CompTIA.N10-009.v2026-09-14.q244

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	244
Version:	v2026-09-14
# of views:	104
# of Questions views:	2475
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-09-14.q244.html	

NEW QUESTION: 1
Which of the following is the best example of a networking appliance that connects different network segments and directs allowed traffic between specific segments?
A. Firewall
B. IDS
C. Unmanaged switch
D. (Not provided)
Answer: (SHOW ANSWER)
A firewall is the best example of an appliance that can sit between network segments and permit or deny traffic flows based on security policy. In Network+ terms, firewalls enforce segmentation controls by applying rules that match on items such as source/destination IP, ports, protocols, and (with next-generation firewalls) even applications. This makes a firewall a common choice for directing allowed traffic between specific segments (for example, allowing users in a workstation VLAN to reach only certain ports on a server VLAN, while blocking everything else). This function is core to network security architecture and is frequently paired with concepts like network segmentation, ACL-style rule sets, and creating security zones.
An IDS (intrusion detection system) primarily monitors traffic and generates alerts on suspicious activity; it does not typically control or "direct allowed traffic" unless it is specifically an IPS (prevention) with inline blocking. An unmanaged switch operates at Layer 2 and forwards frames within a broadcast domain; it does not provide policy-based filtering between security segments. Therefore, the correct answer is Firewall.

NEW QUESTION: 2
A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?
A. The parabolic signal is misaligned.
B. The omnidirectional signal is being jammed.
C. The omnidirectional signal is not strong enough to receive properly.
D. The parabolic signal uses improper routing protocols.
Answer: (SHOW ANSWER)
A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.
The document confirms:
"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

NEW QUESTION: 3
An attack on an internal server is traced to an isolated guest network. Which of the following best describes the attack?
A. On-path
B. DNS poisoning
C. VLAN hopping
D. ARP spoofing
Answer: (SHOW ANSWER)
The correct answer is VLAN hopping, which is a Layer 2 attack specifically associated with bypassing network segmentation controls. According to the CompTIA Network+ N10-009 objectives, VLANs are commonly used to isolate traffic between different network segments, such as separating a guest network from internal production systems. When an attack originates from an isolated guest network and successfully reaches an internal server, it strongly indicates a failure or exploitation of VLAN boundaries.
VLAN hopping occurs when an attacker gains access to traffic on another VLAN by exploiting misconfigured switch ports or trunking protocols. Common techniques include switch spoofing, where the attacker pretends to be a switch to negotiate a trunk link, and double-tagging, where two VLAN tags are inserted to trick switches into forwarding traffic across VLANs.
The other options do not best fit this scenario. An on-path (man-in-the-middle) attack requires interception between two communicating hosts but does not inherently bypass VLAN isolation. DNS poisoning manipulates name resolution, not network segmentation. ARP spoofing affects local Layer 2 address resolution within the same broadcast domain and typically cannot cross VLAN boundaries.
The Network+ objectives emphasize proper VLAN configuration, disabling unused trunk ports, and implementing port security to prevent VLAN hopping attacks. In this case, VLAN hopping most accurately explains how a guest network could access internal servers.

NEW QUESTION: 4
A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business.
When attempting to connect, two networks are listed as possible choices: SSID: business and SSID:
myaccess. Which of the following attacks is occurring?
A. On-path
B. Rogue AP
C. Evil twin
D. Tailgating
Answer: (SHOW ANSWER)
An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.
A). On-path is the consequence of connecting to the evil twin, not the initial attack itself.
B). Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID
- specifically an evil twin.
D). Tailgating is a physical social engineering attack, unrelated to Wi-Fi.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs, evil twins).

NEW QUESTION: 5
Which of the following impacts the availability of a web-based customer portal?
A. MAC flooding

B. ARP spoofing
C. DoS
D. Rogue devices
Answer: (SHOW ANSWER)
A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.
MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability. ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

NEW QUESTION: 6
Which of the following network cables involves bouncing light off of protective cladding?
A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber.
This is effective for shorter distances but more prone to dispersion.
A). Twinaxial is copper, not fiber.
B). Coaxial carries electrical signals, not light.
C). Single-mode fiber uses a single light path directly through the core without bouncing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Fiber optics: single-mode vs. multimode.

NEW QUESTION: 7
Which of the following best describes the transmission format that occurs at the transport layer over connectionless communication?
A. Datagram
B. Segment
C. Frames
D. Packets
Answer: (SHOW ANSWER)
At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 8

A network administrator needs to locate a specific AP using a spectrum analyzer to complete an 802.11ax device migration. Which of the following should display on the analyzer to locate the AP?

A. SSID

B. RSSI

C. Channel number

D. BSSID

Answer: (SHOW ANSWER)

To locate a specific access point (AP), the most reliable identifier to view is the BSSID. In 802.11 networks, the BSSID is the radio interface identifier for the AP (typically the AP radio's MAC address). Unlike an SSID, which can be shared across many APs in the same wireless network (especially in an enterprise deployment using the same SSID across multiple APs), the BSSID uniquely distinguishes one AP radio from another. This is critical during an 802.11ax (Wi-Fi 6) migration, where multiple APs may broadcast identical SSIDs and operate on the same channels in different areas.

While RSSI is useful for physically walking toward the strongest signal (a technique used in locating RF sources), RSSI alone does not confirm you are tracking the correct AP-only that you are near an RF transmitter. Channel number also does not uniquely identify the AP because multiple APs can share the same channel (and channels may overlap depending on band and width). SSID similarly is not unique. Therefore, viewing the BSSID on the analyzer (or Wi-Fi analyzer mode) allows the administrator to confirm the exact AP being measured and located.

NEW QUESTION: 9

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: 10

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.

Freecram.net

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: 11
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: 12
Which of the following types of network architecture typically uses leased lines to provide dedicated, private connections between multiple satellite offices and a head office?
A. Mesh
B. Point to point
C. Hub and spoke
D. Star
Answer: (SHOW ANSWER)
The correct answer is hub-and-spoke. In this design, the head office serves as the hub, and all satellite or branch offices (the spokes) connect directly to the hub using leased lines or VPNs. Communication between spokes typically passes through the hub, which centralizes connectivity and simplifies management.
A). Mesh involves every site connecting to every other site, which is more redundant but costly.
B). Point-to-point describes a single dedicated link between two sites, not a multi-site topology.
D). Star is often used in LAN switching, with all devices connecting to a central switch, but it's not the WAN architecture typically used here.
Hub-and-spoke is a cost-effective WAN design, as fewer circuits are needed compared to full mesh. However, its main disadvantage is reliance on the hub site: if the hub goes down, inter-spoke communication fails.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - WAN topologies (hub-and-spoke, mesh, point-to-point).

NEW QUESTION: 13
A technician is troubleshooting performance and connectivity issues associated with a web server. The technician wants to examine the packets to and from the server but has the following requirements:

* Capture 100% of packets
* Capture all Layer 1 error packets
* Minimize the impact on infrastructure

Which of the following best meets these requirements and allows for the packet capture?

A. Running Nmap from the web server
B. Installing a network tap in-line with the web server
C. Installing a protocol analyzer on the web server
D. Configuring port mirroring on the switch

Answer: (SHOW ANSWER)

The correct answer is B. Installing a network tap in-line with the web server. A network tap (Test Access Point) is a hardware device placed directly in-line between network devices, allowing it to capture all traffic flowing across the link. Because it operates at the physical layer, a tap can capture 100% of packets, including malformed frames and Layer 1 errors, which are often missed by other methods.

This solution also minimizes impact on infrastructure, as taps are passive devices that do not introduce significant latency or processing overhead. They do not rely on switch configuration or consume switch resources, making them ideal for high-fidelity packet capture during troubleshooting.

Other options do not meet all requirements. Port mirroring (SPAN) can capture traffic but may drop packets under heavy load and typically does not capture Layer 1 errors. Installing a protocol analyzer on the server only captures traffic processed by the server's NIC and may miss certain low-level issues. Running Nmap is an active scanning tool used for discovery and security auditing, not packet capture.

Therefore, a network tap is the best solution for complete, accurate, and low-impact packet capture.

NEW QUESTION: 14

Which of the following indicates a computer has reached end-of-support?

A. The computer does not have any users.
B. The antivirus protection is expired.
C. The operating system license is expired.
D. No more patches or bug fixes are available indefinitely.

Answer: (SHOW ANSWER)

A system has reachedend-of-supportwhen thevendor no longer provides patches, updates, or bug fixes. This significantly increases the risk of security vulnerabilities and is a major operational concern.

Reference:Section 3.3 - Disaster Recovery Concepts - "End-of-Support Considerations"

NEW QUESTION: 15

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: 16
Which of the following is the best way to reduce the likelihood of electrostatic discharge?
A. Uninterruptible power supply
B. Surge protector
C. Power distribution units
D. Temperature and humidity control
Answer: (SHOW ANSWER)
Temperature and humidity controlis the best way to reduce the risk of electrostatic discharge (ESD). Dry environments significantly increase the likelihood of static buildup, which can discharge and damage sensitive components. By controlling humidity, the environment becomes less prone to static electricity.
Reference:Section 2.4 - Important Factors of Physical Installations - "Environmental Considerations"

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
Which of the following connection methods allows a network engineer to automate configuration deployment for network devices across the environment?
A. RDP
B. Telnet
C. SSH
D. GUI
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
SSH provides secure, scriptable remote access used by automation/orchestration tools (e.g., leveraging CLI, NETCONF over SSH, or Ansible modules) to push configurations at scale.
* A. RDP is primarily for Windows GUI sessions and is not commonly used for network device automation.
* B. Telnet can be scripted but is insecure (plaintext); modern best practice is to use SSH.
* D. GUI access is typically manual and not ideal for scalable, repeatable automation.
References (CompTIA Network+ N10-009):
* Domain: Network Operations - Configuration management, automation/orchestration, secure management protocols (SSH vs. Telnet), change at scale.

NEW QUESTION: 18
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.

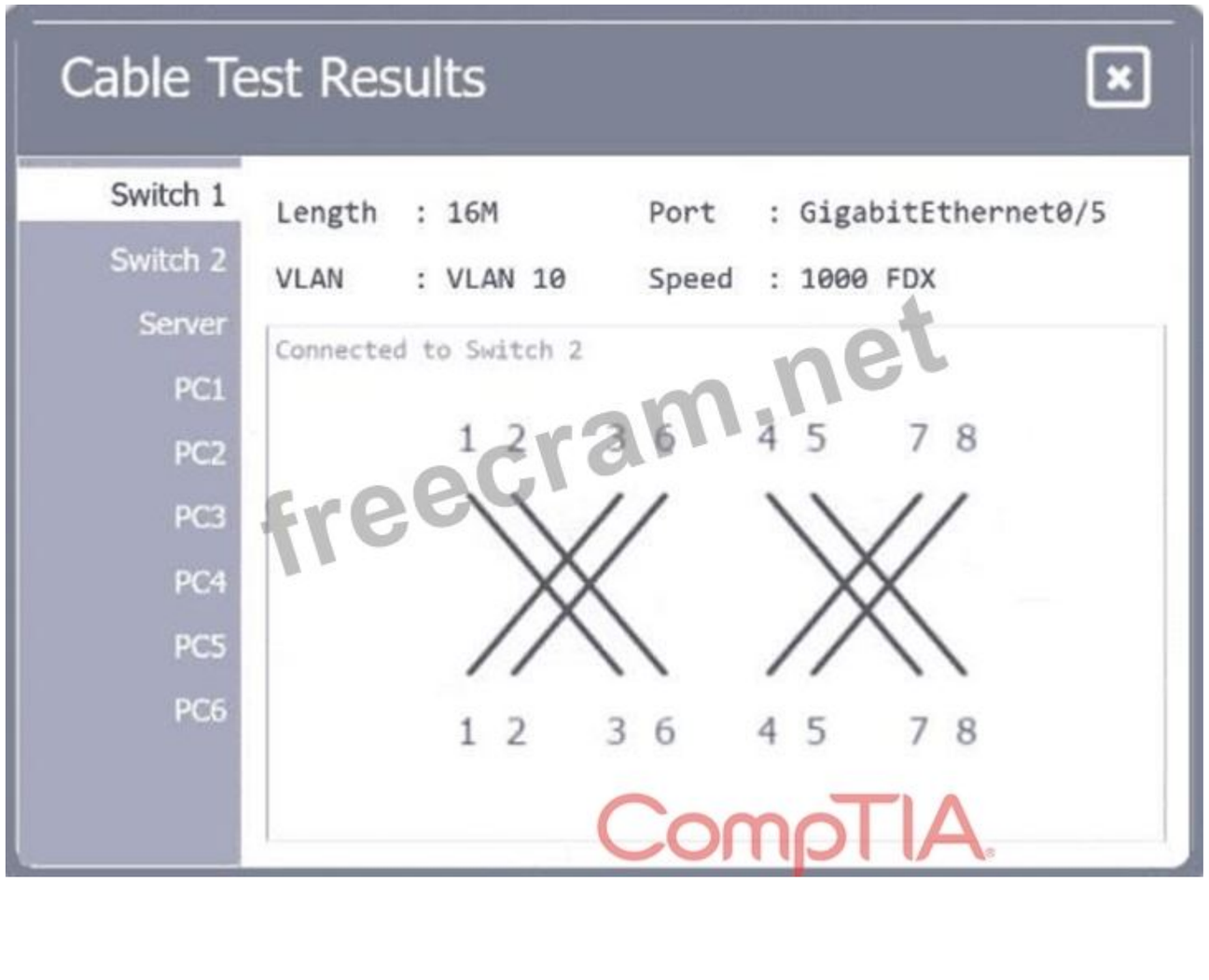
NEW QUESTION: 19
A firewall administrator is mapping a server's internal IP address to an external IP address for public use.
Which of the following is the name of this function?
A. NAT
B. VIP
C. PAT
D. BGP
Answer: (SHOW ANSWER)
Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.
Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.
Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.
PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.
Incorrect Options:
B). VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.
C). PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.
D). BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

NEW QUESTION: 20
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
Freecram.net
Which of the following describes the issue?
A. The server has an incorrect subnet mask

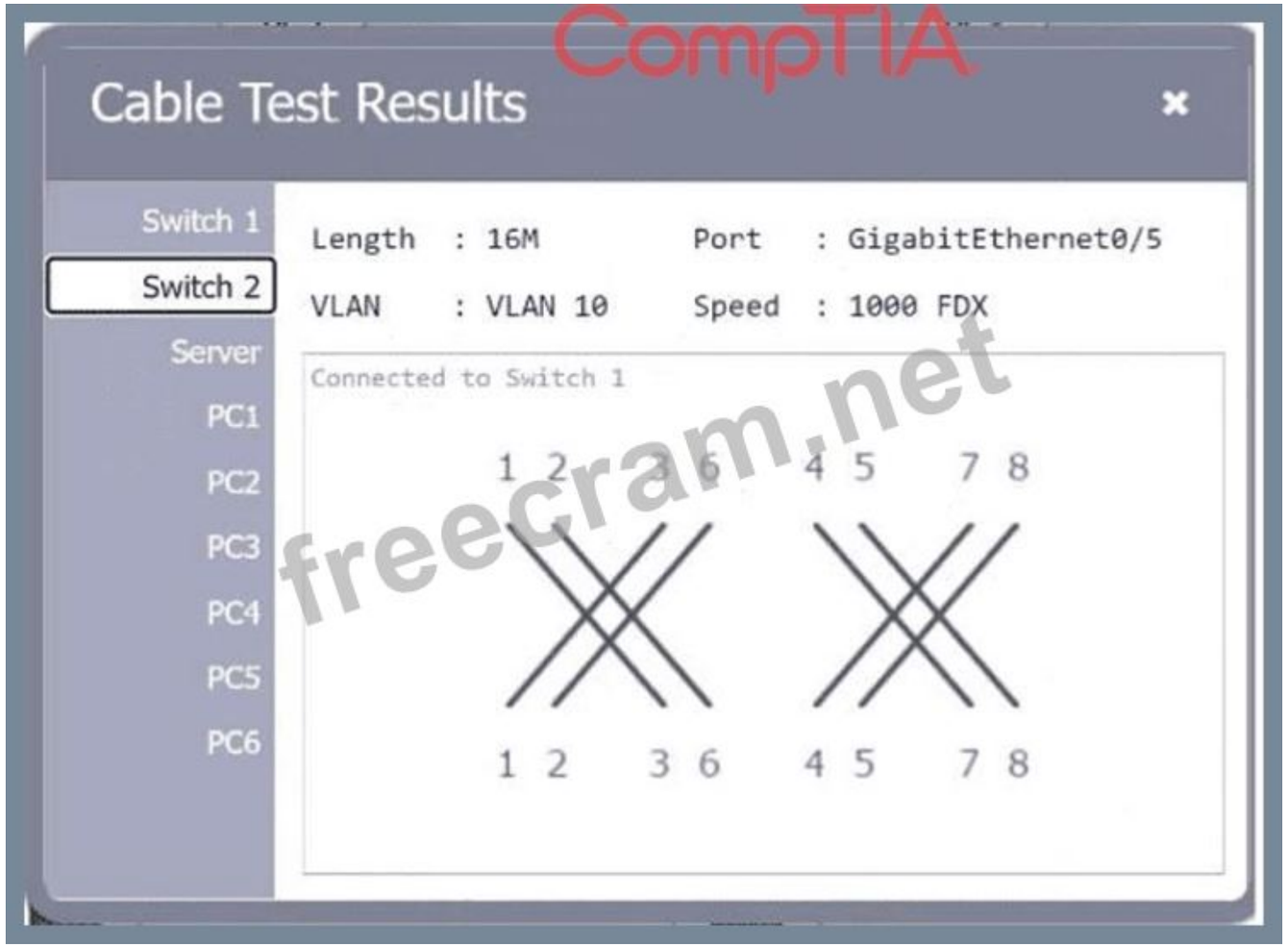
B. There is a duplicate IP address on the network
C. The DHCP address pool is exhausted
D. The router is missing a default route
Answer: (SHOW ANSWER)
The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to
192.168.100.255. However, the router only recognizes 192.168.100.0/24, 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: 21
A network technician is configuring the company's network of 100 Mbps Layer 2 switches. The technician wants increased throughput for the uplinks between switches. The technician connects multiple redundant links between the switches. Which of the following should the technician configure?
A. Spanning Tree Protocol
B. Switch Virtual Interfaces
C. Native VLAN
D. First Hop Redundancy Protocol
Answer: (SHOW ANSWER)
When multiple redundant links exist between switches, Spanning Tree Protocol (STP) is required to prevent switching loops. STP blocks redundant paths but can allow aggregation if configured with protocols like LACP.
B). SVIs provide Layer 3 interfaces, not loop prevention.
C). Native VLAN defines the untagged VLAN but does not manage loops.
D). FHRP (VRRP, HSRP, GLBP) provides gateway redundancy, not switch uplink management.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - STP, redundancy, loop prevention.

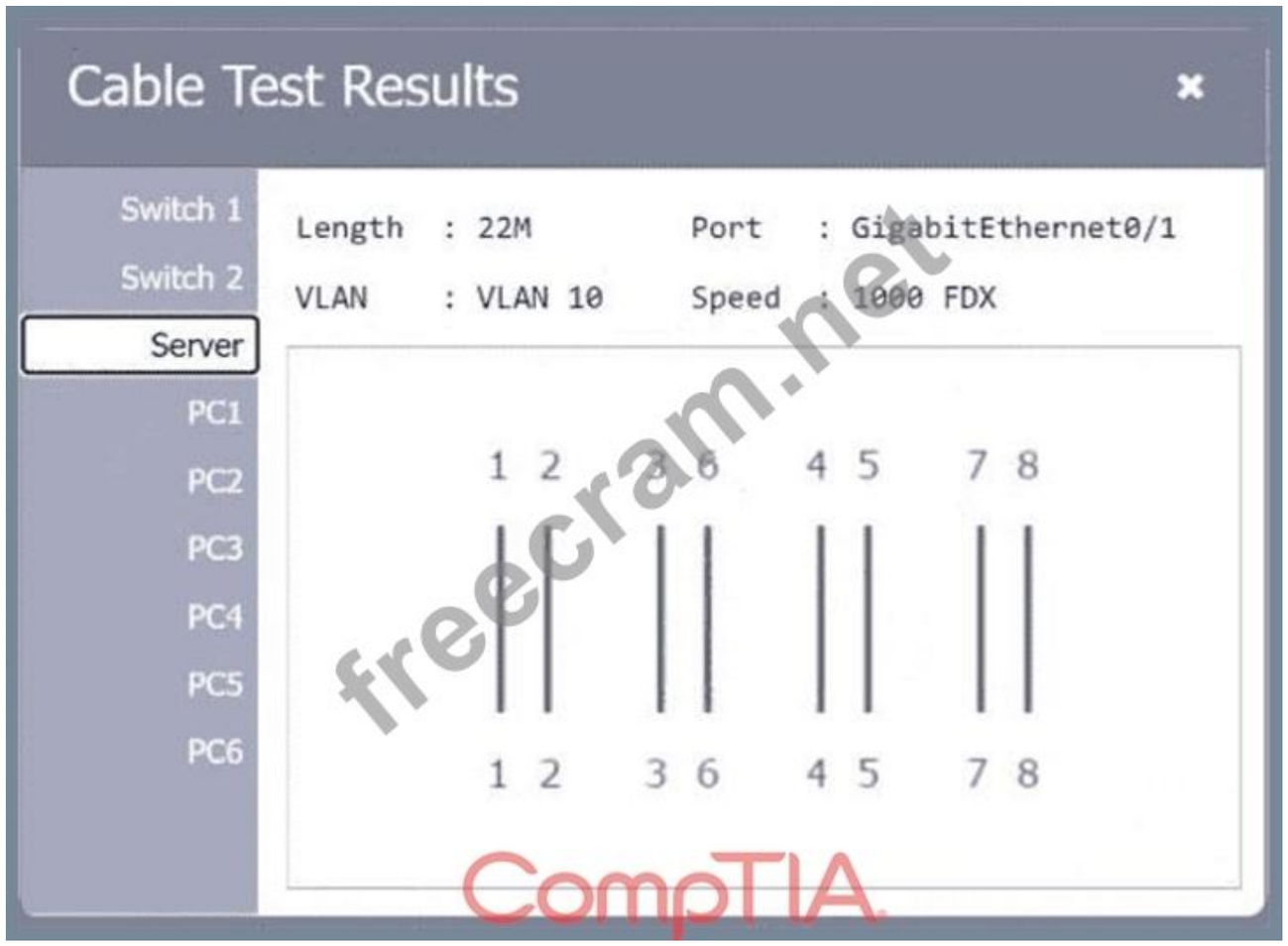
NEW QUESTION: 22
A network technician needs to resolve some issues with a customer ' s SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.
INSTRUCTIONS
Troubleshoot all the network components.
Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.
Identify any components with a problem and recommend a solution to correct each problem.
If at any time you would like to bring back
the initial state of the simulation, please
click the Reset All button.


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 16M
Port : GigabitEthernet0/5
VLAN : VLAN 10
Speed : 1000 FDX
Connected to Switch 2
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8
freecram.net
CompTIA

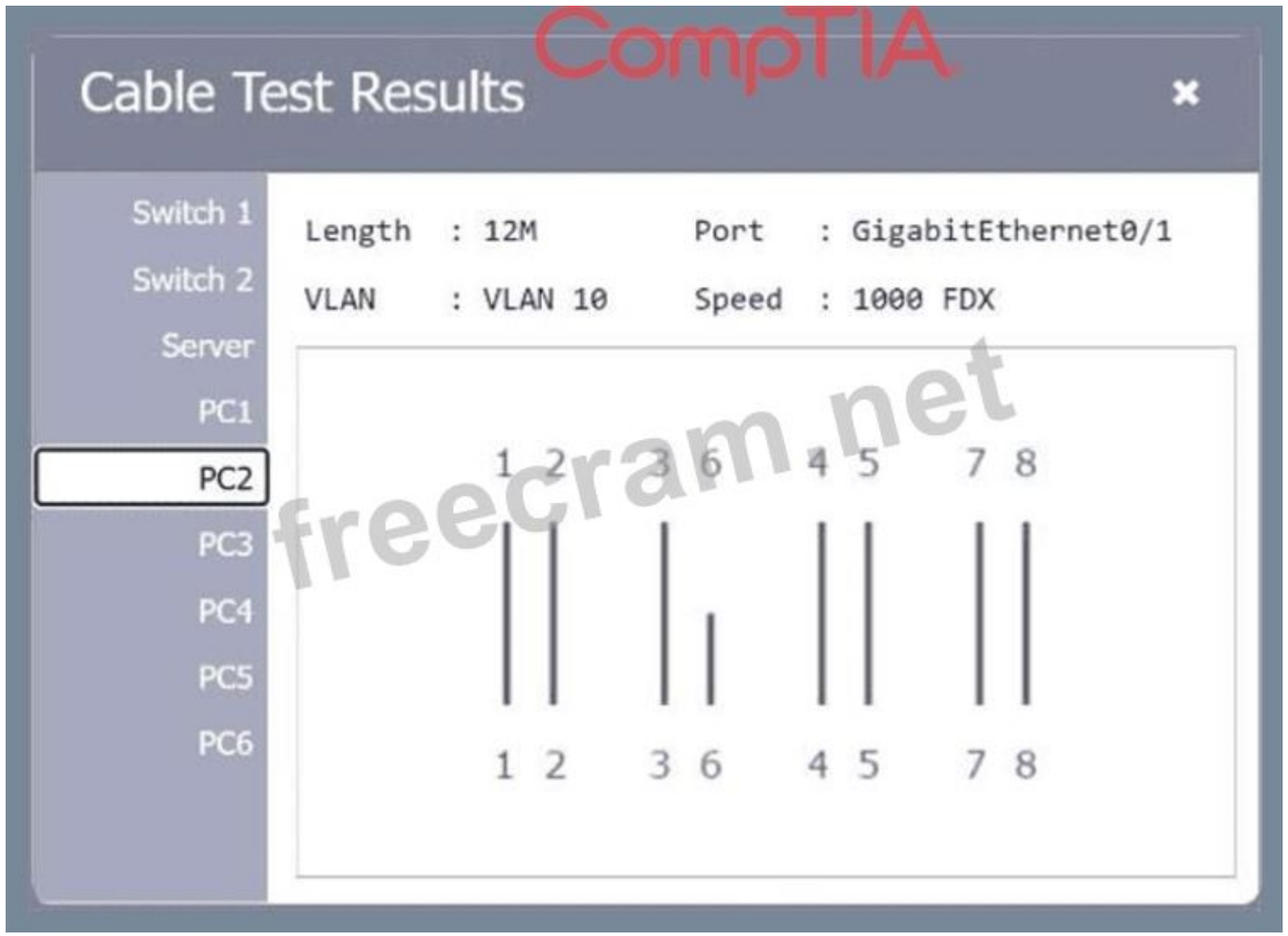
CompTIA



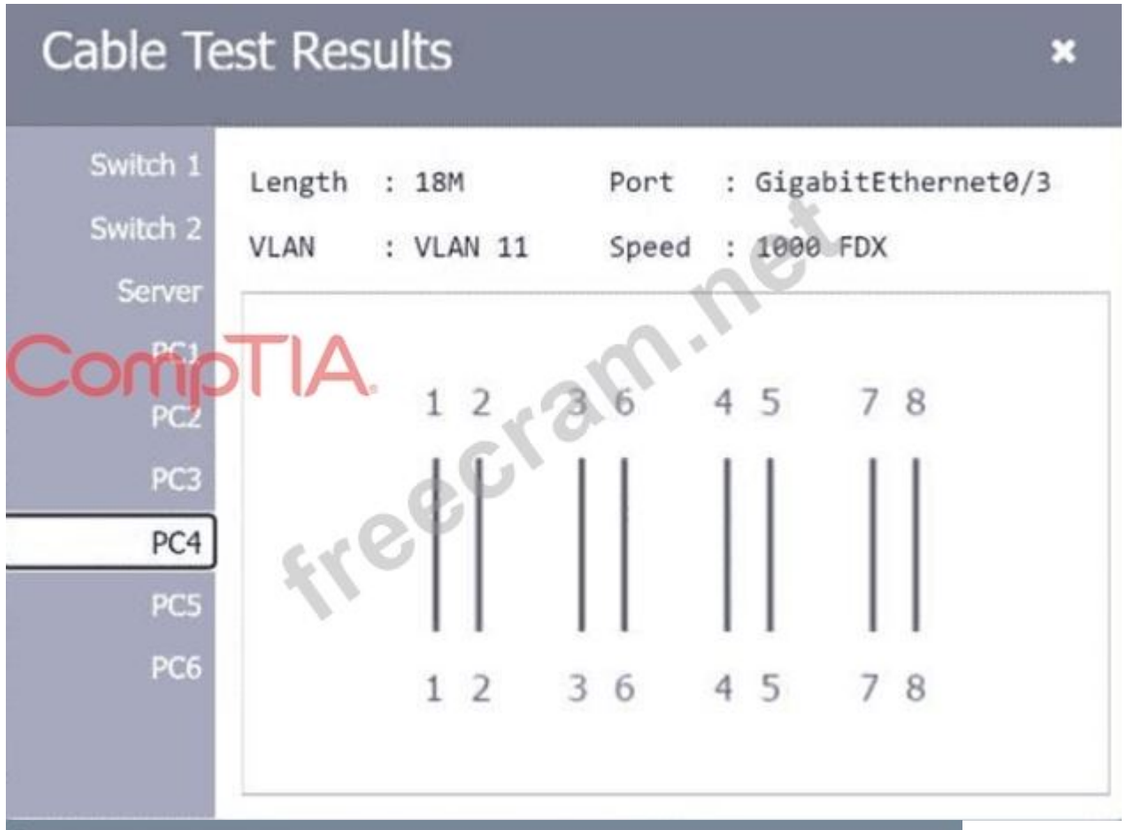
freecram.net

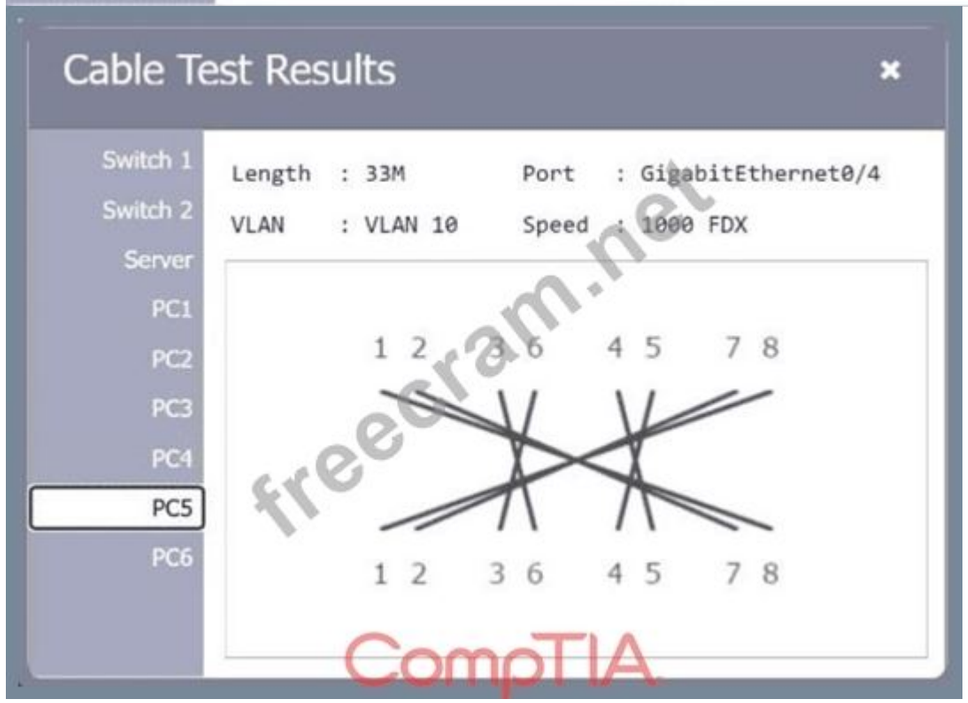


freecram.net
CompTIA

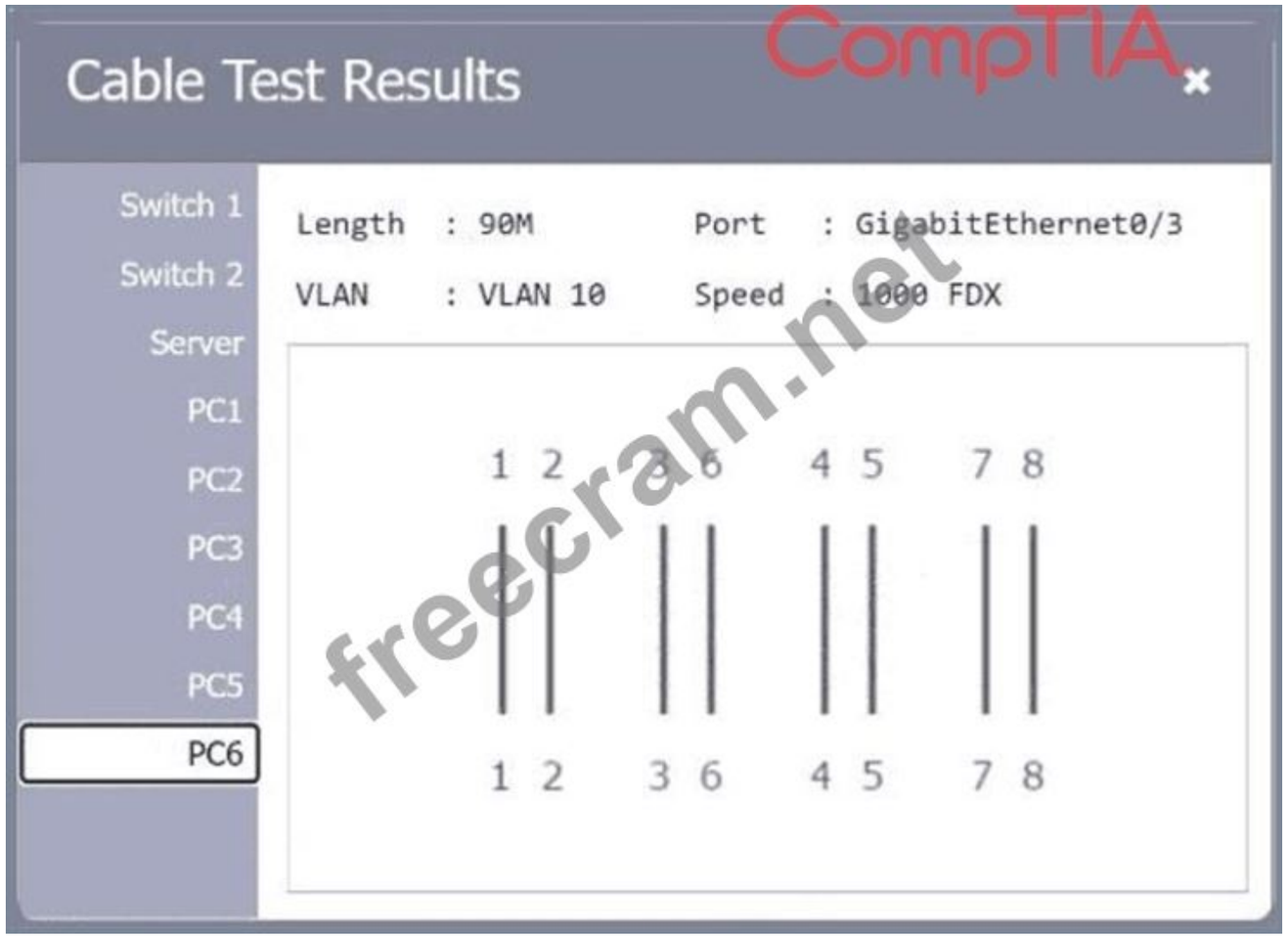


CompTIA
freecram.net





CompTIA
freecram.net



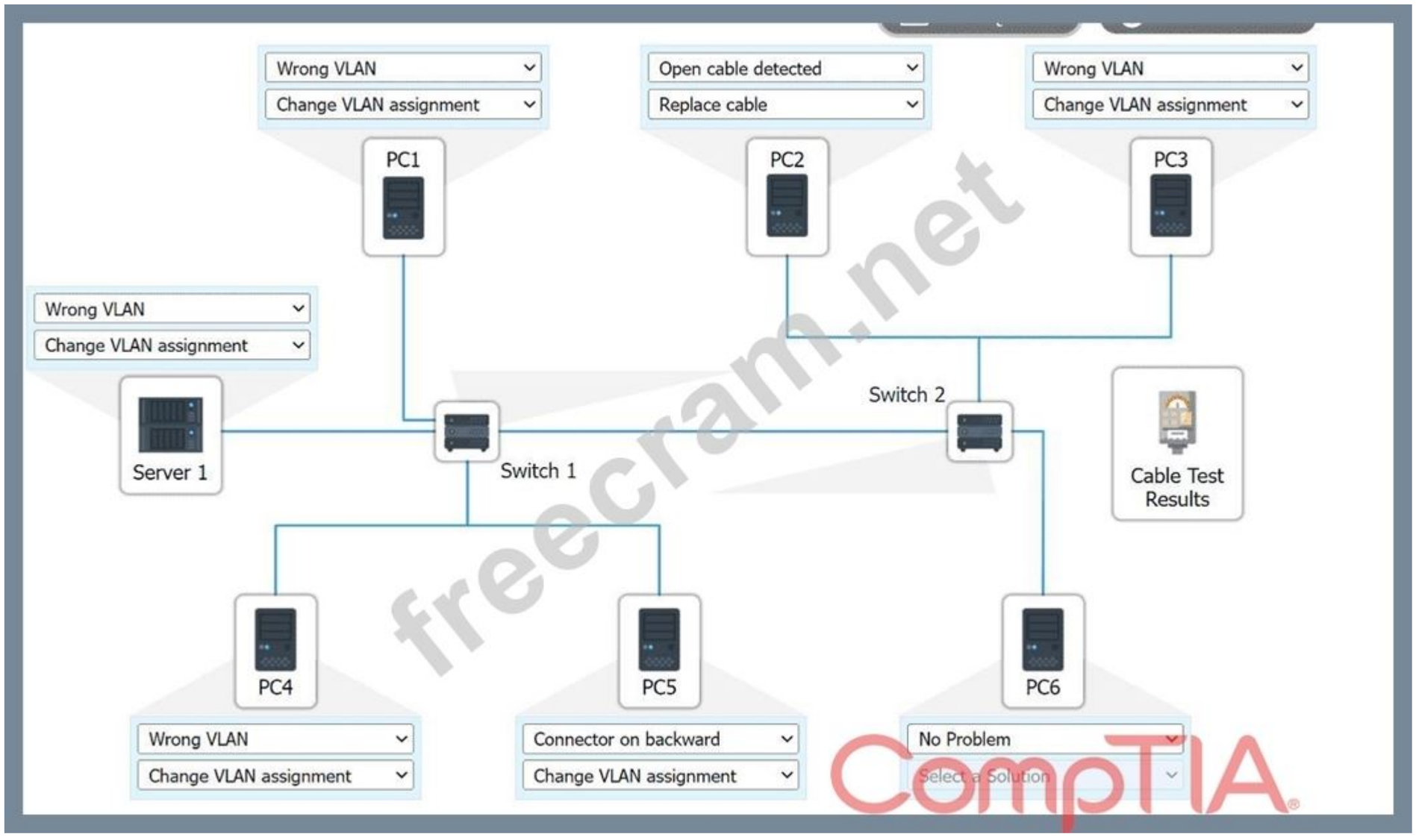
freecram.net

Answer:

See the answer and solution below:

Explanation:

A computer network diagram with many boxes and text AI-generated content may be incorrect.



NEW QUESTION: 23
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: 24
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: D (LEAVE A REPLY)
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: 25
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

freecram.net
CompTIA
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: 26
Which of the following is a cost-effective advantage of a split-tunnel VPN?
A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.
Answer: (SHOW ANSWER)
A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.
* Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.
* Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.
* Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.
* Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.
* Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.
By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

NEW QUESTION: 27
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: 28
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: 29
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: 30
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?
Freecram.net
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: 31
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: A (LEAVE A REPLY)
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
Which of the following is the best way to keep devices on during a loss of power?
A. UPS
B. Power load
C. PDU
D. Voltage
Answer: (SHOW ANSWER)
A UPS (Uninterruptible Power Supply) provides backup power to devices during a power outage, allowing for continuous operation and protecting against sudden shutdowns that could cause data loss or equipment damage. The document confirms:

"A UPS (Uninterruptible Power Supply) is essential for maintaining power to critical devices during an outage, protecting data and ensuring continuous operation until power is restored or a safe shutdown can be performed."

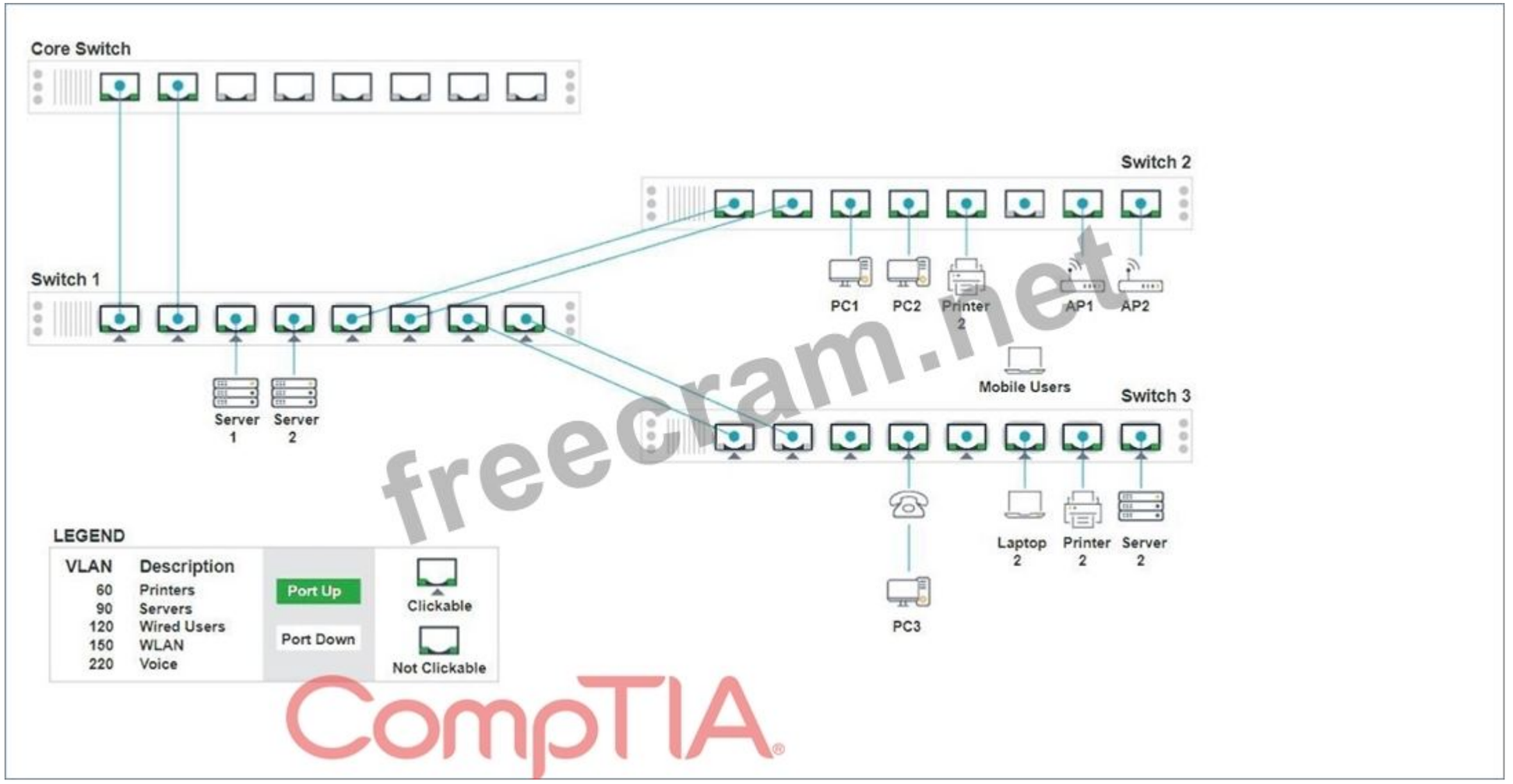
NEW QUESTION: 33
A company reports that their facsimile machine no longer has a dial tone when trying to send a fax. The phone cable is damaged on one end. Which of the following types of connectors should a technician replace?
A. F-type
B. RJ45
C. SC
D. RJ11
Answer: D (LEAVE A REPLY)
Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.
F-type is used for coaxial cables (e.g., TV and cable modems).
RJ45 is used for Ethernet network connections.
SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.4 - Compare and contrast common network connectors.

NEW QUESTION: 34
An IT department is considering implementing a SIEM solution to improve network security. The department wants to ensure that the SIEM system is able to ingest and analyze logs from all of the company's core devices. Which of the following is the most important consideration when selecting a SIEM solution?
A. Easy to manage
B. Cost
C. Compatibility
D. Features
Answer: (SHOW ANSWER)
The correct answer is C. Compatibility . A SIEM is only effective if it can successfully collect, normalize, and analyze data from the systems the organization relies on. Since the question specifically says the department wants the SIEM to ingest and analyze logs from all core devices , the most important factor is whether the SIEM is compatible with those devices, their log formats, and their supported methods of exporting events.
This includes support for common logging methods such as syslog , SNMP traps, API integrations, agent- based collection, and vendor-specific event formats. Even a SIEM with excellent features will not deliver value if it cannot properly receive and interpret logs from firewalls, routers, switches, servers, and security appliances already in use.
The other choices matter, but they come after compatibility. Ease of management is helpful for daily operations. Cost is always a practical concern. Features can improve visibility and automation. However, none of those benefits matter much if the SIEM cannot integrate with the organization's actual environment.
For Network+ exam purposes, when log ingestion across many device types is the requirement, the top selection criterion is compatibility . Without that foundation, correlation, alerting, and security analysis will be incomplete.

NEW QUESTION: 35
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: 36
A network technician replaced an access layer switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
Ensure each device accesses only its
correctly associated network.
Disable all unused switchports.
. Require fault-tolerant connections
between the switches.
. Only make necessary changes to
complete the above requirements.

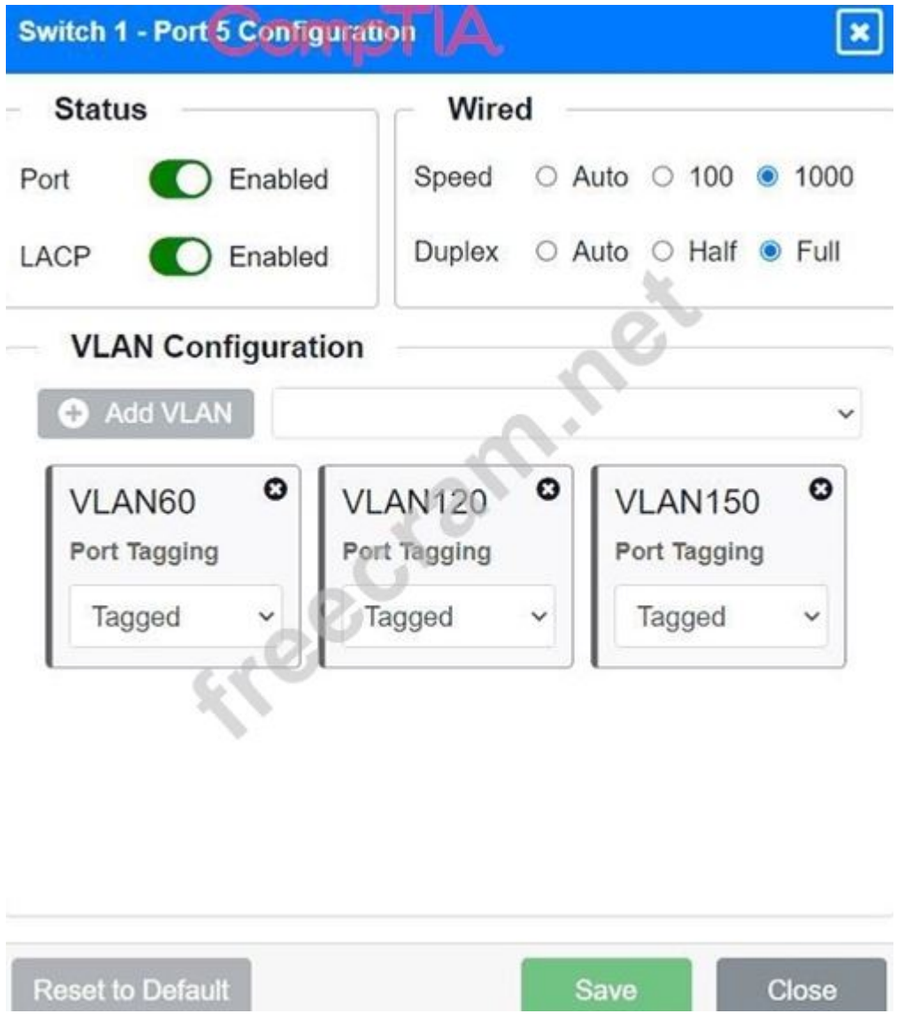


freecram.net

CompTIA®

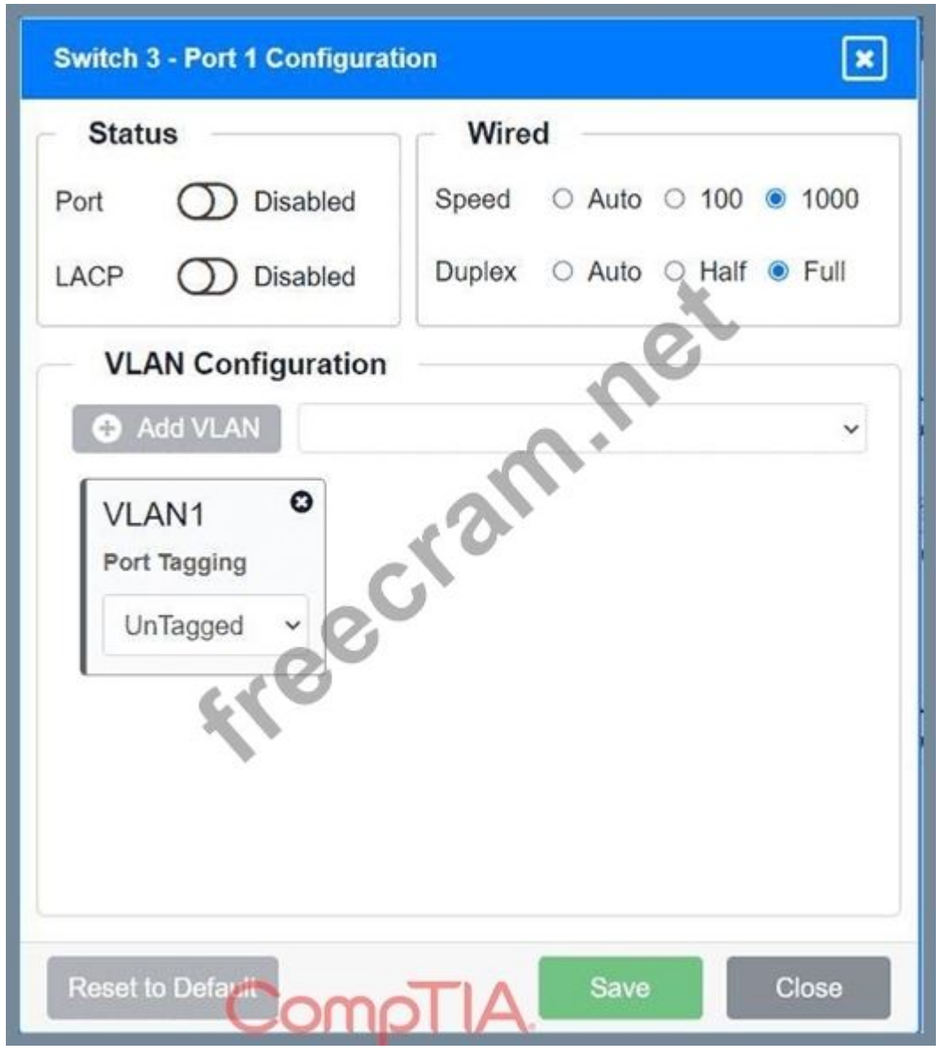
CompTIA
freecram.net

freecram.net

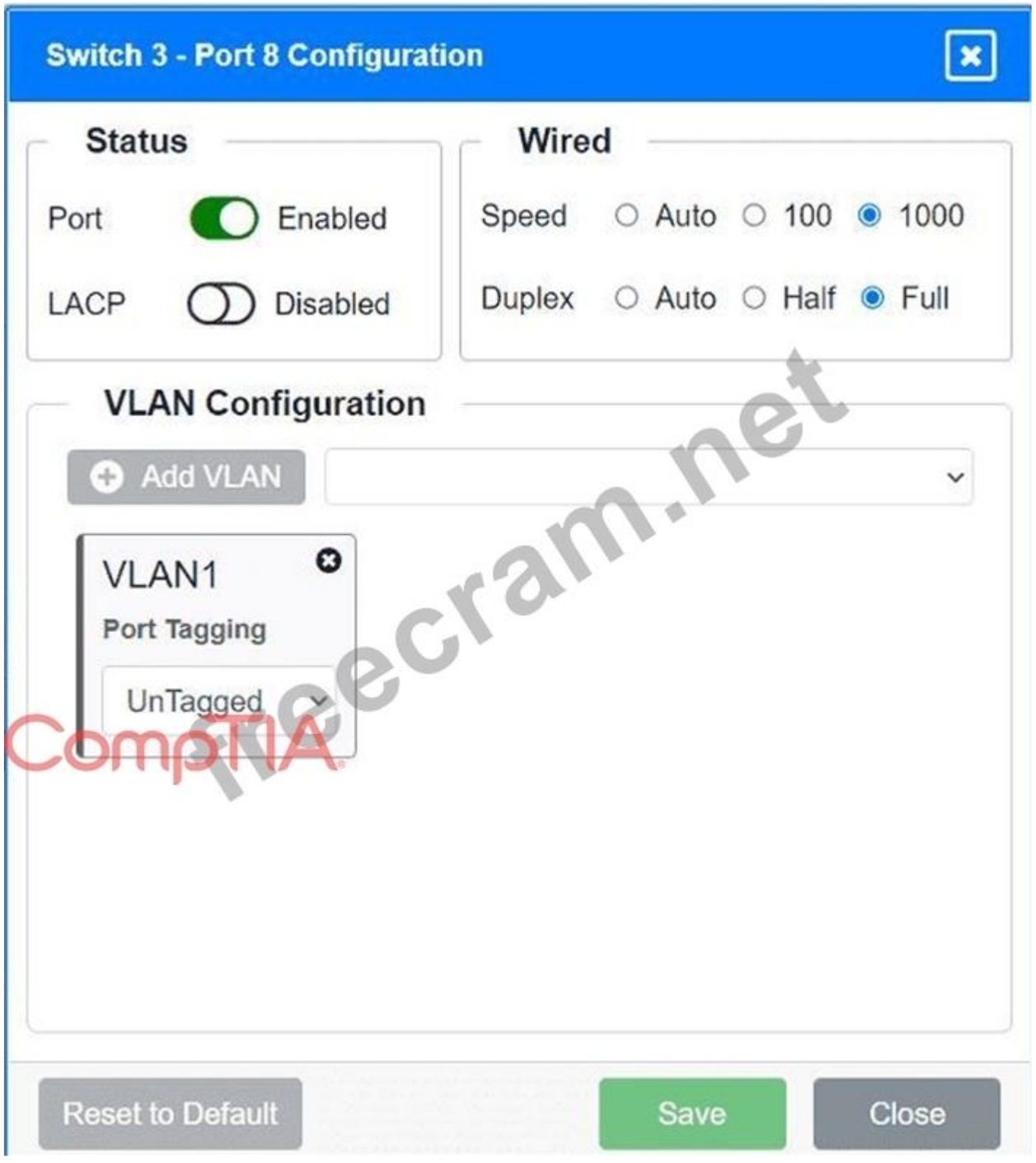


CompTIA
freecram.net

CompTIA
freecram.net



freecram.net
CompTIA.



CompTIA
freecram.net

Answer:

See the solution below in Explanation.

Explanation:

To provide a complete solution for configuring the access layer switches, let ' s proceed with the following steps:

Identify the correct VLANs for each device and port.

Enable necessary ports and disable unused ports.

Configure fault-tolerant connections between the switches.

Port 1 Configuration (Uplink to Core Switch)

Status: Enabled
LACP: Enabled
Speed: 1000
Duplex: Full
VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220 Port 2 Configuration (Uplink to Core Switch) Status: Enabled LACP: Enabled Speed: 1000 Duplex: Full VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN150, VLAN220 Port 3 Configuration (Server Connection) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN90 (Servers) Port 4 Configuration (Server Connection) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN90 (Servers) Port 5 Configuration (Wired Users and WLAN) Status: Enabled LACP: Enabled Speed: 1000 Duplex: Full VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150 Port 6 Configuration (Wired Users and WLAN) Status: Enabled LACP: Enabled Speed: 1000 Duplex: Full VLAN Configuration: Tagged for VLAN60, VLAN120, VLAN150 Port 7 Configuration (Voice and Wired Users) Status: Enabled LACP: Enabled Speed: 1000 Duplex: Full VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220 Port 8 Configuration (Voice, Printers, and Wired Users) Status: Enabled LACP: Enabled Speed: 1000 Duplex: Full VLAN Configuration: Tagged for VLAN60, VLAN90, VLAN120, VLAN220 Port 1 Configuration (Unused) Status: Disabled LACP: Disabled Port 2 Configuration (Unused) Status: Disabled LACP: Disabled Port 3 Configuration (Connection to Device) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN1 (Default) Port 4 Configuration (Connection to Device) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN1 (Default) Port 5 Configuration (Connection to Device) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN1 (Default) Port 6 Configuration (Connection to Device) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN1 (Default) Port 7 Configuration (Connection to Device) Status: Enabled LACP: Disabled Speed: 1000 Duplex: Full VLAN Configuration: Untagged for VLAN1 (Default) Ports 1 and 2 on Switch 1 are configured as trunk ports with VLAN tagging enabled for all necessary VLANs.
Ports 3 and 4 on Switch 1 are configured for server connections with VLAN 90 untagged.
Ports 5, 6, 7, and 8 on Switch 1 are configured for devices needing access to multiple VLANs.
Unused ports on Switch 3 are disabled.
Ports 3, 4, 5, 6, and 7 on Switch 3 are enabled for default VLAN1.
Core Switch Ports should be configured as needed for uplinks to Switch 1.
Ensure LACP is enabled for redundancy on trunk ports between switches.
By following these configurations, each device will access only its correctly associated network, unused switch ports will be disabled, and fault-tolerant connections will be established between the switches.

NEW QUESTION: 37
Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?
A. Identify the problem.
B. Document the findings and outcomes.
C. Test the theory to determine cause.
D. Establish a plan of action.
Answer: A (LEAVE A REPLY)
Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

NEW QUESTION: 38
A technician is troubleshooting wireless connectivity near a break room. Whenever a user turns on the microwave, connectivity to the user ' s laptop is lost. Which of the following frequency bands is the laptop most likely using?
A. 2.4GHz
B. 5GHz
C. 6GHz

D. 900MHz

Answer: (SHOW ANSWER)

The laptop is most likely using the 2.4GHz frequency band. According to the CompTIA Network+ N10-009 objectives, the 2.4GHz band is particularly susceptible to electromagnetic interference (EMI) from common household and office devices, including microwave ovens, cordless phones, Bluetooth devices, and baby monitors. Microwave ovens operate at approximately 2.45GHz, which overlaps directly with the 2.4GHz Wi- Fi spectrum. When the microwave is powered on, it emits interference that can significantly degrade or completely disrupt nearby wireless communications operating in this band.

The 5GHz and 6GHz bands operate at much higher frequencies and do not overlap with microwave emissions, making them far less prone to this type of interference. While higher-frequency bands have shorter range and lower wall penetration, they provide cleaner channels and improved performance in dense environments. The 900MHz band is not used by standard Wi-Fi networks defined in the Network+ objectives and is more commonly associated with legacy cordless phones and certain IoT or proprietary wireless technologies.

Network+ troubleshooting guidance emphasizes identifying environmental interference sources when diagnosing intermittent wireless connectivity. A common mitigation strategy is to migrate affected devices to the 5GHz or 6GHz bands or reposition access points away from interference sources like break room appliances.

NEW QUESTION: 39

A company is expanding to another floor in the same building. The network engineer configures a new switch with the same VLANs as the existing stack. When the network engineer connects the new switch to the existing stack, all users lose connectivity. Which of the following is the MOST likely reason?

A. The new switch has unused ports disabled

B. The new switch does not have a default gateway

C. The new switch is connected to an access port

D. The new switch is in a spanning tree loop

Answer: (SHOW ANSWER)

This describes aSpanning Tree Protocol (STP) loop. If STP isn't correctly configured or a redundant link is added without STP protection, it causesbroadcast storms and network outages.

* A. Unused ports disabledwould not affect the entire network.

* B. Missing default gatewayon a switch doesn't cause total network loss.

* **C. Connecting a switch to an access port can cause VLAN mismatches, but not total connectivity loss unless a loop forms.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 40

Which of the following is a major difference between an IPS and IDS?

A. An IPS needs to be installed in line with traffic and an IDS does not.

B. An IPS is signature-based and an IDS is not.

C. An IPS is less susceptible to false positives than an IDS.

D. An IPS requires less administrative overhead than an IDS.

Answer: (SHOW ANSWER)

The key difference is that an Intrusion Prevention System (IPS) is installed in line with network traffic, allowing it to actively block threats. In contrast, an Intrusion Detection System (IDS) only monitors and alerts without actively blocking traffic.

Breakdown of Options:

A). An IPS needs to be installed in line with traffic and an IDS does not. # Correct answer. IPS actively prevents threats, while IDS only detects them.

B). An IPS is signature-based and an IDS is not. - False, both can use signature-based detection.

C). An IPS is less susceptible to false positives than an IDS. - False, both can produce false positives, depending on configurations.

D). An IPS requires less administrative overhead than an IDS. - False, IPS requires more administrative effort due to real-time blocking decisions.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Explain network security devices.

NEW QUESTION: 41
A network administrator determines that some switch ports have more errors present than expected. The administrator traces the cabling associated with these ports. Which of the following would most likely be causing the errors?
A. nmap
B. tracert
C. arp
D. ipconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 42
An attacker gained access to the hosts file on an endpoint and modified it. Now, a user is redirected from the company's home page to a fraudulent website. Which of the following most likely happened?
A. DNS spoofing
B. Phishing
C. VLAN hopping
D. ARP poisoning
Answer: A (LEAVE A REPLY)
When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.
B). Phishing typically uses emails or messages to trick users, not local file modification.
C). VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.
D). ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.
References (CompTIA Network+ N10-009):
Domain: Network Security - DNS poisoning/spoofing, host file manipulation, endpoint attacks.

NEW QUESTION: 43
An employee has a new laptop and reports slow performance when using the wireless network. Switch firmware was updated the previous night. A network administrator logs in to the switch and sees the following statistics on the switch interface for that employee:
98469 packets input, 1681937 bytes, 0 no buffer
Received 1548 broadcasts (25285 multicasts)
65335 runts, 0 giants, 0 throttles
11546 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
22781 packets output, 858040 bytes, 0 underruns
0 output errors, 89920 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out
Which of the following is most likely the cause of the issue?
A. The patch cord from the wall jack is faulty.
B. The switchport bandwidth needs to be increased.
C. Multicast is not configured correctly on the switch.
D. The NIC is set to half duplex.
Answer: (SHOW ANSWER)
A large number of collisions and input errors typically indicates a duplex mismatch, such as when one device is set to full duplex and the other to half duplex. This leads to communication issues and poor performance.
The document explains:
"Collisions and input errors are clear signs of duplex mismatches... typically caused when one device operates in half duplex while the other is in full duplex, causing performance and connectivity issues."

NEW QUESTION: 44
An organizatin is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that will allow for continous connectivity anywhere in the facility. Which of the following should the network administ rator suggest to ensure the best coverage?
A. Deploying a mesh network in the building
B. Providing more Ethernet drops for user connections
C. Implementing additional ad hoc access points
D. nl Changing the current frequency of the WI-FI
Answer: (SHOW ANSWER)

NEW QUESTION: 45
A network administrator is planning to implement device monitoring to enhance network visibility. The security that the solution provides authentication and encryption. Which of the following meets these requirements?
A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3
Answer: D (LEAVE A REPLY)
SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated.
Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.
Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.
Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers SNMP versions, their features, and security enhancements in SNMPv3.
Cisco Networking Academy: Provides training on implementing and securing SNMP for network management.
Network+ Certification All-in-One Exam Guide: Explains the benefits and security features of SNMPv3 for network monitoring.

NEW QUESTION: 46

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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
A network administrator needs a solution to isolate and potentially identify any threat actors that are attempting to breach the network. Which of the following should the administrator implement to determine the type of attack used?
A. MFA
B. Screened subnet
C. Captive portal
D. Honeypot
Answer: (SHOW ANSWER)
A honeypot is specifically designed to attract, isolate, and observe malicious activity so defenders can learn how an attacker is operating and determine attack techniques. In the context of Network+ (N10-009) security objectives, honeypots (and broader deception technologies) are defensive controls used to detect reconnaissance and exploitation attempts by presenting a decoy system or service that appears legitimate.
Because a honeypot should not receive normal production traffic, any interaction is suspicious, making it valuable for identifying threat actors, collecting indicators of compromise, and analyzing the attacker's tools, commands, and behavior patterns. This supports the goal of understanding the type of attack used (for example, credential stuffing, exploitation attempts, lateral movement probes) while keeping the attacker away from real assets.
MFA strengthens authentication but does not provide a controlled environment to observe attacker techniques.
A screened subnet (DMZ) is for segmentation of public-facing services and reducing exposure of internal systems, but it is not primarily used to "bait" and analyze attackers. A captive portal enforces user acknowledgement/authentication for network access; it is not a deception/analysis system. Therefore, honeypot is the best match.

NEW QUESTION: 48
Which of the following troubleshooting steps would provide 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)
A Change Advisory Board (CAB) reviews and approves network changes. Before approval, they need a detailed action plan outlining the change, potential impacts, and mitigation strategies.
* A Plan of Action includes risk assessments, rollback procedures, and deployment steps, which are critical for decision-making.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Network Troubleshooting Methodologies

NEW QUESTION: 49
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: 50
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?
Freecram.net
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: 51
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: B (LEAVE A REPLY)
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.

NEW QUESTION: 52
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: 53
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: 54
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: 55
A network engineer sees traffic going to 224.7.8.99. Which of the following describes this traffic type?
A. Broadcast
B. Unicast
C. Multicast
D. Anycast
Answer: (SHOW ANSWER)
The answer is C. Multicast . The address 224.7.8.99 falls within the IPv4 Class D range, which is 224.0.0.0 through 239.255.255.255 . That range is reserved for multicast traffic.
Multicast is used when one sender needs to deliver traffic to a specific group of receivers rather than to every device on the network or to just one destination.
That is what separates it from the other choices. Broadcast is intended for all hosts on the local broadcast domain. Unicast is one-to-one communication, where a single source sends traffic to one specific destination.
Anycast is typically associated with sending traffic to the nearest or best member of a group that shares the same address, not to a multicast group address in the 224.0.0.0/4 range.
From a Network+ point of view, this is a basic address-recognition question. Once you recognize that the destination begins with 224 , the answer should immediately point to multicast.
Protocols and streaming applications often use multicast when they need efficient delivery to multiple interested hosts without flooding every device. So in this case, the traffic type is clearly multicast .

NEW QUESTION: 56

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: (SHOW ANSWER)

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: 57

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: 58

Which of the following is an advantage of using an IDS over an IPS?

A. An IDS requires less processing power to analyze traffic.

B. An IDS is less disruptive during the initial deployment of the technology.

C. An IDS is easier to restrict access.

D. An IDS is more accurate due to fewer false positives.

Answer: B (LEAVE A REPLY)

The correct answer is B. An IDS is less disruptive during the initial deployment of the technology. An Intrusion Detection System (IDS) is designed to monitor and alert on suspicious activity, but it does not sit inline to actively block traffic the way an Intrusion Prevention System (IPS) does. Because of that, deploying an IDS usually has less immediate impact on production traffic. It can be introduced to observe network behavior and generate alerts without risking accidental interruption of legitimate communications.
That makes IDS a safer first step in many environments, especially when teams are still tuning signatures, thresholds, or alert rules. If an IPS is deployed too aggressively before it is properly tuned, it may block valid traffic and create service issues. An IDS avoids that risk because it focuses on visibility rather than enforcement.
The other options are weaker. A is not always guaranteed, since processing needs depend on implementation and traffic volume. C is not a defining advantage of IDS over IPS. D is also not reliable, because false positives can occur with either technology depending on configuration and signatures.
For Network+ study purposes, the standard advantage of IDS is that it is passive and less disruptive, especially during initial rollout and monitoring phases.

NEW QUESTION: 59
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 connected to the network. 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: D (LEAVE A REPLY)
IPv4 addresses are divided into classes:
Class A: Supports 16,777,214 hosts (large enterprises).
Class B: Supports 65,534 hosts (medium to large networks).
Class C: Supports 254 hosts (small to medium networks).
Class D: Used for multicast, not for assigning IPs to hosts.
Step-by-step Calculation:
The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.
Each user has two devices, so 160 × 2 = 320 IP addresses needed.
A Class C subnet has 254 usable IPs by default, which is not sufficient.
A Class B subnet can support thousands of hosts, making it the most appropriate option.
Incorrect Options:
A). Class D: Reserved for multicast, not for host assignments.
C). Class A: Overkill for a network of this size.
D). Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on IP Addressing and Subnetting

NEW QUESTION: 60
A help desk technician receives a report that users cannot access internet URLs. The technician performs ping tests and finds that sites fail when a URL is used but succeed when an IP is used. Which of the following tools should the technician utilize next?
Freecram.net
A. tcpdump
B. tracert
C. nmap

D. dig
Answer: D (LEAVE A REPLY)
The issue is clearly related toDNS resolution, as IP-based connections succeed but domain name-based ones fail.
* D. dig(Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.
Other tools are less relevant here:
* A. tcpdumpis a packet analyzer and is more advanced for deeper traffic analysis.
* B. tracertis used to trace the route to a destination, not ideal for DNS issues.
* C. nmapis a port scanner and network mapper, not for resolving DNS problems.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

NEW QUESTION: 61
Which of the following is the MOST appropriate solution to extend the network to a building located across the street from the main facility?
A. Multimode fiber
B. 802.11ac wireless bridge
C. Cat 6 copper
D. Loopback adapter
Answer: (SHOW ANSWER)
An802.11ac wireless bridgeis the most practical solution to connect two nearby buildingswithout trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.
* A. Multimode fiberis effective but expensive and typically limited to 500 meters or less.
* C. Cat 6 copperis only rated for up to 100 meters - not viable for a street-wide distance.
* D. Loopback adapteris a troubleshooting tool, not for network extension.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 1.3 - Compare and contrast various network topologies, types, and technologies.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
Which of the following is the best use case for PAT?
A. Using BGP for internet routing
B. Using a single public IP
C. Using redundant internet service providers
D. Using a dual-stack IP scheme
Answer: (SHOW ANSWER)
The correct choice is B. Using a single public IP. PAT (Port Address Translation) is a form of NAT that allows many internal private IP addresses to share one public IP address by tracking sessions with port numbers. This is one of the most common edge-network designs for homes, small offices, and many enterprise branch environments.

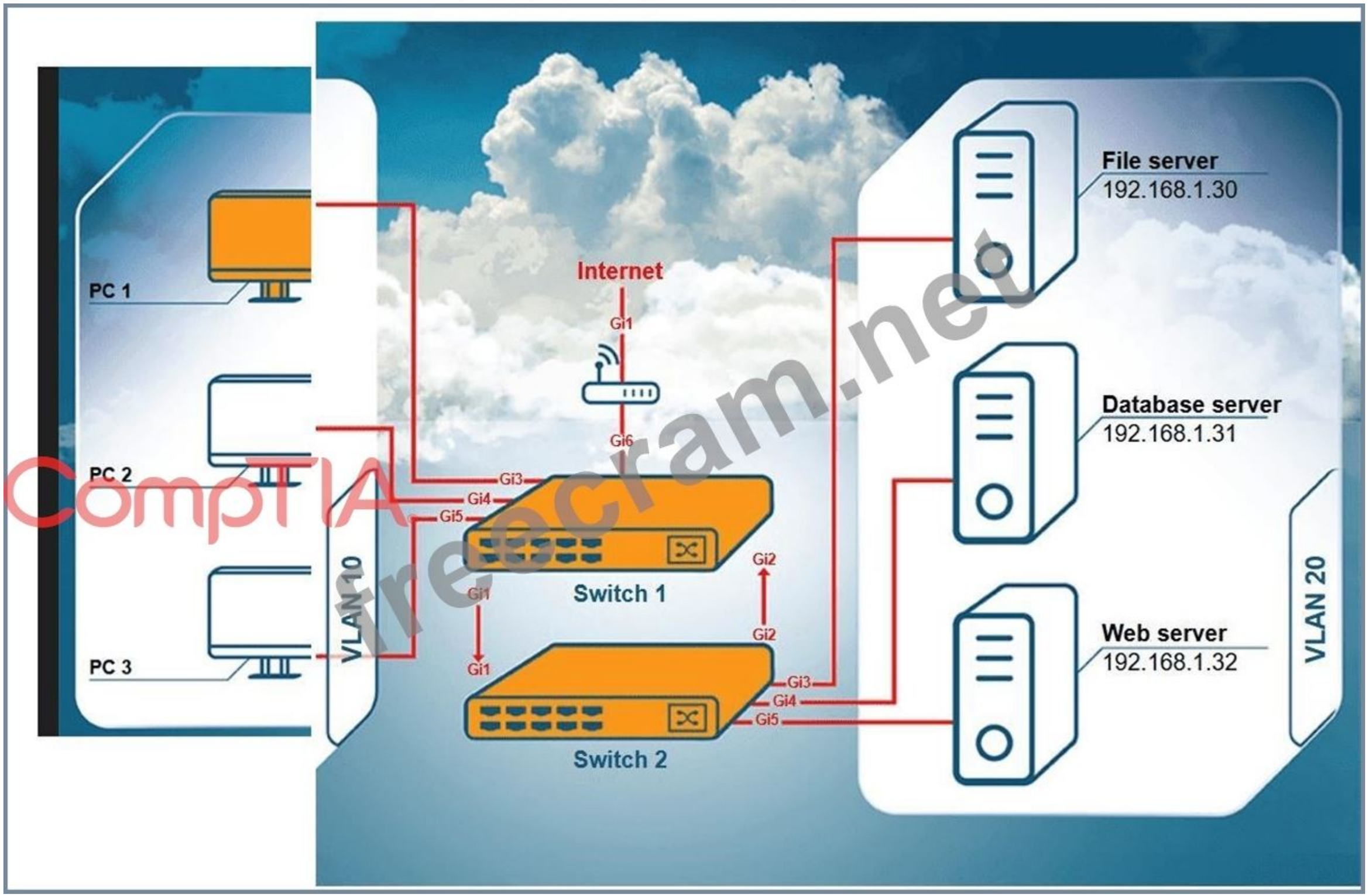
The reason PAT is so useful is that it conserves public IPv4 addresses. Internal hosts keep their private addressing, and when they access external resources, the firewall or router translates those connections so they appear to come from one public address, while still keeping each session unique through port mapping.
The other options are unrelated to PAT's primary purpose. BGP is a routing protocol for route exchange between networks. Redundant ISPs deal with resiliency and multihoming, not port-based address translation.
A dual-stack IP scheme means running IPv4 and IPv6 together, which is separate from the NAT/PAT function.
This question is really asking what situation most naturally calls for PAT. When an organization wants multiple internal devices to reach the internet without assigning each device its own public IPv4 address, PAT is the standard solution. That makes using a single public IP the best answer.

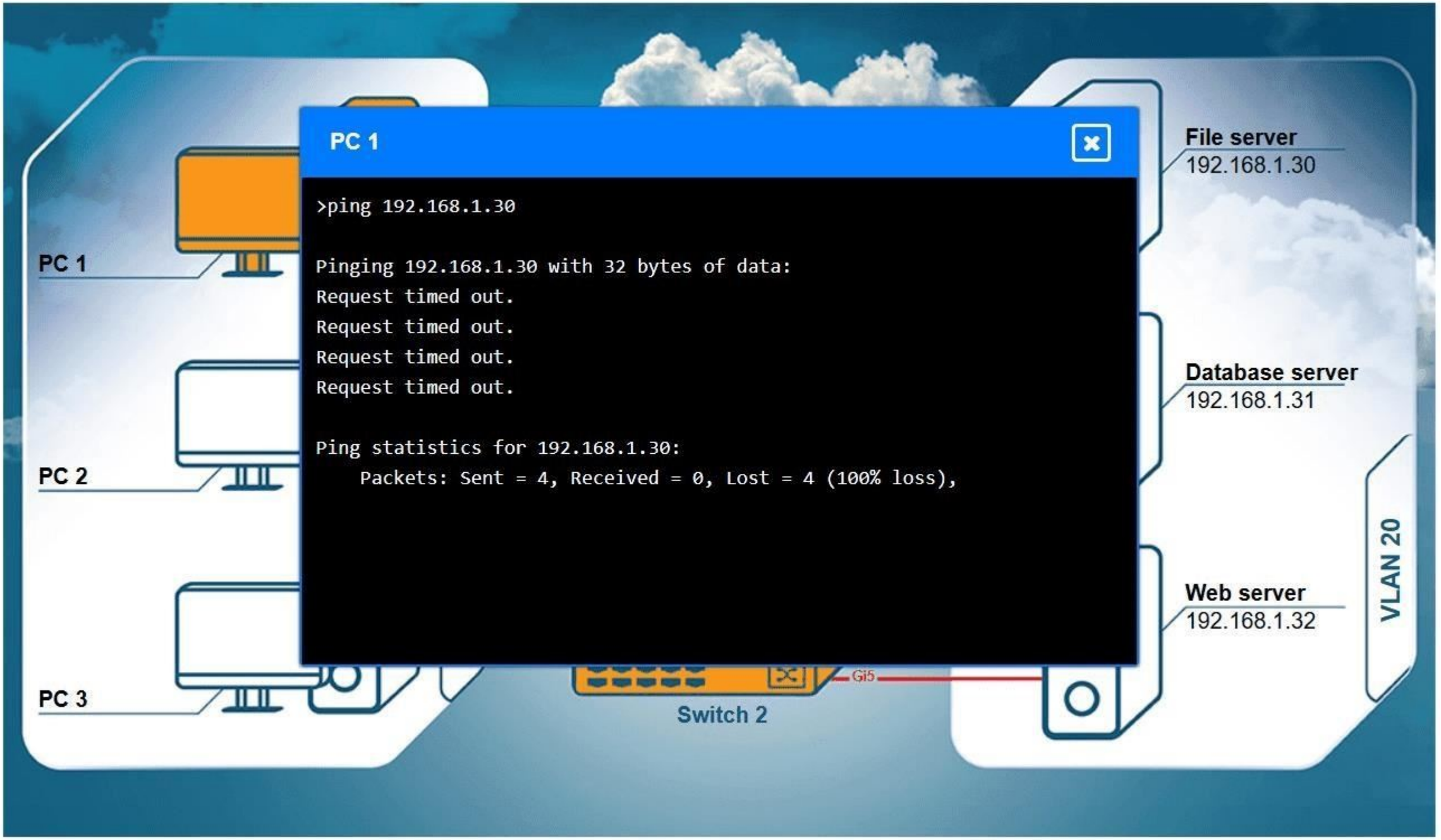
NEW QUESTION: 63
Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?
A. Direct Connect
B. Internet gateway
C. Captive portal
D. VPN
Answer: (SHOW ANSWER)
Direct Connect refers to a dedicated network connection between an on-premises 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: 64
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: 65
A network technician receives a ticket from an employee who is working on PC 1 but is unable to connect to the database server. The technician pings the database server from PC 1, but the request times out. After reviewing the utilization of Switch 1 and Switch 2, the technician finds high CPU utilization and sees that the MAC table is continuously changing.
INSTRUCTIONS
Configure Switch 1 and Switch 2 to remediate the employee ' s issue. Then, validate connectivity between PC
1 and the database server.
Switch 1 and Switch 2 are already in configuration mode. Type help to view a list of available commands.


PC 1
PC 2
PC 3
VLAN 10
Internet
Gi1
Gi6
Gi3
Gi4
Gi5
Switch 1
Gi1
Gi2
Gi2
Gi1
Switch 2
Gi3
Gi4
Gi5
File server
192.168.1.30
Database server
192.168.1.31
Web server
192.168.1.32
VLAN 20


PC 1
>ping 192.168.1.30
Pinging 192.168.1.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.30:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
File server
192.168.1.30
Database server
192.168.1.31
Web server
192.168.1.32
VLAN 20
PC 1
PC 2
PC 3
Gi5
Switch 2

Switch 1
Switch1(config)#
CompTIA
freecram.net

Switch 2
Switch2(config)#
CompTIA
freecram.net

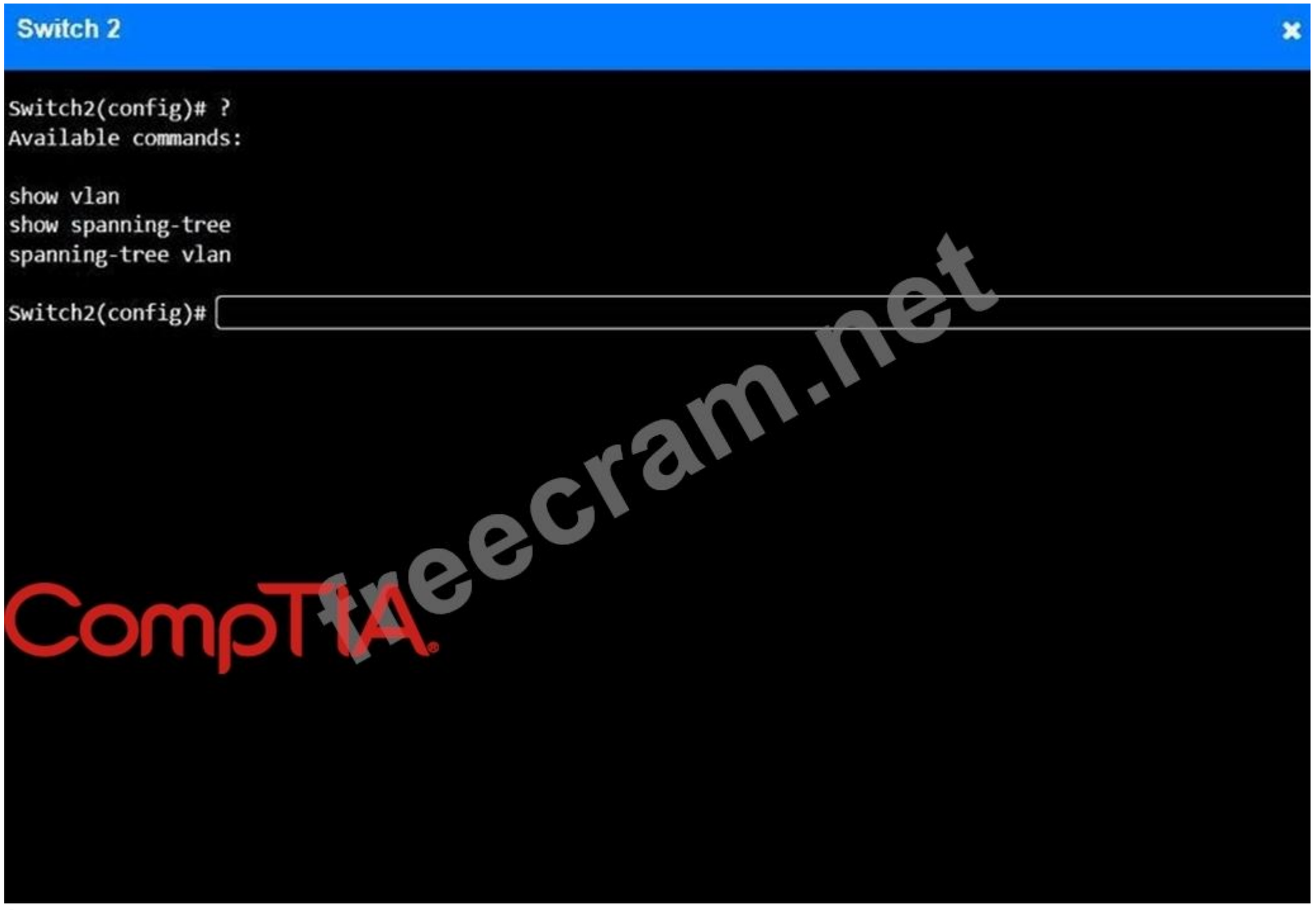
Switch 1

```
Switch1(config)# interface gi2
   % Invalid input detected.
Switch1(config)# ?
Available commands:

show vlan
show spanning-tree
spanning-tree vlan

Switch1(config)# spanning-tree vlan 10
Switch1(config)# spanning-tree vlan 20
Switch1(config)#
```

CompTIA.
freecram.net



Answer:

See the solution in Explanation below.

Explanation:

Switch 1

spanning-tree vlan 10 root primary

spanning-tree vlan 20 root secondary

Switch 2

spanning-tree vlan 20 root primary

spanning-tree vlan 10 root secondary

This PBQ is pointing to a switching loop / MAC flapping problem. The biggest clues are the high CPU utilization and the fact that the MAC table is continuously changing. That behavior is classic for a Layer 2 loop when redundant links exist between switches and no proper spanning-tree root role has been established.

The available commands shown in the screenshots are limited to spanning-tree vlan, so this is not an interface shutdown question. The fix is to use STP per VLAN and make one switch the preferred root for one VLAN and the other switch the preferred root for the other VLAN. That prevents both uplinks from forwarding in an uncontrolled loop while still giving redundancy.
A clean design is:
* Switch 1 root primary for VLAN 10
* Switch 2 root primary for VLAN 20
* Make each opposite switch root secondary for failover
That stabilizes Layer 2 forwarding, stops MAC address flapping, reduces CPU load, and restores normal connectivity. After applying the STP root settings, the user should be able to ping 192.168.1.31 from PC 1 successfully. If your simulator asks for validation, run the ping again from PC 1 to the database server.

NEW QUESTION: 66
Users on the network are experiencing slow throughput. A technician wants to increase throughput without changing any switch hardware. Which of the following solutions should the technician implement?
A. SVI configuration
B. VLAN trunking
C. 802.1Q tagging
D. Link aggregation
Answer: (SHOW ANSWER)
The correct answer is D. Link aggregation. Link aggregation combines multiple physical switch links into one logical connection. This increases available bandwidth and can also add redundancy, all without replacing the switch hardware itself. If users are experiencing slow throughput and the goal is to improve capacity using existing equipment, bundling links is a common and effective solution.
The other options do not directly increase throughput. SVI configuration provides Layer 3 interfaces for VLANs, but it does not add link capacity. VLAN trunking allows multiple VLANs to traverse one connection, but that does not increase bandwidth by itself. 802.1Q tagging identifies VLAN membership on tagged frames; it is related to trunking, not throughput expansion.
In many enterprise environments, link aggregation is implemented through standards such as LACP. This lets several ports act together as one logical channel, which can help distribute traffic more efficiently across the bundled interfaces. For Network+ exam scenarios, when the requirement is to improve throughput using the current switch hardware rather than buying faster switches, link aggregation is the most appropriate answer.

NEW QUESTION: 67
A network administrator is extending a network beyond the primary equipment location. Which of the following is where the administrator should install additional network switches?
A. MDF
B. VPC
C. VXLAN
D. IDF
Answer: (SHOW ANSWER)
When extending a network beyond the primary equipment location, additional access/distribution switches are typically placed in an IDF (Intermediate Distribution Frame). Network+ (N10-009) infrastructure objectives differentiate between the MDF and IDF: the MDF is the main, central wiring/equipment location (often where core switches, routers, WAN demarcation, and main cross-connects reside). As a building grows or spans multiple floors/areas, an IDF is used as a secondary wiring closet to reduce cable runs, provide local switching, and aggregate user access connections back to the MDF using backbone cabling (often fiber). This supports scalability, cable management, and performance by keeping horizontal runs within recommended distance limits.

VPC (Virtual Private Cloud) is a cloud networking construct, not a physical wiring location. VXLAN is an overlay tunneling technology used in virtualized/data center networks, not where you physically install switches. The question specifically references extending the network beyond the primary equipment location, which is a classic use case for deploying an IDF to host additional switches closer to endpoint areas while uplinking back to the MDF.

NEW QUESTION: 68
Which of the following connectors allows a singular QSFP transceiver to have several physical connections?
A. RJ45
B. ST
C. LC
D. MPO
Answer: (SHOW ANSWER)
The MPO (Multi-fiber Push On) connector is designed to handle multiple fiber strands in a single connector, and it is commonly used with high-density transceivers like QSFP (Quad Small Form-factor Pluggable).
QSFP can support up to four channels (hence " quad "), and MPO connectors can interface multiple fibers (e.
g., 8, 12, 24), making them ideal for 40Gbps or 100Gbps deployments.
RJ45 (A) is used for Ethernet over copper.
ST (B) and LC (C) are single-fiber connectors - they don ' t support the multi-fiber needs of QSFP setups.
Therefore, MPO is the correct connector type for this use case.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.1: " Compare and contrast different types of connectors and transceivers. "

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: (SHOW ANSWER)
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
Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?
Freecram.net
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: 71

A user recently moved a workstation to a different part of the office. The user is able to access the internet and print but is unable to access server resources. Which of the following is the most likely cause of the issue?

A. Incorrect default gateway

B. Wrong VLAN assignment

C. Error-disabled port

D. Duplicate IP address

Answer: (SHOW ANSWER)

If a workstation can access the internet and printers (likely in another VLAN) but not internal servers, the port was likely placed into the wrong VLAN after the move. VLAN assignment controls Layer 2 segmentation, restricting access to resources on different VLANs.

A). A wrong default gateway would prevent internet access.

C). An error-disabled port would block all connectivity.

D). A duplicate IP would cause general network issues, not just missing server access.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - VLAN misconfiguration, connectivity issues.

NEW QUESTION: 72

A company's Chief Information Security Officer requires that servers and firewalls have accurate timestamps when creating log files so that security analysts can correlate events during incident investigations. Which of the following should be implemented?

A. Syslog server

B. SMTP

C. SNMP

D. NTP

Answer: (SHOW ANSWER)

NTP (Network Time Protocol) synchronizes clocks across network devices, ensuring accurate timestamps in logs. This is critical for correlating events across different systems during investigations.

A). Syslog collects logs but relies on accurate timestamps already present.

B). SMTP is an email protocol, unrelated to time synchronization.

C). SNMP is for monitoring and management, not time.

References (CompTIA Network+ N10-009):
Domain: Network Operations - Time synchronization (NTP), log correlation, security operations.

NEW QUESTION: 73
A network engineer connects a business to a new ISP. A simple ping test to 8.8.8.8 is successful. However, users complain of extreme slowness to any website and periods of no connectivity. Which of the following is the most likely cause?
A. Incorrect default gateway
B. VLAN mismatch
C. Subnet mask configuration
D. Duplicate ISP IP address
Answer: (SHOW ANSWER)
If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.
A). If the default gateway were incorrect, no external connectivity would work at all.
B). VLAN mismatch is an internal issue, not affecting ISP routing.
C). Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Internet connectivity issues, ISP IP conflicts.

NEW QUESTION: 74
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: B (LEAVE A REPLY)
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: 75
A network administrator is troubleshooting a connectivity issue between two devices on two different subnets.
The administrator verifies that both devices can successfully ping other devices on the same subnet. Which of the following is the most likely cause of the connectivity issue?
A. Incorrect default gateway
B. Faulty Ethernet cable
C. Wrong duplex settings
D. VLAN mismatch
Answer: (SHOW ANSWER)
When two devices on different subnets are unable to communicate, but can communicate with other devices on their own subnet, the issue is most often related to routing. Devices on different subnets require a default gateway to route traffic between networks.

If the default gateway is incorrectly configured, the device won't know how to reach other subnets.
Faulty cables (Option B) or duplex mismatches (Option C) would likely cause connectivity issues even within the local subnet, which is not the case here.
VLAN mismatches (Option D) are typically issues with switch port configurations and would likely cause total loss of connectivity, including within the same subnet.
So, the most probable and logical cause is an incorrect default gateway.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.4: "Compare and contrast routing technologies."

NEW QUESTION: 76
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

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Developers want to create a mobile application that requires a runtime environment, developer tools, and databases. The developers will not be responsible for security patches and updates. Which of the following models meets these requirements?
A. Container as a service
B. Infrastructure as a service
C. Platform as a service
D. Software as a service
Answer: C (LEAVE A REPLY)
The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.

A). CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.
B). IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.
D). SaaS provides end-user applications (e.g., email, CRM), not platforms for development.
By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud service models (IaaS, PaaS, SaaS, CaaS).

NEW QUESTION: 78
Which of the following steps of the troubleshooting methodology would most likely include checking through each level of the OSI model after the problem has been identified?
A. Establish a theory.
B. Implement the solution.
C. Create a plan of action.
D. Verify functionality.
Answer: (SHOW ANSWER)
The CompTIA troubleshooting methodology includes steps like identifying the problem, establishing a theory of probable cause, testing the theory, creating a plan of action, implementing the solution, verifying functionality, and documenting findings. Establishing a theory involves analyzing the problem and considering possible causes, often by systematically checking each level of the OSI model (Physical, Data Link, Network, etc.) to pinpoint the root cause.
Why not Implement the solution? This step involves applying the fix, not analyzing the OSI model.
Why not Create a plan of action? This step focuses on planning the solution, not diagnosing the cause.
Why not Verify functionality? This step confirms the solution worked, not analyzing the OSI model.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) details the troubleshooting steps, noting that establishing a theory often involves using the OSI model to systematically identify the cause of network issues.

NEW QUESTION: 79
Which of the following is the step that a troubleshooter should take immediately after implementing a solution?
A. Review lessons learned during the process.
B. Establish a plan of action.
C. Verify full system functionality.
D. Document actions and outcomes.
Answer: (SHOW ANSWER)
After implementing the solution, the immediate next step is to verify full system functionality. This confirms that the problem has been resolved and helps ensure no new issues have been introduced.
From Andrew Ramdayal's guide:
"After the solution is implemented, test the system to ensure that it is fully operational, and the original problem has been resolved. Also, put in place any measures that could prevent the issue from recurring."

NEW QUESTION: 80
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?
Pgocram.net
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: 81
A customer migrates its phone system from analog to a new hosted VoIP/software application solution with integrated video. After installation, some users notice issues with dropped calls, broken video, and slow internet access. The issues start in the mid-morning and continue into the afternoon. However, remote users do not report the same issues. Which of the following is the most likely cause of the issues?
A. Roaming misconfiguration
B. Signal degradation
C. Insufficient bandwidth
D. Miswired cable
Answer: (SHOW ANSWER)
The best answer is C. Insufficient bandwidth. The pattern in the question matters more than anything else. The company moved to a hosted VoIP and video solution, which means voice and video traffic now depend heavily on the site's internet connection. The problems begin mid-morning and continue into the afternoon, which strongly suggests the link becomes congested during the busiest usage period of the day.
That also explains why users see dropped calls, broken video, and slow internet access all at the same time.
Real-time applications like VoIP and video are very sensitive to delay, jitter, and packet loss. When bandwidth is limited or saturated, those services are usually the first to show noticeable symptoms.
The fact that remote users do not report the same issue is another major clue. If the application platform itself were failing, remote users would likely be affected too. Since the issue seems limited to the main site, the bottleneck is most likely the local office's WAN or internet connection rather than the hosted service.
The other options are weaker. Roaming misconfiguration is more of a wireless mobility issue, signal degradation is too vague for this traffic pattern, and a miswired cable would not usually appear only during peak business hours. This points to insufficient bandwidth.

NEW QUESTION: 82
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: D (LEAVE A REPLY)
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: 83
Which of the following protocols provides remote access utilizing port 22?
A. SSH
B. Telnet
C. TLS
D. RDP
Answer: (SHOW ANSWER)
SSH (Secure Shell) is a protocol used to securely connect to a remote server/system over a network. It operates on port 22 and provides encrypted communication, unlike Telnet which operates on port 23 and is not secure. TLS is used for securing HTTP connections (HTTPS) and operates on ports like 443, while RDP (Remote Desktop Protocol) is used for remote desktop connections and operates on port 3389.
Reference:
The CompTIA Network+ materials and tutorials cover SSH as the standard protocol for secure remote access, highlighting its operation on port 22.

NEW QUESTION: 84
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: 85
Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?
A. Access, distribution, and core
B. Core, root, and distribution
C. Core, spine, and leaf
D. Access, core, and roof
Answer: (SHOW ANSWER)
The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 86
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: 87
While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?
A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1
Answer: (SHOW ANSWER)
The loopback address 127.0.0.1 is used to test the TCP/IP stack of the local machine. Pinging this address confirms whether the local system's networking stack is functioning correctly.

NEW QUESTION: 88
Which of the following objectives does an evil twin achieve?
A. DNS poisoning

B. Login credentials
C. ARP spoofing
D. Denial of service
Answer: (SHOW ANSWER)
An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.
A). DNS poisoning manipulates DNS resolution but is not inherent to evil twin.
C). ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.
D). Denial of service can be a side effect but is not the primary objective of evil twin attacks.
The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless attacks, rogue APs, evil twins.

NEW QUESTION: 89
A systems administrator is looking for operating system information, running services, and network ports that are available on a server. Which of the following software tools should the administrator use to accomplish this task?
A. Nmap
B. Traceroute
C. Netstat
D. Ping
Answer: (SHOW ANSWER)
The correct answer is A. Nmap. Nmap (Network Mapper) is a powerful network scanning and reconnaissance tool specifically designed to gather detailed information about hosts on a network. According to CompTIA Network+ N10-009 objectives, Nmap can be used to identify open ports, running services, and even the operating system of a target device through techniques such as TCP/UDP scanning and OS fingerprinting.
This makes Nmap the best choice when a systems administrator needs a comprehensive view of a server's exposure and configuration. It can enumerate services (e.g., HTTP, SSH), detect service versions, and determine which ports are open, closed, or filtered.
The other options are more limited in scope. Traceroute is used to map the path packets take across a network and identify latency or routing issues, but it does not provide service or OS details. Netstat shows active connections and listening ports on a local machine but does not perform remote OS detection or full service enumeration. Ping simply tests connectivity and reachability using ICMP and does not provide detailed system information.
Therefore, Nmap is the most appropriate and comprehensive tool for this requirement.

NEW QUESTION: 90
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?
Freecram.net
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: 91
A data center administrator is evaluating the use of jumbo frames within a storage environment. Which of the following describes the best reason to use jumbo frames in the storage environment?
A. To reduce device overhead
B. To report on the current root switch in the STP
C. To improve routing convergence
D. To increase drive throughput
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:
"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which of the following describes the type of traffic flow the administrator is analyzing?
A. East-west
B. Point-to-point
C. Horizontal-scaling
D. Hub-and-spoke
Answer: (SHOW ANSWER)
When traffic moves laterally between VMs within the same network or subnet, it is known as east-west traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.
Breakdown of Options:

A). East-west - Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.
B). Point-to-point - Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.
C). Horizontal-scaling - This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.
D). Hub-and-spoke - This network topology describes a centralized design, not lateral traffic.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Analyze traffic patterns and behavior.
NIST SP 800-207: Zero Trust Architecture (ZTA) - East-West traffic monitoring

NEW QUESTION: 93
Which of the following is enforced through legislation?
A. AUP
B. GDPR
C. Code of conduct
D. EULA
Answer: (SHOW ANSWER)
GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences.
Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

NEW QUESTION: 94
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: 95
A network technician sets up a computer on the accounting department floor for a user from the marketing department. The user reports that they cannot access the marketing department's shared drives but can access the internet. Which of the following is the most likely cause of this issue?
A. Mismatched switchport duplex
B. Misconfigured gateway settings
C. Incorrect VLAN assignment

D. SVI is assigned to the wrong IP address

Answer: (SHOW ANSWER)

The user's inability to access the marketing department's shared drives, despite having internet access, suggests a network segmentation issue. The most likely cause is an incorrect VLAN assignment. The computer is physically located on the accounting department floor, and the switchport is likely configured for the accounting VLAN, not the marketing VLAN. VLANs segment network traffic, and if the computer is in the wrong VLAN, it cannot communicate with the marketing department's resources.

Why not Mismatched switchport duplex? Duplex mismatches cause performance issues (e.g., packet loss) but not specific access denials to shared drives.

Why not Misconfigured gateway settings? Incorrect gateway settings would prevent internet access, which the user has.

Why not SVI is assigned to the wrong IP address? A Switch Virtual Interface (SVI) with an incorrect IP address affects inter-VLAN routing, but this would likely impact multiple users, not just one.

Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) explains that VLANs isolate traffic, and incorrect VLAN assignments prevent access to resources on other VLANs.

NEW QUESTION: 96

Which of the following protocols is used to send networking status messages between clients and servers?

A. SSH

B. DHCP

C. NTP

D. SNMP

Answer: (SHOW ANSWER)

The correct answer is SNMP (Simple Network Management Protocol) because it is specifically designed to collect and transmit network management and status information between managed devices and management systems. According to CompTIA Network+ (N10-009) objectives, SNMP is used for monitoring and managing network devices such as routers, switches, servers, and printers.

SNMP operates using a manager-agent model. The SNMP manager (such as a network monitoring server) communicates with SNMP agents installed on network devices. Agents send traps and inform messages, which are unsolicited status alerts indicating events such as device failures, high CPU usage, or link outages.

The manager can also poll agents to retrieve performance metrics and configuration details stored in the Management Information Base (MIB).

SSH (Option A) is used for secure remote administration. DHCP (Option B) dynamically assigns IP addresses. NTP (Option C) synchronizes time between devices. None of these protocols are designed for network status monitoring and alert messaging.

Therefore, SNMP is the correct protocol for sending networking status messages between devices and management systems.

Bottom of Form

NEW QUESTION: 97

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

A. GRE

B. IKE

C. ESP

D. AH

Answer: (SHOW ANSWER)

* Definition of ESP (Encapsulating Security Payload):
* ESP is a part of the IPsec protocol suite designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.
* Ensuring Confidentiality:
* Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.

* Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.
* Comparison with Other Protocols:
* GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.
* IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.
* AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.
* Implementation:
* Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.
References:
* CompTIA Network+ study materials on IPsec and secure communication protocols.

NEW QUESTION: 98
Which of the following standards enables the use of an enterprise authentication for network access control?
A. 802.1Q
B. 802.1X
C. 802.3bt
D. 802.11h
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
802.1X provides port-based Network Access Control (NAC), requiring authentication (often through RADIUS) before granting access. This is the standard for enterprise authentication on both wired and wireless networks.
A). 802.1Q defines VLAN trunking.
C). 802.3bt defines higher-power PoE.
D). 802.11h deals with spectrum management in wireless.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication.

NEW QUESTION: 99
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: 100

A network administrator wants to restrict inbound traffic to allow only HTTPS to the company website, denying all other inbound traffic from the internet. Which of the following would best accomplish this goal?

Freecram.net

A. ACL on the edge firewall
B. Port security on an access switch
C. Content filtering on a web gateway
D. URL filtering on an outbound proxy
Answer: (SHOW ANSWER)
AnAccess Control List (ACL)configured on theedge firewallis the correct and most effective solution tofilter inbound traffic. The administrator can allow TCP port 443 (HTTPS) and deny all other traffic. This is a classic firewall configuration for securing public-facing servers.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "ACLs (Access Control Lists)"

NEW QUESTION: 101
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: 102
Which of the following internal routing protocols is best characterized as having fast convergence and being loop-free?
A. BGP
B. STP
C. OSPF
D. RIP
Answer: (SHOW ANSWER)
The correct answer is OSPF (Open Shortest Path First). OSPF is a link-state routing protocol known for its fast convergence and use of the Dijkstra algorithm to calculate the shortest loop-free path. It efficiently scales to large enterprise networks and avoids routing loops by maintaining a complete topology map.
A). BGP is primarily an external routing protocol used between ISPs, not internal.

B). STP is not a routing protocol; it prevents loops at Layer 2.
D). RIP is an older distance-vector protocol with slower convergence and a maximum hop limit of 15.
OSPF's design makes it the preferred internal gateway protocol (IGP) for medium-to-large organizations requiring speed and loop-free reliability.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - IGPs, OSPF, routing protocols.

NEW QUESTION: 103
A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?
A. Theswitch failed.
B. Thedefault gateway is wrong.
C. Theport Is shut down.
D. TheVLAN assignment is incorrect.
Answer: (SHOW ANSWER)
When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:
* Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.
* No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.
* Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.
Command to Check and Enable Port:
bash
Copy code
Switch> enable
Switch# configure terminal
Switch(config)# interface [interface id]
Switch(config-if)# no shutdown
* The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.
Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

NEW QUESTION: 104
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?
A. Reverse the fibers.
B. Reterminate the fibers.
C. Verify the fiber size.
D. Examine the cable runs for visual faults.
Answer: (SHOW ANSWER)
When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.References:CompTIA Network+ study materials.

NEW QUESTION: 105
A network engineer needs to change, update, and control APs remotely, with real-time visibility over HTTPS.
Which of the following will best allow these actions?
A. Web interface
B. Command line
C. SNMP console
D. API gateway
Answer: D (LEAVE A REPLY)
API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.
From Andrew Ramdayal's guide:
"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

NEW QUESTION: 106
A network technician implements a switch with multiple VLANs. Which of the following items should the technician configure to ensure that clients can communicate with clients in other VLANs?
A. VPC
B. VXLAN
C. ACL
D. SVI
Answer: (SHOW ANSWER)
To enable communication between VLANs, the technician must configure inter-VLAN routing. On a Layer 3 switch, this is commonly done by creating an SVI (Switched Virtual Interface) for each VLAN. An SVI provides a virtual Layer 3 interface with an IP address that acts as the default gateway for hosts in that VLAN.
Once SVIs exist and routing is enabled, the switch can route traffic between VLAN subnets internally, allowing clients in different VLANs to communicate (subject to any security controls). This aligns with Network+ (N10-009) infrastructure objectives covering VLANs, Layer 2/Layer 3 switching, and the requirement for routing to cross broadcast domains.
ACLs can permit or deny inter-VLAN traffic, but they do not create the routing function by themselves.
VXLAN is an overlay tunneling technology used mainly in data centers to extend Layer 2 networks over Layer 3 fabrics, not the standard solution for basic VLAN-to-VLAN connectivity on a switch. VPC is not the required configuration element for inter-VLAN routing in this context. Therefore, configuring SVIs is the correct and most direct answer.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
Ten new laptops are added to an existing network, and they can only communicate with one another. An administrator reviews documentation and sees the following:
Subnet: 10.8.100.1/24
Scope: 10.8.100.50 - 10.8.100.150
Reservation: 10.8.100.151 - 10.8.100.175

A technician scans the network and receives the following results:
IP addresses used: 10.8.100.45 - 10.8.100.175
Which of the following should be done to ensure connectivity on all laptops?
A. Increase the scope to 10.8.100.35 - 10.8.100.150
B. Increase the scope to 10.8.100.40 - 10.8.100.150
C. Increase the scope to 10.8.100.40 - 10.8.100.175
D. Increase the scope to 10.8.100.50 - 10.8.100.175
Answer: (SHOW ANSWER)
The correct answer is D: Increase the scope to 10.8.100.50 - 10.8.100.175. According to the CompTIA Network+ N10-009 objectives, proper DHCP scope configuration is essential to ensure all hosts can obtain valid IP addresses and communicate beyond their local segment.
In this scenario, the DHCP scope is configured for 10.8.100.50 through 10.8.100.150, while a reservation range exists from 10.8.100.151 through 10.8.100.175. The network scan shows that IP addresses up to
10.8.100.175 are already in use. This indicates that some devices are either statically assigned addresses outside the active scope or are failing to receive valid DHCP leases, causing the new laptops to communicate only with each other-often a sign of APIPA or improper addressing.
To ensure full connectivity, the DHCP scope must be expanded to include the entire range of addresses that are actively in use, including the reserved addresses. Option D correctly extends the scope to 10.8.100.175 without overlapping lower addresses that may be statically assigned or intentionally excluded.
The Network+ objectives emphasize avoiding address conflicts and ensuring DHCP scopes align with real- world network usage. Expanding the scope to include all valid addresses ensures that all laptops can obtain proper IP configuration, default gateway information, and full network connectivity.

NEW QUESTION: 108
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: 109
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: B (LEAVE A REPLY)
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: 110
A network administrator is troubleshooting a connection issue and needs to determine the path that a packet will take. Which of the following commands accomplishes this task?
Pass4sure.net
A. netstat
B. traceroute
C. ping
D. nslookup
E. ipconfig
Answer: (SHOW ANSWER)
The correct answer is traceroute, which is the diagnostic command specifically designed to determine the path a packet takes across a network. According to the CompTIA Network+ N10-009 objectives, traceroute is a key network troubleshooting tool used to identify routing paths, hop counts, and points of latency or failure between a source and a destination.
Traceroute works by sending packets with incrementally increasing Time to Live (TTL) values. Each router along the path decrements the TTL by one, and when it reaches zero, the router returns an ICMP Time Exceeded message. This process allows the administrator to see each intermediate hop, its response time, and where packets may be delayed or dropped.
The other options do not fulfill this purpose. Ping only verifies basic connectivity and round-trip time but does not show the route taken. Netstat displays active connections, ports, and routing tables but does not trace packet paths. Nslookup is used to resolve DNS names to IP addresses, and ipconfig displays local network configuration information.
The Network+ objectives emphasize traceroute (or tracert on Windows systems) as the primary tool for diagnosing routing issues, asymmetric paths, and network congestion, making it the correct and most appropriate choice in this scenario.

NEW QUESTION: 111
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: 112
Which of the following should a company implement in order to share a single IP address among all the employees in the office?
A. STP
B. BGP
C. PAT
D. VXLAN
Answer: (SHOW ANSWER)
PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:
"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

NEW QUESTION: 113
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: 114
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: 115
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: 116
Which of the following steps in the troubleshooting methodology comes after using a top-to-top buttom examination of the OSI model to determine cause?
A. Test in the theory
B. Establish a plan of action
C. Verify full system functionality
D. Identify the problem
Answer: (SHOW ANSWER)

NEW QUESTION: 117
A network administrator deployed wireless networking in the office area. When users visit the outdoor patio and try to download emails with large attachments or stream training videos, they notice buffering issues.
Which of the following is the most likely cause?

A. Network congestion
B. Wireless interference
C. Signal degradation
D. Client disassociation
Answer: (SHOW ANSWER)
The most likely cause of buffering issues when moving outdoors is signal degradation. Wireless signals weaken as they travel through obstacles such as walls, glass, and air, leading to weaker connections and reduced data rates.
Breakdown of Options:
A). Network congestion - While congestion can slow down network speeds, it affects all users, not just those moving outdoors.
B). Wireless interference - Interference is possible but is more likely caused by other wireless signals rather than outdoor movement.
C). Signal degradation - Correct answer. Wireless signals weaken with distance and obstacles such as walls, reducing performance.
D). Client disassociation - Disassociation occurs when clients lose connection to the AP, but the question states that users experience buffering, indicating they are still connected but with a weak signal.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Analyze wireless networking technologies.
IEEE 802.11 standards: Wi-Fi propagation characteristics

NEW QUESTION: 118
Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?
A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map
Answer: (SHOW ANSWER)
* Definition of Heat Maps:
* A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.
* Purpose of a Heat Map:
* Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.
* Comparison with Other Options:
* Logical Diagram: Represents the logical connections and relationships within the network.
* Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.
* Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.
* Creation and Use:
* Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
References:
* CompTIA Network+ certification materials and wireless network planning guides.

NEW QUESTION: 119

Which of the following routing technologies allows all users to access the internet using only two public IPs?

A. EIGRP

B. PAT

C. BGP

D. VIP

Answer: B (LEAVE A REPLY)

The correct answer is B. PAT. Port Address Translation allows many internal devices that use private IP addresses to share a small number of public IP addresses when accessing the internet. In this case, the question says all users can access the internet using only two public IPs, which is exactly the kind of situation PAT is designed for. The device performing PAT keeps track of each connection by using source port numbers, so multiple internal sessions can be translated and maintained at the same time without requiring a unique public IP for every user.

The other options do not match this function. EIGRP and BGP are routing protocols used to exchange routing information, not to translate addresses for outbound internet traffic. VIP refers to a virtual IP address, commonly used in high availability or load-balancing scenarios, but it does not provide the many-to-one address translation behavior described in the question.

For Network+ exam purposes, when the scenario talks about conserving public IPv4 addresses and allowing many users to reach external networks through a very small number of public IPs, the expected answer is PAT. This is one of the most common real-world uses of NAT technology at the network edge.

NEW QUESTION: 120

A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?

Freecram.net

A. 255.255.0.0

B. 255.255.254.0

C. 255.255.255.0

D. 255.255.255.128

Answer: (SHOW ANSWER)

* Understanding Subnetting:
* Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).
* Objective: Divide this network into two equal subnets.
* Calculating Subnet Mask:
* New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).
* Subnet Breakdown:
* First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)
* Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)
* Verification:
* Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).
* Comparison with Other Options:
* 255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.
* 255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.
* 255.255.255.0 (/24): Maintains the original subnet size, not dividing it.

References:

* CompTIA Network+ study materials on subnetting and IP addressing.

NEW QUESTION: 121
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
A company implements a video streaming solution that will play on all computers that have joined a particular group, but router ACLs are blocking the traffic. Which of the following is the most appropriate IP address that will be allowed in the ACL?
A. 127.0.0.1
B. 172.17.1.1
C. 224.0.0.1
D. 240.0.0.1
Answer: (SHOW ANSWER)
224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.
*Why not the other options?
*127.0.0.1 (A) - This is the loopback address used for internal device testing, not for multicast traffic.
*172.17.1.1 (B) - This is a private unicast address, meaning it can only send packets to one specific host.
*240.0.0.1 (D) - This falls within the reserved experimental IP address range and is not used for multicast.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 123
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: 124
Which of the following most likely requires the use of subinterfaces?
A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol
Answer: (SHOW ANSWER)
Introduction to Subinterfaces:
Subinterfaces are logical interfaces created on a single physical interface. They are used to enable a router to support multiple networks on a single physical interface.
Use Case for Subinterfaces:
Subinterfaces are commonly used in scenarios where VLANs are implemented. A router with a single physical LAN port can be configured with multiple subinterfaces, each associated with a different VLAN.
This setup allows the router to route traffic between different VLANs.
Example Configuration:
Consider a router with a single physical interface GigabitEthernet0/0 and two VLANs, 10 and 20.
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
The encapsulation dot1Q command specifies the VLAN ID.

Explanation of the Options:
A). A router with only one available LAN port: This is correct. Subinterfaces allow a single physical interface to manage multiple networks, making it essential for routers with limited physical interfaces.
B). A firewall performing deep packet inspection: Firewalls can use subinterfaces, but it is not a requirement for deep packet inspection.
C). A hub utilizing jumbo frames: Hubs do not use subinterfaces as they operate at Layer 1 and do not manage IP addressing.
D). A switch using Spanning Tree Protocol: STP is a protocol for preventing loops in a network and does not require subinterfaces.
Conclusion:
Subinterfaces provide a practical solution for routing between multiple VLANs on a router with limited physical interfaces. They allow network administrators to optimize the use of available hardware resources efficiently.
References:
CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref
9 Basic Configuration Commands).

NEW QUESTION: 125
Due to concerns around single points of failure, a company decided to add an additional WAN to the network.
The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated, significant network issues occur. Which of the following is the most likely cause for the WAN instability?
A. A changed CDP neighbor
B. Asymmetrical routing
C. A switching loop
D. An incorrect IP address
Answer: (SHOW ANSWER)
Asymmetrical routing occurs when packets take different paths to and from the destination, leading to instability in network communication. The use of two different MPLS providers with OSPF can lead to this type of routing issue, especially if the paths aren't carefully configured and managed. This can cause unexpected routing behaviors and instability in a dual-WAN setup. (Reference: CompTIA Network+ Study Guide, Chapter on Network Routing)

NEW QUESTION: 126
Which of the following ports should a network administrator enable for encrypted login to a network switch?
A. 22
B. 23
C. 80
D. 123
Answer: (SHOW ANSWER)
Port 22 is used for Secure Shell (SSH), which enables encrypted remote login and command execution on network devices.
Port 23 = Telnet (unencrypted)
Port 80 = HTTP
Port 123 = NTP
From Andrew Ramdayal's guide:
"SSH uses port 22 to provide secure command-line access to devices such as switches and routers. Unlike Telnet (port 23), SSH encrypts session traffic, making it the preferred method for remote administration."

NEW QUESTION: 127
A company is migrating a data center from on premises to the cloud. Which of the following tools will help maintain consistency, reliability, and efficiency of provisioning and management?
A. IaC
B. CDN
C. SASE
D. ZTA
Answer: (SHOW ANSWER)
The correct answer is A. IaC . Infrastructure as Code is used to define and deploy infrastructure through templates, configuration files, or code rather than building everything manually. During a cloud migration, that approach helps keep deployments consistent across environments and reduces the chance of human error.
This fits the question especially well because it mentions consistency, reliability, and efficiency in both provisioning and management. Those are exactly the kinds of benefits IaC is meant to provide. Instead of configuring servers, networks, and services one by one, administrators can reuse tested deployment definitions and apply the same settings repeatedly. That makes rollouts faster and easier to audit.
The other options do not match the task. A CDN improves content delivery performance. SASE is a networking and security architecture. ZTA focuses on access control and trust decisions. All of those are important in the right context, but none is primarily a provisioning and management automation tool.
In a cloud migration, the organization usually wants repeatable builds, standardization, and faster recovery if something has to be recreated. That is why IaC is the strongest answer here. It directly supports automated, dependable, and scalable infrastructure deployment.

NEW QUESTION: 128
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: 129
A user's VoIP phone and workstation are connected through an inline cable. The user reports that the VoIP phone intermittently reboots, but the workstation is not having any network-related issues Which of the following is the most likely cause?
A. The PoE power budget is exceeded.
B. Port security is violated.
C. The signal is degraded
D. The Ethernet cable is not working
Answer: (SHOW ANSWER)
Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data.
If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 130
Which of the following is the most cost-efficient way to host email services?
A. PaaS
B. IaaS
C. VPC
D. SaaS
Answer: (SHOW ANSWER)
The correct answer is SaaS (Software as a Service). According to the CompTIA Network+ N10-009 objectives, SaaS is the most cost-efficient cloud model for hosting common business applications such as email, collaboration tools, and productivity suites. With SaaS, the cloud provider manages all infrastructure, operating systems, application software, security updates, and maintenance, significantly reducing administrative overhead and operational costs.
Email services are a prime example of workloads that benefit from SaaS solutions such as Microsoft 365 or Google Workspace. Organizations pay a subscription-based fee, typically per user, and avoid expenses related to server hardware, licensing, patching, backups, redundancy, and disaster recovery. This makes SaaS far more economical than deploying and maintaining email servers internally or in lower-level cloud models.

IaaS requires the organization to manage virtual machines, operating systems, email server software, and security configurations, which increases both cost and complexity. PaaS simplifies application development but is not designed for hosting ready-made services like email platforms. A VPC (Virtual Private Cloud) is a networking construct, not a service model, and does not inherently provide email hosting functionality.
The Network+ objectives emphasize selecting cloud service models based on cost, management responsibility, and operational efficiency. For standardized services like email, SaaS offers the lowest total cost of ownership and the least administrative burden, making it the best and most cost-effective choice.

NEW QUESTION: 131
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: 132
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: 133
Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?
A. Verify full system functionality.
B. Document the findings and outcomes.
C. Establish a plan of action.
D. Identify the problem.
Answer: (SHOW ANSWER)
The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.
Troubleshooting Steps:
Identify the problem.
Establish a theory of probable cause.

Test the theory to determine the cause.
Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.
Document findings, actions, and outcomes.
Breakdown of Options:
A: Verify full system functionality - Happens after implementing the solution.
B: Document the findings and outcomes - Final step, happens after resolving the issue.
C: Establish a plan of action - # Correct answer. Comes immediately after confirming the cause.
D: Identify the problem - First step, already completed.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 5.1: Explain network troubleshooting methodology.

NEW QUESTION: 134
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: 135
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)

The correct answer is 802.1X, which is an identity-based Network Access Control (NAC) framework emphasized in the CompTIA Network+ N10-009 objectives under network security and access control. 802.1 X uses a policy-driven authentication process to determine whether a user or device is allowed network access based on verified credentials, such as usernames, passwords, or digital certificates.
802.1X operates using three main components: the supplicant (the client requesting access), the authenticator (the network device such as a switch or wireless access point), and the authentication server (typically a RADIUS server). Once the user's identity is authenticated, predefined policies determine the level of access granted-full access, limited access, or denial. This makes 802.1X a cornerstone of zero trust and enterprise- grade NAC implementations.
A standard ACL controls traffic based on IP addresses and ports, not user identity. MAC filtering allows or denies access based on device MAC addresses, which can be easily spoofed and does not verify user identity.
SSO (Single Sign-On) simplifies authentication across multiple systems but does not control network-layer access.
Network+ highlights 802.1X as a secure, scalable solution for enforcing identity-based network access policies in both wired and wireless environments.

NEW QUESTION: 136
A network administrator needs to configure the core switches where multiple connections between data centers are used. Given the following requirements:
* Fault tolerance and redundancy
* Vendor interoperability
* Increased bandwidth
* Cost effectiveness
* Simplified management
Which of the following should the administrator configure?
A. Spanning tree
B. Interface speeds to 10GB
C. Link aggregation
D. Jumbo frames
Answer: (SHOW ANSWER)
The best answer is C. Link aggregation. The requirements point directly to combining multiple physical links into one logical connection. Link aggregation provides higher total bandwidth, supports redundancy if one member link fails, and simplifies administration because the bundle is managed as a single logical interface instead of several separate ones.
Another important clue is vendor interoperability. Standards-based link aggregation, such as LACP, is designed to work across different vendors when supported properly. That makes it a strong match for inter- data-center switch environments where equipment may not all come from the same manufacturer.
The other choices do not satisfy the full requirement list. Spanning tree helps prevent loops, but it can block redundant links instead of actively using them for extra bandwidth. Setting interface speeds to 10GB increases speed per port, but it does not by itself provide the logical bundling, simplified management, or redundancy benefits described. Jumbo frames can improve efficiency for some traffic types, but they are not the right answer for bandwidth aggregation and resilient uplinks.
Because the question asks for a solution that improves throughput, keeps redundancy, remains cost effective, and is easier to manage, link aggregation is the strongest fit.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137

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: (SHOW ANSWER)

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: 138

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: 139

Which of the following is a characteristic of the application layer?

A. It relies upon other layers for packet delivery.

B. It checks independently for packet loss.

C. It encrypts data in transit.

D. It performs address translation.

Answer: (SHOW ANSWER)

Introduction to OSI Model:

The OSI model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Application Layer:

The application layer (Layer 7) is the topmost layer in the OSI model. It provides network services directly to end-user applications. This layer facilitates communication between software applications and lower layers of the network protocol stack.

Reliance on Other Layers:

The application layer relies on the transport layer (Layer 4) for data transfer across the network. The transport layer ensures reliable data delivery through protocols like TCP and UDP.

The network layer (Layer 3) is responsible for routing packets to their destination.
The data link layer (Layer 2) handles node-to-node data transfer and error detection.
The physical layer (Layer 1) deals with the physical connection between devices.
Explanation of the Options:
A). It relies upon other layers for packet delivery: This is correct. The application layer depends on the lower layers (transport, network, data link, and physical) for the actual delivery of data packets.
B). It checks independently for packet loss: This is incorrect. Packet loss detection is typically handled by the transport layer (e.g., TCP).
C). It encrypts data in transit: This is incorrect. Encryption is typically handled by the presentation layer or at the transport layer (e.g., TLS/SSL).
D). It performs address translation: This is incorrect. Address translation is performed by the network layer (e.
g., NAT).
Conclusion:
The application layer's primary role is to interface with the end-user applications and ensure that data is correctly presented to the user. It relies on the underlying layers to manage the actual data transport and delivery processes.
References:
CompTIA Network+ guide covering the OSI model and the specific roles and functions of each layer (see page Ref 10 How to Use Cisco Packet Tracer).

NEW QUESTION: 140

A technician is planning an equipment installation into a rack in a data center that practices hot aisle/cold aisle ventilation. Which of the following directions should the equipment exhaust face when installed in the rack?

Freecram.net

A. Sides
B. Top
C. Front
D. Rear
Answer: (SHOW ANSWER)
In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

NEW QUESTION: 141
Users report performance issues on the network. A network administrator notices broadcast storms occurring.
Which of the following protocols should the administrator configure to mitigate this issue?
A. Spanning Tree
B. Enhanced Interior Gateway Routing Protocol (EIGRP)
C. Cisco Discovery Protocol (CDP)
D. Link Layer Discovery Protocol (LLDP)
E. Border Gateway Protocol (BGP)
Answer: (SHOW ANSWER)
The correct answer is Spanning Tree because broadcast storms are typically caused by Layer 2 switching loops in Ethernet networks. According to the CompTIA Network+ (N10-009) objectives under switching concepts, the Spanning Tree Protocol (STP) is specifically designed to prevent loops in networks that have redundant switch connections.
In a Layer 2 environment, switches forward broadcast frames out all ports except the one on which they were received. If redundant paths exist without STP, frames can circulate indefinitely, creating a broadcast storm.

This results in excessive traffic, high CPU utilization on switches, MAC address table instability, and significant network performance degradation.
STP prevents this by logically blocking redundant paths while maintaining them as backups. If the active path fails, STP recalculates and activates a previously blocked path, preserving redundancy without loops.
The other options-EIGRP and BGP (routing protocols) and CDP and LLDP (device discovery protocols)- do not prevent Layer 2 loops.
Therefore, configuring Spanning Tree Protocol is the appropriate solution to mitigate broadcast storms.

NEW QUESTION: 142
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: 143
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: 144
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: 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
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: 147
A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?
A. MAC security
B. Content filtering
C. Screened subnet
D. Perimeter network
Answer: (SHOW ANSWER)
Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease- and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.
References: CompTIA Network+ study materials.

NEW QUESTION: 148
Which of the following should be configured so users can authenticate to a wireless network using company credentials?
A. SSO
B. SAML
C. MFA
D. RADIUS
Answer: (SHOW ANSWER)
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.References:CompTIA Network+ study materials.

NEW QUESTION: 149
A small business is choosing between static and dynamic routing for its network. Which of the following is the best reason to use dynamic routing in a growing network?
A. Easier to configure compared to using manually entered routes
B. Does not require additional network security controls
C. Features enhanced network monitoring and visibility
D. Includes automatic changes and updates in network topology
Answer: (SHOW ANSWER)
Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.

Option A can be partly true in large environments, but the core "best reason" emphasized for dynamic routing is the automatic adaptation to topology changes. Option B is incorrect- dynamic routing may introduce additional security considerations (route filtering, authentication, neighbor control). Option C is not a defining advantage; monitoring visibility depends on tools/telemetry rather than routing type. Therefore, the strongest and most correct reason is automatic changes and updates in network topology.

NEW QUESTION: 150

A network administrator upgraded the wireless access points and wants to implement a configuration that will give users higher speed and less channel overlap based on device compatibility. Which of the following will accomplish this goal?

Freecram.net

A. 802.1X
B. MIMO
C. ESSID
D. Band steering
Answer: (SHOW ANSWER)
Band steering allows wireless access points to automatically direct capable devices to the 5GHz band, which typically has higher throughput and less interference than the 2.4GHz band, improving performance. The document confirms:
"Band steering helps balance wireless client loads by steering dual-band capable devices to the 5GHz band, which offers higher speeds and less channel congestion than 2.4GHz."

NEW QUESTION: 151
As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?
A. ARP spoofing
B. Evil twin
C. MAC flooding
D. DNS poisoning
Answer: C (LEAVE A REPLY)
* Definition of MAC Flooding:
* MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.
* Impact of MAC Flooding:
* CAM Table Overflow:When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.
* Switch Behavior:The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.
* Comparison with Other Attacks:
* ARP Spoofing:Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.
* Evil Twin:Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.
* DNS Poisoning:Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.
* Preventive Measures:
* Port Security:Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
* Network Segmentation:Use VLANs to segment network traffic and limit the impact of such attacks.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
A network administrator needs to limit devices that can connect to a small wireless network. The network consists of less than ten unique laptops, and no network changes are anticipated. Which of the following is the simplest way to accomplish this task?
A. ACLs
B. MAC filtering
C. NAC
D. Trusted zones
Answer: (SHOW ANSWER)
The correct answer is B. MAC filtering. MAC filtering is a straightforward method of restricting network access by allowing only specific device MAC (Media Access Control) addresses to connect to a wireless network. In a small, stable environment with fewer than ten devices and no expected changes, this approach is simple to implement and manage.
Each network interface card (NIC) has a unique MAC address, and wireless access points can be configured with a whitelist of approved addresses. Devices not on the list are denied access, effectively limiting connectivity to only authorized laptops. This aligns with CompTIA Network+ guidance for basic access control mechanisms in small or low-complexity networks.
Other options are less suitable in this scenario. ACLs (Access Control Lists) are typically used on routers and switches to control traffic flow based on IP addresses or protocols, not specifically device access to a wireless network. NAC (Network Access Control) provides more advanced authentication and posture assessment but is more complex and unnecessary for a small, static environment. Trusted zones refer to network segmentation concepts rather than device-level access control.
Thus, MAC filtering provides the simplest and most appropriate solution.

NEW QUESTION: 153
Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?
A. On-path
B. DDoS
C. ARP spoofing
D. MAC flooding
Answer: (SHOW ANSWER)
A Distributed Denial of Service (DDoS) attack leverages multiple computers or bots (botnet) to flood a target system with requests, overwhelming its resources and making it unavailable to legitimate users. This is a common tactic used by attackers to disrupt services. The document explains:
"A DDoS (Distributed Denial of Service) attack involves multiple computers (often called bots) simultaneously sending requests to a single resource, overwhelming the system and causing a denial of service to legitimate users."

NEW QUESTION: 154
An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?
A. SD-WAN

B. VXLAN
C. VPN
D. NFV
Answer: (SHOW ANSWER)
* Definition of SD-WAN:
* Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.
* Benefits of SD-WAN:
* Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
* Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
* Scalability: Easily scales to accommodate additional sites and bandwidth requirements.
* Comparison with Other Technologies:
* VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.
* VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.
* NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.
* Implementation:
* SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.
References:
* CompTIA Network+ course materials and networking solution guides.

NEW QUESTION: 155
Which of the following should an installer orient a port-side exhaust to when installing equipment?
A. The patch panel
B. The front of the IDF
C. The warm aisle
D. The administrator console
Answer: (SHOW ANSWER)
In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:
"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

NEW QUESTION: 156
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: 157
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: 158
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: C (LEAVE A REPLY)
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: 159
A network administrator deploys several new desk phones and workstation cubicles. Each cubicle has one assigned switchport. The administrator runs the following commands:
nginx
CopyEdit

switchport mode access
switchport voice vlan 69
With which of the following VLANs will the workstation traffic be tagged?
A. Private VLAN
B. Voice VLAN
C. Native VLAN
D. Data VLAN
Answer: (SHOW ANSWER)
When the command switchport voice vlan 69 is used, it tags the voice traffic with VLAN 69, while the workstation traffic continues untagged on the access VLAN, which is typically considered thedata VLAN.
This configuration enables both voice and data traffic over the same port while keeping them in separate VLANs for QoS and traffic management.
Reference:Section 2.2 - Switching Technologies and Features - "Switchport Voice VLAN Configuration"

NEW QUESTION: 160
Which of the following terms describes the capability in a public cloud to add or remove compute resources based on need?
Freecram.net
A. Scalability
B. Availability
C. Elasticity
D. Multitenancy
Answer: (SHOW ANSWER)
The correct answer is C. Elasticity. In cloud computing, elasticity refers to the ability to increase or decrease resources quickly based on current demand. If workloads rise, more compute resources can be allocated. If demand drops, those resources can be reduced again. That is exactly what the question is describing.
This is slightly different from scalability. Scalability is the broader idea that a system can grow to handle more workload. Elasticity focuses more on the dynamic, on-demand adjustment of resources as conditions change. In exam questions, wording like "add or remove based on need" usually points straight to elasticity.
The other answer choices do not fit. Availability is about uptime and service access. Multitenancy refers to multiple customers sharing underlying cloud infrastructure while remaining logically separated. Neither describes rapid expansion and contraction of compute resources.
From a Network+ study perspective, elasticity is one of the core cloud characteristics to remember because it explains why cloud services are useful for workloads that are unpredictable or variable. Instead of permanently building for peak demand, organizations can consume more or less compute as required. That makes elasticity the best answer.

NEW QUESTION: 161
While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?
A. LLDP
B. IKE
C. VLAN
D. netstat
Answer: (SHOW ANSWER)
Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.

Other options such as IKE (Internet Key Exchange), VLAN (Virtual LAN), and netstat (network statistics) are not suitable for identifying the switch and port information. IKE is used in setting up secure IPsec connections, VLAN is used for segmenting networks, and netstat provides information about active connections and listening ports on a host but not for discovering switch port details.
Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

NEW QUESTION: 162
A user ' s home mesh wireless network is experiencing latency issues. A technician has:
*Performed a speed test.
*Rebooted the devices.
*Performed a site survey.
*Performed a wireless packet capture.
The technician reviews the following information:

SSID	MAC	RSSI	Channel
Home	AAAAAA111112	-83dBm	11
Home	AAAAAA111113	-91dBm	11
Home	AAAAAA111114	-70dBm	11

freecram.net
CompTIA

The technician notices in the packet capture that frames were retransmitted. Which of the following is the most likely cause of the user ' s network issue?
A. The SSIDs should not be the same.
B. The network has too much overlap.
C. The devices are incompatible with the mesh network.
D. The nodes are underpowered.
Answer: (SHOW ANSWER)
*Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
*Same SSIDs (A) are expected in mesh networks.
*Device compatibility (C) would show different symptoms.
*Node power (D) affects coverage, not congestion.
Reference: CompTIA Network+ N10-009 Official Documentation - Wireless Troubleshooting & Signal Interference.

NEW QUESTION: 163
Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?
A. Fire suppression
B. Power budget
C. Temperature
D. Humidity
Answer: (SHOW ANSWER)
Switches in sealed enclosures are at risk of overheating because airflow is restricted. The temperature factor is critical since heat buildup can damage components, shorten device lifespan, and cause outages. Proper cooling or ventilation must be ensured.
A). Fire suppression is important for data centers but not the primary concern in a sealed box.

B). Power budget applies to PoE allocations, not environmental safety.
D). Humidity matters, but overheating is far more immediate in sealed environments.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Environmental considerations, switch installation, temperature control.

NEW QUESTION: 164
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: 165
Which of the following ports creates a secure connection to a directory service?
A. 22
B. 389
C. 445
D. 636
Answer: (SHOW ANSWER)
LDAP (Lightweight Directory Access Protocol) uses port 389 for standard connections and port 636 for LDAP over SSL (LDAPS), which secures directory service communication.
Breakdown of Options:
A). 22 - SSH port, not used for directory services.
B). 389 - Used for LDAP, but not encrypted.
C). 445 - Used for SMB file sharing, not LDAP.
D). 636 - Correct answer. LDAPS (LDAP over SSL/TLS) secures directory authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.
RFC 4511: Lightweight Directory Access Protocol (LDAP)

NEW QUESTION: 166
A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance. Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?
A. Speed mismatches
B. Load balancer settings
C. Flow control settings
D. Infrastructure cabling grade
Answer: (SHOW ANSWER)

Speed Mismatches: If NICs are set to different speeds (e.g., 100 Mbps on one side and 1 Gbps on the other), performance will degrade. Ensuring consistent speed settings between devices is crucial for optimal performance.
Load balancer settings (B): Applies to server load distribution, not endpoint speed.
Flow control settings (C): Can affect performance but is secondary to speed mismatches.
Infrastructure cabling grade (D): Relevant if the cables are unsuitable for gigabit speeds, but speed settings should be checked first.
Reference: CompTIA Network+ Official Study Guide, Domain 2.5 (Troubleshooting Network Issues).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167
An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. The technician examines the configuration and sees a self-assigned IP address. Which of the following is the most likely cause?
A. The DHCP server is not available
B. An RFC1918 address is being used
C. The TCP/IP stack is disabled
D. A static IP is assigned
Answer: (SHOW ANSWER)
When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a "self-assigned IP." This prevents communication outside the local link, including reaching the default gateway.
B). RFC1918 addresses are private ranges (10.x.x.x, 172.16-31.x.x, 192.168.x.x), but these are not self- assigned.
C). If the TCP/IP stack were disabled, the host wouldn't have any IP at all.
D). If a static IP were assigned, it would show a configured value, not self-assigned.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - IP addressing issues, DHCP failures, APIPA behavior.

NEW QUESTION: 168
Which of the following allows a standard user to log in to multiple resources with one account?
A. RADIUS
B. MFA
C. TACACS+
D. SSO
Answer: (SHOW ANSWER)
Single Sign-On (SSO) enables a user to access multiple resources or applications with one set of credentials, improving usability and security. The document confirms:
"Single Sign-On (SSO) allows a user to authenticate once and gain access to multiple resources or applications without needing to log in again for each. It streamlines the login process and improves security by reducing the number of passwords that need to be managed."

NEW QUESTION: 169

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: 170

A user tries to visit a website, but instead of the intended site, the page displays vmw.cba.com. Which of the following should be done to reach the correct website?

Feecram.net

A. Modify the CNAME record

B. Update the PTR record

C. Change the NTP settings

D. Delete the TXT record

Answer: (SHOW ANSWER)

A CNAME (Canonical Name) record maps an alias to the correct fully qualified domain name (FQDN). If a user is redirected to the wrong hostname, correcting or updating the CNAME ensures the alias points to the proper domain.

B). PTR record maps IP to hostname (reverse DNS), not forward website resolution.

C). NTP relates to time sync, irrelevant to DNS resolution.

D). TXT record stores metadata like SPF or DKIM info, not used for hostname aliasing.

References (CompTIA Network+ N10-009):

Domain: Network Standards, Protocols, and Implementations - DNS record types (A, AAAA, CNAME, PTR, TXT).

NEW QUESTION: 171

A network administrator needs to divide a Class B network into four equal subnets, each with a host range of 1,000 hosts. Which of the following subnet masks should the administrator use?

A. 255.255.0.0

B. 255.255.252.0

C. 255.255.255.0

D. 255.255.255.128

Answer: (SHOW ANSWER)

The best answer is B. 255.255.252.0 , which is a /22 mask. A Class B network starts with a default mask of 255.255.0.0 or /16 . The question says the administrator wants four equal subnets , which means borrowing 2 bits from the host portion, since 2 borrowed bits gives $2^2 = 4$ subnets . That moves the mask from /16 to /18 if subnetting is based only on splitting the Class B into four equal parts.

However, the answer choices point toward the host requirement as the deciding factor. Each subnet needs to support about 1,000 hosts . A /22 leaves 10 host bits , which gives 2¹# = 1024 total addresses , or 1022 usable hosts after subtracting the network and broadcast addresses. That fits the requirement. Among the options provided, 255.255.252.0 is the only mask that supports around 1,000 hosts per subnet.
The smaller masks, /24 and /25 , do not allow enough hosts. The default Class B mask, /16 , does not subnet the network at all. Based on the available choices and the host-capacity requirement, 255.255.252.0 is the correct exam answer.

NEW QUESTION: 172
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: 173
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: (SHOW ANSWER)
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: 174
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: 175
A network administrator wants an automatic alert to be sent when a switch ' s link status changes, administered through SNMP. Which of the following SNMP technologies will allow for this alert?
A. Trap
B. Object identifier
C. String
D. MIB
Answer: (SHOW ANSWER)
The right answer is A. Trap . In SNMP, a trap is an unsolicited notification sent from a managed device to the management system when a significant event happens. A switch detecting that an interface has gone up or down is a textbook example of the kind of event that can trigger this kind of message.
That is different from normal SNMP polling, where the monitoring server asks the device for status information on a schedule. With a trap, the device does not wait to be asked. It sends the alert immediately, which makes it useful for link failures, threshold violations, and other time-sensitive conditions.
The other choices are related to SNMP, but not in the same way. An object identifier (OID) points to a specific managed value. A string is commonly associated with SNMP community information in older versions. A MIB is the structured database of manageable objects. None of those are the actual alerting mechanism.
Because the question asks for an automatic alert when link status changes, the feature being described is clearly an SNMP trap .

NEW QUESTION: 176
Which of the following attacks utilizes a network packet that contains multiple network tags?
A. MAC flooding
B. VLAN hopping
C. DNS spoofing
D. ARP poisoning

Answer: (SHOW ANSWER)
VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.
Reference:
According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

NEW QUESTION: 177
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: 178
A junior network technician at a large company needs to create networks from a Class C address with 14 hosts per subnet. Which of the following numbers of host bits is required?
A. Two
B. Four
C. Three
D. One
Answer: (SHOW ANSWER)

NEW QUESTION: 179
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: 180

Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?

Freecram.net

A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.
Answer: (SHOW ANSWER)
After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

NEW QUESTION: 181
A company upgrades its wireless infrastructure with a 1Gbps backbone, new APs, and new tablets for all employees. However, the IT department notes that speeds are not improved from the previous tablets. Given the following network information, which of the following is the most likely cause of the performance issues?
A. AP 4 has no devices connected.
B. Too many devices are causing congestion.
C. APs do not have the correct VLAN assignment.
D. Switch bandwidth is creating a bottleneck.
Answer: (SHOW ANSWER)
The most likely answer is D. Switch bandwidth is creating a bottleneck . Even though the company upgraded the wireless environment with newer access points and new tablets, wireless performance still depends on the capacity of the wired network that the APs connect back to. If multiple APs are sending traffic through a shared switch uplink or limited switch bandwidth, that wired segment can become the choke point, preventing users from seeing the benefit of the newer wireless equipment.
This kind of issue shows up often when organizations focus on upgrading the wireless edge but do not account for the aggregate traffic load feeding into the switching infrastructure. Faster wireless standards can increase the amount of traffic that reaches the switch, but if the switching path cannot handle that volume efficiently, end-user throughput will still feel unchanged.
The other options are less convincing. One AP having no connected devices does not explain why speeds on active clients are not improved. VLAN assignment problems would more likely cause access or segmentation issues rather than a general performance ceiling. Device congestion can hurt performance, but the information given points more strongly to the wired backhaul as the limiting factor.
In this scenario, the wireless upgrade is being held back by the switching side of the network, making switch bandwidth bottleneck the best answer.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182
Which of the following would most likely be used as a replacement for a traditional VPN for remote users?
A. SD-WAN
B. SASE
C. Site-to-site VPN
D. Reverse proxy

Answer: B (LEAVE A REPLY)
A modern replacement for traditional remote-access VPN for users is SASE (Secure Access Service Edge).
Network+ highlights trends in remote connectivity and security where organizations move away from backhauling all user traffic through a VPN concentrator and instead use cloud-delivered security and access controls closer to the user. SASE combines networking and security capabilities-commonly including ZTNA (Zero Trust Network Access), secure web gateway (SWG), CASB, firewall-as-a-service (FWaaS), and centralized policy enforcement-so remote users can securely access applications without relying on a classic "connect to the corporate network first" VPN model.
SD-WAN primarily optimizes connectivity between sites and to cloud services, often for branch networks; it' s not typically the direct replacement for remote user VPN access. Site-to-site VPN connects networks (locations) and is not intended for individual remote users. A reverse proxy can publish specific internal web applications externally and provide some security functions, but it does not replace VPN broadly for remote user access to multiple internal resources the way SASE/Zero Trust access solutions do. Therefore, SASE is the best answer as the likely replacement for traditional remote-access VPN.

NEW QUESTION: 183
Which of the following allows an organization to map multiple internal devices to a single external-facing IP address?
A. NAT
B. BGP
C. OSPF
D. FHRP
Answer: (SHOW ANSWER)
NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.
B). BGP is a routing protocol.
C). OSPF is a link-state IGP.
D). FHRP provides redundant gateways, not IP sharing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - NAT, PAT, private-to-public IP mapping.

NEW QUESTION: 184
Which of the following is the best VPN to use for reducing data bandwidth requirements of the corporate network?
A. Split-tunnel
B. Site-to-site
C. Full-tunnel client
D. GRE tunnel
Answer: (SHOW ANSWER)
A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.
Site-to-site VPNs are for permanent links between locations.
Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.
GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

NEW QUESTION: 185
After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?
A. Check to see if the end connections were wrapped in copper tape before terminating.
B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
C. Connect the RX/TX wires to different pins.
D. Run a speed test on a device that can only achieve 100Mbps speeds.
Answer: (SHOW ANSWER)
* Importance of Proper Termination:
* Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).
* Interference Troubleshooting:
* Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.
* Why Other Options are Less Likely:
* Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.
* Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.
* Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds.
* Corrective Actions:
* Verify that all end connections are properly wrapped with copper tape before termination.
* Ensure that the shielding is continuous and properly grounded throughout the installation.
* Retest the cabling for interference after making corrections.
References:
* CompTIA Network+ study materials and structured cabling installation guides.

NEW QUESTION: 186
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: 187

A network administrator is setting up a firewall to protect the organization's network from external threats.
Which of the following should the administrator consider first when configuring the firewall?
A. Required ports, protocols, and services
B. Inclusion of a deny all rule
C. VPN access
D. Outbound access originating from customer-facing servers
Answer: (SHOW ANSWER)
When configuring a firewall, the first step is identifying which ports, protocols, and services are required for normal business operations. This ensures only legitimate traffic is allowed.
After establishing the required rules, a default deny rule is added for security.
B). Deny all rule is important, but it should come after defining required rules.
C). VPN access is a service to configure, but only after determining baseline needs.
D). Outbound traffic policies are part of refinement, not the first consideration.
References (CompTIA Network+ N10-009):
Domain: Network Security - Firewall configuration, rule order, least privilege.

NEW QUESTION: 188
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: 189
Which of the following allows a user to authenticate to multiple resources without requiring additional passwords?
A. SSO
B. MFA
C. SAML
D. RADIUS
Answer: (SHOW ANSWER)
The correct answer is SSO (Single Sign-On) because it enables a user to authenticate once and gain access to multiple systems or resources without being prompted to log in again. According to CompTIA Network+ (N10-009) security objectives, SSO improves usability and productivity while maintaining centralized authentication control. After the initial authentication, a trust relationship between systems allows the user to access additional applications seamlessly.

MFA (Multi-Factor Authentication) enhances security by requiring two or more authentication factors (something you know, have, or are), but it does not inherently provide access to multiple systems without repeated authentication events.
SAML (Security Assertion Markup Language) is an authentication and authorization protocol commonly used to implement SSO in web-based environments. While SAML supports SSO functionality, it is the underlying protocol rather than the access method itself.
RADIUS is a centralized authentication, authorization, and accounting (AAA) protocol used for network access control but does not specifically provide seamless multi-resource authentication without additional logins.
Therefore, SSO best describes authentication to multiple resources without requiring additional passwords.

NEW QUESTION: 190

After a recent security awareness phishing campaign, the cybersecurity team discovers that additional security measures need to be set up when users access potentially malicious websites. Which of the following security measures will best address this concern?

Freecram.net

A. Implement DNS filtering.
B. Update ACLs to only allow HTTPS.
C. Configure new IPS hardware.
D. Deploy 802.1X security features.
Answer: A (LEAVE A REPLY)
DNS filtering blocks access to known malicious websites by comparing domain requests against a list of allowed or blocked URLs. It is an effective defense against phishing and other web-based attacks.
From Andrew Ramdayal's guide:
"URL filtering restricts access to specific websites or web content by comparing URLs against a predefined list of allowed or blocked sites...commonly used to prevent users from accessing malicious sites."

NEW QUESTION: 191
A network administrator deploys new network hardware. While configuring the network monitoring server, the server could authenticate but could not determine the specific status of the hardware. Which of the following would the administrator most likely do to resolve the issue?
A. Use the public community string
B. Import the appropriate MIB
C. Set up a switchport analyzer and forward traffic
D. Configure SNMPv3 privacy
Answer: (SHOW ANSWER)
MIBs (Management Information Bases) define the variables and objects that SNMP can query on a device. If the monitoring server authenticates but cannot interpret the data, it likely lacks the correct MIB for that vendor or model. Importing the proper MIB allows the monitoring server to correctly display device status and metrics.
A). Using a public community string is insecure and not related to missing MIBs.
C). Switchport analyzer (SPAN) captures traffic for packet analysis, not SNMP monitoring.
D). SNMPv3 privacy adds encryption but doesn't fix missing MIB interpretation.
References (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP, MIBs, network monitoring systems.

NEW QUESTION: 192

A network administrator installs new cabling to connect new computers and access points. After deploying the equipment, the administrator notices a few of the devices are not connecting properly. The administrator moves the devices to a different port, but it does not resolve the issue. Which of the following should the administrator verify next?

A. Power budget

B. Device requirements

C. Port status

D. Cable termination

Answer: (SHOW ANSWER)

*Cable termination issues (e.g., improper crimping, loose connectors) can cause connectivity failures.

*Power budget (A) applies to PoE devices, not general cabling issues.

*Device requirements (B) relate to software/hardware compatibility, not wiring faults.

*Port status (C) would help if the issue was switch-related, but since moving devices didn't help, it's likely a cabling issue.

#Reference: CompTIA Network+ N10-009 Official Documentation - Cabling & Physical Layer Troubleshooting.

NEW QUESTION: 193

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: 194

The leadership team is updated on the results of an approved change request after a breach. Which of the following troubleshooting methodology steps is described in this example?

A. Establishing a theory of probable cause

B. Implementing the solution or escalating as necessary

C. Documenting findings, actions, outcomes, and lessons learned throughout the process

D. Establishing a plan of action to resolve the problem and identifying potential effects

Answer: (SHOW ANSWER)

The correct answer is C. Documenting findings, actions, outcomes, and lessons learned throughout the process. According to the CompTIA Network+ N10-009 troubleshooting methodology, the final step in the structured troubleshooting process involves documenting everything that occurred during the incident. This includes the root cause, actions taken, changes implemented (such as approved change requests), outcomes of those actions, and any lessons learned.

In the scenario, the key phrase is that leadership is being updated on the results after a breach and an approved change request. This clearly aligns with post-resolution communication and documentation, where technical teams report findings and outcomes to stakeholders. This step is critical for organizational knowledge, audit requirements, compliance, and improving future incident response.

The other options represent earlier steps in the troubleshooting process. Establishing a theory of probable cause occurs early when diagnosing the issue. Establishing a plan of action comes before implementing changes. Implementing the solution happens during remediation. However, none of these involve summarizing and communicating results after the fact. Therefore, updating leadership on results corresponds directly to the documentation and lessons-learned phase of the troubleshooting methodology.

NEW QUESTION: 195

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: 196
A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?
A. Security Service Edge
B. Data center interconnect
C. Infrastructure as code
D. Zero Trust architecture
Answer: (SHOW ANSWER)
The correct solution is a Data Center Interconnect (DCI). DCIs extend Layer 2 networks across geographically dispersed data centers, enabling seamless replication of services such as SAN storage, backup synchronization, or VM migrations. This ensures workloads and data can move between sites while maintaining the same VLANs and addressing.
A). Security Service Edge (SSE) provides cloud-delivered security functions like secure web gateways and CASB, not Layer 2 extension.
C). Infrastructure as code (IaC) automates deployment and management of network infrastructure but is unrelated to extending Layer 2 domains.
D). Zero Trust architecture is a security framework ensuring strict access control but doesn't address network connectivity between sites.
In scenarios where backups need replication between sites, Layer 2 extension is often required so systems can communicate as if they are in the same broadcast domain. DCI is specifically designed to provide this functionality reliably and securely.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - WAN technologies, data center interconnect, backup replication.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 197
After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:
LocationSpeed DownSpeed Up
Wireless laptop4.8 Mbps47.1 Mbps
Wired desktop5.2 Mbps49.3 Mbps
Firewall48.8 Mbps49.5 Mbps
Which of the following is the most likely issue?
A. Packet loss
B. Bottlenecking
C. Channel overlap
D. Network congestion
Answer: (SHOW ANSWER)
Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.
*Why not the other options?
*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.
*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.
*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

NEW QUESTION: 198
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: 199
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: 200
Which of the following is the final step in the ticket management process?
A. Escalating to senior management
B. Performing functional and non-functional testing
C. Documenting findings, outcomes, and lessons learned
D. Establishing a detailed action plan
Answer: (SHOW ANSWER)
The correct answer is Documenting findings, outcomes, and lessons learned because proper documentation and closure are the final steps in the ticket management and troubleshooting process. According to CompTIA Network+ (N10-009) objectives under network operations and troubleshooting methodology, once an issue is resolved, technicians must verify full system functionality, implement preventive measures if needed, and document the entire process before closing the ticket.
Documentation ensures that all relevant information-such as the root cause, corrective actions taken, configuration changes made, and lessons learned-is recorded for future reference. This supports knowledge base updates, trend analysis, compliance requirements, and improved response times for similar incidents.

Escalation (Option A) occurs earlier if the issue cannot be resolved at the current support tier. Establishing an action plan (Option D) is part of the remediation phase, not the final step. Functional and non-functional testing (Option B) occurs during verification before closure.
Therefore, comprehensive documentation and formal ticket closure represent the final step in the ticket management lifecycle.

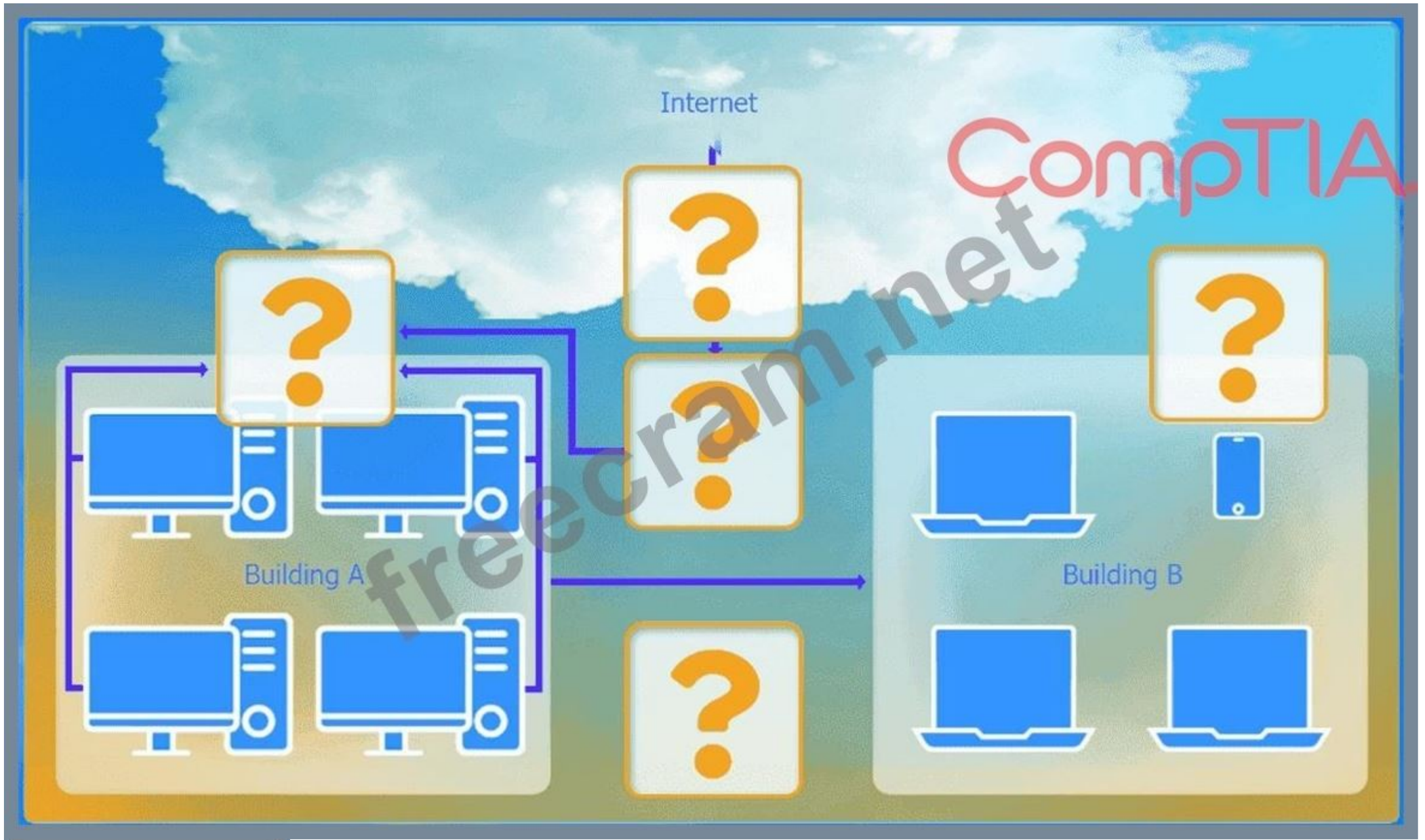
NEW QUESTION: 201
Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?
A. DNS poisoning
B. Denial-of-service
C. Social engineering
D. ARP spoofing
Answer: (SHOW ANSWER)
Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.References: CompTIA Network+ study materials.

NEW QUESTION: 202
A laptop user gets an error when trying to access the company's intranet site. A technician runs ipconfig /all with the following results:
Autoconfiguration IPv4 Address: 169.254.0.5 (Preferred)
Subnet Mask: 255.255.0.0
Default Gateway:
DHCP Server:
Which of the following is most likely causing the issue?
A. Short DHCP lease duration
B. IIS server malfunction
C. Address pool exhaustion
D. IDS misconfiguration
Answer: (SHOW ANSWER)
The correct answer is C. Address pool exhaustion. The laptop has assigned itself an address in the 169.254.x.x range, which is an APIPA address. That happens when the device is configured to use DHCP but cannot successfully obtain an address lease from a DHCP server. The missing default gateway and DHCP server entries support that conclusion.
Among the choices, the most likely reason is that the DHCP scope has run out of available addresses. When the pool is exhausted, new clients cannot receive a valid IP configuration and fall back to an automatic private address. As a result, the laptop will not be able to reach internal company resources like the intranet because it is not properly configured for the network.
The other answers do not fit the evidence. A short DHCP lease duration may cause more frequent renewals, but it does not directly explain the self-assigned APIPA address. An IIS server malfunction would affect the web service itself, not the client's local IP configuration. An IDS misconfiguration also would not normally result in a 169.254 address on the host.
The output clearly indicates a DHCP assignment failure, and from the options provided, address pool exhaustion is the best match.

NEW QUESTION: 203
A network administrator needs to connect a department to a new network segment. They need to use a DHCP server located on another network. Which of the following can the administrator use to complete this task?
A. IP Helper
B. Reservation

C. Exclusion
D. Scope
Answer: (SHOW ANSWER)
An IP Helper (IP Helper Address) allows DHCP requests to pass through routers and reach a DHCP server on another network.
* DHCP broadcasts are not forwarded across routers by default, so an IP Helper Address is needed to relay the request.
* This is crucial for large networks where a single DHCP server serves multiple subnets.
* Option B (Reservation): Ensures a specific IP address is assigned to a MAC address but does not relay DHCP across networks.
* Option C (Exclusion): Prevents specific IP addresses from being assigned, but does not help with DHCP relay.
* Option D (Scope): Defines the range of IP addresses available for DHCP clients but does not assist in cross-network communication.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: DHCP and IP Addressing

NEW QUESTION: 204
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.



- Hub
- Switch
- WAP
- Firewall
- Router
- Wireless range extender

CompTIA
freecram.net

CompTIA

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

freecram.net

freecram.net
CompTIA

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:

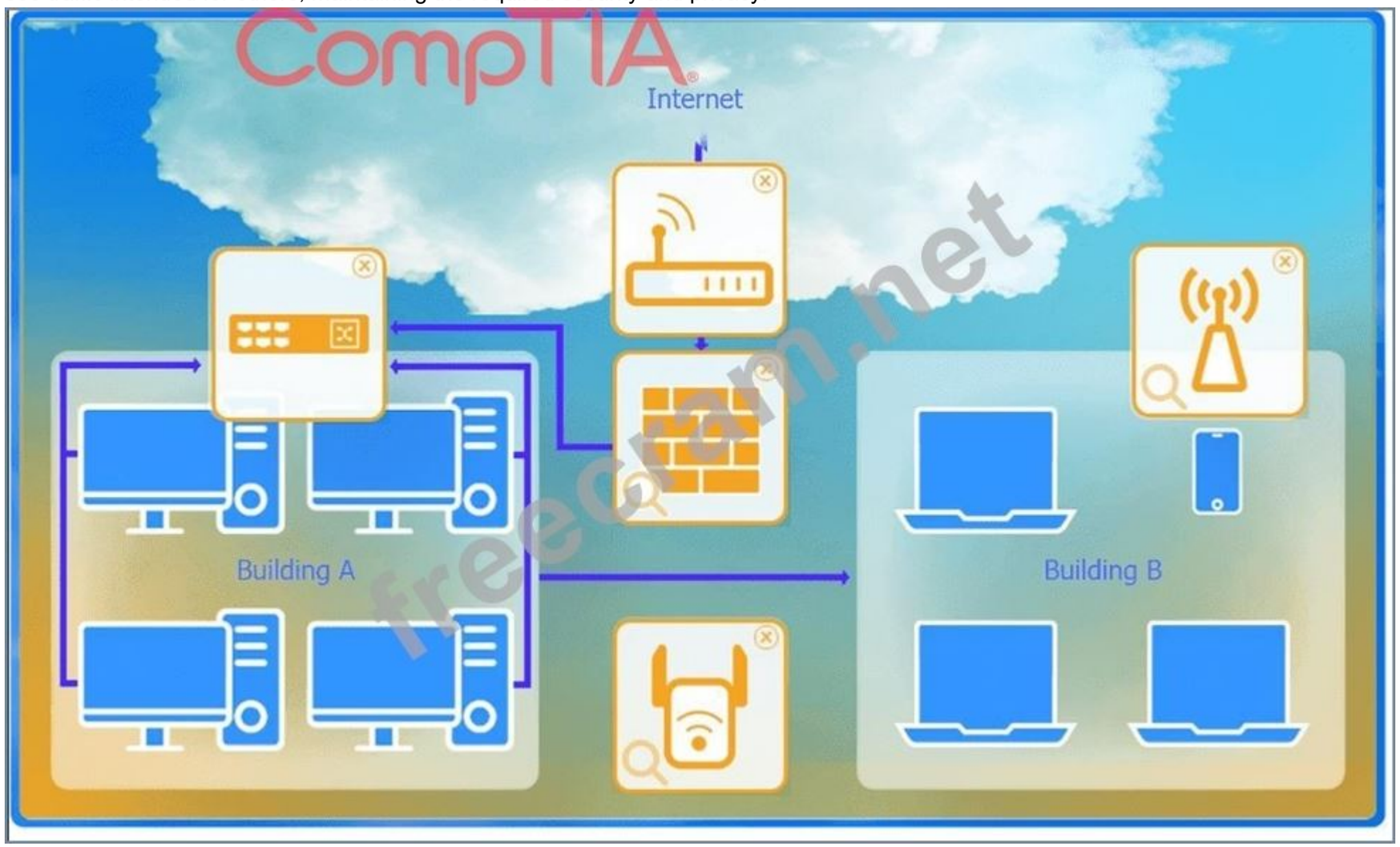
Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

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: 205
Which of the following would most likely be used to implement encryption in transit when using HTTPS?
A. SSH
B. TLS
C. SCADA
D. RADIUS
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.
* A. SSH secures remote shell and tunnels, not HTTPS.
* C. SCADA refers to industrial control systems, not a transport security protocol.
* D. RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.
References (CompTIA Network+ N10-009):
* Domain: Network Standards, Protocols, and Implementations - Web protocols (HTTP/HTTPS), TLS handshake and purpose, encryption in transit.

NEW QUESTION: 206
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: 207
A medical clinic recently configured a guest wireless network on the existing router. Since then, guests have been changing the music on the speaker system. Which of the following actions should the clinic take to prevent unauthorized access? (Select two).
A. Isolate smart devices to their own network segment.
B. Configure IPS to prevent guests from making changes.
C. Install a new AP on the network.
D. Set up a syslog server to log who is making changes.
E. Change the default credentials.
F. Configure GRE on the wireless router.
Answer: (SHOW ANSWER)
*A. Isolate smart devices to their own network segment: Network segmentation using VLANs or separate SSIDs ensures that smart devices (like speakers) are not on the same network as guests, preventing unauthorized control.
*E. Change the default credentials: Many IoT devices (e.g., smart speakers) come with default usernames and passwords. If these are not changed, unauthorized users can easily take control.
*Why not the other options?
*B. Configure IPS: IPS (Intrusion Prevention System) detects threats but cannot block specific guest actions on an IoT device.
*C. Install a new AP: A new access point does not solve the unauthorized control issue.
*D. Set up a syslog server: Helps with logging, but does not prevent unauthorized access.
*F. Configure GRE: Generic Routing Encapsulation (GRE) is used for VPN tunneling, which is irrelevant in this case.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security

NEW QUESTION: 208
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: 209
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: A (LEAVE A REPLY)
* 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: 210
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?
Freecram.net
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: 211
Which of the following is a use case for a PaaS environment?
A. Mobile access
B. E-commerce site

C. Application development
D. Cloud-native software
Answer: (SHOW ANSWER)
PaaS (Platform as a Service) is best suited for application development because it provides a managed platform that includes the runtime environment, development frameworks, middleware, databases (often), and build/deployment tooling. In a PaaS model, the cloud provider manages the underlying infrastructure (servers, storage, networking, OS patching, and often the application runtime), allowing developers to focus on writing code, testing, and releasing applications quickly. This aligns with Network+ cloud concepts where service models are compared by responsibility: PaaS reduces operational overhead for the customer and accelerates development through standardized environments and automation.
Mobile access is a use case for remote access solutions (VPN, zero trust access, MDM), not specifically PaaS.
An e-commerce site could be hosted using many models (IaaS, PaaS, SaaS), so it's not the most specific match. Cloud-native software describes an architectural style (microservices, containers, managed services) and can be built using PaaS components, but it is broader than a single "use case" and is not as directly tied to the PaaS definition as application development is. Therefore, application development is the clearest and most accurate PaaS use case.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 212
A server administrator needs to add a record to the company's DNS server to verify ownership of a web domain. The administrator has the record's name and value. Which of the following record types should the administrator use to add the record to the DNS server?
A. TXT
B. A
C. PTR
D. CNAME
Answer: (SHOW ANSWER)
To verify ownership of a domain, providers commonly require adding a TXT record to DNS containing a specific validation token (a name/value pair). A TXT (text) record is designed to store arbitrary text data associated with a domain or hostname, which makes it ideal for domain verification workflows used by certificate authorities, email security (SPF/DKIM/DMARC-related entries), and third-party services that need proof of administrative control over DNS. This fits Network+ DNS objectives that cover common record types and their practical purposes in real deployments.
An A record maps a hostname to an IPv4 address and is used for name-to-address resolution, not ownership verification. A PTR record provides reverse DNS mapping (IP address to hostname) and is stored in reverse lookup zones, not typically used for validating web domain ownership. A CNAME record creates an alias from one hostname to another canonical hostname; while sometimes used in service integrations, the classic
"record name + token value" ownership verification is most directly and universally satisfied by a TXT record. Therefore, TXT is the correct choice given the requirement and the provided record name and value.

NEW QUESTION: 213
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: 214
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: 215
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: 216
Which of the following is the most closely associated with segmenting compute resources within a single cloud account?
A. Network security group
B. IaaS
C. VPC
D. Hybrid cloud
Answer: C (LEAVE A REPLY)
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

NEW QUESTION: 217
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: 218
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: 219
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: 220
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?
Freecram.net
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: 221
A network administrator is troubleshooting issues with a DHCP server at a university. More students have recently arrived on campus, and the users are unable to obtain an IP address. Which of the following should the administrator do to address the issue?
A. Enable IP helper.
B. Change the subnet mask.
C. Increase the scope size.
D. Add address exclusions.
Answer: (SHOW ANSWER)
The issue is that more students have arrived on campus, meaning the available IP addresses are exhausted. To fix this, the administrator should increase the DHCP scope size to allow more devices to obtain IP addresses.
Breakdown of Options:

A). Enable IP helper - IP helper is used to forward DHCP requests across different subnets. However, the problem here is that the DHCP scope is full, not that requests are not reaching the server.
B). Change the subnet mask - The subnet mask determines the number of available hosts, but changing it without increasing the IP pool does not help.
C). Increase the scope size - Correct answer. Expanding the DHCP scope provides more IP addresses for assignment.
D). Add address exclusions - Exclusions reserve IP addresses, which would further reduce available addresses instead of solving the issue.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Compare and contrast IP addressing schemes.
RFC 2131: Dynamic Host Configuration Protocol (DHCP)

NEW QUESTION: 222
Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?
A. Crash cart
B. Jump box
C. Secure Shell (SSH)
D. Out-of-band management
Answer: (SHOW ANSWER)
If a network appliance fails to start, standard remote access methods like SSH won't work. Instead, Out-of- Band (OOB) management provides a dedicated access path (e.g., a console port or iDRAC/iLO), allowing administrators to troubleshoot devices even when the network is down.
Breakdown of Options:
A). Crash cart - A physical monitor/keyboard setup, not a remote solution.
B). Jump box - A hardened system used for secure remote access but requires the device to be operational.
C). Secure Shell (SSH) - Requires the device to be fully booted and network-connected.
D). Out-of-band management - # Correct answer. Provides independent access for troubleshooting failed network devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network device management concepts.

NEW QUESTION: 223
A company is upgrading its wireless network. Currently, each AP broadcasts a wireless LAN name depending on the location in the building. Which of the following configurations allows a single wireless LAN name to be broadcast across the entire building?
A. ESSID
B. Wireless mesh
C. Band steering
D. WPA3
Answer: (SHOW ANSWER)
The correct answer is A. ESSID. An ESSID (Extended Service Set Identifier) is used when multiple wireless access points are configured to present the same wireless network name (SSID) across a larger coverage area, such as an entire building or campus floor. This allows users to move from one location to another while remaining connected to what appears to be a single wireless network. In practice, this supports seamless roaming between APs when they are properly configured with the same SSID, compatible security settings, and coordinated channel planning.
The other options do not fit the requirement. Wireless mesh is a topology that allows APs to connect to one another wirelessly, but it does not by itself describe using one common WLAN name across all APs. Band steering pushes dual-band clients toward the 5 GHz or 6 GHz band for better performance; it is not about creating one building-wide WLAN name. WPA3 is a wireless security standard and relates to encryption and authentication, not SSID design.

The key phrase in the question is "a single wireless LAN name across the entire building", which points directly to an ESSID deployment.

NEW QUESTION: 224
A network administrator needs to implement a solution to filter access to the internet. Which of the following should the administrator most likely implement?
A. Router
B. Cloud gateway
C. Proxy
D. Intrusion detection system
Answer: (SHOW ANSWER)
A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.
A). A router directs traffic but doesn't filter internet sites by itself.
B). A cloud gateway could also filter, but the most direct answer is proxy.
D). An IDS detects suspicious activity but doesn't filter browsing access.
References (CompTIA Network+ N10-009):
Domain: Network Security - Proxy servers, filtering, access control.

NEW QUESTION: 225
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: 226
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:
1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 '
6 *
7 *
Which of the following command-line tools is the network administrator using?
A. tracert
B. netstat
C. tcpdump
D. nmap
Answer: (SHOW ANSWER)
* Understanding Tracert:
* tracert(Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.
* Output Analysis:
* The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds.
* The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.
* Comparison with Other Tools:
* netstat:Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.
* tcpdump:Captures network packets for analysis, used for detailed network traffic inspection.
* nmap:A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.
* Usage:
* tracerthelps identify the path to a destination and locate points of failure or congestion in the network.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

NEW QUESTION: 228
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: A (LEAVE A REPLY)
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: 229
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: 230
A virtual machine has the following configuration:
*IPv4 address: 169.254.10.10
*Subnet mask: 255.255.0.0
The virtual machine can reach colocated systems but cannot reach external addresses on the Internet.
Which of the following Is most likely the root cause?
Freecram.net
A. Thesubnet mask is incorrect.
B. TheDHCP server is offline.
C. TheIP address is an RFC1918 private address.
D. TheDNS server is unreachable.
Answer: (SHOW ANSWER)
Understanding the 169.254.x.x Address:
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.
DHCP Server Offline:

APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.
Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.
Comparison with Other Options:
The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.
The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-
172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.
The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.
Troubleshooting Steps:
Verify the DHCP server's status and connectivity.
Restart the DHCP service if necessary.
Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).
References:
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

NEW QUESTION: 231
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: 232
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: A (LEAVE A REPLY)
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: 233
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: 234
Which of the following connectors provides console access to a switch?
A. ST
B. RJ45
C. BNC
D. SFP
Answer: (SHOW ANSWER)
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: 235
Which of the following allows a user to connect to an isolated device on a stand-alone network?
A. Jump box
B. API gateway
C. Secure Shell (SSH)
D. Clientless VPN

Answer: (SHOW ANSWER)
A jump box is a hardened system that provides secure access to isolated or sensitive devices on a separate network.
Breakdown of Options:
A). Jump box - # Correct answer. Acts as a middle point for secure remote access.
B). API gateway - Used for managing API calls, not remote access to isolated devices.
C). Secure Shell (SSH) - Requires direct connectivity, which may not be available for an isolated device.
D). Clientless VPN - Allows web-based VPN access, but does not guarantee access to isolated devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Implement secure remote access methods.

NEW QUESTION: 236
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: 237
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: 238
A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?
A. 11MHz
B. 20MHz
C. 40MHz
D. 80MHz
E. 160MHz
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

NEW QUESTION: 239
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: 240
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?
Freecram.net
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: 241
Which of the following best explains the role of confidentiality with regard to data at rest?
A. Datacanbe accessedby anyone on the administrative network.
B. Datacanbe accessedremotely with proper training.
C. Datacanbe accessedafter privileged access Is granted.
D. Datacanbe accessedafter verifying the hash.
Answer: (SHOW ANSWER)
* Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.
* Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.
* Incorrect Options:
* A. "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
* B. "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
* D. "Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.
CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 242
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: 243
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: 244
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: (SHOW ANSWER)
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:

https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)