. TACACS+ encrypts the entire authentication process, which offers better security for sensitive information compared to RADIUS, which encrypts only the password. The other options, like LDAP, are primarily used for directory services and user information lookups, but not specifically tailored for authentication on networking devices. HTTP, on the other hand, is a protocol for transferring hypertext and does not serve the AAA function of authenticating users in the context of networking devices. Thus, RADIUS and TACACS+ are specifically designed for and commonly used in local device authentication within Cisco environments.

10. Which two timers are used by EIGRP to maintain the status of a neighbor?

A. Update Interval and Hold Timer

B. Hello Interval and Hold Timer

C. Keepalive Interval and Hello Interval

D. Retransmit Timer and Update Interval

The two timers used by EIGRP (Enhanced Interior Gateway Routing Protocol) to maintain the status of a neighbor are the Hello Interval and the Hold Timer. The Hello Interval defines how frequently EIGRP routers send hello packets to their neighbors. These packets are essential for establishing and maintaining neighbor relationships, allowing routers to be aware of their peers in the network. If a router does not receive a hello packet from a neighbor within the specified time frame, it considers that neighbor down. The Hold Timer works in conjunction with the Hello Interval. It sets the duration for which a router will wait to receive hello packets from a neighbor before it declares that neighbor as unreachable. If hello packets are not received within the hold time, the neighbor relationship is terminated. The default time for this timer is typically three times the Hello Interval, providing a buffer to ensure that temporary issues do not cause unnecessary neighbor relationship termination. This pairing of timers enhances the robustness of EIGRP by ensuring that routers can quickly detect and respond to changes in the network topology, thus maintaining efficient routing and connectivity.