CompTIA.N10-009.v2026-05-09.q225

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	225
Version:	v2026-05-09
# of views:	111
# of Questions views:	2462
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-05-09.q225.html	

NEW QUESTION: 1
A company is opening a new site that needs to be divided into subnets that accommodate 75 hosts each.
Which of the following is the most efficient subnet?
A. 192.168.13.0/25
B. 192.168.13.0/26
C. 192.168.13.0/27
D. 192.168.13.0/28
Answer: A (LEAVE A REPLY)
To support 75 hosts per subnet , you must choose a subnet size that provides at least 75 usable IP addresses.
In IPv4, usable hosts per subnet equals 2^(host bits) # 2 (subtracting network and broadcast).
A /25 leaves 7 host bits (32-25 = 7), giving 2^7 # 2 = 128 # 2 = 126 usable hosts , which meets the requirement and is the smallest (most efficient) option listed that does so. A /26 leaves 6 host bits, giving 62 usable hosts , which is insufficient. A /27 gives 30 usable , and a /28 gives 14 usable , both far below 75. Network+ subnetting objectives emphasize selecting the smallest subnet that satisfies the host requirement to conserve address space while meeting growth and design constraints. Therefore, 192.168.13.0/25 is the most efficient option that accommodates at least 75 hosts per subnet.

NEW QUESTION: 2
Which of the following allows for the interception of traffic between the source and destination?
A. Self-signed certificate
B. VLAN hopping
C. On-path attack
D. Phishing
Answer: (SHOW ANSWER)

An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping.
Breakdown of Options:
A). Self-signed certificate - These are untrusted SSL certificates but do not intercept traffic.
B). VLAN hopping - VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.
C). On-path attack - Correct answer. This intercepts and modifies traffic between two endpoints.
D). Phishing - Phishing tricks users into revealing credentials rather than intercepting network traffic.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.2: Explain common security concepts.
NIST SP 800-115: Guide to Security Testing and Assessments

NEW QUESTION: 3
Which of the following OSI model layers can utilize a connectionless protocol for data transmission?
A. Physical
B. Network
C. Transport
D. Application
Answer: (SHOW ANSWER)
The Network layer (Layer 3 of the OSI model) can utilize the connectionless protocol IP (Internet Protocol) to send data packets independently without establishing a connection. This approach is typical for protocols like IP, which provide best-effort delivery rather than guaranteed delivery. The document explains:
"The OSI Network Layer is responsible for logical addressing and routing, and it can utilize connectionless protocols like IP to send packets without requiring a session setup. This layer does not guarantee packet delivery, relying on higher layers for error detection or correction if needed."

NEW QUESTION: 4
Which of the following does a router prioritize first in the route selection process?
A. Prefix length
B. Metric
C. Administrative distance
D. Default route
Answer: (SHOW ANSWER)
In the router route selection process, the first priority is the longest prefix match, also known as prefix length.

According to CompTIA Network+ (N10-009) routing concepts, routers examine the destination IP address in the packet and compare it to entries in the routing table. When multiple routes exist, the router selects the route with the most specific match, meaning the route with the longest subnet mask (largest number of matching bits). For example, a /30 route is preferred over a /24, and a /24 is preferred over a /16 if all match the destination.
Only after the longest prefix match is determined do other factors come into play. Administrative distance (AD) is used to determine which routing source is more trustworthy when the same network is learned from different routing protocols (e.g., OSPF vs. RIP). Metric is then used within the same routing protocol to determine the best path (e.g., hop count, cost, bandwidth). A default route (0.0.0.0/0) is used only when no more specific match exists.
Therefore, prefix length is always evaluated first in route selection.

NEW QUESTION: 5
A user reports issues accessing a file server on a LAN with the IP address 192.168.50.140 at a large facility with incomplete infrastructure documentation. The following are the results of the ping command:
ping -c 10 192.168.50.140
Packets: Sent = 10, Received = 5, Lost = 5 (50% loss)
Round-trip times: Minimum = 3ms, Maximum = 144ms, Average = 42ms
Which of the following should a technician do next to continue troubleshooting the issue at the switch with minimal impact ?
A. Perform toning and probe.
B. Replace the cable.
C. Visually locate the fault.
D. Restart the switch.
Answer: A (LEAVE A REPLY)
The ping results show intermittent connectivity (50% packet loss) with highly variable latency, which commonly indicates a Layer 1/Layer 2 problem (e.g., damaged cable pairs, bad patch-panel termination, failing switch port, duplex/negotiation issues, or excessive errors on the interface). Because the facility has incomplete documentation , the technician's first priority at the switch is to positively identify the correct switch port and cable path associated with the file server before making disruptive changes.
Using a tone generator and probe aligns with Network+ troubleshooting objectives that emphasize selecting the appropriate tool and following an efficient, structured process: identify the problem, establish a theory, test, and then implement the least disruptive fix. Toning/probing helps map the server's drop to the switch port (even through patch panels) so the technician can then check that specific interface for errors/discards, CRCs, speed/duplex negotiation status, and link stability -all without rebooting the switch or immediately replacing hardware.
By contrast, restarting the switch is high-impact, and replacing a cable is a change best performed after the correct run/port is confirmed.

NEW QUESTION: 6
Which of the following is an example of a split-tunnel VPN?
A. Only public resources are accessed through the user's internet connection.
B. Encrypted resources are accessed through separate tunnels.
C. All corporate and public resources are accessed through routing to on-site servers.
D. ACLs are used to balance network traffic through different connections.
Answer: (SHOW ANSWER)
In a split-tunnel VPN, only corporate traffic is sent through the VPN tunnel, while public internet traffic goes directly through the user's local ISP. This reduces bandwidth use on the corporate VPN concentrator and improves performance for non-work traffic.
B). Separate tunnels for encrypted traffic describes multi-tunnel VPNs, not split tunneling.
C). All traffic routed through on-site servers is a full-tunnel VPN, not split-tunnel.
D). ACLs balancing traffic relates to routing or load balancing, not VPN split tunneling.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - VPN types, split vs. full tunnel, remote access.

NEW QUESTION: 7
A network administrator prepares a VLAN for a new office while planning for minimal IP address waste. The new office will have approximately 800 workstations. Which of the following network schemes meets the requirements?
A. 10.0.100.0/22
B. 172.16.8.0/23
C. 172.16.15.0/20
D. 192.168.4.0/21
Answer: (SHOW ANSWER)
To support about 800 workstations with minimal IP waste, you choose the smallest subnet that provides at least 800 usable host addresses. In IPv4, usable hosts per subnet are calculated as 2^(host bits) # 2 (subtracting network and broadcast addresses). A /22 leaves 10 host bits (32 # 22 = 10), providing 2^10 # 2 =
1024 # 2 = 1022 usable addresses-enough for 800 devices with relatively low waste.
Check the other options: /23 leaves 9 host bits, giving 2^9 # 2 = 512 # 2 = 510 usable addresses, which is not enough. A /21 provides 2^11 # 2 = 2048 # 2 = 2046 usable addresses-enough, but wastes more than /22. A
/20 provides 2^12 # 2 = 4096 # 2 = 4094 usable addresses-much more waste.
Therefore, 10.0.100.0/22 is the best choice that meets the workstation requirement while minimizing unused addresses.

NEW QUESTION: 8
A network engineer configures a NIC that has an IP address of 192.168.123.232. Which of the following classes is this address an example of?
A. Class A

B. Class B
C. Class C
D. Class D
Answer: (SHOW ANSWER)
The IPv4 address 192.168.123.232 falls within the Class C range under classful addressing. In classful terms, Class C addresses have a first octet from 192 to 223, which makes any address starting with 192.x.x.x a Class C address. Network+ (N10-009) networking concepts cover IPv4 addressing fundamentals and commonly reference class ranges as foundational knowledge, even though modern networks primarily use CIDR (classless) subnetting rather than strict classful boundaries.
This address is also within a well-known private IPv4 block: 192.168.0.0/16 (RFC1918 private addressing), which is frequently used for internal networks and NIC configurations where addresses are not routable on the public internet.
To eliminate the distractors: Class A uses first octet 1-126, Class B uses 128-191, and Class D (224-239) is reserved for multicast. Since the first octet here is 192, it maps to Class C, making option C correct.

NEW QUESTION: 9
After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two.)
A. Ensure a bottleneck is not coming from other devices on the network.
B. Install the latest firmware for the device.
C. Create a new VLAN for the access point.
D. Make sure the SSID is not longer than 16 characters.
E. Configure the AP in autonomous mode.
F. Install a wireless LAN controller.
Answer: (SHOW ANSWER)
Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms:"Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

NEW QUESTION: 10
Which of the following technologies are X.509 certificates most commonly associated with?
A. PKI
B. VLAN tagging
C. LDAP
D. MFA
Answer: (SHOW ANSWER)

X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.
* PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.
* Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.
* Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.
* Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.
* Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

NEW QUESTION: 11
Which of the following attacks forces a switch to send all traffic out of all ports?
A. ARP poisoning
B. Evil twin
C. MAC flooding
D. DNS spoofing
Answer: (SHOW ANSWER)
MAC flooding overwhelms a switch's CAM (Content Addressable Memory) table by sending a flood of frames with spoofed MAC addresses. Once the CAM table overflows, the switch cannot learn legitimate MAC addresses and defaults to flooding all frames out all ports, effectively turning it into a hub. This allows an attacker to capture traffic not originally destined for their port.
A). ARP poisoning corrupts ARP tables to redirect traffic but does not overflow the CAM table.
B). Evil twin is a wireless rogue AP attack, unrelated to switch behavior.
D). DNS spoofing redirects domain queries, not Layer 2 switching.
References (CompTIA Network+ N10-009):
Domain: Network Security - Switch security, CAM table attacks, MAC flooding.

NEW QUESTION: 12
A network analyst is installing a wireless network in a corporate environment. Employees are required to use their domain identities and credentials to authenticate and connect to the WLAN. Which of the following actions should the analyst perform on the AP to fulfill the requirements?
A. Enable MAC security.
B. Generate a PSK for each user.
C. Implement WPS.
D. Set up WPA3 protocol.

Answer: (SHOW ANSWER)
WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user- based authentication.
WPA3-Enterprise Benefits:
Uses 802.1X with EAP (Extensible Authentication Protocol) to authenticate users via a directory service (e.g., Active Directory).
Eliminates shared passwords (PSK) for authentication.
Provides strong encryption and resistance to brute-force attacks.
Incorrect Options:
A). Enable MAC Security:
MAC filtering is not secure because MAC addresses can be spoofed.
B). Generate a PSK for Each User:
Pre-shared keys (PSK) are used in WPA-Personal, not in an enterprise setting.
Does not scale well in corporate environments.
C). Implement WPS:
Wi-Fi Protected Setup (WPS) is a vulnerable security method meant for home users.
Not suitable for enterprise authentication.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Security and Authentication

NEW QUESTION: 13
A network engineer is configuring network ports in a public office. To increase security, the engineer wants the ports to allow network connections only after authentication. Which of the following security features should the engineer use?
A. Port security
B. 802.1X
C. MAC filtering
D. Access control list
Answer: (SHOW ANSWER)
802.1X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be
"always on."
A). Port security restricts by MAC addresses but does not authenticate users.
C). MAC filtering is easily spoofed and weaker than 802.1X.
D). ACLs filter traffic but do not enforce port-based authentication.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, port-based security.

NEW QUESTION: 14
An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?
A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller
Answer: (SHOW ANSWER)
* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.
* Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).
CompTIA Network+ materials discussing SNMP and MIB functionality.

NEW QUESTION: 15
Which of the following facilities is the best example of a warm site in the event of information system disruption?
A. A combination of public and private cloud services to restore data
B. A partial infrastructure, software, and data on site
C. A full electrical infrastructure in place, but no customer devices on site
D. A full infrastructure in place, but no current data on site
Answer: (SHOW ANSWER)
A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

NEW QUESTION: 16
A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?
A. NS
B. SOA
C. PTR
D. CNAME
Answer: (SHOW ANSWER)
To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.

NS (Name Server) Records: These records indicate the servers that are authoritative for a domain. Changing the NS records at the registrar points DNS resolution to the new hosting provider.
SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.
PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names.
CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses DNS records, their purposes, and how to manage them.
Cisco Networking Academy: Provides training on DNS management and the role of different DNS record types.
Network+ Certification All-in-One Exam Guide: Explains DNS records and their configuration for domain management.

NEW QUESTION: 17
A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the following spanning tree information from both switches:
Switch 1
Port State Cost
1 Forward 2
2 Forward 2
Switch 2
Port State Cost
1 Forward 2
2 Forward 2
Which of the following best describes the issue?
A. The port cost should not be equal.
B. The ports should use link aggregation.
C. A root bridge needs to be identified.

D. The switch should be configured for RSTP.

Answer: (SHOW ANSWER)

The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

NEW QUESTION: 18

A new SQL server is identified as allowing FTP access to all users. Which of the following would a systems administrator most likely do to ensure only the required services are allowed?

A. Disable unused ports on the server.

B. Change default passwords on all servers.

C. Delete the NGFW rules that allow all FTP traffic.

D. Configure server ACLs on the switches that the SQL traffic traverses.

Answer: (SHOW ANSWER)

If a SQL server is allowing FTP access to all users, the most direct and best practice action is to disable unused services/ports on the server itself. Network+ (N10-009) security objectives emphasize host hardening and the principle of least functionality: only required services should be running and listening. If FTP is not required for the SQL server's role, stopping and disabling the FTP service (and closing the associated ports on the host firewall) reduces the attack surface regardless of network firewall rules. This approach ensures the server cannot be reached via FTP even if it is placed on a different network segment or if upstream controls are misconfigured later. Changing default passwords is important, but it does not address the unnecessary exposure of an unneeded service. Deleting NGFW rules that allow all FTP traffic could help at the perimeter, but it may unintentionally break legitimate FTP usage elsewhere and still doesn't guarantee the server isn't reachable from internal networks. Switch ACLs along SQL traffic paths are indirect and easy to misapply; they also add operational complexity and may not cover all access paths. The best "only required services are allowed" control is to disable the unused service/ports on the server.

NEW QUESTION: 19

Which of the following routing protocols uses an autonomous system number?

A. IS-IS

B. EIGRP

C. OSPF

D. BGP

Answer: (SHOW ANSWER)

BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.References:CompTIA Network+ study materials and RFC 4271.

NEW QUESTION: 20

Which of the following connector types is most commonly associated with Wi-Fi antennas?

A. BNC

B. SFP

C. MPO

D. RJ45

Answer: (SHOW ANSWER)

BNC (Bayonet Neill-Concelman) connectors are commonly used with coaxial cables in RF and wireless applications, including some older Wi-Fi antennas and specialized networking equipment. The document says:

"BNC (Bayonet Neill-Concelman) connectors are typically used with coaxial cables, especially in radio frequency (RF) and some Wi-Fi antenna applications, providing a secure and quick connect/disconnect."

NEW QUESTION: 21

A user cannot access an external server for a client after connecting to a VPN. Which of the following commands would a support agent most likely use to examine the issue? (Select two).

A. nslookup

B. tcpdump

C. arp

D. dig

E. tracert

F. route print

Answer: (SHOW ANSWER)

When a user connects to a VPN and experiences connectivity issues to an external server, the problem is often related to routing or network path issues.

E). tracert:

Traces the path packets take from the user's device to the destination server.

Helps determine if the traffic is being blocked or misrouted.

F). route print:

Displays the device's routing table.

Helps diagnose whether traffic is being sent to the VPN tunnel instead of the correct external server.

Incorrect Options:

A). nslookup: Used for resolving domain names to IPs (DNS troubleshooting), but this issue is likely routing- related.

B). tcpdump: Captures packets for deep packet analysis, not typically the first step in diagnosing a VPN- related access issue.

C). arp: Used for resolving local network MAC addresses, not relevant for external VPN issues.

D). dig: Like nslookup, used for DNS queries, but not useful for routing problems.

Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Troubleshooting Network Connectivity

NEW QUESTION: 22
Which of the following can support a jumbo frame?
A. Access point
B. Bridge
C. Hub
D. Switch
Answer: (SHOW ANSWER)
* Definition of Jumbo Frames:
* Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.
* Why Switches Support Jumbo Frames:
* Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.
* Incompatibility of Other Devices:
* Access Point: Primarily handles wireless communications and does not typically support jumbo frames.
* Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.
* Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.
* Practical Application:
* Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.
References:
* CompTIA Network+ course materials and networking hardware documentation.

NEW QUESTION: 23
A network engineer needs to virtualize network services, including a router at a remote branch location.
Which of the following solutions meets the requirements?
A. NFV
B. VRF
C. VLAN
D. VPC
Answer: (SHOW ANSWER)

Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.
VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.
VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.
VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.
Reference: CompTIA Network+ Official Study Guide, Domain 2.1 (Virtualization and Cloud Concepts).

NEW QUESTION: 24
Which of the following network traffic type is sent to all nodes on the network?
A. Unicast
B. Broadcast
C. Multicast
D. Anycast
Answer: (SHOW ANSWER)
Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
* Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
* Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
* IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains network traffic types, including broadcast, unicast, and multicast.
* Cisco Networking Academy: Provides training on network communication methods and traffic types.
* Network+ Certification All-in-One Exam Guide: Discusses different types of network traffic and their uses in various network scenarios.
Broadcast traffic is essential for network operations that require communication with all nodes, such as ARP requests or DHCP discovery messages.

NEW QUESTION: 25
Which of the following allows a remote user to connect to the network?
A. Command-line interface

B. API gateway
C. Client-to-site VPN
D. Jump box
Answer: (SHOW ANSWER)
A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

NEW QUESTION: 26
Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?
A. Router
B. Switch
C. Firewall
D. Load balancer
Answer: (SHOW ANSWER)
A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.
Breakdown of Options:
A). Router - Directs traffic between networks, not between web servers.
B). Switch - Works at Layer 2, does not distribute web traffic.
C). Firewall - Secures network traffic, but does not distribute load.
D). Load balancer - # Correct answer. Optimizes web traffic distribution across multiple servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

NEW QUESTION: 27
Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?
A. Site-to-site VPN
B. GRE tunnel
C. VXLAN
D. Dedicated line
Answer: (SHOW ANSWER)
A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.

Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.
Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.
Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.
Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

NEW QUESTION: 28
Users are experiencing significant lag while connecting to a cloud-based application during peak hours. An examination of the network reveals that the bandwidth is being heavily utilized. Further analysis shows that only a few users are using the application at any given time. Which of the following is the most cost-effective solution for this issue?
A. Limit the number of users who can access the application.
B. Lease a Direct Connect connection to the cloud service provider.
C. Implement QoS to prioritize application traffic.
D. Use a CDN to service the application.
Answer: C (LEAVE A REPLY)
Quality of Service (QoS)is the best cost-effective solution. It prioritizes traffic based on application criticality.
If the bandwidth is limited and only a few users are affected, prioritizing that application traffic can improve performance without needing costly bandwidth upgrades or direct connections.
Reference:Section 1.2 - Networking Appliances, Applications, and Functions - "Quality of Service (QoS)"

NEW QUESTION: 29
Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?
A. Patch
B. UPS
C. MDF
D. Rack
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

NEW QUESTION: 30
Which of the following is associated with avoidance, acceptance, mitigation, and transfer?

A. Risk
B. Exploit
C. Threat
D. Vulnerability
Answer: (SHOW ANSWER)
These four terms-avoidance, acceptance, mitigation, and transfer-are strategies used in risk management.
From Andrew Ramdayal's guide:
"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."

NEW QUESTION: 31
Which of the following concepts describes the idea of housing different customers in the same public cloud data center?
A. Elasticity
B. Hybrid cloud
C. Scalability
D. Multitenancy
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
Multitenancy is a cloud concept where multiple customers share the same physical resources (servers, storage, and networks) but remain logically separated for security and privacy.
A). Elasticity is auto-scaling resources.
B). Hybrid cloud combines private and public resources.
C). Scalability is the ability to grow resources but doesn't imply multiple customers.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing models, multitenancy in public cloud.

NEW QUESTION: 32
A user's desk has a workstation and an IP phone. The user is unable to browse the internet on the workstation, but the phone works. Which of the following configurations is required?

A. Voice VLAN
B. Native VLAN
C. Data VLAN
D. Trunk port
Answer: (SHOW ANSWER)
If the IP phone works but the workstation doesn't, it indicates that theVoice VLAN is functioningcorrectly, but theData VLAN (C)is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately usingVLANs.
* A. Voice VLANis for the IP phone, which is already working.
* B. Native VLANis for untagged traffic on trunk ports, but doesn't control access directly.
* D. Trunk portis more relevant to switch interconnections than individual workstation ports.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 33
Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?
A. IPS
B. IDS
C. Load balancer
D. Firewall
Answer: (SHOW ANSWER)
An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-line and can introduce delay.
From Andrew Ramdayal's guide:
"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

NEW QUESTION: 34
A network technician is adding a new switch to increase capacity on the network. The technician connects the two switches using a single cable. Several hosts are moved to the new switch, but none of the hosts can access the network or internet. Which of the following should the technician do to resolve the issue?
A. Configure the connecting ports as trunk ports
B. Install STP cables between the switches
C. Increase the PoE budget for the switches
D. Set up link aggregation on the uplink ports
Answer: (SHOW ANSWER)

The correct solution is to configure the connecting ports as trunk ports. When connecting switches, the uplink ports must be configured to carry traffic for multiple VLANs (trunking), not just a single access VLAN.
Without trunking, VLAN tags may be dropped, and traffic from hosts will not reach the rest of the network or internet.
B). STP cables is a misnomer - STP refers to Spanning Tree Protocol or Shielded Twisted Pair cables, neither of which solves this logical configuration issue.
C). PoE budget is irrelevant because switches and hosts in this context don't require PoE.
D). Link aggregation (LACP, EtherChannel) is for increasing bandwidth/redundancy across multiple links, not required with a single cable.
By enabling trunking on the uplink ports, the switches can pass VLAN-tagged traffic, ensuring hosts connected to the new switch have access to the same resources as those on the existing switch.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN trunking, inter-switch connectivity.

NEW QUESTION: 35
A company wants to implement a disaster recovery site or non-critical applicance, which can tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?
A. Hot
B. Cold
C. Warm
D. Passive
Answer: (SHOW ANSWER)
A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.
* Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non- critical applications that can tolerate short downtimes.
* Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.
* Cisco Networking Academy: Provides training on disaster recovery planning and site selection.
* Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.
Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

NEW QUESTION: 36
Which of the following best describes the amount of time between a disruptive event and the point that affected resources need to be back to fully functional status?
A. RTO
B. MTBF
C. RPO
D. MTTR
Answer: (SHOW ANSWER)
The correct metric is RTO (Recovery Time Objective). RTO defines the maximum acceptable time to restore services after a disruption, ensuring business continuity. For example, if the RTO is 4 hours, systems must be back online within that timeframe after an outage.
B). MTBF (Mean Time Between Failures) measures reliability by calculating the average time between hardware failures.
C). RPO (Recovery Point Objective) defines how much data loss (in terms of time, such as last backup point) is acceptable.
D). MTTR (Mean Time to Repair) measures the average time taken to fix a failure but is not a predefined business requirement like RTO.
Organizations define RTOs during disaster recovery planning to align IT recovery capabilities with business needs.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Business continuity metrics (RTO, RPO, MTBF, MTTR).

NEW QUESTION: 37
A network administrator recently configured an autonomous wireless AP and performed a throughput test via comptiaspeedtester.com. The result was 75 Mbps. When connected to other APs, the results reached 500 Mbps. Which of the following is most likely the reason for this difference?
A. Channel width configuration
B. DNS server issues
C. Authentication failure
D. Incorrect DHCP settings
Answer: (SHOW ANSWER)
The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.
* B. DNS issues affect name resolution, not raw throughput.
* C. Authentication failure would prevent connection, not reduce throughput.
* D. DHCP issues would prevent obtaining an IP, not cause slower speeds.
References (CompTIA Network+ N10-009):

* Domain: Network Troubleshooting - Wireless throughput issues, channel width configuration.

NEW QUESTION: 38
A network technician is designing a LAN for a new facility. The company is expecting more than 300 devices to connect to the network. Which of the following masks will provide the most efficient subnet?
A. 255.255.0.0
B. 255.255.192.0
C. 255.255.254.0
D. 255.255.255.254
Answer: C (LEAVE A REPLY)
The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.
* 255.255.0.0 (/16) provides too many addresses.
* 255.255.192.0 (/18) gives 16384 addresses - overkill.
* 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).
From Andrew Ramdayal's guide:
"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

NEW QUESTION: 39
A network architect of a stock exchange broker is implementing a disaster recovery (DR), high-availability plan. Which of the following approaches would be the best fit?
A. Warm site
B. Active-active
C. Full mesh
D. In-band
Answer: (SHOW ANSWER)
The correct answer is Active-active because a stock exchange broker requires extremely high availability, minimal downtime, and near-zero data loss. According to CompTIA Network+ (N10-009) objectives under high availability and disaster recovery concepts, an active-active configuration involves multiple systems or sites operating simultaneously and sharing the workload. If one system fails, the other continues processing traffic without service interruption. This model provides the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which is critical in financial trading environments where even seconds of downtime can result in major financial loss. Active-active architectures also support load balancing, redundancy, and continuous synchronization between systems.
A warm site (Option A) contains preconfigured hardware but may require data restoration and configuration before becoming fully operational, resulting in some downtime. A full mesh (Option C) is a network topology design and does not specifically address disaster recovery at the service

level. In-band (Option D) refers to management traffic sharing the production network and is unrelated to DR strategy.
Therefore, an active-active approach is the most suitable solution for mission-critical financial operations.

NEW QUESTION: 40

Which of the following is a documented set of requirements, such as quality, availability, and responsibilities delivered by a vendor?

A. MOU
B. EOL
C. EOS
D. SLA
Answer: (SHOW ANSWER)
The correct answer is SLA (Service Level Agreement) because it is a formal, documented contract between a service provider and a customer that defines expected service standards. According to CompTIA Network+ (N10-009) objectives under network operations and service management concepts, an SLA outlines measurable performance metrics such as uptime percentage, response time, throughput, support availability, escalation procedures, and responsibilities of both parties.
An SLA ensures accountability and establishes clear expectations for service delivery. For example, a vendor may guarantee 99.99% uptime, define maximum resolution times for incidents, and specify penalties or credits if performance targets are not met. SLAs are critical in cloud services, ISP agreements, managed services, and enterprise vendor contracts.
An MOU (Memorandum of Understanding) is a non-binding agreement outlining general terms between parties but does not define enforceable service metrics. EOL (End of Life) refers to when a product is no longer sold or supported. EOS (End of Support) indicates when a vendor stops providing updates or assistance for a product.
Therefore, an SLA is the correct document that defines vendor-delivered service requirements.
Top of Form

NEW QUESTION: 41
Two companies successfully merged. Following the merger, a network administrator identified a connection bottleneck. The newly formed company plans to acquire a high-end 40GB switch and redesign the network from a three-tier model to a collapsed core. Which of the following should the administrator do until the new devices are acquired?
A. Implement the FHRP.
B. Configure a route selection metric change.
C. Install a load balancer.
D. Enable link aggregation.
Answer: (SHOW ANSWER)
*The issue described is a network bottleneck due to increased traffic after a merger.

*A collapsed core architecture consolidates the core and distribution layers into a single layer to improve efficiency and reduce latency.
*Until the 40GB switch is acquired, Link Aggregation (LAG) (IEEE 802.3ad / LACP) can be used to combine multiple physical links into a single logical link, increasing bandwidth and reducing bottlenecks.
*FHRP (First Hop Redundancy Protocol) (A) is used for gateway redundancy, not link aggregation.
*Route selection metric changes (B) help with routing decisions but don't address physical link congestion.
*Load balancers (C) distribute traffic for applications, not network links.
#Reference: CompTIA Network+ N10-009 Official Documentation - Network Architecture and Performance Optimization.

NEW QUESTION: 42
Which of the following most likely determines the size of a rack for installation? (Select two).
A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height
Answer: B (LEAVE A REPLY)
Understanding Rack Size Determination:
The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.
Switch Depth:
Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.
Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.
Server Height:
Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals
1.75 inches. The total height of all equipment determines the overall height requirement of the rack.
Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.
Why Other Options are Less Relevant:
KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.

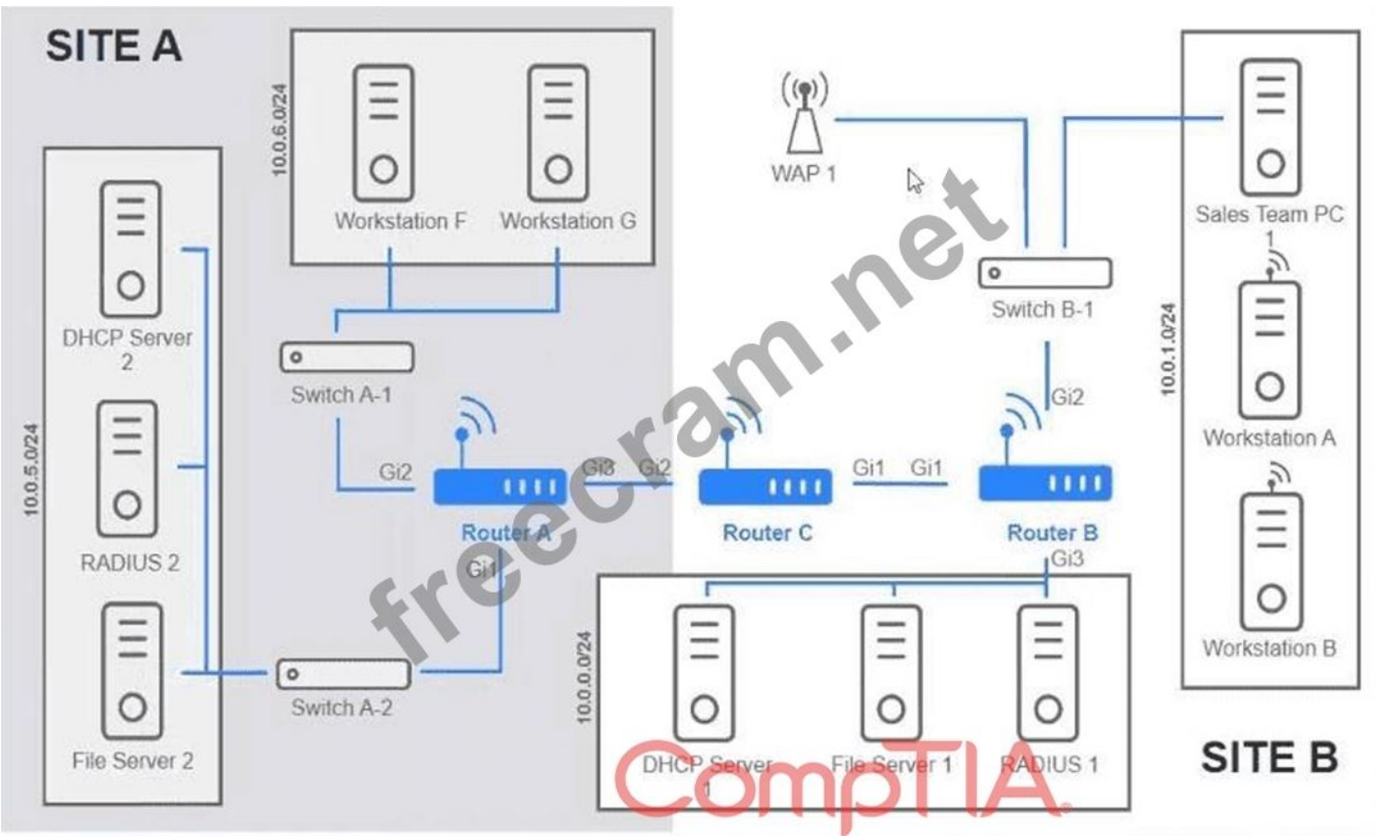
Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.
Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.
Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.
References:
CompTIA Network+ study materials on rack installation and equipment sizing.

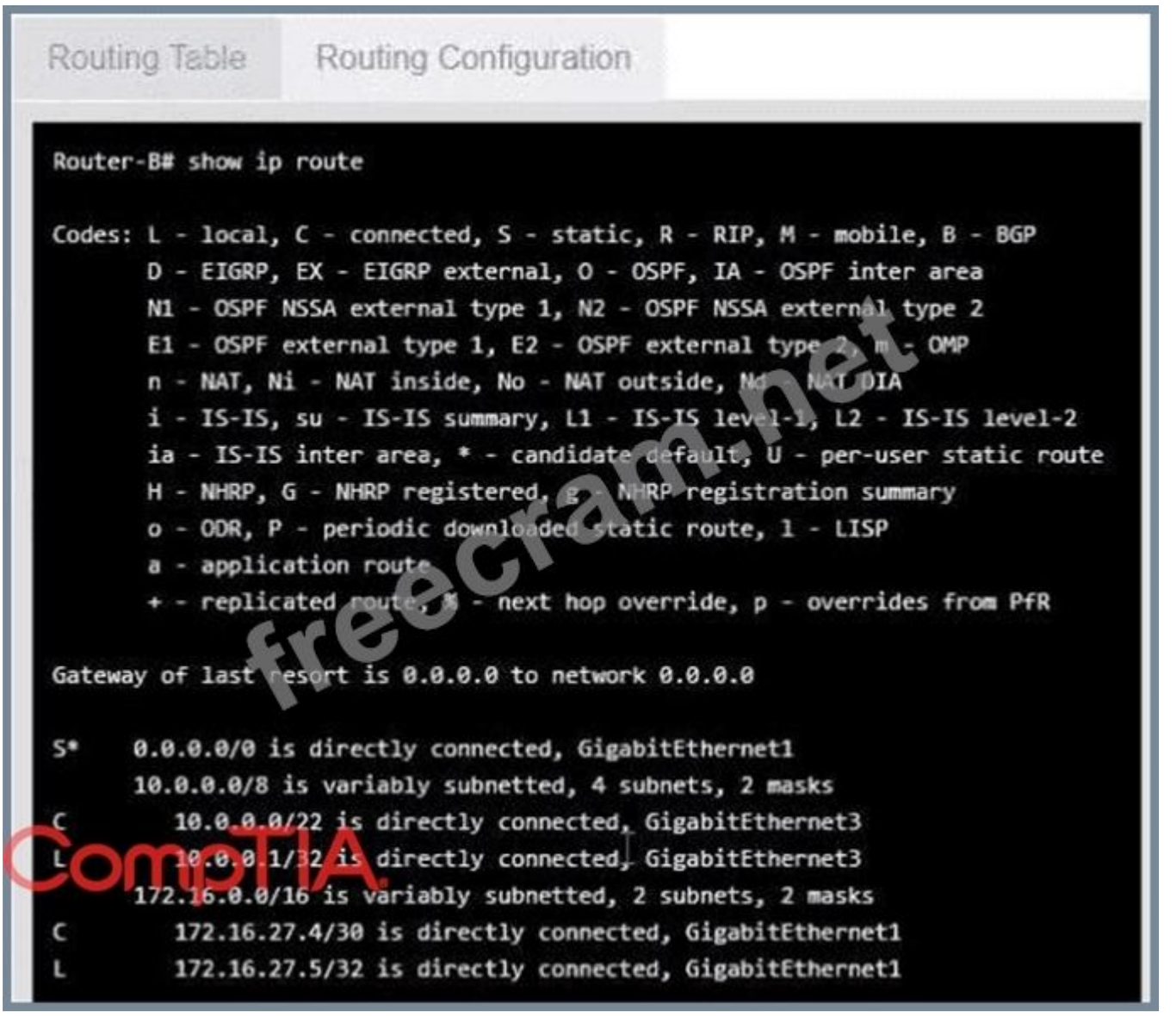
NEW QUESTION: 43
A network administrator notices interference with industrial equipment in the 2.4GHz range.
Which of the following technologies would most likely mitigate this issue? (Select two).
A. Mesh network
B. 5GHz frequency
C. Omnidirectional antenna
D. Non-overlapping channel
E. Captive portal
F. Ad hoc network
Answer: (SHOW ANSWER)
* Understanding 2.4GHz Interference:
* The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
* Mitigation Strategies:
* 5GHz Frequency:
* The 5GHz frequency band offers more channels and less interference compared to the 2.4 GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.
* Non-overlapping Channels:
* In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.
* Why Other Options are Less Effective:
* Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.
* Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.
* Captive Portal: A web page that users must view and interact with before accessing a network, unrelated to frequency interference.
* Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.
* Implementation:

* Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices.
* Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.
References:
* CompTIA Network+ study materials on wireless networking and interference mitigation.

NEW QUESTION: 44
Which of the following is used to redistribute traffic between one source and multiple servers that run the same service?
A. Router
B. Switch
C. Firewall
D. Load balancer
Answer: (SHOW ANSWER)
The correct answer is Load balancer because it is specifically designed to distribute incoming network traffic across multiple backend servers that provide the same application or service. According to CompTIA Network+ (N10-009) objectives under network infrastructure, load balancing improves performance, scalability, and high availability by preventing any single server from becoming overwhelmed.
A load balancer can operate at Layer 4 (transport layer, based on IP address and port) or Layer 7 (application layer, based on content such as HTTP headers or URLs). It uses various algorithms such as round-robin, least connections, or weighted distribution to efficiently allocate client requests among servers. If one server fails, the load balancer can redirect traffic to healthy servers, ensuring service continuity.
A router (Option A) forwards packets between different networks but does not distribute traffic among servers running the same application. A switch (Option B) forwards frames within a local network based on MAC addresses. A firewall (Option C) filters traffic based on security rules but does not perform traffic distribution for load-sharing purposes.
Therefore, a load balancer is the correct solution for redistributing traffic among multiple servers.

NEW QUESTION: 45
Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identity any Issues, and configure the appropriate solution If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;





Answer:

See the solution configuration below in Explanation.

Explanation:

A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.

A screenshot of a computer AI-generated content may be incorrect.

NEW QUESTION: 46
To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?
A. Public
B. Hybrid
C. SaaS
D. Private
Answer: (SHOW ANSWER)

A hybrid cloud deployment model is the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.References: CompTIA Network+ study materials and cloud computing principles.

NEW QUESTION: 47
A user called the help desk after business hours to complain that files on a device are inaccessible and the wallpaper was changed. The network administrator thinks that this issue is an isolated incident, but the security analyst thinks the issue might be a ransomware attack. Which of the following troubleshooting steps should be taken first?
A. Identify the problem
B. Establish a theory
C. Document findings
D. Create a plan of action
Answer: (SHOW ANSWER)
The first step in any troubleshooting process is to identify the problem. This includes gathering information from the user, reviewing logs, and observing the symptoms. In this case, identifying the scope and nature of the issue (e.g., signs of ransomware) is critical before forming any theories or plans.
From Andrew Ramdayal's guide:
"The troubleshooting methodology begins with identifying the problem. This step involves questioning users, identifying user changes, and determining the symptoms."

NEW QUESTION: 48
A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?
A. Configure ACLs.
B. Implement a captive portal.
C. Enable port security.
D. Disable unnecessaryservices.

Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 49
Which of the following is used to stage copies of a website closer to geographically dispersed users?
A. VPN
B. CDN
C. SAN
D. SDN
Answer: (SHOW ANSWER)
A Content Delivery Network (CDN) caches website content across multiple geographically distributed servers to reduce latency and improve load times for users worldwide.
Breakdown of Options:
A). VPN - Encrypts network connections, does not distribute website content.
B). CDN - # Correct answer. A network of caching servers that delivers web content faster.
C). SAN - Storage Area Network, not related to web content distribution.
D). SDN - Software-defined networking, which controls network flows but does not stage website content.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Compare and contrast different networking services.

NEW QUESTION: 50
An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?

A. SSE
B. ACL
C. Perimeter network
D. 802.1x
Answer: (SHOW ANSWER)
802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
* 802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.
* Access Control: Prevents unauthorized devices from connecting to the network, enhancing security in public or semi-public areas.

* Implementation: Typically used in conjunction with a RADIUS server to manage authentication requests.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers 802.1x and its role in network security.
* Cisco Networking Academy: Provides training on implementing 802.1x for secure network access control.
* Network+ Certification All-in-One Exam Guide: Explains the benefits and configuration of 802.1x authentication in securing network access.

NEW QUESTION: 51
Newly crimped 26ft (8m) STP Cat 6 patch cables were recently installed in one room to replace cables that were damaged by a vacuum cleaner. Now, users in that room are unable to connect to the network. A network technician tests the existing cables first. The 177ft (54m) cable that runs from the core switch to the access switch on the floor is working, as is the 115ft (35m) cable run from the access switch to the wall jack in the office. Which of the following is the most likely reason the users cannot connect to the network?
A. Mixed UTP and STP cables are being used.
B. The patch cables are not plenum rated.
C. The cable distance is exceeded.
D. An incorrect pinout on the patch cable is being used.
Answer: (SHOW ANSWER)
An incorrect pinout on the patch cable could prevent network connectivity due to mismatched wiring. Even if the cables are the correct length and type, a pinout issue can cause continuity problems and prevent data transmission. Proper crimping with the correct pinout is essential for network cables to function. (Reference:
CompTIA Network+ Study Guide, Chapter on Network Media and Topologies)

NEW QUESTION: 52
A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?
A. 802.1Q tagging
B. Jumbo frames
C. Half duplex
D. Link aggregation
Answer: (SHOW ANSWER)
Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.
Breakdown of Options:

A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.
IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

NEW QUESTION: 53
A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?
A. 802.1Q tagging
B. Spanning tree
C. Link aggregation
D. Jumbo frames
Answer: (SHOW ANSWER)
VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size.
This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging enables segmentation but does not address fragmentation issues.
B). Spanning tree - STP prevents loops but does not improve performance for VXLAN traffic.
C). Link aggregation - LACP combines links for higher bandwidth but does not prevent fragmentation.
D). Jumbo frames - Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network performance concepts.
RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

NEW QUESTION: 54
A network administrator needs to set up a multicast network for audio and video broadcasting. Which of the following networks would be the most appropriate for this application?
A. 172.16.0.0/24
B. 192.168.0.0/24

C. 224.0.0.0/24
D. 240.0.0.0/24
Answer: (SHOW ANSWER)
* Understanding Multicast:
* Multicast IP Address Range:The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.
* Multicast Applications:
* Use Case:Multicast is used for one-to-many or many-to-many communication, suitable for applications like audio and video broadcasting where the same data is sent to multiple recipients simultaneously.
* Appropriate Network Selection:
* 224.0.0.0/24 Network:This range is reserved for multicast addresses, making it the appropriate choice for setting up a multicast network.
* Comparison with Other Options:
* 172.16.0.0/24:Part of the private IP address space, used for private networks, not designated for multicast.
* 192.168.0.0/24:Another private IP address range, also not for multicast.
* 240.0.0.0/24:Reserved for future use, not suitable for multicast.
References:
* CompTIA Network+ study materials on IP address ranges and multicast.

NEW QUESTION: 55
An imaging workstation at a hospital is experiencing intermittent connectivity loss. Which of the following would most likely be used to resolve the issue at the least expense?
A. Single-mode fiber
B. Twinaxial cable
C. Spanning tree
D. Shielded twisted pair
Answer: D (LEAVE A REPLY)
The correct answer is Shielded Twisted Pair (STP). According to the CompTIA Network+ N10-009 objectives, intermittent connectivity issues-especially in environments like hospitals-are often caused by electromagnetic interference (EMI) from medical imaging equipment, power systems, and other electronic devices. These environments are electrically noisy and can disrupt standard copper Ethernet cabling.
STP cabling is specifically designed to mitigate EMI by incorporating shielding around the twisted pairs. This shielding reduces external interference and improves signal stability without requiring a complete redesign of the network. Importantly, STP is significantly less expensive than deploying fiber-optic solutions while still being highly effective in environments prone to interference.
Single-mode fiber would eliminate EMI entirely, but it is far more costly due to specialized cabling, transceivers, and installation requirements. Twinaxial cable is typically used for short-distance,

high-speed data center connections and is not appropriate for workstation connectivity. Spanning Tree Protocol (STP) is a Layer 2 loop-prevention protocol and has nothing to do with physical connectivity or interference issues.
The Network+ objectives stress choosing solutions that balance effectiveness, cost, and environmental suitability. In this case, upgrading to shielded twisted pair cabling provides the most practical and cost- effective resolution for intermittent connectivity in a hospital imaging environment.

NEW QUESTION: 56
Which of the following provides an opportunity for an on-path attack?
A. Phishing
B. Dumpster diving
C. Evil twin
D. Tailgating
Answer: (SHOW ANSWER)
An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity.
Breakdown of Options:
A: Phishing - Tries to steal credentials through fake emails/websites but does not intercept network traffic.
B: Dumpster diving - Involves physical security breaches, not network interception.
C: Evil twin - # Correct answer. A rogue Wi-Fi AP impersonates a real network, allowing traffic interception.
D: Tailgating - Involves physical access security, not network interception.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain common network security threats.

NEW QUESTION: 57
A network technician is attempting to harden a commercial switch that was recently purchased. Which of the following hardening techniques best mitigates the use of publicly available information?
A. Changing the default password
B. Blocking inbound SSH connections
C. Removing the gateway from the network configuration
D. Restricting physical access to the switch
Answer: (SHOW ANSWER)
Changing the default password is a fundamental step in device hardening, as default credentials are widely known and published online, posing a significant security risk if not updated. The document notes:

"Default passwords are often known by attackers and published on the internet. Changing them to unique, strong passwords is a critical first step in securing network devices against unauthorized access."

NEW QUESTION: 58
Which of the following technologies is most appropriate for a business that requires high-speed access to frequently used web content, such as images and videos?
A. CDN
B. SAN
C. Firewall
D. Switch
Answer: (SHOW ANSWER)
The correct solution is a Content Delivery Network (CDN). A CDN caches web content (like images, videos, scripts) on distributed servers close to end users. This reduces latency, improves load times, and decreases the load on origin servers. For a business requiring high-speed access to media-rich content, a CDN is the most effective option.
B). SAN (Storage Area Network) is used for storage in a data center, not for distributing web content.
C). Firewall secures traffic but doesn't accelerate content delivery.
D). Switches forward packets within a LAN, not globally distribute content.
By leveraging CDNs, businesses can handle large traffic volumes efficiently while improving user experience.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - CDNs, caching, performance optimization.

NEW QUESTION: 59
Which of the following IP transmission types encrypts all of the transmitted data?
A. ESP
B. AH
C. GRE
D. UDP
E. TCP
Answer: (SHOW ANSWER)
Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data.
ESP encrypts the payload and optional ESP trailer, providing data confidentiality.
ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.

ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).
Comparison with Other Protocols:
AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.
GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.
UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.
Use Cases:
ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.
References:
CompTIA Network+ study materials on IPsec and encryption.

NEW QUESTION: 60

Which of the following is used to describe the average duration of an outage for a specific service?

A. RPO
B. MTTR
C. RTO
D. MTBF
Answer: (SHOW ANSWER)
MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

NEW QUESTION: 61
Which of the following attacks would most likely cause duplicate IP addresses in a network?
A. Rogue DHCP server
B. DNS poisoning
C. Social engineering
D. Denial-of-service
Answer: (SHOW ANSWER)
* Definition of a Rogue DHCP Server:
* A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.
* Impact of a Rogue DHCP Server:
* IP Address Conflicts:Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.
* Network Disruption:Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.
* Comparison with Other Attacks:

* DNS poisoning:Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.
* Social engineering:Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.
* Denial-of-service (DoS):Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.
* Prevention and Detection:
* Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.
* Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 62
A user calls the help desk after business hours to complain that files on a device are inaccessible and the wallpaper was changed. The network administrator thinks that this issue is an isolated incident, but the security analyst thinks the issue might be a ransomware attack. Which of the following troubleshooting steps should be taken first?
A. Identify the problem.
B. Establish a theory.
C. Document findings.
D. Create a plan of action.
Answer: (SHOW ANSWER)
The correct answer is Identify the problem, which is always the first step in the CompTIA Network + N10-009 troubleshooting methodology. Before forming theories, creating action plans, or documenting outcomes, technicians must clearly understand what is happening, who is affected, and what symptoms are present.
In this scenario, the symptoms-inaccessible files and a changed wallpaper-are serious and potentially indicative of a security incident such as ransomware. However, at this stage, there is disagreement between the network administrator and the security analyst regarding the nature of the issue. That reinforces the need to begin with problem identification, which includes gathering

information, determining the scope of impact, identifying recent changes, and assessing whether the incident is isolated or widespread.
Establishing a theory comes after the problem has been clearly defined. Creating a plan of action and documenting findings occur later in the process, once the issue has been confirmed and remediation steps are determined. Jumping ahead without properly identifying the problem could result in delayed containment or an incorrect response-especially critical in potential security incidents.
The Network+ objectives emphasize following the structured troubleshooting process precisely to reduce risk, prevent escalation, and ensure accurate resolution-particularly when malware or ransomware may be involved.

NEW QUESTION: 63
After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?
A. Inspect the connectors for any wires that are touching or exposed.
B. Restore default settings on the connected devices.
C. Terminate the connections again.
D. Check for radio frequency interference in the area.
Answer: (SHOW ANSWER)
Cross talk can often be caused by improper termination of cables. The first step in troubleshooting should be to inspect the connectors for any wires that might be touching or exposed. Ensuring that all wires are correctly seated and that no conductors are exposed can help reduce or eliminate cross talk. This step should be taken before attempting to re-terminate the connections or check for other sources of interference.References:
CompTIA Network+ study materials.

NEW QUESTION: 64
An organization wants better network visibility. The organization's requirements include:
Multivendor/OS-monitoring capabilities
Real-time collection
Data correlation
Which of the following meets these requirements?
A. SNMP
B. SIEM
C. Nmap
D. Syslog
Answer: (SHOW ANSWER)
A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments.

Breakdown of Options:
A). SNMP - SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.
B). SIEM - Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.
C). Nmap - Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.
D). Syslog - Syslog collects logs but does not correlate or analyze them in real-time.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain network security concepts.
NIST Special Publication 800-92: Guide to Computer Security Log Management

NEW QUESTION: 65
A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?
A. 802.1X
B. Access control list
C. Port security
D. MAC filtering
Answer: (SHOW ANSWER)
802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means.
802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.References:CompTIA Network+ study materials.

NEW QUESTION: 66
After providing a username and password, a user must input a passcode from a phone application. Which of the following authentication technologies is used in this example?
A. SSO
B. LDAP
C. MFA
D. SAML
Answer: (SHOW ANSWER)
This is an example of Multi-Factor Authentication (MFA) because it requires:
Something you know (username/password)
Something you have (a phone-generated passcode)
Breakdown of Options:

A: SSO (Single Sign-On) - Allows one login for multiple services, but does not add a second authentication factor.
B: LDAP (Lightweight Directory Access Protocol) - Used for directory authentication, not MFA.
C: MFA (Multi-Factor Authentication) - # Correct answer. Uses multiple authentication factors for better security.
D: SAML (Security Assertion Markup Language) - Used for federated identity management, not multi-factor authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement authentication and authorization methods.

NEW QUESTION: 67
After changes were made to a firewall, users are no longer able to access a web server. A network administrator wants to ensure that ports 80 and 443 on the web server are still accessible from the user IP space. Which of the following commands is best suited to perfom this testing?
A. Ifconfig
B. Ping
C. Dig
D. nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 68
A network engineer is troubleshooting connectivity for a newly installed server on an existing VLAN. The engineer reviews the following output:
C:\> ipconfig
IP Address: 192.168.100.225
Mask: 255.255.255.224
Gateway: 192.168.100.254
Router# show ip route
C 192.168.100.0/24 is directly connected, GigabitEthernet0/0
Which of the following describes the issue?
A. The server has an incorrect subnet mask
B. There is a duplicate IP address on the network
C. The DHCP address pool is exhausted
D. The router is missing a default route
Answer: (SHOW ANSWER)
The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to 192.168.100.255. However, the router only recognizes 192.168.100.0/24, indicating a mismatch between the server's subnet and the router's network.
Correct mask for the /24 network is 255.255.255.0, allowing 256 IPs from 192.168.100.0 to 192.168.100.255.

This mismatch would result in routing issues, especially with the gateway outside of the subnet range.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.2 - Given a scenario, troubleshoot common wired connectivity issues.

NEW QUESTION: 69
An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?
A. Implementingenterprise authentication
B. Requiring theuse of PSKs
C. Configuring acaptive portal for users
D. Enforcing wired equivalent protection
Answer: A (LEAVE A REPLY)
Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual accountability. Captive portals can identify users but are less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.
Reference:
CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

NEW QUESTION: 70
A network rack has four servers and four switches with dual power supplies. Only one intelligent PDU is installed in the rack. Which of the following is the reason to add a second PDU?

A. Power redundancy
B. Failed PSU monitoring
C. Surge protection
D. Electricity conservation
Answer: (SHOW ANSWER)
The correct answer is Power redundancy because the devices in the rack are equipped with dual power supplies, which are specifically designed to support redundant power sources. According to CompTIA Network+ (N10-009) objectives under high availability and physical infrastructure concepts, redundancy is a key strategy to eliminate single points of failure.
If only one PDU (Power Distribution Unit) is installed, both power supplies from each device may ultimately rely on the same power source. This creates a single point of failure-if the PDU fails or loses upstream power, all connected equipment will shut down despite having dual power supplies.

By installing a second PDU connected to a separate power circuit (and ideally a separate UPS or power feed), each power supply in the servers and switches can connect to different PDUs. If one PDU fails, the other continues delivering power, ensuring uninterrupted operation.
Option B (Failed PSU monitoring) is not the primary reason for adding another PDU. Option C (Surge protection) can be provided by a single PDU. Option D (Electricity conservation) is unrelated to redundancy design.
Therefore, adding a second PDU provides true power redundancy.

NEW QUESTION: 71
Which of the following does BGP use for loop avoidance?
A. Autonomous system path
B. Peer autonomous system
C. Autonomous system length
D. Public autonomous system
Answer: (SHOW ANSWER)
The correct answer is Autonomous system path because BGP (Border Gateway Protocol) prevents routing loops by using the AS_PATH attribute. According to CompTIA Network+ (N10-009) objectives under routing protocols, BGP is a path vector protocol used to exchange routing information between autonomous systems (AS) on the internet.
When a BGP router advertises a route, it includes its autonomous system number (ASN) in the AS_PATH attribute. As the route passes through additional autonomous systems, each AS appends its own ASN to the path. If a BGP router receives a route advertisement that already contains its own ASN in the AS_PATH list, it recognizes this as a loop and rejects the route. This mechanism effectively prevents routing loops across large-scale networks such as the internet.
Option B (Peer autonomous system) refers to neighboring BGP routers but does not describe the loop prevention mechanism. Option C (Autonomous system length) relates to path selection metrics, as shorter AS_PATH lengths are generally preferred, but this is not the loop avoidance function itself. Option D (Public autonomous system) is not a loop prevention mechanism.
Therefore, BGP uses the AS_PATH attribute for loop avoidance.

NEW QUESTION: 72
A company implements a new network utilizing only IPv6 addressing and needs to connect to the internet.
Which of the following must be enabled in order for the internal network to contact servers on the internet?
A. MPLS
B. NAT64
C. GRE
D. Static routing
Answer: (SHOW ANSWER)

The correct answer is NAT64, which is required when an IPv6-only internal network needs to communicate with IPv4-based servers on the internet. According to the CompTIA Network+ N10-009 objectives, NAT64 is a translation technology that enables interoperability between IPv6 clients and IPv4 resources during the ongoing transition from IPv4 to IPv6.
Although IPv6 is widely deployed, a significant portion of internet services still operate exclusively on IPv4.
An IPv6-only host cannot natively communicate with an IPv4 server because the protocols use different addressing formats. NAT64 solves this problem by translating IPv6 packets into IPv4 packets and translating the responses back into IPv6, allowing seamless communication without requiring dual-stack configuration on internal hosts.
The other options do not address this requirement. MPLS is a WAN forwarding technology used by service providers and does not provide protocol translation. GRE is a tunneling protocol used to encapsulate traffic and does not enable IPv6-to-IPv4 communication. Static routing determines packet paths but does not resolve protocol incompatibility between IPv4 and IPv6.
The Network+ N10-009 exam places strong emphasis on IPv6 transition mechanisms, including NAT64, DNS64, and dual stack. In this scenario, NAT64 is the essential component that enables IPv6-only networks to access legacy IPv4 internet services.

NEW QUESTION: 73
Which of the following disaster recovery metrics is used to describe the amount of data that is lost since the last backup?
A. MTTR
B. RTO
C. RPO
D. MTBF
Answer: (SHOW ANSWER)
* Definition of RPO:
* Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.
* For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.
* Why RPO is Important:
* RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.
* Comparison with Other Metrics:
* MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.
* RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

* MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.
* How RPO is Used in Disaster Recovery:
* Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.
References:
* CompTIA Network+ study materials and certification guides.

NEW QUESTION: 74
Users report latency with a SaaS application. Which of the following should a technician adjust to fix the issue?
A. Server hardware specifications
B. Data-at-rest encryption settings
C. Network bandwidth and utilization
D. Virtual machine configurations
Answer: (SHOW ANSWER)
The correct answer is Network bandwidth and utilization because latency issues with a SaaS (Software as a Service) application are most commonly related to network performance constraints, not local server hardware or virtualization settings. According to CompTIA Network+ (N10-009) troubleshooting objectives, technicians should evaluate bandwidth capacity, throughput, congestion, packet loss, and overall utilization when diagnosing performance issues affecting cloud-based applications.
Since SaaS applications are hosted externally by a service provider, the organization typically does not control the underlying server hardware or virtual machine configurations (Options A and D). Therefore, adjusting internal server specifications would not resolve user-side latency.
Option B, data-at-rest encryption, applies to stored data security and does not impact real-time application responsiveness.
High network utilization, insufficient bandwidth, QoS misconfiguration, or WAN congestion can significantly increase latency. Technicians should review network monitoring tools, check interface statistics, analyze traffic patterns, and verify Quality of Service (QoS) policies to ensure SaaS traffic is prioritized appropriately.
Thus, optimizing bandwidth and reducing network congestion is the most appropriate corrective action.

NEW QUESTION: 75
Which of the following can also provide a security feature when implemented?
A. NAT
B. BGP
C. FHRP
D. EIGRP

Answer: A (LEAVE A REPLY)
NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

NEW QUESTION: 76
A technician is planning an equipement installation into a rack in a data center that practices hot aisle/cold aise ventilation. Which of the following directions should the equipement exhaust face when installed in the rack?
A. Sides
B. Top
C. Front
D. Rear
Answer: (SHOW ANSWER)
In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.
* Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.
* Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses data center design principles, including hot aisle/cold aisle configurations.
* Cisco Data Center Design Guide: Provides best practices for data center layout and equipment installation.
* Network+ Certification All-in-One Exam Guide: Covers data center environmental controls and ventilation strategies.

NEW QUESTION: 77
A network administrator needs to ensure all network ports use a security method that only permits authenticated devices. The solution must meet the following requirements:

* Reduced chance of spoofing
* Centrally managed solution
* Auditable logs

Which of the following technologies provides this functionality?

A. MAC filtering
B. Port security
C. ACLs
D. 802.1X

Answer: (SHOW ANSWER)

802.1X provides port-based network access control that requires authentication before a switch port grants full network access. It uses a supplicant (client), an authenticator (switch/AP), and an authentication server (commonly RADIUS) to validate credentials or certificates. This directly supports the requirements: it reduces spoofing compared with MAC-based controls because authentication can be identity- and certificate- based rather than relying on easily forged MAC addresses; it is centrally managed through AAA infrastructure and policy (users/devices/groups); and it produces auditable logs via the authentication server and network devices, enabling accountability and investigation. Network+ security objectives emphasize AAA, NAC, and strong access controls for both wired and wireless networks. MAC filtering and basic port security rely largely on MAC addresses and are susceptible to spoofing; they also tend to be harder to manage at scale and provide weaker centralized auditing. ACLs control traffic flows but do not authenticate endpoints at the port level, so they cannot ensure "only authenticated devices" can connect. Therefore, 802.1X is the technology that best meets all stated requirements.

NEW QUESTION: 78

Which of the following types of routes takes precedence when building a routing table for a given subnet?

A. Static
B. BGP
C. OSPF
D. Default

Answer: (SHOW ANSWER)

The correct answer is Static because static routes have a lower administrative distance (AD) than most dynamic routing protocols, giving them higher priority when a router selects routes for the same destination network. According to CompTIA Network+ (N10-009) routing objectives, administrative distance is used to determine the trustworthiness of a route source when multiple routing protocols provide a path to the same subnet. The lower the administrative distance, the more preferred the route.

By default, a static route has an administrative distance of 1, which is lower than OSPF (110) and BGP (20 for eBGP, 200 for iBGP). Because of this, when identical routes to a subnet exist from both static and dynamic sources, the router installs the static route in the routing table.

A default route (0.0.0.0/0) is only used when no more specific route exists and does not take precedence over specific static or dynamic routes.
Therefore, when building the routing table for a given subnet and comparing route sources, static routes take precedence due to their lower administrative distance.

NEW QUESTION: 79
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?
A. Trunk all VLANs on the port.
B. Configure the native VLAN.
C. Tag the traffic to voice VLAN.
D. Disable VLANs.
Answer: (SHOW ANSWER)
* Understanding VoIP and VLANs:
* VoIP (Voice over IP) phones often use VLANs (Virtual Local Area Networks) to separate voice traffic from data traffic for improved performance and security.
* Tagging Traffic to Voice VLAN:
* Voice VLAN Configuration:The port on the switch needs to be configured to tag traffic for the specific voice VLAN. This ensures that voice packets are prioritized and handled correctly.
* VLAN Tagging:VLAN tagging allows the switch to identify and separate voice traffic from other types of traffic on the network, reducing latency and jitter for VoIP communications.
* Comparison with Other Options:
* Trunk all VLANs on the port:Trunking all VLANs is typically used for links between switches, not for individual device ports.
* Configure the native VLAN:The native VLAN is for untagged traffic and does not address the need for separating and prioritizing voice traffic.
* Disable VLANs:Disabling VLANs would mix voice and data traffic, leading to potential performance issues and lack of traffic separation.
* Implementation:
* Configure the switch port connected to the VoIP phone to tag the traffic for the designated voice VLAN, ensuring proper network segmentation and quality of service.
References:
* CompTIA Network+ study materials on VLAN configuration and VoIP implementation.

NEW QUESTION: 80

A network engineer is deploying switches at a new remote office. The switches have been preconfigured with hostnames and STP priority values. Based on the following table:

Switch Name	Priority
core-sw01	24576
access-sw01	28672
distribution-sw01	32768
access-sw02	36864

Which of the following switches will become the root bridge?

A. core-sw01

B. access-sw01

C. distribution-sw01

D. access-sw02

Answer: (SHOW ANSWER)

The switch with the lowest STP priority becomes the root bridge.In the given table, core-sw01 has the lowest priority value of 24576. Therefore, it will be elected as the root bridge in the Spanning Tree Protocol topology.

Reference:Section 2.2 - Switching Technologies and Features - "Spanning Tree Protocol (STP)"

NEW QUESTION: 81

A technician needs to quickly set up a network with five wireless devices. Which of the following network types should the technician configure to accomplish this task?

A. Ad hoc

B. Spine and leaf

C. Point to point

D. Mesh

Answer: (SHOW ANSWER)

The correct answer is Ad hoc because it allows wireless devices to communicate directly with one another without requiring a centralized access point or additional infrastructure. According to CompTIA Network+ (N10-009) objectives under wireless networking concepts, an ad hoc network (also known as an Independent Basic Service Set, or IBSS) enables peer-to-peer wireless communication.

This type of network is ideal for temporary or quick setups where only a small number of devices need to connect. In an ad hoc configuration, each device connects directly to others, making it simple and fast to deploy without requiring switches, routers, or wireless access points.

Spine and leaf (Option B) is a data center architecture designed for high scalability and redundancy, not small wireless setups. Point-to-point (Option C) refers to a direct connection between two devices only, which would not support five devices efficiently. Mesh (Option D)

allows multiple nodes to interconnect and provide redundancy, but it is more complex and typically requires compatible infrastructure devices.
Therefore, for a quick setup with five wireless devices, an ad hoc network is the most appropriate choice.

NEW QUESTION: 82
Which of the following VPN types provides secure remote access to the network resources through a web portal?
A. Proxy
B. Clientless
C. Site-to-site
D. Direct connect
Answer: (SHOW ANSWER)
Clientless VPNs allow users to access network resources through a secure web portal using a browser, with no VPN software needed. This is ideal for occasional access to internal resources via HTTPS.
A: Proxy is a gateway for accessing web content, not a VPN.
C: Site-to-site VPN connects entire networks, not individual users.
D: Direct Connect usually refers to dedicated cloud connections, not VPNs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

NEW QUESTION: 83
Which of the following uses the longest prefix match to determine an exit interface?
A. ARP table
B. MAC address table
C. Routing table
D. Netstat table
Answer: (SHOW ANSWER)
The longest prefix match is a routing concept used to find the most specific route to a destination IP address.
The routing table performs this calculation to determine the exit interface for a packet, ensuring the most accurate delivery. The document explains:
"Routers use the longest prefix match when searching the routing table to determine the best path for an IP packet. This ensures that the most specific (and thus optimal) route is chosen, based on the destination IP address."

NEW QUESTION: 84

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare.
Which of the following tools wold help identify which ports are open on the remote file server?
A. Dig
B. Nmap
C. Tracert
D. nslookup
Answer: B (LEAVE A REPLY)
Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
* Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
* Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
* Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.
* Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.
* Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

NEW QUESTION: 85
A network technician is installing a new switch that does not support STP at the access layer of a network.
The technician wants a redundant connection to the distribution switch. Which of the following should the technician use?
A. Link aggregation
B. Subinterfaces
C. Switch virtual interfaces
D. Half-duplex connections
Answer: (SHOW ANSWER)
Link aggregation(also known as port channeling or EtherChannel) allows multiple physical connections to act as one logical connection. This avoids loops that would typically be prevented by STP and provides redundancy and increased bandwidth. It's ideal when STP is not available or desirable.
Reference:Section 2.2 - Switching Technologies and Features - "Link Aggregation"

NEW QUESTION: 86
A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?
A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n
Answer: (SHOW ANSWER)
802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.
802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as
802.11ax.
802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.
802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.
Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.
Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

NEW QUESTION: 87
An ISP provided a company with a pre-configured modem and five public static IP addresses. Which of the following does the company's firewall require to access the internet? (Select TWO).
A. NTP server
B. Default gateway
C. The modem's IP address
D. One static IP address
E. DNS servers
F. DHCP server
Answer: (SHOW ANSWER)
To access the internet using static IPs, the firewall (or router) must be configured correctly:
B). Default gateway: This is essential because it tells the firewall where to send outbound traffic destined for outside the local network.

D). One static IP address: The firewall must be assigned one of the static IPs to communicate over the public internet.
The other options are not essential for basic internet connectivity in this context:
A). NTP server: Useful for time synchronization but not required for internet access.
C). The modem's IP address: Irrelevant unless doing modem-level configuration.
E). DNS servers: Important for name resolution but not for basic layer 3 connectivity.
F). DHCP server: Not used when static IPs are assigned.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.2 - Compare and contrast addressing technologies.

NEW QUESTION: 88
During a VoIP call, a user notices inconsistent audio and logs an incident ticket. A network administrator notices inconsistent delays in arrival of the RTP packets. Which of the following troubleshooting tools should the network administrator use to determine the issue?
A. Toner and probe
B. Protocol analyzer
C. Cable tester
D. Spectrum reader
Answer: (SHOW ANSWER)
Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.
A). Toner and probe locates cable runs, not packet analysis.
C). Cable tester checks wiring faults, not packet timing.
D). Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Protocol analyzers, VoIP troubleshooting, jitter analysis.

NEW QUESTION: 89
Which of the following can be used when a server at a remote site is physically unreachable?
A. OOB management
B. Crash cart
C. Jump box
D. Console
Answer: (SHOW ANSWER)
Out-of-band (OOB) managementallows administrators to manage devices remotely even if the primary network is down. This is especially useful when physical access to the server is not possible. OOB management often uses a separate management interface, ensuring access regardless of the server's operational state.
Reference:Section 3.5 - Network Access and Management Methods - "OOB Management"

NEW QUESTION: 90

Which of the following ports is a secure protocol?

A. 20

B. 23

C. 443

D. 445

Answer: (SHOW ANSWER)

Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL

/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:

"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

NEW QUESTION: 91

You are tasked with verifying the following requirements are met in order to ensure network security.

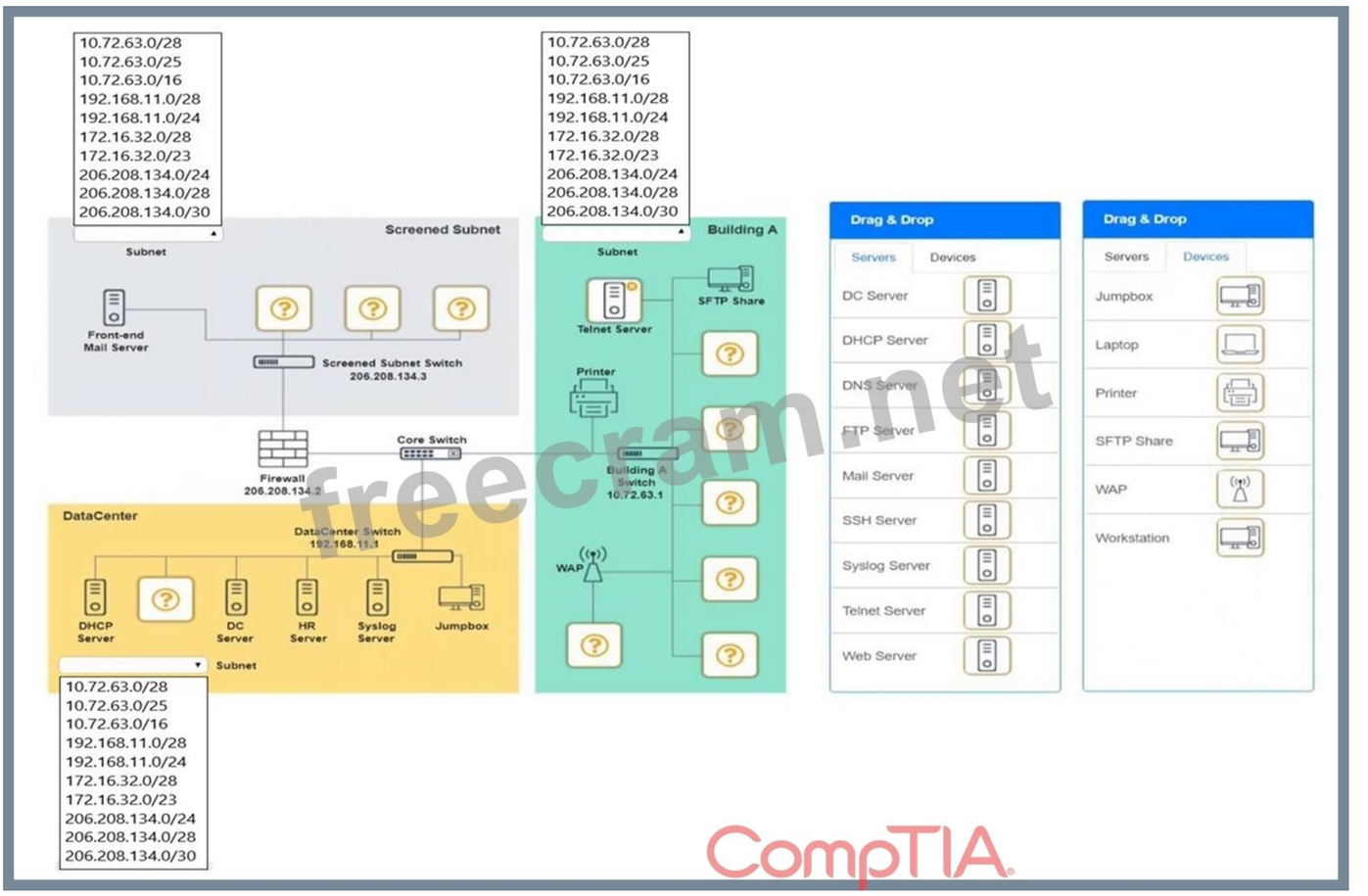
Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

See explanation below.

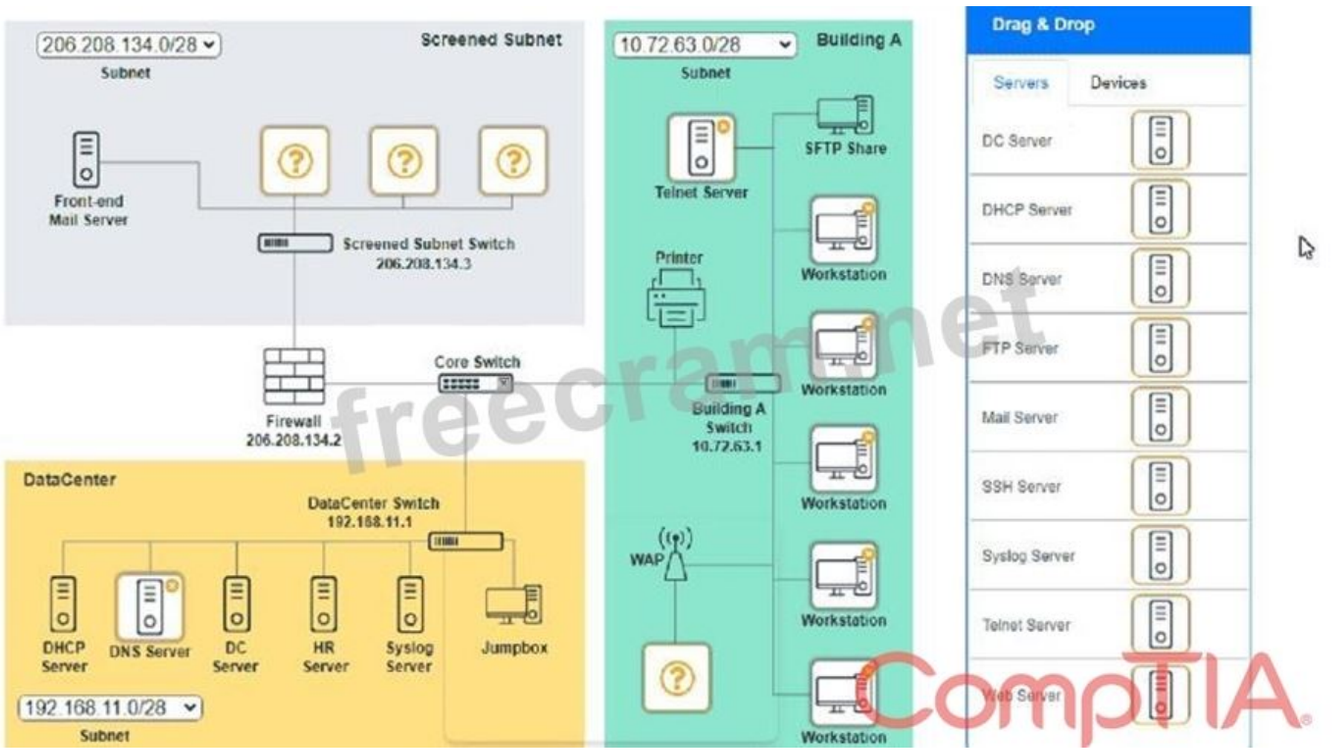
Explanation:

Screened Subnet devices - Web server, FTP server

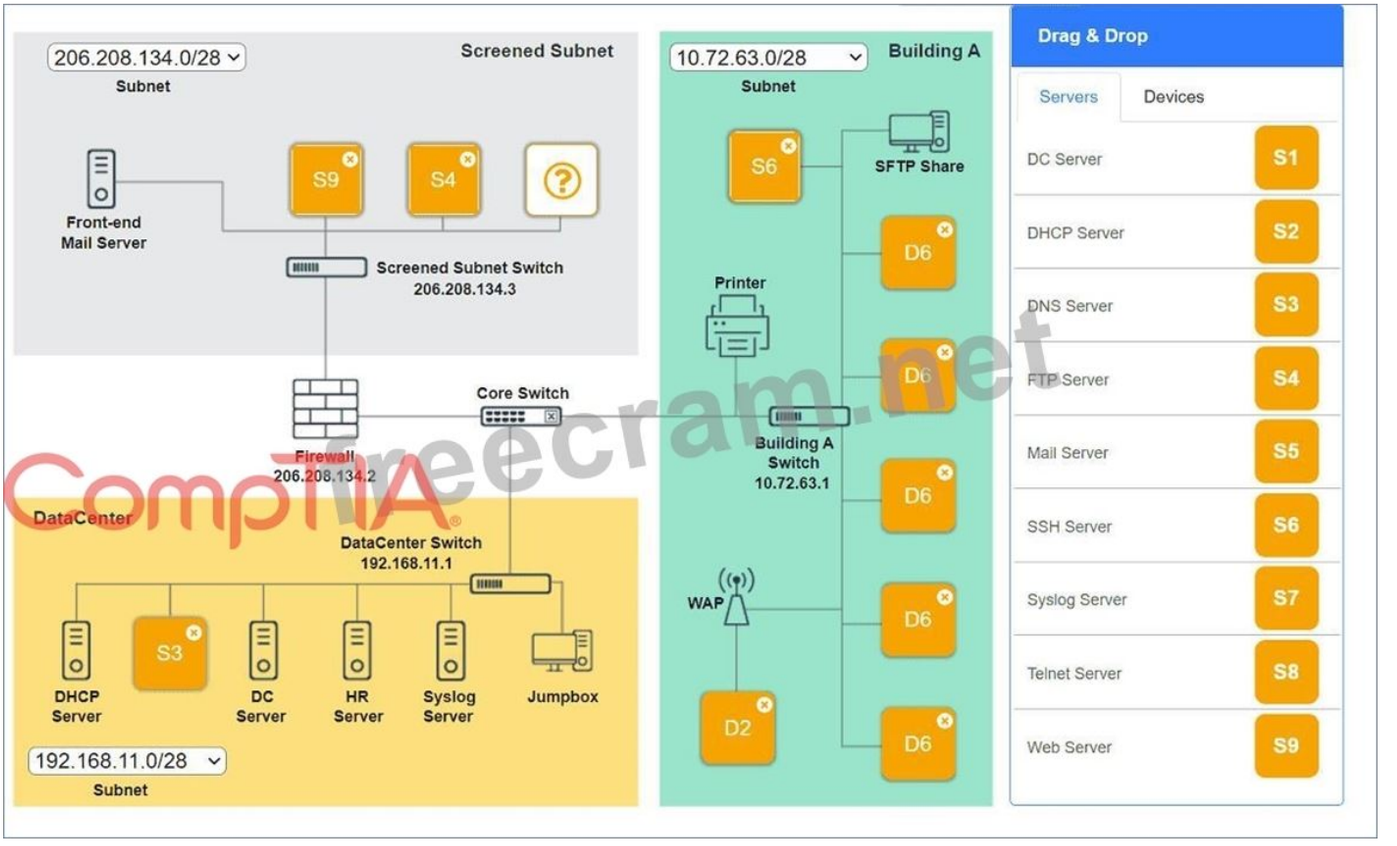
Building A devices - SSH server top left, workstations on all 5 on the right, laptop on bottom left

DataCenter devices - DNS server.

A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.



A screenshot of a computer AI-generated content may be incorrect.

NEW QUESTION: 92
A network administrator wants to update a geofencing policy to limit remote access to the corporate network based on country location. Which of the following would the administrator most likely leverage?
A. MAC filtering
B. Administrative distance
C. Bluetooth beacon signals
D. IP address blocks
Answer: (SHOW ANSWER)
The correct answer is IP address blocks because geofencing policies typically rely on public IP address ranges associated with specific geographic regions or countries. According to CompTIA Network+ (N10-009) security objectives, geofencing is a security control used to restrict or allow traffic based on geographic location. This is commonly implemented on firewalls, VPN concentrators, or security gateways by referencing databases that map IP address blocks to countries or regions.
When configuring geofencing, administrators create access control rules that permit or deny traffic from specific country-based IP ranges. This method is effective for limiting remote access to approved geographic locations and reducing exposure to international threat sources.
MAC filtering (Option A) is used within local networks and does not function over the internet for geographic control. Administrative distance (Option B) is a routing concept that determines route preference and has no relation to access control policies. Bluetooth beacon signals (Option C) are used for proximity-based services and indoor positioning, not for country-level remote access restrictions.
Therefore, leveraging IP address blocks is the correct approach for implementing geofencing controls.

NEW QUESTION: 93
A company's VoIP phone connection is cutting in and out. A senior network engineer is recommending the implementation of a voice VLAN. Which of the following should be configured?
A. 802.1Q tagging
B. Jumbo frames
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link.

This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.
B). Jumbo frames improve throughput for large data transfers, not voice.
C). Native VLAN is the untagged VLAN, not specifically for voice.
D). Link aggregation bundles links for bandwidth/redundancy, not QoS.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - VLANs, voice VLANs, 802.1Q tagging, QoS.

NEW QUESTION: 94
A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?
A. Trusted zones
B. URL filtering
C. ACLs
D. Screened subnet
Answer: (SHOW ANSWER)
Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

NEW QUESTION: 95
An administrator wants to find the top destination for traffic across the infrastructure on a specific day. Which of the following should the administrator use?
A. SNMP
B. Packet capture
C. NetFlow
D. traceroute
Answer: (SHOW ANSWER)
NetFlow (and similar flow technologies like IPFIX/sFlow in concept) is used to collect traffic-flow metadata such as source/destination IPs, ports, protocols, interfaces, and byte/packet counts over time. In Network+ (N10-009) operations and monitoring objectives, flow data is ideal for identifying top talkers and top destinations across the network on a given day because it provides summarized, queryable information at scale without capturing every packet payload. An administrator can review reports to determine which destination IPs/hosts consumed the most bandwidth, which applications were most active, and what time ranges saw spikes-perfect for historical analysis.
SNMP is great for polling device counters (interface utilization, errors, CPU) but it does not natively tell you the "top destination" by conversation/flow without additional flow awareness.
Packet capture can reveal exact conversations and payloads, but it is heavy, localized, and not

efficient for infrastructure-wide daily top- destination reporting. traceroute maps the path to a destination and helps isolate routing/path issues; it does not provide usage statistics. Therefore, NetFlow is the best fit.

NEW QUESTION: 96
A company recently implemented a videoconferencing system that utilizes large amounts of bandwidth. Users start reporting slow internet speeds and an overall decrease in network performance. Which of the following are most likely the causes of the network performance issues? (Select two)
A. DNS misconfiguration
B. Inadequate network security
C. Malware or a virus
D. Outdated software
E. Incorrect QoS settings
F. Network congestion
Answer: (SHOW ANSWER)
When high-bandwidth services like videoconferencing are introduced, two primary factors may degrade performance:
Incorrect QoS Settings (E):QoS (Quality of Service) is used to prioritize traffic. If not configured correctly, critical services like video may not get the necessary bandwidth and prioritization.
Network Congestion (F):Video services consume large amounts of data. If the network doesn't have sufficient bandwidth or is not segmented properly, congestion will slow down all services.
DNS misconfiguration (A) would affect name resolution, not bandwidth.
Malware (C) could degrade performance, but is not tied to the described scenario.
Outdated software (D) may affect performance in some cases, but not directly linked to network congestion in this case.
Inadequate network security (B) isn't likely to cause general slowness related to video traffic.
So, the most likely culprits are E. Incorrect QoS settings and F. Network congestion.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.5: "Explain common performance concepts and issues."

NEW QUESTION: 97
A network administrator is trying to troubleshoot an issue with a newly installed switch that is not connecting to the network. The administrator logs on to the switch and observes collisions on the interface. Which of the following is most likely the issue?
A. Wrong speed
B. Jumbo frames enabled
C. Incorrect VLAN
D. Duplex mismatch
Answer: (SHOW ANSWER)

The most likely issue is a duplex mismatch, which is a well-documented cause of collisions and poor network performance, as outlined in the CompTIA Network+ N10-009 troubleshooting objectives. A duplex mismatch occurs when one end of a network link is configured for full duplex while the other end is operating in half duplex. In half-duplex mode, devices must take turns transmitting and receiving data, which inherently allows for collisions. When paired with a full-duplex device-which expects simultaneous send and receive- collisions and retransmissions occur frequently.
The presence of collisions on a switch interface is a key diagnostic clue. Modern Ethernet switches operating correctly in full duplex should not experience collisions at all. When collisions are observed, it almost always points to a duplex configuration issue, often caused by manual speed/duplex settings on one device and auto- negotiation on the other.
A wrong speed setting may prevent link establishment entirely or cause errors, but it does not typically result in collisions. Jumbo frames can cause packet drops or fragmentation issues, not collisions. An incorrect VLAN configuration affects logical segmentation and connectivity but operates at Layer 2 and does not generate collisions.
CompTIA Network+ emphasizes duplex mismatch as a classic and frequently tested troubleshooting scenario.
Correcting it-usually by enabling auto-negotiation on both ends-restores normal, collision-free communication.

NEW QUESTION: 98
A research facility is expecting to see an exponential increase in global network traffic in the near future. The offices are equipped with 2.5Gbps fiber connections from the ISP, but the facility is currently only utilizing
1Gbps connections. Which of the following would need to be configured in order to use the ISP's connection speed?
A. 802.1Q tagging
B. Network address translation
C. Port duplex
D. Link aggregation
Answer: (SHOW ANSWER)
* Understanding Link Aggregation:
* Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.
* Usage in High-Bandwidth Scenarios:
* Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5 Gbps bandwidth provided by the ISP.
* Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.
* Comparison with Other Options:

* 802.1Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization.
* Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.
* Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of bandwidth.
* Implementation:
* Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.
References:
* CompTIA Network+ study materials on network configuration and link aggregation.

NEW QUESTION: 99
A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?
A. Clientless
B. Client-to-site
C. Full tunnel
D. Site-to-site
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

NEW QUESTION: 100
A company is concerned that the public can use network wall jacks in publicly available conference rooms to access company servers. Which of the following is the best way to mitigate the vulnerability?

A. Create a trusted zone.
B. Disable unused services.
C. Use MAC filtering.
D. Implement 802.1X.
Answer: (SHOW ANSWER)
The best mitigation is implementing 802.1X, which provides port-based Network Access Control (NAC).
With 802.1X enabled on access switch ports, a device plugged into a wall jack cannot gain normal network access until it successfully authenticates using credentials/certificates via an authentication server (commonly RADIUS). This directly addresses the threat of unauthorized users plugging into publicly accessible conference room jacks, because the switch keeps the port in an unauthenticated state (or places it into a restricted/guest VLAN) until authentication succeeds. This aligns with Network+ security objectives that emphasize controlling access at the edge, enforcing authentication, and reducing the risk of rogue or unmanaged devices on internal networks.

MAC filtering is weaker because MAC addresses can be spoofed and managing allow-lists at scale is error- prone. Creating a trusted zone is vague and does not prevent initial port access; segmentation helps limit blast radius but doesn't enforce authentication at the jack. Disabling unused services is a general hardening practice, but it does not stop someone from connecting physically to an active switch port and attempting access. 802.1X is purpose-built for this exact scenario.

NEW QUESTION: 101
A network administrator installed a new VLAN to the network after a company added an additional floor to the office. Users are unable to obtain an IP address on the new VLAN, but ports on existing VLANs are working properly. Which of the following configurations should the administrator update?
A. Scope size
B. Address reservations
C. Lease time
D. IP helper
Answer: (SHOW ANSWER)
When a new VLAN is created, it typically exists on a different subnet. If DHCP servers are on a different VLAN, the network needs an IP helper address to forward DHCP requests correctly. Without it, clients in the new VLAN won't receive an IP address.
Breakdown of Options:
A: Scope size - Increasing the DHCP scope would not resolve the issue if requests aren't reaching the server.
B: Address reservations - Reservations only assign specific addresses to devices; they do not fix DHCP communication issues.
C: Lease time - Changing the lease time does not impact DHCP functionality across VLANs.
D: IP helper - Correct answer. This forwards DHCP requests across VLANs to the DHCP server.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain IP addressing technologies and subnetting.
RFC 1542: BOOTP (Bootstrap Protocol) relay agents

NEW QUESTION: 102
A Chief Information Officer wants a DR solution that runs only after a failure of the primary site and can be brought online quickly once recent backups are imported. Which of the following DR site solutions meets these requirements?
A. Cold
B. Warm
C. Active
D. Hot
Answer: B (LEAVE A REPLY)

Comprehensive and Detailed Explanation (aligned to N10-009):
A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.
A). Cold site has only power and space, requiring full setup, which takes too long.
C). Active (active-active) runs simultaneously with the primary site, not only during failure.
D). Hot site is fully operational at all times and can take over immediately, but it's more expensive.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Disaster recovery sites (cold, warm, hot, active).

NEW QUESTION: 103
An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?
A. TXT
B. AAAA
C. CNAME
D. MX
Answer: (SHOW ANSWER)
A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

NEW QUESTION: 104
Which of the following are the best device-hardening techniques for network security? (Select two).
A. Disabling unused ports
B. Performing regular scanning of unauthorized devices
C. Monitoring system logs for irregularities
D. Enabling logical security such as SSO
E. Changing default passwords
F. Ensuring least privilege concepts are in place
Answer: (SHOW ANSWER)
Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 105

A network administrator wants to configure a backup route in case the primary route fails. A dynamic routing protocol is not installed on the router. Which of the following routing features should the administrator choose to accomplish this task?

A. Neighbor adjacency

B. Link state flooding

C. Administrative distance

D. Hop count

Answer: (SHOW ANSWER)

Introduction to Administrative Distance

Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.

Static Routes and Backup Routes

When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.

Configuring Static Routes with Administrative Distance

The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.

Example Configuration:

plaintext

Copy code

ip route 192.168.1.0 255.255.255.0 10.0.0.1 1

ip route 192.168.1.0 255.255.255.0 10.0.0.2 10

In the above example, 192.168.1.0/24 is the destination network.

10.0.0.1 is the next-hop IP address for the primary route with an AD of 1.

10.0.0.2 is the next-hop IP address for the backup route with an AD of 10.

Verification:

After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.

References:

CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page #Ref9 Basic Configuration Commands).

NEW QUESTION: 106

A company recently experienced outages of one of its critical, customer-facing applications. The root cause was an overutilized network router, but the Chief Technology Officer is concerned that the support staff was unaware of the issue until notified by customers. Which of the following is the best way to address this issue in the future?

A. Packet capture
B. SNMP
C. Syslog collector
D. SIEM
Answer: (SHOW ANSWER)
The best answer is SNMP (Simple Network Management Protocol). SNMP enables monitoring of network devices (routers, switches, firewalls, servers) and provides performance data such as CPU usage, bandwidth utilization, and interface status. In this scenario, if SNMP monitoring had been in place, administrators would have received alerts that the router was overutilized before customers noticed outages.
A). Packet capture (e.g., Wireshark) is useful for deep troubleshooting but is reactive, not proactive, and not scalable for continuous monitoring.
C). Syslog collects log messages but generally does not provide proactive resource utilization metrics. It is complementary but not the best fit for this problem.
D). SIEM aggregates logs and security events for analysis, but the primary requirement here is performance and availability monitoring.
By implementing SNMP monitoring (and potentially integrating it with a network monitoring tool such as Nagios, PRTG, or SolarWinds), the organization can track utilization trends, set thresholds, and automatically generate alerts, thereby preventing downtime from going unnoticed.
References (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP monitoring, proactive network performance management.

NEW QUESTION: 107
A network engineer needs to deploy an access point at a remote office so that it will not communicate back to the wireless LAN controller. Which of the following deployment methods must the engineer use to accomplish this task?
A. Lightweight
B. Autonomous
C. Mesh
D. Ad hoc
Answer: (SHOW ANSWER)

Autonomous access points operate independently without needing to communicate with a central wireless LAN controller. This is ideal for remote deployments.
From Andrew Ramdayal's guide:
"Autonomous access points are stand-alone devices that manage their own configurations and operations.
They do not require a WLC and are ideal for small or remote office deployments."

NEW QUESTION: 108
A technician needs to identify a computer on the network that is reportedly downloading unauthorized content. Which of the following should the technician use?
A. Anomaly alerts
B. Port mirroring
C. Performance monitoring
D. Packet capture
Answer: (SHOW ANSWER)
Packet Capture: This method captures and inspects network traffic to identify unauthorized downloads or malicious behavior. It provides detailed insight into the data being transmitted, making it the best tool for this scenario.
Anomaly alerts (A): Alerts may indicate unusual activity but do not provide detailed traffic analysis.
Port mirroring (B): Port mirroring can redirect traffic for analysis but requires a packet capture tool for deeper inspection.
Performance monitoring (C): Focuses on system performance metrics, not detailed traffic content.
Reference: CompTIA Network+ Official Study Guide, Domain 4.3 (Network Monitoring Tools).

NEW QUESTION: 109
A network technician is requesting a fiber patch cord with a connector that is round and twists to install.
Which of the following is the proper name of this connector type?
A. ST
B. BNC
C. SC
D. LC
Answer: (SHOW ANSWER)
The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.
B). BNC is a coaxial connector.
C). SC (Subscriber Connector) is a square push-pull fiber connector.
D). LC (Lucent Connector) is a small form-factor fiber connector.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Fiber connectors (ST, SC, LC).

NEW QUESTION: 110

An organization requires the ability to send encrypted email messages to a partner from an email server that is hosted on premises. The organization prefers to use the standard default ports when creating firewall rules.

Which of the following ports should be open to satisfy the requirements?

A. 110

B. 143

C. 587

D. 636

Answer: (SHOW ANSWER)

Port 587 is the standard default port for sending email (SMTP) with TLS encryption, which is used to secure email transmissions between mail servers or between clients and mail servers. Allowing traffic over port 587 enables secure email sending while maintaining standard protocol usage. (Reference: CompTIA Network+ Study Guide, Chapter on Ports and Protocols)

NEW QUESTION: 111

A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?

A. Change the email client configuration to match the MX record.

B. Reduce the TTL record prior to the MX record change.

C. Perform a DNS zone transfer prior to the MX record change.

D. Update the NS record to reflect the IP address change.

Answer: (SHOW ANSWER)

Understanding TTL (Time to Live):

TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients.

A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:

When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:

To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making thechanges. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:

After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.
Comparison with Other Options:
Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.
Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.
Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.
References:
CompTIA Network+ study materials and DNS best practices.

NEW QUESTION: 112
Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other non-video applications on the network. Which of the following symptoms describes the users' reported issues?
A. Latency
B. Packet loss
C. Bottlenecking
D. Jitter
Answer: (SHOW ANSWER)
Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:
Users report connectivity issues and lag during video meetings.
The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.
Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.
Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.
Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.
Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Connectivity Issues

NEW QUESTION: 113

A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?

A. Packet capture

B. Data usage reports

C. SNMP traps

D. Configuration monitoring

Answer: (SHOW ANSWER)

To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.

Breakdown of Options:

A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.

B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.

C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.

D). Configuration monitoring - This tracks configuration changes rather than availability.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.

RFC 1157: Simple Network Management Protocol (SNMP)

NEW QUESTION: 114

A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?

A. Update the firmware.

B. Replace the system board.

C. Patch the OS.

D. Isolate the system.

Answer: (SHOW ANSWER)

Understanding the Vulnerability:

Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.

Firmware Update:

Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.

Procedure: Download the latest firmware from the vendor's website, follow the manufacturer's instructions to apply the update, and verify that the update resolves the vulnerability.

Comparison with Other Options:

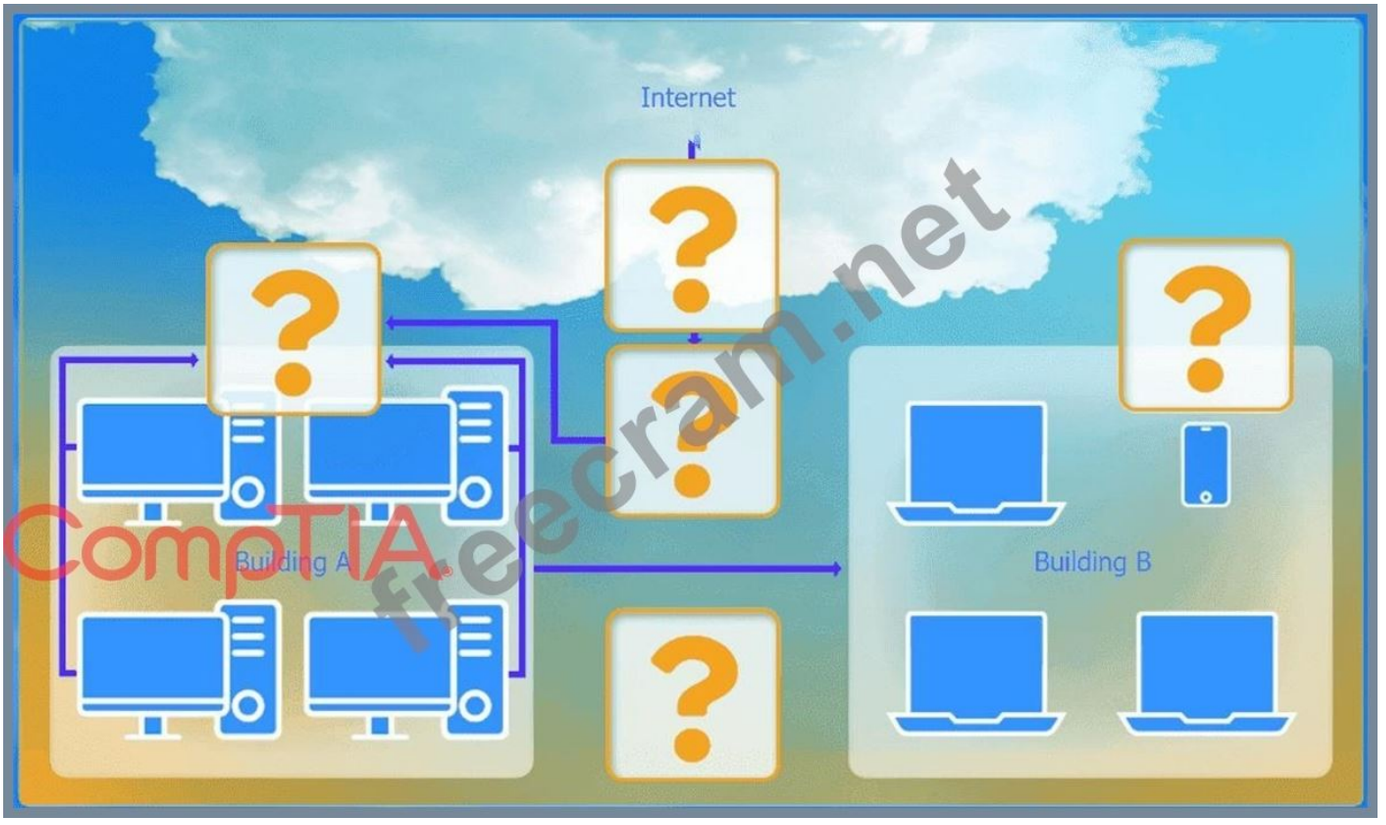
Replace the System Board: This is a costly and often unnecessary step if the issue can be resolved with a firmware update.
Patch the OS: Patching the OS is relevant for devices with a full operating system but not directly applicable to addressing a CPU vulnerability on a router.
Isolate the System: Temporarily isolating the system can mitigate immediate risk but does not resolve the underlying vulnerability.
Best Practice:
Regularly check for and apply firmware updates to ensure that network devices are protected against known vulnerabilities.
References:
CompTIA Network+ study materials on network security and device management.

NEW QUESTION: 115
A network technician is working on a PC with a faulty NIC. The host is connected to a switch with secured ports. After testing the connection cables and using a known-good NIC, the host is still unable to connect to the network. Which of the following is causing the connection issue?
A. MAC address of the new card
B. BPDU guard settings
C. Link aggregation settings
D. PoE power budget
Answer: (SHOW ANSWER)
If a switch has port security enabled (such as sticky MAC or a configured allowed MAC), the port will only allow the original NIC's MAC address. When a new NIC with a different MAC address is installed, the port rejects traffic, preventing network connectivity.
B). BPDU guard protects against rogue switches, not end hosts.
C). Link aggregation applies when bundling multiple uplinks, not a single PC connection.
D). PoE budget applies to powered devices like APs, not PCs.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port security, MAC address filtering, switch security features.

NEW QUESTION: 116
Which of the following is most commonly associated with many systems sharing one IP address in the public IP-addressing space?
A. PAT
B. NAT
C. VIP
D. NAT64
Answer: A (LEAVE A REPLY)
Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used

in environments where many systems need internet access but there are limited public IP addresses.

NEW QUESTION: 117
A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:
. Devices in both buildings should be
able to access the Internet.
. Security insists that all Internet traffic
be inspected before entering the
network.
. Desktops should not see traffic
destined for other devices.
INSTRUCTIONS
Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.
Not all devices will be used, but all locations should be filled.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Wireless range extender settings

Basic Configuration

Access Point Name	WAP extender
Gateway	192.168.0.1
SSID	CORP
SSID Broadcast	Yes / No

Wireless

Mode	
Channel	

Wired

Speed	Auto / 100 / 1000
Duplex	Auto / Half / Full

Security Configuration

Security Settings	None / WEP / WPA / WPA2 / WPA2 - Enterprise
Key or Passphrase	N@En71$90*Ha

Reset to Default | Save | Close

Answer:

See the step by step complete solution below.

Explanation:

Devices in both buildings should be able to access the Internet.

Security insists that all Internet traffic be inspected before entering the network.

Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:

Building A:

Switch: Correctly placed to connect all desktops.

Firewall: Correctly placed to inspect all incoming and outgoing traffic.

Building B:

Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.

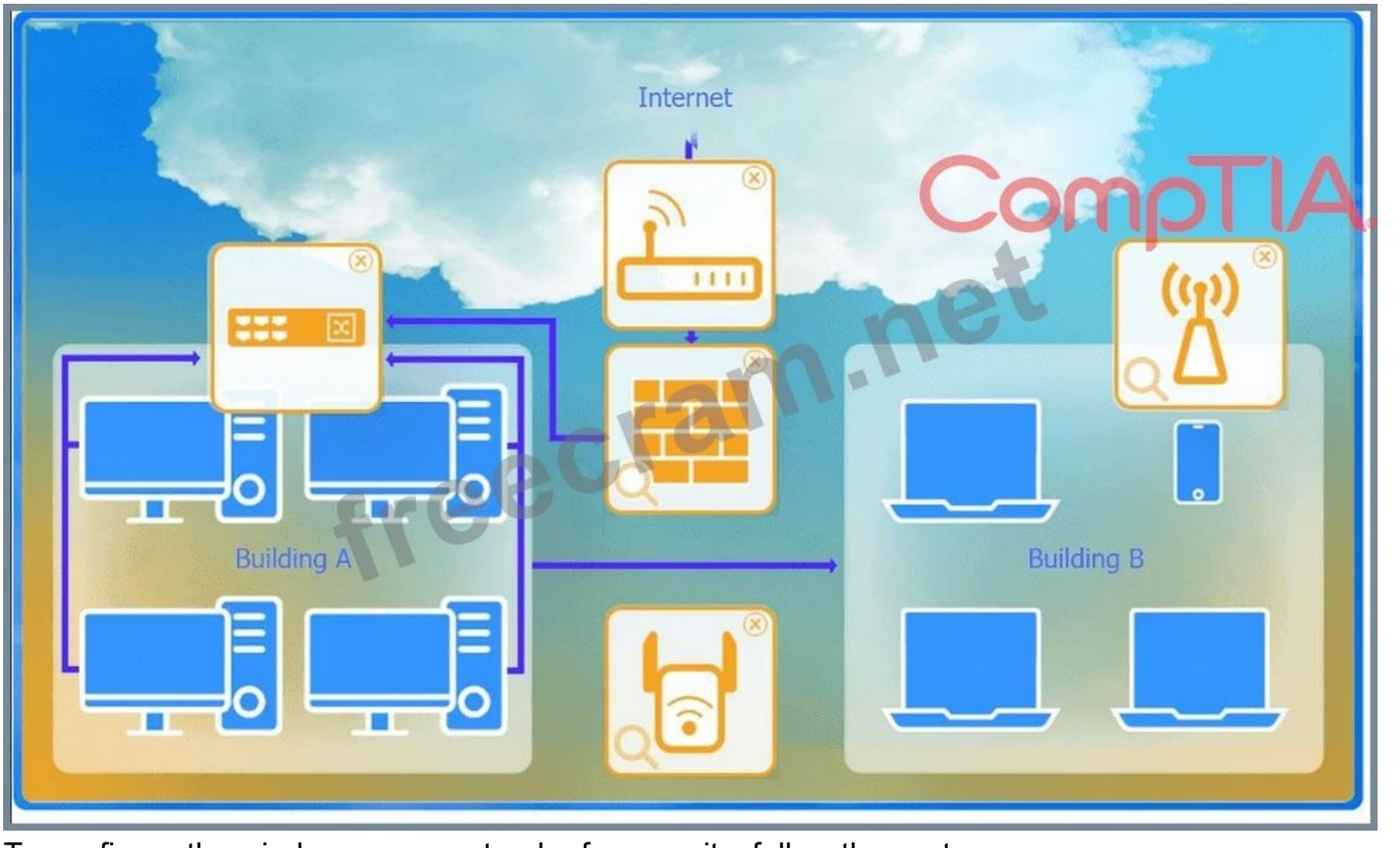
Between Buildings:

Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.

Connection to the Internet:

Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.
Corrected Setup:
Top-left (Building A): Switch
Bottom-left (Building A): Firewall (inspect traffic before it enters the network) Top-middle (Internet connection): Router Bottom-middle (between buildings): Wireless Range Extender Top-right (Building B): Wireless Access Point (WAP) In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.
Configuration for Wireless Range Extender:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.



To configure the wireless range extender for security, follow these steps:
SSID (Service Set Identifier):
Ensure the SSID is set to " CORP " as shown in the exhibit.

Security Settings:
WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.
Key or Passphrase:
If you select WPA2, enter a strong passphrase in the " Key or Passphrase " field.
If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.
Wireless Mode and Channel:
Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.
Wired Speed and Duplex:
Set the speed to " Auto " unless you have specific requirements for 100 or 1000 Mbps.
Set the duplex to " Auto " unless you need to specify half or full duplex based on your network equipment.
Save Configuration:
After making the necessary changes, click the " Save " button to apply the settings.
Here is how the configuration should look after adjustments:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.
Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:
DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.
HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.
Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.
HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.
HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.
Suggested Additional Settings:

Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.
Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.
Firewall Configuration Adjustments:
Correct the Network Typo:
Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.
Permit General Outbound Traffic:
Rule Name: General Outbound
Source: 192.168.0.1/24
Destination: ANY
Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:
Rule Name
Source
Destination
Service
Action
DNS Rule
192.168.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
192.168.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
192.168.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
192.168.0.1/24

HTTPS
DENY
HTTP Inbound
ANY
192.168.0.1/24
HTTP
DENY
General Outbound
192.168.0.1/24
ANY
ANY
PERMIT
Block All
ANY
ANY
ANY
DENY
These settings ensure that:
Internal devices can access DNS and HTTPS services externally.
Management access via SSH is permitted.
Inbound HTTP and HTTPS traffic is denied unless otherwise specified.
General outbound traffic is allowed.
All other traffic is blocked by default, ensuring a secure environment.
Make sure to save the settings after making these adjustments.

NEW QUESTION: 118
Before using a guest network, an administrator requires users to accept the terms of use Which of the following is the best way to accomplish this goal?
A. Pre-shared key
B. Autonomous access point
C. Captive portal
D. WPA2 encryption
Answer: (SHOW ANSWER)
A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 119

An organization has four departments that each need access to different resources that do not overlap. Which of the following should a technician configure in order to implement and assign an ACL?

A. VLAN

B. DHCP

C. VPN

D. STP

Answer: (SHOW ANSWER)

VLANs (Virtual Local Area Networks) segment network traffic by department, allowing ACLs (Access Control Lists) to be applied based on VLAN membership, improving security and resource isolation.

Breakdown of Options:

A). VLAN - Correct answer. VLANs enable logical network segmentation, allowing ACLs per department.

B). DHCP - Assigns IP addresses but does not control access.

C). VPN - Provides remote access, not segmentation within a network.

D). STP - Prevents switching loops, not related to ACL implementation.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain VLANs and network segmentation.

IEEE 802.1Q: VLAN tagging standard

NEW QUESTION: 120

A company discovers on video surveillance recordings that an unauthorized person installed a rogue access point in its secure facility. Which of the following allowed the unauthorized person to do this?

A. Evil twin

B. Honeytrap

C. Wardriving

D. Tailgating

Answer: (SHOW ANSWER)

Tailgatingis a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.

* A. Evil twinis a wireless attack where an attacker sets up a fake AP.

* B. Honeytrapis used to attract attackers for analysis.

* C. Wardrivinginvolves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

NEW QUESTION: 121
A network engineer needs to order cabling to connect two buildings within the same city. Which of the following media types should the network engineer use?
A. Coaxial
B. Twinaxial
C. Single-mode fiber
D. Cat 5
Answer: (SHOW ANSWER)
Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth - making it the ideal choice for connecting buildings across a city.
Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).
Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.
For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

NEW QUESTION: 122
After extremely high temperatures cause a power outage, the servers automatically shut down, even though the UPSs for the servers still have hours of battery life. Which of the following should a technician recommend?
A. Include backup power for air-conditioning units
B. Configure door locks to automatically lock during power outages
C. Increase UPS battery size
D. Add an IoT-enabled thermostat
Answer: (SHOW ANSWER)
Servers shut down due to overheating, not loss of electrical power. Although UPS units had battery life, without cooling systems (HVAC/air conditioning) running on backup power, server rooms overheated.
Backup power for air-conditioning is essential in data center design.

B). Door locks are unrelated to server shutdown.
C). Increasing UPS capacity won't help cooling.
D). IoT thermostats may monitor temperature but won't prevent overheating.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Environmental controls, power redundancy, HVAC systems.

NEW QUESTION: 123
Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?
A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.
Answer: (SHOW ANSWER)
* Troubleshooting Methodology:
* Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
* Confirming a Theory:
* Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
* Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
* Comparison with Other Steps:
* Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
* Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
* Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
* Implementation:
* Use similar equipment or software in a test environment to recreate the issue.
* Observe the results to see if they match the original problem, thereby confirming the theory.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

NEW QUESTION: 124
A Chief Executive Officer (CEO) of a company purchases a new phone that will be used while traveling to different countries. The CEO needs to be able to place outgoing calls and receive

incoming calls on the phone using a SIM card. Which of the following cellular technologies does the CEO's phone need?

A. WDMA

B. CDMA

C. GSM

D. SLA

Answer: (SHOW ANSWER)

GSM (Global System for Mobile communications) is the international standard that uses SIM cards to authenticate and connect phones to the cellular network. GSM allows users to place and receive calls while traveling globally, provided they have a SIM card. CDMA, on the other hand, does not use SIM cards in the same way and is primarily used in the United States. (Reference: CompTIA Network+ Study Guide, Chapter on Network Fundamentals)

NEW QUESTION: 125

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address.

Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file

B. Self-signed certificate

C. Nameserver record

D. IP helper ANS

Answer: (SHOW ANSWER)

* Role of the Hosts File:

* The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.

* Common Issues with the Hosts File:

* If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.

* Why Other Options are Less Likely:

* Self-signed certificate:Relates to SSL/TLS and would cause a security warning, not a navigation failure.

* Nameserver record:Affects all users, not just one.

* IP helper:Used to forward DHCP requests and is unrelated to DNS resolution issues.

* Troubleshooting Steps:

* Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hostson Windows or/etc/hostson Unix/Linux).

* Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.

References:

* CompTIA Network+ study materials and system administration documentation.

NEW QUESTION: 126
An investment bank is seeking a DR backup solution. Which of the following provides the most cost-effective backup site?
A. Hot
B. Cold
C. Cluster
D. Warm
Answer: (SHOW ANSWER)
*Cold sites are the most cost-effective disaster recovery (DR) option since they require the least infrastructure investment. They provide space and power but no pre-configured systems.
*Hot sites (A) are fully operational and very expensive.
*Warm sites (D) offer some pre-configured hardware but still require setup, making them more costly than cold sites.
*Clusters (C) are active failover systems, not DR sites.
#Reference: CompTIA Network+ N10-009 Official Documentation - Disaster Recovery & Business Continuity Planning.

NEW QUESTION: 127
Which of the following network devices converts wireless signals to electronic signals?
A. Router
B. Firewall
C. Access point
D. Load balancer
Answer: (SHOW ANSWER)
* Role of an Access Point (AP):
* Wireless to Wired Conversion:An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.
* Functionality:
* Signal Conversion:The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.
* Connectivity:APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.
* Comparison with Other Devices:
* Router:Directs traffic between different networks and may include built-in AP functionality but is not primarily responsible for converting wireless to electronic signals.
* Firewall:Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.

* Load Balancer:Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.
* Deployment:
* APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.
References:
* CompTIA Network+ study materials on wireless networking and access points.

NEW QUESTION: 128
A network administrator is creating a subnet that will include 45 separate hosts on a small private network within a large network architecture. Which of the following options is the most efficient use of network addresses when assigning this network?
A. 10.0.50.128/25
B. 10.7.142.128/27
C. 10.152.4.192/26
D. 10.192.1.64/28
Answer: (SHOW ANSWER)
For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).
A /26 subnet provides 64 addresses, 62 usable - suitable.
A /27 subnet gives only 30 usable - insufficient.
A /25 offers 126 usable - more than needed.
A /28 provides just 14 - too small.
So, the most efficient subnet with minimal wastage is /26.
From Andrew Ramdayal's guide:
"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts. A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."

NEW QUESTION: 129
A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration:
Which of the following is causing the user's issue?
A. Incorrect DNS
B. Unreachable gateway
C. Failed root bridge
D. Poor upstream routing
Answer: (SHOW ANSWER)
The customer can access local resources (a database server), which means local networking is working.
However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets will not be routed outside the local network.

Breakdown of Options:
A). Incorrect DNS - DNS issues would cause problems resolving domain names, but the user should still be able to access external resources via IP addresses.
B). Unreachable gateway - # Correct answer. If the default gateway is incorrect or unreachable, the device cannot route traffic to the internet.
C). Failed root bridge - STP (Spanning Tree Protocol) failures cause switching issues, but the user can still access local devices, meaning STP is not the problem.
D). Poor upstream routing - Would affect the entire network, not just one user.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network routing concepts.

NEW QUESTION: 130

A network engineer is installing new PoE wireless APs. The first five APs deploy successfully, but the sixth one fails to start. Which of the following should the engineer investigate first?

A. Signal strength
B. Duplex mismatch
C. Power budget
D. CRC
Answer: (SHOW ANSWER)
When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.
A). Signal strength affects wireless connectivity, not whether the AP powers up.
B). Duplex mismatch causes poor throughput, not power failure.
D). CRC errors point to cabling issues but do not prevent booting if no power is available.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - PoE power budget considerations, device startup issues.

NEW QUESTION: 131
A network administrator needs to fail over services to an off-site environment. This process will take four weeks to become fully operational. Which of the following DR (Disaster Recovery) concepts does this describe?
A. Hot site
B. Warm site
C. Cold site
D. Active-active approach
Answer: (SHOW ANSWER)
A cold site is a backup facility that provides infrastructure (such as power, cooling, and space) but does not have active IT resources installed. When a disaster occurs, IT teams must bring in and

configure all necessary hardware and software before services can resume. This process can take weeks or longer-which matches the scenario described.
*Why not the other options?
*Hot site (A) - A hot site is a fully operational backup facility with up-to-date data and pre-configured hardware, allowing almost instant failover (minutes to hours).
*Warm site (B) - A warm site has pre-installed hardware and some software/configurations, but it requires some setup before becoming fully operational (hours to a few days).
*Active-active approach (D) - This means that multiple sites run simultaneously with load balancing, ensuring no downtime in case of a failure.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 15: Business Continuity and Disaster Recovery

NEW QUESTION: 132
A network manager connects two switches together and uses two connecting links. Which of the following configurations will prevent Layer 2 loops?
A. 802.1Q tagging
B. Full duplex
C. Link aggregation
D. QoS
Answer: (SHOW ANSWER)
Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).
From Andrew Ramdayal's guide:
"Link aggregation allows you to combine multiple network connections to increase the bandwidth and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

NEW QUESTION: 133
A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses (one for a computer and one for a phone). Which of the following classful IPv4 address ranges will be best-suited for the network?
A. Class D
B. Class B
C. Class A
D. Class C
Answer: (SHOW ANSWER)

*The total number of devices = (150 + 10) users × 2 IPs per user = 320 devices
*Class C (D) supports a maximum of 254 hosts (2^8 - 2), which is too small.
*Class B (B) supports 65,534 hosts (2^16 - 2), making it the best choice.
*Why not the other options?
*Class A (C): Supports millions of addresses, which is overkill for 320 devices.
*Class D (A): Used for multicast, not for device addressing.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 134
A secure communication link needs to be configured between data centers via the internet. The data centers are located in different regions. Which of the following is the best protocol for the network administrator to use?
A. DCI
B. GRE
C. VXLAN
D. IPSec
Answer: (SHOW ANSWER)
IPSec (Internet Protocol Security) is the best choice for secure communication over the internet, as it provides encryption, authentication, and data integrity. It is widely used in VPNs and site-to-site secure tunnels.
Breakdown of Options:
A). DCI (Data Center Interconnect) - A general term for linking data centers, but it doesn't specify a secure tunneling protocol.
B). GRE (Generic Routing Encapsulation) - Encapsulates traffic but lacks encryption, making it less secure than IPSec.
C). VXLAN (Virtual Extensible LAN) - Used for Layer 2 network overlays, not for securing communication over the internet.
D). IPSec - # Correct answer. Provides encryption, authentication, and integrity for data over the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement secure remote access methods.
RFC 4301: Security Architecture for the Internet Protocol

NEW QUESTION: 135
A network engineer is designing an internal network that needs to support both IPv4 and IPv6 routing. Which of the following routing protocols is capable of supporting both IPv4 and IPv6?
A. OSPFv3
B. RIPv2
C. BGP

D. EIGRP

Answer: (SHOW ANSWER)

EIGRP(Enhanced Interior Gateway Routing Protocol) supports bothIPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.

Reference:Section 2.1 - Characteristics of Routing Technologies - "EIGRP"

NEW QUESTION: 136

A network administrator is managing network traffic so that classified services and applications are prioritized. Which of the following technologies should the network administrator use?

A. Load balancing

B. Time to live

C. Quality of service

D. Content delivery network

Answer: (SHOW ANSWER)

Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion. Network + objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links. TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

NEW QUESTION: 137

A network administrator is responding to a request to configure a new IP phone. Which of the following should the network administrator do to allow data and voice traffic to be properly prioritized?

A. Configure full duplex.
B. Modify QoS.
C. Enable 802.1Q tagging.
D. Change the native VLAN.
Answer: (SHOW ANSWER)
To ensure voice and data traffic are properly prioritized for an IP phone, the administrator should modify (configure) QoS. In Network+ (N10-009), QoS is the primary mechanism used to prioritize latency-sensitive traffic such as VoIP. By classifying and marking voice frames/packets (often using DSCP/CoS values) and applying priority queuing, the network ensures voice traffic experiences minimal delay and jitter even when links are congested. This is essential for call quality because voice is highly sensitive to variation in delivery time and packet loss.
802.1Q tagging is important for VLAN separation (and many IP phone deployments use a voice VLAN), but VLAN tagging alone does not guarantee prioritization; it separates traffic, while QoS provides preferential treatment. Full duplex can reduce collisions on Ethernet links, but it does not implement traffic prioritization policies. Changing the native VLAN is a trunking/security configuration detail and not the correct action to prioritize voice versus data. In practice, networks often use both a voice VLAN (802.1Q) and QoS, but for the explicit requirement of prioritization, QoS is the correct answer.

NEW QUESTION: 138
A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?
A. Jumbo frames
B. 802.1Q tagging
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.
This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.
This method ensures that traffic from different VLANs is properly separated and managed across the network.
References: CompTIA Network+ study materials.

NEW QUESTION: 139
A network technician needs to configure IP addressing in a Class C network with eight subnets total:
Three subnets for 60 hosts
Three subnets for 15 hosts
Two subnets for seven hosts

Which of the following solutions should the technician use to accomplish this task?

A. CIDR

B. APIPA

C. VLSM

D. RFC 1918

Answer: (SHOW ANSWER)

The correct answer is VLSM (Variable Length Subnet Masking). According to the CompTIA Network+ N10-
009 objectives, VLSM allows a network administrator to create subnets of different sizes within the same network, making it ideal for environments where subnet host requirements vary.
In this scenario, the technician must support multiple subnet sizes-60 hosts, 15 hosts, and seven hosts- within a single Class C network. Using a single subnet mask for all eight subnets would either waste a large number of IP addresses or fail to meet host requirements. VLSM solves this problem by allowing each subnet to be assigned a custom subnet mask that closely matches its host needs, maximizing address efficiency.
CIDR enables classless addressing and route aggregation but does not, by itself, describe creating multiple subnet sizes within a single address block. APIPA is a self-assigned addressing mechanism used when DHCP fails and has no relevance to subnet design. RFC 1918 defines private IP address ranges but does not address subnetting strategies.
The Network+ objectives emphasize VLSM as a best practice for efficient IP address management, especially in enterprise environments where conserving address space and meeting diverse departmental requirements are critical. In this case, VLSM is the only solution capable of meeting all stated constraints.

NEW QUESTION: 140

Which of the following is the part of a disaster recovery (DR) plan that identifies the critical systems that should be recovered first after an incident?

A. RTO

B. SLA

C. MTBF

D. SIEM

Answer: (SHOW ANSWER)

RTO stands for Recovery Time Objective, which defines the maximum acceptable amount of time that a system, application, or function can be down after a failure or disaster. It helps prioritize which systems need to be recovered first based on their importance to business operations.
SLA (Service Level Agreement) refers to an agreement between a service provider and a customer regarding expected performance and availability, but it does not dictate recovery order.
MTBF (Mean Time Between Failures) is a measure of reliability and time between hardware or system failures.
SIEM (Security Information and Event Management) is a centralized tool for logging and alerting but not relevant to DR recovery prioritization.

Reference:
CompTIA Network+ N10-009 Official Objectives: 4.4 - Summarize business continuity and disaster recovery concepts.

NEW QUESTION: 141
Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?
A. Private
B. Community
C. Public
D. Hybrid
Answer: (SHOW ANSWER)
The correct answer is public cloud. In public cloud models, a provider (such as AWS, Azure, or Google Cloud) hosts infrastructure and services that are shared across multiple customers, known as multitenancy.
Each tenant is logically isolated, but physical infrastructure is shared, allowing providers to achieve economies of scale.
A). Private cloud is dedicated to one organization, not multitenant.
B). Community cloud is shared among organizations with common interests, but it's less common than public multitenancy.
D). Hybrid cloud combines private and public but does not define tenancy alone.
Public cloud services are the most cost-effective and scalable because they spread costs across many customers, but they require strong security and isolation to protect tenants.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud models, multitenancy, public vs private.

NEW QUESTION: 142
Which of the following protocols has a default administrative distance value of 90?
A. RIP
B. EIGRP
C. OSPF
D. BGP
Answer: (SHOW ANSWER)
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.References:CompTIA Network+ study materials.

NEW QUESTION: 143

Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?

A. Direct Connect

B. Internet gateway

C. Captive portal

D. VPN

Answer: (SHOW ANSWER)

Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.

Reference:

CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

NEW QUESTION: 144

Which of the following devices can operate in multiple layers of the OSI model?

A. Hub

B. Switch

C. Transceiver

D. Modem

Answer: (SHOW ANSWER)

* Understanding Switches:
* Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.
* Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.
* Capabilities of Multilayer Switches:
* VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs.
* Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.
* Comparison with Other Devices:
* Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.
* Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.
* Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.

* Practical Application:
* Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.
References:
* CompTIA Network+ study materials on network devices and the OSI model.

NEW QUESTION: 145
Users at a satellite office are experiencing issues when using videoconferencing. Which of the following should a technician focus on first to rectify these issues?
A. Quality of service
B. Network signal
C. Time to live
D. Load balancing
Answer: (SHOW ANSWER)
Quality of Service (QoS) is crucial for real-time services like video conferencing. It prioritizes voice and video packets over less critical traffic (like file downloads), reducing latency, jitter, and packet loss.
B). Network signal may apply to wireless, but it's not specific to video issues.
C). Time to live (TTL) affects packet lifespan, not performance or quality.
D). Load balancing manages traffic across multiple paths but doesn't prioritize real-time traffic like QoS does.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 146
A new staff member is unable to connect to the network. An IT support staff member finds the following:
The IP configuration is correct.
The TCP/IP stack is working on the workstation.
The gateway is unreachable.
Which of the following would the IT support staff member most likely check next?
A. The DHCP configuration on the workstation
B. The port's VLAN assignment on the switch
C. The DHCP configuration on the router
D. The default gateway on the switch
Answer: (SHOW ANSWER)
The correct answer is The port's VLAN assignment on the switch because the symptoms indicate a Layer 2 segmentation issue. According to CompTIA Network+ (N10-009) troubleshooting methodology and VLAN concepts, if the IP configuration is correct and the TCP/IP stack is

functioning, but the default gateway is unreachable, the issue often involves improper VLAN configuration.
In a switched environment, devices must be assigned to the correct VLAN to communicate with the appropriate default gateway interface (often configured on a router or Layer 3 switch). If the user's switch port is assigned to the wrong VLAN, the workstation may have a valid IP address but will not be able to reach the gateway because it is logically separated into a different broadcast domain.
Option A is unlikely since the IP configuration is already confirmed correct. Option C is not relevant because the issue is localized to a specific user, not a widespread DHCP failure. Option D refers to switch management configuration, which does not affect user traffic routing to the gateway.
Therefore, verifying the switch port's VLAN assignment is the most appropriate next troubleshooting step.

NEW QUESTION: 147
A network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?
A. Access
B. Core
C. Leaf
D. Spine
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
In a spine-leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer-often specifically to a "border leaf" that handles external connectivity.
Why not B. Core or D. Spine? In spine-leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.
Why not A. Access? "Access" is a term from the traditional three-tier model (access-distribution-core). In modern spine-leaf language, the analogous layer for endpoint attachment is the leaf.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Data center and campus architectures (spine-leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

NEW QUESTION: 148
A major natural disaster strikes a company's headquarters, causing significant destruction and data loss. The company needs to quickly recover and resume operations. Which of the following will a network administrator need to do first?
A. Conduct a damage assessment
B. Migrate to the cold site

C. Notify customers of the disaster
D. Establish a communication plan
Answer: (SHOW ANSWER)
In disaster recovery, the first step after an incident is to conduct a thorough damage assessment to understand the extent of the damage and determine the next appropriate steps. This allows for informed decision-making during the recovery process. The document says:
"The first step after a disaster is to conduct a damage assessment. This involves evaluating the extent of damage to equipment, infrastructure, and data, forming the foundation for recovery efforts and prioritizing response actions."

NEW QUESTION: 149
Which of the following would describe a data recovery goal?
A. MTBF
B. RPO
C. BCP
D. MTTR
Answer: B (LEAVE A REPLY)
RPO (Recovery Point Objective) describes a data recovery goal by defining the maximum acceptable amount of data loss measured in time. For example, an RPO of 4 hours means the organization must be able to restore data to a point no more than four hours before the outage-so backups, replication, or snapshots must occur frequently enough to meet that target. In Network+ (N10-009) operations objectives, disaster recovery and business continuity concepts include understanding recovery metrics and how they influence backup strategies, replication design, and service resilience planning. RPO specifically answers: "How much data can we afford to lose?" By contrast, MTBF (Mean Time Between Failures) is a reliability metric describing how often failures occur. MTTR (Mean Time To Repair/Recover) measures how long it takes to restore a system after failure, which is more aligned with service restoration time rather than data loss. BCP (Business Continuity Plan) is the overall plan/process for keeping critical business functions running during disruptions; it is not a single data recovery metric. Therefore, RPO is the correct term for a data recovery goal.

NEW QUESTION: 150
A group of users cannot connect to network resources. The technician runs ipconfig from one user's device and is able to ping the gateway shown from the command. Which of the following is most likely preventing the users from accessing network resources?

A. VLAN hopping
B. Rogue DHCP
C. Distributed DoS
D. Evil twin
Answer: B (LEAVE A REPLY)

A rogue DHCP server occurs when an unauthorized or misconfigured DHCP server assigns incorrect IP addresses, default gateways, or DNS settings to clients.
*In this scenario:
*The user can ping the gateway, meaning local network communication is working.
*However, they cannot access network resources, which suggests incorrect IP configuration (likely due to a rogue DHCP server assigning the wrong gateway or DNS).
*Why not the other options?
*VLAN hopping (A): This is an attack that exploits VLAN configurations to gain access to unauthorized VLANs. It would not typically cause multiple users to lose network access.
*Distributed DoS (C): A DDoS attack floods a network or service with traffic, but this issue is more likely misconfigured IP settings than an actual attack.
*Evil twin (D): This refers to a fraudulent Wi-Fi network mimicking a legitimate one. Since the users are on a wired network (ipconfig output checked), this is not applicable.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security Threats

NEW QUESTION: 151
A firewall receives traffic on port 80 and forwards it to an internal server on port 88. Which of the following technologies is being leveraged?
A. TLS
B. FHRP
C. SSL
D. PAT
Answer: (SHOW ANSWER)
The correct answer is PAT (Port Address Translation). According to the CompTIA Network+ N10-009 objectives, PAT is a form of Network Address Translation (NAT) that allows multiple internal hosts-or services-to be mapped to a single public IP address using different port numbers. PAT can also translate destination port numbers, which is exactly what is occurring in this scenario.
In this case, the firewall receives incoming traffic on port 80 (commonly used for HTTP) and forwards it to an internal server listening on port 88. This process is often referred to as port forwarding, which is a practical implementation of PAT. The firewall rewrites the destination port and potentially the destination IP address so that external clients can access internal services without exposing internal addressing schemes.
The other options do not apply. TLS and SSL are encryption protocols used to secure data in transit; they do not perform port translation. FHRP (First Hop Redundancy Protocol), such as HSRP or VRRP, provides gateway redundancy and high availability, not traffic forwarding or port remapping.
The Network+ objectives emphasize understanding how firewalls and NAT technologies manipulate IP addresses and ports to enable secure access to internal resources. PAT is the technology that enables this functionality, making it the correct answer.

NEW QUESTION: 152
A client with a 2.4GHz wireless network has stated that the entire office is experiencing intermittent issues with laptops after the WAP was moved. Which of the following is the most likely reason for these issues?
A. The network uses a non-overlapping channel.
B. The signal is reflecting too much.
C. The network has excessive noise.
D. A microwave is in the office.
Answer: D (LEAVE A REPLY)
Microwaves are known to interfere with the 2.4GHz frequency, which is the same frequency used by many wireless networks. This can cause signal degradation and intermittent connectivity issues, especially if the WAP is placed near such devices.

NEW QUESTION: 153
Which of the following typically uses compromised systems that become part of a bot network?
A. Evil twin attack
B. DDoS attack
C. XML injection
D. Brute-force password attack
Answer: (SHOW ANSWER)
A DDoS (Distributed Denial of Service) attack is often launched from botnets - networks of compromised systems (bots or zombies) under the control of an attacker. These devices flood the target with traffic to disrupt services.
A: Evil twin attack is a wireless spoofing method.
C: XML injection targets web applications.
D: Brute-force attacks repeatedly guess passwords but don't involve a botnet by default.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

NEW QUESTION: 154

A network technician is terminating a cable to a fiber patch panel in the MDF. Which of the following connector types is most likely in use?

A. F-type

B. RJ11

C. BNC

D. SC

Answer: (SHOW ANSWER)

In a fiber patch panel, the SC (Subscriber Connector or Standard Connector) is commonly used because of its push-pull design and reliability in enterprise environments.

Breakdown of Options:

A). F-type - Used for coaxial cables (e.g., cable TV), not fiber.

B). RJ11 - Used for telephone lines, not fiber.

C). BNC - Used for coaxial connections, not fiber.

D). SC - # Correct answer. A standard fiber optic connector used in patch panels.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.

NEW QUESTION: 155

Three new employees report that they are unable to access company resources, but they can connect to each other's devices. Which of the following would most likely need to be modified to resolve the issue?

A. The routing table on the gateway

B. The DNS configuration on the router

C. The pool on the DHCP server

D. The firewall on the workstation

Answer: C (LEAVE A REPLY)

If the three new employees can communicate with each other's devices, that strongly suggests their local Layer 2/Layer 3 connectivity is working (same VLAN/subnet, switching is fine, and they have IP addressing that allows local communication). The fact that they cannot access company resources (often on other subnets, servers, or the internet via internal routing) points to a problem with how these new endpoints are being addressed or routed beyond their local segment.

The most likely shared root cause affecting only "new employees" is DHCP scope/pool configuration. If the DHCP pool is exhausted, mis-scoped, or handing out incorrect options (such as an incorrect default gateway, wrong subnet mask, or an address range tied to an isolated VLAN), users could still talk locally but fail to reach resources outside their subnet. Modifying the DHCP server pool (expanding the scope, correcting the scope network, or ensuring the correct options are assigned) would resolve this with minimal changes.

A gateway routing table issue would typically affect many users, not just three new ones. DNS misconfiguration on the router would more commonly cause name-resolution problems, not block all resource access (and wouldn't be isolated to only new employees). A workstation firewall

would not usually prevent access to "company resources" in a way that consistently affects three new devices while still allowing peer connectivity.

NEW QUESTION: 156
Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?
A. Theadministrator didnot provisionenough IP addresses.
B. Theadministrator configured an incorrect default gateway.
C. Theadministrator didnot provisionenough routes.
D. Theadministrator didnot provisionenough MAC addresses.
Answer: (SHOW ANSWER)
When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.References:CompTIA Network+ study materials.

NEW QUESTION: 157
A small business is deploying new phones, and some of the phones have full HD videoconferencing features.
The Chief Information Officer (CIO) is concerned that the network might not be able to handle the traffic if it reaches a certain threshold. Which of the following can the network engineer configure to help ease these concerns?
A. A VLAN with 100Mbps speed limits
B. An IP helper to direct VoIP traffic
C. A smaller subnet mask
D. Full duplex on all user ports
Answer: (SHOW ANSWER)
Full duplex mode allows devices to send and receive data simultaneously, improving network performance and reducing congestion, which is critical for VoIP and video conferencing.
Breakdown of Options:
A). A VLAN with 100Mbps speed limits - VLANs segment traffic but limiting speeds to 100Mbps would worsen video performance.
B). An IP helper to direct VoIP traffic - IP helper is used for DHCP relay, not for VoIP optimization.
C). A smaller subnet mask - A smaller subnet reduces IP address availability but does not improve network performance.
D). Full duplex on all user ports - Correct answer. Full duplex eliminates collisions, allowing better VoIP and video performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.2: Compare and contrast various networking devices.

IEEE 802.3: Ethernet Full Duplex Operation

NEW QUESTION: 158
A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?
A. APIPA
B. Multicast
C. Class C
D. Experimental
Answer: (SHOW ANSWER)
APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:
"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

NEW QUESTION: 159
A detective is investigating an identity theft case in which the target had an RFID-protected payment card issued and compromised in the same day. The only place the target claims to have used the card was at a local convenience store. The detective notices a video camera at the store is placed in such a way that customers' credentials can be seen when they pay. Which of the following best explains this social engineering technique?
A. Shoulder surfing
B. Impersonation
C. Vishing
D. Tailgating
Answer: (SHOW ANSWER)
Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.
From Andrew Ramdayal's guide:
"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

NEW QUESTION: 160
Which of the following layers of the OSI model is responsible for end-to-end encryption?
A. Presentation
B. Application
C. Session
D. Transport
Answer: (SHOW ANSWER)

The correct answer is Presentation, which is Layer 6 of the OSI model. According to the CompTIA Network+ N10-009 objectives, the Presentation layer is responsible for data formatting, compression, and encryption, ensuring that data sent from the application layer of one system can be properly interpreted by the receiving system.

End-to-end encryption refers to encrypting data before transmission and decrypting it only at the final destination, preventing intermediaries from accessing the plaintext data. In the OSI model, this encryption and decryption function is logically placed at the Presentation layer, which sits between the Application and Session layers. This layer transforms data into a standardized format and applies security mechanisms such as encryption algorithms.

While modern implementations like TLS/SSL often operate across multiple layers in real-world networking stacks, the Network+ exam adheres to the conceptual OSI model when testing knowledge. From an OSI perspective, encryption is explicitly associated with the Presentation layer.

The Application layer provides network services to end-user applications, the Session layer manages session establishment and teardown, and the Transport layer focuses on segmentation, flow control, and reliability.

None of these layers are primarily responsible for encryption within the OSI framework. CompTIA emphasizes understanding these conceptual responsibilities, making Presentation the correct and expected answer.

NEW QUESTION: 161

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Answer:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:
Click on each switch to open its terminal window.
Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.
Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.
Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.
Fill in the missing information in the diagram using the drop-down menus provided.
Here is an example of how to fill in the missing information for Core Switch 1:
The IP address of Core Switch 1 is 192.168.1.1.
The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3:
192.168.3.0/24.
The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.
The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.
The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 162
A network administrator is conducting an assessment and finds network devices that do not meet standards.
Which of the following configurations is considered a set of rules that devices should adhere to?
A. Production
B. Backup
C. Candidate
D. Golden
Answer: (SHOW ANSWER)
The correct answer is golden configuration. This is a reference standard or baseline that defines the approved settings and rules devices should follow. Any deviation from the golden configuration indicates drift or misconfiguration that must be remediated.
A). Production refers to the live environment but doesn't define a standard.
B). Backup configurations are stored copies, not the standard rules.
C). Candidate configuration is a proposed change being tested, not the final baseline.
By enforcing golden configurations, administrators ensure compliance, maintain security standards, and improve consistency across the enterprise.

References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration standards, golden images/configs.

NEW QUESTION: 163
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

MAC address	IP address	Interface	VLAN
0c00.1134.0001	192.168.1.10	eth4	10
0c00.1983.210a	192.168.2.13	eth5	11
0c00.1298.d239	192.168.1.10	eth6	10
0c00.a291.c113	192.168.2.12	eth7	11
0c00.923b.2391	192.168.1.11	eth8	10
feff.2391.1022	192.168.1.254	eth1	10

Which of the following is the most likely cause of the user ' s connection issues?
A. A port with incorrect VLAN assigned
B. A switch with spanning tree conflict
C. Another PC with manually configured IP
D. A router with overlapping route tables
Answer: (SHOW ANSWER)
This scenario describes a duplicate IP address. The ARP table shows two different MAC addresses (0c00.
1134.0001 and 0c00.1298.d239) associated with the same IP address (192.168.1.10), which leads to ARP table conflicts and intermittent connectivity.
From Andrew Ramdayal's guide:
"Duplicate IP addresses occur when two devices on the same network are assigned the same IP address, causing network conflicts. Common issues include manual configuration errors or DHCP lease issues.
Resolution includes using IP management tools and avoiding overlaps in DHCP and static IP assignments."

NEW QUESTION: 164
Users are reporting latency on the network. The network engineer notes the following:
Confirms the only change was a new network switch
Confirms all users are experiencing latency
Thinks the issue is a network loop caused by the lower bridge ID of the new switch Which of the following describes the next step in the troubleshooting methodology?
A. Identify the problem.

B. Test the theory.
C. Implement the solution.
D. Verify full system functionality.
Answer: (SHOW ANSWER)
The correct answer is Test the theory, which aligns directly with the CompTIA Network+ N10-009 troubleshooting methodology. According to the official troubleshooting steps, once a problem has been identified and relevant information gathered, the next step is to establish a theory of probable cause and then test that theory to determine whether it is valid.
In this scenario, the engineer has already completed the problem identification phase by confirming that all users are experiencing latency and correlating the issue with the installation of a new switch. The engineer has also formed a theory: that a network loop caused by the lower bridge ID of the new switch may be impacting Spanning Tree Protocol (STP), resulting in congestion and latency. Because this theory has already been developed, the next logical and required step is to test the theory-for example, by reviewing STP states, temporarily disabling ports, or adjusting bridge priorities.
Implementing a solution would be premature without validating the theory, and verifying full system functionality occurs only after a fix has been applied. The Network+ objectives stress following a structured methodology to avoid unnecessary changes and minimize network disruption. Testing the theory ensures accuracy before corrective action is taken, reducing risk and downtime.

NEW QUESTION: 165
Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?
A. General Data Protection Regulation
B. Least privilege network access
C. Acceptable use policy
D. End user license agreement
Answer: (SHOW ANSWER)
Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 166
As part of a recovery strategy, a network administrator needs to make sure no more than eight hours of data loss occurs. Which of the following DR metrics describes this requirement?
A. RPO
B. MTTR
C. RTO

D. MTBF

Answer: (SHOW ANSWER)

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. If leadership states "no more than eight hours of data loss," they are describing how far back the organization is willing to roll data after an outage or disaster-meaning backups, replication, snapshots, or journaling must ensure recoverable data is no older than eight hours. In Network+ terms, this is a core availability and resiliency planning concept: you choose an RPO based on business impact, then implement backup frequency
/replication strategy to meet it. By contrast, Recovery Time Objective (RTO) is about how quickly services must be restored (downtime duration), not how much data can be lost. MTTR (Mean Time to Repair/Recover) is an operational reliability metric describing typical time to restore a system, and MTBF (Mean Time Between Failures) indicates expected time between failures-neither directly states acceptable data loss.

Therefore, the metric matching "eight hours of data loss" is RPO.

NEW QUESTION: 167

Which of the following connectors provides console access to a switch?

A. ST

B. RJ45

C. BNC

D. SFP

Answer: B (LEAVE A REPLY)

Console Access:

Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.

RJ45 Connector:

Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.

Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).

Comparison with Other Connectors:

ST (Straight Tip): A fiber optic connector used for networking, not for console access.

BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.
SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.
Practical Application:
Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).
References:
CompTIA Network+ study materials on network devices and connectors.

NEW QUESTION: 168
Which of the following troubleshooting steps provides a change advisory board with the information needed to make a decision?
A. Identify the problem
B. Develop a theory of probable cause
C. Test the theory to determine cause
D. Establish a plan of action
Answer: (SHOW ANSWER)
When dealing with troubleshooting and change management, the plan of action outlines the steps, risks, and mitigation strategies. A change advisory board (CAB) uses this documented plan to decide whether to approve the change.
A). Identify the problem is the first step in troubleshooting, not decision-making for CAB.
B). Develop a theory is diagnostic work, not planning.
C). Test the theory confirms causes but doesn't provide actionable planning information.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Change management, troubleshooting methodology, CAB processes.

NEW QUESTION: 169
A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?
A. With a voice VLAN
B. With too many VLANs
C. With a default VLAN
D. With a native VLAN
Answer: (SHOW ANSWER)
It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

NEW QUESTION: 170

Which of the following network ports is used when a client accesses an SFTP server?

A. 22

B. 80

C. 443

D. 3389

Answer: (SHOW ANSWER)

SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.

Breakdown of Options:

A). 22 - Correct answer. SFTP runs over SSH (port 22) for secure file transfers.

B). 80 - Used for HTTP, not SFTP.

C). 443 - Used for HTTPS (secure web traffic).

D). 3389 - Used for RDP (Remote Desktop Protocol).

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.

RFC 4253: SSH Transport Layer Protocol

NEW QUESTION: 171

A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modern has a signal power of -97 dB.

A. Removing any spliters connecte to the line

B. Switching the devices to wireless

C. Moving the devices closer to the modern

D. Lowering the network speed

Answer: (SHOW ANSWER)

A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds.

Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.

* Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.

* Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.

* Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.

* Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

NEW QUESTION: 172
Which of the following is the best reason to create a golden configuration?
A. To provide configuration consistency
B. To decrease the size of configuration files
C. To increase security by encrypting configurations
D. To set up backup configurations for each device
Answer: (SHOW ANSWER)
A golden configuration is a baseline configuration file that contains approved, standardized settings for network devices. The purpose is to ensure configuration consistency across the environment. This prevents misconfigurations, supports compliance with organizational or regulatory standards, and accelerates recovery if a device needs reconfiguration.
B). Reducing file size is not the goal of golden configs.
C). Golden configs can include security settings, but they are not inherently encrypted - they are simply a baseline template.
D). While configs can be backed up, golden configs are more about standardization, not device-specific backups.
By maintaining a golden configuration, administrators can quickly detect unauthorized changes (by comparing running configs against the golden file) and enforce consistency across devices. This improves network stability, reduces troubleshooting complexity, and enhances security posture.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration management, golden images/configurations.

NEW QUESTION: 173
A network administrator needs to assign IP addresses to a newly installed network. They choose 192.168.1.0
/24 as their network address and need to create three subnets with 30 hosts on each subnet. Which of the following is a valid subnet mask that will meet the requirements?
A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240
Answer: (SHOW ANSWER)
Understanding the Requirements
Network Address: 192.168.1.0/24
The /24 notation means a subnet mask of 255.255.255.0, providing 256 total addresses (192.168.1.0-
192.168.1.255).

Usable hosts: 256 - 2 (network and broadcast) = 254.
Goal: Create 3 subnets, each with 30 hosts.
Each subnet needs enough addresses to accommodate 30 hosts, plus 2 reserved addresses (network and broadcast) per subnet.
Total addresses per subnet = 30 (hosts) + 2 (network/broadcast) = 32 addresses.
Subnetting Basics (Networking Fundamentals)
Subnet Mask: Determines how many bits are borrowed from the host portion to create subnets.
Original Mask: /24 (255.255.255.0) = 24 network bits, 8 host bits.
Formulae:
Number of subnets = 2^(number of borrowed bits).
Number of addresses per subnet = 2^(remaining host bits).
Usable hosts per subnet = 2^(remaining host bits) - 2.
We need:
At least 3 subnets.
At least 32 addresses per subnet (to fit 30 hosts + 2 reserved).
Step-by-Step Analysis
Determine Addresses Needed per Subnet:
32 addresses is a power of 2 (2^5 = 32).
This means each subnet requires 5 host bits (since 2^5 = 32 total addresses, and 32 - 2 = 30 usable hosts).
Calculate Remaining Bits:
Original network has 8 host bits (/24).
If 5 bits are left for hosts, we borrow: 8 - 5 = 3 bits for subnetting.
New Subnet Mask:
Original mask: /24 (24 network bits).
Borrow 3 bits: 24 + 3 = /27.
/27 = 255.255.255.224 (binary: 11111111.11111111.11111111.11100000).
Verify Requirements:
Number of Subnets: 2^3 = 8 subnets (meets the requirement of at least 3).
Addresses per Subnet: 2^5 = 32 addresses.
Usable Hosts per Subnet: 32 - 2 = 30 hosts (exactly meets the requirement).
Subnet Breakdown:
Increment: 256 - 224 = 32 (each subnet increments by 32 in the fourth octet).
Subnets:
192.168.1.0-192.168.1.31 (Network: .0, Broadcast: .31, Hosts: .1-.30)
192.168.1.32-192.168.1.63 (Network: .32, Broadcast: .63, Hosts: .33-.62)
192.168.1.64-192.168.1.95 (Network: .64, Broadcast: .95, Hosts: .65-.94) (And 5 more subnets up to 192.168.1.255.) Three subnets fit perfectly with 30 hosts each.
Evaluating the Options
A). 255.255.255.128 (/25):
Borrow 1 bit: 24 + 1 = /25.

Subnets: 2^1 = 2 (not enough, need 3).
Host bits: 7 (2^7 = 128 addresses, 126 hosts).
Why Not: Only 2 subnets, fails the requirement.
B). 255.255.255.192 (/26):
Borrow 2 bits: 24 + 2 = /26.
Subnets: 2^2 = 4 (meets 3).
Host bits: 6 (2^6 = 64 addresses, 62 hosts).
Why Not: 62 hosts exceeds 30, but it's overkill; /27 is more efficient and still valid.
C). 255.255.255.224 (/27):
Borrow 3 bits: 24 + 3 = /27.
Subnets: 2^3 = 8 (meets 3).
Host bits: 5 (2^5 = 32 addresses, 30 hosts).
Why Yes: Perfectly fits 3 subnets with exactly 30 hosts each.
D). 255.255.255.240 (/28):
Borrow 4 bits: 24 + 4 = /28.
Subnets: 2^4 = 16 (meets 3).
Host bits: 4 (2^4 = 16 addresses, 14 hosts).
Why Not: Only 14 hosts per subnet, fails the 30-host requirement.
Why /27 (255.255.255.224) is Best
It provides exactly 30 usable hosts per subnet, avoiding waste while meeting the minimum requirement.
It allows 8 subnets, exceeding the need for 3, ensuring flexibility.
The study guide emphasizes efficient subnet design, and /27 balances host count and subnet availability.
CompTIA Network+ Context
Networking Fundamentals: Subnetting is a core skill, requiring understanding of CIDR, binary conversion, and address allocation.
Example from Study Guide: Similar problems calculate subnet masks for specific host counts, reinforcing /27 as a common solution for ~30 hosts.

NEW QUESTION: 174
Users usually use RDP to connect to a terminal server with hostname TS19 that points to 10.0.100.19.
However, users recently have been unable to connect to TS19. The technician pings 10.0.100.19 and gets an unreachable error. Which of the following is the most likely cause?
A. The users are on the wrong subnet.
B. The DHCP server renewed the lease.
C. The IP address was not reserved.
D. The hostname was changed.
Answer: (SHOW ANSWER)

If a ping to 10.0.100.19 is unreachable, the most likely issue is that users are on the wrong subnet and cannot communicate with the server.
Breakdown of Options:
A: The users are on the wrong subnet. # Correct answer. If users are on a different subnet without proper routing, they won't reach the server.
B: The DHCP server renewed the lease. - Would change the client's IP, but the server's static IP should remain unchanged.
C: The IP address was not reserved. - DHCP reservations matter for dynamic IPs, but RDP servers typically have static IPs.
D: The hostname was changed. - Would affect DNS resolution, but pinging the IP directly would still work.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting concepts.

NEW QUESTION: 175
Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).
A. Fire suppression system
B. UPS location
C. Humidity control
D. Power load
E. Floor construction type
F. Proximity to nearest MDF
Answer: (SHOW ANSWER)
When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.References:CompTIA Network+ study materials.

NEW QUESTION: 176
Which of the following would be violated if an employee accidentally deleted a customer's data?
A. Integrity
B. Confidentiality
C. Vulnerability
D. Availability
Answer: (SHOW ANSWER)
Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

NEW QUESTION: 177
A network engineer is testing a website to ensure it is compatible with IPv6. After attempting to ping the website by its IPv6 address, the engineer determines that the DNS has not been set up properly. Which of the following should the network engineer complete to resolve this issue?
A. Enable a PTR record.
B. Update the existing TXT record.
C. Add a new AAAA record.
D. Configure a secondary NS record.
Answer: (SHOW ANSWER)
*AAAA records map domain names to IPv6 addresses, enabling proper resolution.
*PTR records (A) are for reverse DNS lookups.
*TXT records (B) store text-based information, not IP addresses.
*NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Configuration & IPv6.

NEW QUESTION: 178
A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?
A. Multitenancy
B. VPC
C. NFV
D. SaaS
Answer: (SHOW ANSWER)
Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 179
A network engineer added more APs to improve wireless coverage. However, users now report that the connectivity disconnects and reconnects repeatedly. Which of the following is causing the issue?
A. Throughput capacity
B. Roaming misconfiguration
C. Channel overlap
D. Packet loss
Answer: (SHOW ANSWER)

Adding more access points can improve coverage, but it also increases the risk of co-channel interference if APs are configured on the same or overlapping channels. Channel overlap causes contention and interference, leading to retries, unstable performance, and symptoms that feel like frequent disconnect
/reconnect events-especially in dense deployments. Network+ (N10-009) wireless troubleshooting objectives highlight proper channel planning (non-overlapping channels, appropriate channel width) as critical when increasing AP density. If adjacent APs are competing on the same channel (or overlapping channels in
2.4 GHz), clients may experience poor signal-to-noise ratios and repeated reassociations as they struggle to maintain a stable link.
Roaming misconfiguration can cause sticky clients or poor handoffs, but the classic problem introduced immediately after "adding more APs" is interference from bad channel design. Throughput capacity is about available bandwidth and airtime efficiency; it can make things slow, but it doesn't inherently cause repeated disconnect/reconnect loops like interference does. Packet loss is a symptom that may occur due to interference, but the root cause in the options that best fits the scenario is channel overlap.

NEW QUESTION: 180

A network administrator configures a new network discovery tool and is concerned that it might disrupt business operations. Which of the following scan types should the administrator configure?

A. Authenticated
B. Ad hoc
C. Unauthenticated
D. Scheduled
Answer: (SHOW ANSWER)
If the administrator is concerned a new discovery tool could disrupt operations, the safest option is to configure scheduled scans. Network+ (N10-009) operations guidance emphasizes minimizing impact by running potentially noisy tasks (discovery, vulnerability checks, inventory scans) during defined maintenance windows or off-peak hours. A scheduled scan allows controlled timing, predictable load, and easier coordination with change management, monitoring, and support teams. This reduces the risk of saturating links, overwhelming devices with queries, or triggering alerts during business-critical periods.
Ad hoc scanning is on-demand and may occur at any time, which increases the chance of disruption if run during peak usage. Authenticated versus unauthenticated describes whether the scanner uses credentials to log into systems for deeper visibility; that choice affects depth and accuracy, but it doesn't directly address when scanning occurs to reduce business impact. An authenticated scan can still be disruptive if run at the wrong time, and an unauthenticated scan can still generate significant traffic. Since the key concern is operational disruption, controlling scan timing via scheduled scans is the best mitigation.

NEW QUESTION: 181

A media company is implementing a global streaming service. Which of the following should the company apply to each regional point of presence in order to comply with local laws?

A. ACL

B. Port security

C. Key management

D. Content filtering

Answer: D (LEAVE A REPLY)

For a global streaming service, different countries and regions often have specific legal requirements about what content can be accessed (for example, age restrictions, prohibited material, censorship rules, or licensing constraints). To comply with these local laws at each regional point of presence (PoP), the company should implement content filtering. In Network+ security objectives, content filtering is a control used to allow, block, or restrict access to specific categories of content, URLs, applications, or media based on policy.

Applied regionally, it supports geo-policy enforcement by ensuring that users served by a given PoP receive only content permitted in that jurisdiction.

An ACL primarily controls network traffic flows (permit/deny based on IPs, ports, and protocols). While ACLs can help block certain services, they are not designed to classify and regulate streaming media content in a way that aligns with legal content rules. Port security is a switch feature to restrict which devices can connect to a port (MAC-based controls) and is unrelated to regional compliance for streamed media. Key management concerns encryption key handling and protects confidentiality/integrity, but it does not determine which content is allowed in a region. Therefore, regional content filtering is the best match for meeting local legal requirements.

NEW QUESTION: 182

A network engineer configures the network settings in a new server as follows:

IP address = 192.163.1.15

Subnet mask = 255.255.255.0

Gateway = 192.163.1.255

The server can reach other hosts on the same subnet successfully, but it cannot reach hosts on different subnets. Which of the following is most likely configured incorrectly?

A. Subnet mask

B. Gateway

C. Default route
D. IP address
Answer: (SHOW ANSWER)
The default gateway for a network should be an IP address within the subnet, but not the broadcast address. In this case:
IP: 192.163.1.15
Subnet Mask: 255.255.255.0
This means the network range is: 192.163.1.0 - 192.163.1.255
192.163.1.255 is the broadcast address for this subnet, so it cannot be used as a gateway.
Hence, the device fails to communicate outside its subnet because it's trying to use a broadcast address as its gateway.
The issue is clearly with the gateway configuration.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 1.4: "Given a scenario, configure and deploy common Ethernet switching features."

NEW QUESTION: 183
A storage network requires reduced overhead and increased efficiency for the amout of data being sent.
Which of the following should an engineer likely configure to meet these requirements>?
A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
* Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.
* Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
* Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.
* Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

* Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

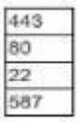
NEW QUESTION: 184
A user tries to visit www.abc.com, but the website that displays is www.cba.com. Which of the following should be done in order to reach the correct website?
A. Modify the CNAME record.
B. Update the PTR record.
C. Change the NTP settings.
D. Delete the TXT record.
Answer: (SHOW ANSWER)
The correct answer is Modify the CNAME record because a CNAME (Canonical Name) record maps one domain name (alias) to another domain name. If a user enters www.abc.com but is redirected to www.cba.
com, it is likely that the DNS configuration includes an incorrect CNAME entry pointing abc.com to cba.com.
Updating or correcting the CNAME record ensures the alias resolves to the intended host.
According to CompTIA Network+ (N10-009) objectives covering DNS record types, a CNAME record is used to alias one domain name to another, commonly for load balancing, CDN services, or website redirection.
A PTR record (Option B) is used for reverse DNS lookups (IP address to hostname) and does not control forward name resolution for websites. NTP settings (Option C) are used for time synchronization and have no impact on DNS resolution. A TXT record (Option D) stores descriptive text information (such as SPF, DKIM, or domain verification data) and does not affect website redirection.
Therefore, correcting the CNAME record resolves the issue and ensures users reach the correct website.

NEW QUESTION: 185
A customer wants to cache commonly used content to reduce the number of full page downloads from the internet. Which of the following should the network administrator recommend?
A. Proxy server
B. Load balancer
C. Open relay
D. Code repository
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
A proxy server (specifically a caching HTTP/HTTPS proxy) stores frequently accessed web objects and serves them locally to clients, reducing external bandwidth consumption and improving response times.
B). Load balancer distributes traffic across servers but does not inherently cache internet content.

C). Open relay is a misconfigured mail server that permits unauthorized relaying-this is a security issue, not a caching solution.
D). Code repository (e.g., for source control) isn't related to web content caching.
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Application-layer services (HTTP/HTTPS), proxies and caching behavior, performance optimization.

NEW QUESTION: 186
A systems administrator is configuring a new device to be added to the network. The administrator is planning to perform device hardening prior to connecting the device. Which of the following should the administrator do first?
A. Update the network ACLs.
B. Place the device in a screened subnet.
C. Enable content filtering.
D. Change the default admin passwords.
Answer: (SHOW ANSWER)
Changing default admin passwords is a fundamental first step in device hardening to prevent unauthorized access.

NEW QUESTION: 187
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:



Which of the following ports should be disabled?
A. 22
B. 80
C. 443
D. 587
Answer: (SHOW ANSWER)
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:
Port 22: Used for SSH, providing secure remote access and file transfers.

Port 587: Used for secure email submission (SMTP) with encryption.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.
Cisco Networking Academy: Provides training on secure web server configuration and port management.
Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

NEW QUESTION: 188
A company has observed increased user traffic to gambling websites and wants to limit this behavior on work computers. Which of the following should the company most likely implement?
A. ACLs
B. Content filter
C. Port security
D. Screened subnet
Answer: (SHOW ANSWER)
A content filter blocks access to specific websites based on category, URL, or keywords. This is the best solution to restrict gambling websites.
Breakdown of Options:
A). ACLs - Control network access, not specific web content.
B). Content filter - # Correct answer. Used to block access to unwanted websites.
C). Port security - Prevents unauthorized device connections, not web traffic filtering.
D). Screened subnet - A DMZ isolates public-facing servers, not user restrictions.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Given a scenario, implement network security measures.

NEW QUESTION: 189
Which of the following would most likely be utilized to implement encryption in transit when using HTTPS?
A. SSH
B. TLS
C. SCADA
D. RADIUS
Answer: (SHOW ANSWER)
TLS (Transport Layer Security)is the protocol that providesencryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.
* A. SSHis used for secure terminal access, not HTTPS.
* C. SCADArefers to control systems, not encryption protocols.

* D. RADIUSis an authentication protocol, not for encrypting HTTPS traffic.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.
CompTIA Network+ N10-009 Official Objectives: 4.6 - Explain authentication and access controls.

NEW QUESTION: 190

Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the attackers' activities?

A. Geofencing
B. Honeynet
C. Jumpbox
D. Screened subnet
Answer: (SHOW ANSWER)
A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 191
Which of the following is most closely associated with having a leased line to a public cloud provider?
A. VPN
B. Direct Connect
C. Internet gateway
D. Private cloud
Answer: (SHOW ANSWER)
Direct Connect is the option most closely associated with having a leased line to a public cloud provider, as defined in the CompTIA Network+ N10-009 objectives under cloud connectivity and WAN technologies.
Direct Connect (or equivalent services such as Azure ExpressRoute or Google Cloud Interconnect) provides a dedicated, private physical connection between an organization's on-premises network and a public cloud provider's infrastructure. This connection bypasses the public internet, offering consistent bandwidth, lower latency, improved performance, and enhanced security.
A VPN uses encrypted tunnels over the public internet, which does not qualify as a leased line and is subject to internet congestion and variable performance. An internet gateway simply allows cloud resources to communicate with the public internet and does not imply a private or dedicated connection. A private cloud refers to a deployment model where cloud resources are dedicated to a single organization; it does not describe the connectivity method or the use of a leased circuit.

According to Network+ objectives, leased-line connectivity to cloud providers is commonly used by enterprises that require high availability, predictable throughput, regulatory compliance, or secure hybrid cloud architectures. Direct Connect is a foundational component of hybrid networking strategies, linking on- premises environments directly to public cloud services using provider-managed circuits.

NEW QUESTION: 192
Which of the following cable types allows the use of QSFP ports without requiring transceivers?
A. Multimode
B. Twinaxial
C. RG11
D. Category 6
Answer: (SHOW ANSWER)
Twinaxial (Direct Attach Copper / DAC) cables can plug directly into QSFP ports without needing separate optical transceivers. They are cost-effective for short-distance, high-speed connections (commonly in data centers).
A). Multimode fiber requires SFP/QSFP transceivers to convert electrical signals to optical.
C). RG11 is coaxial cable for broadband/cable TV, not used in QSFP ports.
D). Category 6 is twisted-pair Ethernet cabling, not directly compatible with QSFP ports.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Cable types, QSFP, DAC (Twinaxial), transceiver requirements.

NEW QUESTION: 193
A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?
A. netstat
B. nslookup
C. ping
D. tracert
Answer: (SHOW ANSWER)
* Understanding Tracert:
* Traceroute Tool:tracert(Windows) ortraceroute(Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.
* Determining Traffic Path:
* Path Identification:By runningtracertto the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.
* Load Balancing Insight:If the office uses load balancing for its internet links,tracertcan help verify which link is currently handling the traffic for the web application.

* Comparison with Other Tools:
* netstat:Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
* nslookup:Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.
* ping:Tests connectivity and measures round-trip time but does not provide path information.
* Implementation:
* Open a command prompt or terminal.
* Executetracert [destination IP]to trace the route.
* Analyze the output to determine the path and the link being used.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

NEW QUESTION: 194
Which of the following is the best use case of a site-to-site VPN?
A. Securing access across an untrusted network
B. Encrypting data at rest
C. Filtering traffic between two internal subnets
D. Hosting public-facing applications that contain company resources
Answer: (SHOW ANSWER)
A site-to-site VPN is used to securely connect two networks over an untrusted network, most commonly the public internet. In Network+ (N10-009) objectives, VPNs are described as providing confidentiality and integrity for data in transit by creating an encrypted tunnel between sites (for example, headquarters and a branch office). This allows systems at both locations to communicate as if on the same private WAN, while preventing eavesdropping or tampering by intermediate networks. Typical implementations use IPsec tunneling and rely on negotiated encryption/authentication parameters to protect traffic end-to-end between VPN gateways. Encrypting data at rest refers to storage encryption (disk/database), not VPN tunneling. Filtering traffic between two internal subnets is usually handled by ACLs, firewalls, or segmentation controls, not a site-to- site VPN. Hosting public-facing applications is a DMZ / reverse proxy / WAF design concern; a VPN is not the primary control for exposing public services (and generally you would not require the public to use a VPN to reach a public website). Therefore, securing site connectivity across an untrusted network is the best match.

NEW QUESTION: 195
A network engineer is implementing a new connection between core switches. The engineer deploys the following configurations:
Core-SW01
vlan 100
name
interface Ethernet 1/1

channel-group 1 mode active
interface Ethernet 1/2
channel-group 1 mode active
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100
Core-SW02
vlan 100
name
interface Ethernet 1/1
switchport mode trunk
switchport trunk allow vlan 100
interface Ethernet 1/2
switchport mode trunk
switchport trunk allow vlan 100
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100
Which of the following is the state of the Core-SW01 port-channel interfaces?
A. Incrementing CRC errors
B. Error disabled
C. Administratively down
D. Suspended
Answer: (SHOW ANSWER)
On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core-SW02, the ports are configured as independent trunks, not as part of an LACP group. Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.
A). CRC errors suggest cabling or signal integrity issues, not config mismatch.
B). Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not LACP mismatch.
C). Administratively down indicates a shutdown command, not the case here.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port-channel/LACP configuration issues, interface states.

NEW QUESTION: 196
Which of the following OSI model layers manages the exchange of HTTP information?
A. Session
B. Data link
C. Network
D. Application

Answer: (SHOW ANSWER)
HTTP is an application-layer protocol, so the OSI layer that manages the exchange of HTTP information is Layer 7 (Application) . In the Network+ (N10-009) objectives, the OSI model is used to map common protocols to the layers where they operate. HTTP defines how web clients and servers format and exchange requests and responses (methods like GET/POST, headers, status codes, and message bodies). Those behaviors are part of the application services provided to end-user software such as web browsers, APIs, and web servers.
While HTTP relies on lower layers to function (for example, TCP at the Transport layer for reliable delivery and IP at the Network layer for addressing and routing), the protocol logic and meaning of the web transactions exist at the Application layer. The distractors do not fit: the Network layer handles IP routing, the Data Link layer handles frames and MAC addressing on local links, and the Session layer is associated with session establishment/management concepts but is not where HTTP is categorized for Network+ mapping. Therefore, Application is the correct answer.

NEW QUESTION: 197
Which of the following types of attacks is most likely to occur after an attacker sets up an evil twin?
A. On-path
B. DDoS
C. ARP spoofing
D. Phishing
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
An evil twin is a malicious wireless access point that impersonates a legitimate SSID. Once victims connect, the attacker can intercept and manipulate traffic, performing an on-path (man-in-the-middle) attack- capturing credentials, injecting content, or downgrading encryption.
B). DDoS overwhelms services with traffic; it's not the typical follow-on from clients joining a rogue AP.
C). ARP spoofing is another way to become on-path on wired segments, but with an evil twin, the wireless association itself enables the on-path position.
D). Phishing is social engineering; while an evil twin could be used to present fake portals, the primary technical posture after connection is on-path.

References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs/evil twins), traffic interception, on-path attacks.

NEW QUESTION: 198
A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?
A. Coaxial cable
B. 9.8ft (3m) cable
C. Plenum cable
D. STP cable
Answer: (SHOW ANSWER)
The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.
A). Coaxial is not used for modern Ethernet server-switch links.
B). Shorter UTP cable does not solve EMI issues.
C). Plenum cable refers to cable jacket type for fire safety, not electrical shielding.
STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

NEW QUESTION: 199
Which of the following routing protocols needs to have an autonomous system set in order to establish communication with neighbor devices?
A. OSPF
B. EIGRP
C. FHRP
D. RIP
Answer: (SHOW ANSWER)
EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary advanced distance-vector routing protocol. While it operates within an Autonomous System (AS), it requires the AS number to be configured for routers to recognize each other as EIGRP neighbors.
OSPF (Open Shortest Path First) uses areas and routers must be in the same area to form adjacencies, but it doesn't require AS numbers in the same way.

FHRP (First Hop Redundancy Protocol) is not a routing protocol but a group of protocols (e.g., HSRP, VRRP) to ensure high availability at the default gateway level.
RIP (Routing Information Protocol) does not use autonomous system numbers.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.

NEW QUESTION: 200

A company recently rearranged some users' workspaces and moved several users to previously used workspaces. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the MOST likely reason?

A. Ports are error-disabled.
B. Ports have an incorrect native VLAN.
C. Ports are having an MDIX issue.
D. Ports are trunk ports.
Answer: (SHOW ANSWER)
The most likely cause is that the switch ports were previously configured for a different VLAN than the one the users' computers are on. If the native VLAN on the port doesn't match the end device's VLAN, communication fails.
A). Ports are error-disabled: Would result in no link at all, not common across multiple ports unless a violation occurred.
C). MDIX issue: Auto-MDIX eliminates most crossover problems on modern switches.
D). Ports are trunk ports: While possible, typical user devices should be on access ports, but if the port is incorrectly trunked, it can cause similar issues. However, "incorrect VLAN" is more precise here.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 201
A technician is deploying new networking hardware for company branch offices. The bridge priority must be properly set. Which of the following should the technician configure?
A. Spanning tree protocol
B. Jumbo frames
C. Perimeter network
D. Port security
Answer: (SHOW ANSWER)
Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology. Correctly configuring bridge priority helps in maintaining a loop-free and efficient network. The document explains:

"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

NEW QUESTION: 202
A network administrator wants to increase network security by preventing client devices from communicating directly with each other on the same subnet. Which of the following technologies should be implemented?
A. ACL
B. Trunking
C. Port security
D. Private VLAN
Answer: (SHOW ANSWER)
Private VLANs (PVLANs) are used to segment devices on the same subnet and switch so they cannot communicate with each other, while still accessing a shared resource like a router or gateway. This is often used in shared hosting or DMZ environments.
A). ACLs (Access Control Lists) control traffic between networks, not within the same VLAN.
B). Trunking carries multiple VLANs between switches but does not isolate devices.
C). Port security limits MAC addresses per port but doesn't isolate communication between ports.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.4 - Compare and contrast access control methods.

NEW QUESTION: 203
A network administrator is unable to ping a remote server from a newly connected workstation that has been added to the network. Ping to 127.0.0.1 on the workstation is failing. Which of the following should the administrator perform to diagnose the problem?
A. Verify the NIC interface status.
B. Verify the network is not congested.
C. Verify the router is not dropping packets.
D. Verify that DNS is resolving correctly.
Answer: (SHOW ANSWER)
The failure of a ping to 127.0.0.1 (the loopback address) indicates a problem with the workstation's TCP/IP stack or network interface card (NIC). Since 127.0.0.1 is a local address, the issue is not related to the network, router, or DNS. The first step in diagnosing this issue is to verify the NIC interface status to ensure the network adapter is functioning and properly configured.
Why not Verify the network is not congested? Network congestion affects external connectivity, not the loopback address.
Why not Verify the router is not dropping packets? Router issues are irrelevant since the loopback ping fails locally.

Why not Verify that DNS is resolving correctly? DNS resolution is not involved in pinging 127.0.0.1, which uses a direct IP address.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) emphasizes that a failed loopback ping indicates a local TCP/IP stack or NIC issue, and checking the NIC status is the first diagnostic step.

NEW QUESTION: 204
Which of the following network access methods is used to securely access resources, such as a corporate cloud or network, as if they were directly connected?
A. Jump box/host
B. Secure Shell
C. Client-to-site VPN
D. GRE tunnel
Answer: (SHOW ANSWER)
A client-to-site VPN (remote-access VPN) is designed to let an individual user securely connect into an organization's network over an untrusted network (like the internet) and access resources as if the user were locally connected . Network+ objectives emphasize VPNs as encrypted tunnels that provide confidentiality and integrity for traffic, commonly using technologies such as IPsec or SSL/TLS-based VPNs. With a client- to-site VPN, the user's device establishes a tunnel to the corporate VPN gateway, receives routes (and sometimes DNS settings), and can reach internal subnets and cloud resources according to policy.
A jump box/host is a hardened intermediate system used to access sensitive segments, but it does not make the user's device behave as if it is directly on the network; it provides controlled administrative access. SSH is a secure remote management protocol for connecting to a host's command line-useful for administration, not full network access to multiple internal resources. A GRE tunnel provides encapsulation but does not provide encryption by itself , so it is not inherently "securely access" unless combined with additional security (e.g., GRE over IPsec). Therefore, client-to-site VPN is the correct choice.

NEW QUESTION: 205
Which of the following ports is used for secure email?
A. 25
B. 110
C. 143
D. 587
Answer: (SHOW ANSWER)
Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.
Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.

Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.
Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL
/TLS.
Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.
Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.
Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

NEW QUESTION: 206
A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up.
Which of the following commands should the administrator run on the server first?
A. traceroute
B. netstat
C. tcpdump
D. arp
Answer: (SHOW ANSWER)
Thenetstatcommand provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Runningnetstaton the server can help the administrator verify that the web server process is listening on the expected port (e.g., port 80 for HTTP or port 443 for HTTPS) and that there are no issues with network connections. This is a crucial first step in diagnosing why the web server is not accessible via a browser.References:CompTIA Network+ study materials.

NEW QUESTION: 207
Which of the following offers the ability to manage access at the cloud VM instance?
A. Security group
B. Internet gateway
C. Direct Connect
D. Network ACL
Answer: (SHOW ANSWER)
Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.
From Andrew Ramdayal's guide:

"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC.
They act as a virtual firewall for associated instances..."

NEW QUESTION: 208
Which of the following protocols uses the Dijkstra's Link State Algorithm to establish routes inside its routing table?
A. OSPF
B. EIGRP
C. BGP
D. RIP
Answer: (SHOW ANSWER)
OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.
From Andrew Ramdayal's guide:
"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

NEW QUESTION: 209
An employee in a corporate office clicks on a link in an email that was forwarded to them. The employee is redirected to a splash page that says the page is restricted. Which of the following security solutions is most likely in place?
A. DLP
B. Captive portal
C. Content filtering
D. DNS sinkholing
Answer: (SHOW ANSWER)
Content filtering blocks access to restricted or malicious websites. When a user attempts to visit a site that violates company policies, they are redirected to a restriction page.
* This is a common security measure to prevent employees from accessing phishing or malware-infected sites.
* Content filters work by scanning URLs, keywords, or categories and blocking inappropriate or harmful content.
* Option A (DLP - Data Loss Prevention): Focuses on preventing sensitive data leaks rather than blocking web access.
* Option B (Captive portal): Used mainly in public Wi-Fi to authenticate users before granting access, not to restrict sites.
* Option D (DNS sinkholing): Redirects malicious domain requests to a safe address but is not responsible for policy-based restrictions on general content.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Security Solutions

NEW QUESTION: 210

Employees report that the network is slow. The network engineer thinks the performance issue is with an upstream router. Which of the following tools should the engineer use to determine the location of the issue?

A. nslookup and dig

B. Nmap and speed tester

C. tracert and ping

D. tcpdump and protocol analyzer

Answer: (SHOW ANSWER)

To determine where slowness is occurring-especially if an upstream router is suspected-the best tools are ping and tracert/traceroute . Network+ (N10-009) troubleshooting objectives emphasize using these to test connectivity, latency, and the path packets take through the network. Ping measures reachability and round- trip time; rising latency or packet loss can indicate congestion or a failing link/device. Tracert identifies each hop along the route and reports per-hop response times, helping pinpoint whether delays begin at a specific hop (for example, the default gateway, the upstream router, or a provider edge). This allows the engineer to localize the problem area and decide whether the issue is internal, at the upstream router, or beyond.

nslookup and dig are DNS tools; they diagnose name resolution, not general network slowness location.

Nmap focuses on scanning ports/hosts, and a "speed tester" measures throughput but does not locate the failing hop. tcpdump and protocol analyzer can reveal retransmissions, windowing, or application behavior, but they are not the fastest first-choice tools for locating an upstream routing/performance bottleneck across hops. Hence, tracert and ping are the correct pair.

NEW QUESTION: 211

Which of the following VPN configurations forces a remote user to access internet resources through the corporate network?

A. Clientless

B. Site-to-site

C. SSE

D. Full-tunnel

Answer: (SHOW ANSWER)

A full-tunnel VPN forces a remote user's traffic-including access to public internet resources-to traverse the corporate VPN tunnel and egress from the organization's network. This is commonly required to ensure consistent enforcement of corporate security controls such as web filtering, IDS/IPS inspection, DLP policies, logging, and access control. In Network+ terms, full-tunnel VPNing routes the user's default gateway through the VPN, meaning both internal traffic (to corporate subnets) and external traffic (to internet destinations) is sent through the encrypted tunnel.

By contrast, a split-tunnel VPN (not listed) would send only corporate-bound traffic through the VPN while allowing internet traffic to go directly out the user's local ISP-reducing corporate

bandwidth usage but also reducing centralized inspection and control. Clientless VPN usually refers to browser-based access to specific internal applications without a full network tunnel for all traffic. Site-to-site VPN connects entire networks to each other (e.g., branch office to HQ) rather than an individual remote user. SSE (Security Service Edge) is a cloud security framework/service model, not the classic VPN configuration described in the question. Hence, full-tunnel is the correct answer.

NEW QUESTION: 212
Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?
A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO
Answer: (SHOW ANSWER)
802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.
A). Standard ACL filters traffic by IP, not identity.
B). MAC filtering controls devices by hardware address but can be spoofed.
D). SSO (Single Sign-On) provides user convenience across services, not network-level access control.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, identity-based access.

NEW QUESTION: 213
During a security audit, a consulting firm notices inconsistencies between the documentation and the actual environment. Which of the following can keep a record of who made the changes and what the changes are?
A. Network access control
B. Configuration monitoring
C. Zero Trust

D. Syslog

Answer: (SHOW ANSWER)

Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.

A). Network access control (NAC) manages endpoint access policies but does not track device config changes.

C). Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.

D). Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Change management, configuration management, auditing.

NEW QUESTION: 214

Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?

A. Infrastructure as a service

B. Software as a service

C. Platform as a service

D. Network as a service

Answer: (SHOW ANSWER)

Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

NEW QUESTION: 215

A network administrator needs to ensure that users accept internet usage rules. Which of the following will help the administrator accomplish this task?

A. Captive portal

B. Acceptable use policy

C. Network access control

D. DNS filtering

Answer: (SHOW ANSWER)

A captive portal is designed to present terms, conditions, or usage rules to users and require them to acknowledge/accept those rules before granting network or internet access. In Network+ (N10-009) security and access control concepts, captive portals are commonly associated with guest wireless or public access scenarios, where users are redirected to a web page that displays acceptable-use language and requires a click- through acceptance (and sometimes authentication). This provides a technical enforcement point: users must actively accept the rules to proceed, which supports organizational policy compliance and creates a recordable control in many implementations.

An Acceptable Use Policy (AUP) is the document that defines the rules, but by itself it does not technically force a user to acknowledge them at the time of access. NAC controls who/what can connect and can enforce posture and segmentation, but it does not inherently ensure users "accept" usage rules unless paired with a portal workflow. DNS filtering blocks or allows domain access categories (malware, adult content, etc.), which enforces browsing restrictions but does not guarantee user acceptance of rules. Therefore, the best answer to ensure users accept the rules is captive portal.

NEW QUESTION: 216
A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?
A. 802.11a
B. 802.11b
C. 802.11g
D. 802.11n
Answer: D (LEAVE A REPLY)
The 802.11n standard supports MIMO (Multiple Input Multiple Output), which allows multiple antennas to increase data throughput and improve reliability. Additionally, it uses non-overlapping channels in the 5 GHz band (and optionally the 2.4 GHz band), making it a good choice for high-speed, interference-resistant wireless connections. (Reference: CompTIA Network+ Study Guide, Chapter on Wireless Technologies)

NEW QUESTION: 217
Which of the following allows a network administrator to analyze attacks coming from the internet without affecting latency?
A. IPS
B. IDS
C. Load balancer
D. Firewall
Answer: (SHOW ANSWER)
An IDS (Intrusion Detection System) is deployed out-of-band, meaning it passively monitors network traffic using a SPAN/mirror port or network tap. It detects and analyzes suspicious traffic without introducing latency since it does not sit in-line.
A). IPS (Intrusion Prevention System) is in-line and can block traffic but may add latency.
C). Load balancer distributes traffic across servers for performance and redundancy, not for threat detection.
D). Firewall filters traffic at the perimeter or internally; it can affect latency but does not provide the same in- depth attack analysis.
References (CompTIA Network+ N10-009):
Domain: Network Security - IDS vs. IPS, in-band vs. out-of-band monitoring, passive detection methods.

NEW QUESTION: 218
Which of the following would an adversary do while conducting an evil twin attack?
A. Trick users into using an AP with an SSID that is identical to a legitimate network
B. Manipulate address resolution to point devices to a malicious endpoint
C. Present an identical MAC to gain unauthorized access to network resources
D. Capture data in transit between two legitimate endpoints to steal data
Answer: A (LEAVE A REPLY)
An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting. Once connected, the attacker can intercept traffic or harvest credentials.
B). Describes ARP spoofing.
C). Describes MAC spoofing.
D). Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats, rogue APs, evil twin.

NEW QUESTION: 219
A network administrator changed an external DNS to point customers to a new server. Which of the following tools should the administrator use to test the new server's configuration?
A. ping
B. tracert
C. tcpdump
D. nslookup
Answer: (SHOW ANSWER)
*nslookup allows querying DNS records to verify if the new server is correctly resolving domain names.
*ping (A) tests basic connectivity, not DNS configuration.
*tracert (B) shows network path latency but doesn't test DNS.
*tcpdump (C) captures packets but isn't ideal for DNS verification.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Testing Tools.

NEW QUESTION: 220
Which of the following tools uses ICMP to help determine whether a network host is reachable?
A. tcpdump
B. netstat
C. nslookup
D. ping
Answer: (SHOW ANSWER)

Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.
A). tcpdump captures packets but does not test reachability.
B). netstat displays open ports and network sessions.
C). nslookup queries DNS servers for name resolution.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - ICMP operation, troubleshooting tools.

NEW QUESTION: 221
A network administrator installs wireless access points (APs) inside an industrial warehouse. A wireless survey shows a large amount of electromagnetic interference. Which of the following cable types should the administrator use to connect the APs to the switch?
A. UTP
B. STP
C. Multimode
D. Single-mode
Answer: (SHOW ANSWER)
The correct answer is STP (Shielded Twisted Pair). According to the CompTIA Network+ N10-009 objectives, environments with high levels of electromagnetic interference (EMI)-such as industrial warehouses with heavy machinery, motors, and electrical equipment-require additional protection at the physical layer to maintain signal integrity.
STP cabling includes shielding around the twisted copper pairs that helps block external electromagnetic signals from interfering with data transmission. This shielding significantly reduces crosstalk and EMI, making STP far more suitable than UTP (Unshielded Twisted Pair) in electrically noisy environments. UTP lacks this shielding and is more prone to signal degradation under such conditions.
While fiber-optic cabling (multimode or single-mode) is completely immune to EMI, it is typically not used to directly connect wireless APs in most enterprise deployments. Wireless access points commonly rely on copper Ethernet connections to support Power over Ethernet (PoE), which supplies both data and electrical power over the same cable. Fiber does not natively support PoE, making it impractical for directly powering APs without additional equipment.
The Network+ objectives emphasize selecting appropriate cabling based on environmental factors and operational requirements. In this scenario, STP provides the optimal balance of EMI resistance, Ethernet compatibility, and PoE support, making it the best choice for connecting APs in an industrial warehouse.

NEW QUESTION: 222
A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space.
Which of the following subnets should the administrator use?
A. 724

B. /26
C. /28
D. /30
Answer: (SHOW ANSWER)
Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.References: CompTIA Network+ study materials and subnetting principles.

NEW QUESTION: 223
Which of the following protocols is commonly associated with TCP port 443?
A. Telnet
B. SMTP
C. HTTPS
D. SNMP
Answer: (SHOW ANSWER)
TCP port 443 is reserved for HTTPS (Hypertext Transfer Protocol Secure), which uses TLS encryption to secure web traffic. It is the standard port for encrypted web communications.
A). Telnet uses TCP port 23.
B). SMTP commonly uses TCP ports 25, 465, or 587.
D). SNMP typically uses UDP ports 161 (queries) and 162 (traps).
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Common ports and services.

NEW QUESTION: 224
Which of the following is used most often when implementing a secure VPN?
A. IPSec
B. GRE
C. BGP
D. SSH
Answer: A (LEAVE A REPLY)
The most common protocol for secure VPNs is IPsec (Internet Protocol Security). IPsec provides confidentiality, integrity, and authentication for VPN traffic, typically using ESP (Encapsulating Security Payload). It is used in both site-to-site and remote access VPNs.
B). GRE encapsulates traffic but does not provide encryption.
C). BGP is a routing protocol, not a VPN technology.
D). SSH can be used for secure tunneling but is not the standard for VPN deployment.
IPsec is the industry standard because it operates at Layer 3, securing IP traffic regardless of the application, making it highly versatile.
References (CompTIA Network+ N10-009):

Domain: Network Security - VPN protocols, IPsec, ESP.

NEW QUESTION: 225
A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?
A. EIGRP
B. OSPFv3
C. BGP4
D. iBGP
Answer: (SHOW ANSWER)
For an internal network using IPv6, the best option listed is OSPFv3, which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence.
BGP4 and iBGP are associated with BGP, primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor- neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.