CompTIA.N10-009.v2026-02-20.q205

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	205
Version:	v2026-02-20
# of views:	112
# of Questions views:	2050
https://www.freepdfdumps.com/CompTIA.N10-009.v2026-02-20.q205.html	

NEW QUESTION: 1
A network administrator deploys new network hardware. While configuring the network monitoring server, the server could authenticate but could not determine the specific status of the hardware. Which of the following would the administrator most likely do to resolve the issue?
A. Use the public community string
B. Import the appropriate MIB
C. Set up a switchport analyzer and forward traffic
D. Configure SNMPv3 privacy
Answer: (SHOW ANSWER)
MIBs (Management Information Bases) define the variables and objects that SNMP can query on a device. If the monitoring server authenticates but cannot interpret the data, it likely lacks the correct MIB for that vendor or model. Importing the proper MIB allows the monitoring server to correctly display device status and metrics.
A . Using a public community string is insecure and not related to missing MIBs.
C . Switchport analyzer (SPAN) captures traffic for packet analysis, not SNMP monitoring.
D . SNMPv3 privacy adds encryption but doesn't fix missing MIB interpretation.
Reference (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP, MIBs, network monitoring systems.

NEW QUESTION: 2
A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?
A. Mesh
B. Ad hoc
C. Point-to-point
D. Infrastructure
Answer: (SHOW ANSWER)

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

NEW QUESTION: 3
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: 4
Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?
A. Verify full system functionality.
B. Document the findings and outcomes.
C. Establish a plan of action.
D. Identify the problem.
Answer: (SHOW ANSWER)
The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.
Troubleshooting Steps:
Identify the problem.
Establish a theory of probable cause.

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

NEW QUESTION: 5
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: A,E (LEAVE A REPLY)
*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: 6
Which of the following is used most often when implementing a secure VPN?

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

NEW QUESTION: 7
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: 8
A network technician is requesting a fiber patch cord with a connector that is round and twists to install. Which of the following is the proper name of this connector type?
A. ST
B. BNC
C. SC

D. LC

Answer: A (LEAVE A REPLY)

The ST (Straight Tip) fiber connector is round with a bayonet twist-lock mechanism. It is older but still used in some fiber installations.

B . BNC is a coaxial connector.

C . SC (Subscriber Connector) is a square push-pull fiber connector.

D . LC (Lucent Connector) is a small form-factor fiber connector.

Reference (CompTIA Network+ N10-009):

Domain: Networking Concepts - Fiber connectors (ST, SC, LC).

NEW QUESTION: 9

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: D (LEAVE A REPLY)

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: 10

A small company has the following IP addressing strategy:

A user is unable to connect to the company fileshare server located at 192.168.10.1. The user's networking configuration is:

Which of the following will most likely correct the issue?

A. Changing the IPv4 address to 192.168.10.1

B. Changing the subnet mask to 255.255.255.0

C. Changing the DNS servers to internet IPs

D. Changing the physical address to 7A-01-7A-21-01-50

Answer: (SHOW ANSWER)

If the user cannot communicate with 192.168.10.1, they might be on a different subnet. Changing the subnet mask to 255.255.255.0 ensures the user and the file server are in the same subnet.

Breakdown of Options:
A . Changing the IPv4 address to 192.168.10.1 - This would conflict with the server's IP.
B . Changing the subnet mask to 255.255.255.0 - ✅ Correct answer. Ensures both the user and the server are on the same subnet.
C . Changing the DNS servers - DNS does not affect local network connectivity.
D . Changing the physical address - The MAC address does not impact subnet communication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting and addressing concepts.

NEW QUESTION: 11
A network engineer is designing an internal network that needs to support both IPv4 and IPv6 routing. Which of the following routing protocols is capable of supporting both IPv4 and IPv6?
A. OSPFv3
B. RIPv2
C. BGP
D. EIGRP
Answer: D (LEAVE A REPLY)
EIGRP(Enhanced Interior Gateway Routing Protocol) supports bothIPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.
Reference:

NEW QUESTION: 12
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: D (LEAVE A REPLY)
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: 13
A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access
B. Dynamic inventeries
C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits
Answer: A,C (LEAVE A REPLY)
To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.
Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.
Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.
Cisco Networking Academy: Provides training on implementing security policies and access controls.
Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

NEW QUESTION: 14
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: 15
A technician is troubleshooting a computer issue for a user who works in a new annex of an office building. The user is reporting slow speeds and intermittent connectivity. The computer is connected via a Cat 6 cable to a distribution switch that is 492ft (150m) away. Which of the following should the technician implement to correct the issue?
A. Increase the bandwidth allocation to the computer.
B. Install an access switch in the annex and run fiber to the distribution switch.
C. Run a Cat 7 cable from the computer to the distribution switch.
D. Enable the computer to support jumbo frames.
Answer: (SHOW ANSWER)
The maximum recommended length for Ethernet cable runs is 100 meters (328 feet). At 150 meters, the Cat 6 cable is too long, causing signal degradation and connectivity issues. Running fiber from the distribution switch to an access switch in the annex will allow for reliable connectivity over longer distances, as fiber can cover greater distances without signal loss.
(Reference: CompTIA Network+ Study Guide, Chapter on Network Cable Standards)

NEW QUESTION: 16
A help desk technician receives a report that users cannot access internet URLs. The technician performs ping tests and finds that sites fail when a URL is used but succeed when an IP is used. Which of the following tools should the technician utilize next?
A. tcpdump
B. tracert
C. nmap
D. dig
Answer: D (LEAVE A REPLY)
Other tools are less relevant here:
A). tcpdump is a packet analyzer and is more advanced for deeper traffic analysis.
B). tracert is used to trace the route to a destination, not ideal for DNS issues.
C). nmap is a port scanner and network mapper, not for resolving DNS problems.
D). dig (Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.
Explanation:
The issue is clearly related to DNS resolution, as IP-based connections succeed but domain name-based ones fail.

NEW QUESTION: 17
A detective is investigating an identity theft case in which the target had an RFID-protected payment card issued and compromised in the same day. The only place the target claims to have used the card was at a local convenience store. The detective notices a video camera at the store is placed in such a way that customers' credentials can be seen when they pay. Which of the following best explains this social engineering technique?
A. Shoulder surfing
B. Impersonation
C. Vishing
D. Tailgating
Answer: A (LEAVE A REPLY)
Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.
From Andrew Ramdayal's guide:
"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

NEW QUESTION: 18
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: B (LEAVE A REPLY)
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.Reference: CompTIA Network+ study materials.

NEW QUESTION: 19
An attacker gained access to the hosts file on an endpoint and modified it. Now, a user is redirected from the company's home page to a fraudulent website. Which of the following most likely happened?
A. DNS spoofing
B. Phishing
C. VLAN hopping
D. ARP poisoning
Answer: (SHOW ANSWER)
When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.
B . Phishing typically uses emails or messages to trick users, not local file modification.
C . VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.
D . ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 20
A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?
A. With a voice VLAN
B. With too many VLANs
C. With a default VLAN
D. With a native VLAN
Answer: A (LEAVE A REPLY)
It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

NEW QUESTION: 21
A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses (one for a computer and one for a phone). Which of the following classful IPv4 address ranges will be best-suited for the network?
A. Class D
B. Class B
C. Class A
D. Class C
Answer: B (LEAVE A REPLY)
*The total number of devices = (150 + 10) users × 2 IPs per user = 320 devices
*Class C (D) supports a maximum of 254 hosts (2^8 - 2), which is too small.

*Class B (B) supports 65,534 hosts (2^16 - 2), making it the best choice.
*Why not the other options?
*Class A (C): Supports millions of addresses, which is overkill for 320 devices.
*Class D (A): Used for multicast, not for device addressing.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 22
Which of the following is an XML-based security concept that works by passing sensitve information about users, such as log-in information and attributes, to providers.
A. IAM
B. MFA
C. RADIUS
D. SAML
Answer: D (LEAVE A REPLY)
Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP). SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity provider and the service provider.
SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.
XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.
Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Covers authentication protocols, including SAML.
Cisco Networking Academy: Provides training on identity management and federation technologies.
Network+ Certification All-in-One Exam Guide: Explains SAML and its role in secure identity management and SSO.

NEW QUESTION: 23
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: B (LEAVE A REPLY)
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. Reference: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 24
A technician is planning an equipment installation into a rack in a data center that practices hot aisle/cold aisle ventilation. Which of the following directions should the equipment exhaust face when installed in the rack?
A. Sides
B. Top
C. Front
D. Rear
Answer: D (LEAVE A REPLY)
In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

NEW QUESTION: 25
A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?
A. NS
B. SOA
C. PTR
D. CNAME
Answer: A (LEAVE A REPLY)
To change where the outside DNS records are hosted, the network administrator needs to update the NS (Name Server) records at the domain registrar. NS records specify the authoritative name servers for a domain, directing where DNS queries should be sent.
NS (Name Server) Records: These records indicate the servers that are authoritative for a domain. Changing the NS records at the registrar points DNS resolution to the new hosting provider.
SOA (Start of Authority): Contains administrative information about the domain, including the primary name server.
PTR (Pointer) Records: Used for reverse DNS lookups, mapping IP addresses to domain names.
CNAME (Canonical Name) Records: Used to alias one domain name to another, not relevant for changing DNS hosting.
Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses DNS records, their purposes, and how to manage them.
Cisco Networking Academy: Provides training on DNS management and the role of different DNS record types.
Network+ Certification All-in-One Exam Guide: Explains DNS records and their configuration for domain management.

NEW QUESTION: 26
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: D (LEAVE A REPLY)
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:

NEW QUESTION: 27
Which of the following most likely determines the size of a rack for installation? (Select two).
A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height
Answer: (SHOW ANSWER)
Understanding Rack Size Determination:
The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.
Switch Depth:
Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.

Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.
Server Height:
Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals 1.75 inches. The total height of all equipment determines the overall height requirement of the rack.
Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.
Why Other Options are Less Relevant:
KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.
Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.
Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.
Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.
Reference:
CompTIA Network+ study materials on rack installation and equipment sizing.

NEW QUESTION: 28
A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?
A. 802.1X
B. Access control list
C. Port security
D. MAC filtering
Answer: A (LEAVE A REPLY)
802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means. 802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.Reference:
CompTIA Network+ study materials.

NEW QUESTION: 29
A network engineer is completing a new VoIP installation, but the phones cannot find the TFTP server to download the configuration files. Which of the following DHCP features would help the phone reach the TFTP server?
A. Exclusions
B. Lease time

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

NEW QUESTION: 30
Which of the following will allow secure, remote access to internal applications?
A. VPN
B. CDN
C. SAN
D. IDS
Answer: A (LEAVE A REPLY)
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: 31
Which of the following troubleshooting steps would provide a change advisory board with the information needed to make a decision?
A. Identify the problem.
B. Develop a theory of probable cause.
C. Test the theory to determine cause.
D. Establish a plan of action.
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 32
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: A (LEAVE A REPLY)
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.
Reference:
CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref 9 Basic Configuration Commands).

NEW QUESTION: 33
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: 34

A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed

B. Jumbo frames

C. QoS

D. 802.1q tagging

Answer: B (LEAVE A REPLY)

Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.

Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.

Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).

Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.

Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.

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

NEW QUESTION: 35

An employee has a new laptop and reports slow performance when using the wireless network. Switch firmware was updated the previous night. A network administrator logs in to the switch and sees the following statistics on the switch interface for that employee:

98469 packets input, 1681937 bytes, 0 no buffer

Received 1548 broadcasts (25285 multicasts)

65335 runts, 0 giants, 0 throttles

11546 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored

0 input packets with dribble condition detected

22781 packets output, 858040 bytes, 0 underruns

0 output errors, 89920 collisions, 0 interface resets

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

Which of the following is most likely the cause of the issue?

A. The patch cord from the wall jack is faulty.

B. The switchport bandwidth needs to be increased.

C. Multicast is not configured correctly on the switch.

D. The NIC is set to half duplex.

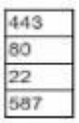
Answer: D (LEAVE A REPLY)

A large number of collisions and input errors typically indicates a duplex mismatch, such as when one device is set to full duplex and the other to half duplex. This leads to communication issues and poor performance. The document explains:

"Collisions and input errors are clear signs of duplex mismatches... typically caused when one device operates in half duplex while the other is in full duplex, causing performance and connectivity issues."

NEW QUESTION: 36

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: B (LEAVE A REPLY)

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 Reference:

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: 37
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: C (LEAVE A REPLY)
* 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: 38
A network administrator performed upgrades on a server and installed a new NIC to improve performance. Following the upgrades, usera are unable to reach the server. Which of the following is the most likely reason.
A. The PoE power budget was exceeded.
B. TX/RX was transposed.
C. A port security violation occured.
D. An incorrect cable type was installed.
Answer: D (LEAVE A REPLY)
When a network administrator installs a new Network Interface Card (NIC) and users are unable to reach the server, one of the common issues is the use of an incorrect cable type. Network cables must match the specifications required by the NIC and the network infrastructure (e.g., Cat5e, Cat6 for Ethernet).
NIC Compatibility: The new NIC might require a specific type of cable to function properly. Using a cable not rated for the NIC's required speeds or capabilities can result in connectivity issues.
Cable Standards: Different NICs and network devices might need different cabling standards (straight-through vs. crossover cables, or specific fiber optic types).
Connection Types: Ensuring that the cable connectors are appropriate for the NIC ports (e.g., RJ45 for Ethernet, LC connectors for fiber optics).
Network Reference:

CompTIA Network+ N10-007 Official Certification Guide: Discusses network cabling standards and NIC specifications.
Cisco Networking Academy: Provides insights into cabling and NIC configurations for optimal network performance.
Network+ Certification All-in-One Exam Guide: Offers comprehensive details on troubleshooting network connectivity issues, including cabling problems.

NEW QUESTION: 39
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: D (LEAVE A REPLY)
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.

NEW QUESTION: 40
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: (SHOW ANSWER)
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.

NEW QUESTION: 41
A support engineer is troubleshooting a network outage that is affecting 3,000 users. The engineer has isolated the issue to the internet firewall. Packet captures confirm that the firewall is blocking the traffic. Which of the following is the next step in troubleshooting?
A. Implement the solution or escalate as necessary
B. Create a plan of action to resolve the issue and identify potential effects
C. Establish a theory of probable cause
D. Document findings, actions, outcomes, and lessons learned throughout the process
Answer: B (LEAVE A REPLY)
The troubleshooting methodology requires following a logical sequence. In this case, the engineer has already identified the problem (firewall blocking traffic) and confirmed it with evidence (packet captures). The next appropriate step is to create a plan of action that outlines how to resolve the issue and considers potential effects.
A . Implementing the solution is premature without planning.
C . Establishing a theory was already completed during problem isolation.
D . Documentation occurs after resolution.
By carefully planning, the engineer ensures that corrective action won't cause additional outages or security issues, especially given the scale of the incident (3,000 users).

NEW QUESTION: 42
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: A (LEAVE A REPLY)
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.
Reference (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs/evil twins), traffic interception, on-path attacks.

NEW QUESTION: 43
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: 44
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: A (LEAVE A REPLY)
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. Reference: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 45
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.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 46
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: D (LEAVE A REPLY)
*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: 47

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.

Reference:

CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9 Basic Configuration Commands).

NEW QUESTION: 48
An organization wants better network visibility. The organization's requirements include:
Multivendor/OS-monitoring capabilities
Real-time collection
Data correlation
Which of the following meets these requirements?
A. SNMP
B. SIEM
C. Nmap
D. Syslog
Answer: B (LEAVE A REPLY)
A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments.
Breakdown of Options:
A). SNMP - SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.
B). SIEM - Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.
C). Nmap - Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.
D). Syslog - Syslog collects logs but does not correlate or analyze them in real-time.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain network security concepts.
NIST Special Publication 800-92: Guide to Computer Security Log Management

NEW QUESTION: 49
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: D (LEAVE A REPLY)
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.Reference: CompTIA Network+ study materials.

NEW QUESTION: 50
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: C (LEAVE A REPLY)
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: 51
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: B (LEAVE A REPLY)
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.Reference: CompTIA Network+ study materials.

NEW QUESTION: 52
A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration: Which of the following is causing the user's issue?
A. Incorrect DNS
B. Unreachable gateway
C. Failed root bridge
D. Poor upstream routing
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 53
A company's VoIP phone connection is cutting in and out. A senior network engineer is recommending the implementation of a voice VLAN. Which of the following should be configured?
A. 802.1Q tagging
B. Jumbo frames
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link. This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.
B . Jumbo frames improve throughput for large data transfers, not voice.
C . Native VLAN is the untagged VLAN, not specifically for voice.
D . Link aggregation bundles links for bandwidth/redundancy, not QoS.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 54
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: B (LEAVE A REPLY)

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: 55
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: D (LEAVE A REPLY)
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.
Reference:
CompTIA Network+ study materials on subnetting and IP addressing.

NEW QUESTION: 56
Which of the following is a major difference between an IPS and IDS?
A. An IPS requires less administrative overhead than an IDS.
B. An IPS needs to be installed in line with traffic and an IDS does not.
C. An IPS is signature-based and an IDS is not.
D. An IPS is less susceptible to false positives than an IDS.
Answer: B (LEAVE A REPLY)
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: 57
A technician is designing a cloud service solution that will accommodate the company's current size, compute capacity, and storage capacity. Which of the following cloud deployment models will fulfill these requirements?
A. SaaS
B. PaaS
C. IaaS
D. IaC
Answer: C (LEAVE A REPLY)
Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.
IaaS Benefits:
Provides virtual machines, storage, and networking resources.
Scalable based on company needs.

Reduces the need for physical infrastructure.
Incorrect Options:
A: SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.
B: PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.
D: IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Cloud Computing Models

NEW QUESTION: 58
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 as show spanning-tree to 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.
Reference:
CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

NEW QUESTION: 59
A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and

sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?

A. Theswitch failed.

B. Thedefault gateway is wrong.

C. Theport Is shut down.

D. TheVLAN assignment is incorrect.

Answer: C (LEAVE A REPLY)

When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue. Here is the detailed reasoning:

* Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.

* No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.

* Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.

Command to Check and Enable Port:

bash

Copy code

Switch> enable

Switch# configure terminal

Switch(config)# interface [interface id]

Switch(config-if)# no shutdown

* The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.

Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

NEW QUESTION: 60

Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?

A. Router

B. Switch

C. Access point

D. Firewall

Answer: (SHOW ANSWER)

An access point (AP) provides users with an extended footprint that allows connections from multiple devices within a designated Wireless Local Area Network (WLAN).

Router: Typically used to connect different networks, not specifically for extending wireless coverage.

Switch: Used to connect devices within a wired network, not for providing wireless access.

Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.
Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.
Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

NEW QUESTION: 61
A company recently experienced outages of one of its critical, customer-facing applications. The root cause was an overutilized network router, but the Chief Technology Officer is concerned that the support staff was unaware of the issue until notified by customers. Which of the following is the best way to address this issue in the future?
A. Packet capture
B. SNMP
C. Syslog collector
D. SIEM
Answer: B (LEAVE A REPLY)
The best answer is SNMP (Simple Network Management Protocol). SNMP enables monitoring of network devices (routers, switches, firewalls, servers) and provides performance data such as CPU usage, bandwidth utilization, and interface status. In this scenario, if SNMP monitoring had been in place, administrators would have received alerts that the router was overutilized before customers noticed outages.
A . Packet capture (e.g., Wireshark) is useful for deep troubleshooting but is reactive, not proactive, and not scalable for continuous monitoring.
C . Syslog collects log messages but generally does not provide proactive resource utilization metrics. It is complementary but not the best fit for this problem.
D . SIEM aggregates logs and security events for analysis, but the primary requirement here is performance and availability monitoring.
By implementing SNMP monitoring (and potentially integrating it with a network monitoring tool such as Nagios, PRTG, or SolarWinds), the organization can track utilization trends, set thresholds, and automatically generate alerts, thereby preventing downtime from going unnoticed.

NEW QUESTION: 62
Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?
A. Rack
B. Patch
C. MDF
D. UPS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
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. Platform as a service
C. Software as a service
D. Network as a service
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
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: D (LEAVE A REPLY)
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:

NEW QUESTION: 65
Which of the following objectives does an evil twin achieve?
A. DNS poisoning
B. Login credentials
C. ARP spoofing
D. Denial of service
Answer: B (LEAVE A REPLY)
An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.
A . DNS poisoning manipulates DNS resolution but is not inherent to evil twin.
C . ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.
D . Denial of service can be a side effect but is not the primary objective of evil twin attacks.
The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.

NEW QUESTION: 66
Which of the following would an adversary do while conducting an evil twin attack?
A. Trick users into using an AP with an SSID that is identical to a legitimate network
B. Manipulate address resolution to point devices to a malicious endpoint
C. Present an identical MAC to gain unauthorized access to network resources
D. Capture data in transit between two legitimate endpoints to steal data
Answer: A (LEAVE A REPLY)
An evil twin attack sets up a rogue AP with the same SSID as a legitimate wireless network, tricking users into connecting. Once connected, the attacker can intercept traffic or harvest credentials.
B . Describes ARP spoofing.
C . Describes MAC spoofing.
D . Describes on-path attacks, which may follow, but the evil twin method begins with SSID impersonation.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 67
Which of the following tools uses ICMP to help determine whether a network host is reachable?
A. tcpdump
B. netstat
C. nslookup
D. ping
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 68
Which of the following protocols uses the Dijkstra's Link State Algorithm to establish routes inside its routing table?
A. OSPF
B. EIGRP
C. BGP
D. RIP
Answer: A (LEAVE A REPLY)
OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.
From Andrew Ramdayal's guide:
"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

NEW QUESTION: 69
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: A (LEAVE A REPLY)
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:

NEW QUESTION: 70
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: B (LEAVE A REPLY)
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.
Reference:
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: 71
A network administrator needs to assign IP addresses to a newly installed network. They choose 192.168.1.0/24 as their network address and need to create three subnets with 30 hosts on each subnet. Which of the following is a valid subnet mask that will meet the requirements?
A. 255.255.255.128

B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240
Answer: C (LEAVE A REPLY)
Understanding the Requirements
Network Address: 192.168.1.0/24
The /24 notation means a subnet mask of 255.255.255.0, providing 256 total addresses (192.168.1.0-192.168.1.255).
Usable hosts: 256 - 2 (network and broadcast) = 254.
Goal: Create 3 subnets, each with 30 hosts.
Each subnet needs enough addresses to accommodate 30 hosts, plus 2 reserved addresses (network and broadcast) per subnet.
Total addresses per subnet = 30 (hosts) + 2 (network/broadcast) = 32 addresses.
Subnetting Basics (Networking Fundamentals)
Subnet Mask: Determines how many bits are borrowed from the host portion to create subnets.
Original Mask: /24 (255.255.255.0) = 24 network bits, 8 host bits.
Formulae:
Number of subnets = 2^(number of borrowed bits).
Number of addresses per subnet = 2^(remaining host bits).
Usable hosts per subnet = 2^(remaining host bits) - 2.
We need:
At least 3 subnets.
At least 32 addresses per subnet (to fit 30 hosts + 2 reserved).
Step-by-Step Analysis
Determine Addresses Needed per Subnet:
32 addresses is a power of 2 (2^5 = 32).
This means each subnet requires 5 host bits (since 2^5 = 32 total addresses, and 32 - 2 = 30 usable hosts).
Calculate Remaining Bits:
Original network has 8 host bits (/24).
If 5 bits are left for hosts, we borrow: 8 - 5 = 3 bits for subnetting.
New Subnet Mask:
Original mask: /24 (24 network bits).
Borrow 3 bits: 24 + 3 = /27.
/27 = 255.255.255.224 (binary: 11111111.11111111.11111111.11100000).
Verify Requirements:
Number of Subnets: 2^3 = 8 subnets (meets the requirement of at least 3).
Addresses per Subnet: 2^5 = 32 addresses.
Usable Hosts per Subnet: 32 - 2 = 30 hosts (exactly meets the requirement).
Subnet Breakdown:
Increment: 256 - 224 = 32 (each subnet increments by 32 in the fourth octet).

Subnets:
192.168.1.0-192.168.1.31 (Network: .0, Broadcast: .31, Hosts: .1-.30)
192.168.1.32-192.168.1.63 (Network: .32, Broadcast: .63, Hosts: .33-.62)
192.168.1.64-192.168.1.95 (Network: .64, Broadcast: .95, Hosts: .65-.94) (And 5 more subnets up to 192.168.1.255.) Three subnets fit perfectly with 30 hosts each.
Evaluating the Options
A . 255.255.255.128 (/25):
Borrow 1 bit: 24 + 1 = /25.
Subnets: 2^1 = 2 (not enough, need 3).
Host bits: 7 (2^7 = 128 addresses, 126 hosts).
Why Not: Only 2 subnets, fails the requirement.
B . 255.255.255.192 (/26):
Borrow 2 bits: 24 + 2 = /26.
Subnets: 2^2 = 4 (meets 3).
Host bits: 6 (2^6 = 64 addresses, 62 hosts).
Why Not: 62 hosts exceeds 30, but it's overkill; /27 is more efficient and still valid.
C . 255.255.255.224 (/27):
Borrow 3 bits: 24 + 3 = /27.
Subnets: 2^3 = 8 (meets 3).
Host bits: 5 (2^5 = 32 addresses, 30 hosts).
Why Yes: Perfectly fits 3 subnets with exactly 30 hosts each.
D . 255.255.255.240 (/28):
Borrow 4 bits: 24 + 4 = /28.
Subnets: 2^4 = 16 (meets 3).
Host bits: 4 (2^4 = 16 addresses, 14 hosts).
Why Not: Only 14 hosts per subnet, fails the 30-host requirement.
Why /27 (255.255.255.224) is Best
It provides exactly 30 usable hosts per subnet, avoiding waste while meeting the minimum requirement.
It allows 8 subnets, exceeding the need for 3, ensuring flexibility.
The study guide emphasizes efficient subnet design, and /27 balances host count and subnet availability.
CompTIA Network+ Context
Networking Fundamentals: Subnetting is a core skill, requiring understanding of CIDR, binary conversion, and address allocation.
Example from Study Guide: Similar problems calculate subnet masks for specific host counts, reinforcing /27 as a common solution for ~30 hosts.

NEW QUESTION: 72
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: D (LEAVE A REPLY)
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 Reference:
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: 73
A user's home mesh wireless network is experiencing latency issues. A technician has:
*Performed a speed test.
*Rebooted the devices.
*Performed a site survey.
*Performed a wireless packet capture.
The technician reviews the following information:
The technician notices in the packet capture that frames were retransmitted. Which of the following is the most likely cause of the user's network issue?
A. The SSIDs should not be the same.
B. The network has too much overlap.
C. The devices are incompatible with the mesh network.
D. The nodes are underpowered.
Answer: (SHOW ANSWER)
*Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
*Same SSIDs (A) are expected in mesh networks.
*Device compatibility (C) would show different symptoms.

*Node power (D) affects coverage, not congestion.
#Reference: CompTIA Network+ N10-009 Official Documentation - Wireless Troubleshooting & Signal Interference.

NEW QUESTION: 74
Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the attackers' activities?
A. Geofencing
B. Honeynet
C. Jumpbox
D. Screened subnet
Answer: B (LEAVE A REPLY)
A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. Reference: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 75
A network administrator's device is experiencing severe Wi-Fi interference within the corporate headquarters causing the device to constantly drop off the network. Which of the following is most likely the cause of the issue?
A. Too many client connections
B. Too many wireless repeaters
C. Too much wireless absorption
D. Too much wireless reflection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 76
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: B (LEAVE A REPLY)
Understanding the 169.254.x.x Address:

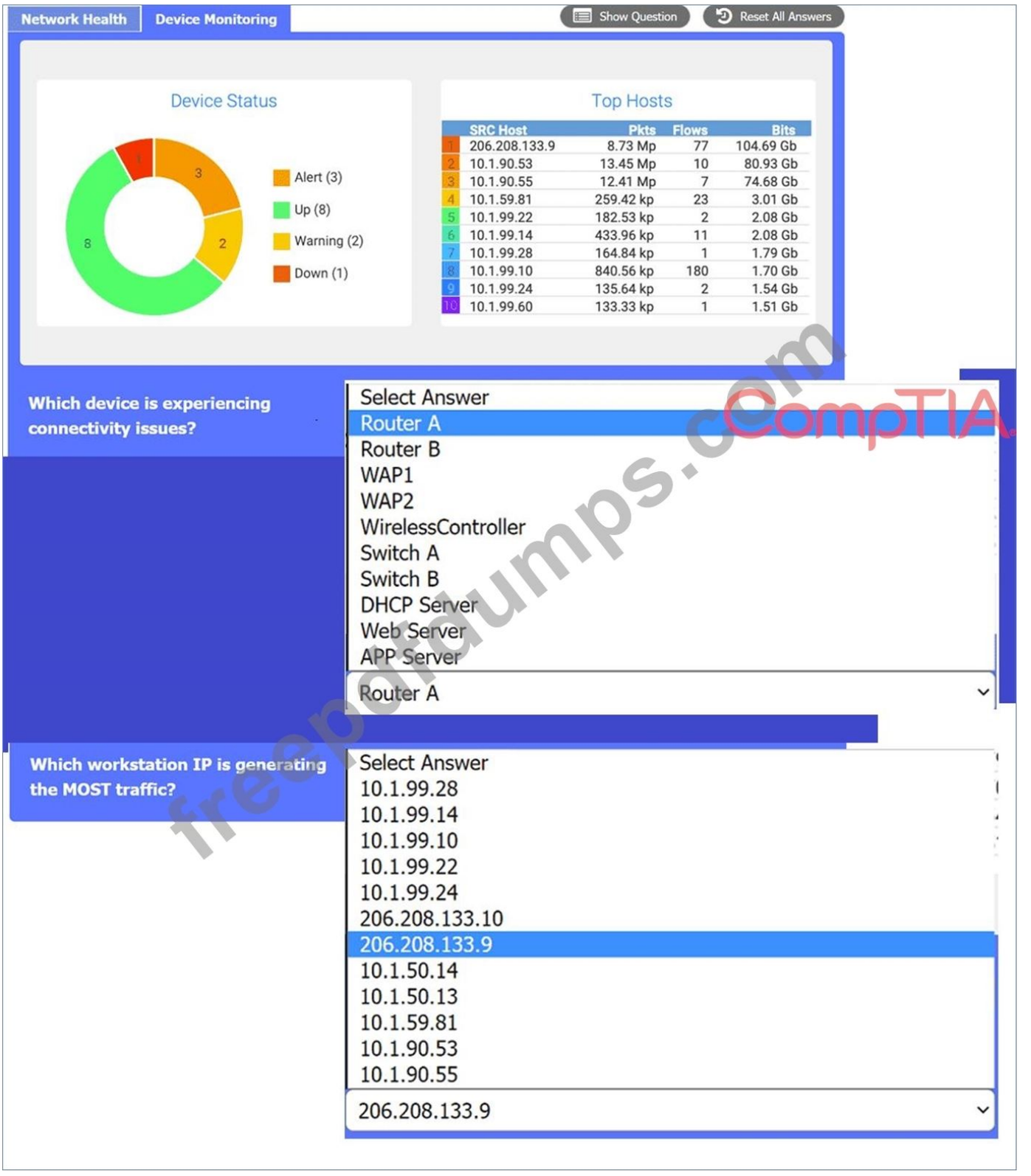
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.
DHCP Server Offline:
APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network 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).
Reference:
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

NEW QUESTION: 77
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: (SHOW ANSWER)

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: 78
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: 79
SIMULATION
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.



Answer:

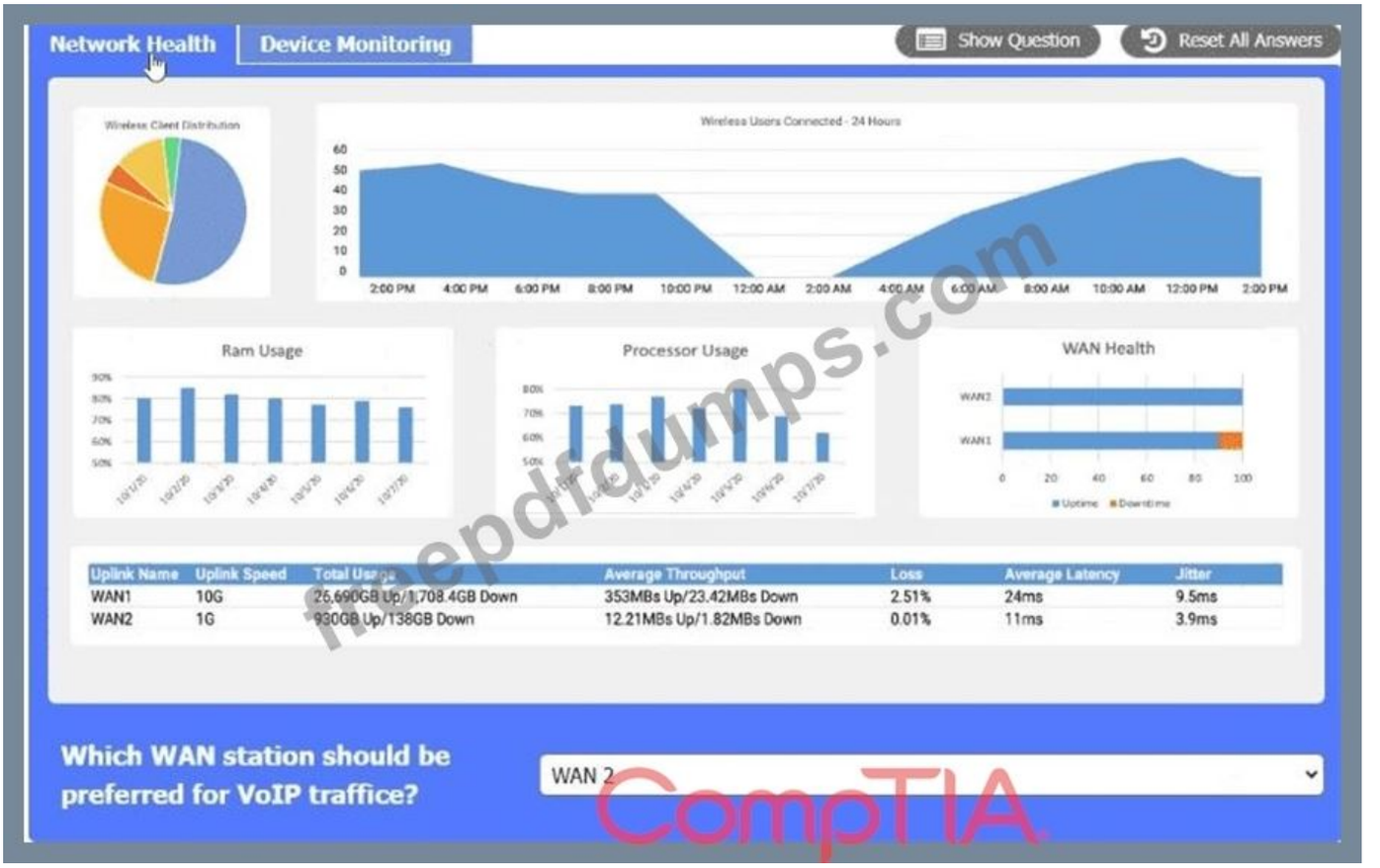
See the solution below in Explanation

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

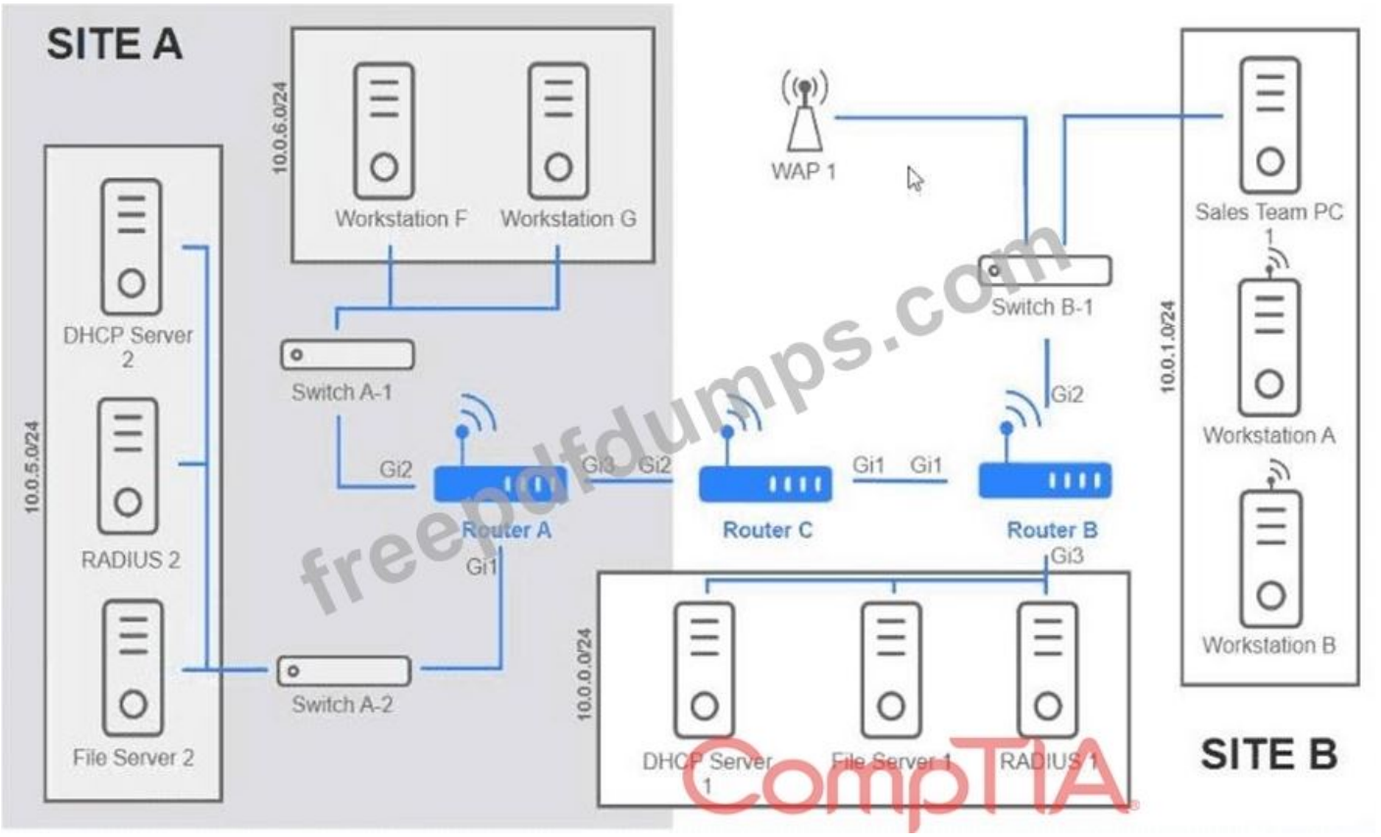
good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.
Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:
WAN 1:
Uplink Speed: 10G
Total Usage: 26.969GB Up / 1.748GB Down
Average 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 dat a. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.



NEW QUESTION: 80
Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?
A. Access, distribution, and core
B. Core, root, and distribution
C. Core, spine, and leaf
D. Access, core, and roof
Answer: (SHOW ANSWER)
The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. Reference: CompTIA Network + Exam Objectives and official study guides.

NEW QUESTION: 81
SIMULATION
Users are unable to access files on their department share located on flle_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS

Click on each router to review output, identity any Issues, and configure the appropriate solution If at any time you would like to bring back the initial state of trie simulation, please click the reset All button;

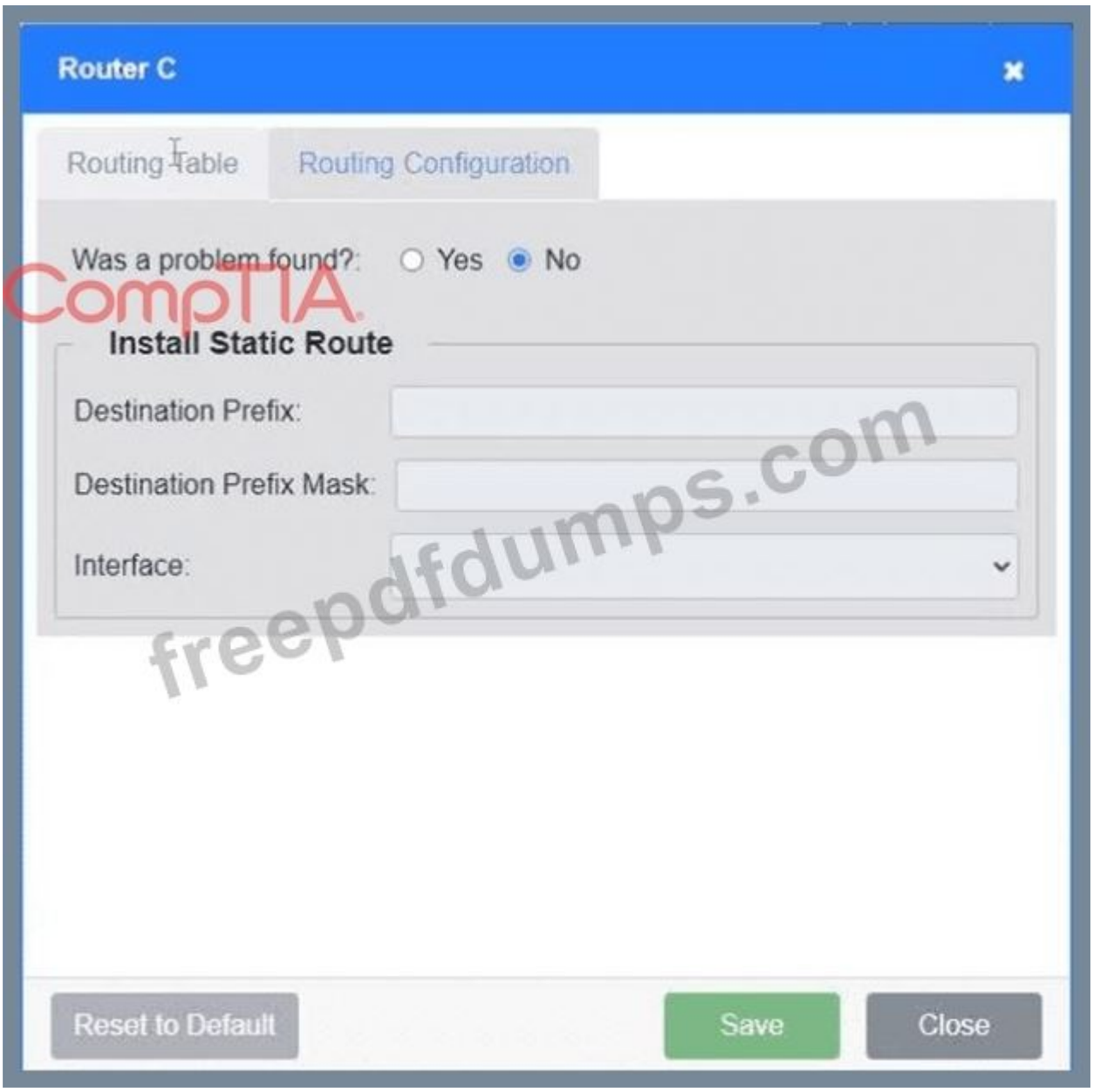


Answer:

See the solution configuration below in Explanation

Explanation:

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



NEW QUESTION: 82
A firewall administrator is mapping a server's internal IP address to an external IP address for public use. Which of the following is the name of this function?
A. NAT
B. VIP
C. PAT
D. BGP
Answer: A (LEAVE A REPLY)
Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.
Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.

Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.
PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.
Incorrect Options:
B . VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.
C . PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.
D . BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

NEW QUESTION: 83
A network technician is designing a LAN for a new facility. The company is expecting more than 300 devices to connect to the network. Which of the following masks will provide the most efficient subnet?
A. 255.255.0.0
B. 255.255.192.0
C. 255.255.254.0
D. 255.255.255.254
Answer: C (LEAVE A REPLY)
The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.
* 255.255.0.0 (/16) provides too many addresses.
* 255.255.192.0 (/18) gives 16384 addresses - overkill.
* 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).
From Andrew Ramdayal's guide:
"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

NEW QUESTION: 84
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 dat a. Which of the following is the minimum version of SNMP that supports this requirement?
A. v1
B. v2c
C. v2u
D. v3

Answer: D (LEAVE A REPLY)
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.Reference: CompTIA Network+ study materials.

NEW QUESTION: 85
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: A (LEAVE A REPLY)
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: 86
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: C (LEAVE A REPLY)
* 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.

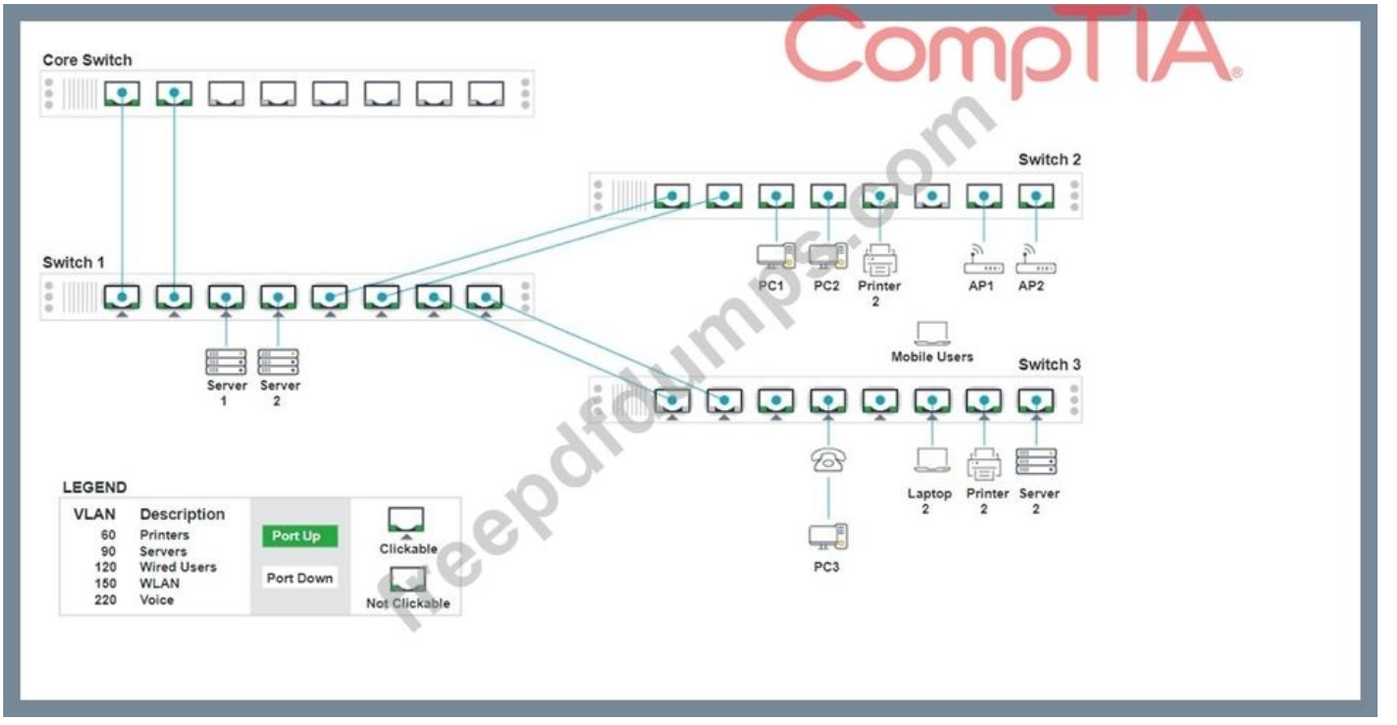
* Incorrect Options:
* A. "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
* B. "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
* 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.

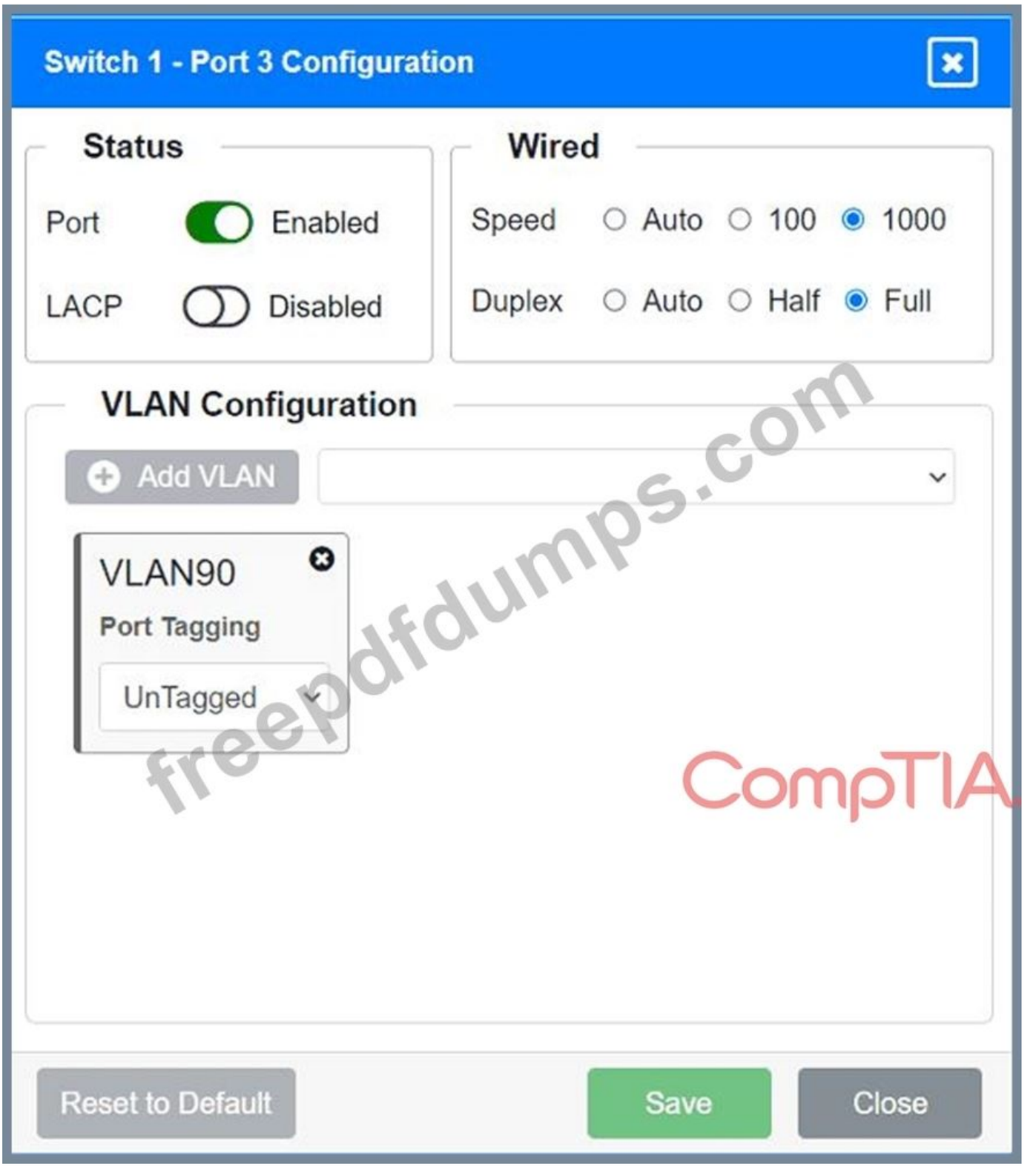
NEW QUESTION: 87
A network engineer discovers network traffic that is sending confidential information to an unauthorized and unknown destination. Which of the following best describes the cause of this network traffic?
A. Adware
B. Ransomware
C. Darkware
D. Malware
Answer: D (LEAVE A REPLY)
Malware 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

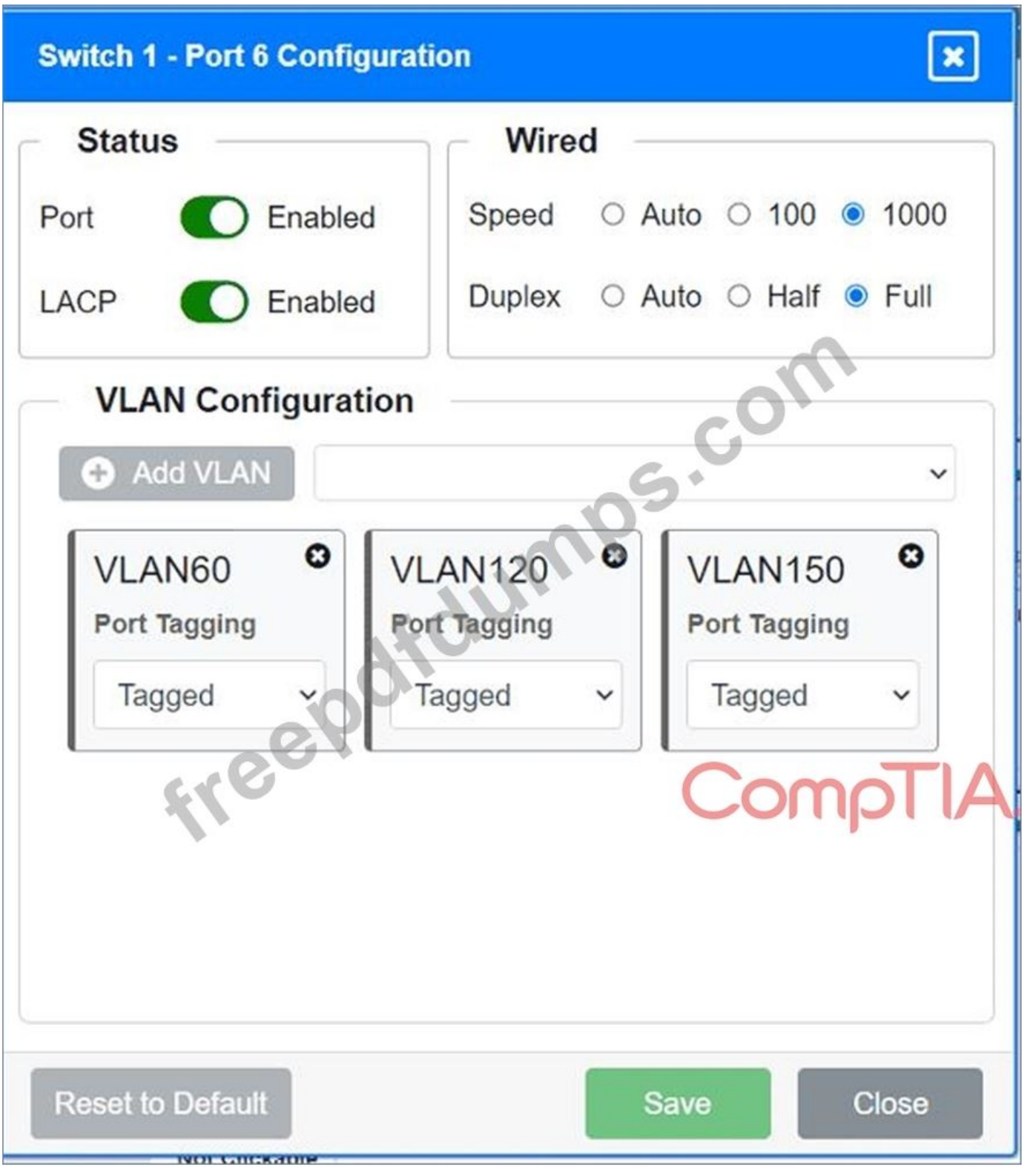
NEW QUESTION: 88
A new backup system takes too long to copy files to the new SAN each night. A network administrator makes a simple change to the network and the devices to decrease backup times. Which of the following does the network administrator change?
A. QoS
B. SDN
C. MTU
D. VXLAN
E. TTL
Answer: C (LEAVE A REPLY)

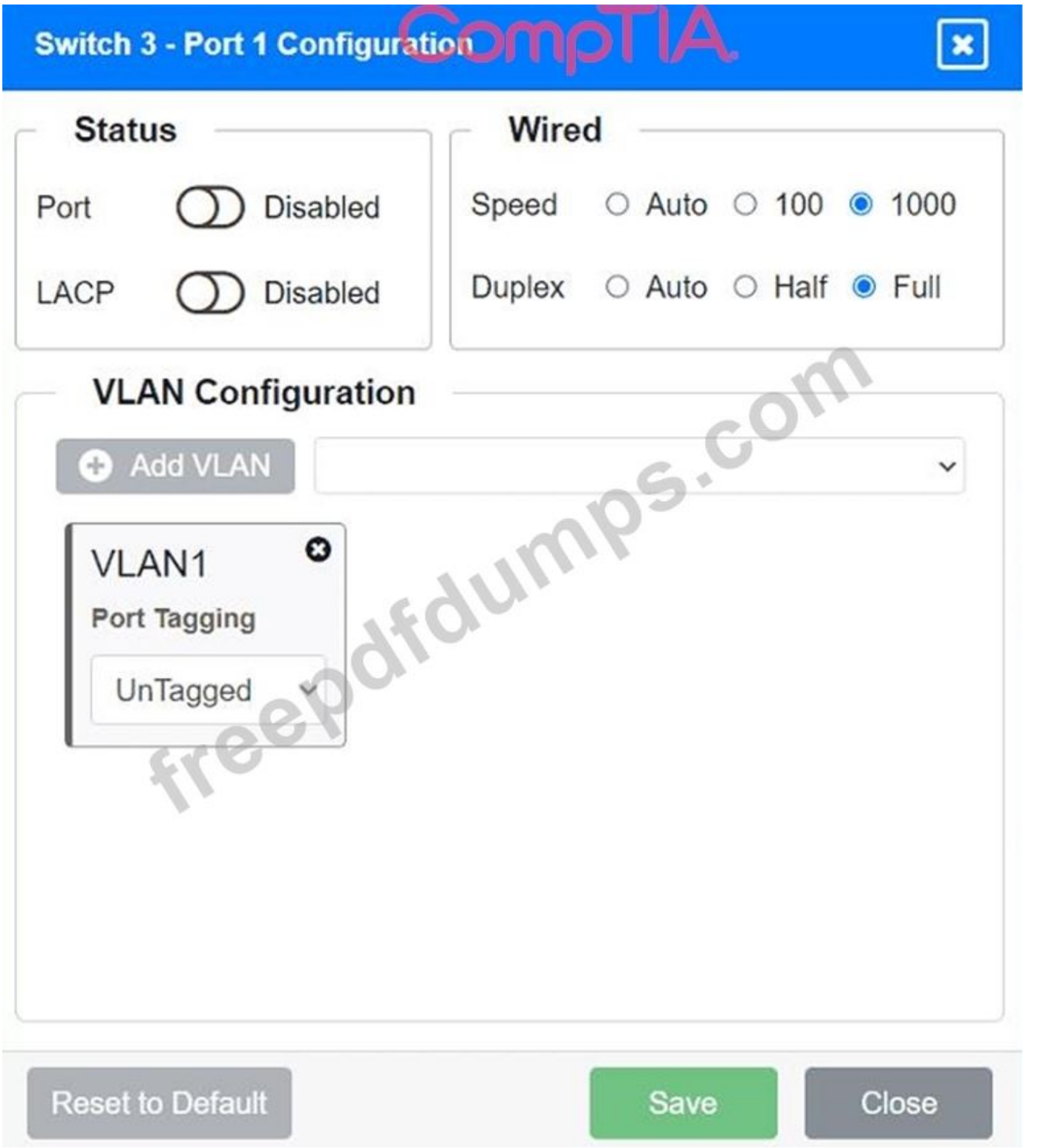
Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput - especially for large file transfers like backups.
A . QoS prioritizes traffic but doesn't reduce backup times directly.
B . SDN is a network management model, not a parameter change.
D . VXLAN encapsulates VLANs, not relevant to backup speeds.
E . TTL is for packet lifetime, not throughput.
Reference:
Domain: Network Infrastructure - MTU, jumbo frames, performance tuning.

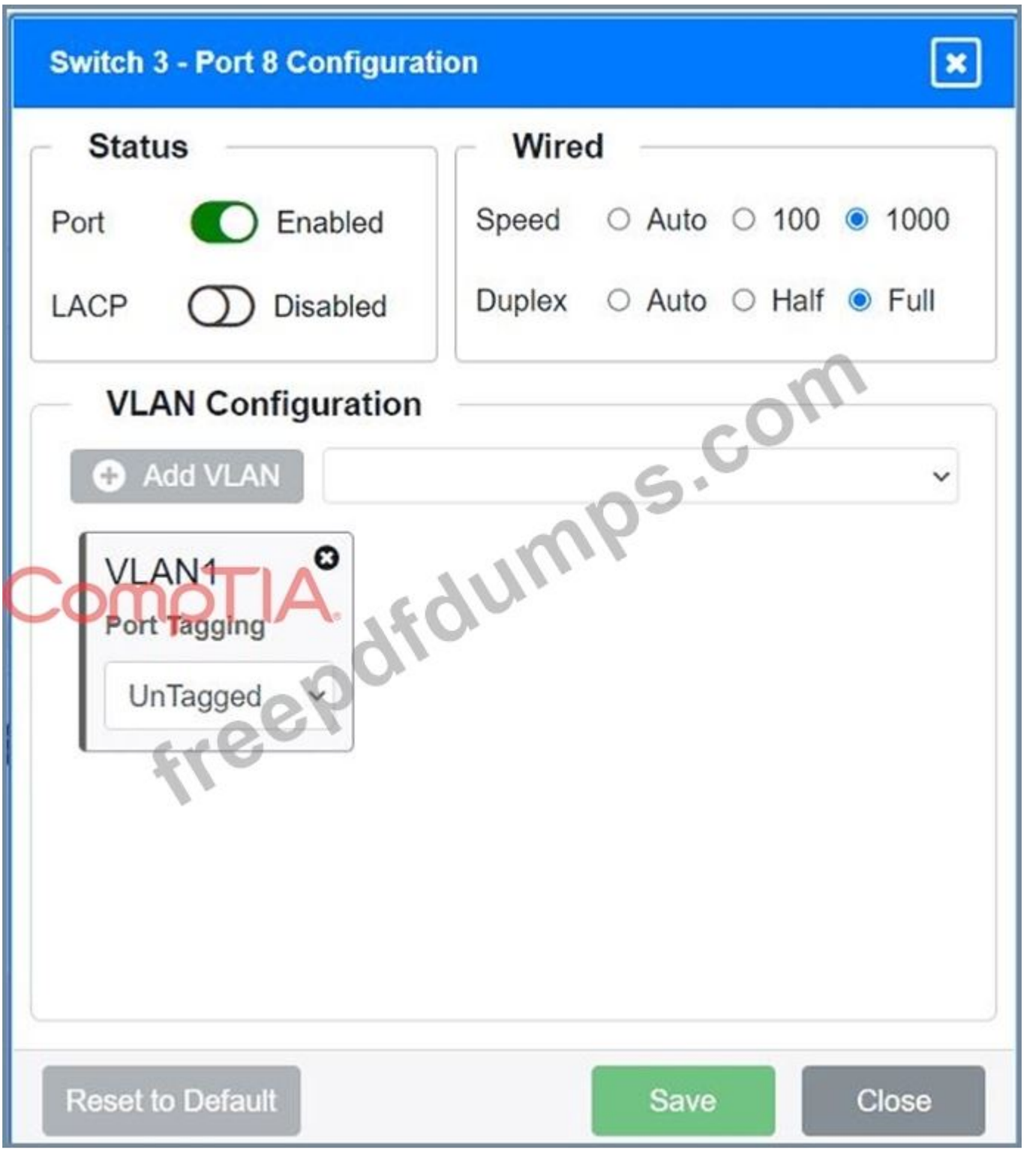
NEW QUESTION: 89
SIMULATION
A network technician replaced an access layer switch and needs to reconfigure it to allow the connected devices to connect to the correct networks.
INSTRUCTIONS
Click on the appropriate port(s) on Switch 1 and Switch 3 to verify or reconfigure the correct settings:
* Ensure each device accesses only its
correctly associated network.
* Disable all unused switchports.
. Require fault-tolerant connections
between the switches.
. Only make necessary changes to
complete the above requirements.











Answer:

See the solution below in Explanation

Explanation:

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

Identify the correct VLANs for each device and port.

Enable necessary ports and disable unused ports.

Configure fault-tolerant connections between the switches.

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

NEW QUESTION: 90

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: C (LEAVE A REPLY)

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: 91

A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business. When attempting to connect, two networks are listed as possible choices: SSID: business and SSID: myaccess. Which of the following attacks is occurring?

A. On-path

B. Rogue AP

C. Evil twin

D. Tailgating

Answer: (SHOW ANSWER)

An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.

A . On-path is the consequence of connecting to the evil twin, not the initial attack itself.

B . Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID - specifically an evil twin.

D . Tailgating is a physical social engineering attack, unrelated to Wi-Fi.

Reference (CompTIA Network+ N10-009):

Domain: Network Security - Wireless threats (rogue APs, evil twins).

NEW QUESTION: 92

SIMULATION

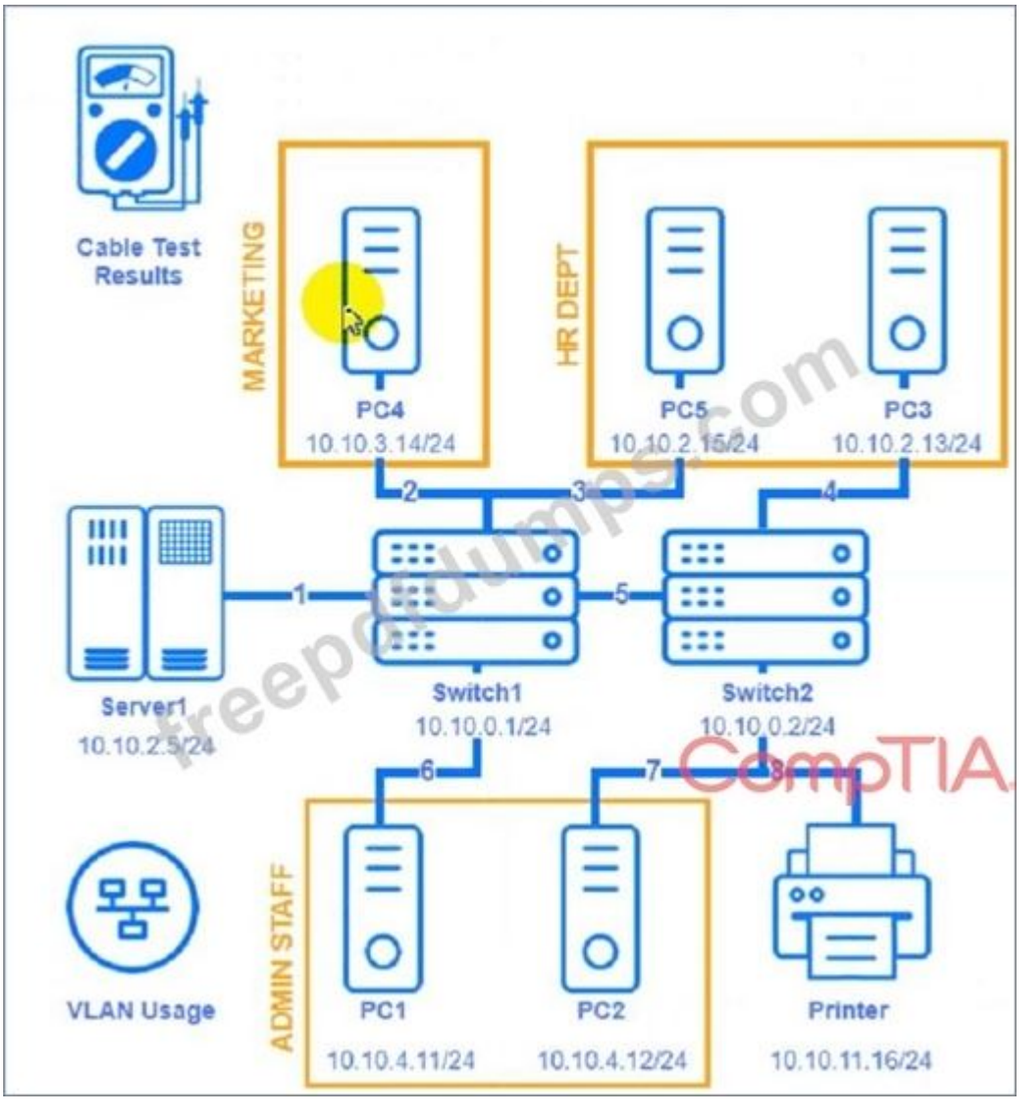
A network technician needs to resolve some issues with a customer's SOHO network.

The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.

INSTRUCTIONS

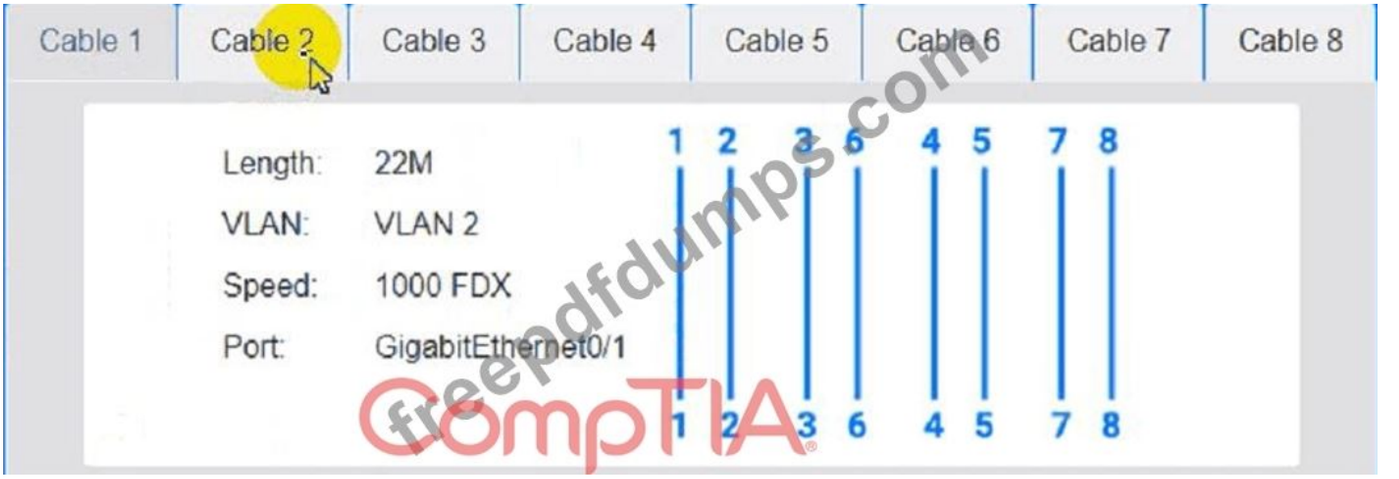
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.



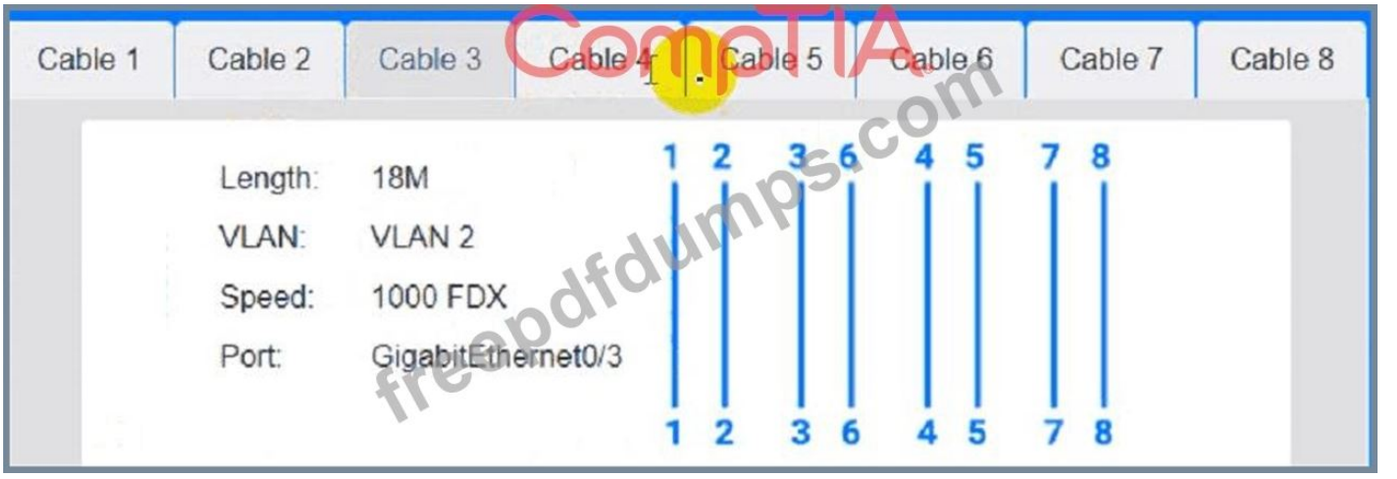
Cable Test Results:

Cable 1:

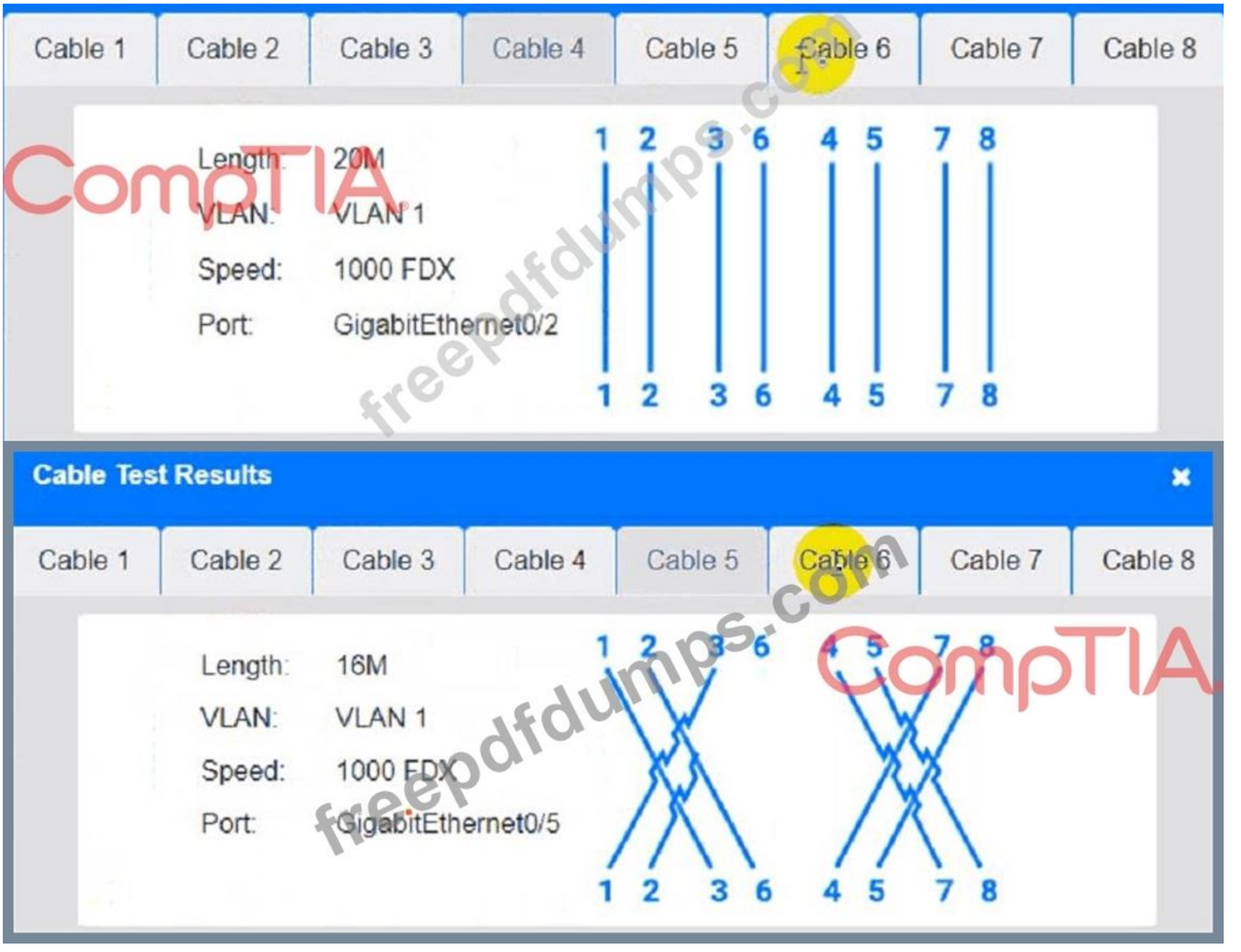


Cable 2:

Cable 3:



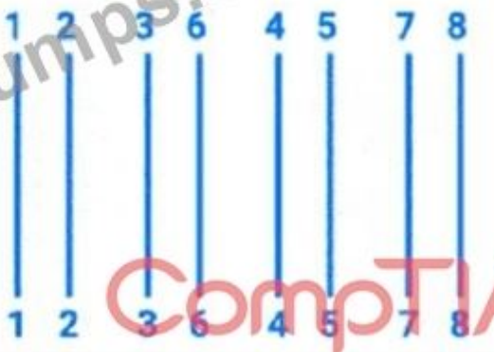
Cable 4:



Cable Test Results

Cable 1 | Cable 2 | Cable 3 | Cable 4 | Cable 5 | Cable 6 | Cable 7 | Cable 8

Length: 12M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/1



Printer

HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC, http://192.168.2.9
Firmware Revision	FDP1CN1347AR
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

Hardware Address (MAC)	9c:b6:54:4d:30:ec

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 troubleshoot all the network components and review the cable test results, you can use the following steps:

Click on each device and cable to open its information window.

Review the information and identify any problems or errors that may affect the network connectivity or performance.

Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.

Fill in the remediation form using the drop-down menus provided.

Here is an example of how to fill in the remediation form for PC1:

The component with a problem is PC1.

The problem is Incorrect IP address.

The solution is Change the IP address to 192.168.1.10.
You can use the same steps to fill in the remediation form for other components.
To enter commands in each device, you can use the following steps:
Click on the device to open its terminal window.
Enter the command ipconfig /all to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.
Enter the command ping <IP address> to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
Enter the command tracert <IP address> to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values. Replace <IP address> with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.
Here is an example of how to enter commands in PC1:
Click on PC1 to open its terminal window.
Enter the command ipconfig /all to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.
Enter the command ping 192.168.1.1 to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.
Enter the command tracert 192.168.1.1 to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.
You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION: 93
A network engineer is installing new PoE wireless APs. The first five APs deploy successfully, but the sixth one fails to start. Which of the following should the engineer investigate first?
A. Signal strength
B. Duplex mismatch
C. Power budget
D. CRC
Answer: (SHOW ANSWER)
When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.
A . Signal strength affects wireless connectivity, not whether the AP powers up.
B . Duplex mismatch causes poor throughput, not power failure.
D . CRC errors point to cabling issues but do not prevent booting if no power is available.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 94

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: 95

A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?

A. Trusted zones

B. URL filtering

C. ACLs

D. Screened subnet

Answer: D (LEAVE A REPLY)

Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.

NEW QUESTION: 96

A network engineer connects a business to a new ISP. A simple ping test to 8.8.8.8 is successful. However, users complain of extreme slowness to any website and periods of no connectivity. Which of the following is the most likely cause?

A. Incorrect default gateway

B. VLAN mismatch

C. Subnet mask configuration

D. Duplicate ISP IP address

Answer: D (LEAVE A REPLY)

If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain

conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.
A . If the default gateway were incorrect, no external connectivity would work at all.
B . VLAN mismatch is an internal issue, not affecting ISP routing.
C . Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 97
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: 98
A secure communication link needs to be configured between data centers via the internet. The data centers are located in different regions. Which of the following is the best protocol for the network administrator to use?
A. DCI
B. GRE
C. VXLAN
D. IPSec
Answer: D (LEAVE A REPLY)
IPSec (Internet Protocol Security) is the best choice for secure communication over the internet, as it provides encryption, authentication, and data integrity. It is widely used in VPNs and site-to-site secure tunnels.
Breakdown of Options:

A . DCI (Data Center Interconnect) - A general term for linking data centers, but it doesn't specify a secure tunneling protocol.
B . GRE (Generic Routing Encapsulation) - Encapsulates traffic but lacks encryption, making it less secure than IPSec.
C . VXLAN (Virtual Extensible LAN) - Used for Layer 2 network overlays, not for securing communication over the internet.
D . IPSec - ✅ Correct answer. Provides encryption, authentication, and integrity for data over the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement secure remote access methods.
RFC 4301: Security Architecture for the Internet Protocol

NEW QUESTION: 99
An employee in a corporate office clicks on a link in an email that was forwarded to them. The employee is redirected to a splash page that says the page is restricted. Which of the following security solutions is most likely in place?
A. DLP
B. Captive portal
C. Content filtering
D. DNS sinkholing
Answer: C (LEAVE A REPLY)
Content filtering blocks access to restricted or malicious websites. When a user attempts to visit a site that violates company policies, they are redirected to a restriction page.
* This is a common security measure to prevent employees from accessing phishing or malware-infected sites.
* Content filters work by scanning URLs, keywords, or categories and blocking inappropriate or harmful content.
* Option A (DLP - Data Loss Prevention): Focuses on preventing sensitive data leaks rather than blocking web access.
* Option B (Captive portal): Used mainly in public Wi-Fi to authenticate users before granting access, not to restrict sites.
* Option D (DNS sinkholing): Redirects malicious domain requests to a safe address but is not responsible for policy-based restrictions on general content.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Security Solutions

NEW QUESTION: 100
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: 101
A network administrator deployed wireless networking in the office are
a. When users visit the outdoor patio and try to download emails with large attachments or stream training videos, they notice buffering issues. Which of the following is the most likely cause?
A. Network congestion
B. Wireless interference
C. Signal degradation
D. Client disassociation
Answer: C (LEAVE A REPLY)
The most likely cause of buffering issues when moving outdoors is signal degradation. Wireless signals weaken as they travel through obstacles such as walls, glass, and air, leading to weaker connections and reduced data rates.
Breakdown of Options:
A . Network congestion - While congestion can slow down network speeds, it affects all users, not just those moving outdoors.
B . Wireless interference - Interference is possible but is more likely caused by other wireless signals rather than outdoor movement.

C . Signal degradation - Correct answer. Wireless signals weaken with distance and obstacles such as walls, reducing performance.
D . Client disassociation - Disassociation occurs when clients lose connection to the AP, but the question states that users experience buffering, indicating they are still connected but with a weak signal.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Analyze wireless networking technologies.
IEEE 802.11 standards: Wi-Fi propagation characteristics

NEW QUESTION: 102
A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?
A. SNMP trap
B. Port mirroring
C. Syslog collection
D. API integration
Answer: B (LEAVE A REPLY)
Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring.Reference: CompTIA Network+ study materials.

NEW QUESTION: 103
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.
Reference (CompTIA Network+ N10-009):
Domain: Networking Concepts - VPN types, split vs. full tunnel, remote access.

NEW QUESTION: 104

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

NEW QUESTION: 105
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: 106
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: D (LEAVE A REPLY)
*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: 107
Which of the following connector types would most likely be used to connect to an external antenna?
A. BNC
B. ST
C. LC
D. MPO
Answer: (SHOW ANSWER)
BNC connectors are commonly used for coaxial cables, including those connecting to external antennas in Wi- Fi, radio, and surveillance systems.
Breakdown of Options:
A). BNC - Correct answer. Used for coaxial cables in wireless and antenna connections.
B). ST - Used for fiber optic cables, not antennas.
C). LC - A fiber optic connector, not for antennas.
D). MPO - Used for multi-fiber optic cables, not RF antennas.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.
IEEE 802.11: Wireless standards and antenna connectors

NEW QUESTION: 108
A customer recently moved into a new office and notices that some wall plates are not working and are not properly labeled Which of the following tools would be best to identify the proper wiring in the IDF?

A. Toner and probe
B. Cable tester
C. Visual fault locator
D. Network tap
Answer: A (LEAVE A REPLY)
A toner and probe tool, also known as a tone generator and probe, is used to trace and identify individual cables within a bundle or to locate the termination points of cables in wiring closets and patch panels. It generates a tone that can be picked up by the probe, helping technicians quickly and accurately identify and label wall plates and wiring. This is the best tool for identifying proper wiring in the Intermediate Distribution Frame (IDF). Reference: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 109
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: D (LEAVE A REPLY)
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.

NEW QUESTION: 110
An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?

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

NEW QUESTION: 111
Which of the following is the MOST appropriate solution to extend the network to a building located across the street from the main facility?
A. Multimode fiber
B. 802.11ac wireless bridge
C. Cat 6 copper
D. Loopback adapter
Answer: (SHOW ANSWER)
An802.11ac wireless bridgeis the most practical solution to connect two nearby buildingswithout trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.
* A. Multimode fiberis effective but expensive and typically limited to 500 meters or less.
* C. Cat 6 copperis only rated for up to 100 meters - not viable for a street-wide distance.

* D. Loopback adapteris a troubleshooting tool, not for network extension.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 1.3 - Compare and contrast various network topologies, types, and technologies.

NEW QUESTION: 112
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. ipconfig
B. tracert
C. nmap
D. arp
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
A network administrator is reviewing a production web server and observes the following output from the netstat command:
Which of the following actions should the network administrator take to harden the security of the web server?
A. Disable the unused ports.
B. Enforce access control lists.
C. Perform content filtering.
D. Set up a screened subnet.
Answer: A (LEAVE A REPLY)
The netstat output shows that multiple ports are open, including Telnet (23), FTP (20), and TFTP (69), which are potential security risks. Disabling unused ports minimizes the attack surface, reducing security vulnerabilities.
Breakdown of Options:
A). Disable the unused ports - Correct answer. Unused ports should be closed to prevent unauthorized access.
B). Enforce access control lists - ACLs help control access but do not disable unnecessary services.
C). Perform content filtering - Content filtering controls web traffic, not port security.
D). Set up a screened subnet - A DMZ (screened subnet) improves security but does not address open ports.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Given a scenario, implement network security measures.
CIS Benchmark for Linux & Windows Server Hardening

NEW QUESTION: 114
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: C (LEAVE A REPLY)
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.

NEW QUESTION: 115
Which of the following would most likely be used to implement encryption in transit when using HTTPS?
A. SSH
B. TLS
C. SCADA
D. RADIUS
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.
A . SSH secures remote shell and tunnels, not HTTPS.
C . SCADA refers to industrial control systems, not a transport security protocol.
D . RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 116
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: C (LEAVE A REPLY)
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: 117
An organization has four departments that each need access to different resources that do not overlap. Which of the following should a technician configure in order to implement and assign an ACL?
A. VLAN
B. DHCP
C. VPN
D. STP
Answer: A (LEAVE A REPLY)
VLANs (Virtual Local Area Networks) segment network traffic by department, allowing ACLs (Access Control Lists) to be applied based on VLAN membership, improving security and resource isolation.
Breakdown of Options:
A). VLAN - Correct answer. VLANs enable logical network segmentation, allowing ACLs per department.
B). DHCP - Assigns IP addresses but does not control access.
C). VPN - Provides remote access, not segmentation within a network.
D). STP - Prevents switching loops, not related to ACL implementation.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain VLANs and network segmentation.
IEEE 802.1Q: VLAN tagging standard

NEW QUESTION: 118
Which of the following allows for interactive, secure remote management of a network infrastructure device?
A. SSH
B. VNC
C. RDP
D. SNMP
Answer: (SHOW ANSWER)
SSH (Secure Shell) is a cryptographic network protocol that enables secure remote management and operation of network devices, including routers and switches. SSH encrypts traffic, making it more secure than alternatives like Telnet, which sends data in plaintext. The document states: "SSH (Secure Shell) is the recommended protocol for secure, interactive remote management of network devices. It provides a secure channel over an unsecured network by encrypting the traffic between the administrator's workstation and the managed device."

NEW QUESTION: 119
A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?
A. 802.1Q tagging
B. Jumbo frames
C. Half duplex
D. Link aggregation
Answer: D (LEAVE A REPLY)
Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.
IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

NEW QUESTION: 120

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: 121
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.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 122
A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).
A. Mesh network
B. 5GHz frequency
C. Omnidirectional antenna
D. Non-overlapping channel
E. Captive portal
F. Ad hoc network
Answer: B (LEAVE A REPLY)
Understanding 2.4GHz Interference:
The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
Mitigation Strategies:
5GHz Frequency:
The 5GHz frequency band offers more channels and less interference compared to the 2.4GHz 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.
Reference:
CompTIA Network+ study materials on wireless networking and interference mitigation.

NEW QUESTION: 123
Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other non-video applications on the network. Which of the following symptoms describes the users' reported issues?
A. Latency
B. Packet loss
C. Bottlenecking
D. Jitter
Answer: B (LEAVE A REPLY)
Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:
Users report connectivity issues and lag during video meetings.
The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.
Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.
Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.
Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.
Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Connectivity Issues

NEW QUESTION: 124
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: D (LEAVE A REPLY)

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:

NEW QUESTION: 125
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

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

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

NEW QUESTION: 126

After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two.)

A. Ensure a bottleneck is not coming from other devices on the network.

B. Install the latest firmware for the device.

C. Create a new VLAN for the access point.

D. Make sure the SSID is not longer than 16 characters.

E. Configure the AP in autonomous mode.

F. Install a wireless LAN controller.

Answer: A,B (LEAVE A REPLY)

Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms:"Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

NEW QUESTION: 127

After providing a username and password, a user must input a passcode from a phone application. Which of the following authentication technologies is used in this example?

A. SSO

B. LDAP

C. MFA

D. SAML

Answer: C (LEAVE A REPLY)

This is an example of Multi-Factor Authentication (MFA) because it requires:

Something you know (username/password)

Something you have (a phone-generated passcode)

Breakdown of Options:

A . SSO (Single Sign-On) - Allows one login for multiple services, but does not add a second authentication factor.

B . LDAP (Lightweight Directory Access Protocol) - Used for directory authentication, not MFA.

C . MFA (Multi-Factor Authentication) - ✓ Correct answer. Uses multiple authentication factors for better security.

D). SAML (Security Assertion Markup Language) - Used for federated identity management, not multi-factor authentication.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement authentication and authorization methods.

NEW QUESTION: 128

Which of the following steps in the troubleshooting methodology comes after using a top-to-top buttom examination of the OSI model to determine cause?

A. Identify the problem

B. Test in the theory

C. Establish a plan of action

D. Verify full system functionality

Answer: (SHOW ANSWER)

NEW QUESTION: 129

Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).

A. Fire suppression system

B. UPS location

C. Humidity control

D. Power load

E. Floor construction type

F. Proximity to nearest MDF

Answer: A (LEAVE A REPLY)

When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such ascorrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.Reference: CompTIA Network+ study materials.

NEW QUESTION: 130

A network administrator's device is experiencing severe Wi-Fi interference within the corporate headquarters causing the device to constantly drop off the network. Which of the following is most likely the cause of the issue?

A. Too many client connections

B. Too much wireless absorption

C. Too much wireless reflection

D. Too many wireless repeaters

Answer: C (LEAVE A REPLY)

NEW QUESTION: 131

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: A (LEAVE A REPLY)
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: 132
Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?
A. Fire suppression
B. Power budget
C. Temperature
D. Humidity
Answer: C (LEAVE A REPLY)
Switches in sealed enclosures are at risk of overheating because airflow is restricted. The temperature factor is critical since heat buildup can damage components, shorten device lifespan, and cause outages. Proper cooling or ventilation must be ensured.
A . Fire suppression is important for data centers but not the primary concern in a sealed box.
B . Power budget applies to PoE allocations, not environmental safety.
D . Humidity matters, but overheating is far more immediate in sealed environments.
Reference (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Environmental considerations, switch installation, temperature control.

NEW QUESTION: 133
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: 134
Which of the following technologies are X.509 certificates most commonly associated with?
A. PKI
B. VLAN tagging
C. LDAP
D. MFA
E. 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.
Answer: A (LEAVE A REPLY)
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 Reference:
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: 135
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: C (LEAVE A REPLY)
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.

NEW QUESTION: 136
Which of the following network topologies contains a direct connection between every node in the network?
A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point
Answer: A (LEAVE A REPLY)
In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.Reference: CompTIA Network + study materials.

NEW QUESTION: 137
Which of the following routing protocols is most commonly used to interconnect WANs?
A. IGP

B. EIGRP
C. BGP
D. OSPF
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 138
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.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 139
Which of the following OSI model layers can utilize a connectionless protocol for data transmission?
A. Physical
B. Network
C. Transport
D. Application
Answer: (SHOW ANSWER)

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

NEW QUESTION: 140
A Chief Information Officer wants a DR solution that runs only after a failure of the primary site and can be brought online quickly once recent backups are imported. Which of the following DR site solutions meets these requirements?
A. Cold
B. Warm
C. Active
D. Hot
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Explanation (aligned to N10-009):
A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.
A . Cold site has only power and space, requiring full setup, which takes too long.
C . Active (active-active) runs simultaneously with the primary site, not only during failure.
D . Hot site is fully operational at all times and can take over immediately, but it's more expensive.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 141
A network technician is terminating a cable to a fiber patch panel in the MDF. Which of the following connector types is most likely in use?
A. F-type
B. RJ11
C. BNC
D. SC
Answer: D (LEAVE A REPLY)
In a fiber patch panel, the SC (Subscriber Connector or Standard Connector) is commonly used because of its push-pull design and reliability in enterprise environments.
Breakdown of Options:
A . F-type - Used for coaxial cables (e.g., cable TV), not fiber.
B . RJ11 - Used for telephone lines, not fiber.
C . BNC - Used for coaxial connections, not fiber.

D . SC - ✓ Correct answer. A standard fiber optic connector used in patch panels.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.

NEW QUESTION: 142
A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?
A. A physical interface used for trunking logical ports
B. A physical interface used for management access
C. A logical interface used for the routing of VLANs
D. A logical interface used when the number of physical ports is insufficent.
Answer: C (LEAVE A REPLY)
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.
Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.
Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

NEW QUESTION: 143
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: B (LEAVE A REPLY)

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.Reference: CompTIA Network+ study materials and cloud computing principles.

NEW QUESTION: 144
Which of the following protocols provides remote access utilizing port 22?
A. SSH
B. Telnet
C. TLS
D. RDP
Answer: (SHOW ANSWER)
SSH (Secure Shell) is a protocol used to securely connect to a remote server/system over a network. It operates on port 22 and provides encrypted communication, unlike Telnet which operates on port 23 and is not secure. TLS is used for securing HTTP connections (HTTPS) and operates on ports like 443, while RDP (Remote Desktop Protocol) is used for remote desktop connections and operates on port 3389.
Reference:
The CompTIA Network+ materials and tutorials cover SSH as the standard protocol for secure remote access, highlighting its operation on port 22.

NEW QUESTION: 145
A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org.
Which of the following records should the administrator use?
A. SOA
B. MX
C. CNAME
D. NS
Answer: C (LEAVE A REPLY)
A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.
Reference:
The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

NEW QUESTION: 146
A user tries to visit a website, but instead of the intended site, the page displays vmw.cba.com. Which of the following should be done to reach the correct website?
A. Modify the CNAME record
B. Update the PTR record
C. Change the NTP settings
D. Delete the TXT record
Answer: (SHOW ANSWER)
A CNAME (Canonical Name) record maps an alias to the correct fully qualified domain name (FQDN). If a user is redirected to the wrong hostname, correcting or updating the CNAME ensures the alias points to the proper domain.
B . PTR record maps IP to hostname (reverse DNS), not forward website resolution.
C . NTP relates to time sync, irrelevant to DNS resolution.
D . TXT record stores metadata like SPF or DKIM info, not used for hostname aliasing.
Reference (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - DNS record types (A, AAAA, CNAME, PTR, TXT).

NEW QUESTION: 147
A network engineer is deploying switches at a new remote office. The switches have been preconfigured with hostnames and STP priority values. Based on the following table:
Switch Name
Priority
core-sw01
24576
access-sw01
28672
distribution-sw01
32768
access-sw02
36864
Which of the following switches will become the root bridge?
A. core-sw01
B. access-sw01
C. distribution-sw01
D. access-sw02
Answer: A (LEAVE A REPLY)
The switch with the lowest STP priority becomes the root bridge.In the given table, core-sw01 has the lowest priority value of 24576. Therefore, it will be elected as the root bridge in the Spanning Tree Protocol topology.
Reference:

NEW QUESTION: 148
After changes were made to a firewall, users are no longer able to access a web server. A network administrator wants to ensure that ports 80 and 443 on the web server are still accessible from the user IP space. Which of the following commands is best suited to perfom this testing?
A. Ifconfig
B. nmap
C. Ping
D. Dig
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following routing protocols uses an autonomous system number?
A. IS-IS
B. EIGRP
C. OSPF
D. BGP
Answer: D (LEAVE A REPLY)
BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.Reference: CompTIA Network+ study materials and RFC 4271.

NEW QUESTION: 150
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: 151
Users are experiencing significant lag while connecting to a cloud-based application during peak hours. An examination of the network reveals that the bandwidth is being heavily utilized. Further analysis shows that only a few users are using the application at any given time. Which of the following is the most cost-effective solution for this issue?
A. Limit the number of users who can access the application.
B. Lease a Direct Connect connection to the cloud service provider.
C. Implement QoS to prioritize application traffic.
D. Use a CDN to service the application.
Answer: C (LEAVE A REPLY)
Quality of Service (QoS)is the best cost-effective solution. It prioritizes traffic based on application criticality. If the bandwidth is limited and only a few users are affected, prioritizing that application traffic can improve performance without needing costly bandwidth upgrades or direct connections.
Reference:

NEW QUESTION: 152
Which of the following is the best reason to create a golden configuration?
A. To provide configuration consistency
B. To decrease the size of configuration files
C. To increase security by encrypting configurations
D. To set up backup configurations for each device
Answer: A (LEAVE A REPLY)
A golden configuration is a baseline configuration file that contains approved, standardized settings for network devices. The purpose is to ensure configuration consistency across the environment. This prevents misconfigurations, supports compliance with organizational or regulatory standards, and accelerates recovery if a device needs reconfiguration.
B . Reducing file size is not the goal of golden configs.
C . Golden configs can include security settings, but they are not inherently encrypted - they are simply a baseline template.
D . While configs can be backed up, golden configs are more about standardization, not device-specific backups.

By maintaining a golden configuration, administrators can quickly detect unauthorized changes (by comparing running configs against the golden file) and enforce consistency across devices. This improves network stability, reduces troubleshooting complexity, and enhances security posture.

NEW QUESTION: 153
Which of the following is the most secure way to provide site-to-site connectivity?
A. VXLAN
B. IKE
C. GRE
D. IPsec
Answer: D (LEAVE A REPLY)
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, ensuringthat 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.Reference: CompTIA Network+ study materials and NIST Special Publication 800-77.

NEW QUESTION: 154
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: A (LEAVE A REPLY)
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: 155
Which of the following protocols has a default administrative distance value of 90?
A. RIP
B. EIGRP
C. OSPF
D. BGP
Answer: B (LEAVE A REPLY)
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.Reference: CompTIA Network+ study materials.

NEW QUESTION: 156
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: C (LEAVE A REPLY)
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).
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 157

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: A (LEAVE A REPLY)

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: 158

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: 159
Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?
A. Establish a plan of action.
B. Test the theory to determine cause.
C. Document the findings and outcomes.
D. Identify the problem.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
Which of the following requires network devices to be managed using a different set of IP addresses?
A. Console
B. Split tunnel
C. Jump box
D. Out of band
Answer: (SHOW ANSWER)
Out-of-band (OOB) management refers to using a dedicated management network that is physically separate from the regular data network. This management network uses a different set of IP addresses to ensure that management traffic is isolated from user data traffic, providing a secure way to manage network devices even if the main network is down or compromised.Reference: CompTIA Network+ study materials.

NEW QUESTION: 161
A network administrator needs to connect a department to a new network segment. They need to use a DHCP server located on another network. Which of the following can the administrator use to complete this task?
A. IP Helper
B. Reservation
C. Exclusion
D. Scope
Answer: A (LEAVE A REPLY)
An IP Helper (IP Helper Address) allows DHCP requests to pass through routers and reach a DHCP server on another network.
* DHCP broadcasts are not forwarded across routers by default, so an IP Helper Address is needed to relay the request.
* This is crucial for large networks where a single DHCP server serves multiple subnets.
* Option B (Reservation): Ensures a specific IP address is assigned to a MAC address but does not relay DHCP across networks.

* Option C (Exclusion): Prevents specific IP addresses from being assigned, but does not help with DHCP relay.
* Option D (Scope): Defines the range of IP addresses available for DHCP clients but does not assist in cross-network communication.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: DHCP and IP Addressing

NEW QUESTION: 162
A data center administrator is evaluating the use of jumbo frames within a storage environment. Which of the following describes the best reason to use jumbo frames in the storage environment?
A. To reduce device overhead
B. To report on the current root switch in the STP
C. To improve routing convergence
D. To increase drive throughput
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:
"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

NEW QUESTION: 163
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.
Reference:
CompTIA Network+ study materials on network maintenance and security best practices.

NEW QUESTION: 164
An ISP provided a company with a pre-configured modem and five public static IP addresses. Which of the following does the company's firewall require to access the internet? (Select TWO).
A. NTP server
B. Default gateway
C. The modem's IP address
D. One static IP address
E. DNS servers
F. DHCP server
Answer: B,D (LEAVE A REPLY)
To access the internet using static IPs, the firewall (or router) must be configured correctly:
B). Default gateway: This is essential because it tells the firewall where to send outbound traffic destined for outside the local network.
D). One static IP address: The firewall must be assigned one of the static IPs to communicate over the public internet.
The other options are not essential for basic internet connectivity in this context:
A). NTP server: Useful for time synchronization but not required for internet access.
C). The modem's IP address: Irrelevant unless doing modem-level configuration.
E). DNS servers: Important for name resolution but not for basic layer 3 connectivity.
F). DHCP server: Not used when static IPs are assigned.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.2 - Compare and contrast addressing technologies.

NEW QUESTION: 165

A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switch ports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select TWO).

A. Change network translation definitions

B. Enable 802.1Q

C. Implement a routing protocol

D. Set up voice VLANs

E. Reconfigure the DNS

F. Place devices in the perimeter network

Answer: B,D (LEAVE A REPLY)

To support VoIP on the same physical ports used by computers:

B). Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.

D). Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.

Other options are not directly related to configuring VoIP over existing ports:

A). Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.

C). Routing protocols are not necessary at the switch level for VLAN setup.

E). DNS is not required for the switch or VLAN setup.

F). Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

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

NEW QUESTION: 166

Which of the following ports should a network administrator enable for encrypted login to a network switch?

A. 22

B. 23

C. 80

D. 123

Answer: (SHOW ANSWER)

Port 22 is used for Secure Shell (SSH), which enables encrypted remote login and command execution on network devices.

Port 23 = Telnet (unencrypted)

Port 80 = HTTP

Port 123 = NTP

From Andrew Ramdayal's guide:

"SSH uses port 22 to provide secure command-line access to devices such as switches and routers. Unlike Telnet (port 23), SSH encrypts session traffic, making it the preferred method for remote administration."

NEW QUESTION: 167
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: B (LEAVE A REPLY)
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.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 168
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: A (LEAVE A REPLY)
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: 169
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: A (LEAVE A REPLY)
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.Reference: CompTIA Network+ study materials.

NEW QUESTION: 170
A network engineer needs to virtualize network services, including a router at a remote branch location. Which of the following solutions meets the requirements?
A. NFV
B. VRF
C. VLAN
D. VPC
Answer: A (LEAVE A REPLY)
Network Functions Virtualization (NFV): NFV is a technology that virtualizes network services like routing, firewalls, and load balancers. It allows these services to run on virtual machines rather than requiring dedicated hardware. This is ideal for remote branch locations where deploying physical devices is costly and complex.
VRF (B): Virtual Routing and Forwarding is used for segmenting routing tables but does not virtualize services.
VLAN (C): Virtual Local Area Networks help segregate broadcast domains but are unrelated to virtualizing network functions.
VPC (D): Virtual Private Cloud is used for cloud computing but does not pertain to virtualizing network services.
Reference:

NEW QUESTION: 171
A network engineer needs to deploy an access point at a remote office so that it will not communicate back to the wireless LAN controller. Which of the following deployment methods must the engineer use to accomplish this task?

A. Lightweight
B. Autonomous
C. Mesh
D. Ad hoc
Answer: (SHOW ANSWER)
Autonomous access points operate independently without needing to communicate with a central wireless LAN controller. This is ideal for remote deployments.
From Andrew Ramdayal's guide:
"Autonomous access points are stand-alone devices that manage their own configurations and operations. They do not require a WLC and are ideal for small or remote office deployments."

NEW QUESTION: 172
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.
Reference (CompTIA Network+ N10-009):
Domain: Network Security - Switch security, CAM table attacks, MAC flooding.

NEW QUESTION: 173
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. Four
B. Three
C. Two
D. One
Answer: A (LEAVE A REPLY)

NEW QUESTION: 174
After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:

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

NEW QUESTION: 175
A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?
A. Coaxial cable
B. 9.8ft (3m) cable
C. Plenum cable
D. STP cable
Answer: D (LEAVE A REPLY)
The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.
A . Coaxial is not used for modern Ethernet server-switch links.
B . Shorter UTP cable does not solve EMI issues.
C . Plenum cable refers to cable jacket type for fire safety, not electrical shielding.

STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.
Reference:
Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

NEW QUESTION: 176
A company recently rearranged some users' workspaces and moved several users to previously used workspaces. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the MOST likely reason?
A. Ports are error-disabled.
B. Ports have an incorrect native VLAN.
C. Ports are having an MDIX issue.
D. Ports are trunk ports.
Answer: B (LEAVE A REPLY)
The most likely cause is that the switch ports were previously configured for a different VLAN than the one the users' computers are on. If the native VLAN on the port doesn't match the end device's VLAN, communication fails.
A). Ports are error-disabled: Would result in no link at all, not common across multiple ports unless a violation occurred.
C). MDIX issue: Auto-MDIX eliminates most crossover problems on modern switches.
D). Ports are trunk ports: While possible, typical user devices should be on access ports, but if the port is incorrectly trunked, it can cause similar issues. However, "incorrect VLAN" is more precise here.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 177
Which of the following, in addition to a password, can be asked of a user for MFA?
A. PIN
B. Favorite color
C. Hard token
D. Mother's maiden name
Answer: C (LEAVE A REPLY)
Multi-factor authentication (MFA) requires two or more different categories of authentication factors:
Something you know (password, PIN)
Something you have (smart card, hardware token)
Something you are (biometric)
The only valid second factor here is a hard token (e.g., a key fob generating one-time codes).
A . PIN is still "something you know," the same category as a password.

B . Favorite color is a weak knowledge-based factor, not a true second factor.
D . Mother's maiden name is also "something you know" and insecure.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 178
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: 179
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: 180

A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?

A. Port

B. Content

C. MAC

D. DNS

Answer: B (LEAVE A REPLY)

NEW QUESTION: 181

Which of the following ports is used for secure email?

A. 25

B. 110

C. 143

D. 587

Answer: D (LEAVE A REPLY)

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 Reference:

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: 182
Which of the following devices can operate in multiple layers of the OSI model?
A. Hub
B. Switch
C. Transceiver
D. Modem
Answer: B (LEAVE A REPLY)
Understanding Switches:
Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.
Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.
Capabilities of Multilayer Switches:
VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs.
Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.
Comparison with Other Devices:
Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.
Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.
Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.
Practical Application:
Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.
Reference:
CompTIA Network+ study materials on network devices and the OSI model.

NEW QUESTION: 183
A network engineer is completing a wireless installation in a new building. A requirement is that all clients be able to automatically connect to the fastest supported network. Which of the following best supports this requirement?
A. Enabling band steering
B. Disabling the 5GHz SSID
C. Adding a captive portal
D. Configuring MAC filtering

Answer: A (LEAVE A REPLY)
Band steering is a feature in wireless networks that encourages dual-band capable devices to connect to the 5GHz band instead of the 2.4GHz band.
Why Band Steering?
The 5GHz band supports higher speeds and less interference compared to 2.4GHz.
If a device supports both bands, the access point (AP) can "steer" it to connect to 5GHz instead of 2.4GHz.
This helps ensure users always connect to the fastest available network.
Incorrect Options:
B . Disabling the 5GHz SSID: Would force devices onto 2.4GHz, which is slower and more congested.
C . Adding a Captive Portal: Used for guest authentication, not for speed optimization.
D . Configuring MAC Filtering: Used for security, not for optimizing network speed.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Technologies and Optimization

NEW QUESTION: 184
Which of the following can be implemented to add an additional layer of security between a corporate network and network management interfaces?
A. Jump box
B. Console server
C. API interface
D. In-band management
Answer: A (LEAVE A REPLY)
A jump box is a hardened, isolated system that provides secure access to critical infrastructure devices like routers and firewalls.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network security techniques.

NEW QUESTION: 185
Which of the following connectors provides console access to a switch?
A. ST
B. RJ45
C. BNC
D. SFP
Answer: B (LEAVE A REPLY)
Console Access:
Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.

RJ45 Connector:
Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.
Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).
Comparison with Other Connectors:
ST (Straight Tip): A fiber optic connector used for networking, not for console access.
BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.
SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.
Practical Application:
Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).
Reference:
CompTIA Network+ study materials on network devices and connectors.

NEW QUESTION: 186
Which of the following allows a standard user to log in to multiple resources with one account?
A. RADIUS
B. MFA
C. TACACS+
D. SSO
Answer: (SHOW ANSWER)
Single Sign-On (SSO) enables a user to access multiple resources or applications with one set of credentials, improving usability and security. The document confirms:
"Single Sign-On (SSO) allows a user to authenticate once and gain access to multiple resources or applications without needing to log in again for each. It streamlines the login process and improves security by reducing the number of passwords that need to be managed."

NEW QUESTION: 187
A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?
A. Packet capture
B. Data usage reports
C. SNMP traps
D. Configuration monitoring
Answer: (SHOW ANSWER)

To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.
Breakdown of Options:
A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.
B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.
C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.
D). Configuration monitoring - This tracks configuration changes rather than availability.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.
RFC 1157: Simple Network Management Protocol (SNMP)

NEW QUESTION: 188
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. Quality of Service
B. Load balancing
C. Port mirroring
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.

NEW QUESTION: 189
Which of the following can support a jumbo frame?
A. Access point
B. Bridge
C. Hub
D. Switch

Answer: D (LEAVE A REPLY)
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.
Reference:
CompTIA Network+ course materials and networking hardware documentation.

NEW QUESTION: 190
Which of the following protocols is used to route traffic on the public internet?
A. BGP
B. OSPF
C. EIGRP
D. RIP
Answer: (SHOW ANSWER)
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: 191
A company discovers on video surveillance recordings that an unauthorized person installed a rogue access point in its secure facility. Which of the following allowed the unauthorized person to do this?
A. Evil twin
B. Honeytrap
C. Wardriving
D. Tailgating
Answer: D (LEAVE A REPLY)
Tailgatingis a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.
* A. Evil twinis a wireless attack where an attacker sets up a fake AP.
* B. Honeytrapis used to attract attackers for analysis.
* C. Wardrivinginvolves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

NEW QUESTION: 192
Which of the following allows an organization to map multiple internal devices to a single external-facing IP address?
A. NAT
B. BGP
C. OSPF
D. FHRP
Answer: A (LEAVE A REPLY)
NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.
B . BGP is a routing protocol.
C . OSPF is a link-state IGP.
D . FHRP provides redundant gateways, not IP sharing.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 193
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: B (LEAVE A REPLY)
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: 194
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: A (LEAVE A REPLY)
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.

NEW QUESTION: 195
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.

NEW QUESTION: 196
A support agent receives a report that a remote user's wired devices are constantly disconnecting and have slow speeds. Upon inspection, the support agent sees that the user's coaxial modern has a signal power of -97dB.
A. Removing any spliters connecte to the line
B. Switching the devices to wireless
C. Moving the devices closer to the modern
D. Lowering the network speed
Answer: A (LEAVE A REPLY)
A signal power of -97dB indicates a very weak signal, which can cause connectivity issues and slow speeds. Splitters on a coaxial line can degrade the signal quality further, so removing them can help improve the signal strength and overall connection quality.
Signal Quality: Splitters can reduce the signal strength by dividing the signal among multiple lines, which can be detrimental when the signal is already weak.
Direct Connection: Ensuring a direct connection from the modem to the incoming line can maximize signal quality and reduce potential points of failure.
Network Reference:
CompTIA Network+ N10-007 Official Certification Guide: Discusses troubleshooting connectivity issues and the impact of signal strength on network performance.
Cisco Networking Academy: Provides insights on maintaining optimal signal quality in network setups.
Network+ Certification All-in-One Exam Guide: Covers common network issues, including those related to signal degradation and ways to mitigate them.

NEW QUESTION: 197
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: 198
A network administrator needs to set up a multicast network for audio and video broadcasting. Which of the following networks would be the most appropriate for this application?
A. 172.16.0.0/24
B. 192.168.0.0/24
C. 224.0.0.0/24
D. 240.0.0.0/24
Answer: (SHOW ANSWER)
Understanding Multicast:
Multicast IP Address Range: The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.

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

NEW QUESTION: 199
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: A (LEAVE A REPLY)
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: 200
A network administrator recently upgraded a wireless infrastructure with new APs. Users report that when stationary, the wireless connection drops and reconnects every 20 to 30 seconds. While reviewing logs, the administrator notices the APs are changing channels.
Which of the following is the most likely reason for the service interruptions?
A. Channel interference
B. Roaming misconfiguration
C. Network congestion
D. Insufficient wireless coverage
Answer: (SHOW ANSWER)
If APs are changing channels frequently, it indicates automatic channel selection due to interference. This can cause temporary disconnections as the APs switch frequencies.
Breakdown of Options:
A . Channel interference - ✓ Correct answer. APs change channels automatically to avoid interference, causing disconnections.

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

NEW QUESTION: 201
Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?
A. Router
B. Switch
C. Firewall
D. Load balancer
Answer: D (LEAVE A REPLY)
A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.
Breakdown of Options:
A . Router - Directs traffic between networks, not between web servers.
B . Switch - Works at Layer 2, does not distribute web traffic.
C . Firewall - Secures network traffic, but does not distribute load.
D . Load balancer - ✓ Correct answer. Optimizes web traffic distribution across multiple servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

NEW QUESTION: 202
Which of the following is associated with avoidance, acceptance, mitigation, and transfer?
A. Risk
B. Exploit
C. Threat
D. Vulnerability
Answer: A (LEAVE A REPLY)
These four terms-avoidance, acceptance, mitigation, and transfer-are strategies used in risk management.
From Andrew Ramdayal's guide:
"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."

NEW QUESTION: 203
Which of the following attacks utilizes a network packet that contains multiple network tags?
A. MAC flooding
B. VLAN hopping
C. DNS spoofing
D. ARP poisoning
Answer: (SHOW ANSWER)
VLAN hopping is an attack where an attacker crafts packets with multiple VLAN tags, allowing them to traverse VLAN boundaries improperly. This can result in gaining unauthorized access to network segments that are supposed to be isolated. The other options do not involve the use of multiple network tags. MAC flooding aims to overwhelm a switch's MAC address table, DNS spoofing involves forging DNS responses, and ARP poisoning involves sending fake ARP messages.
Reference:
According to the CompTIA Network+ course materials, VLAN hopping exploits the tagging mechanism in network packets to gain unauthorized access.

NEW QUESTION: 204
Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed. Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?
A. WPS configuration
B. Signal strength
C. Channel frequency
D. Power budget
Answer: B (LEAVE A REPLY)
When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.
A . WPS applies to Wi-Fi, not cellular repeaters.
C . Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.
D . Power budget applies to PoE and wired devices, not mobile phones.
Reference (CompTIA Network+ N10-009):

NEW QUESTION: 205
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: