CCNA 3 Enterprise Networking, Security, and Automation, Version 7.0 Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Questions

1. **What is the purpose of sending Hello packets in the OSPF link-state routing process?**

   A. To initiate a routing table update

   B. To establish neighbor adjacencies

   C. To propagate LSAs

   D. To calculate the best path

2. **What role does DNS play in a network?**

   A. It provides IP addresses for devices

   B. It resolves hostnames to IP addresses

   C. It manages email routing

   D. It encrypts network traffic

3. **In which OSPF state is the Designated Router (DR) and Backup Designated Router (BDR) election conducted?**

   A. Exstart

   B. Two-way

   C. Full

   D. Loading

4. **Which command would you use to check the OSPF router ID of a neighboring router?**

   A. show ip interface

   B. show ip ospf neighbor

   C. show ip route

   D. show version

5. **Which two statements are characteristics of a virus? (Choose two.)**

   A. A virus can be dormant and activate at a specific time

   B. A virus is permanently active once installed

   C. A virus typically requires end-user activation

   D. A virus needs an external device to replicate

6. What command would be used to display any dynamic PAT translations that have been created by traffic?

A. show ip nat statistics

B. show ip nat translation

C. show ip access-lists

D. show ip interface brief

7. Which technology is used to provide redundancy at the network layer?

A. EtherChannel

B. HSRP (Hot Standby Router Protocol)

C. MPLS (Multiprotocol Label Switching)

D. VTP (VLAN Trunking Protocol)

8. When configuring single-area OSPF, what wildcard mask would be used for the network 172.20.0.0 255.255.252.0?

A. 0.0.3.255

B. 0.0.0.255

C. 0.0.15.255

D. 0.0.0.0

9. Which HTTP method is associated with deleting a resource in a RESTful context?

A. GET

B. PUT

C. POST

D. DELETE

10. Which protocol is responsible for sending periodic advertisements to learn device information in Cisco networks?

A. LLDP

B. CDP

C. STP

D. PPP

Answers

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

Explanations

1. What is the purpose of sending Hello packets in the OSPF link-state routing process?

A. To initiate a routing table update

B. To establish neighbor adjacencies

C. To propagate LSAs

D. To calculate the best path

Sending Hello packets in the OSPF (Open Shortest Path First) link-state routing process is essential for establishing neighbor adjacencies. When OSPF routers come up, they send these Hello packets to discover and identify other OSPF routers on the same physical segment or link. This is a critical step because, without knowing its neighbors, a router cannot effectively exchange routing information or maintain an accurate routing table. The Hello packets serve several purposes: they help determine the state of the network, facilitate the selection of router priorities, and allow routers to establish whether they will become neighbors based on certain parameters such as area IDs and authentication settings. Once the routers have successfully exchanged Hello packets and established neighbor relationships, they can then proceed to share link-state advertisements (LSAs) to communicate the state of their links and ultimately build a complete picture of the network topology necessary for OSPF to function correctly. In the context of OSPF, initiating routing table updates, propagating LSAs, and calculating the best path are subsequent processes that rely on the successful establishment of these neighbor adjacencies through Hello packets. Thus, the primary purpose of sending Hello packets centers around building those necessary relationships for effective routing communication in the OSPF protocol.

2. What role does DNS play in a network?

A. It provides IP addresses for devices

B. It resolves hostnames to IP addresses

C. It manages email routing

D. It encrypts network traffic

DNS, or Domain Name System, plays a critical role in network communications by resolving hostnames to IP addresses. When a user types a website address (hostname) into a browser, DNS translates that friendly name into the numerical IP address that computers use to identify each other on the network. This process allows users to access websites and online services without needing to memorize complex numeric addresses. The function of DNS is paramount because it simplifies the user experience, facilitating ease of navigation on the internet and within local networks. When a browser sends a request for a specific hostname, it queries a DNS server, which responds with the corresponding IP address. This resolution enables the browser to initiate a connection to the web server hosting the requested content. In contrast, the other options do not accurately describe the main role of DNS. While IP addresses are crucial for identifying devices, DNS does not directly provide these addresses; rather, it resolves the hostnames to these numbers. Managing email routing pertains to Mail Exchange (MX) records within DNS, but it is not the primary function of DNS itself. Lastly, encryption of network traffic is handled by different protocols and technologies, such as SSL/TLS, not DNS.

3. In which OSPF state is the Designated Router (DR) and Backup Designated Router (BDR) election conducted?

A. Exstart

B. Two-way

C. Full

D. Loading

The OSPF state where the Designated Router (DR) and Backup Designated Router (BDR) election takes place is the Two-way state. During this state, OSPF routers exchange hello packets to establish neighbor relationships and to determine which routers are on the same segment.   In the Two-way state, each router will recognize the other routers it can communicate with and will identify eligible routers that can participate in the election of the DR and BDR. The criteria for election usually favor the router with the highest OSPF priority, or if the priorities are the same, the highest Router ID. Once the election process is completed in this state, the selected DR and BDR will be responsible for generating and distributing link state updates within that broadcast domain, which is essential for efficient OSPF operation. This process helps to minimize routing traffic, as only the DR will communicate with other OSPF routers, and the BDR provides redundancy in case the DR fails. Subsequent states, such as Exstart, Full, and Loading, focus on the exchange of link-state information but do not involve the election of the DR and BDR; this is why the Two-way state is specifically significant in the context of establishing who will serve

4. Which command would you use to check the OSPF router ID of a neighboring router?

A. show ip interface

B. show ip ospf neighbor

C. show ip route

D. show version

The command to check the OSPF router ID of a neighboring router is "show ip ospf neighbor." This command provides detailed information about OSPF neighbors and their current state. Among the output is the OSPF router ID of each neighbor, which is crucial for understanding the network topology and diagnosing OSPF-related issues. Using this command allows network engineers to verify neighbor relationships, Router IDs, and the status of OSPF adjacencies, which are essential for ensuring efficient routing and troubleshooting OSPF configurations. The information retrieved can help determine if there are any issues with OSPF neighbor formation, such as mismatched configurations or network connectivity problems. Other options would not provide the OSPF router ID. The command for interfaces focuses on interface configurations, the routing table command displays routes but not neighbor associations, and the version command provides information about the device's software and hardware but does not include OSPF specifics.

5. Which two statements are characteristics of a virus? (Choose two.)

A. A virus can be dormant and activate at a specific time

B. A virus is permanently active once installed

C. A virus typically requires end-user activation

D. A virus needs an external device to replicate

A virus often has the characteristic of being able to remain dormant for a period of time before it activates itself, which can occur at a predetermined time or in response to certain conditions. This dormant phase is a strategy employed by many viruses to evade detection by antivirus software and users until it is ready to execute its payload—like corrupting files, stealing information, or spreading to other systems. Another characteristic of a virus is that it typically requires some form of end-user activation to start its replication process. This could involve the user unknowingly opening an infected file or executing a program. Without this activation, the virus would remain harmless and inert on the system. These two statements highlight the stealthy and user-dependent nature of viruses, helping to explain their functionality and the ways they propagate through systems. Understanding these characteristics is crucial for developing effective cybersecurity measures to prevent and mitigate virus infections.

6. What command would be used to display any dynamic PAT translations that have been created by traffic?

A. show ip nat statistics

B. show ip nat translation

C. show ip access-lists

D. show ip interface brief

The command used to display any dynamic Port Address Translation (PAT) translations created by traffic is "show ip nat translation." This command reveals the current translations that have occurred on the router, showing how local IP addresses and ports have been mapped to a public IP address and port.   When a device on a private network sends traffic to the internet, the router or firewall performs dynamic PAT by replacing the private IP address and port with its own public IP address and a unique port number. By using the "show ip nat translation" command, network administrators can effectively monitor and troubleshoot NAT configurations. This information is crucial for understanding how internal addresses are translated and for resolving any issues related to NAT. The other command options serve different purposes. For example, "show ip nat statistics" displays statistical data related to NAT operations, but it does not show the specific translation entries. The "show ip access-lists" command provides information about configured Access Control Lists (ACLs) rather than NAT translations. Lastly, "show ip interface brief" presents a summary of the status and IP addresses of interfaces but does not relate to NAT translations.

7. Which technology is used to provide redundancy at the network layer?

A. EtherChannel

B. HSRP (Hot Standby Router Protocol)

C. MPLS (Multiprotocol Label Switching)

D. VTP (VLAN Trunking Protocol)

HSRP (Hot Standby Router Protocol) is a technology specifically designed to provide redundancy at the network layer. It allows for automatic failover between routers in a LAN environment, ensuring high availability and maintaining connectivity. HSRP operates by allowing multiple routers to work together to present the appearance of a single virtual router to the hosts on the network. One router is designated as the active router, while the others remain in standby mode and are ready to take over if the active router fails. This redundancy helps prevent downtime and keeps the network operational even if one router goes offline. While EtherChannel, MPLS, and VTP serve important roles in a networking environment, they do not specifically focus on providing redundancy at the network layer in the same manner as HSRP does. EtherChannel is primarily used for link aggregation to increase bandwidth between switches, MPLS enhances the efficiency of data transport across different networks, and VTP manages VLAN configurations within a switched network. These technologies contribute to overall network performance and organization but lack the failover capabilities essential for redundancy at the network layer that HSRP offers.

8. When configuring single-area OSPF, what wildcard mask would be used for the network 172.20.0.0 255.255.252.0?

A. 0.0.3.255

B. 0.0.0.255

C. 0.0.15.255

D. 0.0.0.0

When configuring OSPF with a specific network, the wildcard mask is used to determine which bits of the IP address will be matched by the OSPF configuration. In this case, the IP address is 172.20.0.0 and the subnet mask is 255.255.252.0. To convert the subnet mask to a wildcard mask, you need to subtract each octet of the subnet mask from 255. The subnet mask 255.255.252.0 can be broken down as follows: - The first octet: 255 - 255 = 0 - The second octet: 255 - 255 = 0 - The third octet: 255 - 252 = 3 - The fourth octet: 255 - 0 = 255 Combining these results gives you the wildcard mask 0.0.3.255. This wildcard mask indicates that the first two octets (172.20) are fixed and must match exactly, while the last two octets can vary based on the OSPF configuration. The "3" in the third octet corresponds to the binary representation where the subnet allows for a range of addresses, specifically the

9. Which HTTP method is associated with deleting a resource in a RESTful context?

A. GET

B. PUT

C. POST

D. DELETE

In a RESTful context, the HTTP method that is specifically designed for deleting a resource is DELETE. This method is part of the standard set of HTTP verbs that define actions in the context of web services. When a client issues a DELETE request to a server, it is indicating that a specified resource should be removed from the server.   The use of DELETE aligns with the REST architectural style principles, which emphasize the use of distinct verbs for specific actions. This clear mapping of HTTP methods to actions allows for a more intuitive interaction with web resources. In this case, issuing a DELETE request signals to the server that it should locate the identified resource and remove it, effectively freeing up any associated resources or data on the server. Understanding the functions of other HTTP methods can help clarify why DELETE is the correct choice. For instance, GET is used to retrieve resources without making changes, PUT is intended for updating existing resources or creating new ones at a specified resource URL, and POST is used primarily for submitting data to a server, often resulting in the creation of a new resource. Thus, DELETE's role in removing resources makes it the appropriate choice for this scenario.

10. Which protocol is responsible for sending periodic advertisements to learn device information in Cisco networks?

A. LLDP

B. CDP

C. STP

D. PPP

The correct choice is the protocol that facilitates the exchange of information between directly connected Cisco devices, specifically Cisco Discovery Protocol (CDP). CDP operates at the Data Link Layer and is used primarily in Cisco environments to gather information about neighboring devices such as their device type, IP address, and capabilities. By sending periodic advertisements, CDP enables devices to discover relevant details automatically without manual configuration. This automatic discovery process helps network administrators gain visibility into the network topology and quickly troubleshoot connectivity issues. As devices periodically send CDP advertisements, they maintain updated information about themselves and their surroundings, creating a dynamic view of the network. In contrast, the other protocols mentioned serve different purposes. Link Layer Discovery Protocol (LLDP) is a vendor-neutral protocol similar to CDP but is not specific to Cisco devices. Spanning Tree Protocol (STP) is used for preventing loops in network topologies, and Point-to-Point Protocol (PPP) is primarily used for establishing direct connections between two nodes in point-to-point links. These protocols do not focus on advertisement and discovery of device information like CDP does.