# CompTIA.N10-009.v2026-07-27.q223

| | |
|---|---|
| **Exam Code:** | N10-009 |
| **Exam Name:** | CompTIA Network+ Certification Exam |
| **Certification Provider:** | CompTIA |
| **Free Question Number:** | 223 |
| **Version:** | v2026-07-27 |
| **# of views:** | 104 |
| **# of Questions views:** | 2349 |
| https://www.freecram.net/torrent/CompTIA.N10-009.v2026-07-27.q223.html | |

**NEW QUESTION: 1**
A network administrator is reviewing a production web server and observes the following output from the netstat command:
Which of the following actions should the network administrator take to harden the security of the web server?
**A.** Disable the unused ports.
**B.** Enforce access control lists.
**C.** Perform content filtering.
**D.** Set up a screened subnet.
**Answer: A (LEAVE A REPLY)**
The netstat output shows that multiple ports are open, including Telnet (23), FTP (20), and TFTP (69), which are potential security risks. Disabling unused ports minimizes the attack surface, reducing security vulnerabilities.
Breakdown of Options:
A). Disable the unused ports - Correct answer. Unused ports should be closed to prevent unauthorized access.
B). Enforce access control lists - ACLs help control access but do not disable unnecessary services.
C). Perform content filtering - Content filtering controls web traffic, not port security.
D). Set up a screened subnet - A DMZ (screened subnet) improves security but does not address open ports.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Given a scenario, implement network security measures.
CIS Benchmark for Linux & Windows Server Hardening

**NEW QUESTION: 2**
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: 3**
Which of the following steps of the troubleshooting methodology would most likely involve comparing current throughput tests to a baseline?
**A.** Implement the solution
**B.** Verify full system functionality
**C.** Document findings
**D.** Test the theory
**Answer: (SHOW ANSWER)**
Verifying full system functionality occurs after implementing a fix. This step ensures the solution resolved the issue and that performance is back to expected levels. Comparing current throughput to baseline measurements is part of validation testing to confirm everything is within normal operational parameters.
A). Implement the solution applies the fix but does not confirm results.
C). Document findings happens at the end of troubleshooting.
D). Test the theory comes earlier, when trying to confirm the suspected cause.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Troubleshooting methodology steps, baselines, verification testing.

**NEW QUESTION: 4**
Which of the following cable types allows the use of QSFP ports without requiring transceivers?
**A.** Multimode
**B.** Twinaxial
**C.** RG11
**D.** Category 6
**Answer: (SHOW ANSWER)**
Twinaxial (Direct Attach Copper / DAC) cables can plug directly into QSFP ports without needing separate optical transceivers. They are cost-effective for short-distance, high-speed connections (commonly in data centers).
A). Multimode fiber requires SFP/QSFP transceivers to convert electrical signals to optical.
C). RG11 is coaxial cable for broadband/cable TV, not used in QSFP ports.
D). Category 6 is twisted-pair Ethernet cabling, not directly compatible with QSFP ports.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Cable types, QSFP, DAC (Twinaxial), transceiver requirements.

**NEW QUESTION: 5**
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: 6**
A network administrator wants to implement security zones in the corporate network to control access to only individuals inside of the corporation. Which of the following security zones is the best solution?
**A.** Extranet
**B.** Trusted
**C.** VPN
**D.** Public
**Answer: (SHOW ANSWER)**
Introduction to Security Zones:
Security zones are logical segments within a network designed to enforce security policies and control access.
They help in segregating and securing different parts of the network.
Types of Security Zones:
Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.
Extranet: This zone allows controlled access to external partners, vendors, or customers.
VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.
Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.
Trusted Zone Implementation:
The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone.
Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.
Example Configuration:
Firewall Rules: Set up rules to allow traffic only from internal IP addresses.
Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.

Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.
Explanation of the Options:
A). Extranet: Suitable for external partners, not for internal-only access.
B). Trusted: The correct answer, as it provides controlled access to internal corporate users.
C). VPN: A method for secure remote access, not a security zone itself.
D). Public: Suitable for public access, not for internal corporate users.
Conclusion:
Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security.
References:
CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9 Basic Configuration Commands).

**NEW QUESTION: 7**
A customer wants to separate the finance department from the marketing department. The network administrator suggests segmenting the existing Class C network into two sections and readdressing all devices appropriately. Which of the following subnet masks should the network administrator use?
**A.** /24
**B.** /25
**C.** /26
**D.** /27
**Answer: (SHOW ANSWER)**
The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.
A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128). This creates two subnets, each with
128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.
A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.
The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

**NEW QUESTION: 8**
Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other non-video applications on the network. Which of the following symptoms describes the users' reported issues?
**A.** Latency
**B.** Packet loss
**C.** Bottlenecking
**D.** Jitter
**Answer: B (LEAVE A REPLY)**
Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:
Users report connectivity issues and lag during video meetings.
The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.

Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.
Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.
Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.
Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Connectivity Issues

**NEW QUESTION: 9**
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: 10**
A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org. Which of the following records should the administrator use?

**A.** SOA
**B.** MX
**C.** CNAME
**D.** NS
**Answer: (SHOW ANSWER)**
A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.
Reference:
The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

**NEW QUESTION: 11**
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: 12**
A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switch ports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select TWO).
**A.** Change network translation definitions
**B.** Enable 802.1Q
**C.** Implement a routing protocol
**D.** Set up voice VLANs
**E.** Reconfigure the DNS
**F.** Place devices in the perimeter network
**Answer: (SHOW ANSWER)**
To support VoIP on the same physical ports used by computers:
B). Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.
D). Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.
Other options are not directly related to configuring VoIP over existing ports:
A). Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.
C). Routing protocols are not necessary at the switch level for VLAN setup.
E). DNS is not required for the switch or VLAN setup.
F). Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.
# Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

**NEW QUESTION: 13**
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: 14**
A company security policy requires all network traffic from remote employees ' corporate laptops to use the company's VPN. Which of the following network access methods best describes this scenario?
**A.** Clientless VPN
**B.** Full-tunnel
**C.** Site-to-site tunnel
**D.** Split-tunnel
**Answer: (SHOW ANSWER)**
The correct answer is Full-tunnel because the policy requires all network traffic from remote corporate laptops to pass through the company's VPN. In a full-tunnel VPN configuration, once the VPN connection is established, all traffic-including internet-bound traffic-is routed through the corporate network before reaching its destination. This ensures centralized monitoring, content filtering, logging, and enforcement of security controls such as IDS/IPS and firewalls.
According to CompTIA Network+ (N10-009) security objectives, full-tunnel VPNs enhance security by preventing users from directly accessing the internet from their local connection, thereby reducing exposure to local network threats (e.g., public Wi-Fi attacks).
A split-tunnel VPN (Option D) allows users to access the internet directly while only sending corporate- bound traffic through the VPN, which does not meet the "all traffic" requirement. A site-to-site tunnel (Option C) connects entire networks rather than individual remote users. A clientless VPN (Option A) typically provides web-based access without a full network tunnel and does not necessarily route all traffic.
Therefore, full-tunnel best matches the policy requirement.

**NEW QUESTION: 15**
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:

**NEW QUESTION: 16**
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: 17**
Which of the following describes the best reason for using BGP?
**A.** Preventing a loop within a LAN
**B.** Improving reconvergence times
**C.** Exchanging router updates with a different ISP
**D.** Sharing routes with a Layer 3 switch
**Answer: (SHOW ANSWER)**
BGP (Border Gateway Protocol) is used for routing data between different ISPs, making it essential for the functioning of the internet. Its primary use is for exchanging routing information between autonomous systems, especially different ISPs. Preventing loops within a LAN is handled by protocols like Spanning Tree Protocol (STP), while improving reconvergence times and sharing routes with a Layer 3 switch are functions of other protocols or internal mechanisms.
Reference:
The CompTIA Network+ training emphasizes BGP's role in the exchange of routing information across different ISPs and autonomous systems.

**NEW QUESTION: 18**

A new backup system takes too long to copy files to the new SAN each night. A network administrator makes a simple change to the network and the devices to decrease backup times. Which of the following does the network administrator change?

**A.** QoS

**B.** SDN

**C.** MTU

**D.** VXLAN

**E.** TTL

**Answer: (SHOW ANSWER)**

Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput - especially for large file transfers like backups.

A). QoS prioritizes traffic but doesn't reduce backup times directly.

B). SDN is a network management model, not a parameter change.

D). VXLAN encapsulates VLANs, not relevant to backup speeds.

E). TTL is for packet lifetime, not throughput.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - MTU, jumbo frames, performance tuning.

**NEW QUESTION: 19**

A user reports issues accessing a file server on a LAN with the IP address 192.168.50.140 at a large facility with incomplete infrastructure documentation. The following are the results of the ping command:

ping -c 10 192.168.50.140

Packets: Sent = 10, Received = 5, Lost = 5 (50% loss)

Round-trip times: Minimum = 3ms, Maximum = 144ms, Average = 42ms

Which of the following should a technician do next to continue troubleshooting the issue at the switch with minimal impact ?

**A.** Perform toning and probe.

**B.** Replace the cable.

**C.** Visually locate the fault.

**D.** Restart the switch.

**Answer: (SHOW ANSWER)**

The ping results show intermittent connectivity (50% packet loss) with highly variable latency, which commonly indicates a Layer 1/Layer 2 problem (e.g., damaged cable pairs, bad patch-panel termination, failing switch port, duplex/negotiation issues, or excessive errors on the interface). Because the facility has incomplete documentation , the technician's first priority at the switch is to positively identify the correct switch port and cable path associated with the file server before making disruptive changes.

Using a tone generator and probe aligns with Network+ troubleshooting objectives that emphasize selecting the appropriate tool and following an efficient, structured process: identify the problem, establish a theory, test, and then implement the least disruptive fix. Toning/probing helps map the server's drop to the switch port (even through patch panels) so the technician can then check that specific interface for errors/discards, CRCs, speed/duplex negotiation status, and link stability -all without rebooting the switch or immediately replacing hardware.

By contrast, restarting the switch is high-impact, and replacing a cable is a change best performed after the correct run/port is confirmed.

**NEW QUESTION: 20**

A network engineer is configuring network ports in a public office. To increase security, the engineer wants the ports to allow network connections only after authentication. Which of the following security features should the engineer use?



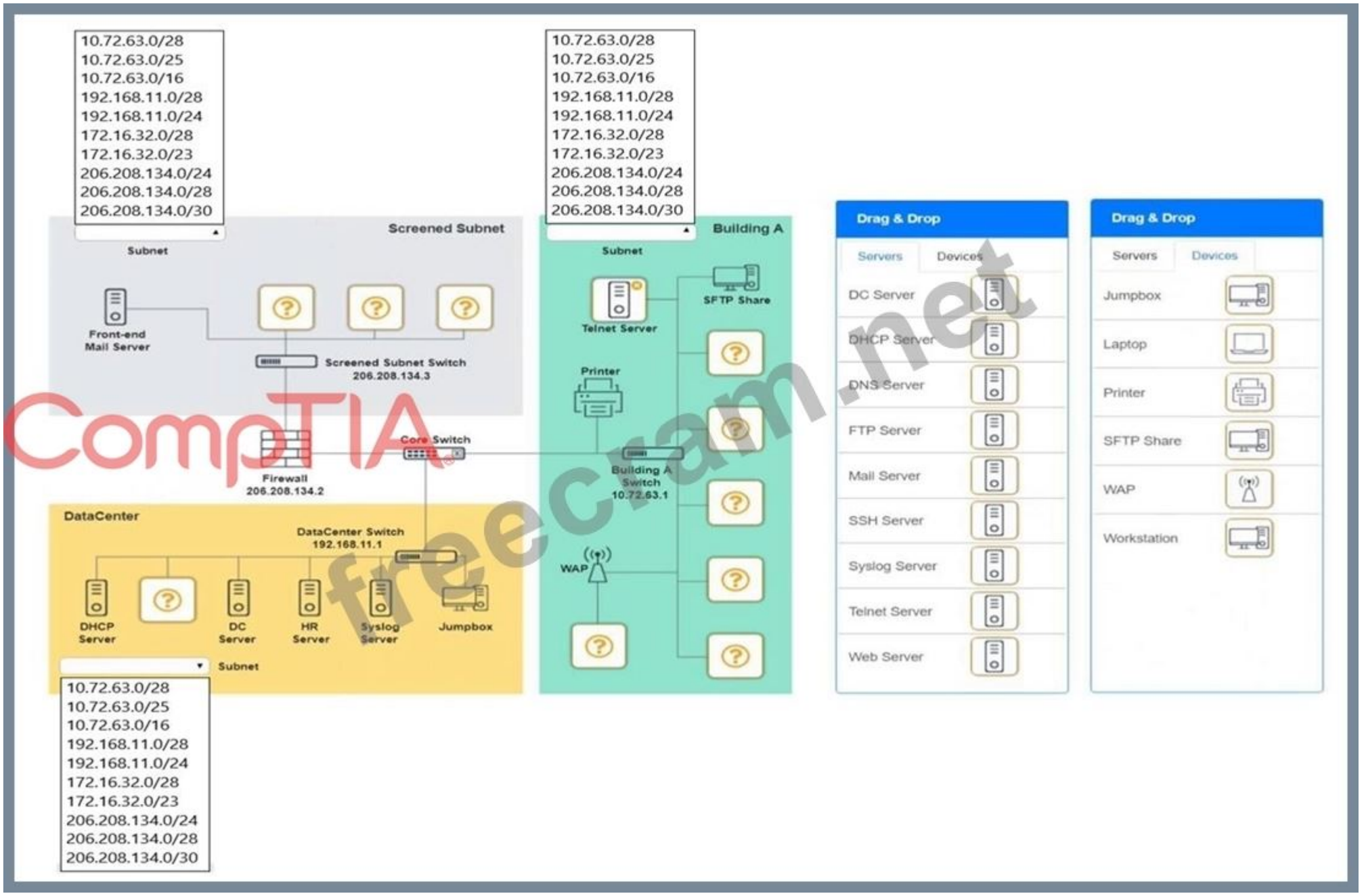
**A.** Port security
**B.** 802.1X
**C.** MAC filtering
**D.** Access control list
**Answer: (SHOW ANSWER)**
802.1X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be
"always on."
A). Port security restricts by MAC addresses but does not authenticate users.
C). MAC filtering is easily spoofed and weaker than 802.1X.
D). ACLs filter traffic but do not enforce port-based authentication.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, port-based security.

**NEW QUESTION: 21**
A customer purchases a new UTM device and wants the development team to integrate some of the device's data-reporting capabilities into the company's custom internal support software. Which of the following features should the development team use to obtain the device's data?
**A.** API
**B.** SNMPv2c
**C.** SIEM
**D.** MIB
**Answer: (SHOW ANSWER)**
An API (Application Programming Interface) is the best choice when a development team needs to integrate a device's reporting data directly into custom software. In Network+ (N10-009) objectives, network operations commonly include device management, monitoring, and automation, and APIs are a key method for programmatic access to operational data (often via REST/HTTPS with structured formats like JSON). This enables the internal support application to pull dashboards, health metrics, events, configuration details, and reporting outputs in a controlled, developer-friendly way.
SNMPv2c is primarily used for network monitoring and polling counters/alerts, but it is less secure (community strings) and is not as flexible for modern application integration as an API. A MIB is not a data- access "feature" by itself; it's the schema/definitions SNMP uses to describe managed objects. A SIEM is a separate security analytics platform that collects and correlates logs/events-useful for security operations, but not the direct interface a custom support tool would typically call to retrieve device reporting data.

**NEW QUESTION: 22**
Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed.
Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?
**A.** WPS configuration
**B.** Signal strength
**C.** Channel frequency
**D.** Power budget
**Answer: (SHOW ANSWER)**

When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.
A). WPS applies to Wi-Fi, not cellular repeaters.
C). Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.
D). Power budget applies to PoE and wired devices, not mobile phones.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

**NEW QUESTION: 23**
You are tasked with verifying the following requirements are met in order to ensure network security.
Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.




**Answer:**

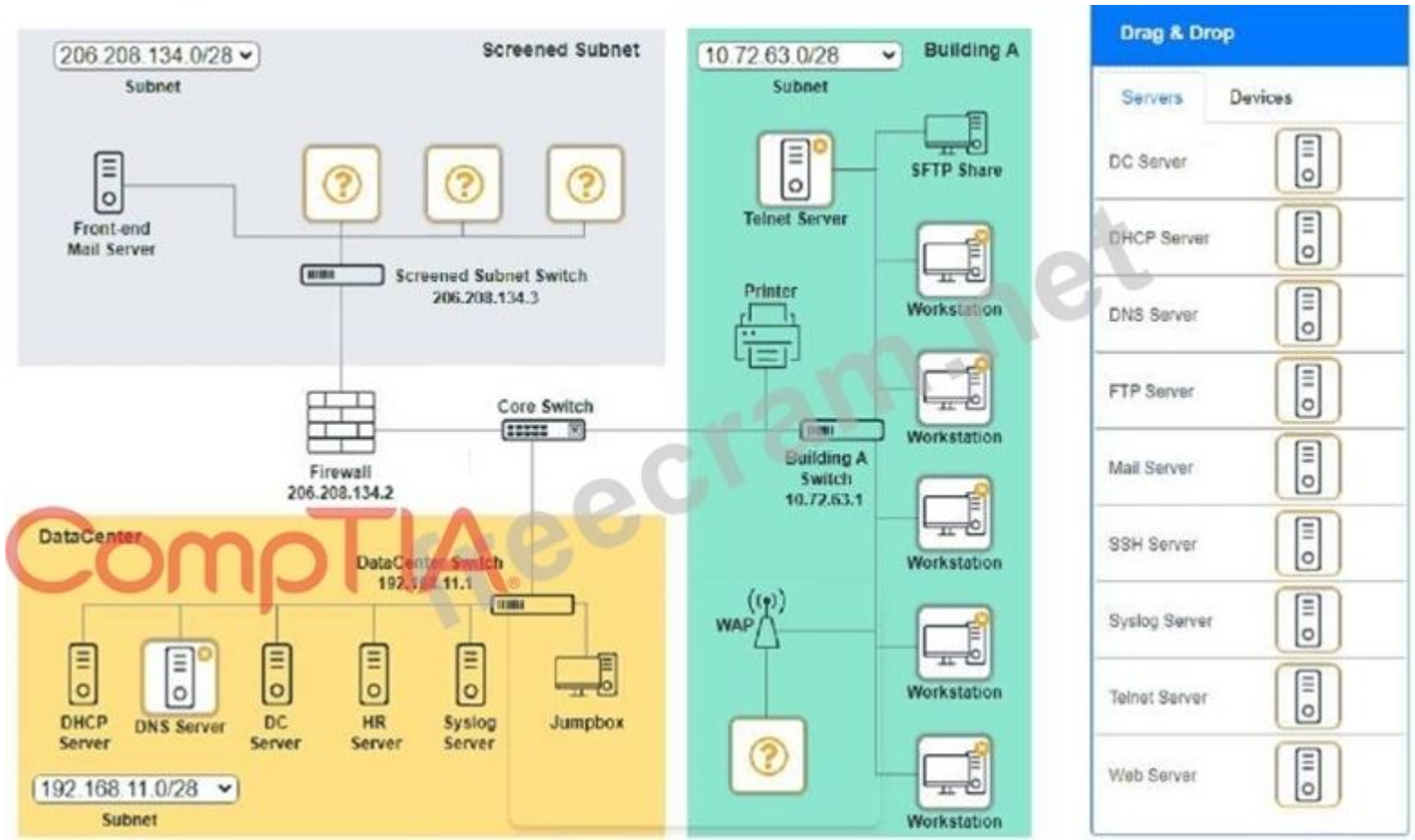
See explanation below.

Explanation:

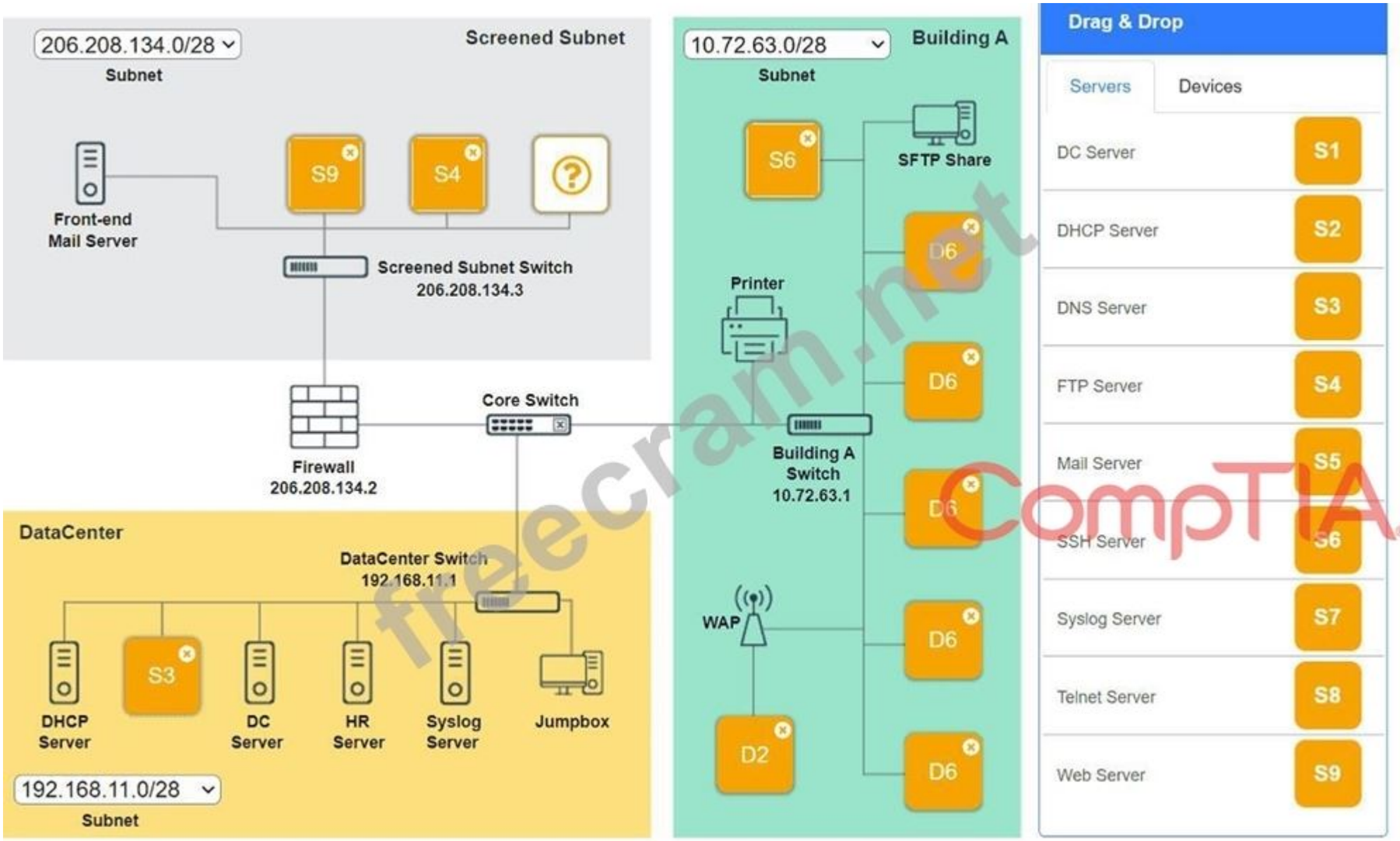
Screened Subnet devices - Web server, FTP server

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

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




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




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

**NEW QUESTION: 24**
A network administrator receives complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?
**A.** Enable spanning tree
**B.** Configure port security
**C.** Change switchport speed limits
**D.** Enforce 802.1Q tagging
**Answer: (SHOW ANSWER)**
Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.
B). Port security controls endpoint MAC addresses, not loops.
C). Speed limits address bandwidth, not loop prevention.
D). 802.1Q tagging allows VLAN separation but does not resolve loops.
References (CompTIA Network+ N10-009):

Domain: Network Operations - Loop prevention, spanning tree, switch design.

**NEW QUESTION: 25**
A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?
**A.** Multitenancy
**B.** VPC
**C.** NFV
**D.** SaaS
**Answer: (SHOW ANSWER)**
Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. References: CompTIA Network+ Exam Objectives and official study guides.

**NEW QUESTION: 26**
Which of the following services runs on port 636?
**A.** SMTP
**B.** Syslog
**C.** TFTP
**D.** LDAPS
**Answer: (SHOW ANSWER)**
LDAP over SSL (LDAPS) uses port 636 to provide secure, encrypted authentication for directory services.
Breakdown of Options:
A). SMTP (Simple Mail Transfer Protocol) - Uses port 25, not 636.
B). Syslog - Uses port 514 (UDP), not 636.
C). TFTP (Trivial File Transfer Protocol) - Uses port 69 (UDP), not 636.
D). LDAPS (Lightweight Directory Access Protocol Secure) - # Correct answer. Uses port 636 for secure 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: 27**
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: A (LEAVE A REPLY)**
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: 28**
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:

| |
|---|
| 443 |
| 80 |
| 22 |
| 587 |

Which of the following ports should be disabled?
**A.** 22
**B.** 80
**C.** 443
**D.** 587
**Answer: (SHOW ANSWER)**
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:
Port 22: Used for SSH, providing secure remote access and file transfers.
Port 587: Used for secure email submission (SMTP) with encryption.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.
Cisco Networking Academy: Provides training on secure web server configuration and port management.
Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

**NEW QUESTION: 29**
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: 30**
Which of the following dynamic routing protocols is used on the internet?
**A.** EIGRP
**B.** BGP
**C.** RIP
**D.** OSPF
**Answer: (SHOW ANSWER)**
BGP (Border Gateway Protocol) is the only dynamic routing protocol used across the internet. It's classified as an Exterior Gateway Protocol (EGP), responsible for routing between different autonomous systems (ASes).
A). EIGRP and D. OSPF are Interior Gateway Protocols (IGPs), used within organizations.
C). RIP is an outdated IGP with limited use, unsuitable for internet-scale routing.
# Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.

**NEW QUESTION: 31**
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: 32**
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: 33**
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.** Providing more Ethernet drops for user connections
**B.** Implementing additional ad hoc access points
**C.** Deploying a mesh network in the building
**D.** nl Changing the current frequency of the WI-FI
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 34**
Which of the following best describes a characteristic of a DNS poisoning attack?
**A.** DNS address records are edited and changed on a DNS server.
**B.** An attacker sets up a malicious DNS server in place of a legitimate server.
**C.** DNS client requests are intercepted and false responses are returned.
**D.** False DNS records are injected into cache on a DNS server.
**Answer: D (LEAVE A REPLY)**
DNS poisoning (also commonly called DNS cache poisoning) is characterized by inserting fraudulent DNS data into a resolver's cache so that subsequent queries return incorrect IP mappings. Option D describes this precisely: false DNS records are injected into a DNS server's cache, causing users to be redirected to attacker- controlled destinations even when they request a legitimate hostname. This aligns with Network+ security objectives covering common network attacks targeting name resolution and trust relationships. Editing authoritative DNS records on a DNS server (A) implies direct compromise or unauthorized administrative change, which is a different scenario than cache poisoning. Setting up a malicious DNS server in place of a legitimate server (B) is closer to DNS hijacking or rogue DNS configuration rather than cache poisoning.
Intercepting client requests and returning false responses (C) describes man-in-the-middle style spoofing on the wire; while related, the defining "poisoning" trait is the persistence created by corrupting the cache so the bad answer continues to be served. For defensive relevance in Network+ scope, cache poisoning highlights the importance of DNS security controls such as source port randomization, transaction ID entropy, and DNSSEC validation where applicable.

**NEW QUESTION: 35**
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: 36**
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: 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: (SHOW ANSWER)**
Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

**NEW QUESTION: 38**
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: 39**
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:

| Location | Speed Down | Speed Up |
|---|---|---|
| Wireless laptop | 4.8 Mbps | 47.1 Mbps |
| Wired desktop | 5.2 Mbps | 49.3 Mbps |
| Firewall | 48.8 Mbps | 49.5 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: 40**
Which of the following does a router prioritize first in the route selection process?
**A.** Prefix length
**B.** Metric
**C.** Administrative distance
**D.** Default route

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

**NEW QUESTION: 41**
A university is implementing a new campus wireless network. A network administrator needs to configure the network to support a large number of devices and high-bandwidth demands from students.
Which of the following wireless technologies should the administrator consider for this scenario?
**A.** Bluetooth
**B.** Wi-Fi 6E
**C.** 5G
**D.** LTE
**Answer: (SHOW ANSWER)**
Wi-Fi 6E is the best choice for high-density environments, such as a university campus. It:
Supports more devices with OFDMA (Orthogonal Frequency-Division Multiple Access) Uses the 6GHz band, reducing congestion Provides faster speeds and lower latency This makes Wi-Fi 6E ideal for large networks with high-bandwidth demands, like those in a university setting.
Breakdown of Options:
A). Bluetooth - Used for short-range, low-power connections, not large-scale wireless networks.
B). Wi-Fi 6E - # Correct answer. Designed for high-density environments, improving speed and efficiency.
C). 5G - Used for mobile networks, but not ideal for campus-wide local wireless infrastructure.
D). LTE - Used for cellular data, not for campus-wide Wi-Fi.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Compare and contrast wireless networking technologies.
IEEE 802.11ax (Wi-Fi 6E): Enhancements for high-efficiency wireless networking

**NEW QUESTION: 42**
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: 43**
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?
**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: 44**
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: 45**
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: 46**
A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?
**A.** Port
**B.** DNS
**C.** MAC
**D.** Content
**Answer: (SHOW ANSWER)**
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.



**NEW QUESTION: 47**
A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).
**A.** Mesh network
**B.** 5GHz frequency
**C.** Omnidirectional antenna
**D.** Non-overlapping channel
**E.** Captive portal
**F.** Ad hoc network
**Answer: B (LEAVE A REPLY)**
* Understanding 2.4GHz Interference:
* The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
* Mitigation Strategies:
* 5GHz Frequency:
* The 5GHz frequency band offers more channels and less interference compared to the 2.4 GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.
* Non-overlapping Channels:

* In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.
* Why Other Options are Less Effective:
* Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.
* Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.
* Captive Portal: A web page that users must view and interact with before accessing a network, unrelated to frequency interference.
* Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.
* Implementation:
* Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices.
* Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.
References:
* CompTIA Network+ study materials on wireless networking and interference mitigation.

**NEW QUESTION: 48**
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: 49**
Which of the following is the part of a disaster recovery (DR) plan that identifies the critical systems that should be recovered first after an incident?
**A.** RTO
**B.** SLA
**C.** MTBF
**D.** SIEM
**Answer: (SHOW ANSWER)**
RTO stands for Recovery Time Objective, which defines the maximum acceptable amount of time that a system, application, or function can be down after a failure or disaster. It helps prioritize which systems need to be recovered first based on their importance to business operations.
SLA (Service Level Agreement) refers to an agreement between a service provider and a customer regarding expected performance and availability, but it does not dictate recovery order.
MTBF (Mean Time Between Failures) is a measure of reliability and time between hardware or system failures.
SIEM (Security Information and Event Management) is a centralized tool for logging and alerting but not relevant to DR recovery prioritization.
# Reference:
CompTIA Network+ N10-009 Official Objectives: 4.4 - Summarize business continuity and disaster recovery concepts.

**NEW QUESTION: 50**

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



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

**NEW QUESTION: 51**
A network engineer is testing a website to ensure it is compatible with IPv6. After attempting to ping the website by its IPv6 address, the engineer determines that the DNS has not been set up properly. Which of the following should the network engineer complete to resolve this issue?
**A.** Enable a PTR record.
**B.** Update the existing TXT record.
**C.** Add a new AAAA record.
**D.** Configure a secondary NS record.
**Answer: (SHOW ANSWER)**
*AAAA records map domain names to IPv6 addresses, enabling proper resolution.
*PTR records (A) are for reverse DNS lookups.
*TXT records (B) store text-based information, not IP addresses.
*NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Configuration & IPv6.

**NEW QUESTION: 52**
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: 53**
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: 54**
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: D (LEAVE A REPLY)**
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: 55**
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: (SHOW ANSWER)**
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: 56**
A network technician receives a new ticket while working on another issue. The new ticket is critical to business operations. Which of the following documents should the technician reference to determine which ticket to complete first?
**A.** NDA
**B.** AUP
**C.** SLA
**D.** MOU
**Answer: (SHOW ANSWER)**
AnSLA (Service Level Agreement)defines performance expectations, includingresponse time, prioritization, and resolution timefor services and support issues. It helps the technician determine which task hashigher priority based on business impact.
* A. NDA (Non-Disclosure Agreement)relates to confidentiality, not task prioritization.
* B. AUP (Acceptable Use Policy)defines user behavior, not issue handling.
* D. MOU (Memorandum of Understanding)outlines informal agreements and doesn't define ticket priorities.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.1 - Compare and contrast common documentation types.

**NEW QUESTION: 57**
A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?
**A.** Trusted zones
**B.** URL filtering
**C.** ACLs
**D.** Screened subnet
**Answer: (SHOW ANSWER)**
Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

**NEW QUESTION: 58**
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: 59**
Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?
**A.** IPS
**B.** IDS
**C.** Load balancer
**D.** Firewall
**Answer: (SHOW ANSWER)**
An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-line and can introduce delay.
From Andrew Ramdayal's guide:
"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

**NEW QUESTION: 60**
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: C (LEAVE A REPLY)**

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: 61**
A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?
**A.** APIPA
**B.** Multicast
**C.** Class C
**D.** Experimental
**Answer: (SHOW ANSWER)**
APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:
"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."



**NEW QUESTION: 62**
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.** arp
**B.** ipconfig
**C.** nmap
**D.** tracert
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 63**

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: 64**

A network engineer is completing a new VoIP installation, but the phones cannot find the TFTP server to download the configuration files. Which of the following DHCP features would help the phone reach the TFTP server?

**A.** Exclusions

**B.** Lease time

**C.** Options

**D.** Scope

**Answer: (SHOW ANSWER)**

DHCP Options: DHCP options allow additional configuration parameters, such as the address of a TFTP server, to be provided to clients during the DHCP lease process. This is essential for VoIP phones to locate the server for configuration files.
Exclusions (A): Prevents certain IP addresses from being assigned by DHCP but does not direct devices to servers.
Lease time (B): Determines how long an IP address is assigned but does not impact TFTP settings.
Scope (D): Defines a range of IP addresses but does not include additional server information.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (DHCP Configuration).

**NEW QUESTION: 65**

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: (SHOW ANSWER)**

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: 66**
A network administrator configures a new network discovery tool and is concerned that it might disrupt business operations. Which of the following scan types should the administrator configure?
**A.** Authenticated
**B.** Ad hoc
**C.** Unauthenticated
**D.** Scheduled
**Answer: D (LEAVE A REPLY)**
If the administrator is concerned a new discovery tool could disrupt operations, the safest option is to configure scheduled scans. Network+ (N10-009) operations guidance emphasizes minimizing impact by running potentially noisy tasks (discovery, vulnerability checks, inventory scans) during defined maintenance windows or off-peak hours. A scheduled scan allows controlled timing, predictable load, and easier coordination with change management, monitoring, and support teams. This reduces the risk of saturating links, overwhelming devices with queries, or triggering alerts during business-critical periods.
Ad hoc scanning is on-demand and may occur at any time, which increases the chance of disruption if run during peak usage. Authenticated versus unauthenticated describes whether the scanner uses credentials to log into systems for deeper visibility; that choice affects depth and accuracy, but it doesn't directly address when scanning occurs to reduce business impact. An authenticated scan can still be disruptive if run at the wrong time, and an unauthenticated scan can still generate significant traffic. Since the key concern is operational disruption, controlling scan timing via scheduled scans is the best mitigation.

**NEW QUESTION: 67**
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: 68**
A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?
**A.** 802.11a
**B.** 802.11b
**C.** 802.11g
**D.** 802.11n
**Answer: (SHOW ANSWER)**
The 802.11n standard supports MIMO (Multiple Input Multiple Output), which allows multiple antennas to increase data throughput and improve reliability. Additionally, it uses non-overlapping channels in the 5 GHz band (and optionally the 2.4 GHz band), making it a good choice for high-speed, interference-resistant wireless connections. (Reference: CompTIA Network+ Study Guide, Chapter on Wireless Technologies)

**NEW QUESTION: 69**
Which of the following is the most closely associated with segmenting compute resources within a single cloud account?
**A.** Network security group
**B.** laaS
**C.** VPC
**D.** Hybrid cloud
**Answer: (SHOW ANSWER)**
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

**NEW QUESTION: 70**
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: 71**
A network administrator wants to update a geofencing policy to limit remote access to the corporate network based on country location. Which of the following would the administrator most likely leverage?
**A.** MAC filtering
**B.** Administrative distance
**C.** Bluetooth beacon signals
**D.** IP address blocks
**Answer: (SHOW ANSWER)**
The correct answer is IP address blocks because geofencing policies typically rely on public IP address ranges associated with specific geographic regions or countries. According to CompTIA Network+ (N10-009) security objectives, geofencing is a security control used to restrict or allow traffic based on geographic location. This is commonly implemented on firewalls, VPN concentrators, or security gateways by referencing databases that map IP address blocks to countries or regions.
When configuring geofencing, administrators create access control rules that permit or deny traffic from specific country-based IP ranges. This method is effective for limiting remote access to approved geographic locations and reducing exposure to international threat sources.
MAC filtering (Option A) is used within local networks and does not function over the internet for geographic control. Administrative distance (Option B) is a routing concept that determines route preference and has no relation to access control policies. Bluetooth beacon signals (Option C) are used for proximity-based services and indoor positioning, not for country-level remote access restrictions.
Therefore, leveraging IP address blocks is the correct approach for implementing geofencing controls.

**NEW QUESTION: 72**
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: 73**
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: 74**
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)**
The correct answer is Temperature because a sealed enclosure restricts airflow, which can cause heat to accumulate rapidly. According to CompTIA Network+ (N10-009) objectives under physical installations and environmental factors, maintaining proper temperature control is critical for network equipment reliability and longevity.
Network switches generate heat during operation, particularly models with high port density or Power over Ethernet (PoE) capabilities. In a sealed enclosure without proper ventilation or cooling mechanisms, excessive heat buildup can lead to thermal throttling, unexpected shutdowns, hardware degradation, or permanent equipment failure. Manufacturers specify operating temperature ranges, and exceeding these limits significantly reduces device lifespan and performance.
While humidity (Option D) is important to prevent condensation and corrosion, temperature fluctuations pose a more immediate risk in a sealed environment. Power budget (Option B) is relevant when calculating PoE load capacity but does not directly address environmental installation conditions. Fire suppression (Option A) is important in data centers but is not the primary concern specific to a sealed enclosure scenario.
Therefore, ensuring proper temperature management is the most critical installation factor.

**NEW QUESTION: 75**
An imaging workstation at a hospital is experiencing intermittent connectivity loss. Which of the following would most likely be used to resolve the issue at the least expense?

**A.** Single-mode fiber
**B.** Twinaxial cable
**C.** Spanning tree
**D.** Shielded twisted pair
**Answer: (SHOW ANSWER)**
The correct answer is Shielded Twisted Pair (STP). According to the CompTIA Network+ N10-009 objectives, intermittent connectivity issues-especially in environments like hospitals-are often caused by electromagnetic interference (EMI) from medical imaging equipment, power systems, and other electronic devices. These environments are electrically noisy and can disrupt standard copper Ethernet cabling.
STP cabling is specifically designed to mitigate EMI by incorporating shielding around the twisted pairs. This shielding reduces external interference and improves signal stability without requiring a complete redesign of the network. Importantly, STP is significantly less expensive than deploying fiber-optic solutions while still being highly effective in environments prone to interference.
Single-mode fiber would eliminate EMI entirely, but it is far more costly due to specialized cabling, transceivers, and installation requirements. Twinaxial cable is typically used for short-distance, high-speed data center connections and is not appropriate for workstation connectivity. Spanning Tree Protocol (STP) is a Layer 2 loop-prevention protocol and has nothing to do with physical connectivity or interference issues.
The Network+ objectives stress choosing solutions that balance effectiveness, cost, and environmental suitability. In this case, upgrading to shielded twisted pair cabling provides the most practical and cost- effective resolution for intermittent connectivity in a hospital imaging environment.

**NEW QUESTION: 76**
Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?
**A.** Duplicate the problem.
**B.** Identify the symptoms.
**C.** Gather information.
**D.** Determine any changes.
**Answer: (SHOW ANSWER)**
To confirm a theory in the troubleshooting process, the technician should duplicate (replicate) the problem under controlled conditions. In the Network+ (N10-009) methodology, confirming a theory means validating that the suspected cause actually produces the observed symptoms. Replicating the issue helps ensure the technician is not chasing a coincidence, and it allows changes to be tested safely (for example, reproducing the issue with a specific user account, endpoint, cable, port, SSID, or configuration). If the problem can be duplicated, the technician can then try targeted actions to see whether the symptoms change in predictable ways-strengthening or disproving the hypothesis.
The other choices occur earlier as part of forming the theory. Identify the symptoms is an initial step to define the problem clearly. Gather information is part of the discovery phase-collect logs, error messages, topology details, and user observations. Determine any changes is also an early step used to correlate recent modifications (patches, new devices, config changes) with the onset of the issue. Those steps help create a theory; duplication helps confirm it before implementing a full fix.



**NEW QUESTION: 77**
Which of the following does a router use to determine the preferred route?
**A.** Shortest prefix match

**B.** Routes learned from EIGRP
**C.** Longest prefix match
**D.** Routes learned from OSPF
**Answer: (SHOW ANSWER)**
Routers determine the best route to a destination using longest prefix match. This means the router chooses the route entry with the most specific matching network prefix for the destination IP address. For example, if a routing table contains 10.1.0.0/16 and 10.1.2.0/24, a packet destined to 10.1.2.50 matches both entries, but the router prefers /24 because it is more specific (longer mask). Network+ (N10-009) routing fundamentals emphasize that route selection begins with prefix length specificity before considering other factors within the same prefix length (such as administrative distance and metric, depending on the platform).
"Shortest prefix match" is the opposite of correct behavior. "Routes learned from EIGRP" and "routes learned from OSPF" describe sources of routes, not the general selection rule routers use when multiple matching routes exist. Even if routes come from different protocols, the router still applies selection logic; the universal rule for matching destination networks is longest prefix match. Hence, option C is correct.

**NEW QUESTION: 78**
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: 79**
Which of the following is the next step to take after successfully testing a root cause theory?
**A.** Determine resolution steps.
**B.** Duplicate the problem in a lab.
**C.** Present the theory for approval.
**D.** Implement the solution to the problem.
**Answer: (SHOW ANSWER)**
* Troubleshooting Methodology:
* Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.
* Implementation of the Solution:
* Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.
* Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.
* Comparison with Other Steps:
* Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.
* Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.

* Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.
* Final Verification:
* After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

**NEW QUESTION: 80**
Which of the following is an example of a split-tunnel VPN?
**A.** Only public resources are accessed through the user's internet connection.
**B.** Encrypted resources are accessed through separate tunnels.
**C.** All corporate and public resources are accessed through routing to on-site servers.
**D.** ACLs are used to balance network traffic through different connections.
**Answer: (SHOW ANSWER)**
In a split-tunnel VPN, only corporate traffic is sent through the VPN tunnel, while public internet traffic goes directly through the user's local ISP. This reduces bandwidth use on the corporate VPN concentrator and improves performance for non-work traffic.
B). Separate tunnels for encrypted traffic describes multi-tunnel VPNs, not split tunneling.
C). All traffic routed through on-site servers is a full-tunnel VPN, not split-tunnel.
D). ACLs balancing traffic relates to routing or load balancing, not VPN split tunneling.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - VPN types, split vs. full tunnel, remote access.

**NEW QUESTION: 81**
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: 82**
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: 83**

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.

**NEW QUESTION: 84**

Which of the following provides an opportunity for an on-path attack?

**A.** Phishing

**B.** Dumpster diving

**C.** Evil twin

**D.** Tailgating

**Answer: (SHOW ANSWER)**

An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity.

Breakdown of Options:

A: Phishing - Tries to steal credentials through fake emails/websites but does not intercept network traffic.
B: Dumpster diving - Involves physical security breaches, not network interception.
C: Evil twin - # Correct answer. A rogue Wi-Fi AP impersonates a real network, allowing traffic interception.
D: Tailgating - Involves physical access security, not network interception.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain common network security threats.

**NEW QUESTION: 85**
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: 86**
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: 87**
A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?
**A.** A physical interface used for trunking logical ports
**B.** A physical interface used for management access
**C.** A logical interface used for the routing of VLANs
**D.** A logical interface used when the number of physical ports is insufficent.
**Answer: (SHOW ANSWER)**
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
* SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
* VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
* Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.
* Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.
* Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

**NEW QUESTION: 88**
Two network switches at different locations are connected via fiber-optic cable at a distance of 10 miles (16 km). The duplex fiber-optic patch cord between the patch panel and switch is accidentally pinched, stopping connectivity between the two switches. A network technician replaces the broken cable with a new, single- mode patch cord. However, connectivity between both switches is still down and the link lights are still off.
Which of the following actions should the technician perform first?
**A.** Replace the fiber-optic transceiver in the switch
**B.** Log in to the switch to shut down and re-enable the switchport
**C.** Transpose the two fiber connectors at one end of the new patch cord
**D.** Swap the single-mode fiber patch cord with a multimode fiber patch cord
**Answer: (SHOW ANSWER)**
Fiber connections require Tx on one end to connect to Rx on the other end. If the patch cord is replaced and link lights remain off, the most common cause is that the connectors are reversed. Swapping (transposing) the connectors ensures proper transmit/receive alignment.
A). Replacing the transceiver may eventually be necessary, but only after verifying correct connections.
B). Restarting the switchport won't resolve a physical misconnection.
D). Using multimode fiber would be incorrect here, as the link was designed for single-mode (10 miles/16 km requires SMF).
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Fiber connectivity, Tx/Rx alignment, link light diagnostics.

**NEW QUESTION: 89**
Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0
/24 subnet. Which of the following tools should the administrator use to best identify the devices?
**A.** dig
**B.** nmap
**C.** tracert

**D.** telnet

**Answer: B (LEAVE A REPLY)**

nmap (Network Mapper) is the best tool in this scenario. It can scan the 192.168.1.0/24 subnet to discover live hosts, open ports (like Telnet on port 23), and device types. It's ideal for mapping and auditing the network.

A). dig is a DNS lookup tool; not useful for identifying hosts on a subnet.

C). tracert shows the path packets take to a destination, not for host discovery.

D). telnet is the protocol being used, not a tool for scanning or identifying devices.

# Reference:

CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

**NEW QUESTION: 90**

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: 91**

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: 92**
Which of the following must be implemented to securely connect a company's headquarters with a branch location?
**A.** Split-tunnel VPN
**B.** Clientless VPN
**C.** Full-tunnel VPN
**D.** Site-to-site VPN
**Answer: (SHOW ANSWER)**
Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.
Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.
Clientless VPN (B): Used for individual users to access the network without VPN client software.
Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Secure Network Connections).

**NEW QUESTION: 93**
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: 94**
A company's network is experiencing high levels of suspicious network traffic. The security team finds that the traffic is coming from an unknown, foreign IP address. Which of the following is the most cost-efficient way to mitigate this threat?
**A.** ACL
**B.** IDS
**C.** NAT
**D.** DoS prevention
**Answer: (SHOW ANSWER)**
The correct answer is ACL (Access Control List). According to the CompTIA Network+ N10-009 objectives, ACLs are a fundamental and cost-effective method for controlling traffic flow at routers and firewalls. An ACL allows administrators to permit or deny traffic based on source IP address, destination IP address, protocol, or port number.
In this scenario, the suspicious traffic is identified as originating from a specific unknown foreign IP address.
The most direct and economical mitigation strategy is to configure an ACL rule that denies traffic from that specific IP address (or subnet) at the network perimeter. This approach leverages existing network infrastructure without requiring additional hardware or licensing costs.
An IDS (Intrusion Detection System) monitors and alerts on malicious activity but does not actively block traffic unless paired with IPS functionality, and it may involve additional cost and complexity. NAT is used for address translation and does not provide traffic filtering based on threat intelligence. DoS prevention solutions are typically more advanced, specialized, and costly, often intended for large-scale distributed denial-of-service attacks rather than blocking traffic from a single suspicious IP.
The Network+ objectives emphasize implementing layered security controls, starting with simple and effective measures. In this case, applying an ACL at the firewall or router is the most cost-efficient and immediate method to mitigate the identified threat.

**NEW QUESTION: 95**
Which of the following is the most secure way to provide site-to-site connectivity?
**A.** VXLAN
**B.** IKE
**C.** GRE
**D.** IPsec
**Answer: (SHOW ANSWER)**
IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.References: CompTIA Network+ study materials and NIST Special Publication
800-77.

**NEW QUESTION: 96**
Which of the following best describes the purpose of a UPS and PDU in a network installation?
**A.** To support voltage requirements for devices in an IDF
**B.** To manage power consumption in the MDF
**C.** To connect multiple devices to a single network connection
**D.** To regulate temperature in the MDF and IDF
**Answer: (SHOW ANSWER)**
A UPS (Uninterruptible Power Supply) and PDU (Power Distribution Unit) are installed to provide reliable, properly distributed electrical power to network equipment-especially in wiring closets such as an IDF and in main equipment rooms. In Network+ (N10-009) infrastructure objectives, a UPS protects against power loss and instability by supplying battery-backed power during outages and often providing conditioning to reduce the impact of sags, spikes, and brief interruptions. A PDU then distributes that power to multiple devices in a rack (switches, routers, firewalls, AP controllers), often offering organized outlets and, in managed models, monitoring/control features.
Option A is the best match because it reflects the practical purpose: ensuring network devices receive appropriate and continuous power in distribution frames/closets. Option B is partially related, but "managing power consumption in the MDF" is too narrow and not as accurate as the broader function of providing backup and distribution power. Option C describes a network switch, not power equipment. Option D refers to HVAC/environmental controls, not UPS/PDU functionality. Hence, A is correct.

**NEW QUESTION: 97**
Three access points have Ethernet that runs through the ceiling. One of the access points cannot reach the internet. Which of the following tools can help identify the issue?
**A.** Network tap
**B.** Cable tester
**C.** Visual fault locator
**D.** Toner and probe
**Answer: (SHOW ANSWER)**
A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

**NEW QUESTION: 98**
Which of the following protocol ports should be used to securely transfer a file?
**A.** 22
**B.** 69
**C.** 80
**D.** 3389
**Answer: (SHOW ANSWER)**
Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.
*Why not the other options?
*Port 69 (B) - TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).
*Port 80 (C) - HTTP: Used for web traffic, not for file transfer.
*Port 3389 (D) - RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 5: Network Protocols and Ports

**NEW QUESTION: 99**
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: D (LEAVE A REPLY)**
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"

**NEW QUESTION: 100**
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: 101**
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

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


Which of the following is the most likely cause of the user ' s connection issues?

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

**NEW QUESTION: 102**
Which of the following involves an attacker traversing from one part of a network to another part that should be inaccessible?
**A.** MAC flooding
**B.** DNS poisoning
**C.** VLAN hopping
**D.** ARP spoofing
**Answer: (SHOW ANSWER)**
VLAN hopping allows an attacker to send traffic into another VLAN without authorization, often by impersonating a switch and negotiating a trunk link. This lets the attacker traverse into normally inaccessible VLANs.
A). MAC flooding disrupts switch operations but does not cross VLANs.
B). DNS poisoning corrupts name resolution.
D). ARP spoofing reroutes local traffic but doesn't grant VLAN traversal.
References (CompTIA Network+ N10-009):
Domain: Network Security - VLAN attacks, unauthorized lateral movement.

**NEW QUESTION: 103**
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: 104**
Which of the following concepts describes the idea of housing different customers in the same public cloud data center?
**A.** Elasticity
**B.** Hybrid cloud
**C.** Scalability
**D.** Multitenancy
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation (aligned to N10-009):
Multitenancy is a cloud concept where multiple customers share the same physical resources (servers, storage, and networks) but remain logically separated for security and privacy.
A). Elasticity is auto-scaling resources.
B). Hybrid cloud combines private and public resources.
C). Scalability is the ability to grow resources but doesn't imply multiple customers.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing models, multitenancy in public cloud.

**NEW QUESTION: 105**
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: 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.



**NEW QUESTION: 107**
A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?
**A.** Packet capture
**B.** Data usage reports
**C.** SNMP traps
**D.** Configuration monitoring
**Answer: (SHOW ANSWER)**
To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.
Breakdown of Options:
A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.
B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.
C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.
D). Configuration monitoring - This tracks configuration changes rather than availability.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.
RFC 1157: Simple Network Management Protocol (SNMP)

**NEW QUESTION: 108**
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: 109**
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."

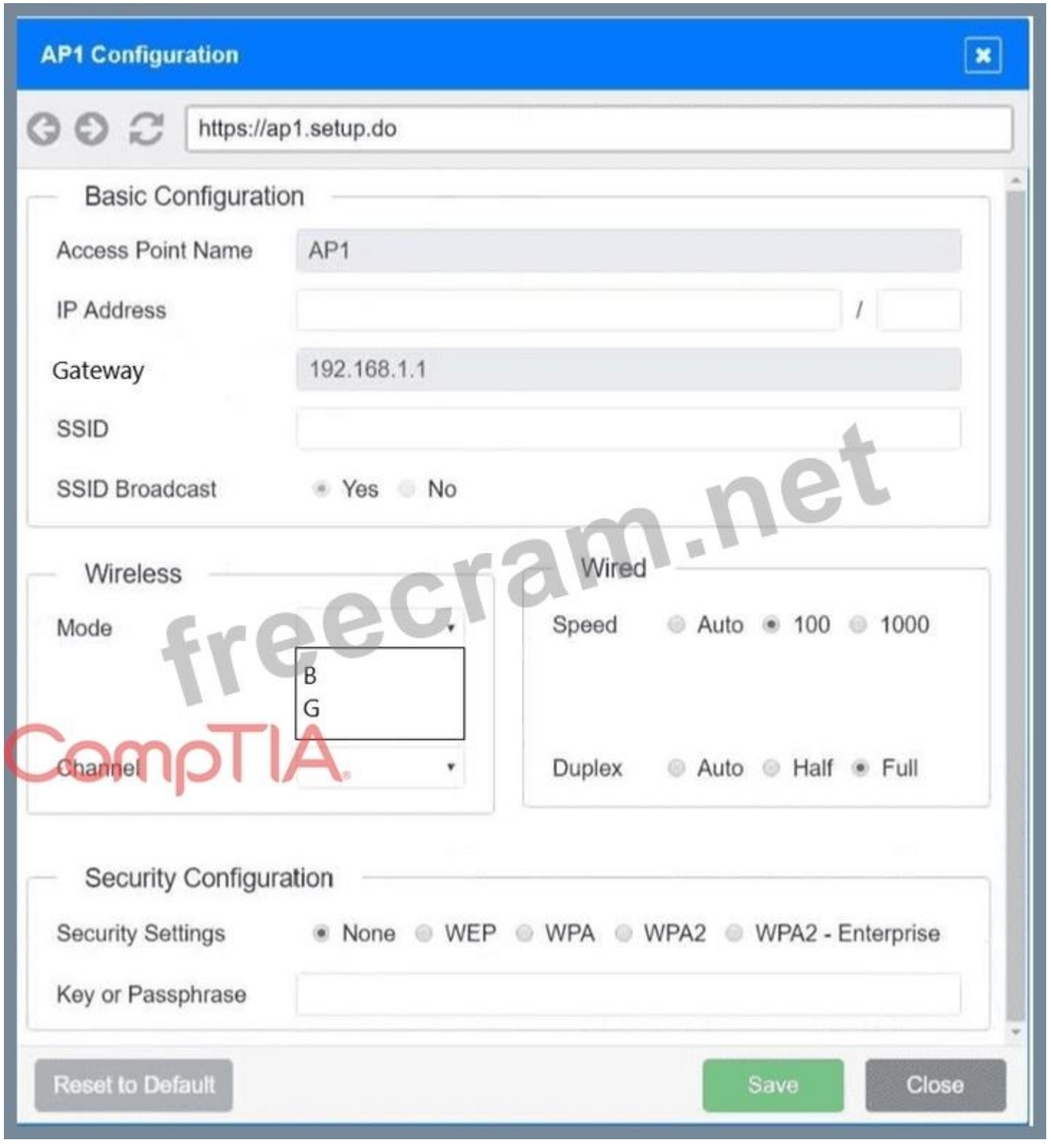
**NEW QUESTION: 110**
A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?

**A.** ACLs
**B.** Port security
**C.** Content filtering
**D.** NAC
**Answer: (SHOW ANSWER)**
* Understanding ACLs:
* Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.

* Implementing Security Zones:
* Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.
* Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.
* Comparison with Other Options:
* Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.
* Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.
* NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.
* Implementation Steps:
* Define ACL rules based on the requirements of each department.
* Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.
References:
* CompTIA Network+ study materials on network security and access control methods.

**NEW QUESTION: 111**
Which of the following would an adversary do while conducting an evil twin attack?
**A.** Trick users into using an AP with an SSID that is identical to a legitimate network
**B.** Manipulate address resolution to point devices to a malicious endpoint
**C.** Present an identical MAC to gain unauthorized access to network resources
**D.** Capture data in transit between two legitimate endpoints to steal data
**Answer: (SHOW ANSWER)**
An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting. Once connected, the attacker can intercept traffic or harvest credentials.
B). Describes ARP spoofing.
C). Describes MAC spoofing.
D). Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats, rogue APs, evil twin.

**NEW QUESTION: 112**
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t!
The wireless signals should not interfere with each other
The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



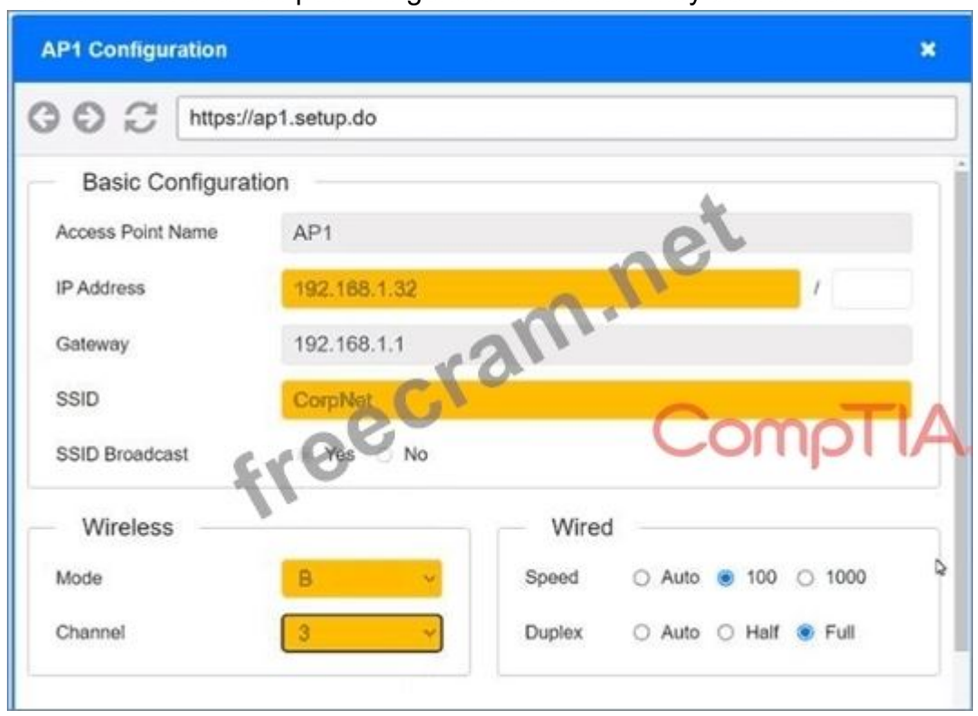

**Answer:**

See explanation below.

Explanation:

On the first exhibit, the layout should be as follows

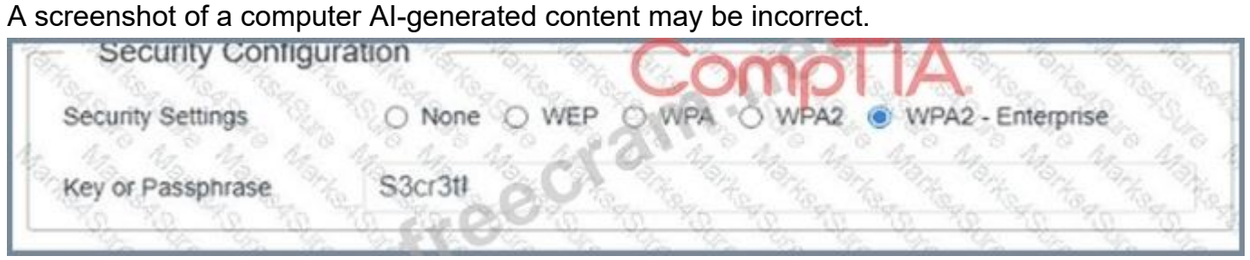
A screenshot of a computer AI-generated content may be incorrect.




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


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

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




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

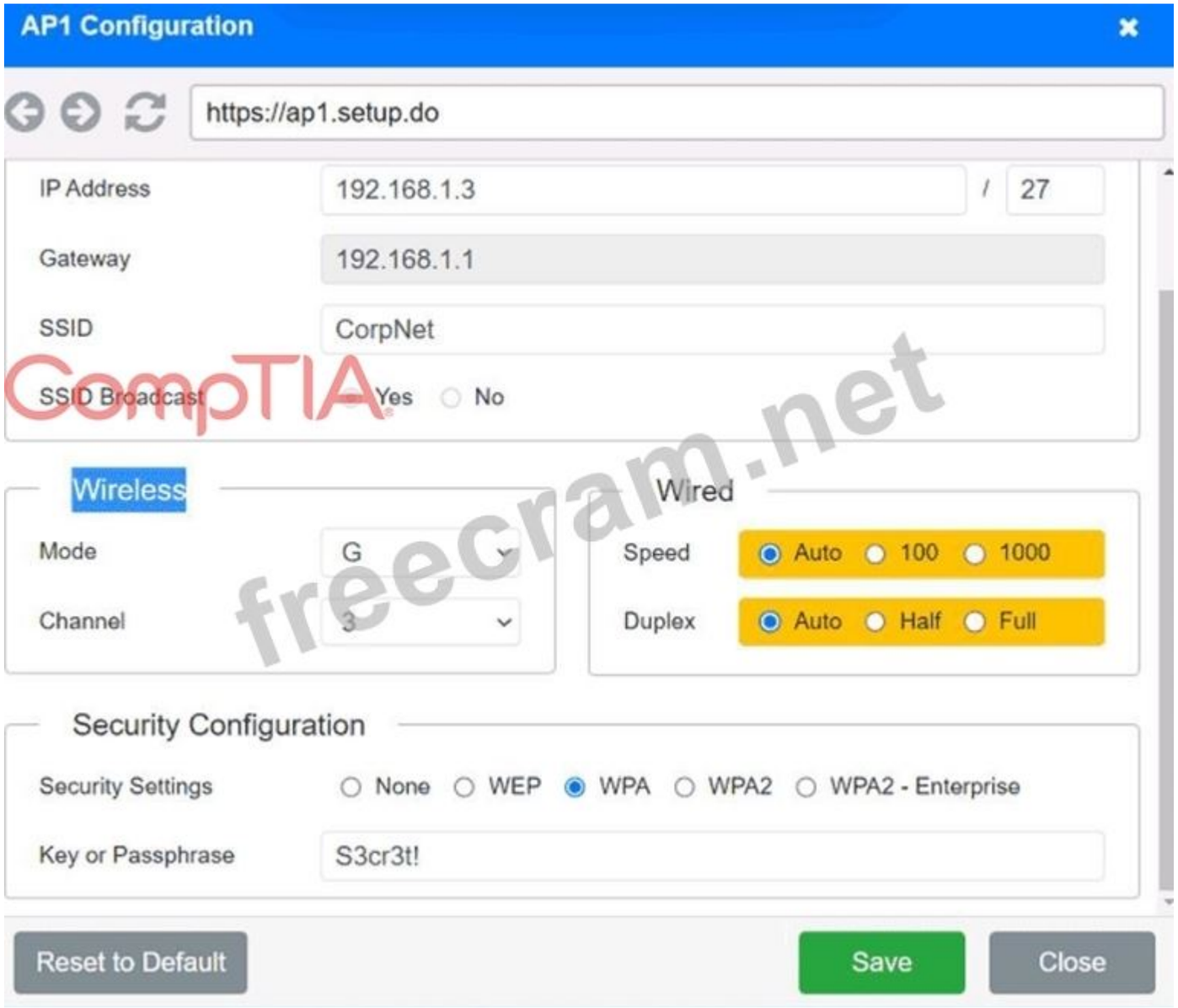
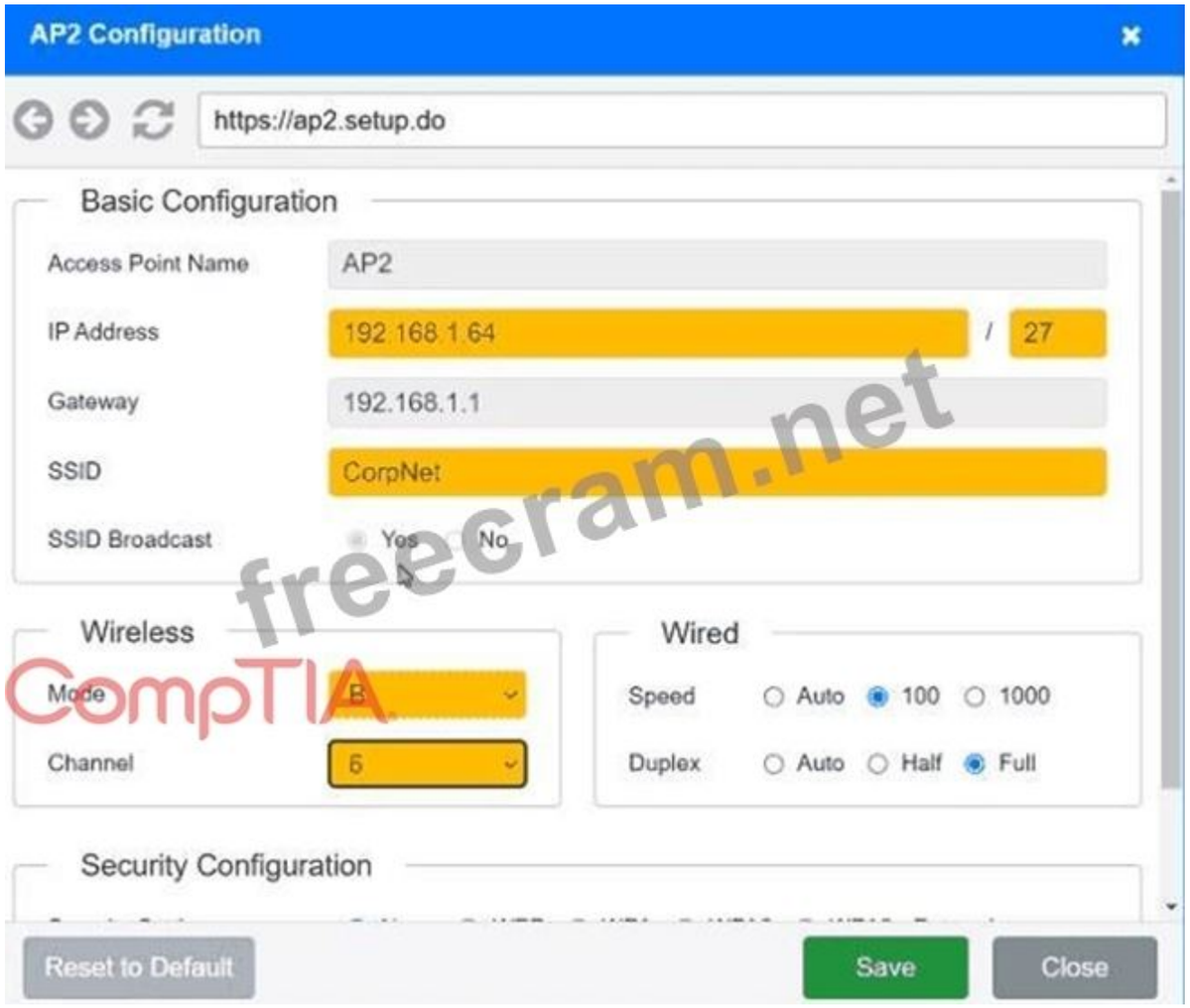



Exhibit 2 as follows

Access Point Name AP2

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






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

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

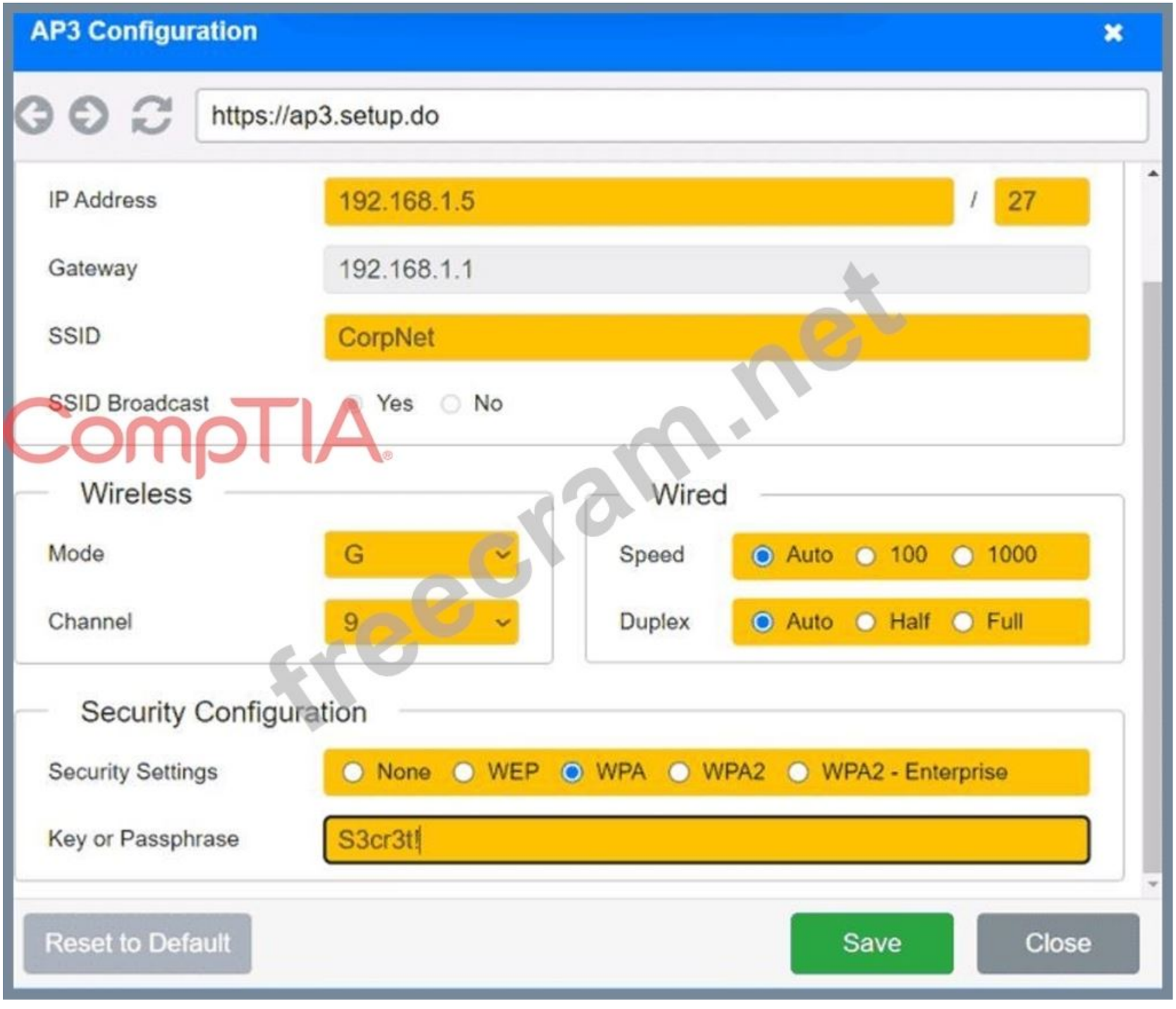
Exhibit 3 as follows

Access Point Name AP3

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


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


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






**NEW QUESTION: 113**

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

**A.** Stronger wireless connection

**B.** Roaming between access points

**C.** Advanced security
**D.** Increased throughput
**Answer: (SHOW ANSWER)**
An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses.References:CompTIA Network+ study materials.

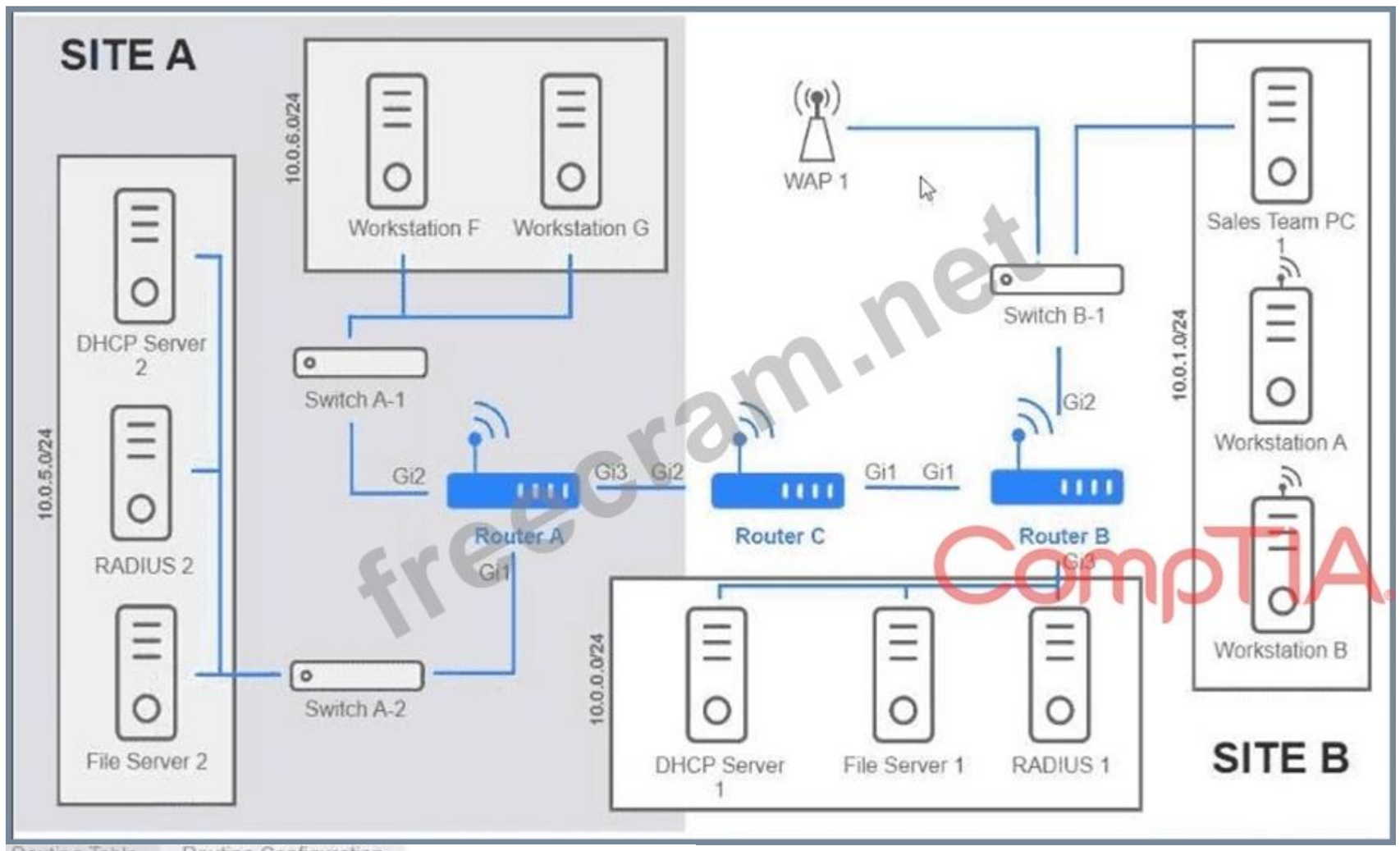
**NEW QUESTION: 114**
A server administrator needs to add a record to the company's DNS server to verify ownership of a web domain. The administrator has the record's name and value. Which of the following record types should the administrator use to add the record to the DNS server?
**A.** TXT
**B.** 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: 115**
A customer needs six usable IP addresses. Which of the following best meets this requirement?
**A.** 255.255.255.128
**B.** 255.255.255.192
**C.** 255.255.255.224
**D.** 255.255.255.240
**Answer: D (LEAVE A REPLY)**
Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

**NEW QUESTION: 116**
A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?
**A.** Change the email client configuration to match the MX record.
**B.** Reduce the TTL record prior to the MX record change.
**C.** Perform a DNS zone transfer prior to the MX record change.
**D.** Update the NS record to reflect the IP address change.

**Answer: (SHOW ANSWER)**
Understanding TTL (Time to Live):
TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients.
A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.
Impact of TTL on DNS Changes:
When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.
Best Practice Before Making DNS Changes:
To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making thechanges. This ensures that any cached records will expire quickly, and the new records will be used sooner.
Verification of DNS Changes:
After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.
Comparison with Other Options:
Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.
Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.
Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.
References:
CompTIA Network+ study materials and DNS best practices.

**NEW QUESTION: 117**
Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identity any Issues, and configure the appropriate solution If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;




Routing Table | Routing Configuration

```
Router-B# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.0.0/22 is directly connected, GigabitEthernet3
L        10.0.0.1/32 is directly connected, GigabitEthernet3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.5/32 is directly connected, GigabitEthernet1
```



**Answer:**

See the solution configuration below in Explanation.

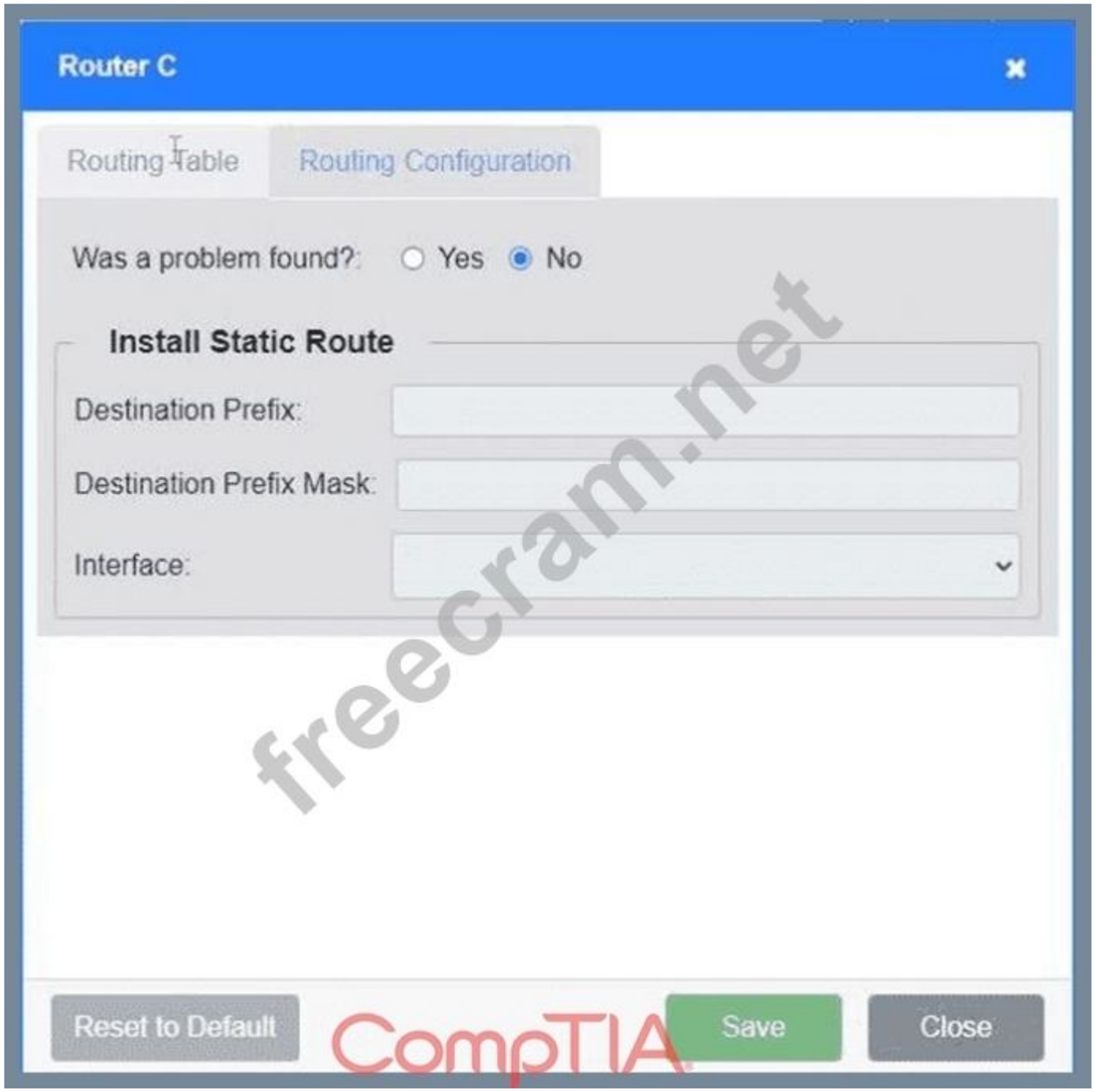
Explanation:

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




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

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





**NEW QUESTION: 118**
A Chief Information Officer wants a DR solution that runs only after a failure of the primary site and can be brought online quickly once recent backups are imported. Which of the following DR site solutions meets these requirements?
**A.** Cold
**B.** Warm
**C.** Active
**D.** Hot
**Answer: B (LEAVE A REPLY)**
Comprehensive and Detailed Explanation (aligned to N10-009):
A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.

A). Cold site has only power and space, requiring full setup, which takes too long.
C). Active (active-active) runs simultaneously with the primary site, not only during failure.
D). Hot site is fully operational at all times and can take over immediately, but it's more expensive.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Disaster recovery sites (cold, warm, hot, active).

**NEW QUESTION: 119**
Which of the following actions should be taken as part of the first step of the troubleshooting methodology?
**A.** Create a theory about the possible root cause
**B.** Conduct tests to verify ideas
**C.** Handle multiple problems individually
**D.** Use a top-down approach
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 120**
A company wants to implement a disaster recovery site or non-critical applicance, which can tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?

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

**NEW QUESTION: 121**
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: 122**
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: 123**
Which of the following ports is used to transfer data between mail exchange servers?
**A.** 21
**B.** 25
**C.** 53
**D.** 69
**Answer: (SHOW ANSWER)**
The correct answer is 25, which is the default port used by SMTP (Simple Mail Transfer Protocol) for communication between mail servers. According to CompTIA Network+ (N10-009) objectives under common port numbers and protocols, SMTP operates over TCP port 25 for server-to-server email transmission.
When an email is sent from one domain to another, the sending mail server queries DNS for the recipient domain's MX (Mail Exchange) record and then establishes an SMTP session over TCP port 25 to deliver the message. This port is specifically designated for mail relay between mail transfer agents (MTAs).
Port 21 is used for FTP (File Transfer Protocol), 53 is used for DNS (Domain Name System), and 69 is used for TFTP (Trivial File Transfer Protocol). None of these are responsible for transferring email between mail servers.
While SMTP can also use ports 587 (submission) and 465 (SMTPS) for client-to-server communication, port 25 remains the standard for mail server-to-mail server communication.

Therefore, TCP port 25 is the correct answer.

**NEW QUESTION: 124**
A network administrator is managing network traffic so that classified services and applications are prioritized. Which of the following technologies should the network administrator use?
**A.** Load balancing
**B.** Time to live
**C.** Quality of service
**D.** Content delivery network
**Answer: (SHOW ANSWER)**
Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion. Network+ objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links. TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

**NEW QUESTION: 125**
Which of the following technologies are X.509 certificates most commonly associated with?
**A.** PKI
**B.** VLAN tagging
**C.** LDAP
**D.** MFA
**Answer: (SHOW ANSWER)**
X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.
* PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.
* Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.
* Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.
* Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.
* Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

**NEW QUESTION: 126**
Which of the following OSI model layers manages the exchange of HTTP information?
**A.** Session
**B.** Data link
**C.** Network

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

**NEW QUESTION: 127**
A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?
**A.** TXT
**B.** AAA
**C.** PTR
**D.** CNAME
**Answer: (SHOW ANSWER)**
To redirect a network resource that has moved from a local network to a Software-as-a-Service (SaaS) solution, the network administrator needs to configure a DNS record that maps an alias to the new canonical name (hostname) of the SaaS provider's server. The CNAME (Canonical Name) record is used to alias one domain name to another, effectively redirecting requests to the new hostname without needing to update the IP address directly. This is ideal for SaaS solutions, where the provider's server hostname is used, and the IP address may change dynamically.
Why not TXT? A TXT record is used to store arbitrary text data, such as SPF records for email authentication or verification strings, not for redirecting resources.
Why not AAA? There is no such thing as an "AAA" record in DNS. This might be a typo for AAAA (IPv6 address record), but AAAA maps a hostname to an IPv6 address, not an alias.
Why not PTR? A PTR record is used for reverse DNS lookups (mapping an IP address to a hostname), not for redirecting a resource to a new hostname.
Reference:CompTIA Network+ N10-009 Objective 1.5: Compare and contrast common network services and ports. The CNAME record is discussed under DNS configuration in the CompTIA Network+ Certification Study Guide (e.g., Mike Meyers' CompTIA Network+ Guide, Chapter 7: TCP/IP Applications). The guide explains that CNAME records are used to create aliases for hostnames, particularly useful for redirecting services to external providers like SaaS solutions.

**NEW QUESTION: 128**
Users are reporting latency on the network. The network engineer notes the following:
Confirms the only change was a new network switch
Confirms all users are experiencing latency
Thinks the issue is a network loop caused by the lower bridge ID of the new switch Which of the following describes the next step in the troubleshooting methodology?
**A.** Identify the problem.
**B.** Test the theory.
**C.** Implement the solution.
**D.** Verify full system functionality.
**Answer: (SHOW ANSWER)**

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

**NEW QUESTION: 129**
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: 130**

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: 131**

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: 132**

A network engineer wants to implement an 802.1X architecture in which BYOD devices must access a trusted wireless network securely. Which of the following should the engineer implement?

**A.** ACL
**B.** MAC filtering
**C.** Port security
**D.** NAC
**Answer: (SHOW ANSWER)**
For a secure 802.1X design that includes BYOD access to a trusted wireless network, the engineer should implement NAC (Network Access Control). In the Network+ (N10-009) objectives, 802.1X provides authentication (commonly via EAP to a RADIUS server), but NAC expands this by enforcing policy-based access decisions-such as device posture checks, user/device identity validation, and dynamic assignment to the appropriate VLAN/role. With BYOD, the organization often needs to confirm whether devices meet requirements (OS version, encryption, security software) and then grant the correct level of access (full, limited, or quarantine/remediation). NAC is the architecture that ties these controls together in a scalable way for wireless networks.
An ACL can restrict traffic after a device connects, but it doesn't perform authentication/posture assessment.
MAC filtering is weak because MAC addresses can be spoofed and it does not provide strong identity assurance. Port security is mainly a wired switch control (limiting MAC addresses per port) and is not the right control set for secure BYOD wireless access. NAC best matches the requirement of secure, policy- driven 802.1X BYOD access.

**NEW QUESTION: 133**
A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?
**A.** 4096
**B.** 8192
**C.** 32768
**D.** 36684
**Answer: (SHOW ANSWER)**
* Understanding Spanning Tree Protocol (STP):
* STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.
* Default Priority Value:
* Bridge Priority:STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.
* Priority Range:The bridge priority can be set in increments of 4096, ranging from 0 to 61440.
* Configuration and Verification:
* When deploying a new switch, the network administrator can verify the bridge priority using commands such asshow spanning-treeto ensure it is set to the default value of 32768.
* Comparison with Other Values:
* 4096 and 8192:Lower than the default priority, indicating these would be manually configured for higher preference.
* 36684:A non-standard value, likely a result of specific configuration changes.
References:
* CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

**NEW QUESTION: 134**
A network administrator suspects users are being sent to malware sites that are posing as legitimate sites. The network administrator investigates and discovers that user workstations are configured with incorrect DNS IP addresses. Which of the following should the network administrator implement to prevent this from happening again?
**A.** Dynamic ARP inspection
**B.** Access control lists
**C.** DHCP snooping

**D.** Port security
**Answer: (SHOW ANSWER)**
DHCP snooping is a security feature on network switches that helps to prevent unauthorized (rogue) DHCP servers from assigning IP addresses to clients. By implementing DHCP snooping, the network administrator can restrict DHCP responses to authorized servers only, preventing unauthorized DHCP configurations, such as incorrect DNS IPs, from being assigned to clients. This helps prevent man-in-the-middle attacks where malicious actors misconfigure DNS to redirect users to fraudulent sites. (Reference: CompTIA Network+ Study Guide, Chapter on Network Security)

**NEW QUESTION: 135**
A network analyst is installing a wireless network in a corporate environment. Employees are required to use their domain identities and credentials to authenticate and connect to the WLAN. Which of the following actions should the analyst perform on the AP to fulfill the requirements?
**A.** Enable MAC security.
**B.** Generate a PSK for each user.
**C.** Implement WPS.
**D.** Set up WPA3 protocol.
**Answer: (SHOW ANSWER)**
WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user- based authentication.
WPA3-Enterprise Benefits:
Uses 802.1X with EAP (Extensible Authentication Protocol) to authenticate users via a directory service (e.g., Active Directory).
Eliminates shared passwords (PSK) for authentication.
Provides strong encryption and resistance to brute-force attacks.
Incorrect Options:
A). Enable MAC Security:
MAC filtering is not secure because MAC addresses can be spoofed.
B). Generate a PSK for Each User:
Pre-shared keys (PSK) are used in WPA-Personal, not in an enterprise setting.
Does not scale well in corporate environments.
C). Implement WPS:
Wi-Fi Protected Setup (WPS) is a vulnerable security method meant for home users.
Not suitable for enterprise authentication.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Security and Authentication

**NEW QUESTION: 136**
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: 137**
Which of the following network traffic types is sent to all nodes on the network?
**A.** Unicast
**B.** Broadcast
**C.** Multicast
**D.** Anycast
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation (aligned to N10-009):
A broadcast message is delivered to all nodes in a broadcast domain (e.g., ARP requests).
A). Unicast is one-to-one.
C). Multicast is one-to-many but only to subscribed members.
D). Anycast is one-to-one-of-many, sending to the nearest node.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Traffic types: unicast, multicast, broadcast, anycast.

**NEW QUESTION: 138**
A network administrator recently upgraded a wireless infrastructure with new APs. Users report that when stationary, the wireless connection drops and reconnects every 20 to 30 seconds. While reviewing logs, the administrator notices the APs are changing channels.
Which of the following is the most likely reason for the service interruptions?
**A.** Channel interference
**B.** Roaming misconfiguration
**C.** Network congestion
**D.** Insufficient wireless coverage
**Answer: (SHOW ANSWER)**
If APs are changing channels frequently, it indicates automatic channel selection due to interference. This can cause temporary disconnections as the APs switch frequencies.
Breakdown of Options:
A). Channel interference - # Correct answer. APs change channels automatically to avoid interference, causing disconnections.
B). Roaming misconfiguration - Roaming only affects moving users, but users report issues while stationary.

C). Network congestion - Causes slow speeds, not frequent disconnects.
D). Insufficient wireless coverage - Would cause weak signals, but not channel switching issues.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Explain wireless troubleshooting techniques.

**NEW QUESTION: 139**
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: 140**
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: 141**
A technician is designing a cloud service solution that will accommodate the company's current size, compute capacity, and storage capacity. Which of the following cloud deployment models will fulfill these requirements?

**A.** SaaS
**B.** PaaS
**C.** IaaS
**D.** IaC
**Answer: C (LEAVE A REPLY)**
Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.
IaaS Benefits:
Provides virtual machines, storage, and networking resources.
Scalable based on company needs.
Reduces the need for physical infrastructure.
Incorrect Options:
A: SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.
B: PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.
D: IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Cloud Computing Models

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

**NEW QUESTION: 143**
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: 144**
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?
**A.** Implement DNS filtering.
**B.** Update ACLs to only allow HTTPS.
**C.** Configure new IPS hardware.
**D.** Deploy 802.1X security features.
**Answer: (SHOW ANSWER)**
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: 145**
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: 146**
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?
**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: 147**

Which of the following devices functions mainly at the data link layer of the OSI model and is used to connect a fiber-optic cable to a network interface?

**A.** SC

**B.** DAC

**C.** SFP transceiver

**D.** Twinaxial cable

**Answer: (SHOW ANSWER)**

An SFP (Small Form-factor Pluggable) transceiver is a modular device that provides the interface between fiber-optic or copper cabling and the networking equipment (e.g., switch or router). It operates primarily at Layer 2 (Data Link), converting optical or electrical signals into frames usable by the network device.

A). SC is a fiber connector type, not the transceiver.

B). DAC (Direct Attach Copper) is a passive copper cable assembly with fixed transceivers, not a general- purpose module.

D). Twinaxial cable is a copper medium, not an interface device.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Transceivers (SFP, GBIC, QSFP), fiber connectivity, OSI model mapping.

**NEW QUESTION: 148**

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.** Active-active approach

**C.** Warm site

**D.** Cold site

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 149**

Which of the following is used most often when implementing a secure VPN?

**A.** IPSec

**B.** GRE

**C.** BGP

**D.** SSH

**Answer: A (LEAVE A REPLY)**

The most common protocol for secure VPNs is IPsec (Internet Protocol Security). IPsec provides confidentiality, integrity, and authentication for VPN traffic, typically using ESP (Encapsulating Security Payload). It is used in both site-to-site and remote access VPNs.

B). GRE encapsulates traffic but does not provide encryption.

C). BGP is a routing protocol, not a VPN technology.

D). SSH can be used for secure tunneling but is not the standard for VPN deployment.

IPsec is the industry standard because it operates at Layer 3, securing IP traffic regardless of the application, making it highly versatile.

References (CompTIA Network+ N10-009):

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

**NEW QUESTION: 150**

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: C (LEAVE A REPLY)**
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: 151**
Which of the following is associated with avoidance, acceptance, mitigation, and transfer?
**A.** Risk
**B.** Exploit
**C.** Threat
**D.** Vulnerability
**Answer: (SHOW ANSWER)**
These four terms-avoidance, acceptance, mitigation, and transfer-are strategies used in risk management.
From Andrew Ramdayal's guide:
"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."



**NEW QUESTION: 152**
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: 153**
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: 154**
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.** Verify full system functionality
**B.** Establish a plan of action
**C.** Identify the problem
**D.** Test in the theory
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 155**
A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?
**A.** Mesh
**B.** Ad hoc
**C.** Point-to-point
**D.** Infrastructure
**Answer: (SHOW ANSWER)**

A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel.
This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail.
Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.References:CompTIA Network+ study materials.

**NEW QUESTION: 156**
An organization wants better network visibility. The organization's requirements include:
Multivendor/OS-monitoring capabilities
Real-time collection
Data correlation
Which of the following meets these requirements?
**A.** SNMP
**B.** SIEM
**C.** Nmap
**D.** Syslog
**Answer: (SHOW ANSWER)**
A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments.
Breakdown of Options:
A). SNMP - SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.
B). SIEM - Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.
C). Nmap - Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.
D). Syslog - Syslog collects logs but does not correlate or analyze them in real-time.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain network security concepts.
NIST Special Publication 800-92: Guide to Computer Security Log Management

**NEW QUESTION: 157**
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: A (LEAVE A REPLY)**
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: 158**
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: (SHOW ANSWER)**
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: 159**
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: B (LEAVE A REPLY)**
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: 160**
A network engineer needs to correlate findings and receive alerts if there are brute force attacks, DDoS attacks, or port scanning happening within their network. Which of the following network monitoring technologies should the engineer implement?

**A.** Packet capture
**B.** SNMPv3
**C.** SIEM
**D.** Syslog collector
**Answer: (SHOW ANSWER)**
A SIEM (Security Information and Event Management) platform is built to collect, correlate, and alert on security-relevant events across many sources, which is exactly what's needed to identify patterns such as brute force attempts, port scanning, and DDoS indicators. In Network+ (N10-009) security operations concepts, correlation is key: a SIEM can ingest logs from firewalls, IDS/IPS, servers, authentication systems, endpoint agents, and network devices, then apply rules/analytics to detect suspicious behavior that might not

be obvious from a single log source. It can also generate real-time alerts, dashboards, and incident timelines-helping the engineer respond quickly and prioritize threats.
Packet capture provides deep visibility into traffic but is not inherently designed for enterprise-wide correlation and alerting without significant additional tooling and expertise.
SNMPv3 is used for secure device monitoring (status, counters, performance) rather than detecting coordinated attack patterns. A syslog collector centralizes logs but generally does not provide the same level of correlation, enrichment, and automated alerting capabilities as a SIEM. Therefore, SIEM is the best answer.

**NEW QUESTION: 161**
A network administrator prepares a VLAN for a new office while planning for minimal IP address waste. The new office will have approximately 800 workstations. Which of the following network schemes meets the requirements?
**A.** 10.0.100.0/22
**B.** 172.16.8.0/23
**C.** 172.16.15.0/20
**D.** 192.168.4.0/21
**Answer: (SHOW ANSWER)**
To support about 800 workstations with minimal IP waste, you choose the smallest subnet that provides at least 800 usable host addresses. In IPv4, usable hosts per subnet are calculated as 2^(host bits) # 2 (subtracting network and broadcast addresses). A /22 leaves 10 host bits (32 # 22 = 10), providing 2^10 # 2 =
1024 # 2 = 1022 usable addresses-enough for 800 devices with relatively low waste.
Check the other options: /23 leaves 9 host bits, giving 2^9 # 2 = 512 # 2 = 510 usable addresses, which is not enough. A /21 provides 2^11 # 2 = 2048 # 2 = 2046 usable addresses-enough, but wastes more than /22. A
/20 provides 2^12 # 2 = 4096 # 2 = 4094 usable addresses-much more waste.
Therefore, 10.0.100.0/22 is the best choice that meets the workstation requirement while minimizing unused addresses.

**NEW QUESTION: 162**
A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?
**A.** 802.1Q tagging
**B.** Jumbo frames
**C.** Half duplex
**D.** Link aggregation
**Answer: D (LEAVE A REPLY)**
Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.
IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

**NEW QUESTION: 163**

A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?
**A.** Configure ACLs.
**B.** Implement a captive portal.
**C.** Enable port security.
**D.** Disable unnecessaryservices.
**Answer: (SHOW ANSWER)**
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

**NEW QUESTION: 164**
Which of the following explains what happens if a packet is lost in transit when using UDP?
**A.** The data link layer will recognize the error and resend the packet.
**B.** IP uses the TTL field to track packet hops and will resend the packet if necessary.
**C.** If the sender does not receive a UDP acknowledgement, the packet will be resent.
**D.** Some applications will recognize the loss and initiate a resend of the packet if necessary.
**Answer: (SHOW ANSWER)**
UDP (User Datagram Protocol) is a connectionless protocol that does not provide built-in mechanisms for error detection, retransmission, or acknowledgments. If a UDP packet is lost in transit, the protocol itself does not handle retransmission. However, some applications using UDP (e.g., TFTP or custom streaming protocols) may implement their own mechanisms to detect packet loss and request retransmission if needed.
Why not A? The data link layer (Layer 2) handles frame-level errors within a single network segment, not end- to-end packet loss across networks.
Why not B? The IP TTL (Time to Live) field prevents routing loops by decrementing with each hop, but IP does not handle retransmission.
Why not C? UDP does not use acknowledgments, so the sender does not expect or receive them.
Reference:CompTIA Network+ N10-009 Objective 1.4: Explain the characteristics of network topologies and protocols. The CompTIA Network+ Study Guide (e.g., Chapter 4: Network Protocols) explains that UDP is a
"fire-and-forget" protocol, and any retransmission logic must be handled by the application layer.

**NEW QUESTION: 165**
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: D (LEAVE A REPLY)**
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: 166**
Which of the following is the best networking appliance for interconnecting multiple logical networks and forwarding data packets between them while minimizing latency?
**A.** Firewall
**B.** Router
**C.** Layer 2 switch
**D.** Load balancer
**Answer: (SHOW ANSWER)**
The correct appliance is a router, which is specifically designed to interconnect multiple networks and forward packets based on IP addresses. Routers operate at Layer 3 (Network layer) of the OSI model and make intelligent forwarding decisions to ensure data reaches the correct destination network.
A). Firewall can also forward traffic, but its primary function is security, not routing efficiency.
C). Layer 2 switches connect devices within the same LAN but do not forward packets between different networks without routing capability.
D). Load balancers distribute traffic among servers but are not general-purpose routers.
Modern enterprise routers are optimized to minimize latency by using fast switching and hardware acceleration, making them ideal for interconnecting logical networks securely and efficiently.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Routers, Layer 3 devices, inter-network communication.



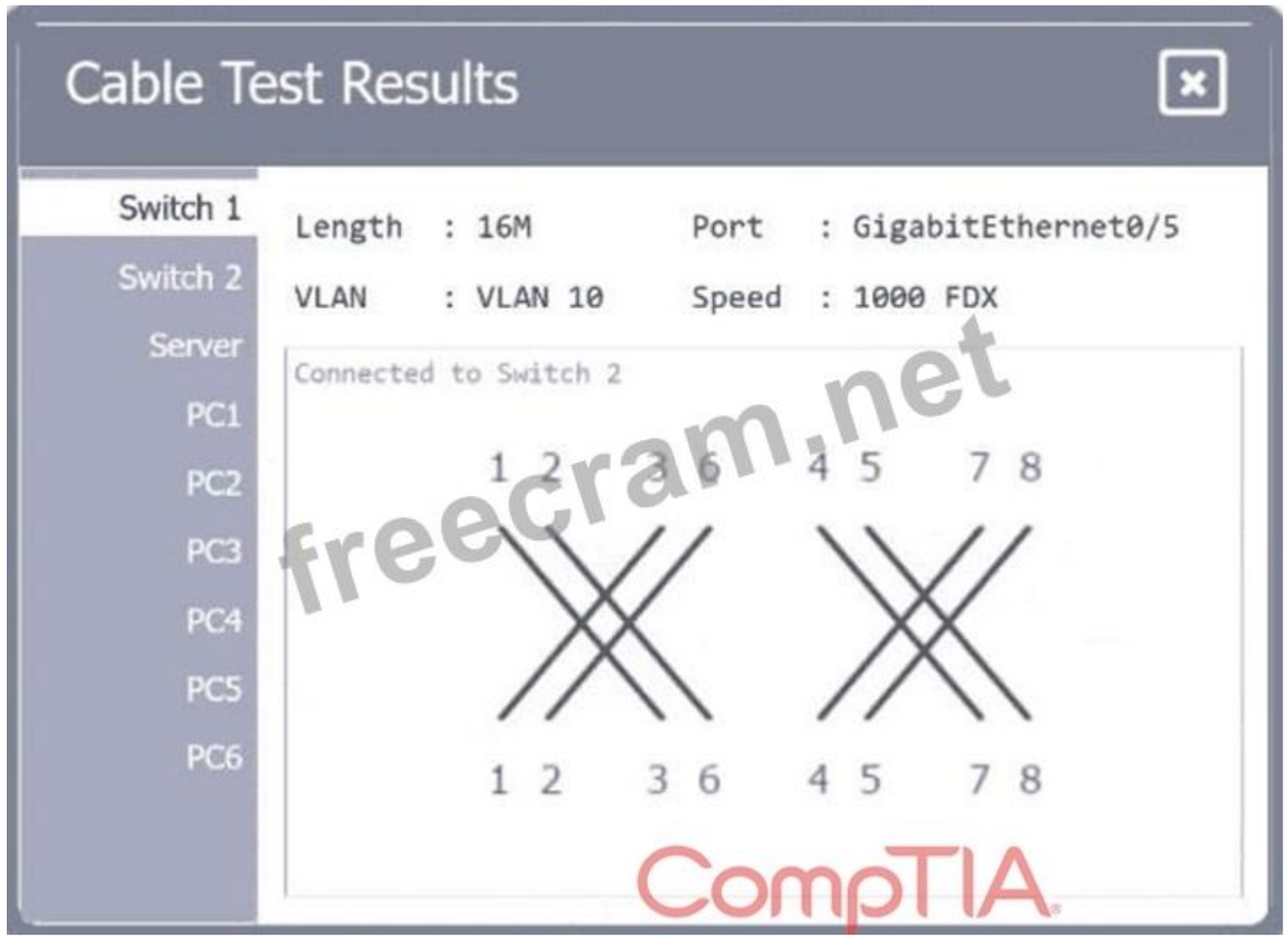
**NEW QUESTION: 167**
Which of the following would be violated if an employee accidentally deleted a customer's data?
**A.** Integrity
**B.** Confidentiality
**C.** Vulnerability
**D.** Availability
**Answer: (SHOW ANSWER)**
Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

**NEW QUESTION: 168**
A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?
**A.** NS
**B.** SOA
**C.** PTR
**D.** CNAME
**Answer: (SHOW ANSWER)**
To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the

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

**NEW QUESTION: 169**
Which of the following routing protocols needs to have an autonomous system set in order to establish communication with neighbor devices?
**A.** OSPF
**B.** EIGRP
**C.** FHRP
**D.** RIP
**Answer: (SHOW ANSWER)**
EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary advanced distance-vector routing protocol. While it operates within an Autonomous System (AS), it requires the AS number to be configured for routers to recognize each other as EIGRP neighbors.
OSPF (Open Shortest Path First) uses areas and routers must be in the same area to form adjacencies, but it doesn't require AS numbers in the same way.
FHRP (First Hop Redundancy Protocol) is not a routing protocol but a group of protocols (e.g., HSRP, VRRP) to ensure high availability at the default gateway level.
RIP (Routing Information Protocol) does not use autonomous system numbers.
# Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.

**NEW QUESTION: 170**
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

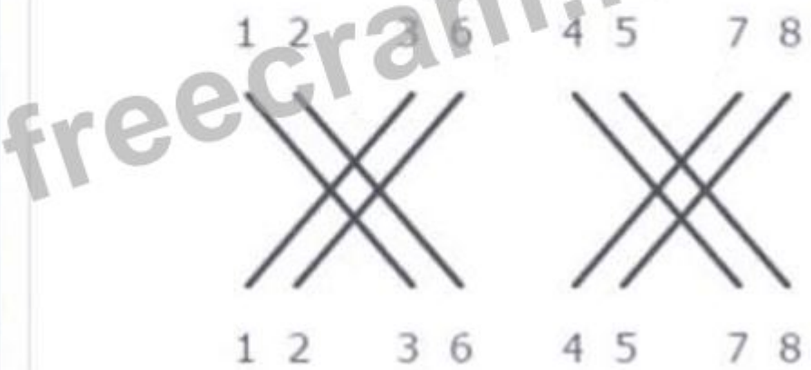
## Cable Test Results

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 1



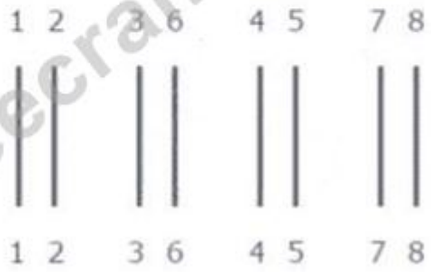


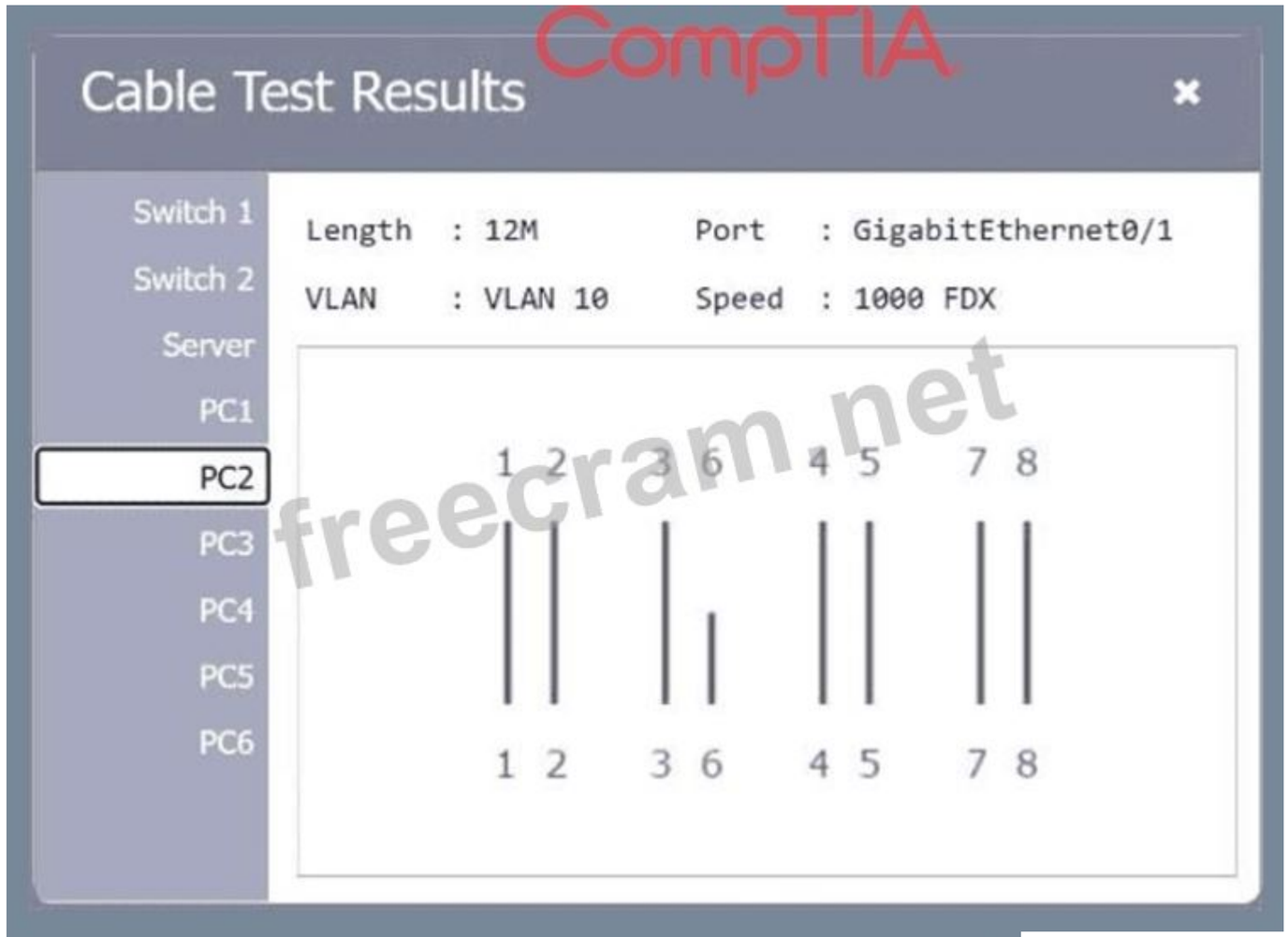

## Cable Test Results

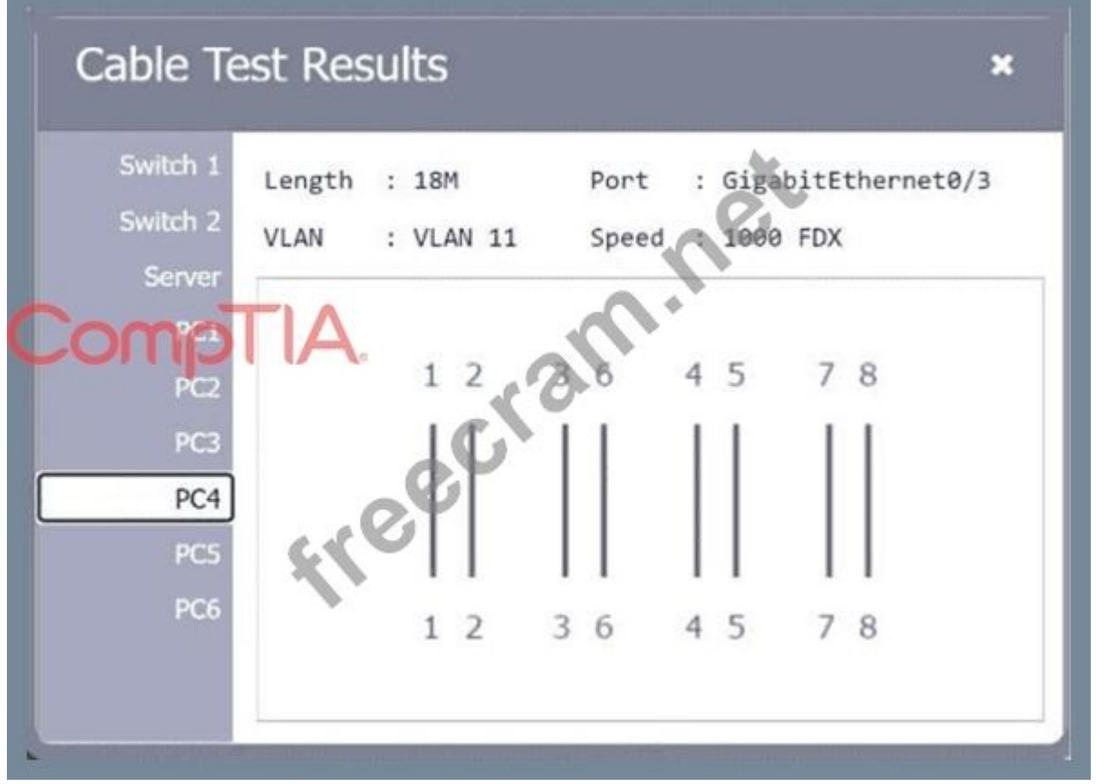
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6

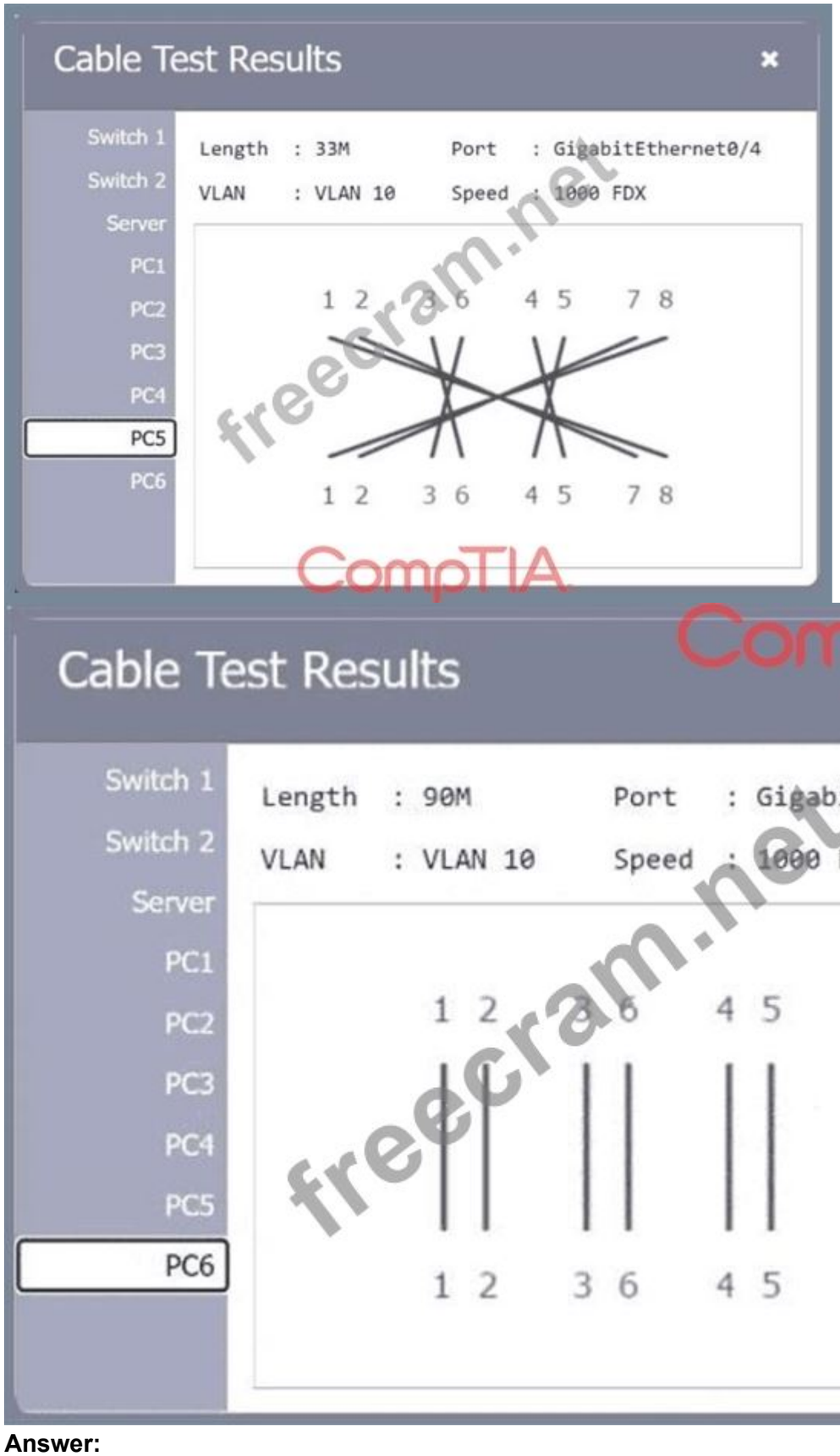
Length : 22M Port : GigabitEthernet0/1

VLAN : VLAN 10 Speed : 1000 FDX





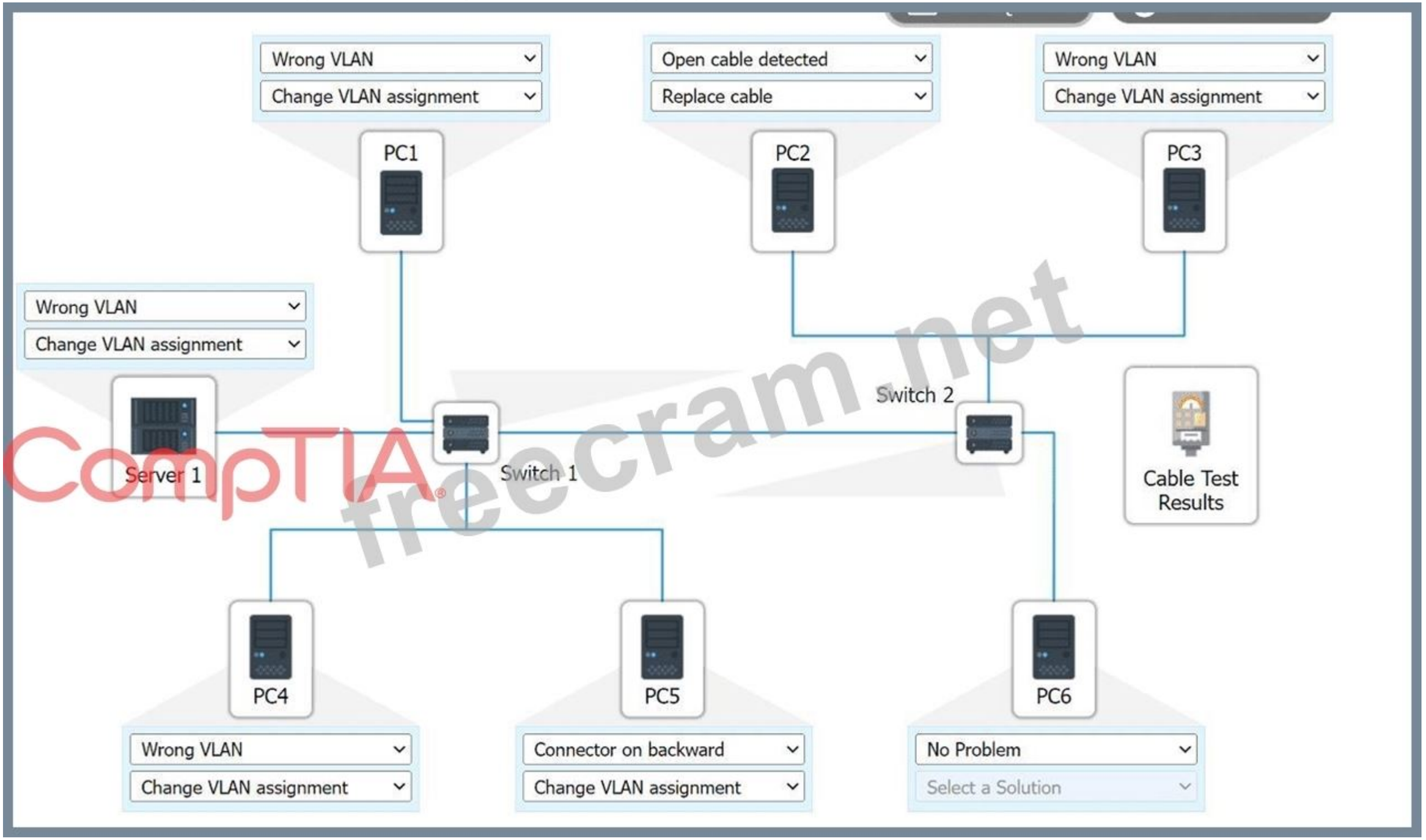





**Answer:**

See the answer and solution below:

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

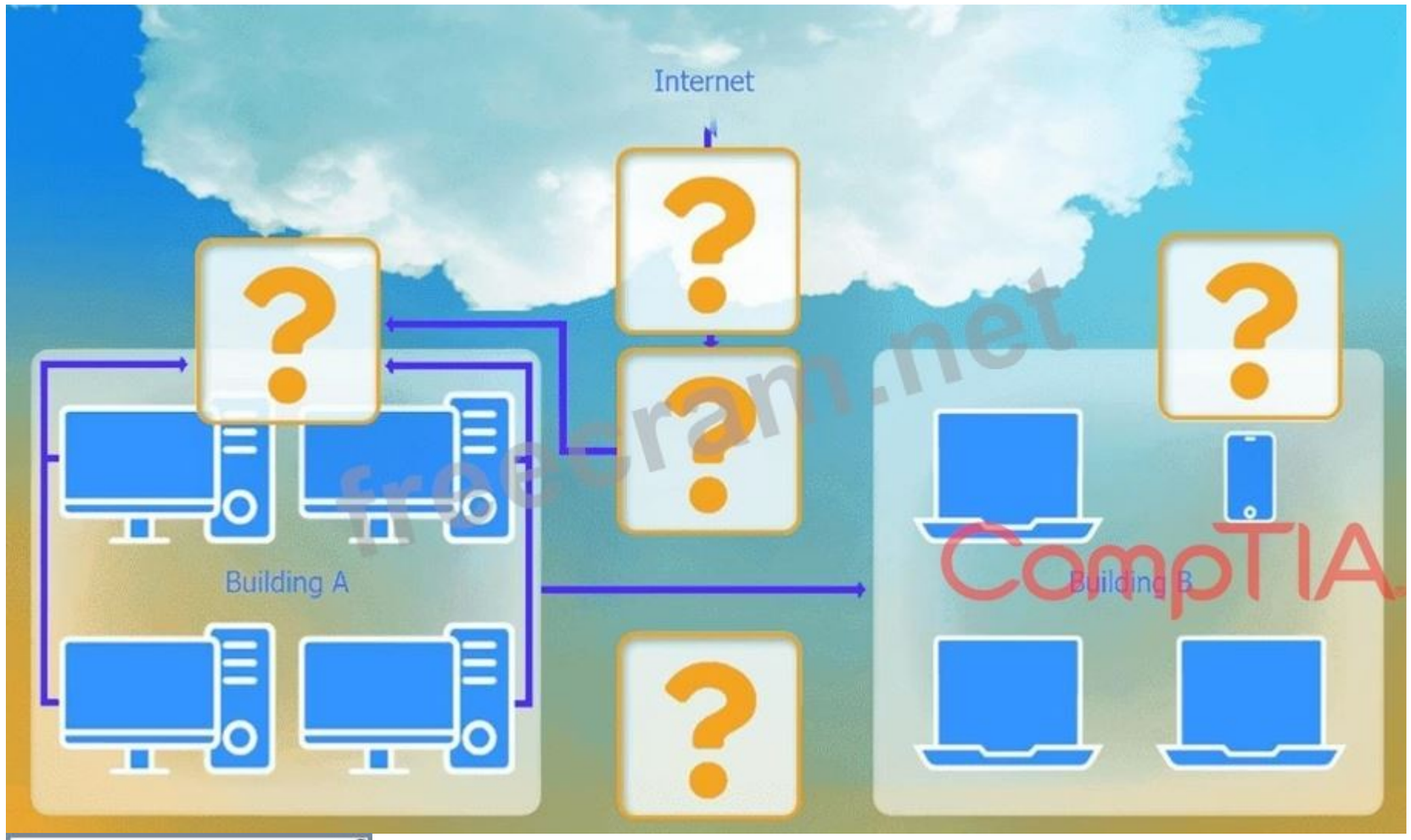





**NEW QUESTION: 171**
During a security audit, a consulting firm notices inconsistencies between the documentation and the actual environment. Which of the following can keep a record of who made the changes and what the changes are?
**A.** Network access control
**B.** Configuration monitoring
**C.** Zero Trust
**D.** Syslog

**Answer: (SHOW ANSWER)**
Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.
A). Network access control (NAC) manages endpoint access policies but does not track device config changes.
C). Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.
D). Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Change management, configuration management, auditing.

**NEW QUESTION: 172**
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

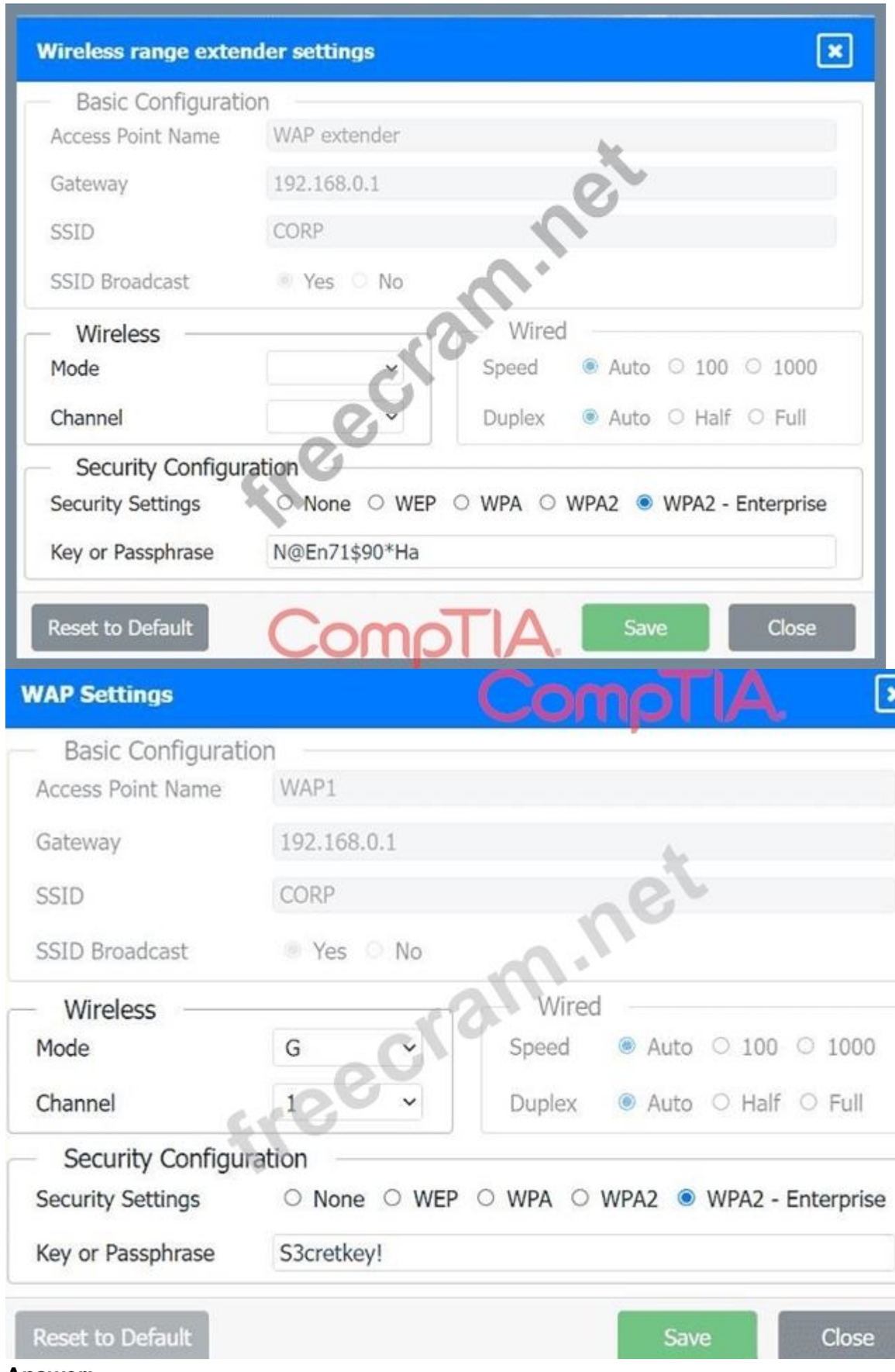
Switch

WAP

Firewall

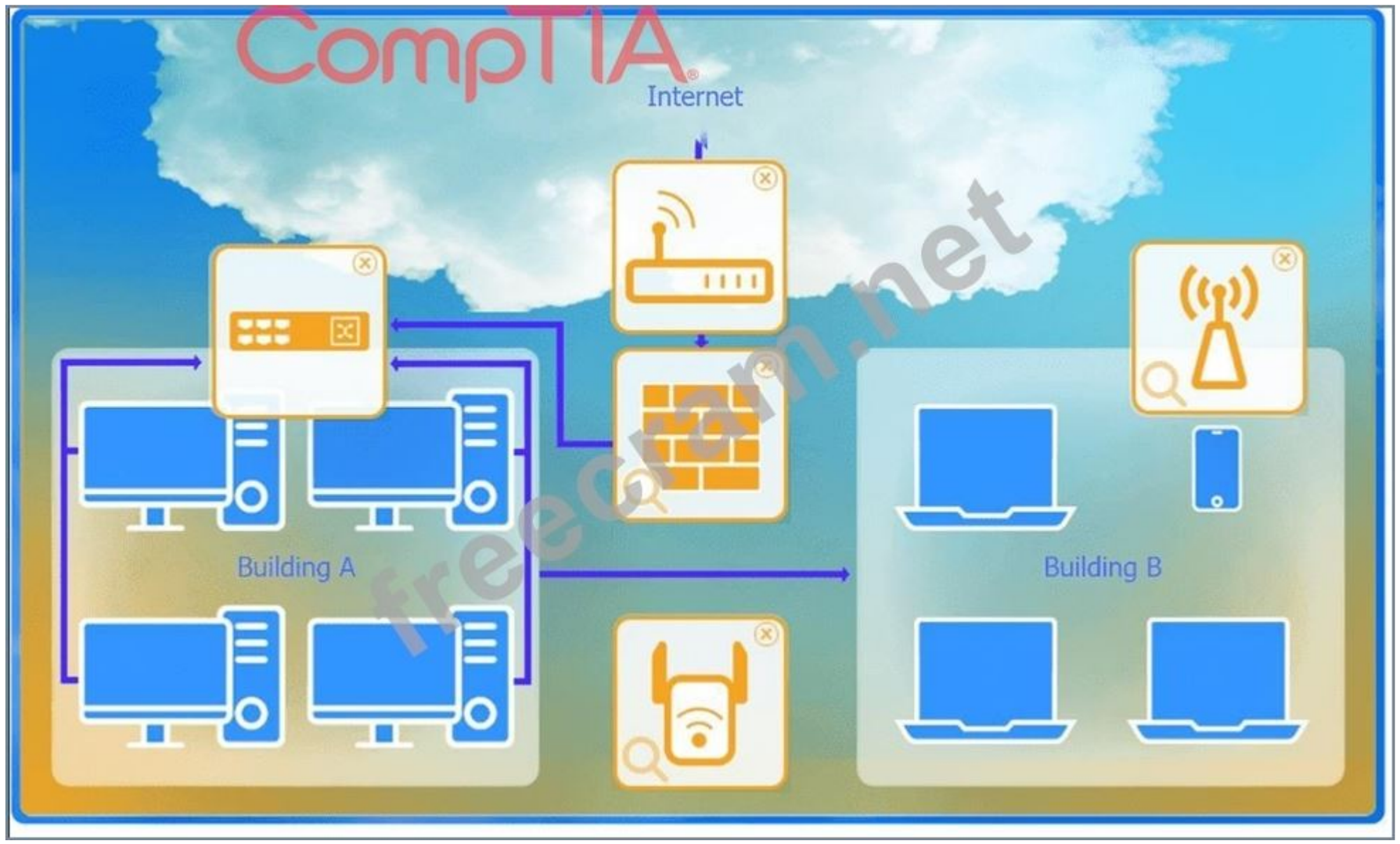
Router

Wireless range extender


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
WAP Settings
Basic Configuration
Access Point Name
WAP1
Gateway
192.168.0.1
SSID
CORP
SSID Broadcast
Yes
No
Wireless
Mode
G
Channel
1
Wired
Speed
Auto
100
1000
Duplex
Auto
Half
Full
Security Configuration
Security Settings
None
WEP
WPA
WPA2
WPA2 - Enterprise
Key or Passphrase
S3cretkey!
Reset to Default
Save
Close

**Answer:**

See the step by step complete solution below.
Explanation:
Devices in both buildings should be able to access the Internet.
Security insists that all Internet traffic be inspected before entering the network.
Desktops should not see traffic destined for other devices.
Here is the corrected layout with explanation:
Building A:
Switch: Correctly placed to connect all desktops.
Firewall: Correctly placed to inspect all incoming and outgoing traffic.
Building B:
Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.
Between Buildings:
Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.
Connection to the Internet:
Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.
Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.
Corrected Setup:
Top-left (Building A): Switch
Bottom-left (Building A): Firewall (inspect traffic before it enters the network) Top-middle (Internet connection): Router Bottom-middle (between buildings): Wireless Range Extender Top-right (Building B): Wireless Access Point (WAP) In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.
Configuration for Wireless Range Extender:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.




To configure the wireless range extender for security, follow these steps:

SSID (Service Set Identifier):

Ensure the SSID is set to " CORP " as shown in the exhibit.

Security Settings:

WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.

Key or Passphrase:

If you select WPA2, enter a strong passphrase in the " Key or Passphrase " field.

If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.

Wireless Mode and Channel:

Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.

Wired Speed and Duplex:

Set the speed to " Auto " unless you have specific requirements for 100 or 1000 Mbps.

Set the duplex to " Auto " unless you need to specify half or full duplex based on your network equipment.

Save Configuration:

After making the necessary changes, click the " Save " button to apply the settings.
Here is how the configuration should look after adjustments:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.
Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:
DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.
HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.
Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.
HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.
HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.
Suggested Additional Settings:
Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.
Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.
Firewall Configuration Adjustments:
Correct the Network Typo:
Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.
Permit General Outbound Traffic:
Rule Name: General Outbound
Source: 192.168.0.1/24
Destination: ANY
Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:
Rule Name
Source
Destination
Service
Action

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

Make sure to save the settings after making these adjustments.

**NEW QUESTION: 173**
A network administrator receives a ticket from a user. The user reports that they cannot access any websites and that they have already checked everything on their computer. Which of the following is the first action the administrator should take?
**A.** Divide and conquer.
**B.** Establish a theory of probable cause.
**C.** Question the user.
**D.** Document the findings.
**Answer: (SHOW ANSWER)**
The correct answer is Question the user because the first step in the CompTIA Network+ (N10-009) troubleshooting methodology is to identify the problem. Identifying the problem involves gathering information, asking clarifying questions, determining if anything has changed, and establishing the scope of the issue.
Even though the user states they have "checked everything," the administrator should not assume that all relevant troubleshooting steps were properly performed. The technician must ask specific questions such as:
Are other users affected? Is the issue limited to certain websites? Are there any error messages? When did the issue start? Were there recent updates or configuration changes?
Only after gathering sufficient information should the administrator move to the next steps, such as establishing a theory of probable cause (Option B) or using divide-and-conquer methods (Option A).
Documentation (Option D) occurs after resolving and verifying the issue.
Therefore, questioning the user to clearly define and scope the problem is the correct first action according to the structured troubleshooting process.

**NEW QUESTION: 174**
A user calls the help desk after business hours to complain that files on a device are inaccessible and the wallpaper was changed. The network administrator thinks that this issue is an isolated incident, but the security analyst thinks the issue might be a ransomware attack. Which of the following troubleshooting steps should be taken first?
**A.** Identify the problem.
**B.** Establish a theory.
**C.** Document findings.
**D.** Create a plan of action.
**Answer: (SHOW ANSWER)**
The correct answer is Identify the problem, which is always the first step in the CompTIA Network+ N10-009 troubleshooting methodology. Before forming theories, creating action plans, or documenting outcomes, technicians must clearly understand what is happening, who is affected, and what symptoms are present.
In this scenario, the symptoms-inaccessible files and a changed wallpaper-are serious and potentially indicative of a security incident such as ransomware. However, at this stage, there is disagreement between the network administrator and the security analyst regarding the nature of the issue. That reinforces the need to begin with problem identification, which includes gathering information, determining the scope of impact, identifying recent changes, and assessing whether the incident is isolated or widespread.
Establishing a theory comes after the problem has been clearly defined. Creating a plan of action and documenting findings occur later in the process, once the issue has been confirmed and remediation steps are determined. Jumping ahead without properly identifying the problem could result in delayed containment or an incorrect response-especially critical in potential security incidents.
The Network+ objectives emphasize following the structured troubleshooting process precisely to reduce risk, prevent escalation, and ensure accurate resolution-particularly when malware or ransomware may be involved.

**NEW QUESTION: 175**
Which of the following fiber connector types is the most likely to be used on a network interface card?

**A.** LC
**B.** SC
**C.** ST
**D.** MPO
**Answer: (SHOW ANSWER)**
* Definition of Fiber Connector Types:
* LC (Lucent Connector):A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.
* SC (Subscriber Connector or Standard Connector):A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.
* ST (Straight Tip):A bayonet-style connector, typically used in multimode fiber optic networks.
* MPO (Multi-fiber Push On):A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.
* Common Usage:
* LC Connectors:Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.
* SC and ST Connectors:These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.
* MPO Connectors:Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.
* Selection Criteria:
* The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.
References:
* CompTIA Network+ study materials on fiber optics and connector types.

**NEW QUESTION: 176**
A network administrator needs to add 255 useable IP addresses to the network. A /24 is currently in use.
Which of the following prefixes would fulfill this need?
**A.** /23
**B.** /25
**C.** /29
**D.** /32
**Answer: (SHOW ANSWER)**
A /23 subnet provides 512 total addresses, of which 510 are usable (subtracting 2 for network and broadcast addresses). This would satisfy the need for 255 additional addresses.

**NEW QUESTION: 177**
A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?
**A.** netstat
**B.** nslookup
**C.** ping
**D.** tracert
**Answer: (SHOW ANSWER)**
* Understanding Tracert:
* Traceroute Tool:tracert(Windows) ortraceroute(Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the

intermediate routers the packets traverse.
* Determining Traffic Path:
* Path Identification:By runningtracertto the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.
* Load Balancing Insight:If the office uses load balancing for its internet links,tracertcan help verify which link is currently handling the traffic for the web application.
* Comparison with Other Tools:
* netstat:Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
* nslookup:Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.
* ping:Tests connectivity and measures round-trip time but does not provide path information.
* Implementation:
* Open a command prompt or terminal.
* Executetracert [destination IP]to trace the route.
* Analyze the output to determine the path and the link being used.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

**NEW QUESTION: 178**
Voice traffic is experiencing excessive jitter. A network engineer wants to improve call performance and clarity. Which of the following features should the engineer configure?
**A.** QoS
**B.** STP
**Answer: (SHOW ANSWER)**
Quality of Service (QoS) prioritizes delay-sensitive traffic such as VoIP by assigning higher priority in queues, reducing jitter, latency, and packet loss. Implementing QoS policies ensures stable and clear voice communication.
B). STP (Spanning Tree Protocol) prevents switching loops, but it does not address jitter or real-time traffic performance.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - QoS, traffic shaping, prioritization of voice/video.

**NEW QUESTION: 179**
Which of the following connection methods allows a network engineer to automate the configuration deployment for network devices across the environment?
**A.** RDP
**B.** Telnet
**C.** GUI
**D.** API
**Answer: (SHOW ANSWER)**
Comprehensive and Detailed Explanation (aligned to N10-009):
APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to ensure consistency and scalability.
A). RDP is remote desktop for Windows systems, not automation.
B). Telnet is insecure and manual.
C). GUI requires manual configuration, not automation.
References (CompTIA Network+ N10-009):

Domain: Network Operations - Automation, orchestration, APIs in network management.

**NEW QUESTION: 180**

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: 181**

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: 182**

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: 183**
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: 184**
Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?
**A.** Router
**B.** Switch
**C.** Firewall
**D.** Load balancer
**Answer: (SHOW ANSWER)**
A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.
Breakdown of Options:
A). Router - Directs traffic between networks, not between web servers.
B). Switch - Works at Layer 2, does not distribute web traffic.
C). Firewall - Secures network traffic, but does not distribute load.
D). Load balancer - # Correct answer. Optimizes web traffic distribution across multiple servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

**NEW QUESTION: 185**
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: 186**

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

**A.** Geofencing

**B.** Honeynet

**C.** Jumpbox

**D.** Screened subnet

**Answer: (SHOW ANSWER)**

A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. References: CompTIA Network + Exam Objectives and official study guides.

**NEW QUESTION: 187**

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: 188**
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: 189**
Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?
**A.** To encrypt sensitive data in transit
**B.** To secure the endpoint
**C.** To maintain contractual agreements
**D.** To comply with data retentin requirements
**Answer: (SHOW ANSWER)**
The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
* Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
* Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
* Security: Enhances overall network security by providing secure remote access for employees.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.
* Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.
* Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

**NEW QUESTION: 190**

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?



**A.** tcpdump
**B.** dig
**C.** tracert
**D.** arp
**Answer: (SHOW ANSWER)**
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.References: CompTIA Network+ study materials and common network troubleshooting commands.

**NEW QUESTION: 191**
Which of the following is the most cost-efficient way to host email services?
**A.** PaaS
**B.** IaaS
**C.** VPC
**D.** SaaS
**Answer: D (LEAVE A REPLY)**
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: 192**
A network technician is working on a PC with a faulty NIC. The host is connected to a switch with secured ports. After testing the connection cables and using a known-good NIC, the host is still unable to connect to the network. Which of the following is causing the connection issue?
**A.** MAC address of the new card
**B.** BPDU guard settings
**C.** Link aggregation settings
**D.** PoE power budget
**Answer: (SHOW ANSWER)**
If a switch has port security enabled (such as sticky MAC or a configured allowed MAC), the port will only allow the original NIC's MAC address. When a new NIC with a different MAC address is installed, the port rejects traffic, preventing network connectivity.
B). BPDU guard protects against rogue switches, not end hosts.

C). Link aggregation applies when bundling multiple uplinks, not a single PC connection.
D). PoE budget applies to powered devices like APs, not PCs.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port security, MAC address filtering, switch security features.

**NEW QUESTION: 193**
Which of the following most directly secures sensitive information on a network?
**A.** Data-in-transit encryption
**B.** Principle of least privilege
**C.** Role-based access controls
**D.** Multifactor authentication
**Answer: (SHOW ANSWER)**
The option that most directly secures sensitive information on the network is data-in-transit encryption. This ensures that data packets are unreadable to attackers who intercept them while moving across the network.
Protocols such as TLS, HTTPS, IPsec, and SSH protect confidentiality and integrity of sensitive information.
B). Principle of least privilege (PoLP) secures access control but does not directly protect data in motion.
C). Role-based access control (RBAC) enforces permissions but again does not secure the data while transmitted.
D). Multifactor authentication (MFA) strengthens identity verification but does not directly protect the data itself once transmitted.
Thus, while all options contribute to overall security, encryption of data-in-transit most directly addresses protection of sensitive information on the network.
References (CompTIA Network+ N10-009):
Domain: Network Security - Encryption methods, confidentiality, data-in-transit protection.

**NEW QUESTION: 194**
Which of the following routing protocols is most commonly used to interconnect WANs?
**A.** IGP
**B.** EIGRP
**C.** BGP
**D.** OSPF
**Answer: (SHOW ANSWER)**
Border Gateway Protocol (BGP): BGP is the most commonly used routing protocol for interconnecting WANs, especially across the internet. It is used for exchanging routing information between autonomous systems (AS), making it the backbone protocol for large-scale WANs.
IGP (A): Interior Gateway Protocols like OSPF and EIGRP are typically used within a single AS, not between them.
EIGRP (B): While it is efficient, EIGRP is primarily used for intra-domain routing and not ideal for WAN interconnection.
OSPF (D): While OSPF can be used for WANs, it is not as common as BGP for inter-AS communication.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (WAN Concepts), Domain 2.5 (Routing Protocols).

**NEW QUESTION: 195**
Which of the following can also provide a security feature when implemented?
**A.** NAT
**B.** BGP
**C.** FHRP

**D.** EIGRP
**Answer: (SHOW ANSWER)**
NAT (Network Address Translation) helps hide internal IP addresses from external networks, adding a layer of security by preventing direct access to internal systems from the outside.

**NEW QUESTION: 196**
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: 197**
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: 198**
A company ' s Chief Information Security Officer requires that servers and firewalls have accurate time stamps 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.** NTP

**D.** SNMP

**Answer: (SHOW ANSWER)**

The correct solution is NTP (Network Time Protocol). Accurate timestamps across servers, firewalls, and network devices are critical for correlating logs during incident response. NTP synchronizes device clocks to a trusted time source, ensuring consistency across the network.

A). Syslog centralizes logs but does not synchronize time.

B). SMTP is email transfer, unrelated to time.

D). SNMP monitors devices but does not correct time discrepancies.

By implementing NTP, analysts can ensure that logs from different devices are time-aligned, which is essential for reconstructing attack timelines and detecting anomalies.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Time synchronization, NTP, log correlation.

**NEW QUESTION: 199**

Which of the following can support a jumbo frame?

**A.** Access point

**B.** Bridge

**C.** Hub

**D.** Switch

**Answer: (SHOW ANSWER)**

* Definition of Jumbo Frames:

* Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.

* Why Switches Support Jumbo Frames:

* Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.

* Incompatibility of Other Devices:

* Access Point: Primarily handles wireless communications and does not typically support jumbo frames.

* Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.

* Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.

* Practical Application:

* Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.

References:

* CompTIA Network+ course materials and networking hardware documentation.

**NEW QUESTION: 200**

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: 201**
A Linux server is running a log collector that needs to be hardened. A network administrator executes netstat to find open ports on the server. Which of the following ports should be disabled?
**A.** 22
**B.** 80
**C.** 162
**D.** 514
**Answer: B (LEAVE A REPLY)**
Comprehensive and Detailed Explanation (aligned to N10-009):
For a log collector server, the primary needed service is Syslog, which typically uses UDP port 514. Other ports may be open for management (e.g., 22 for SSH) or SNMP traps (162) if integrated. However, port 80 (HTTP) should not be open unless required, as it increases attack surface and does not directly serve the log collection purpose. Disabling it hardens the server.
A). 22 (SSH) is needed for secure management.
C). 162 (SNMP trap) may be required for monitoring/log correlation.
D). 514 (Syslog) is essential for log collection.
References (CompTIA Network+ N10-009):
Domain: Network Security - Hardening servers, disabling unnecessary services and ports.

**NEW QUESTION: 202**
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: 203**
Which of the following allows for the interception of traffic between the source and destination?
**A.** Self-signed certificate
**B.** VLAN hopping
**C.** On-path attack
**D.** Phishing
**Answer: (SHOW ANSWER)**
An on-path attack (formerly known as a man-in-the-middle (MITM) attack) involves intercepting and potentially altering communications between two parties without their knowledge. This can be done via techniques like ARP poisoning, rogue access points, or SSL stripping.
Breakdown of Options:
A). Self-signed certificate - These are untrusted SSL certificates but do not intercept traffic.
B). VLAN hopping - VLAN hopping exploits VLAN misconfigurations but does not necessarily intercept communications.
C). On-path attack - Correct answer. This intercepts and modifies traffic between two endpoints.
D). Phishing - Phishing tricks users into revealing credentials rather than intercepting network traffic.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.2: Explain common security concepts.
NIST SP 800-115: Guide to Security Testing and Assessments

**NEW QUESTION: 204**
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: 205**
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: 206**

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: 207**

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: 208**
A network administrator is trying to troubleshoot an issue with a newly installed switch that is not connecting to the network. The administrator logs on to the switch and observes collisions on the interface. Which of the following is most likely the issue?
**A.** Wrong speed
**B.** Jumbo frames enabled
**C.** Incorrect VLAN
**D.** Duplex mismatch
**Answer: (SHOW ANSWER)**
The most likely issue is a duplex mismatch, which is a well-documented cause of collisions and poor network performance, as outlined in the CompTIA Network+ N10-009 troubleshooting objectives. A duplex mismatch occurs when one end of a network link is configured for full duplex while the other end is operating in half duplex. In half-duplex mode, devices must take turns transmitting and receiving data, which inherently allows for collisions. When paired with a full-duplex device-which expects simultaneous send and receive- collisions and retransmissions occur frequently.
The presence of collisions on a switch interface is a key diagnostic clue. Modern Ethernet switches operating correctly in full duplex should not experience collisions at all. When collisions are observed, it almost always points to a duplex configuration issue, often caused by manual speed/duplex settings on one device and auto- negotiation on the other.
A wrong speed setting may prevent link establishment entirely or cause errors, but it does not typically result in collisions. Jumbo frames can cause packet drops or fragmentation issues, not collisions. An incorrect VLAN configuration affects logical segmentation and connectivity but operates at Layer 2 and does not generate collisions.
CompTIA Network+ emphasizes duplex mismatch as a classic and frequently tested troubleshooting scenario.
Correcting it-usually by enabling auto-negotiation on both ends-restores normal, collision-free communication.

**NEW QUESTION: 209**
A new network is being created to support 126 users. Which of the following CIDR ranges provides the most efficient use of space?
**A.** 10.2.2.0/23
**B.** 10.2.2.0/24
**C.** 10.2.2.0/25
**D.** 10.2.2.0/26
**Answer: (SHOW ANSWER)**
To support 126 users, the subnet must provide at least 126 usable host addresses. In IPv4 subnetting, usable hosts are calculated as: (2^(host bits)) # 2, subtracting the network and broadcast addresses.
A /25 leaves 7 host bits (because 32 # 25 = 7). That yields 2^7 = 128 total addresses, and 128 # 2 = 126 usable-an exact fit and therefore the most efficient option listed.
A /24 provides 256 total addresses and 254 usable, which would waste more addresses than necessary. A /23 provides 512 total addresses and 510 usable-far more waste. A /26 leaves 6 host bits, giving 64 total addresses and 62 usable, which is not enough for 126 users.
The 10.2.2.0 address is within the private 10.0.0.0/8 range, so it's appropriate for internal addressing.
Therefore, 10.2.2.0/25 is the correct CIDR range for efficiently supporting 126 hosts.

**NEW QUESTION: 210**
Which of the following connector types is most commonly associated with Wi-Fi antennas?
**A.** BNC

**B.** SFP
**C.** MPO
**D.** RJ45
**Answer: (SHOW ANSWER)**
BNC (Bayonet Neill-Concelman) connectors are commonly used with coaxial cables in RF and wireless applications, including some older Wi-Fi antennas and specialized networking equipment. The document says:
"BNC (Bayonet Neill-Concelman) connectors are typically used with coaxial cables, especially in radio frequency (RF) and some Wi-Fi antenna applications, providing a secure and quick connect/disconnect."

**NEW QUESTION: 211**
Which of the following are the best device-hardening techniques for network security? (Select two).
**A.** Disabling unused ports
**B.** Performing regular scanning of unauthorized devices
**C.** Monitoring system logs for irregularities
**D.** Enabling logical security such as SSO
**E.** Changing default passwords
**F.** Ensuring least privilege concepts are in place
**Answer: (SHOW ANSWER)**
Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. References: CompTIA Network+ Exam Objectives and official study guides.



**NEW QUESTION: 212**
Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).
**A.** The switches are not the correct voltage.
**B.** The HVAC system was not verified as fully functional after the fire.
**C.** The VLAN database was not deleted before the equipment was brought back online.
**D.** The RJ45 cables were replaced with unshielded cables.
**E.** The wrong transceiver type was used for the new termination.
**F.** The new RJ45 cables are a higher category than the old ones.
**Answer: (SHOW ANSWER)**
* Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.
* Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

**NEW QUESTION: 213**
A network engineer needs to virtualize network services, including a router at a remote branch location.

Which of the following solutions meets the requirements?

**A.** NFV

**B.** VRF

**C.** VLAN

**D.** VPC

**Answer: (SHOW ANSWER)**

Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.

VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.

VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.

VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.

Reference: CompTIA Network+ Official Study Guide, Domain 2.1 (Virtualization and Cloud Concepts).

**NEW QUESTION: 214**

Which of the following is the greatest advantage of maintaining a cold DR site compared to other DR sites?

**A.** Redundancy

**B.** Availability

**C.** Security

**D.** Cost

**Answer: (SHOW ANSWER)**

Acold disaster recovery (DR) siteis a backup facility equipped withminimal infrastructure, often lacking active systems or real-time data replication. Itsgreatest advantage is cost-efficiency. Cold sites aremuch cheaperto maintain than warm or hot sites, which require continuous synchronization and operational readiness. They are used when low cost is more important than recovery speed.

Reference:Section 3.3 - Disaster Recovery Concepts - "Cold, Warm, and Hot Sites Comparison"

**NEW QUESTION: 215**

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?

**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: 216**
A company experiences an incident involving a user who connects an unmanaged switch to the network.
Which of the following technologies should the company implement to help avoid similar incidents without conducting an asset inventory?
**A.** Screened subnet
**B.** 802.1X
**C.** MAC filtering
**D.** Port security
**Answer: (SHOW ANSWER)**
Port security is a Layer 2 security feature that restricts the number of devices connecting to a network switch port. It helps prevent unauthorized devices, such as an unmanaged switch, from being connected to the network.
How Port Security Works:
Limits the number of MAC addresses that can connect to a port.
Can shut down or restrict the port if an unauthorized device is detected.
Prevents users from plugging in unauthorized networking equipment (e.g., unmanaged switches, hubs).
Incorrect Options:
A). Screened Subnet: A screened subnet (DMZ) is used for isolating external-facing servers, not for controlling unauthorized network connections.
B). 802.1X: Provides authentication for devices but requires a RADIUS server, which is a more complex solution than port security.
C). MAC Filtering: Controls which MAC addresses can connect but is difficult to manage and can be spoofed.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Security Controls

**NEW QUESTION: 217**
A junior network administrator gets a text message from a number posing as the domain registrar of the firm.
The administrator is tricked into providing global administrator credentials. Which of the following attacks is taking place?
**A.** DNS poisoning
**B.** ARP spoofing
**C.** Vishing
**D.** Smishing
**Answer: (SHOW ANSWER)**

Smishing (SMS phishing) occurs when attackers send fraudulent text messages pretending to be a trusted source, tricking the victim into giving up sensitive credentials. Since this came via text message, it qualifies as smishing.
A). DNS poisoning corrupts name resolution.
B). ARP spoofing manipulates MAC-to-IP mappings.
C). Vishing is phishing via voice calls, not text.
References (CompTIA Network+ N10-009):
Domain: Network Security - Social engineering, phishing types (smishing, vishing, spear phishing).

**NEW QUESTION: 218**
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: 219**
A network engineer is troubleshooting connectivity for a newly installed server on an existing VLAN. The engineer reviews the following output:
C:\> ipconfig
IP Address: 192.168.100.225
Mask: 255.255.255.224
Gateway: 192.168.100.254
Router# show ip route
C 192.168.100.0/24 is directly connected, GigabitEthernet0/0
Which of the following describes the issue?
**A.** The server has an incorrect subnet mask
**B.** There is a duplicate IP address on the network
**C.** The DHCP address pool is exhausted
**D.** The router is missing a default route
**Answer: (SHOW ANSWER)**
The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to

192.168.100.255. However, the router only recognizes 192.168.100.0/24, indicating a mismatch between the server's subnet and the router's network.
Correct mask for the /24 network is 255.255.255.0, allowing 256 IPs from 192.168.100.0 to 192.168.100.255.
This mismatch would result in routing issues, especially with the gateway outside of the subnet range.
# Reference:
CompTIA Network+ N10-009 Official Objectives: 5.2 - Given a scenario, troubleshoot common wired connectivity issues.

**NEW QUESTION: 220**
Which of the following is used to estimate the average life span of a device?
**A.** RTO
**B.** RPO
**C.** MTBF
**D.** MTTR
**Answer: (SHOW ANSWER)**
* Understanding MTBF:
* Mean Time Between Failures (MTBF):A reliability metric that estimates the average time between successive failures of a device or system.
* Calculation and Importance:
* Calculation:MTBF is calculated as the total operational time divided by the number of failures during that period.
* Usage:Used by manufacturers and engineers to predict the lifespan and reliability of a device, helping in maintenance planning and lifecycle management.
* Comparison with Other Metrics:
* RTO (Recovery Time Objective):The maximum acceptable time to restore a system after a failure.
* RPO (Recovery Point Objective):The maximum acceptable amount of data loss measured in time.
* MTTR (Mean Time to Repair):The average time required to repair a device or system and return it to operational status.
* Application:
* MTBF is crucial for planning maintenance schedules, spare parts inventory, and improving the overall reliability of systems.
References:
* CompTIA Network+ study materials on reliability and maintenance metrics.

**NEW QUESTION: 221**
Which of the following is a documented set of requirements, such as quality, availability, and responsibilities delivered by a vendor?
**A.** MOU
**B.** EOL
**C.** EOS
**D.** SLA
**Answer: (SHOW ANSWER)**
The correct answer is SLA (Service Level Agreement) because it is a formal, documented contract between a service provider and a customer that defines expected service standards. According to CompTIA Network+ (N10-009) objectives under network operations and service management concepts, an SLA outlines measurable performance metrics such as uptime percentage, response time, throughput, support availability, escalation procedures, and responsibilities of both parties.
An SLA ensures accountability and establishes clear expectations for service delivery. For example, a vendor may guarantee 99.99% uptime, define maximum resolution times for incidents, and specify penalties or credits if performance targets are not met. SLAs are critical in cloud services, ISP agreements, managed services, and enterprise vendor contracts.
An MOU (Memorandum of Understanding) is a non-binding agreement outlining general terms between parties but does not define enforceable service metrics. EOL (End of Life)

refers to when a product is no longer sold or supported. EOS (End of Support) indicates when a vendor stops providing updates or assistance for a product.
Therefore, an SLA is the correct document that defines vendor-delivered service requirements.
Top of Form

**NEW QUESTION: 222**
A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25.
However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?
**A.** 255.255.254.0
**B.** 255.255.255.1
**C.** 255.255.255.128
**D.** 255.255.255.192
**Answer: (SHOW ANSWER)**
A /25 subnet mask means 25 bits are reserved for the network portion, leaving 7 bits for host addresses. In dotted decimal, that is:
11111111.11111111.11111111.10000000
Decimal equivalent: 255.255.255.128
A). 255.255.254.0 corresponds to /23.
B). 255.255.255.1 is invalid as a subnet mask.
D). 255.255.255.192 corresponds to /26.
Thus, the correct subnet mask for a /25 network is 255.255.255.128.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Subnetting, CIDR notation, dotted decimal.

**NEW QUESTION: 223**
A network administrator configured a router interface as 10.0.0.95 255.255.255.240. The administrator discovers that the router is not routing packets to a web server with IP 10.0.0.81/28. Which of the following is the best explanation?
**A.** Theweb server Is In adifferent subnet.
**B.** Therouter interface isa broadcast address.
**C.** TheIP address spaceis a class A network.
**D.** Thesubnet is in a private address space.
**Answer: (SHOW ANSWER)**
Understanding Subnetting:
The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).
Calculating the Subnet Range:
Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:
Network address: 10.0.0.80
Usable IP range: 10.0.0.81 to 10.0.0.94
Broadcast address: 10.0.0.95
Router Interface Configuration:
Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28.
Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.
Comparison with Other Options:
The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80

/28).
The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.
The subnet is in a private address space: The private address space designation (RFC 1918) does not impact the routing issue related to the broadcast address configuration.
Resolution:
Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.
References:
CompTIA Network+ study materials on subnetting and IP address configuration.