Cisco

100-150

Cisco Certified Support Technician (CCST) Networking

Latest Version: 6.0

Question: 1

Which of the following statements is true about VLANs?

A. ANs increase network performance.
B. ANs increase security.
C. ANs reduce network congestion.
D. ANs reduce the need for routers.

Answer: B

Explanation:
Option 1: VLANs do not directly increase network performance. They are used to logically segment a network and provide better control over network traffic. However, by separating network traffic into different VLANs, it may be possible to improve performance by reducing broadcast traffic and optimizing network resources within each VLAN. Option 2: Correct. VLANs increase security by isolating network traffic into different logical segments. This separation helps to prevent unauthorized access and potential threats from spreading across the network. VLANs can also be used in conjunction with other security measures, such as access control lists (ACLs), to enhance network security. Option 3: VLANs do not directly reduce network congestion. However, by separating network traffic into different VLANs, it may be possible to mitigate network congestion by optimizing network resources within each VLAN. Option 4: VLANs do not reduce the need for routers. While VLANs can segment a network, routers are still required to facilitate communication between different VLANs or different networks.

Question: 2

What is a common cause of a network link failure?

A. faulty cable
B. overloaded switch
C. correct routing table entries
D. terference from other devices

Answer: A

Explanation:
Option 1: Correct: A faulty cable can cause a network link failure. It could be a broken or damaged cable that is not properly transmitting the signals. Option 2: Incorrect: An overloaded switch can cause slow network performance, but it is not a common cause of network link failure. Option 3: Incorrect: Incorrect routing table entries can cause routing issues, but they do not typically cause network link failures. Option 4: Incorrect: Interference from other devices can cause network performance issues, but it is not a common cause of network link failure.

You are configuring a new network operations center (NOC) for a rapidly expanding IoT technology firm. The network infrastructure must support a variety of communication protocols and connectivity options to accommodate diverse device types, from high-capacity servers to field sensors and security devices. Given the complexity and the need for high configurability and future scalability, it's critical to correctly identify and utilize the various ports on your networking devices to optimize both data throughput and device management.

Question: 3

During the initial setup of the core network switches, which port type should be prioritized for connecting management terminals directly for initial configuration and ongoing network adjustments?

A. SFP+
B. Consoleright
C. PoE
D. USB

Answer: B

Explanation:
The console port is specifically designed for configuring network devices directly through a management terminal, usually using a CLI (Command Line Interface). This port provides a direct, out-of-band access method that doesn't depend on the network being operational, making it ideal for initial setups and troubleshooting. Option A is incorrect While SFP+ ports are crucial for high-speed network connections and can handle up to 10 Gbps, they are primarily used for fiber connections and not suitable for direct management terminal connections which require console access for configuration. Option C is incorrect Power over Ethernet (PoE) ports are designed to deliver power along with data over the network cable, commonly used for powering devices such as IP cameras, wireless access points, and other IoT devices. PoE ports do not facilitate direct device management or configuration.
Option D is incorrect USB ports on network devices are typically used for tasks such as firmware updates or exporting/importing configuration files. Although they can sometimes be used for console access via a USB-to-Serial adapter, they are not the primary choice for network device management compared to dedicated console ports.
https://www.lantronix.com/blog/whats-difference-console-port-management-port/

Question: 4

Which feature allows a network device to consolidate multiple physical interfaces into a single logical interface?

A. rt Channel
B. AN
C. LS
D. P

Answer: A

Explanation:
Option 1: Correct: Port Channel is a feature that allows for the aggregation of multiple physical interfaces into a single logical interface, increasing bandwidth and providing redundancy. Option 2: Incorrect: VLAN (Virtual Local Area Network) is used to segment a network into multiple broadcast domains, but it does not consolidate physical interfaces into a single logical interface. Option 3: Incorrect: MPLS (Multiprotocol Label Switching) is a technique used for forwarding data across a network, but it does not consolidate physical interfaces into a single logical interface. Option 4: Incorrect: BGP (Border Gateway Protocol) is a routing protocol used between different autonomous systems, but it does not consolidate physical interfaces into a single logical interface.

Question: 5

Which feature of DNS allows a server to send updates to the DNS server for a particular zone when the server's IP address changes?

A. namic DNS
B. main Name System Security Extensions (DNSSEC)
C. lit DNS
D. und Robin DNS

Answer: A

Explanation:
Option 1: Dynamic DNS (DDNS) is the correct answer. DDNS allows a server to send updates to the DNS server for a particular zone when its IP address changes. This is useful for servers with dynamic IP addresses, such as those connected to the Internet via DHCP. Option 2: DNSSEThis is a security extension to the DNS protocol, which provides authentication and integrity for DNS responses. It does not handle IP address updates. Option 3: Split DNS is a configuration where separate DNS servers are used for internal and external DNS resolution. It does not handle IP address updates. Option 4: Round Robin DNS is a method of load balancing where multiple IP addresses are returned in response to DNS queries in a round-robin fashion. It does not handle IP address updates.

Question: 6

Which of the following is NOT a valid reason for a network device to be unable to establish a connection?

A. correct IP address configuration
B. ulty network cable
C. rewall blocking traffic
D. cessive network traffic

Answer: D

Explanation:

Option 1: Incorrect. An incorrect IP address configuration can prevent a network device from establishing a connection. Option 2: Incorrect. A faulty network cable can prevent a network device from establishing a connection. Option 3: Incorrect. A firewall blocking traffic can prevent a network device from establishing a connection. Option 4: Correct. Excessive network traffic does not directly prevent a network device from establishing a connection. It may, however, lead to network congestion and degraded performance.

Question: 7

Which routing protocol is best suited for large enterprise networks with multiple routing domains and requires a metric that incorporates both bandwidth and delay?

A. P
B. PF
C. GRP
D. P

Answer: C

Explanation:
Option 1: RIP (Routing Information Protocol) is a dynamic routing protocol that uses the hop-count as the metric. It is not wellsuited for large enterprise networks with multiple routing domains as it does not support the complex network topologies and routing hierarchies typically found in such networks. The metric used by RIP (hop-count) does not take into consideration factors like bandwidth and delay. Therefore, this option is incorrect. Option 2: OSPF (Open Shortest Path First) is a link-state routing protocol that is well-suited for large enterprise networks with multiple routing domains. OSPF uses a cost metric that incorporates both bandwidth and delay to calculate the best path. OSPF supports complex network topologies and routing hierarchies, making it a suitable choice for this scenario. Therefore, this option is incorrect. Option 3: EIGRP (Enhanced Interior Gateway Routing Protocol) is a hybrid routing protocol that combines the characteristics of both distance-vector and link-state routing protocols. It is well-suited for large enterprise networks with multiple routing domains. EIGRP uses a composite metric that incorporates bandwidth, delay, reliability, load, and MTU to calculate the best path. This makes EIGRP an ideal choice for this scenario. Therefore, this option is correct. Option 4: BGP (Border Gateway Protocol) is an exterior gateway protocol primarily used for inter-domain routing on the Internet. While BGP can be used in large enterprise networks, it is typically used for connecting autonomous systems and not within a single network. BGP does not use a metric that incorporates bandwidth and delay. Therefore, this option is incorrect.

Question: 8

What feature allows a router to learn routes from multiple routing protocols and choose the best route based on configured criteria?

A. ute summarization
B. ute redistribution
C. ute filtering

D. ute caching

Answer: B

Explanation:
Option 1: Incorrect. Route summarization involves consolidating multiple network addresses into a single summarized route. Option 2: Correct. Route redistribution allows a router to share routes between different routing protocols, allowing it to learn routes from multiple sources and choose the best route based on configured criteria. Option 3: Incorrect. Route filtering involves selectively permitting or denying specific routes based on defined criteria. Option 4: Incorrect. Route caching involves temporarily storing network routes in a router's memory for faster lookup and retrieval.

Question: 9

Which of the following is a security feature of a next-generation firewall?

A. trusion Detection System (IDS)
B. Filtering
C. ality of Service (QoS)
D. rtual Private Network (VPN)

Answer: B

Explanation:
Option 1: A next-generation firewall is designed to provide advanced security features beyond traditional firewalls. While an Intrusion Detection System (IDS) can be a part of a next-generation firewall's security features, it is not the only feature. Therefore, option This is incorrect. Option 2: Web Filtering is a security feature of a next-generation firewall that allows organizations to control and monitor web traffic to prevent users from accessing malicious websites or inappropriate content. This feature helps enhance the security posture of the organization by blocking access to potentially harmful websites. Therefore, option This is correct. Option 3: Quality of Service (QoS) is a network management feature that prioritizes certain types of network traffic to ensure better performance and reliability. While QoS is an important feature, it is not specifically related to security. Therefore, option This is incorrect. Option 4: Virtual Private Network (VPN) is a network security feature that allows users to securely connect to a private network over the public internet. While VPNs can be used with next generation firewalls, they are not specifically a security feature of the firewall itself. Therefore, option This is incorrect.

Question: 10

Which feature provides secure device management for Cisco networking equipment?

A. co Discovery Protocol (CDP)
B. namic Host Configuration Protocol (DHCP)
C. cure Shell (SSH)
D. nk Layer Discovery Protocol (LLDP)

Answer: C

Explanation:
Option 1: Incorrect. Cisco Discovery Protocol (CDP) is a proprietary Layer 2 network protocol used for device discovery, not secure device management. Option 2: Incorrect. Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses to devices on a network, not for secure device management. Option 3: Correct. Secure Shell (SSH) provides secure remote access to networking devices and is commonly used for device management. Option 4: Incorrect. Link Layer Discovery Protocol (LLDP) is a vendor-neutral protocol used for device discovery and is not specifically designed for secure device management.