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

Study Guide

Everything you need from our exam experts!

Questions

1. **What should be the final command to save your configuration after setting up a Cisco device?**

   A. #end

   B. #copy run start

   C. #save config

   D. #backup config

2. **What does it indicate if the line status is up and the protocol status is down?**

   A. Layer 1 issue

   B. Layer 2 issue

   C. Configuration mismatch

   D. No incoming traffic

3. **What is the Cisco proprietary etherchannel protocol?**

   A. Link Aggregation Control Protocol (LACP)

   B. Port Aggregation Control Protocol (PAgP)

   C. Rapid Spanning Tree Protocol (RSTP)

   D. Ethernet Channel Grouping Protocol (ECGP)

4. **What are the two essential components of a Netflow system?**

   A. Netflow enabled router and a Netflow server

   B. Netflow enabled router and Netflow collector

   C. Netflow collector and a router

   D. Netflow server and Netflow interface

5. **What is an important function of the configuration register on a Cisco router?**

   A. To control the boot sequence

   B. To enable packet filtering

   C. To monitor bandwidth

   D. To set the maximum MTU size

6. What protocol allows for load balancing across multiple routers?

A. Hot Standby Router Protocol (HSRP)

B. Virtual Router Redundancy Protocol (VRRP)

C. Gateway Load Balancing Protocol (GLBP)

D. Enhanced Interior Gateway Routing Protocol (EIGRP)

7. Which of the following is NOT a mode of IPsec?

A. Transport mode

B. Tunnel mode

C. Secure mode

D. End-to-end mode

8. In a Cisco router, what does the command 'enable' do?

A. Promotes a user to privileged EXEC mode

B. Initiates the configuration mode

C. Starts the debugging process

D. Changes the device hostname

9. What is the command to copy an IOS image to a TFTP server?

A. copy flash: tftp:

B. backup ios tftp:

C. send ios tftp:

D. upload ios tftp:

10. What command is used to configure a default gateway on a switch?

A. (config)#ip default-gateway IP ADDRESS

B. (config)#ip address IP ADDRESS

C. (config)#set gateway IP ADDRESS

D. (config)#router default IP ADDRESS

Answers

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

Explanations

1. What should be the final command to save your configuration after setting up a Cisco device?

A. #end

B. #copy run start

C. #save config

D. #backup config

The final command to save your configuration on a Cisco device is indeed "copy run start." This command is short for "copy running-config startup-config," which means you are taking the current (running) configuration that is actively being used by the device and saving it to the startup configuration file. This ensures that when the device is restarted, it will load the configurations you have just defined, maintaining any changes or settings you've applied during the current session. Using this command is important because the running configuration is stored in volatile memory (RAM), meaning it will be lost if the device loses power or is restarted. By saving it to the startup configuration, which is stored in non-volatile memory (NVRAM), you ensure that your changes persist across reboots. The other choices do not accomplish the task of saving the configuration: - Ending a session with "end" does not save configurations; it merely exits the configuration mode. - A command like "save config" is not recognized in Cisco IOS as a valid command for saving the configuration. - Similarly, "backup config" does not represent a valid command in the context of saving configurations on Cisco devices. Thus, "copy run start" is the essential command to ensure that all configurations are saved

2. What does it indicate if the line status is up and the protocol status is down?

A. Layer 1 issue

B. Layer 2 issue

C. Configuration mismatch

D. No incoming traffic

When the line status is up but the protocol status is down, it indicates that the physical layer of the connection is functioning correctly, meaning there is a valid physical link between the devices. However, the protocol layer is experiencing a problem, which may point to a Layer 2 issue. This situation often arises due to issues such as mismatched encapsulation types, VLAN mismatches, or problems with spanning tree protocol. Each of these issues affects how data is being processed at the data link layer, which results in the protocol being down despite the physical connection being good. While it might seem like the issue could stem from configuration mismatches in some cases, the specific indication of the protocol being down while the line status is up firmly situates the problem at Layer 2, where the data link layer must manage how data packets are formatted for transmission over the physical medium.

3. What is the Cisco proprietary etherchannel protocol?

A. Link Aggregation Control Protocol (LACP)

B. Port Aggregation Control Protocol (PAgP)

C. Rapid Spanning Tree Protocol (RSTP)

D. Ethernet Channel Grouping Protocol (ECGP)

The correct answer is Port Aggregation Control Protocol (PAgP). PAgP is a Cisco proprietary protocol used to automatically create an EtherChannel, which allows multiple physical Ethernet connections to aggregate and function as a single logical link. This aggregation provides increased bandwidth and redundancy. PAgP helps in the negotiation and establishment of EtherChannels between Cisco switches. It detects and maintains an EtherChannel by exchanging packets that carry information about the ports and their configurations. When these ports are configured correctly, PAgP can dynamically form the EtherChannel without manual intervention, which simplifies network management. Understanding the function of PAgP is crucial for network engineers working with Cisco equipment, as it ensures efficient use of bandwidth and enhances the resiliency of connections in a network environment. The other protocols mentioned either do not pertain to EtherChannel or are not Cisco-specific.

4. What are the two essential components of a Netflow system?

A. Netflow enabled router and a Netflow server

B. Netflow enabled router and Netflow collector

C. Netflow collector and a router

D. Netflow server and Netflow interface

A NetFlow system is primarily composed of two essential components that work together to capture and analyze network traffic data. The first component is the NetFlow-enabled router, which is responsible for gathering and exporting flow data. This router collects information about the packets passing through it, such as source and destination IP addresses, ports, and the protocol used. The second component is the NetFlow collector. This is a centralized system or server that receives, stores, and processes the flow data sent from the NetFlow-enabled router. The collector can analyze the data to provide insights into network usage, performance, and security. Together, these two components allow for effective traffic analysis and monitoring, which is crucial for network management and troubleshooting. While other options mention components like a NetFlow server and interface, they do not capture the fundamental relationship between the router exporting data and the collector receiving and analyzing it, which is vital for a comprehensive NetFlow system.

5. What is an important function of the configuration register on a Cisco router?

A. To control the boot sequence

B. To enable packet filtering

C. To monitor bandwidth

D. To set the maximum MTU size

The configuration register on a Cisco router plays a crucial role in controlling the boot sequence of the device. It determines how the router will start up by specifying various settings, such as the method by which it locates and loads the operating system (IOS). For example, the configuration register can dictate whether the router boots from the primary flash memory or from an alternative source, which is particularly useful for recovery scenarios. The value of the configuration register allows for customization of the boot process, including options for password recovery and enabling or disabling certain features during startup. While packet filtering, bandwidth monitoring, and maximum MTU size settings are important aspects of network operation, they are not functions related to the configuration register. These functionalities are handled by other configurations and features within the router's operating system rather than being controlled by the configuration register itself.

6. What protocol allows for load balancing across multiple routers?

A. Hot Standby Router Protocol (HSRP)

B. Virtual Router Redundancy Protocol (VRRP)

C. Gateway Load Balancing Protocol (GLBP)

D. Enhanced Interior Gateway Routing Protocol (EIGRP)

The Gateway Load Balancing Protocol (GLBP) is designed specifically for load balancing across multiple routers. It allows multiple routers to work together while providing a single virtual IP address to clients. GLBP enables traffic distribution across several gateways by assigning each active router a portion of the outgoing traffic, which results in efficient utilization of the available resources and increases redundancy. This is done by using a unique feature where each participating router can take turns handling requests, allowing for a more balanced load compared to other protocols that primarily focus on redundancy rather than simultaneous data routing. It ensures that no single router becomes a bottleneck, thus enhancing overall network performance and reliability. In contrast, while the other protocols mentioned may provide redundancy, they do not inherently support load balancing in the same way. Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) primarily focus on providing failover capabilities, where only one router actively forwards traffic while the others remain in standby mode unless a failure occurs. Enhanced Interior Gateway Routing Protocol (EIGRP), although it supports route load balancing among equal-cost paths, is more about routing efficiency rather than load balancing across multiple routers providing a single virtual IP for clients. Hence, GLBP stands out as the protocol specifically

7. Which of the following is NOT a mode of IPsec?

A. Transport mode

B. Tunnel mode

C. Secure mode

D. End-to-end mode

IPsec (Internet Protocol Security) is a comprehensive suite of protocols aimed at securing Internet Protocol (IP) communications through authentication and encryption of each IP packet in a communication session. The two primary modes of IPsec are Transport mode and Tunnel mode. Transport mode is utilized for end-to-end communication between two hosts. In this mode, only the payload of the IP packet is encrypted and/or authenticated, leaving the original IP header intact. This is optimal for scenarios where security is needed between two communicating hosts without altering routing information. Tunnel mode, on the other hand, is designed for network-to-network communications and is commonly used in Virtual Private Networks (VPNs). In this mode, the entire original IP packet is encapsulated within a new IP packet, which has a new IP header. This allows for secure communication across untrusted networks while effectively masking the original IP addresses. The term "Secure mode" does not correspond to any established mode within IPsec, therefore, it is identified as the option that is NOT a mode of IPsec. Similarly, "End-to-end mode," while it might describe a model of communication, does not specifically describe a mode within the IPsec framework. Recognizing the common modes of IPsec helps in understanding how secure communication

8. In a Cisco router, what does the command 'enable' do?

A. Promotes a user to privileged EXEC mode

B. Initiates the configuration mode

C. Starts the debugging process

D. Changes the device hostname

The command 'enable' in a Cisco router is used to switch the user from user EXEC mode to privileged EXEC mode. This is a crucial aspect of Cisco device management because privileged EXEC mode grants users access to more advanced commands and configurations that are not accessible in the user EXEC mode. In user EXEC mode, the user is limited to basic monitoring commands that do not allow for configuration changes or detailed information access. By using the 'enable' command, the router prompts for an optional password, and upon successful entry, the user can access a broader range of commands, including those that are necessary to modify system settings and troubleshoot issues. The significance of this command lies in its role in establishing the permission level necessary for effective network management, which is vital for maintaining and configuring network devices.

9. What is the command to copy an IOS image to a TFTP server?

A. copy flash: tftp:

B. backup ios tftp:

C. send ios tftp:

D. upload ios tftp:

The command to copy an IOS image to a TFTP server is indeed 'copy flash: tftp:'. This command specifies the source from where the IOS image is to be copied, which is the flash memory of the device, and the destination, which is the TFTP server. When executing this command, you will typically be prompted to provide the IP address of the TFTP server and the filename of the IOS image that you wish to copy. The use of 'copy' in the command denotes that you are transferring a file, which is a standard practice in Cisco IOS. Other choices presented do not follow the correct syntax used in Cisco devices for copying files or do not accurately represent commands used to perform this specific action, so they would not successfully initiate the process of sending an IOS image to a TFTP server.

10. What command is used to configure a default gateway on a switch?

A. (config)#ip default-gateway IP ADDRESS

B. (config)#ip address IP ADDRESS

C. (config)#set gateway IP ADDRESS

D. (config)#router default IP ADDRESS

The command to configure a default gateway on a switch is indeed "ip default-gateway IP ADDRESS". This command allows the switch to communicate with devices outside its local subnet, such as routers and other switches, by providing a path for traffic that is destined for a different network. Switches operate primarily at Layer 2 (Data Link layer) of the OSI model, which means they do not have IP routing capabilities unless they are Layer 3 switches. The "ip default-gateway" command is essential for Layer 2 switches, enabling them to send traffic to the configured gateway when they encounter a destination outside their own network. This is critical in environments where switches are managing multiple VLANs or need to reach devices across different IP networks. The other options do not correctly set a default gateway on a switch. For instance, "ip address IP ADDRESS" is used for assigning an IP address to an interface, which is not relevant for configuring a default gateway. "set gateway IP ADDRESS" is not a recognized command in Cisco IOS for configuring a default gateway. Finally, "router default IP ADDRESS" is also not a valid configuration command for setting a default gateway on a switch.