CompTIA.N10-009.v2026-08-13.q237

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	237
Version:	v2026-08-13
# of views:	104
# of Questions views:	2370
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-08-13.q237.html	

NEW QUESTION: 1
A network administrator configures a new network discovery tool and is concerned that it might disrupt business operations. Which of the following scan types should the administrator configure?
A. Authenticated
B. Ad hoc
C. Unauthenticated
D. Scheduled
Answer: (SHOW ANSWER)
If the administrator is concerned a new discovery tool could disrupt operations, the safest option is to configure scheduled scans. Network+ (N10-009) operations guidance emphasizes minimizing impact by running potentially noisy tasks (discovery, vulnerability checks, inventory scans) during defined maintenance windows or off-peak hours. A scheduled scan allows controlled timing, predictable load, and easier coordination with change management, monitoring, and support teams. This reduces the risk of saturating links, overwhelming devices with queries, or triggering alerts during business-critical periods.
Ad hoc scanning is on-demand and may occur at any time, which increases the chance of disruption if run during peak usage. Authenticated versus unauthenticated describes whether the scanner uses credentials to log into systems for deeper visibility; that choice affects depth and accuracy, but it doesn't directly address when scanning occurs to reduce business impact. An authenticated scan can still be disruptive if run at the wrong time, and an unauthenticated scan can still generate significant traffic. Since the key concern is operational disruption, controlling scan timing via scheduled scans is the best mitigation.

NEW QUESTION: 2
A company reports that their facsimile machine no longer has a dial tone when trying to send a fax. The phone cable is damaged on one end. Which of the following types of connectors should a technician replace?
A. F-type
B. RJ45
C. SC
D. RJ11
Answer: (SHOW ANSWER)
Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.
F-type is used for coaxial cables (e.g., TV and cable modems).

RJ45 is used for Ethernet network connections.
SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.4 - Compare and contrast common network connectors.

NEW QUESTION: 3
A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?
A. 255.255.0.0
B. 255.255.254.0
C. 255.255.255.0
D. 255.255.255.128
Answer: (SHOW ANSWER)
* Understanding Subnetting:
* Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).
* Objective: Divide this network into two equal subnets.
* Calculating Subnet Mask:
* New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).
* Subnet Breakdown:
* First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)
* Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)
* Verification:
* Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).
* Comparison with Other Options:
* 255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.
* 255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.
* 255.255.255.0 (/24): Maintains the original subnet size, not dividing it.
References:
* CompTIA Network+ study materials on subnetting and IP addressing.

NEW QUESTION: 4
Which of the following disaster recovery concepts is calculated by dividing the total hours of operation by the total number of units?
A. MTTR
B. MTBF
C. RPO
D. RTO
Answer: (SHOW ANSWER)
Introduction to Disaster Recovery Concepts:
Disaster recovery involves strategies and measures to ensure business continuity and data recovery in the event of a disaster.
Mean Time Between Failures (MTBF):
MTBF is a reliability metric used to predict the time between failures of a system during operation. It is calculated by dividing the total operational time by the number of failures.

Formula: MTBF=Total Operational TimeNumber of Failures\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}MTBF=Number of FailuresTotal Operational Time This metric helps in understanding the reliability and expected lifespan of systems and components.
Example Calculation:
If a server operates for 1000 hours and experiences 2 failures, the MTBF is:
MTBF=1000 hours2=500 hours\text{MTBF} = \frac{1000 \text{ hours}}{2} = 500 \text{ hours} MTBF=21000 hours=500 hours Explanation of the Options:
A). MTTR (Mean Time to Repair): The average time required to repair a system after a failure.
B). MTBF (Mean Time Between Failures): The correct answer, representing the average time between failures.
C). RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time.
D). RTO (Recovery Time Objective): The target time set for the recovery of IT and business activities after a disaster.
Conclusion:
MTBF is a crucial metric in disaster recovery and system reliability, helping organizations plan maintenance and predict system performance.
References:
CompTIA Network+ guide explaining MTBF, MTTR, RPO, and RTO concepts and their calculations (see page Ref 10 How to Use Cisco Packet Tracer).

NEW QUESTION: 5
A network administrator is troubleshooting a connection issue and needs to determine the path that a packet will take. Which of the following commands accomplishes this task?
A. netstat
B. traceroute
C. ping
D. nslookup
E. ipconfig
Answer: (SHOW ANSWER)
The correct answer is traceroute, which is the diagnostic command specifically designed to determine the path a packet takes across a network. According to the CompTIA Network+ N10-009 objectives, traceroute is a key network troubleshooting tool used to identify routing paths, hop counts, and points of latency or failure between a source and a destination.
Traceroute works by sending packets with incrementally increasing Time to Live (TTL) values. Each router along the path decrements the TTL by one, and when it reaches zero, the router returns an ICMP Time Exceeded message. This process allows the administrator to see each intermediate hop, its response time, and where packets may be delayed or dropped.
The other options do not fulfill this purpose. Ping only verifies basic connectivity and round-trip time but does not show the route taken. Netstat displays active connections, ports, and routing tables but does not trace packet paths. Nslookup is used to resolve DNS names to IP addresses, and ipconfig displays local network configuration information.
The Network+ objectives emphasize traceroute (or tracert on Windows systems) as the primary tool for diagnosing routing issues, asymmetric paths, and network congestion, making it the correct and most appropriate choice in this scenario.

NEW QUESTION: 6
A company recently implemented a videoconferencing system that utilizes large amounts of bandwidth. Users start reporting slow internet speeds and an overall decrease in network performance. Which of the following are most likely the causes of the network performance issues? (Select two)
A. DNS misconfiguration
B. Inadequate network security
C. Malware or a virus
D. Outdated software
E. Incorrect QoS settings
F. Network congestion
Answer: (SHOW ANSWER)

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

NEW QUESTION: 7
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: C (LEAVE A REPLY)
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: 8
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: 9
Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?
A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map
Answer: (SHOW ANSWER)
* Definition of Heat Maps:
* A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.
* Purpose of a Heat Map:
* Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.
* Comparison with Other Options:
* Logical Diagram: Represents the logical connections and relationships within the network.
* Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.
* Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.
* Creation and Use:
* Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
References:
* CompTIA Network+ certification materials and wireless network planning guides.

NEW QUESTION: 10
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: 11
Users report latency with a SaaS application. Which of the following should a technician adjust to fix the issue?
A. Server hardware specifications

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

NEW QUESTION: 12
Which of the following allows a remote user to connect to the network?
A. Command-line interface
B. API gateway
C. Client-to-site VPN
D. Jump box
Answer: (SHOW ANSWER)
A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

NEW QUESTION: 13
A company implements a video streaming solution that will play on all computers that have joined a particular group, but router ACLs are blocking the traffic. Which of the following is the most appropriate IP address that will be allowed in the ACL?
A. 127.0.0.1
B. 172.17.1.1
C. 224.0.0.1
D. 240.0.0.1
Answer: (SHOW ANSWER)
224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.
*Why not the other options?
*127.0.0.1 (A) - This is the loopback address used for internal device testing, not for multicast traffic.
*172.17.1.1 (B) - This is a private unicast address, meaning it can only send packets to one specific host.
*240.0.0.1 (D) - This falls within the reserved experimental IP address range and is not used for multicast.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 14

Which of the following types of routes takes precedence when building a routing table for a given subnet?
A. Static
B. BGP
C. OSPF
D. Default
Answer: (SHOW ANSWER)
The correct answer is Static because static routes have a lower administrative distance (AD) than most dynamic routing protocols, giving them higher priority when a router selects routes for the same destination network. According to CompTIA Network+ (N10-009) routing objectives, administrative distance is used to determine the trustworthiness of a route source when multiple routing protocols provide a path to the same subnet. The lower the administrative distance, the more preferred the route.
By default, a static route has an administrative distance of 1, which is lower than OSPF (110) and BGP (20 for eBGP, 200 for iBGP). Because of this, when identical routes to a subnet exist from both static and dynamic sources, the router installs the static route in the routing table.
A default route (0.0.0.0/0) is only used when no more specific route exists and does not take precedence over specific static or dynamic routes.
Therefore, when building the routing table for a given subnet and comparing route sources, static routes take precedence due to their lower administrative distance.

NEW QUESTION: 15
Which of the following offers the ability to manage access at the cloud VM instance?
A. Security group
B. Internet gateway
C. Direct Connect
D. Network ACL
Answer: (SHOW ANSWER)
Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.
From Andrew Ramdayal's guide:
"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC.
They act as a virtual firewall for associated instances..."

NEW QUESTION: 16
Which of the following impacts the availability of a web-based customer portal?
A. MAC flooding
B. ARP spoofing
C. DoS
D. Rogue devices
Answer: (SHOW ANSWER)
A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.
MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability. ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

NEW QUESTION: 17
A network engineer is implementing a new connection between core switches. The engineer deploys the following configurations:
Core-SW01
vlan 100
name
interface Ethernet 1/1
channel-group 1 mode active
interface Ethernet 1/2
channel-group 1 mode active
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100
Core-SW02
vlan 100
name
interface Ethernet 1/1
switchport mode trunk
switchport trunk allow vlan 100
interface Ethernet 1/2
switchport mode trunk
switchport trunk allow vlan 100
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100
Which of the following is the state of the Core-SW01 port-channel interfaces?
A. Incrementing CRC errors
B. Error disabled
C. Administratively down
D. Suspended
Answer: (SHOW ANSWER)
On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core-SW02, the ports are configured as independent trunks, not as part of an LACP group. Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.
A). CRC errors suggest cabling or signal integrity issues, not config mismatch.
B). Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not LACP mismatch.

C). Administratively down indicates a shutdown command, not the case here.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port-channel/LACP configuration issues, interface states.

NEW QUESTION: 18
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: 19
Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?
A. General Data Protection Regulation
B. Least privilege network access
C. Acceptable use policy
D. End user license agreement
Answer: (SHOW ANSWER)
Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 20
A network administrator needs a solution to isolate and potentially identify any threat actors that are attempting to breach the network. Which of the following should the administrator implement to determine the type of attack used?

A. MFA
B. Screened subnet
C. Captive portal
D. Honeypot
Answer: (SHOW ANSWER)

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

NEW QUESTION: 21
Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?
A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.
Answer: (SHOW ANSWER)
* Troubleshooting Methodology:
* Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
* Confirming a Theory:
* Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
* Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
* Comparison with Other Steps:
* Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
* Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
* Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
* Implementation:
* Use similar equipment or software in a test environment to recreate the issue.
* Observe the results to see if they match the original problem, thereby confirming the theory.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

NEW QUESTION: 22
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: 23
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: 24
A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?
A. Update the firmware.
B. Replace the system board.
C. Patch the OS.
D. Isolate the system.
Answer: (SHOW ANSWER)
Understanding the Vulnerability:
Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.
Firmware Update:
Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.
Procedure: Download the latest firmware from the vendor's website, follow the manufacturer's instructions to apply the update, and verify that the update resolves the vulnerability.
Comparison with Other Options:

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

NEW QUESTION: 25
Which of the following actions should be taken as part of the first step of the troubleshooting methodology?
A. Conduct tests to verify ideas
B. Handle multiple problems individually
C. Use a top-down approach
D. Create a theory about the possible root cause
Answer: (SHOW ANSWER)

NEW QUESTION: 26
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: 27
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: D (LEAVE A REPLY)
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: 28
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: 29
During a VoIP call, a user notices inconsistent audio and logs an incident ticket. A network administrator notices inconsistent delays in arrival of the RTP packets. Which of the following troubleshooting tools should the network administrator use to determine the issue?
A. Toner and probe
B. Protocol analyzer

C. Cable tester
D. Spectrum reader
Answer: (SHOW ANSWER)
Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.
A). Toner and probe locates cable runs, not packet analysis.
C). Cable tester checks wiring faults, not packet timing.
D). Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Protocol analyzers, VoIP troubleshooting, jitter analysis.

NEW QUESTION: 30
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: 31
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: 32
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: 33
Which of the following technologies is most appropriate for a business that requires high-speed access to frequently used web content, such as images and videos?
A. CDN
B. SAN
C. Firewall
D. Switch
Answer: (SHOW ANSWER)
The correct solution is a Content Delivery Network (CDN). A CDN caches web content (like images, videos, scripts) on distributed servers close to end users. This reduces latency, improves load times, and decreases the load on origin servers. For a business requiring high-speed access to media-rich content, a CDN is the most effective option.
B). SAN (Storage Area Network) is used for storage in a data center, not for distributing web content.
C). Firewall secures traffic but doesn't accelerate content delivery.
D). Switches forward packets within a LAN, not globally distribute content.
By leveraging CDNs, businesses can handle large traffic volumes efficiently while improving user experience.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - CDNs, caching, performance optimization.

NEW QUESTION: 34
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: 35
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: 36
A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?
A. Traffic analysis
B. Availability monitoring
C. Baseline metrics
D. Network discovery
Answer: (SHOW ANSWER)
Traffic analysis involves monitoring and inspecting network traffic flows to detect unusual patterns, such as a workstation sending large volumes of outbound SMTP (spam). This process enables identification of malware as the root cause.
B). Availability monitoring checks uptime but doesn't diagnose spam traffic.
C). Baseline metrics show normal usage but don't pinpoint infected hosts.
D). Network discovery identifies devices, not malicious traffic flows.
References (CompTIA Network+ N10-009):
Domain: Network Security - Traffic analysis, malware detection, identifying compromised hosts.

NEW QUESTION: 37
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?
A. Reverse the fibers.
B. Reterminate the fibers.
C. Verify the fiber size.
D. Examine the cable runs for visual faults.
Answer: (SHOW ANSWER)
When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.References:CompTIA Network+ study materials.

NEW QUESTION: 38
A network engineer discovers network traffic that is sending confidential information to an unauthorized and unknown destination. Which of the following best describes the cause of this network traffic?
A. Adware
B. Ransomware
C. Darkware
D. Malware
Answer: (SHOW ANSWER)

Malware refers to any malicious software that can exfiltrate confidential data, including spyware, trojans, and rootkits. This fits the scenario where unauthorized data transfer is occurring.
Breakdown of Options:
A). Adware - Displays ads, does not typically steal data.
B). Ransomware - Encrypts files but does not exfiltrate data.
C). Darkware - Not a real cybersecurity term.
D). Malware - Correct answer. Malicious software is responsible for unauthorized data exfiltration.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Given a scenario, implement cybersecurity measures.
NIST 800-83: Malware Incident Prevention & Handling

NEW QUESTION: 39
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: 40
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: 41
Which of the following is the most likely benefit of installing server equipment in a rack?
A. Simplified troubleshooting process
B. Decreased power consumption
C. Improved network performance
D. Increased compute density
Answer: (SHOW ANSWER)
Installing server equipment in a rack increases compute density by allowing multiple servers to be organized efficiently in a vertical configuration, saving space while housing more devices in a smaller footprint. This is critical for data centers and businesses with high hardware demands.
Simplified troubleshooting process (A): While racks can aid in organizing equipment, this is a secondary benefit, not the primary purpose.
Decreased power consumption (B): Rack installation does not directly reduce power usage; equipment power consumption remains the same.
Improved network performance (C): Racking servers does not inherently improve network performance; that depends on network configurations.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Rack Installations).

NEW QUESTION: 42
A network administrator is unable to ping a remote server from a newly connected workstation that has been added to the network. Ping to 127.0.0.1 on the workstation is failing. Which of the following should the administrator perform to diagnose the problem?
A. Verify the NIC interface status.
B. Verify the network is not congested.
C. Verify the router is not dropping packets.
D. Verify that DNS is resolving correctly.
Answer: A (LEAVE A REPLY)
The failure of a ping to 127.0.0.1 (the loopback address) indicates a problem with the workstation's TCP/IP stack or network interface card (NIC). Since 127.0.0.1 is a local address, the issue is not related to the network, router, or DNS. The first step in diagnosing this issue is to verify the NIC interface status to ensure the network adapter is functioning and properly configured.
Why not Verify the network is not congested? Network congestion affects external connectivity, not the loopback address.
Why not Verify the router is not dropping packets? Router issues are irrelevant since the loopback ping fails locally.
Why not Verify that DNS is resolving correctly? DNS resolution is not involved in pinging 127.0.0.1, which uses a direct IP address.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) emphasizes that a failed loopback ping indicates a local TCP/IP stack or NIC issue, and checking the NIC status is the first diagnostic step.

NEW QUESTION: 43
A network architect is implementing an off-premises computing facility and needs to ensure that operations will not be impacted by major outages. Which of the following should the architect consider?
A. Hot site
B. DCI
C. Direct Connect
D. Active-passive approach
Answer: (SHOW ANSWER)
Ahot siteis a fully operational backup facility with hardware, network, and data synchronization already in place. It allows forimmediate failoverin the event of a disaster, minimizing downtime.
* B. DCI (Data Center Interconnect)connects data centers but doesn't guarantee availability unless built redundantly.
* C. Direct Connectrefers to a private link to cloud providers, not disaster recovery.
* D. Active-passivecan help with failover but may involve delay unless combined with hot site principles.

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

NEW QUESTION: 44
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: 45
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: 46
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: 47
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: 48
Which of the following is the most cost-efficient way to host email services?
A. PaaS
B. IaaS
C. VPC
D. SaaS
Answer: (SHOW ANSWER)
The correct answer is SaaS (Software as a Service). According to the CompTIA Network+ N10-009 objectives, SaaS is the most cost-efficient cloud model for hosting common business applications such as email, collaboration tools, and productivity suites. With SaaS, the cloud provider manages all infrastructure, operating systems, application software, security updates, and maintenance, significantly reducing administrative overhead and operational costs.
Email services are a prime example of workloads that benefit from SaaS solutions such as Microsoft 365 or Google Workspace. Organizations pay a subscription-based fee, typically per user, and avoid expenses related to server hardware, licensing, patching, backups, redundancy, and disaster recovery. This makes SaaS far more economical than deploying and maintaining email servers internally or in lower-level cloud models.
IaaS requires the organization to manage virtual machines, operating systems, email server software, and security configurations, which increases both cost and complexity. PaaS simplifies application development but is not designed for hosting ready-made services like email platforms. A VPC (Virtual Private Cloud) is a networking construct, not a service model, and does not inherently provide email hosting functionality.
The Network+ objectives emphasize selecting cloud service models based on cost, management responsibility, and operational efficiency. For standardized services like email, SaaS offers the lowest total cost of ownership and the least administrative burden, making it the best and most cost-effective choice.

NEW QUESTION: 49
A wireless technician wants to implement a technology that will allow user devices to automatically navigate to the best available frequency standard. Which of the following technologies should the technician use?
A. Band steering
B. Wireless LAN controller
C. Directional antenna
D. Autonomous access point
Answer: (SHOW ANSWER)
Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band.
Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.
Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.
Autonomous access point (D): This operates independently but lacks advanced features like band steering.
Reference: CompTIA Network+ Official Study Guide, Domain 1.6 (Wireless Standards and Technologies).

NEW QUESTION: 50
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: 51
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: 52
A network administrator upgrades the wireless access points and wants to implement a configuration that gives users higher speed and less channel overlap based on device compatibility. Which of the following accomplishes this goal?
A. 802.1X
B. MIMO
C. ESSID
D. Band steering
Answer: (SHOW ANSWER)
The best solution here is band steering. Band steering allows modern wireless access points to automatically direct dual-band capable clients toward the 5 GHz band instead of the crowded 2.4 GHz band. The 5 GHz band has more available non-overlapping channels and can provide faster speeds with less interference, especially in dense environments. Devices that only support 2.4 GHz will remain on that band, while compatible devices enjoy the improved performance of 5 GHz.
A). 802.1X is a port-based network access control method for authentication. While important for security, it does not affect wireless channel utilization or client throughput.
B). MIMO (Multiple Input, Multiple Output) is a technology that improves throughput by using multiple antennas to send/receive simultaneously, but it does not actively steer clients between frequency bands.
C). ESSID (Extended Service Set Identifier) is just the network name for a set of APs in the same WLAN; it has no role in optimizing performance by band.

By implementing band steering, administrators reduce channel overlap on the 2.4 GHz band, improve spectral efficiency, and provide higher performance to capable devices, directly meeting the requirements described in the scenario.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Wireless optimization, band steering, dual-band client management.

NEW QUESTION: 53
A small business is choosing between static and dynamic routing for its network. Which of the following is the best reason to use dynamic routing in a growing network?
A. Easier to configure compared to using manually entered routes
B. Does not require additional network security controls
C. Features enhanced network monitoring and visibility
D. Includes automatic changes and updates in network topology
Answer: (SHOW ANSWER)
Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.
Option A can be partly true in large environments, but the core "best reason" emphasized for dynamic routing is the automatic adaptation to topology changes. Option B is incorrect-dynamic routing may introduce additional security considerations (route filtering, authentication, neighbor control). Option C is not a defining advantage; monitoring visibility depends on tools/telemetry rather than routing type. Therefore, the strongest and most correct reason is automatic changes and updates in network topology.

NEW QUESTION: 54
A user cannot access an external server for a client after connecting to a VPN. Which of the following commands would a support agent most likely use to examine the issue? (Select two).
A. nslookup
B. tcpdump
C. arp
D. dig
E. tracert
F. route print
Answer: (SHOW ANSWER)
When a user connects to a VPN and experiences connectivity issues to an external server, the problem is often related to routing or network path issues.
E). tracert:
Traces the path packets take from the user's device to the destination server.
Helps determine if the traffic is being blocked or misrouted.
F). route print:
Displays the device's routing table.
Helps diagnose whether traffic is being sent to the VPN tunnel instead of the correct external server.
Incorrect Options:
A). nslookup: Used for resolving domain names to IPs (DNS troubleshooting), but this issue is likely routing- related.
B). tcpdump: Captures packets for deep packet analysis, not typically the first step in diagnosing a VPN- related access issue.
C). arp: Used for resolving local network MAC addresses, not relevant for external VPN issues.
D). dig: Like nslookup, used for DNS queries, but not useful for routing problems.

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

NEW QUESTION: 55
In an environment with one router, which of the following will allow a network engineer to communicate between VLANs without purchasing additional hardware?
A. Subinterfaces
B. VXLAN
C. Layer 3 switch
D. VIR
Answer: (SHOW ANSWER)
A subinterface is a logical interface created on a single physical router interface that allows routing between VLANs (known as Router-on-a-Stick (ROAS)). This method is commonly used when only one physical router is available, allowing inter-VLAN communication without additional hardware.
*Why not the other options?
*VXLAN (B) - This is used for extending Layer 2 networks over a Layer 3 infrastructure, primarily in data centers. It does not directly enable inter-VLAN communication.
*Layer 3 switch (C) - A Layer 3 switch can route between VLANs, but the scenario states that purchasing additional hardware is not an option.
*VIR (D) - This is not a standard networking term in the context of VLAN communication.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 8: VLANs and Inter-VLAN Routing

NEW QUESTION: 56
A network engineer queries a hostname using dig, and a valid IP address is returned. However, when the engineer queries that same IP address using dig, no hostname is returned. Which of the following DNS records is missing?
A. MX
B. CNAME
C. AAAA
D. PTR
Answer: (SHOW ANSWER)
This scenario describes a successful forward DNS lookup (hostname # IP address) but a failed reverse DNS lookup (IP address # hostname). Reverse lookups rely on a PTR (Pointer) record, which is stored in a reverse lookup zone (in-addr.arpa for IPv4, ip6.arpa for IPv6). If the engineer can resolve the hostname to an IP, that indicates an A record (or possibly AAAA for IPv6) exists and is functioning. But when querying the IP directly and receiving no hostname, the most likely issue is that the reverse mapping is not configured- meaning the PTR record is missing.
An MX record is used for mail exchange routing, not hostname resolution. A CNAME provides an alias from one hostname to another and does not create reverse mappings. An AAAA record maps a hostname to an IPv6 address; it is not used for reverse lookups of an IP to a name. Network+ objectives emphasize understanding common DNS record types and the difference between forward and reverse resolution, making PTR the correct missing record here.

NEW QUESTION: 57
Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:
1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 '

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

NEW QUESTION: 58
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: 59
Which of the following would describe a data recovery goal?
A. MTBF
B. RPO

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

NEW QUESTION: 60
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: 61
Which of the following attacks forces a switch to send all traffic out of all ports?
A. ARP poisoning
B. Evil twin
C. MAC flooding
D. DNS spoofing
Answer: (SHOW ANSWER)
MAC flooding overwhelms a switch's CAM (Content Addressable Memory) table by sending a flood of frames with spoofed MAC addresses. Once the CAM table overflows, the switch cannot learn legitimate MAC addresses and defaults to flooding all frames out all ports, effectively turning it into a hub. This allows an attacker to capture traffic not originally destined for their port.
A). ARP poisoning corrupts ARP tables to redirect traffic but does not overflow the CAM table.
B). Evil twin is a wireless rogue AP attack, unrelated to switch behavior.
D). DNS spoofing redirects domain queries, not Layer 2 switching.
References (CompTIA Network+ N10-009):
Domain: Network Security - Switch security, CAM table attacks, MAC flooding.

NEW QUESTION: 62
Two companies successfully merged. Following the merger, a network administrator identified a connection bottleneck. The newly formed company plans to acquire a high-end 40GB switch and redesign the network from a three-tier model to a collapsed core. Which of the following should the administrator do until the new devices are acquired?
A. Implement the FHRP.
B. Configure a route selection metric change.
C. Install a load balancer.
D. Enable link aggregation.
Answer: (SHOW ANSWER)
*The issue described is a network bottleneck due to increased traffic after a merger.
*A collapsed core architecture consolidates the core and distribution layers into a single layer to improve efficiency and reduce latency.
*Until the 40GB switch is acquired, Link Aggregation (LAG) (IEEE 802.3ad / LACP) can be used to combine multiple physical links into a single logical link, increasing bandwidth and reducing bottlenecks.
*FHRP (First Hop Redundancy Protocol) (A) is used for gateway redundancy, not link aggregation.
*Route selection metric changes (B) help with routing decisions but don't address physical link congestion.
*Load balancers (C) distribute traffic for applications, not network links.
#Reference: CompTIA Network+ N10-009 Official Documentation - Network Architecture and Performance Optimization.

NEW QUESTION: 63
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: 64

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

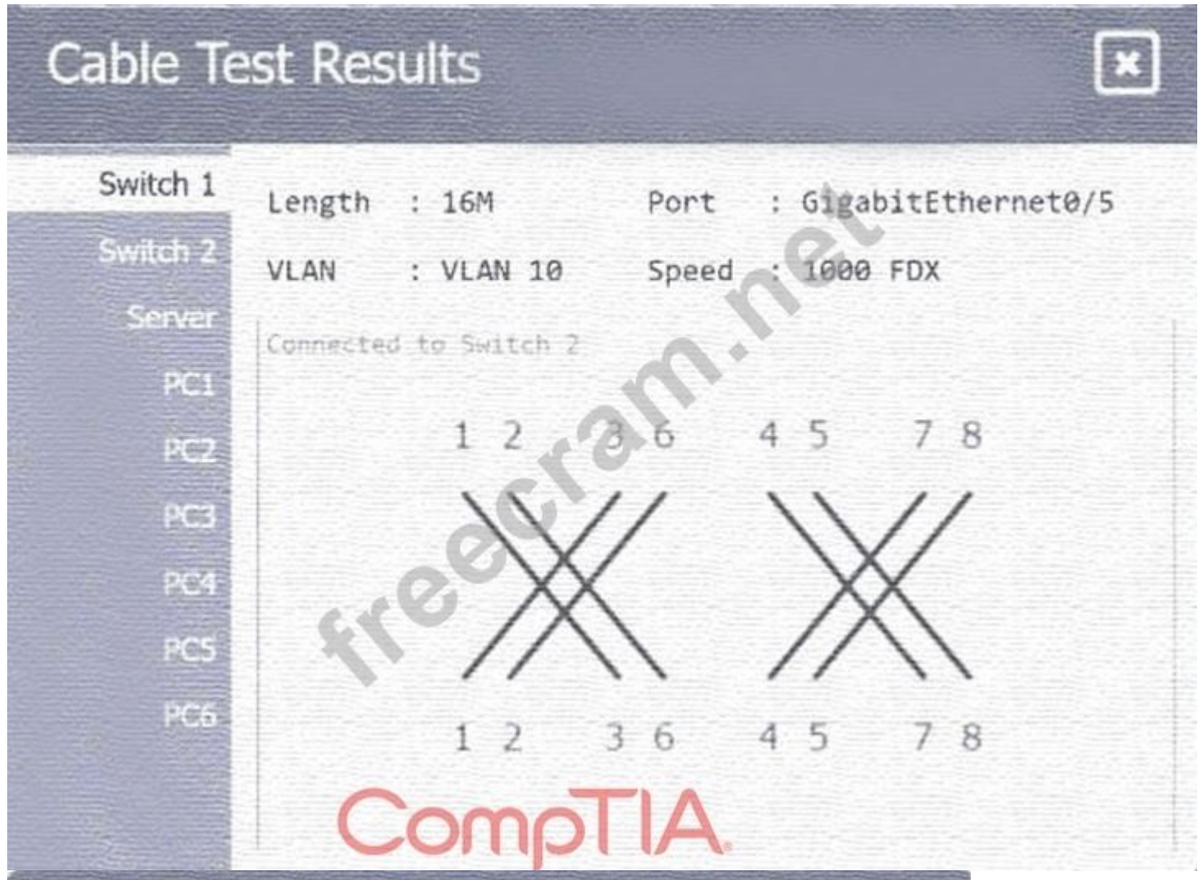
NEW QUESTION: 65
A network engineer configures an application server so that it automatically adjusts resource allocation as demand changes. This server will host a new application and demand is not predictable.
Which of the following concepts does this scenario demonstrate?
A. Scalability
B. Software as a Service
C. Hybrid cloud
D. Elasticity
Answer: D (LEAVE A REPLY)
Elasticity is the ability of a system (often in cloud environments) to automatically scale resources up or down in real time based on demand.
A). Scalability means the ability to grow over time but not necessarily dynamically.
B). SaaS is a service model, not a resource-allocation concept.
C). Hybrid cloud is a deployment model, not a performance behavior.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing, elasticity vs. scalability.

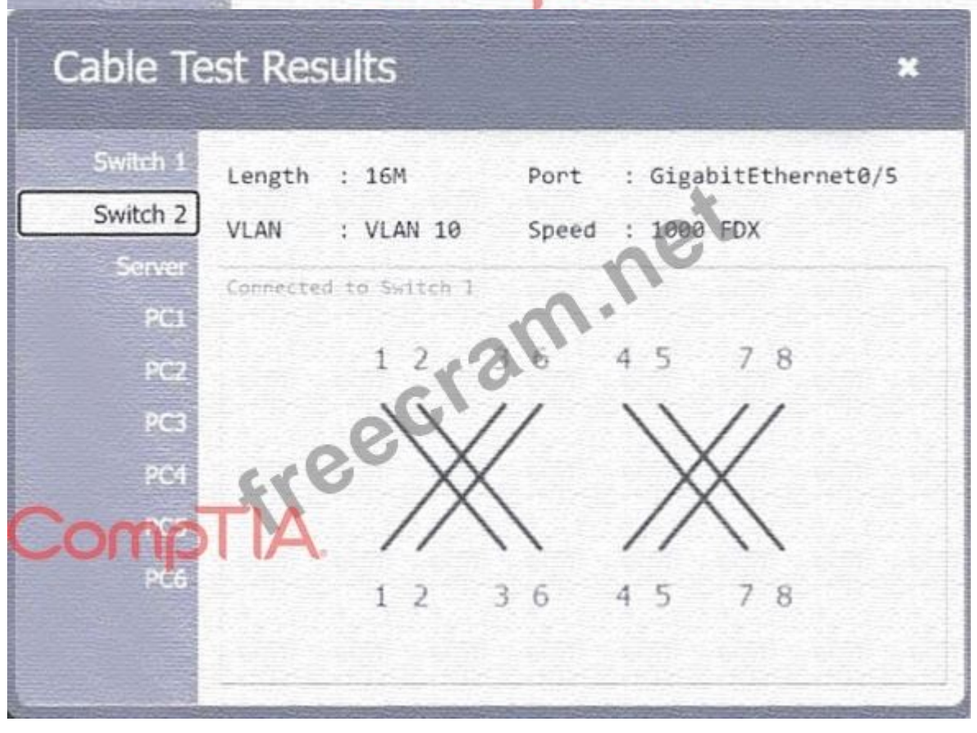
NEW QUESTION: 66
A network administrator installed a new VLAN to the network after a company added an additional floor to the office. Users are unable to obtain an IP address on the new VLAN, but ports on existing VLANs are working properly. Which of the following configurations should the administrator 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.

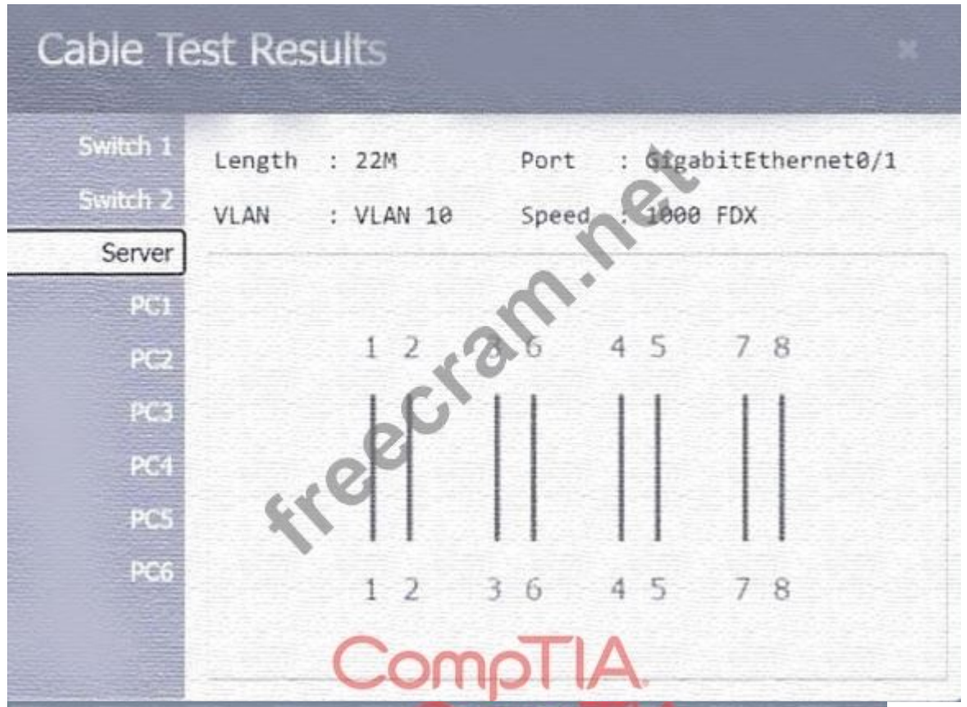
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain IP addressing technologies and subnetting.
RFC 1542: BOOTP (Bootstrap Protocol) relay agents

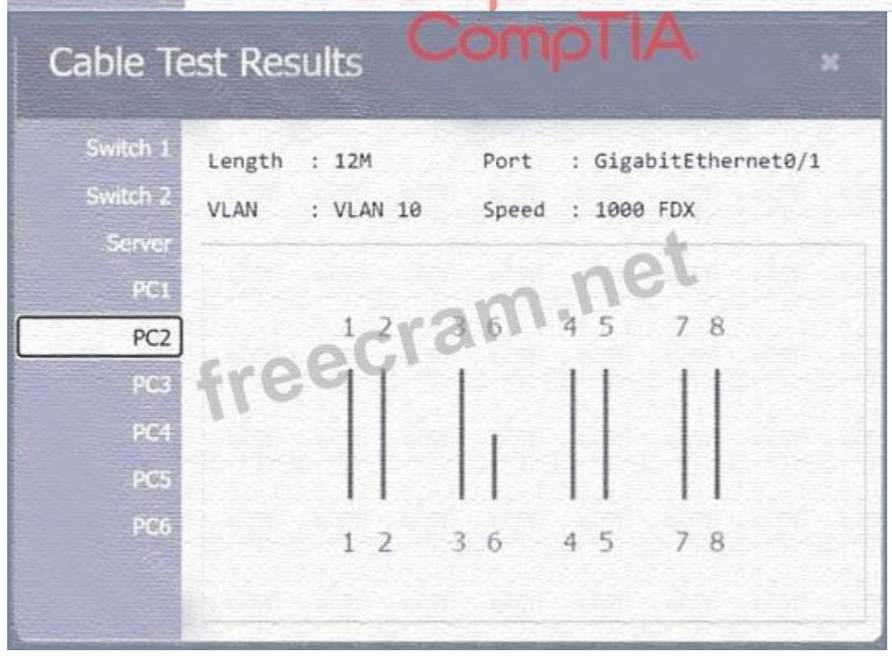
NEW QUESTION: 67
Which of the following involves an attacker traversing from one part of a network to another part that should be inaccessible?
A. MAC flooding
B. DNS poisoning
C. VLAN hopping
D. ARP spoofing
Answer: C (LEAVE A REPLY)
VLAN hopping allows an attacker to send traffic into another VLAN 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.

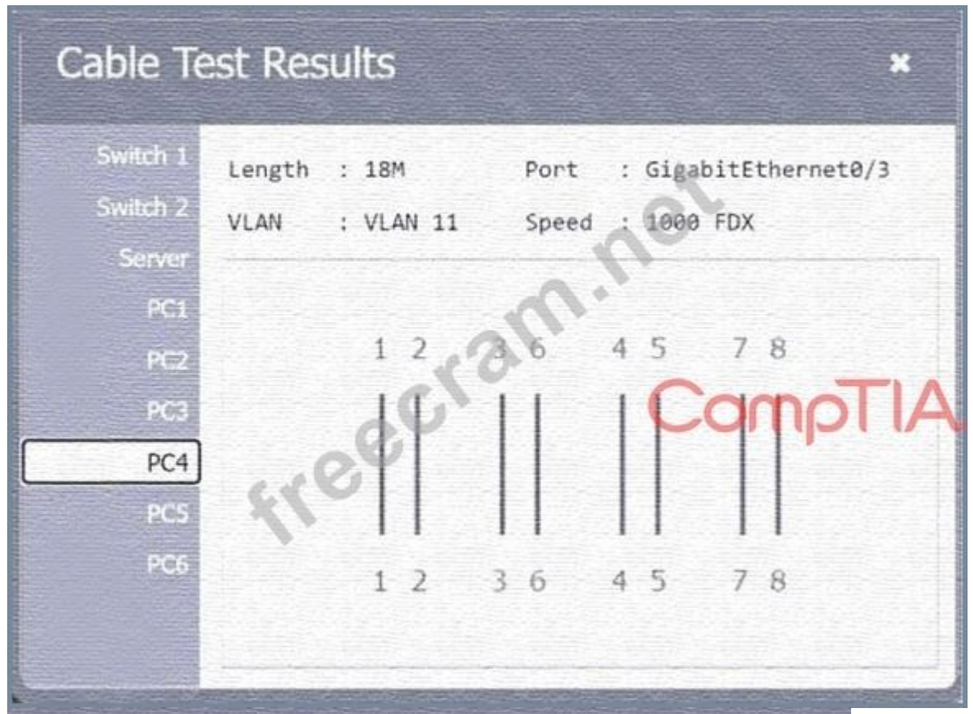
NEW QUESTION: 68
A network technician needs to resolve some issues with a customer's SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.
INSTRUCTIONS
Troubleshoot all the network components.
Review the cable test results 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.

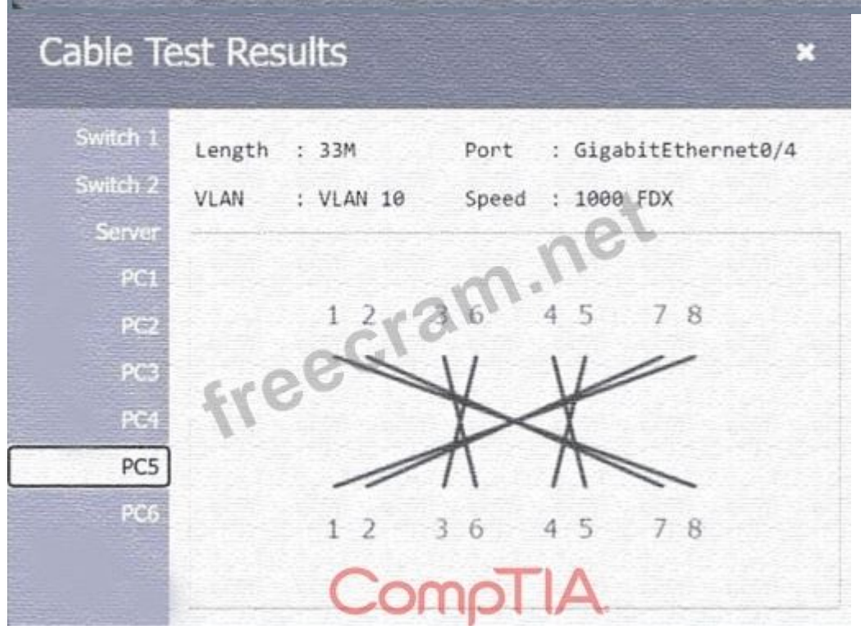


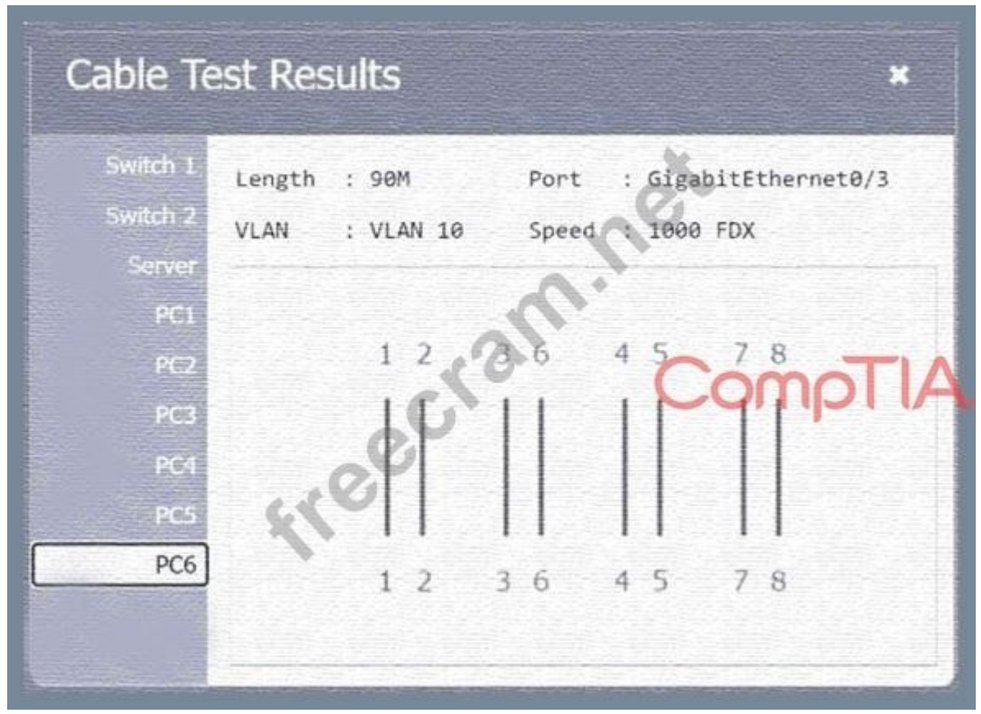







Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 18M
Port : GigabitEthernet0/3
VLAN : VLAN 11
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8
freecram.net
CompTIA


Cable Test Results
Switch 1
Switch 2
Server
PC1
PC2
PC3
PC4
PC5
PC6
Length : 33M
Port : GigabitEthernet0/4
VLAN : VLAN 10
Speed : 1000 FDX
1 2 3 6 4 5 7 8
1 2 3 6 4 5 7 8
freecram.net
CompTIA

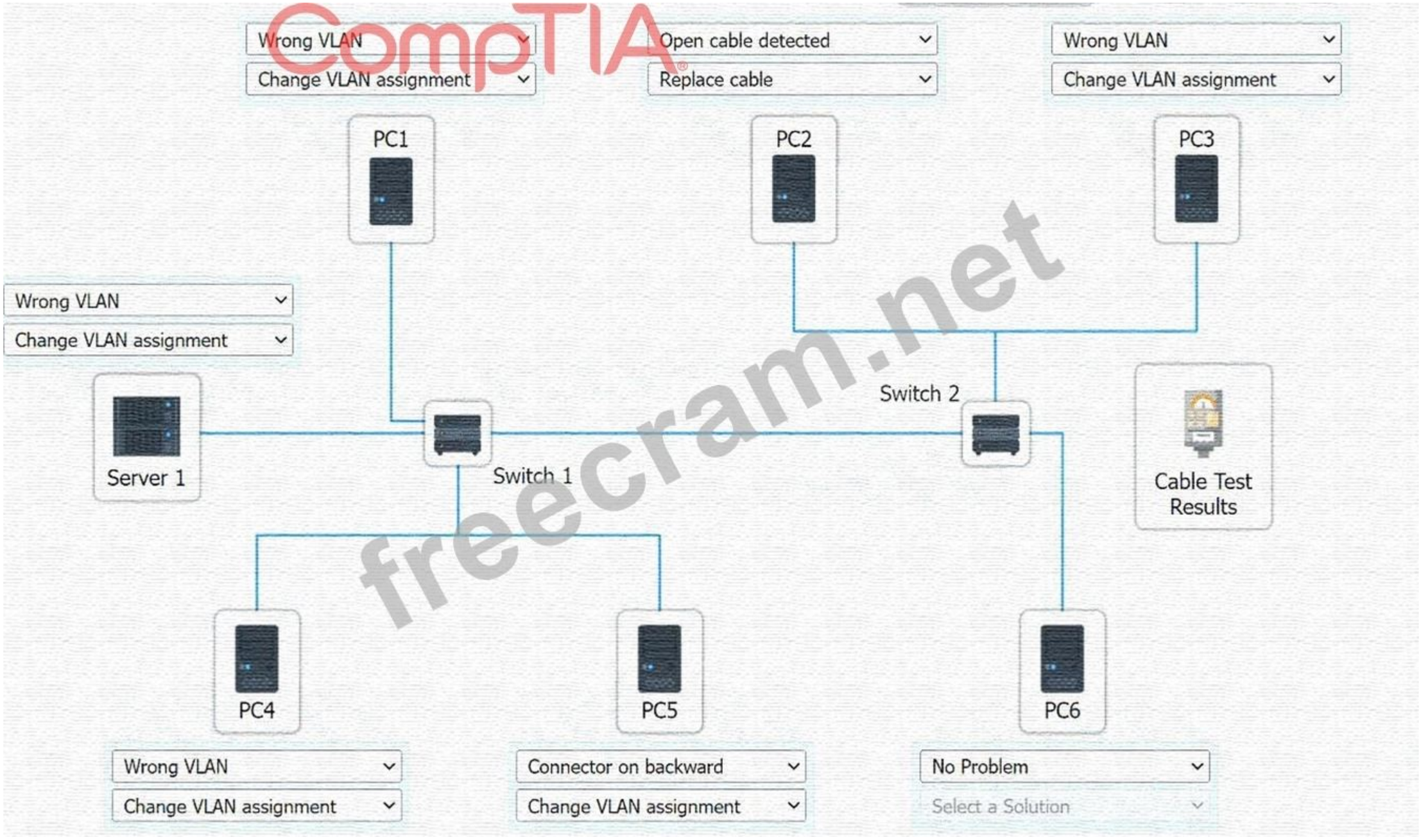


Answer:

See the answer and solution below:

Explanation:

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



NEW QUESTION: 69
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: 70

A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which of the following describes the type of traffic flow the administrator is analyzing?

A. East-west

B. Point-to-point

C. Horizontal-scaling

D. Hub-and-spoke

Answer: (SHOW ANSWER)

When traffic moves laterally between VMs within the same network or subnet, it is known as east-west traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.

Breakdown of Options:

A). East-west - Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.

B). Point-to-point - Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.

C). Horizontal-scaling - This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.

D). Hub-and-spoke - This network topology describes a centralized design, not lateral traffic.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Analyze traffic patterns and behavior.

NIST SP 800-207: Zero Trust Architecture (ZTA) - East-West traffic monitoring

NEW QUESTION: 71

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: 72
Which of the following should a company implement in order to share a single IP address among all the employees in the office?
A. STP
B. BGP
C. PAT
D. VXLAN
Answer: (SHOW ANSWER)
PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:
"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

NEW QUESTION: 73
A company is concerned that the public can use network wall jacks in publicly available conference rooms to access company servers. Which of the following is the best way to mitigate the vulnerability?
A. Create a trusted zone.
B. Disable unused services.
C. Use MAC filtering.
D. Implement 802.1X.
Answer: D (LEAVE A REPLY)
The best mitigation is implementing 802.1X, which provides port-based Network Access Control (NAC).
With 802.1X enabled on access switch ports, a device plugged into a wall jack cannot gain normal network access until it successfully authenticates using credentials/certificates via an authentication server (commonly RADIUS). This directly addresses the threat of unauthorized users plugging into publicly accessible conference room jacks, because the switch keeps the port in an unauthenticated state (or places it into a restricted/guest VLAN) until authentication succeeds. This aligns with Network+ security objectives that emphasize controlling access at the edge, enforcing authentication, and reducing the risk of rogue or unmanaged devices on internal networks.
MAC filtering is weaker because MAC addresses can be spoofed and managing allow-lists at scale is error- prone. Creating a trusted zone is vague and does not prevent initial port access; segmentation helps limit blast radius but doesn't enforce authentication at the jack. Disabling unused services is a general hardening practice, but it does not stop someone from connecting physically to an active switch port and attempting access. 802.1X is purpose-built for this exact scenario.

NEW QUESTION: 74
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: 75
A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on.
Which of the following should the engineer check first?
A. Ethernet cable type
B. Voltage
C. Transceiver compatibility
D. DHCP addressing
Answer: (SHOW ANSWER)
Power over Ethernet (PoE) allows devices such as cameras, access points, and VoIP phones to receive both power and data over the same Ethernet cable. If only eight out of twelve cameras turn on, the most likely issue is that the PoE switch has exceeded its power budget (total wattage capacity).
PoE Budget Limitation: PoE switches have a maximum power output, which can limit the number of devices they support simultaneously.
Voltage Check: Different PoE standards exist:
802.3af (PoE): Supplies up to 15.4W per port
802.3at (PoE+): Supplies up to 30W per port
802.3bt (PoE++): Supplies up to 60-100W per port
Power Draw Calculation: If each camera requires 15W and the switch can only provide 120W, then only 8 cameras (8 × 15W = 120W) will turn on.
Incorrect Options:
A). Ethernet Cable Type: Most PoE devices work with Cat5e and above. Cable type could be an issue, but power limitation is the more immediate concern.
C). Transceiver Compatibility: Only relevant if fiber transceivers or modules are in use, but not likely the root cause for power-related issues.
D). DHCP Addressing: DHCP issues affect network connectivity, not power delivery.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Power over Ethernet (PoE)

NEW QUESTION: 76
After a recent merger, a large number of alerts are coming in regarding extremely high utilization. Which of the following should be generated to help inform new alerting requirements?
A. SLA
B. Network diagram
C. Baseline
D. Heat map
Answer: C (LEAVE A REPLY)
A baseline establishes normal performance levels for network utilization, latency, jitter, and other metrics.
After a merger, traffic patterns change, so a new baseline is needed to recalibrate monitoring thresholds and avoid excessive false alerts.
A). SLA defines performance agreements with customers but doesn't adjust alerting.
B). Network diagrams show topology, not traffic norms.
D). Heat maps show wireless coverage, not utilization baselines.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Baselines, monitoring, alerting, performance tuning.

NEW QUESTION: 77
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: (SHOW ANSWER)
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: 78
A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?
A. EIGRP
B. OSPFv3
C. BGP4
D. iBGP
Answer: (SHOW ANSWER)
For an internal network using IPv6, the best option listed is OSPFv3, which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence.
BGP4 and iBGP are associated with BGP, primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor- neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.

NEW QUESTION: 79

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

NEW QUESTION: 80
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: 81
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: 82
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: 83
A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?
A. Jumbo frames
B. 802.1Q tagging
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.
This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.
This method ensures that traffic from different VLANs is properly separated and managed across the network.
References: CompTIA Network+ study materials.

NEW QUESTION: 84
An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?
A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller
Answer: (SHOW ANSWER)
* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.

* Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).
CompTIA Network+ materials discussing SNMP and MIB functionality.

NEW QUESTION: 85
After extremely high temperatures cause a power outage, the servers automatically shut down, even though the UPSs for the servers still have hours of battery life. Which of the following should a technician recommend?
A. Include backup power for air-conditioning units
B. Configure door locks to automatically lock during power outages
C. Increase UPS battery size
D. Add an IoT-enabled thermostat
Answer: (SHOW ANSWER)
Servers shut down due to overheating, not loss of electrical power. Although UPS units had battery life, without cooling systems (HVAC/air conditioning) running on backup power, server rooms overheated.
Backup power for air-conditioning is essential in data center design.
B). Door locks are unrelated to server shutdown.
C). Increasing UPS capacity won't help cooling.
D). IoT thermostats may monitor temperature but won't prevent overheating.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Environmental controls, power redundancy, HVAC systems.

NEW QUESTION: 86
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.
Instructions:
Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Answer:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To perform a network discovery by entering commands into the terminal, you can use the following steps:

Click on each switch to open its terminal window.

Enter the command show ip interface brief to display the IP addresses and statuses of the switch interfaces.

Enter the command show vlan brief to display the VLAN configurations and assignments of the switch interfaces.

Enter the command show cdp neighbors to display the information about the neighboring devices that are connected to the switch.

Fill in the missing information in the diagram using the drop-down menus provided.

Here is an example of how to fill in the missing information for Core Switch 1:

The IP address of Core Switch 1 is 192.168.1.1.
The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.
The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.
The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.
The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.
You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 87
Which of the following is a cost-effective advantage of a split-tunnel VPN?
A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.
Answer: (SHOW ANSWER)
A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company's VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.References:CompTIA Network+ study materials.

NEW QUESTION: 88
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: 89
After a networking intern plugged in a switch, a significant number of users in a building lost connectivity.
Which of the following is the most likely root cause?
A. VTP update
B. Port security issue

C. LLDP misconfiguration
D. Native VLAN mismatch
Answer: D (LEAVE A REPLY)
When a switch is improperly connected to a network, it can cause widespread connectivity issues, especially if there's a misconfiguration in VLAN settings. A Native VLAN mismatch occurs when two switches connected via a trunk link have different native VLANs configured for untagged traffic. This can cause traffic to be sent to the wrong VLAN or dropped, resulting in connectivity loss for users.
Scenario Analysis: The intern likely connected the switch without ensuring that the trunk port's native VLAN matched the existing network configuration. This is a common issue in Cisco-based networks when trunk links are misconfigured.
Why not VTP update? VLAN Trunking Protocol (VTP) updates propagate VLAN configurations across switches. While a VTP misconfiguration could cause issues, it's less likely to immediately disrupt connectivity for many users unless the VTP server deleted critical VLANs, which is not implied here.
Why not Port security issue? Port security restricts access based on MAC addresses, typically affecting individual ports, not causing widespread outages.
Why not LLDP misconfiguration? Link Layer Discovery Protocol (LLDP) is used for device discovery, and misconfiguration is unlikely to cause a broad loss of connectivity.
Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) discusses VLAN trunking and the importance of matching native VLANs on trunk links to prevent connectivity issues. Native VLAN mismatches are highlighted as a common cause of network disruptions.

NEW QUESTION: 90
A network administrator wants to configure a backup route in case the primary route fails. A dynamic routing protocol is not installed on the router. Which of the following routing features should the administrator choose to accomplish this task?

A. Neighbor adjacency
B. Link state flooding
C. Administrative distance
D. Hop count
Answer: (SHOW ANSWER)
Introduction to Administrative Distance
Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.
Static Routes and Backup Routes
When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.
Configuring Static Routes with Administrative Distance
The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.
Example Configuration:
plaintext
Copy code
ip route 192.168.1.0 255.255.255.0 10.0.0.1 1
ip route 192.168.1.0 255.255.255.0 10.0.0.2 10
In the above example, 192.168.1.0/24 is the destination network.
10.0.0.1 is the next-hop IP address for the primary route with an AD of 1.
10.0.0.2 is the next-hop IP address for the backup route with an AD of 10.

Verification:
After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.
References:
CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page #Ref9 Basic Configuration Commands).

NEW QUESTION: 91
A network administrator deployed wireless networking in the office area. When users visit the outdoor patio and try to download emails with large attachments or stream training videos, they notice buffering issues.
Which of the following is the most likely cause?
A. Network congestion
B. Wireless interference
C. Signal degradation
D. Client disassociation
Answer: (SHOW ANSWER)
The most likely cause of buffering issues when moving outdoors is signal degradation. Wireless signals weaken as they travel through obstacles such as walls, glass, and air, leading to weaker connections and reduced data rates.
Breakdown of Options:
A). Network congestion - While congestion can slow down network speeds, it affects all users, not just those moving outdoors.
B). Wireless interference - Interference is possible but is more likely caused by other wireless signals rather than outdoor movement.
C). Signal degradation - Correct answer. Wireless signals weaken with distance and obstacles such as walls, reducing performance.
D). Client disassociation - Disassociation occurs when clients lose connection to the AP, but the question states that users experience buffering, indicating they are still connected but with a weak signal.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Analyze wireless networking technologies.
IEEE 802.11 standards: Wi-Fi propagation characteristics

NEW QUESTION: 92
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: 93
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: 94
A network administrator needs to monitor data from recently installed firewalls in multiple locations. Which of the following solutions would best meet the administrator's needs?
A. IDS
B. IPS
C. SIEM
D. SNMPv2
Answer: (SHOW ANSWER)
SIEM (Security Information and Event Management) systems are used to aggregate and analyze log data from various sources, including firewalls, to detect potential security incidents and assist in regulatory compliance.
The document explains:
"SIEM solutions aggregate and analyze log and event data from multiple devices, including firewalls, across different locations. They help in real-time monitoring, incident response, and ensuring compliance with security policies."

NEW QUESTION: 95
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: 96
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: 97
A network administrator needs to deploy a subnet using an IP address range that can support at least 260 devices with the fewest wasted addresses. Which of the following subnets should the administrator use?
A. 172.16.0.0/24
B. 172.25.2.0/23
C. 172.30.1.0/22
D. 172.33.0.0/21
Answer: (SHOW ANSWER)
To support at least 260 hosts, you need at least 512 total IP addresses (accounting for network/broadcast overhead).
/23 (255.255.254.0) gives 510 usable IPs, ideal for 260 devices with minimal waste.
/24 (255.255.255.0) gives only 254 usable - not enough.
/22 (1022 usable) and /21 (2046 usable) would work but result in significant address waste.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.1 - Given a scenario, configure and apply IP addressing schemes.

NEW QUESTION: 98
A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).

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

NEW QUESTION: 99
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: 100

Which of the following standards enables the use of an enterprise authentication for network access control?

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

NEW QUESTION: 101
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. tracert
B. arp
C. ipconfig
D. nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 102
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: 103
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: 104
Which of the following ports creates a secure connection to a directory service?
A. 22
B. 389
C. 445
D. 636
Answer: D (LEAVE A REPLY)
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: 105
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: 106
After changes were made to a firewall, users are no longer able to access a web server. A network administrator wants to ensure that ports 80 and 443 on the web server are still accessible from the user IP space. Which of the following commands is best suited to perfom this testing?
A. Dig
B. Ping
C. nmap
D. Ifconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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: 108
Which of the following is most closely associated with having a leased line to a public cloud provider?
A. VPN
B. Direct Connect
C. Internet gateway
D. Private cloud
Answer: (SHOW ANSWER)
Direct Connect is the option most closely associated with having a leased line to a public cloud provider, as defined in the CompTIA Network+ N10-009 objectives under cloud connectivity and WAN technologies.
Direct Connect (or equivalent services such as Azure ExpressRoute or Google Cloud Interconnect) provides a dedicated, private physical connection between an organization's on-premises network and a public cloud provider's infrastructure. This connection bypasses the public internet, offering consistent bandwidth, lower latency, improved performance, and enhanced security.
A VPN uses encrypted tunnels over the public internet, which does not qualify as a leased line and is subject to internet congestion and variable performance. An internet gateway simply allows cloud resources to communicate with the public internet and does not imply a private or dedicated connection. A private cloud refers to a deployment model where cloud resources are dedicated to a single organization; it does not describe the connectivity method or the use of a leased circuit.
According to Network+ objectives, leased-line connectivity to cloud providers is commonly used by enterprises that require high availability, predictable throughput, regulatory compliance, or secure hybrid cloud architectures. Direct Connect is a foundational component of hybrid networking strategies, linking on- premises environments directly to public cloud services using provider-managed circuits.

NEW QUESTION: 109
A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the following spanning tree information from both switches:
Switch 1
Port State Cost
1 Forward 2
2 Forward 2
Switch 2
Port State Cost
1 Forward 2
2 Forward 2
Which of the following best describes the issue?
A. The port cost should not be equal.

B. The ports should use link aggregation.
C. A root bridge needs to be identified.
D. The switch should be configured for RSTP.
Answer: (SHOW ANSWER)
The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

NEW QUESTION: 110
A Chief Executive Officer (CEO) of a company purchases a new phone that will be used while traveling to different countries. The CEO needs to be able to place outgoing calls and receive incoming calls on the phone using a SIM card. Which of the following cellular technologies does the CEO's phone need?

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

NEW QUESTION: 111
A network administrator is troubleshooting issues with a DHCP server at a university. More students have recently arrived on campus, and the users are unable to obtain an IP address. Which of the following should the administrator do to address the issue?
A. Enable IP helper.
B. Change the subnet mask.
C. Increase the scope size.
D. Add address exclusions.
Answer: (SHOW ANSWER)
The issue is that more students have arrived on campus, meaning the available IP addresses are exhausted. To fix this, the administrator should increase the DHCP scope size to allow more devices to obtain IP addresses.
Breakdown of Options:
A). Enable IP helper - IP helper is used to forward DHCP requests across different subnets. However, the problem here is that the DHCP scope is full, not that requests are not reaching the server.
B). Change the subnet mask - The subnet mask determines the number of available hosts, but changing it without increasing the IP pool does not help.
C). Increase the scope size - Correct answer. Expanding the DHCP scope provides more IP addresses for assignment.
D). Add address exclusions - Exclusions reserve IP addresses, which would further reduce available addresses instead of solving the issue.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Compare and contrast IP addressing schemes.
RFC 2131: Dynamic Host Configuration Protocol (DHCP)

NEW QUESTION: 112

A network technician sets up a computer on the accounting department floor for a user from the marketing department. The user reports that they cannot access the marketing department's shared drives but can access the internet. Which of the following is the most likely cause of this issue?

A. Mismatched switchport duplex

B. Misconfigured gateway settings

C. Incorrect VLAN assignment

D. SVI is assigned to the wrong IP address

Answer: (SHOW ANSWER)

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

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

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

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

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

NEW QUESTION: 113

Which of the following types of attacks is most likely to occur after an attacker sets up an evil twin?

A. On-path

B. DDoS

C. ARP spoofing

D. Phishing

Answer: (SHOW ANSWER)

Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

An evil twin is a malicious wireless access point that impersonates a legitimate SSID. Once victims connect, the attacker can intercept and manipulate traffic, performing an on-path (man-in-the-middle) attack- capturing credentials, injecting content, or downgrading encryption.

B). DDoS overwhelms services with traffic; it's not the typical follow-on from clients joining a rogue AP.

C). ARP spoofing is another way to become on-path on wired segments, but with an evil twin, the wireless association itself enables the on-path position.

D). Phishing is social engineering; while an evil twin could be used to present fake portals, the primary technical posture after connection is on-path.

References (CompTIA Network+ N10-009):

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

NEW QUESTION: 114

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: 115
Which of the following best describes the transmission format that occurs at the transport layer over connectionless communication?
A. Datagram
B. Segment
C. Frames
D. Packets
Answer: (SHOW ANSWER)
At the transport layer, connectionless communication is typically handled using the User Datagram Protocol (UDP), which transmits data in units called datagrams. Unlike TCP, UDP does not establish a connection before sending data and does not guarantee delivery, making datagrams the correct term for the transmission format in this context. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 116
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: 117
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: 118
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: 119
A company's network is experiencing high latency and packet loss during peak hours. Network monitoring tools show increased traffic on a switch. Which of the following should a network technician implement to reduce the network congestion and improve performance?
A. Load balancing
B. Port mirroring
C. Quality of Service
D. Spanning Tree Protocol
Answer: (SHOW ANSWER)
Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.
Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.
Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.
Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.
Reference: CompTIA Network+ Official Study Guide, Domain 1.5 (Network Optimization), Domain 2.1 (Network Management).

NEW QUESTION: 120
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: 121
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: 122
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: 123
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: A (LEAVE A REPLY)
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: 124
Which of the following source control features allows an administrator to test a new configuration without changing the primary configuration?
A. Central repository
B. Conflict identification
C. Branching
D. Version control
Answer: (SHOW ANSWER)
Branchingallows developers and administrators tocreate an isolated copyof the main configuration so they can test changes independently. This avoids impacting the primary environment and allows for safer testing and development.
Reference:Section 3.5 - Network Access and Management Methods - "Source Control: Branching"

NEW QUESTION: 125
An IT department asks a newly hired employee to use a personal laptop until the company can provide one.
Which of the following policies is most applicable to this situation?
A. IAM
B. BYOD
C. DLP
D. AUP
Answer: (SHOW ANSWER)
BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network.
Since the new employee is using a personal laptop, this policy applies.
Breakdown of Options:
A). IAM (Identity and Access Management) - Governs user permissions, not device policies.
B). BYOD (Bring Your Own Device) - # Correct answer. Covers using personal devices for work.
C). DLP (Data Loss Prevention) - Focuses on preventing sensitive data leaks, not device usage policies.
D). AUP (Acceptable Use Policy) - Covers internet and system usage, but not personal device rules.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.6: Explain security policies and best practices.

NEW QUESTION: 126
A network engineer is now in charge of all SNMP management in the organization. The engineer must use a SNMP version that does not utilize plaintext data. Which of the following is the minimum version of SNMP that supports this requirement?
A. v1
B. v2c
C. v2u
D. v3
Answer: (SHOW ANSWER)
SNMPv3 is the version of the Simple Network Management Protocol that introduces security enhancements, including message integrity, authentication, and encryption. Unlike previous versions (v1 and v2c), SNMPv3 supports encrypted communication, ensuring that data is not transmitted in plaintext. This provides confidentiality and protects against eavesdropping and unauthorized access.References:CompTIA Network+ study materials.

NEW QUESTION: 127
Developers want to create a mobile application that requires a runtime environment, developer tools, and databases. The developers will not be responsible for security patches and updates. Which of the following models meets these requirements?
A. Container as a service
B. Infrastructure as a service
C. Platform as a service
D. Software as a service
Answer: (SHOW ANSWER)
The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.
A). CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.
B). IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.
D). SaaS provides end-user applications (e.g., email, CRM), not platforms for development.
By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud service models (IaaS, PaaS, SaaS, CaaS).

NEW QUESTION: 128
While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?
A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1
Answer: (SHOW ANSWER)
The loopback address 127.0.0.1 is used to test the TCP/IP stack of the local machine. Pinging this address confirms whether the local system's networking stack is functioning correctly.

NEW QUESTION: 129

A user submits an escalated ticket regarding failed logins on their laptop. The user states that the time displayed on the laptop is incorrect. An administrator thinks the issue is related to the NTP. Which of the following should the administrator do next?

A. Create a plan of action

B. Implement a solution

C. Identify the problem

D. Test the theory

Answer: (SHOW ANSWER)

The first step of troubleshooting is always to identify the problem, which includes verifying the symptoms (incorrect time), asking the user clarifying questions, and checking system logs. Only after confirming the problem can the administrator proceed to form a theory and plan.

A). Plan of action is later.

B). Implement solution comes after testing a theory.

D). Test the theory requires a defined problem first.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Troubleshooting methodology (Identify # Theory # Test # Plan # Implement # Verify # Document).

NEW QUESTION: 130

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: 131

Which of the following is the best way to securely access a network appliance from an external location?

A. RDP

B. Telnet

C. FTPS

D. SSH

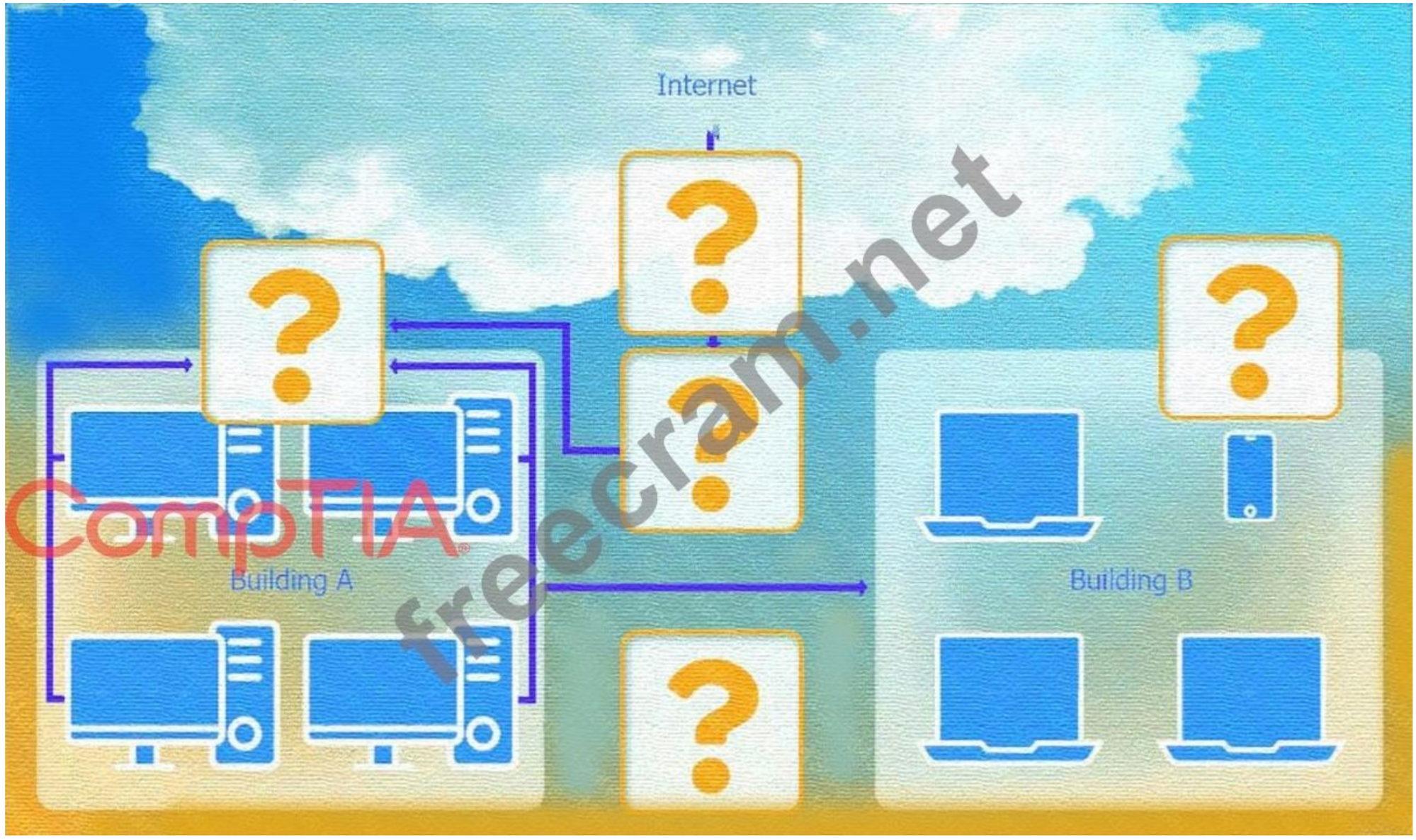
Answer: (SHOW ANSWER)
SSH (Secure Shell) is the best and most secure method for accessing a network appliance from an external location, according to the CompTIA Network+ N10-009 objectives related to secure management protocols and network security. SSH provides encrypted remote command-line access, ensuring that authentication credentials, commands, and session data are protected from interception, eavesdropping, and man-in-the- middle attacks.
Telnet is an insecure legacy protocol that transmits all data, including usernames and passwords, in cleartext, making it unsuitable for any external or untrusted network access. RDP is primarily used for graphical remote desktop access to Windows systems and is not commonly used for managing network appliances such as routers, switches, firewalls, or load balancers. Additionally, RDP introduces a larger attack surface if exposed externally. FTPS is a secure file transfer protocol and is designed for transferring files, not for interactive device management or configuration.
The Network+ N10-009 exam emphasizes the use of secure administrative access methods, and SSH is the industry-standard protocol for managing network infrastructure devices. It supports strong encryption, key- based authentication, and secure tunneling, making it ideal for remote administration over untrusted networks such as the internet.

NEW QUESTION: 132
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: 133
A group of users cannot connect to network resources. The technician runs ipconfig from one user's device and is able to ping the gateway shown from the command. Which of the following is most likely preventing the users from accessing network resources?
A. VLAN hopping
B. Rogue DHCP
C. Distributed DoS
D. Evil twin
Answer: B (LEAVE A REPLY)
A rogue DHCP server occurs when an unauthorized or misconfigured DHCP server assigns incorrect IP addresses, default gateways, or DNS settings to clients.
*In this scenario:
*The user can ping the gateway, meaning local network communication is working.
*However, they cannot access network resources, which suggests incorrect IP configuration (likely due to a rogue DHCP server assigning the wrong gateway or DNS).
*Why not the other options?
*VLAN hopping (A): This is an attack that exploits VLAN configurations to gain access to unauthorized VLANs. It would not typically cause multiple users to lose network access.
*Distributed DoS (C): A DDoS attack floods a network or service with traffic, but this issue is more likely misconfigured IP settings than an actual attack.
*Evil twin (D): This refers to a fraudulent Wi-Fi network mimicking a legitimate one. Since the users are on a wired network (ipconfig output checked), this is not applicable.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security Threats

NEW QUESTION: 134
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 beable to access the Internet.
* Security insists that all Internet trafficbe inspected before entering the network.
* Desktops should not see traffic destined for other devices.
INSTRUCTIONS
Answer:
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

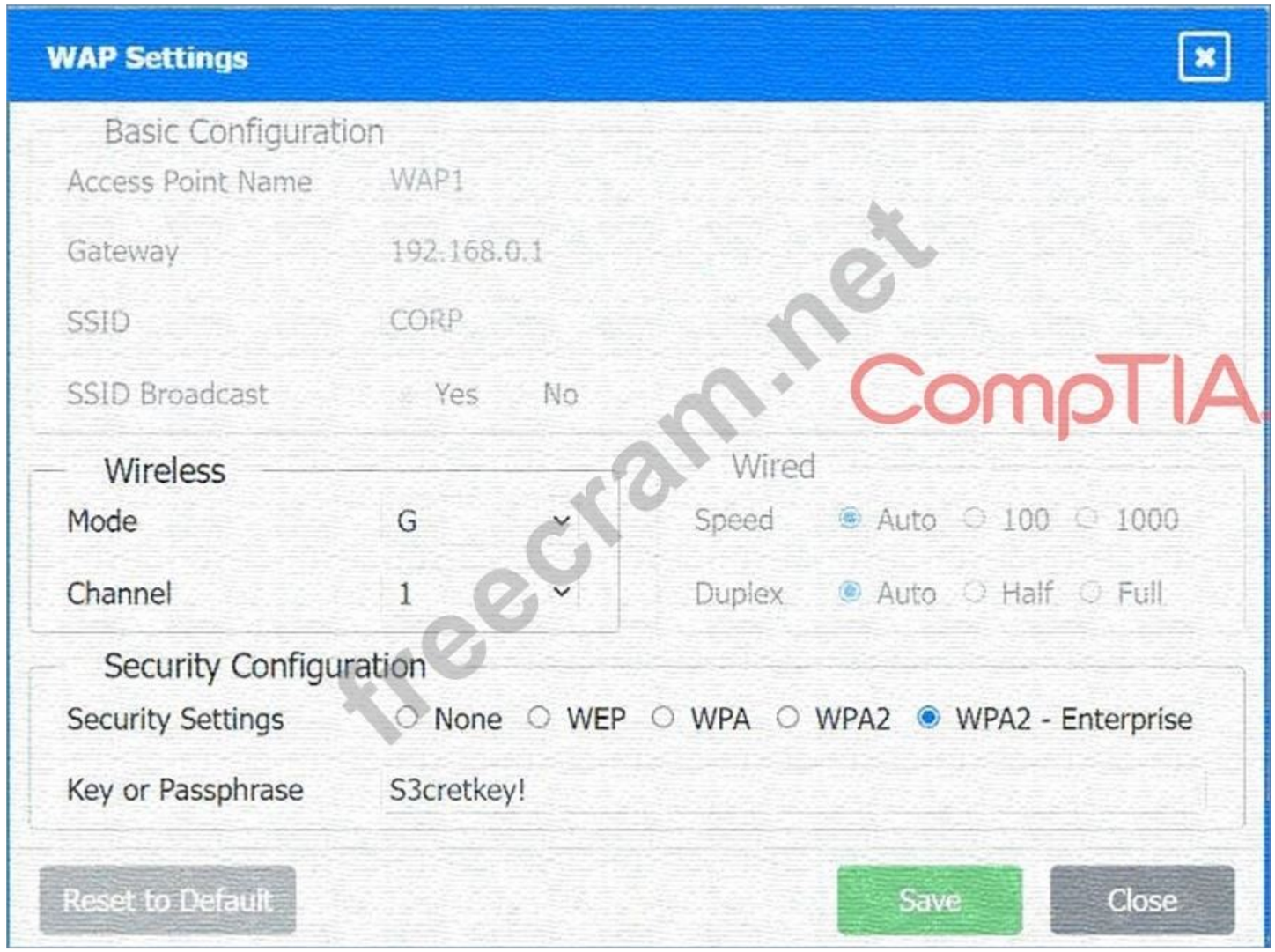
Duplex: Auto Half Full

Security Configuration

Security Settings: None WEP WPA WPA2 WPA2 - Enterprise

Key or Passphrase: N@En71$90*Ha

Reset to Default | Save | Close



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:

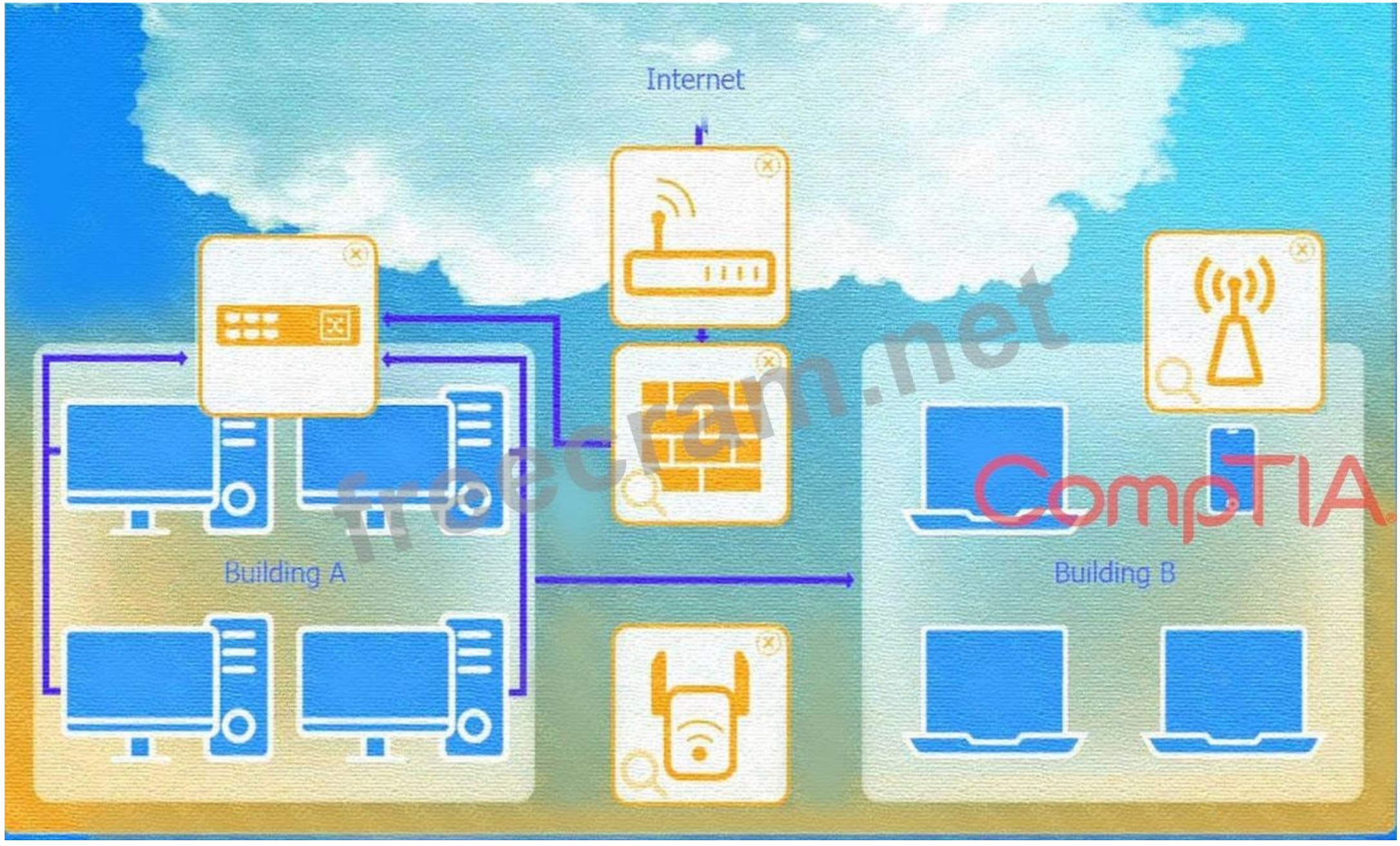
Switch: Not needed. Instead, place a Wireless Access Point (WAP) to provide wireless connectivity for laptops and mobile devices.

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: 135
A network consultant needs to decide between running an ethernet uplink or using the built-in 5GHz-to-point functionality on a WAP. Which of the following documents provides the best information to assist the consultant with this decision?
A. Service-level agreement
B. Physical diagram
C. Logical diagram
D. Site survey results
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Which of the following protocols is used to route traffic on the public internet?
A. BGP
B. OSPF
C. EIGRP
D. RIP
Answer: A (LEAVE A REPLY)
Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).
Breakdown of Options:
A). BGP - Correct answer. Used for internet routing and exchanges routing information between ISPs.
B). OSPF - An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).
C). EIGRP - Cisco's proprietary IGP, used within private networks, not the public internet.
D). RIP - An older distance-vector protocol, not scalable for the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Explain routing technologies.
RFC 4271: Border Gateway Protocol 4 (BGP-4)

NEW QUESTION: 137
A network administrator needs to connect a multimode fiber cable from the MDF to the server room. The administrator connects the cable to Switch 2, but there is no link light. The administrator tests the fiber and finds it does not have any issues. Swapping the connection to Switch 1 in a working port is successful, but the swapped connection does not work on Switch 2. Which of the following should the administrator verify next?
A. Fiber length
B. Transceiver model
C. Connector type
D. Port speed
Answer: (SHOW ANSWER)
The most probable issue is with thetransceiver model. Not all transceivers are compatible with multimode fiber, and the specific type (e.g., SFP, SFP+) and its wavelength must match the fiber cable type. If a port works on one switch but not the other with the same cable, this is a strong indicator of incompatible or faulty transceiver hardware.
Reference:Section 1.5 - Transmission Media and Transceivers - "Transceivers and Compatibility"

NEW QUESTION: 138
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: 139
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: 140

Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?

A. Site-to-site VPN
B. GRE tunnel
C. VXLAN
D. Dedicated line
Answer: (SHOW ANSWER)
A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.
Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.
Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.
Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.
Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

NEW QUESTION: 141
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: 142
While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?
A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1
Answer: (SHOW ANSWER)
The loopback address (127.0.0.1) is used to test a host's local TCP/IP stack, ensuring that the networking components of the operating system are functioning properly.
* This test does not require network connectivity because it only checks if the local machine's TCP/IP stack is operational.
* If the loopback test fails, it indicates a misconfigured TCP/IP stack, corrupt drivers, or an issue with the OS networking components.
* Option B (ping 169.254.1.1) - This is an APIPA (Automatic Private IP Addressing) address, which is assigned when DHCP fails. It does not test the local TCP/IP stack.
* Option C (ping 172.16.1.1) and Option D (ping 192.168.1.1) - These are private network addresses and test connectivity to other devices, not the local TCP/IP stack.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Network Connectivity

NEW QUESTION: 143
A network administrator wants to increase network security by preventing client devices from communicating directly with each other on the same subnet. Which of the following technologies should be implemented?
A. ACL
B. Trunking
C. Port security
D. Private VLAN
Answer: (SHOW ANSWER)
Private VLANs (PVLANs) are used to segment devices on the same subnet and switch so they cannot communicate with each other, while still accessing a shared resource like a router or gateway. This is often used in shared hosting or DMZ environments.
A). ACLs (Access Control Lists) control traffic between networks, not within the same VLAN.
B). Trunking carries multiple VLANs between switches but does not isolate devices.
C). Port security limits MAC addresses per port but doesn't isolate communication between ports.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.4 - Compare and contrast access control methods.

NEW QUESTION: 144
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: D (LEAVE A REPLY)
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: 145
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: 146
A network administrator recently updated configurations on a Layer 3 switch. Following the updates, users report being unable to reach a specific file server. Which of the following is the most likely cause?
A. Incorrect ACLs
B. Switching loop
C. Duplicate IP addresses
D. Wrong default route
Answer: (SHOW ANSWER)
*Since this issue occurred after a configuration change on a Layer 3 switch, the most likely cause is misconfigured ACLs (Access Control Lists).
*ACLs control which traffic is allowed or denied, so an incorrect ACL may be blocking access to the file server.
*Why not the other options?
*Switching loop (B): A switching loop occurs at Layer 2 (not Layer 3) and causes network-wide broadcast storms, not just loss of access to a file server.
*Duplicate IP addresses (C): This would cause connectivity issues for the devices with the conflict, but not necessarily prevent all users from accessing the file server.
*Wrong default route (D): The default route is used for traffic leaving the local network. If users are unable to access an internal file server, this is unlikely to be the issue.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 8: Network Access Control and ACLs

NEW QUESTION: 147
Which of the following connectors allows a singular QSFP transceiver to have several physical connections?
A. RJ45
B. ST
C. LC
D. MPO
Answer: (SHOW ANSWER)
The MPO (Multi-fiber Push On) connector is designed to handle multiple fiber strands in a single connector, and it is commonly used with high-density transceivers like QSFP (Quad Small Form-factor Pluggable).
QSFP can support up to four channels (hence "quad"), and MPO connectors can interface multiple fibers (e.g.,
8, 12, 24), making them ideal for 40Gbps or 100Gbps deployments.
RJ45 (A) is used for Ethernet over copper.
ST (B) and LC (C) are single-fiber connectors - they don't support the multi-fiber needs of QSFP setups.
Therefore, MPO is the correct connector type for this use case.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.1: "Compare and contrast different types of connectors and transceivers."

NEW QUESTION: 148
A network manager connects two switches together and uses two connecting links. Which of the following configurations will prevent Layer 2 loops?
A. 802.1Q tagging
B. Full duplex
C. Link aggregation
D. QoS
Answer: (SHOW ANSWER)
Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).
From Andrew Ramdayal's guide:
"Link aggregation allows you to combine multiple network connections to increase the bandwidth and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

NEW QUESTION: 149
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?
A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator
Answer: (SHOW ANSWER)
A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.
* Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.

* Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.
* Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Details tools used for cable identification and troubleshooting.
* Cisco Networking Academy: Provides training on using toner probes and other cable testing tools.
* Network+ Certification All-in-One Exam Guide: Explains the use of different tools for network cable identification and management.

NEW QUESTION: 150

Which of the following connection methods allows a network engineer to automate the configuration deployment for network devices across the environment?

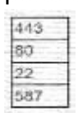
A. RDP
B. Telnet
C. GUI
D. API
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to 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: 151
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: C (LEAVE A REPLY)
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: 152
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: 153
Which of the following should a network administrator configure when adding OT devices to an organization's architecture?
A. Honeynet
B. Data-at-rest encryption
C. Time-based authentication
D. Network segmentation
Answer: (SHOW ANSWER)
Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.References:CompTIA Network+ study materials.

NEW QUESTION: 154
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:



Which of the following ports should be disabled?
A. 22
B. 80
C. 443
D. 587
Answer: (SHOW ANSWER)
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.

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

NEW QUESTION: 155
Which of the following is most commonly associated with many systems sharing one IP address in the public IP-addressing space?
A. PAT
B. NAT
C. VIP
D. NAT64
Answer: (SHOW ANSWER)
Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used in environments where many systems need internet access but there are limited public IP addresses.

NEW QUESTION: 156
A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?
A. GRE
B. IKE
C. ESP
D. AH
Answer: (SHOW ANSWER)
* Definition of ESP (Encapsulating Security Payload):
* ESP is a part of the IPsec protocol suite designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.
* Ensuring Confidentiality:
* Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.
* Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.
* Comparison with Other Protocols:
* GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.
* IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.
* AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.
* Implementation:
* Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.
References:
* CompTIA Network+ study materials on IPsec and secure communication protocols.

NEW QUESTION: 157
Which of the following network cables involves bouncing light off of protective cladding?
A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Explanation (aligned to N10-009):
Multimode fiber uses multiple paths (modes) of light that bounce off the cladding to travel through the fiber.
This is effective for shorter distances but more prone to dispersion.
A). Twinaxial is copper, not fiber.
B). Coaxial carries electrical signals, not light.
C). Single-mode fiber uses a single light path directly through the core without bouncing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Fiber optics: single-mode vs. multimode.

NEW QUESTION: 158
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: 159
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: 160

A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?

A. The parabolic signal is misaligned.
B. The omnidirectional signal is being jammed.
C. The omnidirectional signal is not strong enough to receive properly.
D. The parabolic signal uses improper routing protocols.
Answer: A (LEAVE A REPLY)
A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.
The document confirms:
"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

NEW QUESTION: 161
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: 162
A network administrator recently configured an autonomous wireless AP and performed a throughput test via comptiaspeedtester.com. The result was 75 Mbps. When connected to other APs, the results reached 500 Mbps. Which of the following is most likely the reason for this difference?
A. Channel width configuration
B. DNS server issues
C. Authentication failure
D. Incorrect DHCP settings
Answer: (SHOW ANSWER)
The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.
* B. DNS issues affect name resolution, not raw throughput.
* C. Authentication failure would prevent connection, not reduce throughput.

* D. DHCP issues would prevent obtaining an IP, not cause slower speeds.
References (CompTIA Network+ N10-009):
* Domain: Network Troubleshooting - Wireless throughput issues, channel width configuration.

NEW QUESTION: 163
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: 164
A network engineer configures a NIC that has an IP address of 192.168.123.232. Which of the following classes is this address an example of?
A. Class A
B. Class B
C. Class C
D. Class D
Answer: C (LEAVE A REPLY)
The IPv4 address 192.168.123.232 falls within the Class C range under classful addressing. In classful terms, Class C addresses have a first octet from 192 to 223, which makes any address starting with 192.x.x.x a Class C address. Network+ (N10-009) networking concepts cover IPv4 addressing fundamentals and commonly reference class ranges as foundational knowledge, even though modern networks primarily use CIDR (classless) subnetting rather than strict classful boundaries.
This address is also within a well-known private IPv4 block: 192.168.0.0/16 (RFC1918 private addressing), which is frequently used for internal networks and NIC configurations where addresses are not routable on the public internet.
To eliminate the distractors: Class A uses first octet 1-126, Class B uses 128-191, and Class D (224-239) is reserved for multicast. Since the first octet here is 192, it maps to Class C, making option C correct.

NEW QUESTION: 165
An organization is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that allows for continuous connectivity anywhere in the facility. Which of the following should the network administrator suggest to ensure the best coverage?
A. Implementing additional ad hoc access points
B. Providing more Ethernet drops for user connections
C. Deploying a mesh network in the building
D. Changing the current frequency of the Wi-Fi
Answer: (SHOW ANSWER)
The correct answer is deploying a mesh network. A mesh wireless network uses multiple interconnected access points that automatically route traffic through the best available path. This ensures seamless coverage throughout a facility, even when users move between APs. Mesh APs can extend coverage without requiring each AP to be directly wired, making them ideal for large or hard-to-wire environments.
A). Ad hoc access points are peer-to-peer connections and cannot provide enterprise-grade continuous coverage.
B). Ethernet drops provide wired connectivity but do not solve wireless coverage issues.

D). Changing the frequency (from 2.4 GHz to 5 GHz or vice versa) may reduce interference but will not guarantee building-wide seamless connectivity.
Mesh networks are particularly effective in environments with roaming devices (smartphones, tablets, handheld scanners) and ensure that there are no dead spots, thereby delivering continuous wireless access.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Wireless architectures, mesh networking, seamless connectivity.

NEW QUESTION: 166
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: 167
A user recently moved a workstation to a different part of the office. The user is able to access the internet and print but is unable to access server resources. Which of the following is the most likely cause of the issue?
A. Incorrect default gateway
B. Wrong VLAN assignment
C. Error-disabled port
D. Duplicate IP address
Answer: (SHOW ANSWER)
If a workstation can access the internet and printers (likely in another VLAN) but not internal servers, the port was likely placed into the wrong VLAN after the move. VLAN assignment controls Layer 2 segmentation, restricting access to resources on different VLANs.
A). A wrong default gateway would prevent internet access.

C). An error-disabled port would block all connectivity.
D). A duplicate IP would cause general network issues, not just missing server access.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN misconfiguration, connectivity issues.

NEW QUESTION: 168
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: 169
An organization wants to ensure that incoming emails were sent from a trusted source. Which of the following DNS records is used to verify the source?
A. TXT
B. AAAA
C. CNAME
D. MX
Answer: (SHOW ANSWER)
A TXT record can be used to store SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) information, which help verify that an email has been sent from a trusted source.

NEW QUESTION: 170
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: 171
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: 172
Which of the following is a cost-effective advantage of a split-tunnel VPN?
A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.
Answer: (SHOW ANSWER)
A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.
* Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.
* Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.
* Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.
* Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.
* Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.
By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

NEW QUESTION: 173
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: D (LEAVE A REPLY)
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: 174
A network administrator needs to implement a solution to filter access to the internet. Which of the following should the administrator most likely implement?
A. Router
B. Cloud gateway
C. Proxy
D. Intrusion detection system
Answer: (SHOW ANSWER)
A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.
A). A router directs traffic but doesn't filter internet sites by itself.
B). A cloud gateway could also filter, but the most direct answer is proxy.
D). An IDS detects suspicious activity but doesn't filter browsing access.
References (CompTIA Network+ N10-009):
Domain: Network Security - Proxy servers, filtering, access control.

NEW QUESTION: 175
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: 176
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: 177
Which of the following VPN types provides secure remote access to the network resources through a web portal?
A. Proxy
B. Clientless
C. Site-to-site
D. Direct connect
Answer: (SHOW ANSWER)
Clientless VPNs allow users to access network resources through a secure web portal using a browser, with no VPN software needed. This is ideal for occasional access to internal resources via HTTPS.
A: Proxy is a gateway for accessing web content, not a VPN.
C: Site-to-site VPN connects entire networks, not individual users.
D: Direct Connect usually refers to dedicated cloud connections, not VPNs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

NEW QUESTION: 178
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: 179
A junior network technician at a large company needs to create networks from a Class C address with 14 hosts per subnet. Which of the following numbers of host bits is required?
A. Three

B. Two
C. One
D. Four
Answer: (SHOW ANSWER)

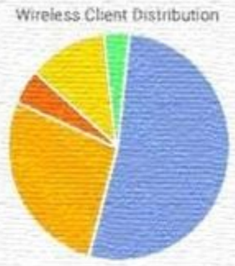
NEW QUESTION: 180
A government entity wants to implement technology that can block websites based on country code.
Which of the following will best enable this requirement?

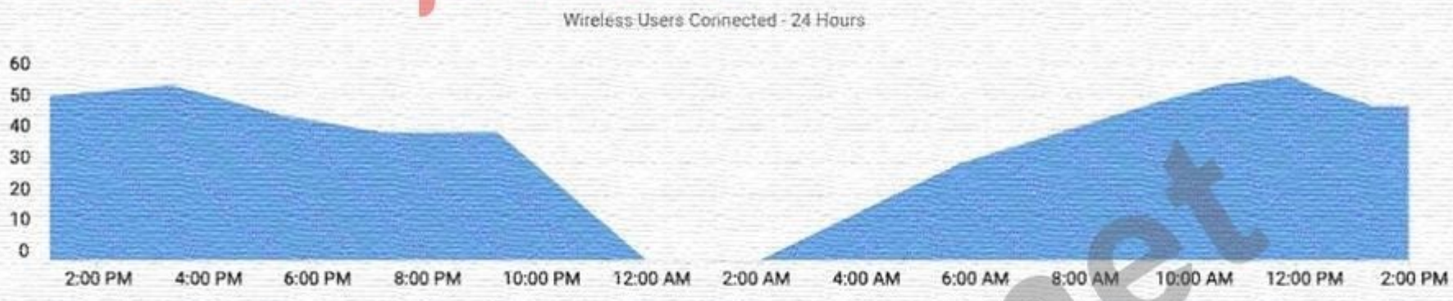
A. URL filtering
B. Content filtering
C. DNS poisoning
D. MAC filtering
Answer: (SHOW ANSWER)
URL filtering can block access to websites based on their domain or country code TLDs (e.g., .cn, .ru). This is the correct method to block by location identifiers in URLs.
B). Content filtering blocks based on keywords or categories within websites, not country code.
C). DNS poisoning is an attack, not a control mechanism.
D). MAC filtering restricts devices, not websites.
References (CompTIA Network+ N10-009):
Domain: Network Security - Filtering technologies, URL vs content filtering.

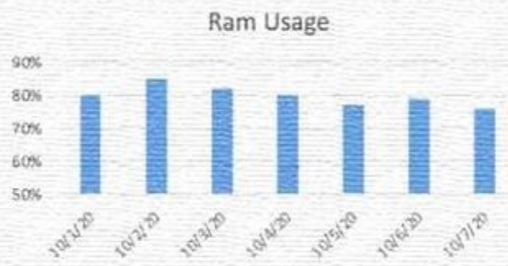
NEW QUESTION: 181
After a recent power outage, users are reporting performance issues accessing the application servers.
Wireless users are also reporting intermittent Internet issues.
INSTRUCTIONS
Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

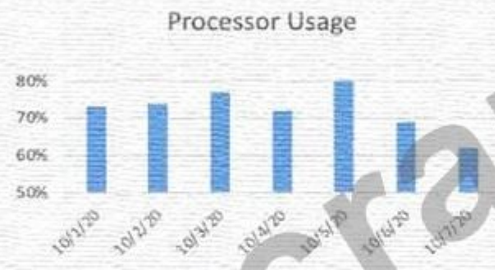
Network Health | Device Monitoring

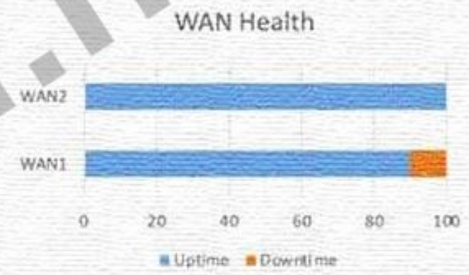
Show Question | Reset All Answers











Uplink Name	Uplink Speed	Total Usage	Average Throughput	Loss	Average Latency	Jitter
WAN1	10G	26,690GB Up/1,708.4GB Down	353MBs Up/23.42MBs Down	2.51%	24ms	9.5ms
WAN2	1G	930GB Up/138GB Down	12.21MBs Up/1.82MBs Down	0.01%	11ms	3.9ms

Which WAN station should be preferred for VoIP traffice?

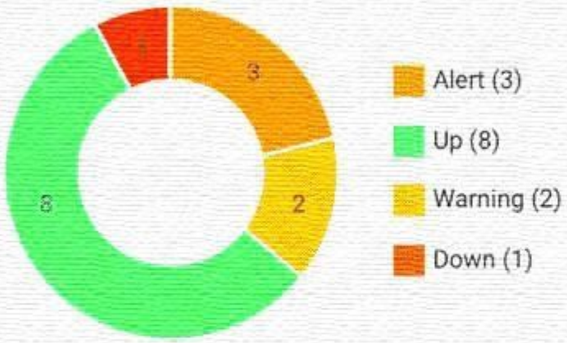
WAN 1

Select WAN
WAN 1
WAN 2

Network Health | Device Monitoring

Show Question | Reset All Answers

Device Status



Top Hosts

	SRC Host	Pkts	Flows	Bits
1	206.208.133.9	8.73 Mp	77	104.69 Gb
2	10.1.90.53	13.45 Mp	10	80.93 Gb
3	10.1.90.55	12.41 Mp	7	74.68 Gb
4	10.1.59.81	259.42 kp	23	3.01 Gb
5	10.1.99.22	182.53 kp	2	2.08 Gb
6	10.1.99.14	433.96 kp	11	2.08 Gb
7	10.1.99.28	164.84 kp	1	1.79 Gb
8	10.1.99.10	840.56 kp	180	1.70 Gb
9	10.1.99.24	135.64 kp	2	1.54 Gb
10	10.1.99.60	133.33 kp	1	1.51 Gb

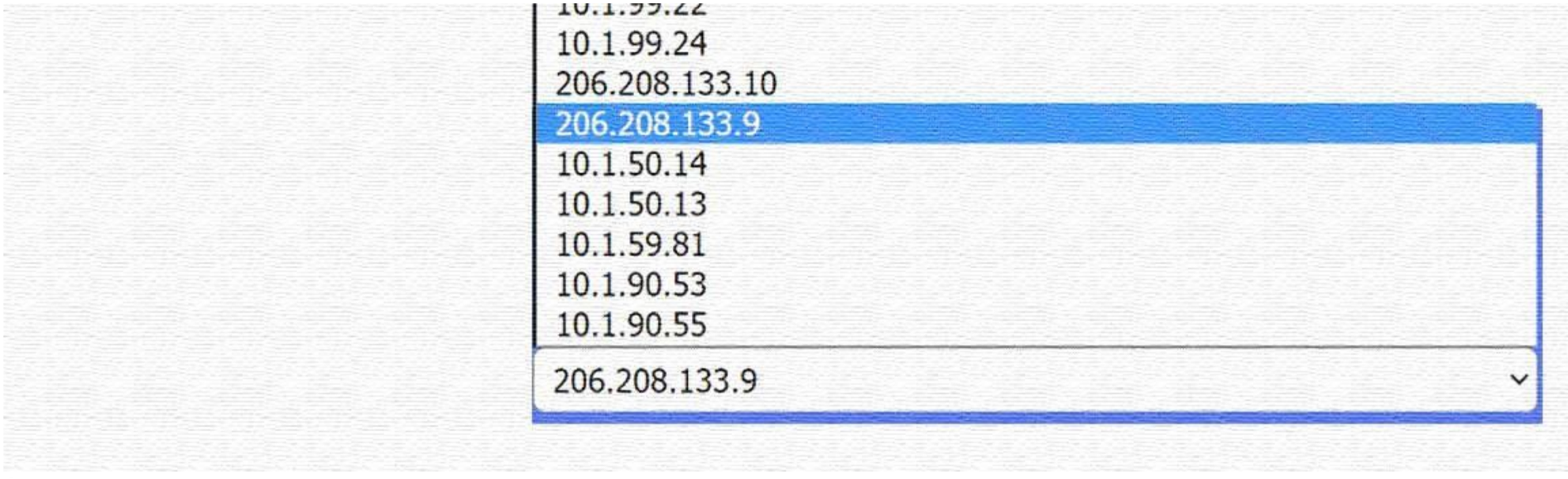
Which device is experiencing connectivity issues?

Select Answer
Router A
Router B
WAP1
WAP2
WirelessController
Switch A
Switch B
DHCP Server
Web Server
APP Server

Router A

Which workstation IP is generating the MOST traffic?

Select Answer
10.1.99.28
10.1.99.14
10.1.99.10
10.1.99.22



Answer:

See the answer and solution below.

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.

Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

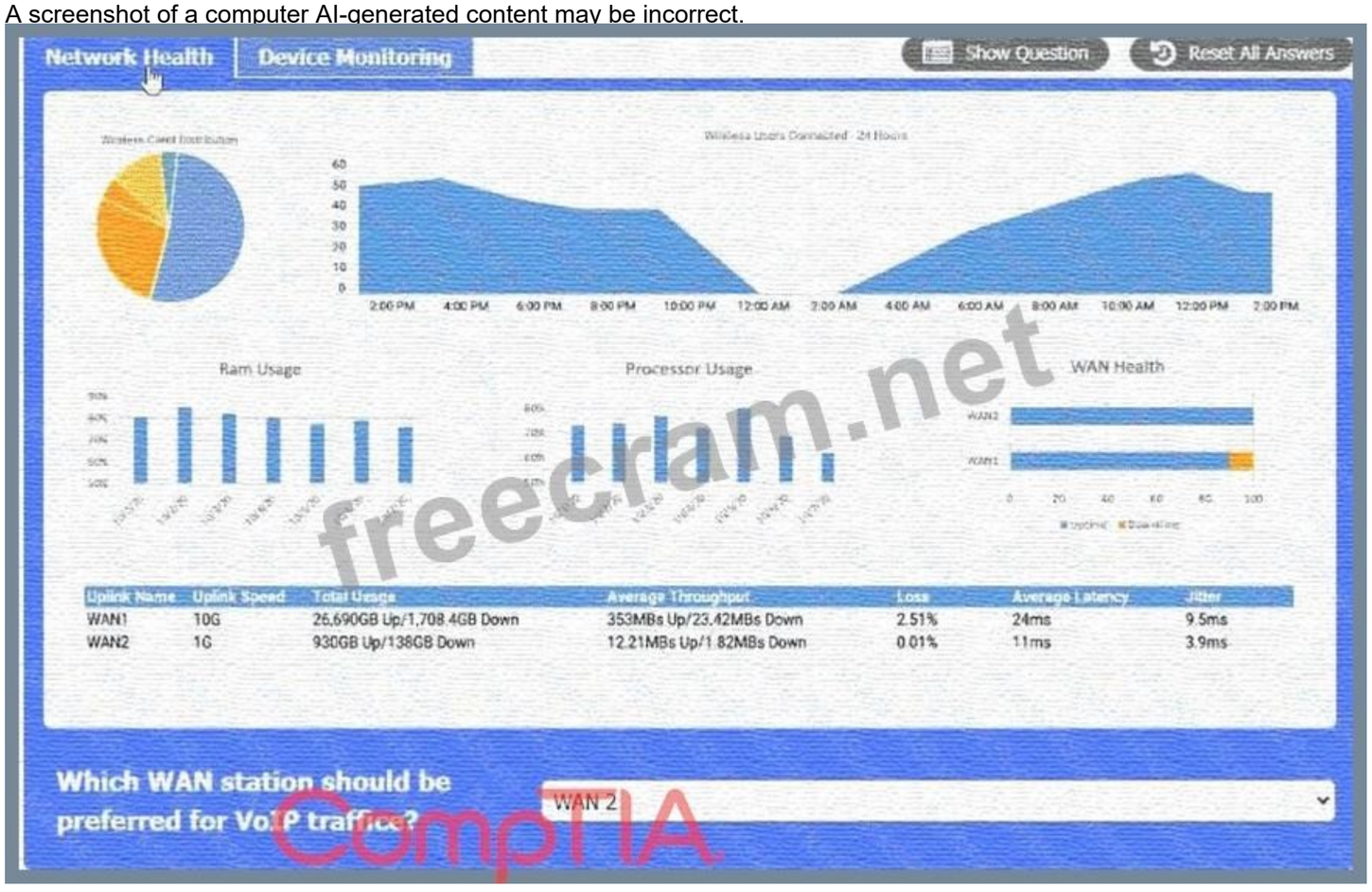
Jitter: 3.9ms

For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.

Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.

Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down.
This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.
A screenshot of a computer AI-generated content may be incorrect.



NEW QUESTION: 182
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: 183
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: C (LEAVE A REPLY)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 184
Which of the following is used to describe the average duration of an outage for a specific service?
A. RPO
B. MTTR
C. RTO
D. MTBF
Answer: (SHOW ANSWER)
MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

NEW QUESTION: 185
A network technician is installing a new switch that does not support STP at the access layer of a network.
The technician wants a redundant connection to the distribution switch. Which of the following should the technician use?
A. Link aggregation
B. Subinterfaces
C. Switch virtual interfaces
D. Half-duplex connections
Answer: (SHOW ANSWER)
Link aggregation(also known as port channeling or EtherChannel) allows multiple physical connections to act as one logical connection. This avoids loops that would typically be prevented by STP and provides redundancy and increased bandwidth. It's ideal when STP is not available or desirable.
Reference:Section 2.2 - Switching Technologies and Features - "Link Aggregation"

NEW QUESTION: 186

A network administrator is looking for a solution to extend Layer 2 capabilities and replicate backups between sites. Which of the following is the best solution?

A. Security Service Edge

B. Data center interconnect

C. Infrastructure as code

D. Zero Trust architecture

Answer: B (LEAVE A REPLY)

The correct solution is a Data Center Interconnect (DCI). DCIs extend Layer 2 networks across geographically dispersed data centers, enabling seamless replication of services such as SAN storage, backup synchronization, or VM migrations. This ensures workloads and data can move between sites while maintaining the same VLANs and addressing.

A). Security Service Edge (SSE) provides cloud-delivered security functions like secure web gateways and CASB, not Layer 2 extension.

C). Infrastructure as code (IaC) automates deployment and management of network infrastructure but is unrelated to extending Layer 2 domains.

D). Zero Trust architecture is a security framework ensuring strict access control but doesn't address network connectivity between sites.

In scenarios where backups need replication between sites, Layer 2 extension is often required so systems can communicate as if they are in the same broadcast domain. DCI is specifically designed to provide this functionality reliably and securely.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - WAN technologies, data center interconnect, backup replication.

NEW QUESTION: 187

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: 188

Users are unable to access files on their department share located on file 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, identify any issues, and configure the appropriate solution.

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

Router A

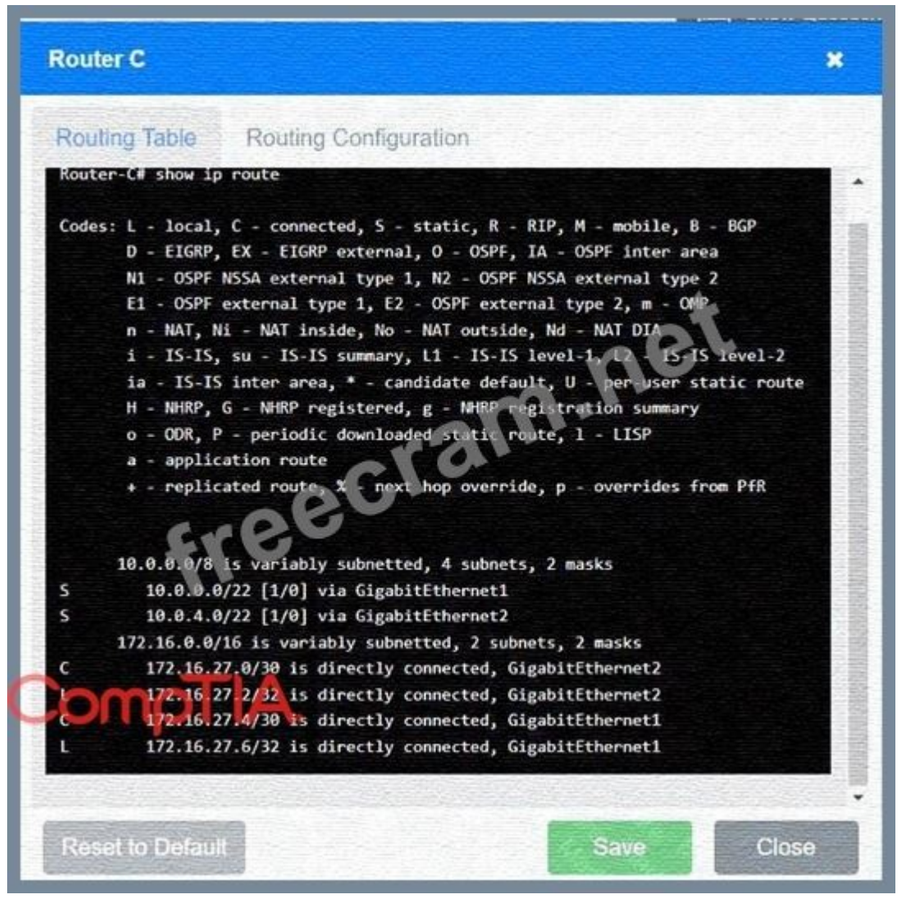
Routing Table | Routing Configuration

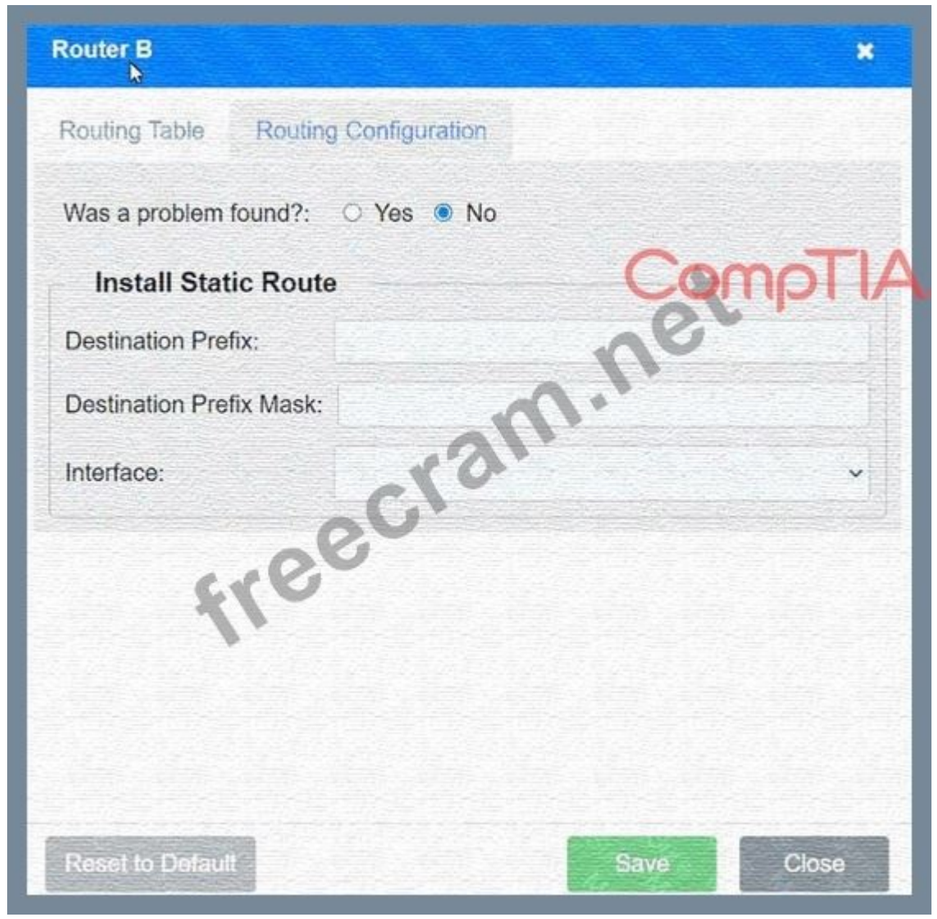
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, 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, GigabitEthernet3
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.4.0/22 is directly connected, GigabitEthernet2
C        10.0.6.0/24 is directly connected, GigabitEthernet2
L        10.0.6.1/32 is directly connected, GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet3
L        172.16.27.1/32 is directly connected, GigabitEthernet3
```

Reset to Default | Save | Close





Answer:

See the solution in Explanation.

Explanation:

To validate routing between networks hosting Workstation A and File Server 2, follow these steps:

Review Routing Tables:

Check the routing tables of Router A, Router B, and Router C to identify any missing routes.

Identify Missing Routes:

Ensure that each router has routes to the networks on which Workstation A and File Server 2 are located.

Add Static Routes:

If a route is missing, add a static route to the relevant destination network via the correct interface.

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet3
L 172.16.27.1/32 is directly connected, GigabitEthernet3
Routing Table:
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, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1
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
Routing Table:
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.0.0.0/22 [1/0] via GigabitEthernet1
S 10.0.4.0/22 [1/0] via GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet2
L 172.16.27.2/32 is directly connected, GigabitEthernet2
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.6/32 is directly connected, GigabitEthernet1
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router C's IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet3
Install Static Route to 10.0.4.0/22 via 172.16.27.5 (assuming Router C's IP is 172.16.27.5):
Destination Prefix: 10.0.4.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Install Static Route to 10.0.6.0/24 via 172.16.27.2 (assuming Router A's IP is 172.16.27.2):
Destination Prefix: 10.0.6.0
Destination Prefix Mask: 255.255.255.0
Interface: GigabitEthernet2
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router B's IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Summary of Static Routes:
Router A:
ip route 10.0.0.0 255.255.252.0 GigabitEthernet3

Router B:
ip route 10.0.4.0 255.255.252.0 GigabitEthernet1
Router C:
ip route 10.0.6.0 255.255.255.0 GigabitEthernet2
ip route 10.0.0.0 255.255.252.0 GigabitEthernet1
These configurations ensure that each router knows the correct paths to reach Workstation A and File Server
2, resolving the connectivity issue.

NEW QUESTION: 189
After installing a new 6E wireless router in a small office, a technician notices that some wireless devices are not able to achieve the rated speeds.
Which of the following should the technician check to troubleshoot the issue? (Select two)
A. Back-end cabling
B. Interference levels
C. Client device compatibility
D. Processing power
E. Weather phenomena
F. Voltage source requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 190
A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity. Which of the following should be implemented to comply with the cease-and-desist order?

A. MAC security
B. Content filtering
C. Screened subnet
D. Perimeter network
Answer: (SHOW ANSWER)
Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease- and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.
References: CompTIA Network+ study materials.

NEW QUESTION: 191
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: 192
A technician needs to quickly set up a network with five wireless devices. Which of the following network types should the technician configure to accomplish this task?
A. Ad hoc
B. Spine and leaf
C. Point to point
D. Mesh
Answer: (SHOW ANSWER)
The correct answer is Ad hoc because it allows wireless devices to communicate directly with one another without requiring a centralized access point or additional infrastructure. According to CompTIA Network+ (N10-009) objectives under wireless networking concepts, an ad hoc network (also known as an Independent Basic Service Set, or IBSS) enables peer-to-peer wireless communication.
This type of network is ideal for temporary or quick setups where only a small number of devices need to connect. In an ad hoc configuration, each device connects directly to others, making it simple and fast to deploy without requiring switches, routers, or wireless access points.
Spine and leaf (Option B) is a data center architecture designed for high scalability and redundancy, not small wireless setups. Point-to-point (Option C) refers to a direct connection between two devices only, which would not support five devices efficiently. Mesh (Option D) allows multiple nodes to interconnect and provide redundancy, but it is more complex and typically requires compatible infrastructure devices.
Therefore, for a quick setup with five wireless devices, an ad hoc network is the most appropriate choice.

NEW QUESTION: 193
A network administrator is creating a subnet that will include 45 separate hosts on a small private network within a large network architecture. Which of the following options is the most efficient use of network addresses when assigning this network?
A. 10.0.50.128/25
B. 10.7.142.128/27
C. 10.152.4.192/26
D. 10.192.1.64/28
Answer: (SHOW ANSWER)
For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).
A /26 subnet provides 64 addresses, 62 usable - suitable.
A /27 subnet gives only 30 usable - insufficient.
A /25 offers 126 usable - more than needed.
A /28 provides just 14 - too small.
So, the most efficient subnet with minimal wastage is /26.
From Andrew Ramdayal's guide:
"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts. A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."
NEW QUESTION: 194
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: 195
A network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?
A. Access
B. Core
C. Leaf
D. Spine
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
In a spine-leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer-often specifically to a "border leaf" that handles external connectivity.
Why not B. Core or D. Spine? In spine-leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.
Why not A. Access? "Access" is a term from the traditional three-tier model (access-distribution-core). In modern spine-leaf language, the analogous layer for endpoint attachment is the leaf.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Data center and campus architectures (spine-leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

NEW QUESTION: 196
A network engineer needs to order cabling to connect two buildings within the same city. Which of the following media types should the network engineer use?
A. Coaxial
B. Twinaxial
C. Single-mode fiber
D. Cat 5
Answer: (SHOW ANSWER)
Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth - making it the ideal choice for connecting buildings across a city.
Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).
Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.
For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

NEW QUESTION: 197
Which of the following ports is used for secure email?
A. 25
B. 110
C. 143
D. 587
Answer: (SHOW ANSWER)
Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.
Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.
Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.
Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL
/TLS.
Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.
Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.
Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

NEW QUESTION: 198
A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?
A. Develop a theory.
B. Establish a plan of action.
C. Implement the solution.
D. Document the findings.
Answer: C (LEAVE A REPLY)
Once the theory has been tested and confirmed, the next step is to implement the solution based on the CompTIA troubleshooting model.
CompTIA Troubleshooting Model:
Identify the problem.
Establish a theory of probable cause.
Test the theory.
Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.
Document findings, actions, and outcomes.
Breakdown of Options:
A). Develop a theory - The theory has already been developed and tested.
C). Implement the solution - Correct answer. The problem is confirmed, so the fix should be applied.
B). Establish a plan of action - This happens before implementation, but since the issue is confirmed, it's time to act.
D). Document the findings - Documentation is the final step, not the next one.
Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 5.1: Explain network troubleshooting methodology.

NEW QUESTION: 199
Which of the following is used to redistribute traffic between one source and multiple servers that run the same service?
A. Router
B. Switch
C. Firewall
D. Load balancer
Answer: (SHOW ANSWER)
The correct answer is Load balancer because it is specifically designed to distribute incoming network traffic across multiple backend servers that provide the same application or service. According to CompTIA Network+ (N10-009) objectives under network infrastructure, load balancing improves performance, scalability, and high availability by preventing any single server from becoming overwhelmed.
A load balancer can operate at Layer 4 (transport layer, based on IP address and port) or Layer 7 (application layer, based on content such as HTTP headers or URLs). It uses various algorithms such as round-robin, least connections, or weighted distribution to efficiently allocate client requests among servers. If one server fails, the load balancer can redirect traffic to healthy servers, ensuring service continuity.
A router (Option A) forwards packets between different networks but does not distribute traffic among servers running the same application. A switch (Option B) forwards frames within a local network based on MAC addresses. A firewall (Option C) filters traffic based on security rules but does not perform traffic distribution for load-sharing purposes.
Therefore, a load balancer is the correct solution for redistributing traffic among multiple servers.

NEW QUESTION: 200
Ten new laptops are added to an existing network, and they can only communicate with one another.
An administrator reviews documentation and sees the following:
Subnet: 10.8.100.1/24
Scope: 10.8.100.50 - 10.8.100.150
Reservation: 10.8.100.151 - 10.8.100.175
A technician scans the network and receives the following results:
IP addresses used: 10.8.100.45 - 10.8.100.175
Which of the following should be done to ensure connectivity on all laptops?

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

NEW QUESTION: 201
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: 202
Which of the following is the best use case of a site-to-site VPN?
A. Securing access across an untrusted network
B. Encrypting data at rest
C. Filtering traffic between two internal subnets
D. Hosting public-facing applications that contain company resources
Answer: (SHOW ANSWER)
A site-to-site VPN is used to securely connect two networks over an untrusted network, most commonly the public internet. In Network+ (N10-009) objectives, VPNs are described as providing confidentiality and integrity for data in transit by creating an encrypted tunnel between sites (for example, headquarters and a branch office). This allows systems at both locations to communicate as if on the same private WAN, while preventing eavesdropping or tampering by intermediate networks. Typical implementations use IPsec tunneling and rely on negotiated encryption/authentication parameters to protect traffic end-to-end between VPN gateways.
Encrypting data at rest refers to storage encryption (disk/database), not VPN tunneling. Filtering traffic between two internal subnets is usually handled by ACLs, firewalls, or segmentation controls, not a site-to- site VPN. Hosting public-facing applications is a DMZ / reverse proxy / WAF design concern; a VPN is not the primary control for exposing public services (and generally you would not require the public to use a VPN to reach a public website). Therefore, securing site connectivity across an untrusted network is the best match.

NEW QUESTION: 203
An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. The technician examines the configuration and sees a self-assigned IP address. Which of the following is the most likely cause?
A. The DHCP server is not available
B. An RFC1918 address is being used
C. The TCP/IP stack is disabled
D. A static IP is assigned
Answer: (SHOW ANSWER)

When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a "self-assigned IP." This prevents communication outside the local link, including reaching the default gateway.
B). RFC1918 addresses are private ranges (10.x.x.x, 172.16-31.x.x, 192.168.x.x), but these are not self- assigned.
C). If the TCP/IP stack were disabled, the host wouldn't have any IP at all.
D). If a static IP were assigned, it would show a configured value, not self-assigned.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - IP addressing issues, DHCP failures, APIPA behavior.

NEW QUESTION: 204
A network engineer added more APs to improve wireless coverage. However, users now report that the connectivity disconnects and reconnects repeatedly. Which of the following is causing the issue?
A. Throughput capacity
B. Roaming misconfiguration
C. Channel overlap
D. Packet loss
Answer: (SHOW ANSWER)
Adding more access points can improve coverage, but it also increases the risk of co-channel interference if APs are configured on the same or overlapping channels. Channel overlap causes contention and interference, leading to retries, unstable performance, and symptoms that feel like frequent disconnect /reconnect events-especially in dense deployments. Network+ (N10-009) wireless troubleshooting objectives highlight proper channel planning (non-overlapping channels, appropriate channel width) as critical when increasing AP density. If adjacent APs are competing on the same channel (or overlapping channels in 2.4 GHz), clients may experience poor signal-to-noise ratios and repeated reassociations as they struggle to maintain a stable link.
Roaming misconfiguration can cause sticky clients or poor handoffs, but the classic problem introduced immediately after "adding more APs" is interference from bad channel design. Throughput capacity is about available bandwidth and airtime efficiency; it can make things slow, but it doesn't inherently cause repeated disconnect/reconnect loops like interference does. Packet loss is a symptom that may occur due to interference, but the root cause in the options that best fits the scenario is channel overlap.

NEW QUESTION: 205
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: 206
Which of the following is enforced through legislation?
A. AUP
B. GDPR
C. Code of conduct

D. EULA

Answer: (SHOW ANSWER)

GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences.

Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

NEW QUESTION: 207

Users at an organization report that the wireless network is not working in some areas of the building. Users report that other wireless network SSIDs are visible when searching for the network, but the organization's network is not displayed. Which of the following is the most likely cause?

A. Interference or channel overlap

B. Insufficient wireless coverage

C. Roaming misconfiguration

D. Client disassociation issues

Answer: (SHOW ANSWER)

If the company's SSID is not visible in some areas while other networks are still visible, the most likely cause is insufficient wireless coverage. The wireless signal does not reach those areas, meaning additional access points or signal boosters may be required.

Breakdown of Options:

A: Interference or channel overlap - Would cause slow or unstable connections, but the SSID should still be visible.

B: Insufficient wireless coverage - # Correct answer. If the SSID is not appearing, the signal is too weak in that area.

C: Roaming misconfiguration - Would cause devices to stay on weaker APs instead of switching, but the SSID should still be visible.

D: Client disassociation issues - This would disconnect users, but they should still see the network.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Explain wireless concepts and technologies.

NEW QUESTION: 208

Which of the following network cables involves bounding light off of protective cladding?

A. Twinaxial

B. Coaxial

C. Single-mode

D. Multimode

Answer: (SHOW ANSWER)

Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.

Here are some detailed points about multimode fiber cables:

Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single- mode fibers, which have a core diameter of about 9 microns.

Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.

Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers.

Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.

Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.

Network References:

CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.
Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.
Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.
Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

NEW QUESTION: 209
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: 210
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: 211
Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?

A. Infrastructure as a service
B. Software as a service
C. Platform as a service
D. Network as a service
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

NEW QUESTION: 212
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: 213
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: 214

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: 215

A technician needs to identify a computer on the network that is reportedly downloading unauthorized content. Which of the following should the technician use?

A. Anomaly alerts

B. Port mirroring

C. Performance monitoring

D. Packet capture

Answer: (SHOW ANSWER)

Packet Capture: This method captures and inspects network traffic to identify unauthorized downloads or malicious behavior. It provides detailed insight into the data being transmitted, making it the

best tool for this scenario.
Anomaly alerts (A): Alerts may indicate unusual activity but do not provide detailed traffic analysis.
Port mirroring (B): Port mirroring can redirect traffic for analysis but requires a packet capture tool for deeper inspection.
Performance monitoring (C): Focuses on system performance metrics, not detailed traffic content.
Reference: CompTIA Network+ Official Study Guide, Domain 4.3 (Network Monitoring Tools).

NEW QUESTION: 216
Which of the following could provide a lightweight and private connection to a remote box?
A. Site-to-site VPN
B. Telnet
C. Console
D. Secure Shell
Answer: D (LEAVE A REPLY)
Secure Shell (SSH)is a protocol used tosecurely access remote devices over an unsecured network. It provides encrypted command-line access and is a lightweight and secure method of remote administration.
* A. Site-to-site VPNconnects entire networks, not just a single host.
* B. Telnetis not secure; it transmits data (including credentials) in plaintext.
* C. Consoleaccess is direct via serial cable, not remote.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 2.6 - Configure and troubleshoot remote access.

NEW QUESTION: 217
Which of the following layers of the OSI model is responsible for end-to-end encryption?
A. Presentation
B. Application
C. Session
D. Transport
Answer: (SHOW ANSWER)
The correct answer is Presentation, which is Layer 6 of the OSI model. According to the CompTIA Network+ N10-009 objectives, the Presentation layer is responsible for data formatting, compression, and encryption, ensuring that data sent from the application layer of one system can be properly interpreted by the receiving system.
End-to-end encryption refers to encrypting data before transmission and decrypting it only at the final destination, preventing intermediaries from accessing the plaintext data. In the OSI model, this encryption and decryption function is logically placed at the Presentation layer, which sits between the Application and Session layers. This layer transforms data into a standardized format and applies security mechanisms such as encryption algorithms.
While modern implementations like TLS/SSL often operate across multiple layers in real-world networking stacks, the Network+ exam adheres to the conceptual OSI model when testing knowledge.
From an OSI perspective, encryption is explicitly associated with the Presentation layer.
The Application layer provides network services to end-user applications, the Session layer manages session establishment and teardown, and the Transport layer focuses on segmentation, flow control, and reliability.
None of these layers are primarily responsible for encryption within the OSI framework.
CompTIA emphasizes understanding these conceptual responsibilities, making Presentation the correct and expected answer.

NEW QUESTION: 218

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: 219
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: 220
Which of the following will allow secure, remote access to internal applications?

A. VPN
B. CDN
C. SAN
D. IDS
Answer: (SHOW ANSWER)
A Virtual Private Network (VPN) creates an encrypted connection between a remote user and an internal network, ensuring secure access to internal applications.
* VPNs use encryption protocols like IPSec and SSL/TLS to protect data during transmission.
* They are widely used for secure remote work, accessing company resources, and bypassing geographic restrictions.
* Option B (CDN - Content Delivery Network): Used for speeding up website content delivery, not for remote access security.
* Option C (SAN - Storage Area Network): Used for high-speed storage, unrelated to remote access.
* Option D (IDS - Intrusion Detection System): Monitors for malicious activities but does not provide secure access to applications.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Secure Remote Access Technologies

NEW QUESTION: 221
A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance. Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?
A. Speed mismatches
B. Load balancer settings
C. Flow control settings
D. Infrastructure cabling grade
Answer: (SHOW ANSWER)
Speed Mismatches: If NICs are set to different speeds (e.g., 100 Mbps on one side and 1 Gbps on the other), performance will degrade. Ensuring consistent speed settings between devices is crucial for optimal performance.
Load balancer settings (B): Applies to server load distribution, not endpoint speed.
Flow control settings (C): Can affect performance but is secondary to speed mismatches.
Infrastructure cabling grade (D): Relevant if the cables are unsuitable for gigabit speeds, but speed settings should be checked first.
Reference: CompTIA Network+ Official Study Guide, Domain 2.5 (Troubleshooting Network Issues).

NEW QUESTION: 222
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: B (LEAVE A REPLY)
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: 223
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: (SHOW ANSWER)
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: 224
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: 225
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: 226
A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?
A. 802.1Q tagging
B. Spanning tree
C. Link aggregation
D. Jumbo frames
Answer: D (LEAVE A REPLY)
VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size.
This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging enables segmentation but does not address fragmentation issues.
B). Spanning tree - STP prevents loops but does not improve performance for VXLAN traffic.
C). Link aggregation - LACP combines links for higher bandwidth but does not prevent fragmentation.
D). Jumbo frames - Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.

Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network performance concepts.
RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

NEW QUESTION: 227
Users usually use RDP to connect to a terminal server with hostname TS19 that points to 10.0.100.19.
However, users recently have been unable to connect to TS19. The technician pings 10.0.100.19 and gets an unreachable error. Which of the following is the most likely cause?
A. The users are on the wrong subnet.
B. The DHCP server renewed the lease.
C. The IP address was not reserved.
D. The hostname was changed.
Answer: (SHOW ANSWER)
If a ping to 10.0.100.19 is unreachable, the most likely issue is that users are on the wrong subnet and cannot communicate with the server.
Breakdown of Options:
A: The users are on the wrong subnet. # Correct answer. If users are on a different subnet without proper routing, they won't reach the server.
B: The DHCP server renewed the lease. - Would change the client's IP, but the server's static IP should remain unchanged.
C: The IP address was not reserved. - DHCP reservations matter for dynamic IPs, but RDP servers typically have static IPs.
D: The hostname was changed. - Would affect DNS resolution, but pinging the IP directly would still work.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting concepts.

NEW QUESTION: 228
Which of the following most likely requires the use of subinterfaces?
A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol
Answer: (SHOW ANSWER)
Introduction to Subinterfaces:
Subinterfaces are logical interfaces created on a single physical interface. They are used to enable a router to support multiple networks on a single physical interface.
Use Case for Subinterfaces:
Subinterfaces are commonly used in scenarios where VLANs are implemented. A router with a single physical LAN port can be configured with multiple subinterfaces, each associated with a different VLAN.
This setup allows the router to route traffic between different VLANs.
Example Configuration:

Consider a router with a single physical interface GigabitEthernet0/0 and two VLANs, 10 and 20.
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
The encapsulation dot1Q command specifies the VLAN ID.
Explanation of the Options:
A). A router with only one available LAN port: This is correct. Subinterfaces allow a single physical interface to manage multiple networks, making it essential for routers with limited physical interfaces.
B). A firewall performing deep packet inspection: Firewalls can use subinterfaces, but it is not a requirement for deep packet inspection.
C). A hub utilizing jumbo frames: Hubs do not use subinterfaces as they operate at Layer 1 and do not manage IP addressing.
D). A switch using Spanning Tree Protocol: STP is a protocol for preventing loops in a network and does not require subinterfaces.
Conclusion:
Subinterfaces provide a practical solution for routing between multiple VLANs on a router with limited physical interfaces. They allow network administrators to optimize the use of available hardware resources efficiently.
References:
CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref
9 Basic Configuration Commands).

NEW QUESTION: 229
A critical infrastructure switch is identified as end-of-support. Which of the following is the best next step to ensure security?
A. Apply the latest patches and bug fixes.
B. Decommission and replace the switch.
C. Ensure the current firmware has no issues.
D. Isolate the switch from the network.
Answer: (SHOW ANSWER)
* Understanding End-of-Support:
* End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.
* Risks of Keeping an End-of-Support Device:
* Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats.
* Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.
* Best Next Step - Replacement:
* Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.
* Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.
* Comparison with Other Options:
* Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.
* Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.

* Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.
References:
* CompTIA Network+ study materials on network maintenance and security best practices.

NEW QUESTION: 230

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.

NEW QUESTION: 231
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: 232
During a recent security assessment, an assessor attempts to obtain user credentials by pretending to be from the organization's help desk. Which of the following attacks is the assessor using?
A. Social engineering
B. Tailgating
C. Shoulder surfing
D. Smishing
E. Evil twin
Answer: (SHOW ANSWER)
This is a classic example of social engineering, where an attacker manipulates individuals into giving up confidential information, such as credentials, by pretending to be someone trustworthy (like help desk staff).
B). Tailgating involves physical access without authentication.
C). Shoulder surfing is spying over someone's shoulder to steal info.
D). Smishing is phishing via SMS.
E). Evil twin involves a rogue Wi-Fi access point impersonating a legitimate one.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

NEW QUESTION: 233
Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?
A. Direct Connect
B. Internet gateway
C. Captive portal
D. VPN
Answer: (SHOW ANSWER)
Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet, providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.
Reference:
CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

NEW QUESTION: 234
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: A (LEAVE A REPLY)
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: 235
An organization moved its DNS servers to new IP addresses. After this move, customers are no longer able to access the organization's website. Which of the following DNS entries should be updated?
A. AAAA
B. CNAME
C. MX
D. NS
Answer: (SHOW ANSWER)
When an organization moves its DNS servers to new IP addresses, the NS (Name Server) records must be updated. The NS record defines which DNS servers are authoritative for a domain. Ifthese records still point to the old IP addresses, clients will continue to query the outdated servers, leading to connectivity issues.
Breakdown of Options:
A). AAAA - This record maps a domain name to an IPv6 address. Since the issue is with DNS resolution, not IP versioning, this is incorrect.
B). CNAME - A CNAME (Canonical Name) record is used for domain aliasing, not for defining authoritative name servers.
C). MX - Mail Exchange (MX) records direct email traffic to the correct mail server, which does not impact general website accessibility.
D). NS - Correct answer. NS records must be updated to reflect the new authoritative DNS servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain the purpose and properties of DNS records.
RFC 1035: Domain Names - Implementation and Specification

NEW QUESTION: 236
Which of the following routing technologies uses an attribute list for path selection?
A. BGP
B. RIP
C. EIGRP
D. OSPF
Answer: (SHOW ANSWER)
BGP (Border Gateway Protocol) uses attributes like AS path, origin, and MED (multi-exit discriminator) to determine the best path among multiple available routes.
From Andrew Ramdayal's guide:
"BGP is the protocol underlying the global routing system of the internet. It is used for routing data between autonomous systems (ASes)... BGP uses a path vector mechanism and maintains a list of attributes for route selection."

NEW QUESTION: 237

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.