CompTIA.N10-009.v2026-01-21.q154

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	154
Version:	v2026-01-21
# of views:	107
# of Questions views:	2125
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-01-21.q154.html	

NEW QUESTION: 1
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: 2
A network administrator deploys several new desk phones and workstation cubicles. Each cubicle has one assigned switchport. The administrator runs the following commands:
nginx
CopyEdit
switchport mode access
switchport voice vlan 69
With which of the following VLANs will the workstation traffic be tagged?
A. Private VLAN
B. Voice VLAN

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

NEW QUESTION: 3
A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?
A. 802.1X
B. Access control list
C. Port security
D. MAC filtering
Answer: (SHOW ANSWER)
802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means.
802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.References:CompTIA Network+ study materials.

NEW QUESTION: 4
A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?
A. tcpdump
B. dig
C. tracert
D. arp
Answer: C (LEAVE A REPLY)
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing

issues.References: CompTIA Network+ study materials and common network troubleshooting commands.

NEW QUESTION: 5
Which of the following most likely requires the use of subinterfaces?
A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol
Answer: (SHOW ANSWER)
Introduction to Subinterfaces:
Subinterfaces are logical interfaces created on a single physical interface. They are used to enable a router to support multiple networks on a single physical interface.
Use Case for Subinterfaces:
Subinterfaces are commonly used in scenarios where VLANs are implemented. A router with a single physical LAN port can be configured with multiple subinterfaces, each associated with a different VLAN.
This setup allows the router to route traffic between different VLANs.
Example Configuration:
Consider a router with a single physical interface GigabitEthernet0/0 and two VLANs, 10 and 20.
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
The encapsulation dot1Q command specifies the VLAN ID.
Explanation of the Options:
A). A router with only one available LAN port: This is correct. Subinterfaces allow a single physical interface to manage multiple networks, making it essential for routers with limited physical interfaces.
B). A firewall performing deep packet inspection: Firewalls can use subinterfaces, but it is not a requirement for deep packet inspection.
C). A hub utilizing jumbo frames: Hubs do not use subinterfaces as they operate at Layer 1 and do not manage IP addressing.
D). A switch using Spanning Tree Protocol: STP is a protocol for preventing loops in a network and does not require subinterfaces.
Conclusion:

Subinterfaces provide a practical solution for routing between multiple VLANs on a router with limited physical interfaces. They allow network administrators to optimize the use of available hardware resources efficiently.
References:
CompTIA Network+ guide detailing VLAN configurations and the use of subinterfaces (see page Ref
9 Basic Configuration Commands).

NEW QUESTION: 6
Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other non-video applications on the network. Which of the following symptoms describes the users' reported issues?
A. Latency
B. Packet loss
C. Bottlenecking
D. Jitter
Answer: (SHOW ANSWER)
Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:
Users report connectivity issues and lag during video meetings.
The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.
Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.
Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.
Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.
Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Troubleshooting Connectivity Issues

NEW QUESTION: 7
Which of the following is most likely responsible for the security and handling of personal data in Europe?
A. GDPR
B. SCADA
C. SAML
D. PCI DSS

Answer: (SHOW ANSWER)

* Definition of GDPR:
* General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
* Scope and Objectives:
* GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
* It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
* Comparison with Other Options:
* SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.
* SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.
* PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.
* Key Provisions:
* GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.

References:

* CompTIA Network+ study materials on regulatory and compliance standards.

NEW QUESTION: 8

Which of the following is the most secure way to provide site-to-site connectivity?

A. VXLAN

B. IKE

C. GRE

D. IPsec

Answer: (SHOW ANSWER)

IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.References: CompTIA Network+ study materials and NIST Special Publication
800-77.

NEW QUESTION: 9

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

A. Public

B. Hybrid

C. SaaS

D. Private

Answer: (SHOW ANSWER)

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

NEW QUESTION: 10

Which of the following can be used when a server at a remote site is physically unreachable?

A. OOB management

B. Crash cart

C. Jump box

D. Console

Answer: (SHOW ANSWER)

Out-of-band (OOB) managementallows administrators to manage devices remotely even if the primary network is down. This is especially useful when physical access to the server is not possible. OOB management often uses a separate management interface, ensuring access regardless of the server's operational state.

Reference:Section 3.5 - Network Access and Management Methods - "OOB Management"

NEW QUESTION: 11

Which of the following should a company implement in order to share a single IP address among all the employees in the office?

A. STP

B. BGP

C. PAT

D. VXLAN

Answer: (SHOW ANSWER)

PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:

"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

NEW QUESTION: 12
Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?
A. DNS poisoning
B. Denial-of-service
C. Social engineering
D. ARP spoofing
Answer: (SHOW ANSWER)
Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance.References: CompTIA Network+ study materials.

NEW QUESTION: 13
A technician needs to identify a computer on the network that is reportedly downloading unauthorized content. Which of the following should the technician use?
A. Anomaly alerts
B. Port mirroring
C. Performance monitoring
D. Packet capture
Answer: (SHOW ANSWER)
Packet Capture: This method captures and inspects network traffic to identify unauthorized downloads or malicious behavior. It provides detailed insight into the data being transmitted, making it the best tool for this scenario.
Anomaly alerts (A): Alerts may indicate unusual activity but do not provide detailed traffic analysis.
Port mirroring (B): Port mirroring can redirect traffic for analysis but requires a packet capture tool for deeper inspection.
Performance monitoring (C): Focuses on system performance metrics, not detailed traffic content.
Reference: CompTIA Network+ Official Study Guide, Domain 4.3 (Network Monitoring Tools).

NEW QUESTION: 14
A network administrator recently updated configurations on a Layer 3 switch. Following the updates, users report being unable to reach a specific file server. Which of the following is the most likely cause?

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

NEW QUESTION: 15
Which of the following ports is a secure protocol?
A. 20
B. 23
C. 443
D. 445
Answer: (SHOW ANSWER)
Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL
/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:
"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

NEW QUESTION: 16
Which of the following provides an opportunity for an on-path attack?
A. Phishing
B. Dumpster diving
C. Evil twin
D. Tailgating
Answer: C (LEAVE A REPLY)

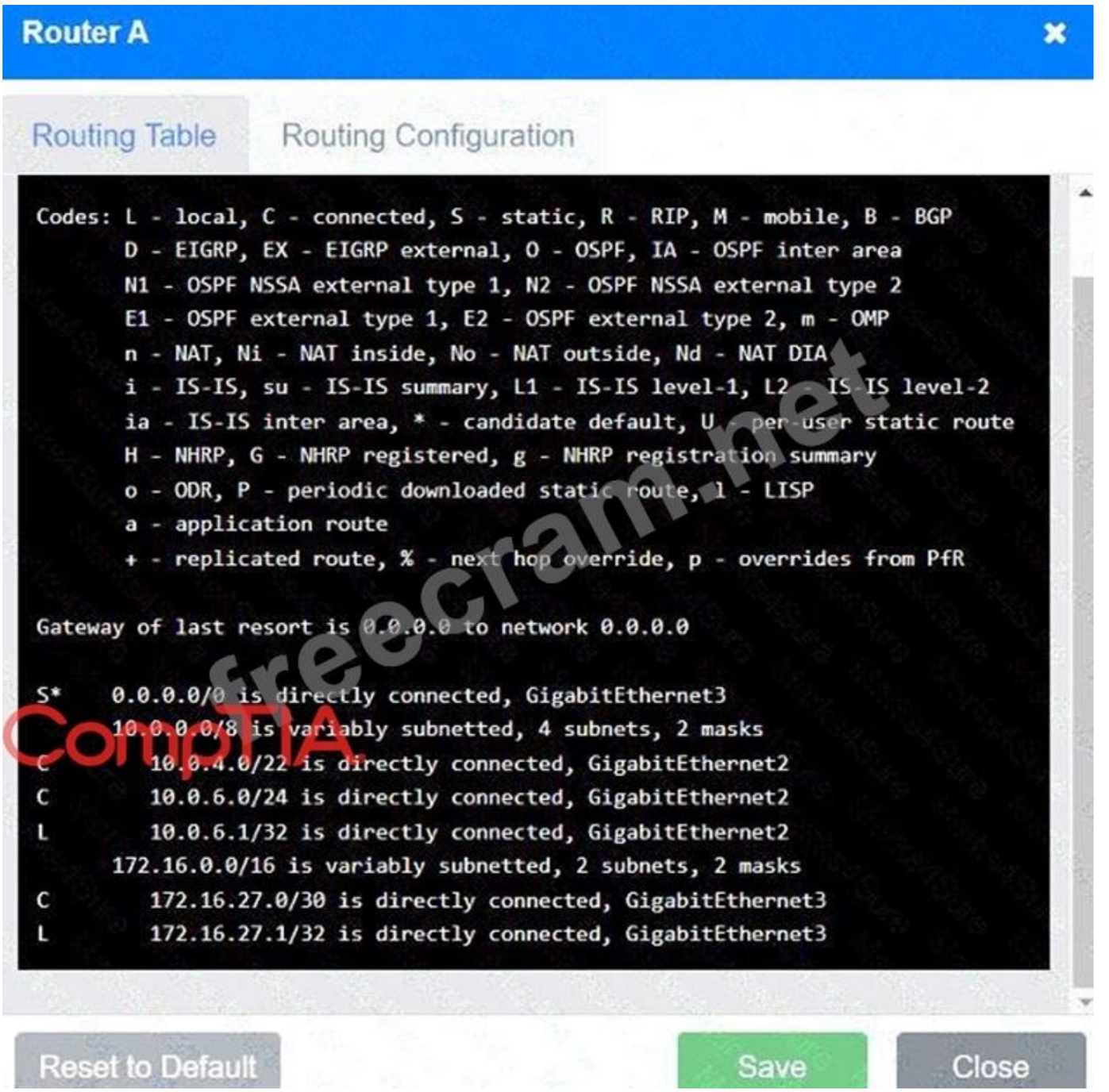
An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity.
Breakdown of Options:
A: Phishing - Tries to steal credentials through fake emails/websites but does not intercept 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.

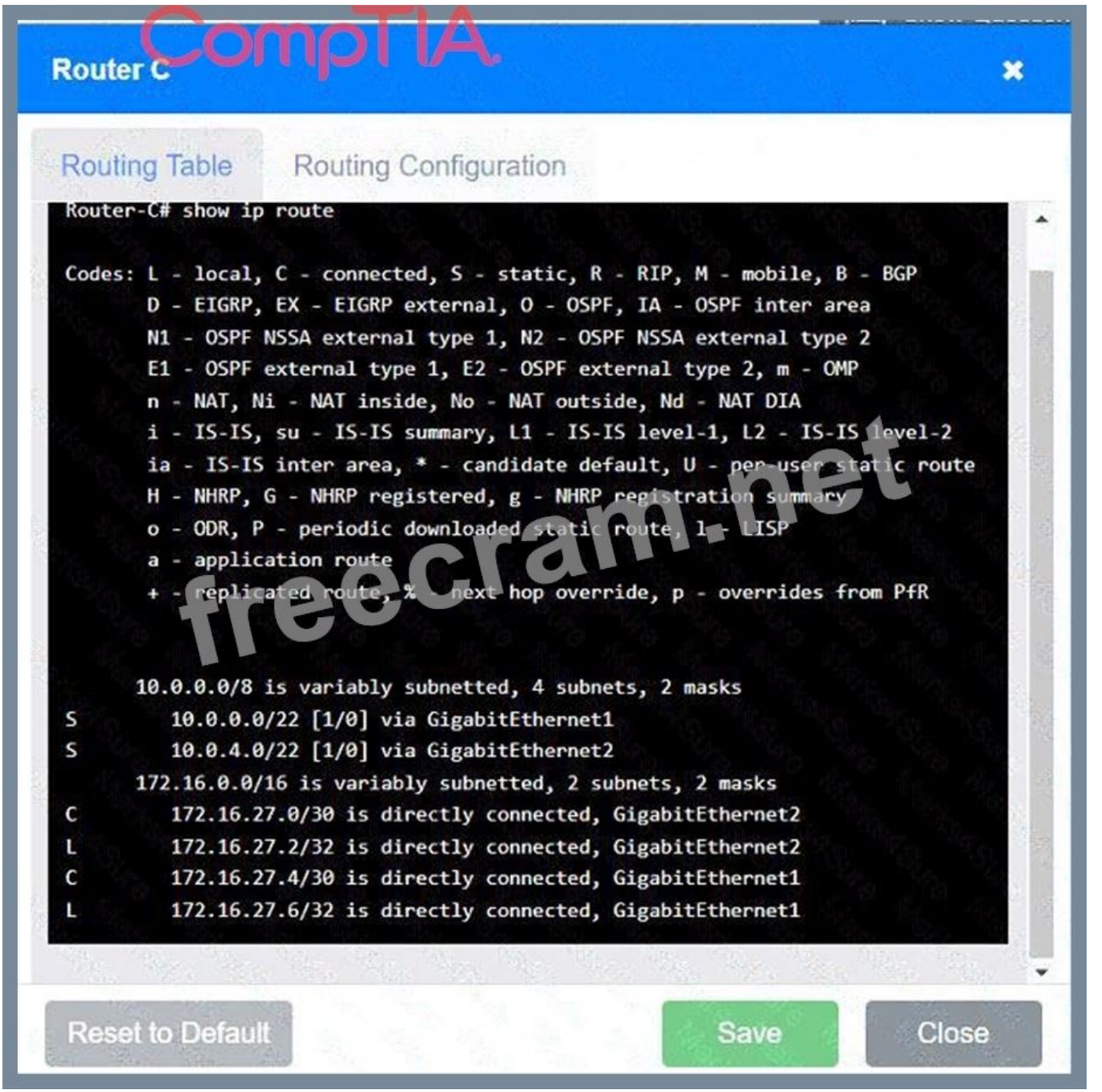
NEW QUESTION: 17
Which of the following network traffic type is sent to all nodes on the network?
A. Unicast
B. Broadcast
C. Multicast
D. Anycast
Answer: B (LEAVE A REPLY)
Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
* Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
* Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
* IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains network traffic types, including broadcast, unicast, and multicast.

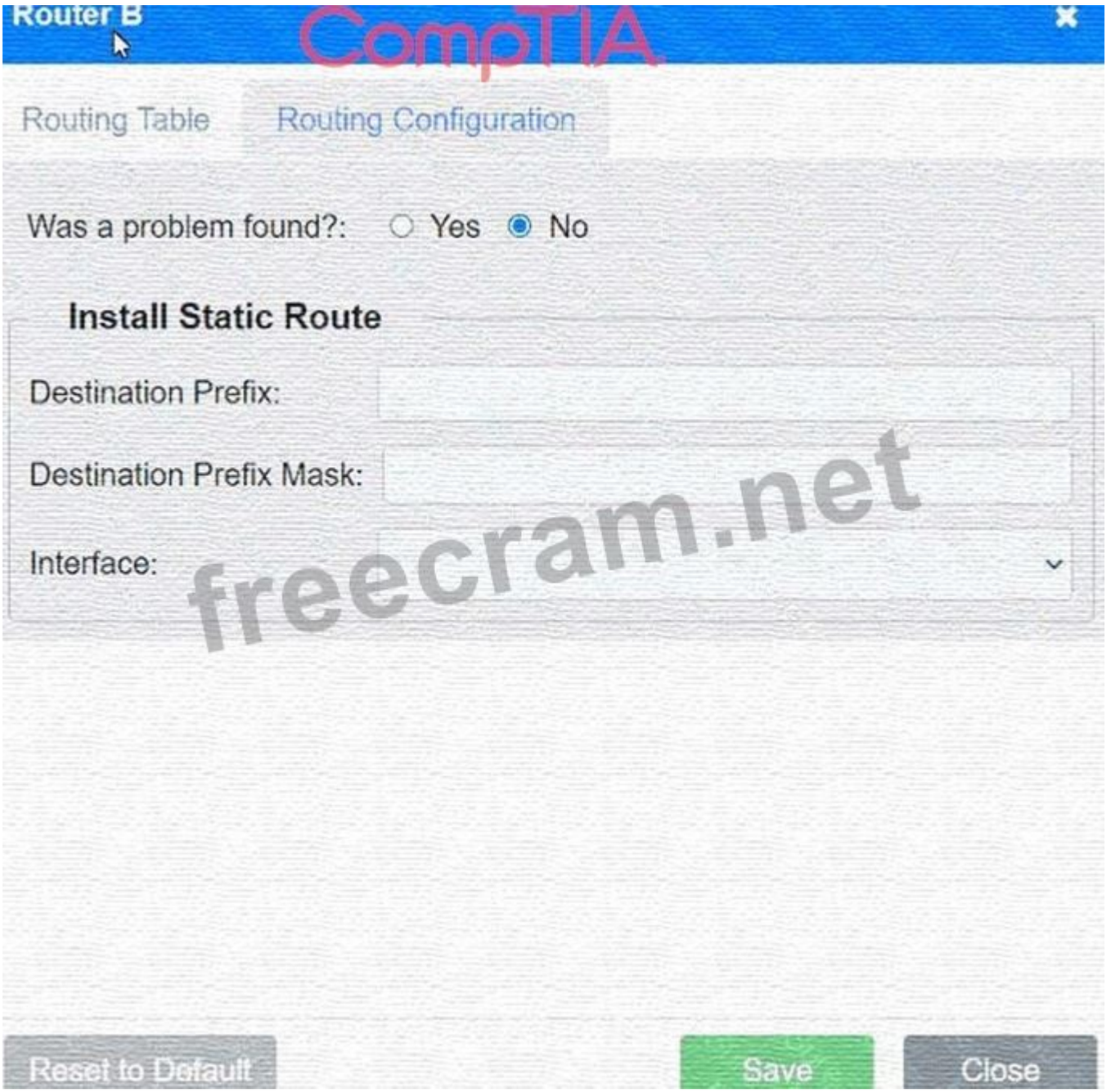
* Cisco Networking Academy: Provides training on network communication methods and traffic types.
* Network+ Certification All-in-One Exam Guide: Discusses different types of network traffic and their uses in various network scenarios.
Broadcast traffic is essential for network operations that require communication with all nodes, such as ARP requests or DHCP discovery messages.

NEW QUESTION: 18
A network administrator is configuring a new switch and wants to ensure that only assigned devices can connect to the switch. Which of the following should the administrator do?
A. Configure ACLs.
B. Implement a captive portal.
C. Enable port security.
D. Disable unnecessaryservices.
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 19
Users are unable to access files on their department share located on file server 2.
The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identify any issues, and configure the appropriate solution.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.






Router B
CompTIA
Routing Table
Routing Configuration
Was a problem found?: Yes No
Install Static Route
Destination Prefix:
Destination Prefix Mask:
Interface:
freecram.net
Reset to Default
Save
Close

Answer:

See the solution in Explanation.

Explanation:

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

Review Routing Tables:

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

Identify Missing Routes:

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

Add Static Routes:

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

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3

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

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks

C 172.16.27.0/30 is directly connected, GigabitEthernet3
L 172.16.27.1/32 is directly connected, GigabitEthernet3
Routing Table:
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S* 0.0.0.0/0 is directly connected, GigabitEthernet1
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C 10.0.0.0/22 is directly connected, GigabitEthernet1
L 10.0.0.1/32 is directly connected, GigabitEthernet1
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.5/32 is directly connected, GigabitEthernet1
Routing Table:
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S 10.0.0.0/22 [1/0] via GigabitEthernet1
S 10.0.4.0/22 [1/0] via GigabitEthernet2
172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.27.0/30 is directly connected, GigabitEthernet2
L 172.16.27.2/32 is directly connected, GigabitEthernet2
C 172.16.27.4/30 is directly connected, GigabitEthernet1
L 172.16.27.6/32 is directly connected, GigabitEthernet1
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router C's IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet3
Install Static Route to 10.0.4.0/22 via 172.16.27.5 (assuming Router C's IP is 172.16.27.5):
Destination Prefix: 10.0.4.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Install Static Route to 10.0.6.0/24 via 172.16.27.2 (assuming Router A's IP is 172.16.27.2):
Destination Prefix: 10.0.6.0
Destination Prefix Mask: 255.255.255.0
Interface: GigabitEthernet2
Install Static Route to 10.0.0.0/22 via 172.16.27.1 (assuming Router B's IP is 172.16.27.1):
Destination Prefix: 10.0.0.0
Destination Prefix Mask: 255.255.252.0
Interface: GigabitEthernet1
Summary of Static Routes:
Router A:
ip route 10.0.0.0 255.255.252.0 GigabitEthernet3
Router B:
ip route 10.0.4.0 255.255.252.0 GigabitEthernet1

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

NEW QUESTION: 20

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: 21
A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?
A. 4096
B. 8192
C. 32768
D. 36684

Answer: (SHOW ANSWER)

* Understanding Spanning Tree Protocol (STP):
* STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.
* Default Priority Value:
* Bridge Priority:STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.
* Priority Range:The bridge priority can be set in increments of 4096, ranging from 0 to 61440.
* Configuration and Verification:
* When deploying a new switch, the network administrator can verify the bridge priority using commands such asshow spanning-treeto ensure it is set to the default value of 32768.
* Comparison with Other Values:
* 4096 and 8192:Lower than the default priority, indicating these would be manually configured for higher preference.
* 36684:A non-standard value, likely a result of specific configuration changes.

References:

* CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

NEW QUESTION: 22

Which of the following should an installer orient a port-side exhaust to when installing equipment?

A. The patch panel

B. The front of the IDF

C. The warm aisle

D. The administrator console

Answer: (SHOW ANSWER)

In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:

"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

NEW QUESTION: 23

Which of the following is the most cost-effective way to safely expand outlet capacity in an IDF?

A. PDU

B. Surge protector

C. UPS

D. Power strip

Answer: (SHOW ANSWER)

A Power Distribution Unit (PDU) provides multiple power outlets in a data center or IDF (Intermediate Distribution Frame), while offering features like surge protection, load balancing,

and sometimes remote monitoring, making it a cost-effective and reliable solution. The document confirms:
"PDUs (Power Distribution Units) are a cost-effective way to expand outlet capacity in a structured cabling environment like an IDF. They ensure safe power delivery to networking equipment and often include monitoring features."

NEW QUESTION: 24
A network technician receives a new ticket while working on another issue. The new ticket is critical to business operations. Which of the following documents should the technician reference to determine which ticket to complete first?
A. NDA
B. AUP
C. SLA
D. MOU
Answer: (SHOW ANSWER)
AnSLA (Service Level Agreement)defines performance expectations, includingresponse time, prioritization, and resolution timefor services and support issues. It helps the technician determine which task hashigher priority based on business impact.
* A. NDA (Non-Disclosure Agreement)relates to confidentiality, not task prioritization.
* B. AUP (Acceptable Use Policy)defines user behavior, not issue handling.
* D. MOU (Memorandum of Understanding)outlines informal agreements and doesn't define ticket priorities.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.1 - Compare and contrast common documentation types.

NEW QUESTION: 25
Two companies successfully merged. Following the merger, a network administrator identified a connection bottleneck. The newly formed company plans to acquire a high-end 40GB switch and redesign the network from a three-tier model to a collapsed core. Which of the following should the administrator do until the new devices are acquired?
A. Implement the FHRP.
B. Configure a route selection metric change.
C. Install a load balancer.
D. Enable link aggregation.
Answer: (SHOW ANSWER)
*The issue described is a network bottleneck due to increased traffic after a merger.
*A collapsed core architecture consolidates the core and distribution layers into a single layer to improve efficiency and reduce latency.

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

NEW QUESTION: 26
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. Ping
B. Ifconfig
C. nmap
D. Dig
Answer: (SHOW ANSWER)

NEW QUESTION: 27
An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?
A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller
Answer: (SHOW ANSWER)
* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.
* Function of MIB: MIBs contain definitions and information about all objects that can be managed on a network using SNMP. These objects are defined using a hierarchical namespace containing object identifiers (OIDs).
CompTIA Network+ materials discussing SNMP and MIB functionality.

NEW QUESTION: 28
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

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

NEW QUESTION: 29
Which of the following source control features allows an administrator to test a new configuration without changing the primary configuration?
A. Central repository
B. Conflict identification
C. Branching
D. Version control
Answer: (SHOW ANSWER)
Branchingallows developers and administrators tocreate an isolated copyof the main configuration so they can test changes independently. This avoids impacting the primary environment and allows for safer testing and development.
Reference:Section 3.5 - Network Access and Management Methods - "Source Control: Branching"

NEW QUESTION: 30

A network engineer needs to virtualize network services, including a router at a remote branch location. Which of the following solutions meets the requirements?

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

NEW QUESTION: 31
A firewall administrator is mapping a server's internal IP address to an external IP address for public use.
Which of the following is the name of this function?
A. NAT
B. VIP
C. PAT
D. BGP
Answer: (SHOW ANSWER)
Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.
Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.
Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.
PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.
Incorrect Options:
B). VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.

C). PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.
D). BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

NEW QUESTION: 32
A network administrator notices uncommon communication between VMs on ephemeral ports on the same subnet. The administrator is concerned about that traffic moving laterally within the network. Which of the following describes the type of traffic flow the administrator is analyzing?
A. East-west
B. Point-to-point
C. Horizontal-scaling
D. Hub-and-spoke
Answer: (SHOW ANSWER)
When traffic moves laterally between VMs within the same network or subnet, it is known as east-west traffic. This contrasts with north-south traffic, which refers to communication between internal and external networks.
Breakdown of Options:
A). East-west - Correct answer. This refers to traffic between internal servers or VMs, which is a common security concern.
B). Point-to-point - Point-to-point describes a direct connection between two devices, but does not specifically define lateral movement.
C). Horizontal-scaling - This refers to adding more instances or nodes in cloud computing, unrelated to traffic flow.
D). Hub-and-spoke - This network topology describes a centralized design, not lateral traffic.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Analyze traffic patterns and behavior.
NIST SP 800-207: Zero Trust Architecture (ZTA) - East-West traffic monitoring

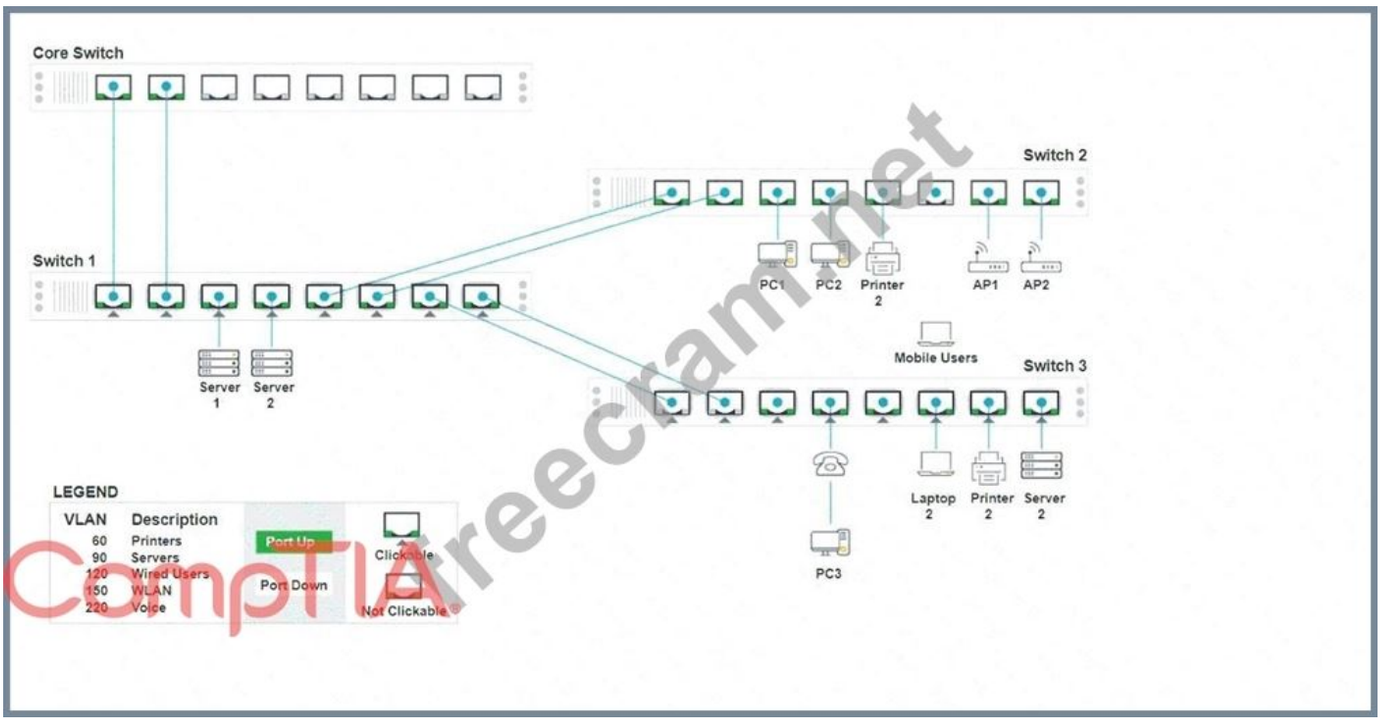
NEW QUESTION: 33
Which of the following network topologies contains a direct connection between every node in the network?
A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point
Answer: (SHOW ANSWER)
In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.References:CompTIA Network + study materials.

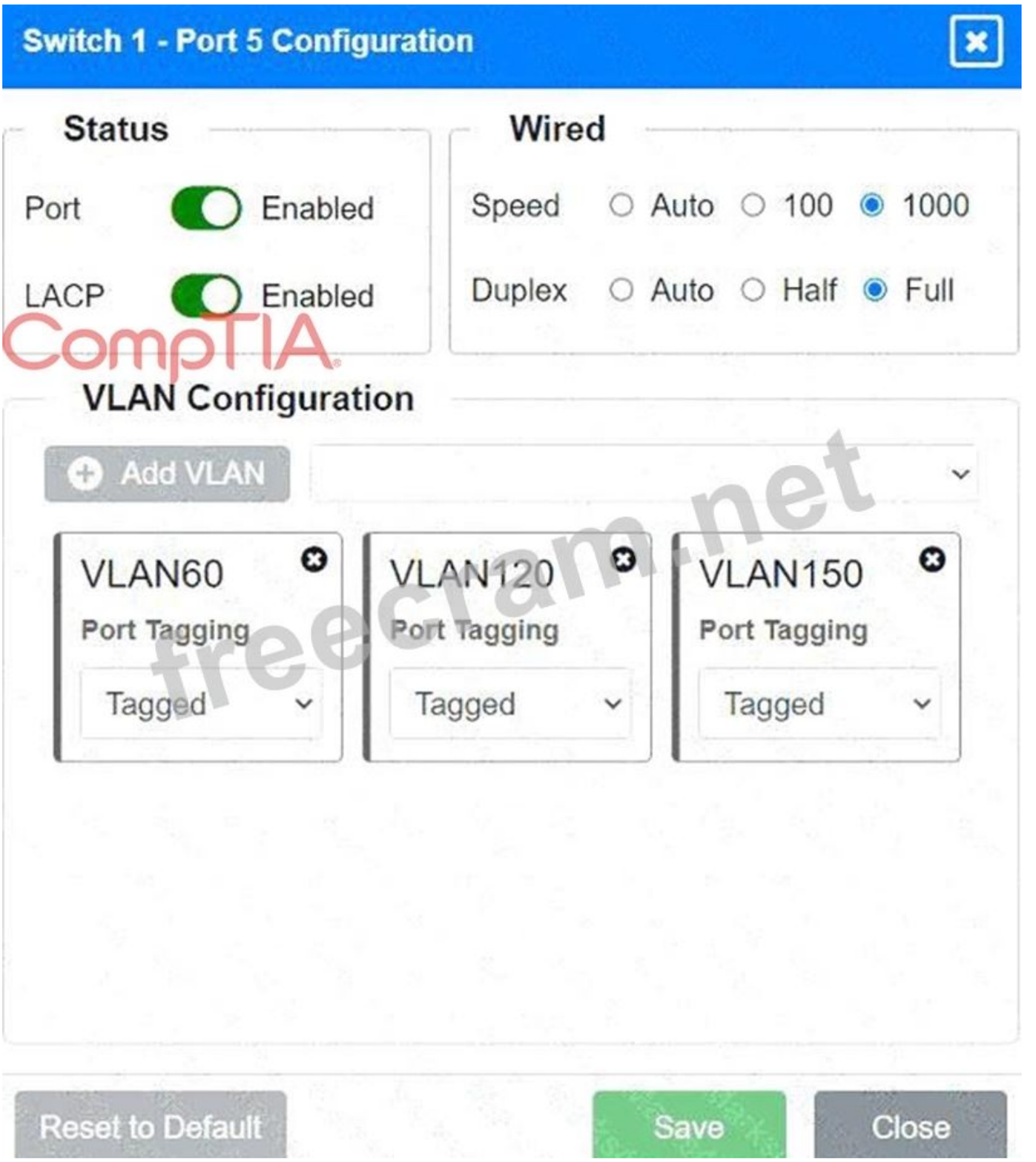
NEW QUESTION: 34
Which of the following explains what happens if a packet is lost in transit when using UDP?
A. The data link layer will recognize the error and resend the packet.
B. IP uses the TTL field to track packet hops and will resend the packet if necessary.
C. If the sender does not receive a UDP acknowledgement, the packet will be resent.
D. Some applications will recognize the loss and initiate a resend of the packet if necessary.
Answer: (SHOW ANSWER)
UDP (User Datagram Protocol) is a connectionless protocol that does not provide built-in mechanisms for error detection, retransmission, or acknowledgments. If a UDP packet is lost in transit, the protocol itself does not handle retransmission. However, some applications using UDP (e.g., TFTP or custom streaming protocols) may implement their own mechanisms to detect packet loss and request retransmission if needed.
Why not A? The data link layer (Layer 2) handles frame-level errors within a single network segment, not end- to-end packet loss across networks.
Why not B? The IP TTL (Time to Live) field prevents routing loops by decrementing with each hop, but IP does not handle retransmission.
Why not C? UDP does not use acknowledgments, so the sender does not expect or receive them.
Reference:CompTIA Network+ N10-009 Objective 1.4: Explain the characteristics of network topologies and protocols. The CompTIA Network+ Study Guide (e.g., Chapter 4: Network Protocols) explains that UDP is a
"fire-and-forget" protocol, and any retransmission logic must be handled by the application layer.

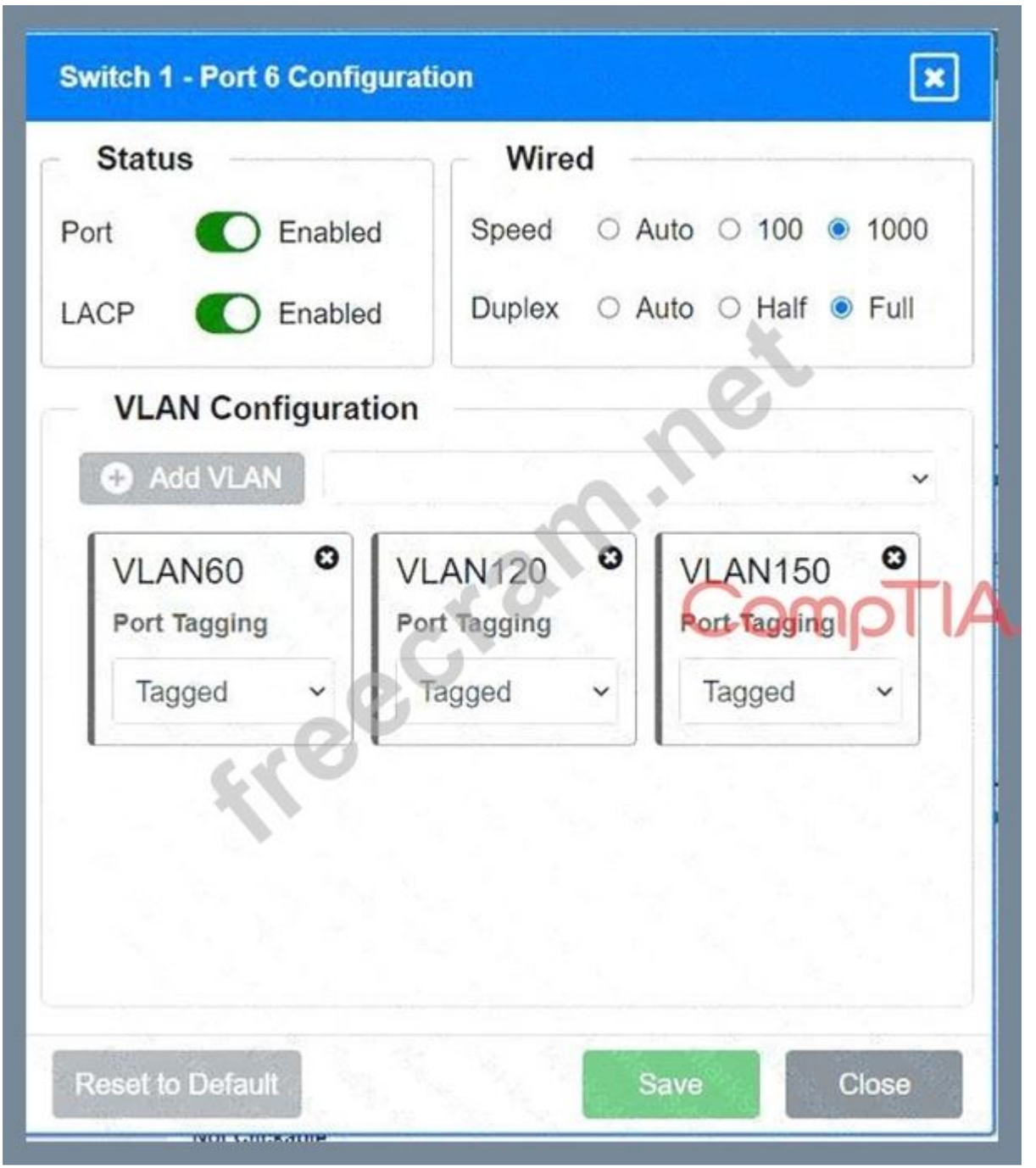
NEW QUESTION: 35
Which of the following best explains the role of confidentiality with regard to data at rest?
A. Datacanbe accessedafter privileged access Is granted.
B. Datacanbe accessedremotely with proper training.

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

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







Answer:

See the solution below in Explanation.

Explanation:

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

Identify the correct VLANs for each device and port.

Enable necessary ports and disable unused ports.

Configure fault-tolerant connections between the switches.

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

NEW QUESTION: 37

A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface's indicator lights are not blinking on either the computer or the switch. Which of the following Is the most likely cause?

A. Theswitch failed.

B. Thedefault gateway is wrong.

C. Theport Is shut down.

D. TheVLAN assignment is incorrect.

Answer: (SHOW ANSWER)

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

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

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

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

Command to Check and Enable Port:

bash

Copy code

Switch> enable

Switch# configure terminal

Switch(config)# interface [interface id]

Switch(config-if)# no shutdown

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

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

NEW QUESTION: 38

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: 39

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

A. BNC

B. SFP

C. MPO

D. RJ45

Answer: (SHOW ANSWER)

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

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

NEW QUESTION: 40

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.

References: CompTIA Network+ study materials.

NEW QUESTION: 41

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: (SHOW ANSWER)

The issue is clearly related toDNS resolution, as IP-based connections succeed but domain name-based ones fail.

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

NEW QUESTION: 42
Which of the following network ports is used when a client accesses an SFTP server?
A. 22
B. 80
C. 443
D. 3389
Answer: (SHOW ANSWER)
SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.
Breakdown of Options:
A). 22 - Correct answer. SFTP runs over SSH (port 22) for secure file transfers.
B). 80 - Used for HTTP, not SFTP.
C). 443 - Used for HTTPS (secure web traffic).
D). 3389 - Used for RDP (Remote Desktop Protocol).
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.
RFC 4253: SSH Transport Layer Protocol

NEW QUESTION: 43
A network analyst is installing a wireless network in a corporate environment. Employees are required to use their domain identities and credentials to authenticate and connect to the WLAN. Which of the following actions should the analyst perform on the AP to fulfill the requirements?
A. Enable MAC security.
B. Generate a PSK for each user.
C. Implement WPS.
D. Set up WPA3 protocol.
Answer: D (LEAVE A REPLY)
WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user- based authentication.

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

NEW QUESTION: 44
Which of the following technologies is the best choice to listen for requests and distribute user traffic across web servers?
A. Router
B. Switch
C. Firewall
D. Load balancer
Answer: (SHOW ANSWER)
A load balancer is designed to distribute user requests across multiple servers to ensure high availability and performance.
Breakdown of Options:
A). Router - Directs traffic between networks, not between web servers.
B). Switch - Works at Layer 2, does not distribute web traffic.
C). Firewall - Secures network traffic, but does not distribute load.
D). Load balancer - # Correct answer. Optimizes web traffic distribution across multiple servers.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Explain load balancing and redundancy concepts.

NEW QUESTION: 45
Which of the following attacks would most likely cause duplicate IP addresses in a network?
A. Rogue DHCP server
B. DNS poisoning

C. Social engineering
D. Denial-of-service
Answer: (SHOW ANSWER)
* Definition of a Rogue DHCP Server:
* A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.
* Impact of a Rogue DHCP Server:
* IP Address Conflicts:Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.
* Network Disruption:Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.
* Comparison with Other Attacks:
* DNS poisoning:Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.
* Social engineering:Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.
* Denial-of-service (DoS):Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.
* Prevention and Detection:
* Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.
* Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 46
A network engineer is setting up a new VoIP network for a customer. The current network is segmented only for computers and servers. No additional switch ports can be used in the new network. Which of the following does the engineer need to do to configure the network correctly? (Select TWO).
A. Change network translation definitions
B. Enable 802.1Q
C. Implement a routing protocol
D. Set up voice VLANs
E. Reconfigure the DNS
F. Place devices in the perimeter network
Answer: (SHOW ANSWER)
To support VoIP on the same physical ports used by computers:
B). Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.

D). Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.
Other options are not directly related to configuring VoIP over existing ports:
A). Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.
C). Routing protocols are not necessary at the switch level for VLAN setup.
E). DNS is not required for the switch or VLAN setup.
F). Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 47
A network architect is implementing an off-premises computing facility and needs to ensure that operations will not be impacted by major outages. Which of the following should the architect consider?
A. Hot site
B. DCI
C. Direct Connect
D. Active-passive approach
Answer: (SHOW ANSWER)
Ahot siteis a fully operational backup facility with hardware, network, and data synchronization already in place. It allows forimmediate failoverin the event of a disaster, minimizing downtime.
* B. DCI (Data Center Interconnect)connects data centers but doesn't guarantee availability unless built redundantly.
* C. Direct Connectrefers to a private link to cloud providers, not disaster recovery.
* D. Active-passivecan help with failover but may involve delay unless combined with hot site principles.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.4 - Summarize business continuity and disaster recovery concepts.

NEW QUESTION: 48
Which of the following VPN types provides secure remote access to the network resources through a web portal?
A. Proxy
B. Clientless
C. Site-to-site
D. Direct connect
Answer: (SHOW ANSWER)
Clientless VPNs allow users to access network resources through a secure web portal using a browser, with no VPN software needed. This is ideal for occasional access to internal resources via HTTPS.
A: Proxy is a gateway for accessing web content, not a VPN.
C: Site-to-site VPN connects entire networks, not individual users.
D: Direct Connect usually refers to dedicated cloud connections, not VPNs.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

NEW QUESTION: 49
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 much wireless reflection
B. Too much wireless absorption
C. Too many wireless repeaters
D. Too many client connections
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

NEW QUESTION: 50
Which of the following best explains the role of confidentiality with regard to data at rest?
A. Datacanbe accessedby anyone on the administrative network.
B. Datacanbe accessedremotely with proper training.
C. Datacanbe accessedafter privileged access Is granted.
D. Datacanbe accessedafter verifying the hash.
Answer: (SHOW ANSWER)
* Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.

* Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.
* Incorrect Options:
* A. "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
* B. "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
* D. "Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.
CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

NEW QUESTION: 51
A virtual machine has the following configuration:
*IPv4 address: 169.254.10.10
*Subnet mask: 255.255.0.0
The virtual machine can reach colocated systems but cannot reach external addresses on the Internet. Which of the following Is most likely the root cause?
A. Thesubnet mask is incorrect.
B. TheDHCP server is offline.
C. TheIP address is an RFC1918 private address.
D. TheDNS server is unreachable.
Answer: (SHOW ANSWER)
Understanding the 169.254.x.x Address:
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address, assigned when a DHCP server is unavailable.
DHCP Server Offline:
APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.
Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.
Comparison with Other Options:
The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.
The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-
172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.

The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.
Troubleshooting Steps:
Verify the DHCP server's status and connectivity.
Restart the DHCP service if necessary.
Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).
References:
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

NEW QUESTION: 52
A network administrator is planning to implement device monitoring to enhance network visibility. The security that the solution provides authentication and encryption. Which of the following meets these requirements?
A. SIEM
B. Syslog
C. NetFlow
D. SNMPv3
Answer: (SHOW ANSWER)
SNMPv3 (Simple Network Management Protocol version 3) provides device monitoring with authentication and encryption. This enhances network visibility and security by ensuring that monitoring data is securely transmitted and access to network devices is authenticated.
Authentication: SNMPv3 includes robust mechanisms for authenticating users accessing network devices.
Encryption: It provides encryption to protect the integrity and confidentiality of the data being transmitted.
Network Management: SNMPv3 allows for detailed monitoring and management of network devices, ensuring better control and security.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers SNMP versions, their features, and security enhancements in SNMPv3.
Cisco Networking Academy: Provides training on implementing and securing SNMP for network management.
Network+ Certification All-in-One Exam Guide: Explains the benefits and security features of SNMPv3 for network monitoring.

NEW QUESTION: 53
A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?
A. 802.1Q tagging

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

NEW QUESTION: 54
A company reports that their facsimile machine no longer has a dial tone when trying to send a fax. The phone cable is damaged on one end. Which of the following types of connectors should a technician replace?
A. F-type
B. RJ45
C. SC
D. RJ11
Answer: (SHOW ANSWER)
Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.
F-type is used for coaxial cables (e.g., TV and cable modems).
RJ45 is used for Ethernet network connections.
SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.4 - Compare and contrast common network connectors.

NEW QUESTION: 55
Which of the following allows for the interception of traffic between the source and destination?

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

NEW QUESTION: 56
A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?
A. TXT
B. AAA
C. PTR
D. CNAME
Answer: (SHOW ANSWER)
To redirect a network resource that has moved from a local network to a Software-as-a-Service (SaaS) solution, the network administrator needs to configure a DNS record that maps an alias to the new canonical name (hostname) of the SaaS provider's server. The CNAME (Canonical Name) record is used to alias one domain name to another, effectively redirecting requests to the new hostname without needing to update the IP address directly. This is ideal for SaaS solutions, where the provider's server hostname is used, and the IP address may change dynamically.
Why not TXT? A TXT record is used to store arbitrary text data, such as SPF records for email authentication or verification strings, not for redirecting resources.
Why not AAA? There is no such thing as an "AAA" record in DNS. This might be a typo for AAAA (IPv6 address record), but AAAA maps a hostname to an IPv6 address, not an alias.
Why not PTR? A PTR record is used for reverse DNS lookups (mapping an IP address to a hostname), not for redirecting a resource to a new hostname.

Reference:CompTIA Network+ N10-009 Objective 1.5: Compare and contrast common network services and ports. The CNAME record is discussed under DNS configuration in the CompTIA Network+ Certification Study Guide (e.g., Mike Meyers' CompTIA Network+ Guide, Chapter 7: TCP/IP Applications). The guide explains that CNAME records are used to create aliases for hostnames, particularly useful for redirecting services to external providers like SaaS solutions.

NEW QUESTION: 57
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: 58
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: 59
Which of the following typically uses compromised systems that become part of a bot network?

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

NEW QUESTION: 60
After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?

A. Inspect the connectors for any wires that are touching or exposed.
B. Restore default settings on the connected devices.
C. Terminate the connections again.
D. Check for radio frequency interference in the area.
Answer: (SHOW ANSWER)
Cross talk can often be caused by improper termination of cables. The first step in troubleshooting should be to inspect the connectors for any wires that might be touching or exposed. Ensuring that all wires are correctly seated and that no conductors are exposed can help reduce or eliminate cross talk. This step should be taken before attempting to re-terminate the connections or check for other sources of interference.References:
CompTIA Network+ study materials.

NEW QUESTION: 61
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: 62
A network manager wants to implement a SIEM system to correlate system events. Which of the following protocols should the network manager verify?
A. NTP
B. DNS
C. LDAP
D. DHCP
Answer: (SHOW ANSWER)
* Role of NTP (Network Time Protocol):
* NTP is used to synchronize the clocks of network devices to a reference time source. Accurate time synchronization is critical for correlating events and logs from different systems.
* Importance for SIEM Systems:
* Event Correlation:SIEM (Security Information and Event Management) systems collect and analyze log data from various sources. Accurate timestamps are essential for correlating events across multiple systems.
* Time Consistency:Without synchronized time, it is challenging to piece together the sequence of events during an incident, making forensic analysis difficult.
* Comparison with Other Protocols:
* DNS (Domain Name System):Translates domain names to IP addresses but is not related to time synchronization.
* LDAP (Lightweight Directory Access Protocol):Used for directory services, such as user authentication and authorization.
* DHCP (Dynamic Host Configuration Protocol):Assigns IP addresses to devices on a network but does not handle time synchronization.
* Implementation:

* Ensure that all network devices, servers, and endpoints are synchronized using NTP. This can be achieved by configuring devices to use an NTP server, which could be a local server or an external time source.
References:
* CompTIA Network+ study materials on network protocols and SIEM systems.

NEW QUESTION: 63
A technician is deploying new networking hardware for company branch offices. The bridge priority must be properly set. Which of the following should the technician configure?
A. Spanning tree protocol
B. Jumbo frames
C. Perimeter network
D. Port security
Answer: (SHOW ANSWER)
Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology. Correctly configuring bridge priority helps in maintaining a loop-free and efficient network. The document explains:
"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

NEW QUESTION: 64
Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?
A. Theadministrator didnot provisionenough IP addresses.
B. Theadministrator configured an incorrect default gateway.
C. Theadministrator didnot provisionenough routes.
D. Theadministrator didnot provisionenough MAC addresses.
Answer: (SHOW ANSWER)
When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues.References:CompTIA Network+ study materials.

NEW QUESTION: 65
Which of the following network devices converts wireless signals to electronic signals?
A. Router
B. Firewall
C. Access point
D. Load balancer
Answer: (SHOW ANSWER)

* Role of an Access Point (AP):
* Wireless to Wired Conversion:An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.
* Functionality:
* Signal Conversion:The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.
* Connectivity:APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.
* Comparison with Other Devices:
* Router:Directs traffic between different networks and may include built-in AP functionality but is not primarily responsible for converting wireless to electronic signals.
* Firewall:Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.
* Load Balancer:Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.
* Deployment:
* APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.
References:
* CompTIA Network+ study materials on wireless networking and access points.

NEW QUESTION: 66
Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0
/24 subnet. Which of the following tools should the administrator use to best identify the devices?
A. dig
B. nmap
C. tracert
D. telnet
Answer: (SHOW ANSWER)
nmap (Network Mapper) is the best tool in this scenario. It can scan the 192.168.1.0/24 subnet to discover live hosts, open ports (like Telnet on port 23), and device types. It's ideal for mapping and auditing the network.
A). dig is a DNS lookup tool; not useful for identifying hosts on a subnet.
C). tracert shows the path packets take to a destination, not for host discovery.
D). telnet is the protocol being used, not a tool for scanning or identifying devices.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.1 - Given a scenario, use the appropriate network troubleshooting tools.

NEW QUESTION: 67
Which of the following will allow secure, remote access to internal applications?
A. VPN
B. CDN
C. SAN
D. IDS
Answer: (SHOW ANSWER)
A Virtual Private Network (VPN) creates an encrypted connection between a remote user and an internal network, ensuring secure access to internal applications.
* VPNs use encryption protocols like IPSec and SSL/TLS to protect data during transmission.
* They are widely used for secure remote work, accessing company resources, and bypassing geographic restrictions.
* Option B (CDN - Content Delivery Network): Used for speeding up website content delivery, not for remote access security.
* Option C (SAN - Storage Area Network): Used for high-speed storage, unrelated to remote access.
* Option D (IDS - Intrusion Detection System): Monitors for malicious activities but does not provide secure access to applications.
? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Secure Remote Access Technologies

NEW QUESTION: 68
A user's desk has a workstation and an IP phone. The user is unable to browse the internet on the workstation, but the phone works. Which of the following configurations is required?
A. Voice VLAN
B. Native VLAN
C. Data VLAN
D. Trunk port
Answer: C (LEAVE A REPLY)
If the IP phone works but the workstation doesn't, it indicates that theVoice VLAN is functioningcorrectly, but theData VLAN (C)is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately usingVLANs.
* A. Voice VLANis for the IP phone, which is already working.
* B. Native VLANis for untagged traffic on trunk ports, but doesn't control access directly.
* D. Trunk portis more relevant to switch interconnections than individual workstation ports.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 69

Before using a guest network, an administrator requires users to accept the terms of use Which of the following is the best way to accomplish this goal?

A. Pre-shared key

B. Autonomous access point

C. Captive portal

D. WPA2 encryption

Answer: (SHOW ANSWER)

A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. References: CompTIA Network+ Exam Objectives and official study guides.

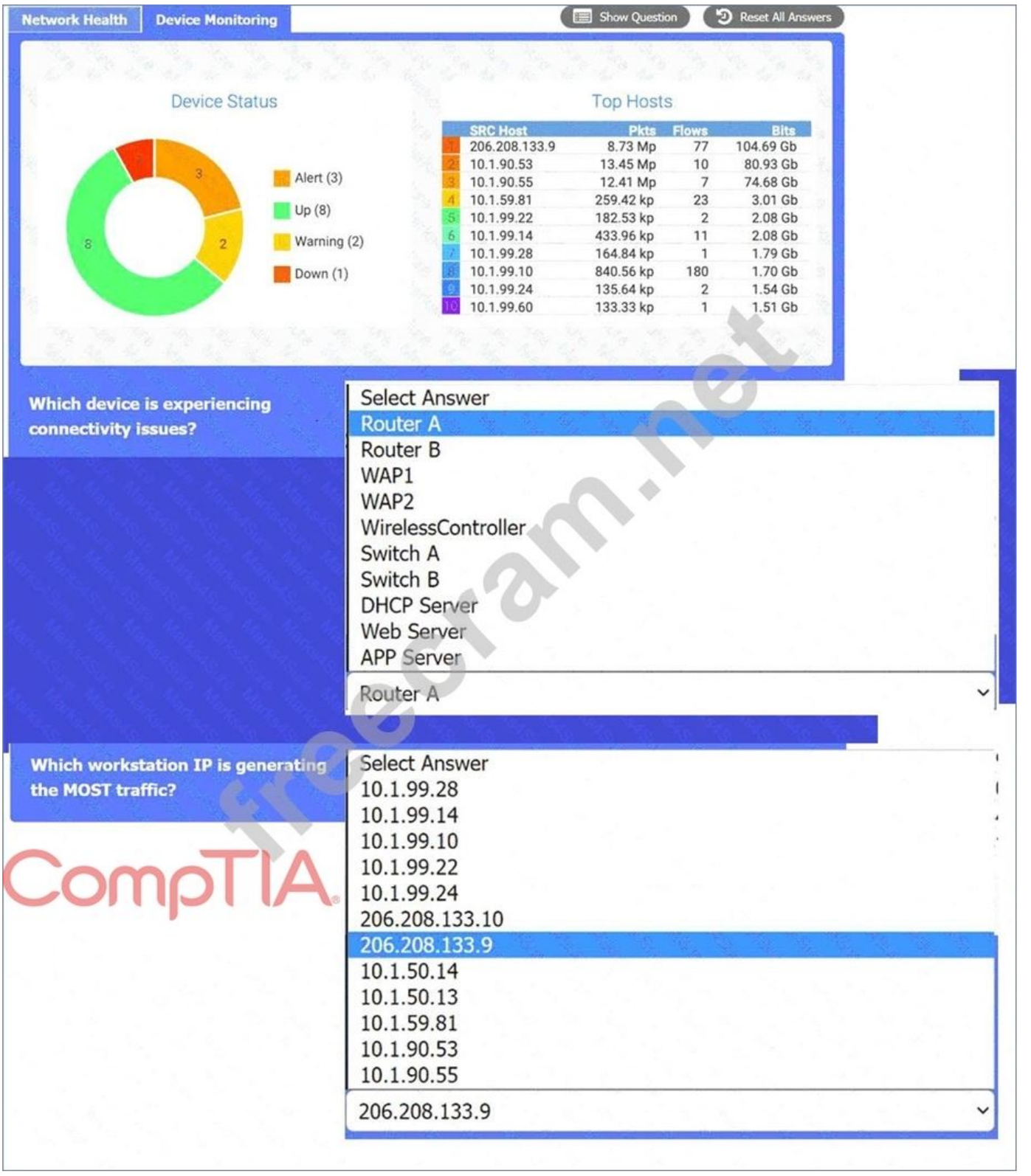
NEW QUESTION: 70

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:

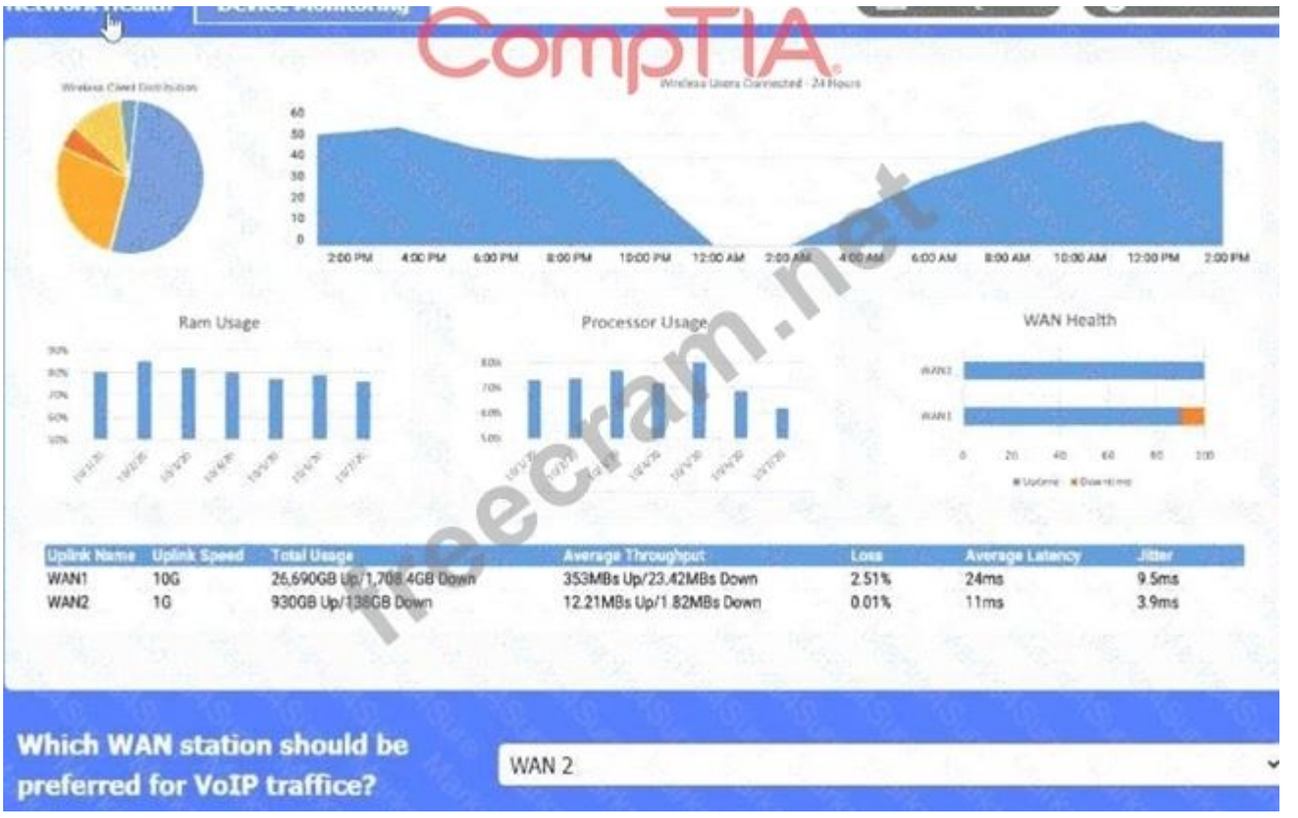
See the answer and solution below.

Explanation:

Network Health:

WAN 2 appears to have a lower average latency and loss percentage, which would make it the preferred WAN station for VoIP traffic. VoIP traffic requires low latency and packet loss to ensure

good voice quality and reliability. WAN 1 seems to have higher RAM and processor usage, which could also affect the performance of VoIP traffic.
Here's the summary of the key metrics for WAN 1 and WAN 2 from the image provided:
WAN 1:
Uplink Speed: 10G
Total Usage: 26.969GB Up / 1.748GB Down
Average Throughput: 353MBps Up / 23.42MBps Down
Loss: 2.51%
Average Latency: 24ms
Jitter: 9.5ms
WAN 2:
Uplink Speed: 1G
Total Usage: 930GB Up / 138GB Down
Average Throughput: 12.21MBps Up / 1.82MBps Down
Loss: 0.01%
Average Latency: 11ms
Jitter: 3.9ms
For VoIP traffic, low latency and jitter are particularly important to ensure voice quality. While WAN 1 has higher bandwidth and throughput, it also has higher latency and jitter compared to WAN 2. However, WAN 2 has much lower loss, lower latency, and lower jitter, which are more favorable for VoIP traffic that is sensitive to delays and variation in packet arrival times.
Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive to latency and jitter, such as bulk data transfers.
Device Monitoring:
the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down.
This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.
A screenshot of a computer AI-generated content may be incorrect.



NEW QUESTION: 71
Which of the following fiber connector types is the most likely to be used on a network interface card?
A. LC
B. SC
C. ST
D. MPO
Answer: (SHOW ANSWER)
* Definition of Fiber Connector Types:
* LC (Lucent Connector):A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.
* SC (Subscriber Connector or Standard Connector):A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.
* ST (Straight Tip):A bayonet-style connector, typically used in multimode fiber optic networks.
* MPO (Multi-fiber Push On):A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.
* Common Usage:
* LC Connectors:Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.
* SC and ST Connectors:These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.

* MPO Connectors:Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.
* Selection Criteria:
* The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.
References:
* CompTIA Network+ study materials on fiber optics and connector types.

NEW QUESTION: 72
After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?
A. Check to see if the end connections were wrapped in copper tape before terminating.
B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
C. Connect the RX/TX wires to different pins.
D. Run a speed test on a device that can only achieve 100Mbps speeds.
Answer: (SHOW ANSWER)
* Importance of Proper Termination:
* Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).
* Interference Troubleshooting:
* Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.
* Why Other Options are Less Likely:
* Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.
* Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.
* Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds.
* Corrective Actions:
* Verify that all end connections are properly wrapped with copper tape before termination.
* Ensure that the shielding is continuous and properly grounded throughout the installation.
* Retest the cabling for interference after making corrections.
References:
* CompTIA Network+ study materials and structured cabling installation guides.

NEW QUESTION: 73

An employee in a corporate office clicks on a link in an email that was forwarded to them. The employee is redirected to a splash page that says the page is restricted. Which of the following security solutions is most likely in place?

A. DLP

B. Captive portal

C. Content filtering

D. DNS sinkholing

Answer: (SHOW ANSWER)

Content filtering blocks access to restricted or malicious websites. When a user attempts to visit a site that violates company policies, they are redirected to a restriction page.

* This is a common security measure to prevent employees from accessing phishing or malware-infected sites.
* Content filters work by scanning URLs, keywords, or categories and blocking inappropriate or harmful content.
* Option A (DLP - Data Loss Prevention): Focuses on preventing sensitive data leaks rather than blocking web access.
* Option B (Captive portal): Used mainly in public Wi-Fi to authenticate users before granting access, not to restrict sites.
* Option D (DNS sinkholing): Redirects malicious domain requests to a safe address but is not responsible for policy-based restrictions on general content.

? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Security Solutions

NEW QUESTION: 74

A critical infrastructure switch is identified as end-of-support. Which of the following is the best next step to ensure security?

A. Apply the latest patches and bug fixes.

B. Decommission and replace the switch.

C. Ensure the current firmware has no issues.

D. Isolate the switch from the network.

Answer: (SHOW ANSWER)

* Understanding End-of-Support:
* End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.
* Risks of Keeping an End-of-Support Device:
* Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats.
* Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.
* Best Next Step - Replacement:

* Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.
* Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.
* Comparison with Other Options:
* Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.
* Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.
* Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.
References:
* CompTIA Network+ study materials on network maintenance and security best practices.

NEW QUESTION: 75
A major natural disaster strikes a company's headquarters, causing significant destruction and data loss. The company needs to quickly recover and resume operations. Which of the following will a network administrator need to do first?
A. Conduct a damage assessment
B. Migrate to the cold site
C. Notify customers of the disaster
D. Establish a communication plan
Answer: (SHOW ANSWER)
In disaster recovery, the first step after an incident is to conduct a thorough damage assessment to understand the extent of the damage and determine the next appropriate steps. This allows for informed decision-making during the recovery process. The document says:
"The first step after a disaster is to conduct a damage assessment. This involves evaluating the extent of damage to equipment, infrastructure, and data, forming the foundation for recovery efforts and prioritizing response actions."

NEW QUESTION: 76
A company discovers on video surveillance recordings that an unauthorized person installed a rogue access point in its secure facility. Which of the following allowed the unauthorized person to do this?
A. Evil twin
B. Honeytrap
C. Wardriving
D. Tailgating
Answer: (SHOW ANSWER)

Tailgatingis a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.
* A. Evil twinis a wireless attack where an attacker sets up a fake AP.
* B. Honeytrapis used to attract attackers for analysis.
* C. Wardrivinginvolves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.

NEW QUESTION: 77
Which of the following layers in the OSI model is responsible for establishing, maintaining, and terminating connections between nodes?
A. Physical
B. Network
C. Session
D. Transport
Answer: (SHOW ANSWER)
TheSession Layer(Layer 5 of the OSI Model) is responsible for setting up, managing, and tearing down sessions between applications. It maintains dialog control and synchronizes data exchange between systems.
Reference:Section 1.1 - OSI Reference Model Concepts - "Layer 5 - Session"

NEW QUESTION: 78
A user cannot access an external server for a client after connecting to a VPN. Which of the following commands would a support agent most likely use to examine the issue? (Select two).
A. nslookup
B. tcpdump
C. arp
D. dig
E. tracert

F. route print

Answer: (SHOW ANSWER)

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

E). tracert:

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

Helps determine if the traffic is being blocked or misrouted.

F). route print:

Displays the device's routing table.

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

Incorrect Options:

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

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

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

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

Reference:

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

NEW QUESTION: 79

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

A. Geofencing

B. Honeynet

C. Jumpbox

D. Screened subnet

Answer: (SHOW ANSWER)

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

NEW QUESTION: 80

Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?

A. Crash cart

B. Jump box

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

NEW QUESTION: 81
A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?
A. netstat
B. nslookup
C. ping
D. tracert
Answer: (SHOW ANSWER)
* Understanding Tracert:
* Traceroute Tool:tracert(Windows) ortraceroute(Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.
* Determining Traffic Path:
* Path Identification:By runningtracertto the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.
* Load Balancing Insight:If the office uses load balancing for its internet links,tracertcan help verify which link is currently handling the traffic for the web application.
* Comparison with Other Tools:
* netstat:Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
* nslookup:Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.

* ping:Tests connectivity and measures round-trip time but does not provide path information.
* Implementation:
* Open a command prompt or terminal.
* Executetracert [destination IP]to trace the route.
* Analyze the output to determine the path and the link being used.
References:
* CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

NEW QUESTION: 82
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: 83
Following a fire in a data center, the cabling was replaced. Soon after, an administrator notices network issues. Which of the following are the most likely causes of the network issues? (Select two).
A. The switches are not the correct voltage.
B. The HVAC system was not verified as fully functional after the fire.
C. The VLAN database was not deleted before the equipment was brought back online.
D. The RJ45 cables were replaced with unshielded cables.
E. The wrong transceiver type was used for the new termination.
F. The new RJ45 cables are a higher category than the old ones.
Answer: (SHOW ANSWER)
* Unshielded cables (D) are more prone to interference and may not be suitable for certain environments, especially after a fire where interference could be heightened.
* Using the wrong transceiver (E) for new terminations can lead to compatibility issues, causing network failures.

NEW QUESTION: 84

Which of the following would most likely be utilized to implement encryption in transit when using HTTPS?

A. SSH

B. TLS

C. SCADA

D. RADIUS

Answer: (SHOW ANSWER)

TLS (Transport Layer Security)is the protocol that providesencryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.

* A. SSHis used for secure terminal access, not HTTPS.
* C. SCADArefers to control systems, not encryption protocols.
* D. RADIUSis an authentication protocol, not for encrypting HTTPS traffic.

#Reference:

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

CompTIA Network+ N10-009 Official Objectives: 4.6 - Explain authentication and access controls.

NEW QUESTION: 85

A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?

A. Toner

B. Laptop

C. Cable tester

D. Visual fault locator

Answer: (SHOW ANSWER)

A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.

* Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.
* Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.
* Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.

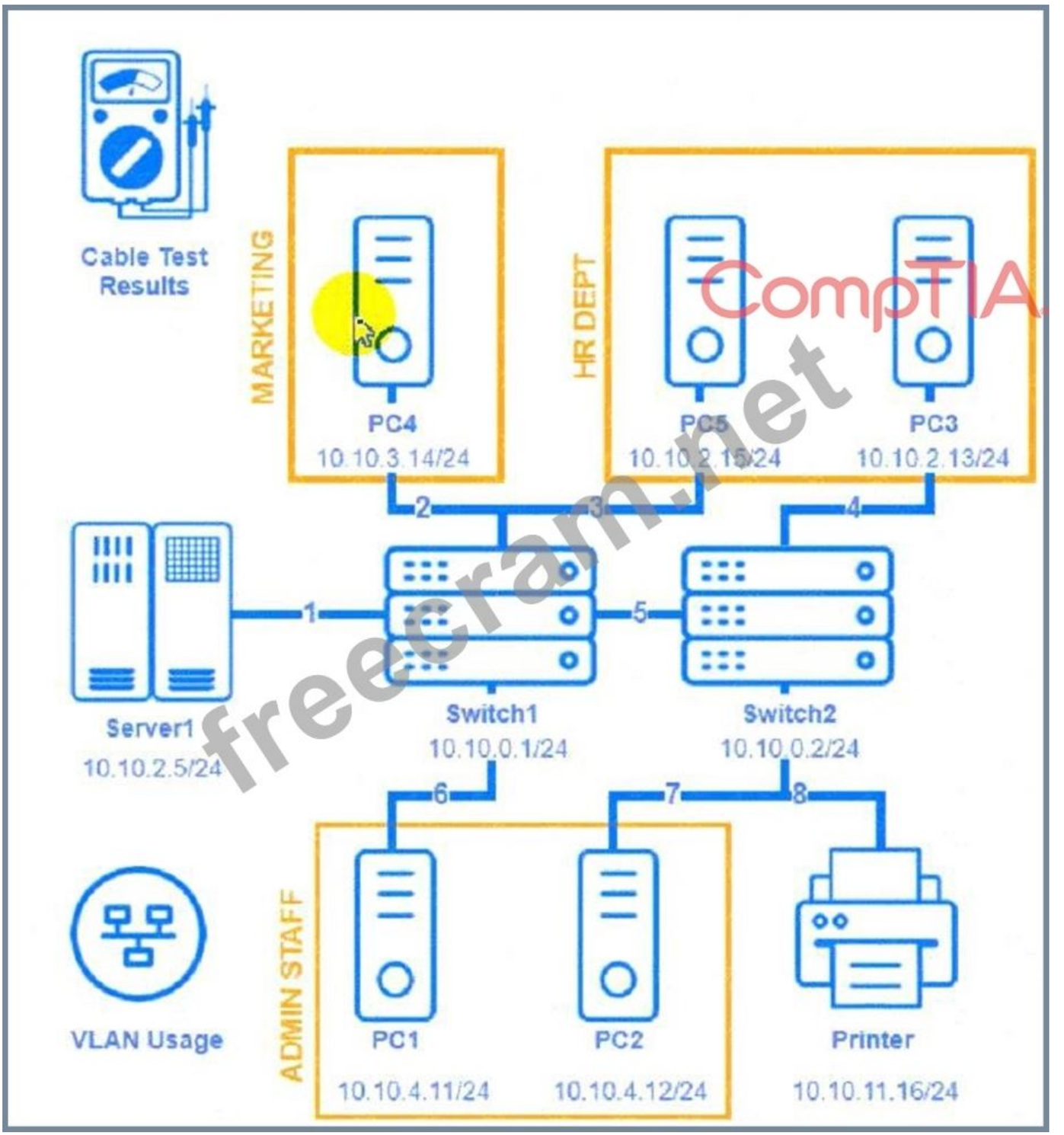
Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Details tools used for cable identification and troubleshooting.

* Cisco Networking Academy: Provides training on using toner probes and other cable testing tools.
* Network+ Certification All-in-One Exam Guide: Explains the use of different tools for network cable identification and management.

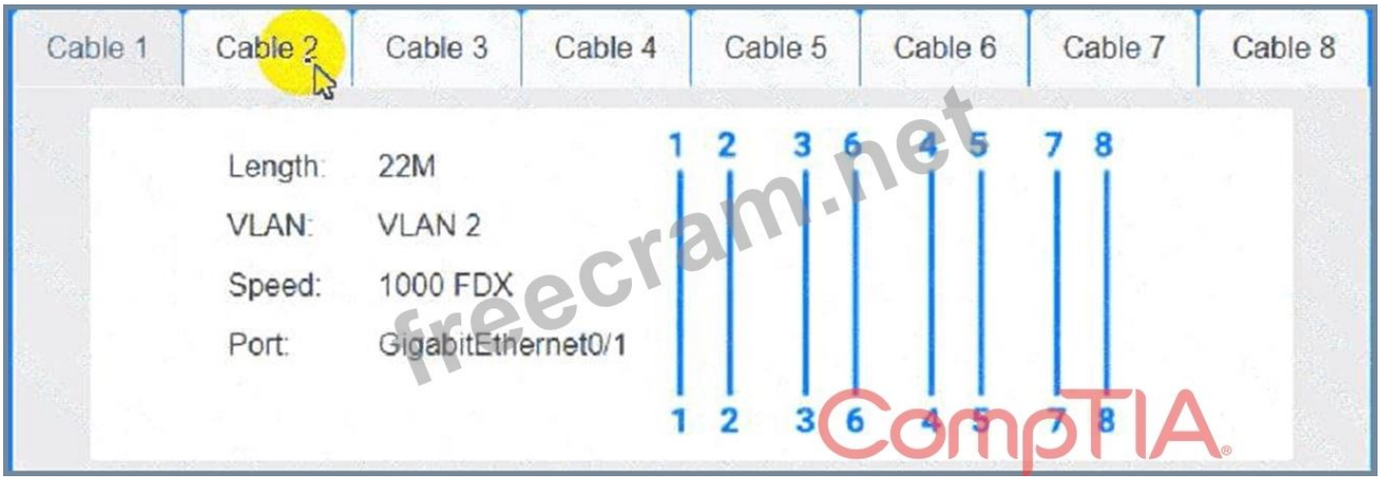
NEW QUESTION: 86
A network engineer is troubleshooting connectivity for a newly installed server on an existing VLAN. The engineer reviews the following output:
C:\> ipconfig
IP Address: 192.168.100.225
Mask: 255.255.255.224
Gateway: 192.168.100.254
Router# show ip route
C 192.168.100.0/24 is directly connected, GigabitEthernet0/0
Which of the following describes the issue?
A. The server has an incorrect subnet mask
B. There is a duplicate IP address on the network
C. The DHCP address pool is exhausted
D. The router is missing a default route
Answer: A (LEAVE A REPLY)
The server's subnet mask is 255.255.255.224 (/27), which covers IPs from 192.168.100.224 to 192.168.100.255. However, the router only recognizes 192.168.100.0/24, indicating a mismatch between the server's subnet and the router's network.
Correct mask for the /24 network is 255.255.255.0, allowing 256 IPs from 192.168.100.0 to 192.168.100.255.
This mismatch would result in routing issues, especially with the gateway outside of the subnet range.
Reference:
CompTIA Network+ N10-009 Official Objectives: 5.2 - Given a scenario, troubleshoot common wired connectivity issues.

NEW QUESTION: 87
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.



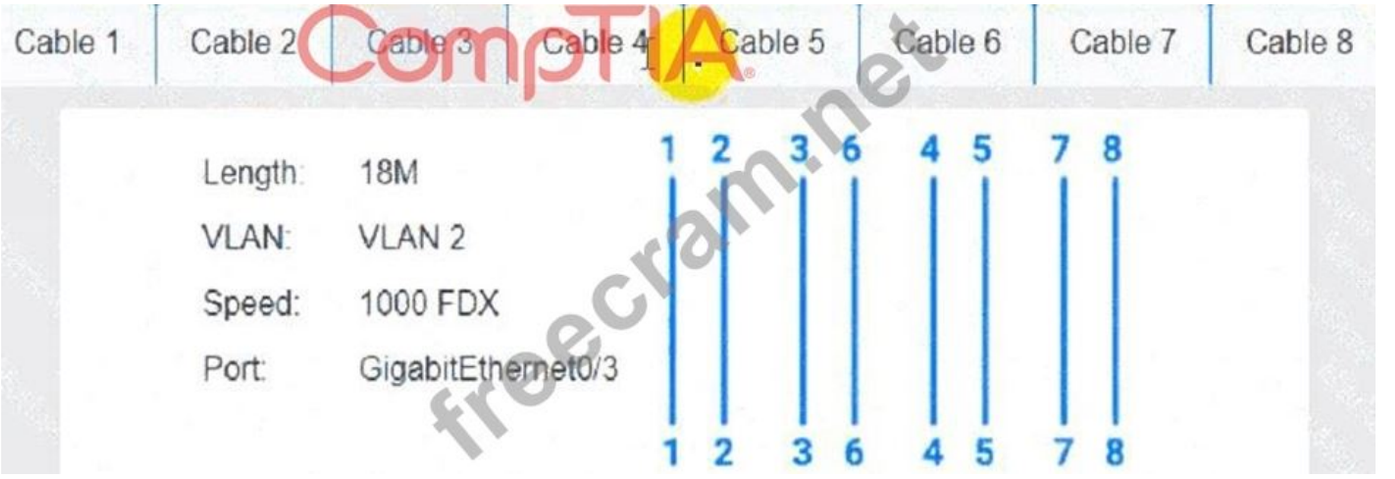
Cable Test Results:

Cable 1:

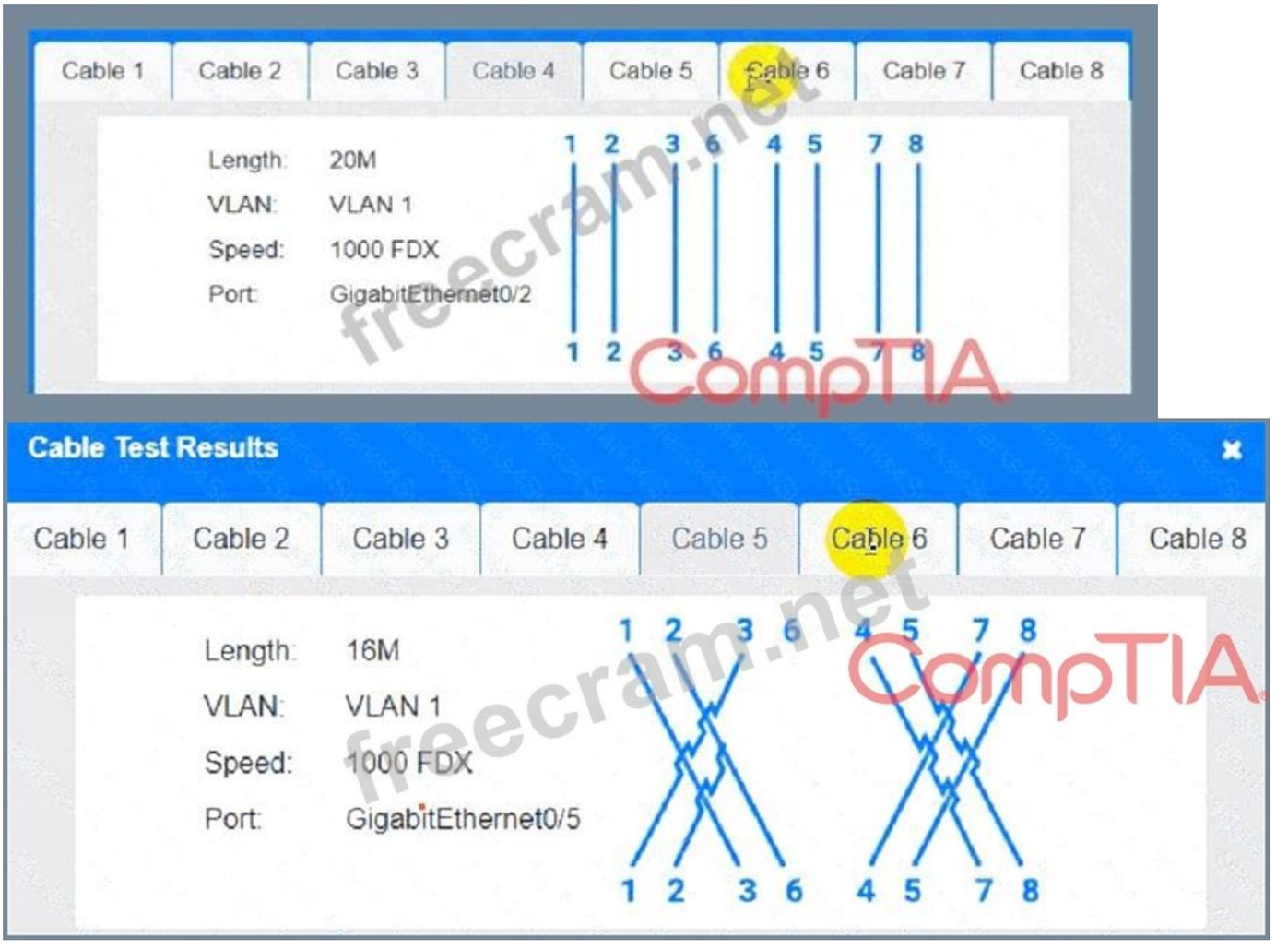


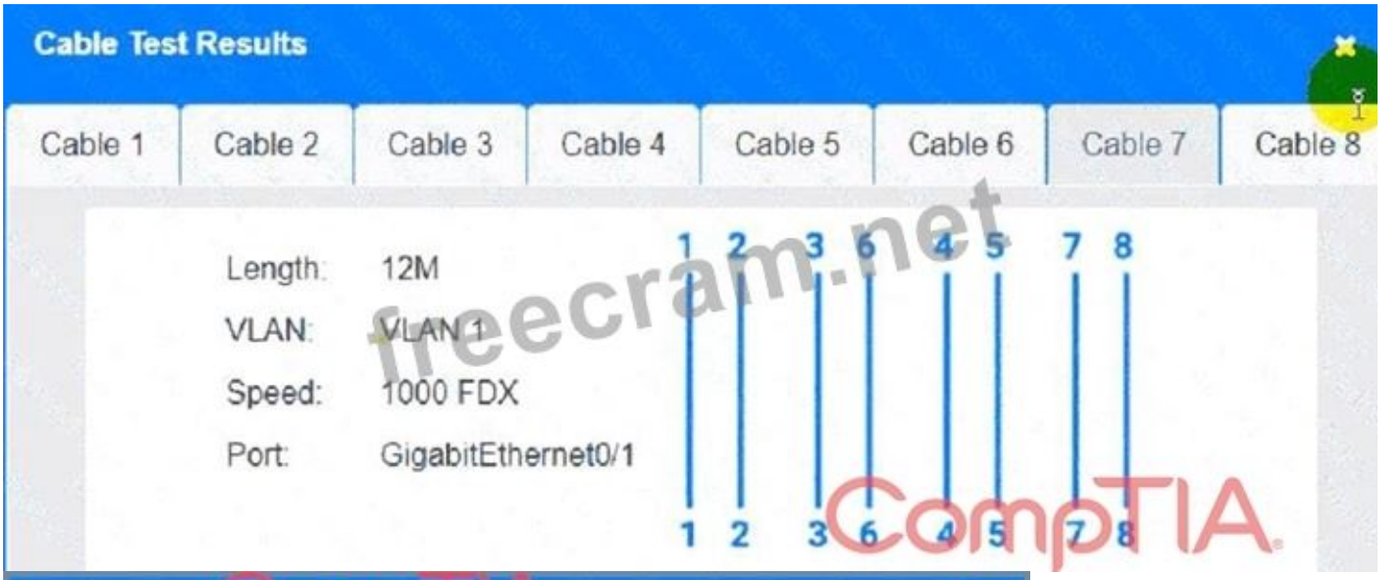
Cable 2:

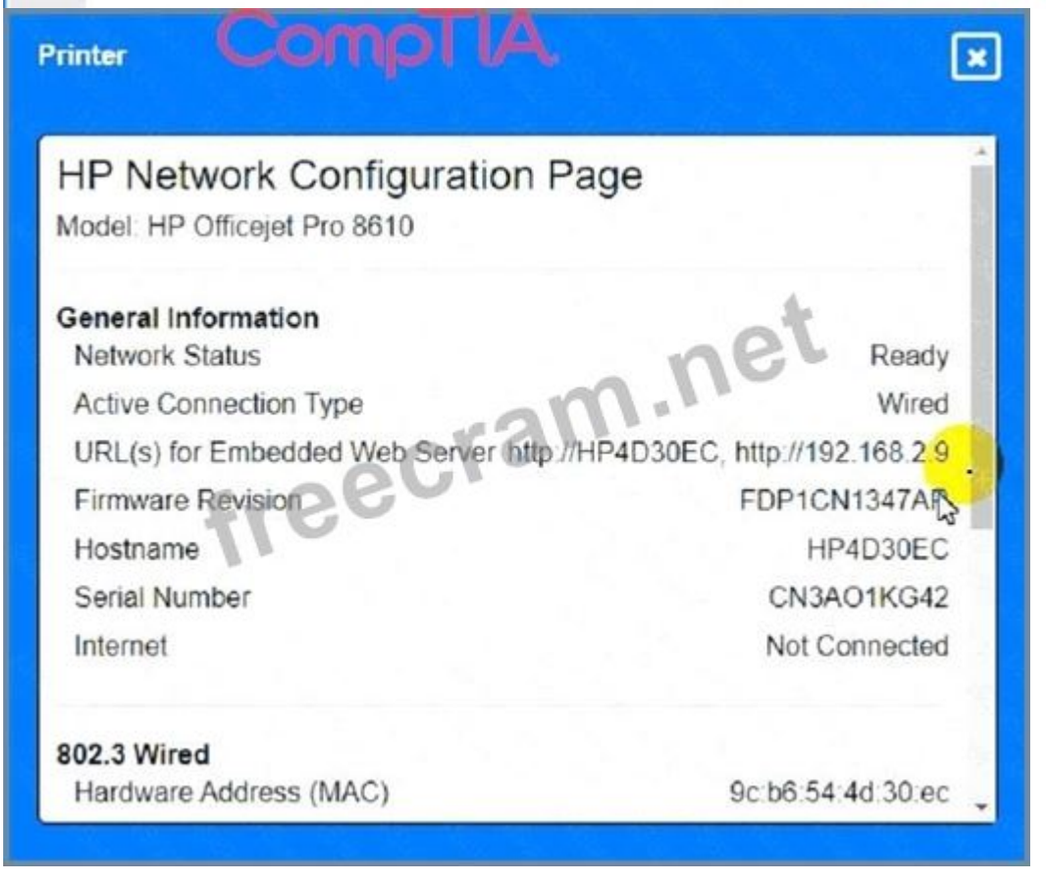
Cable 3:

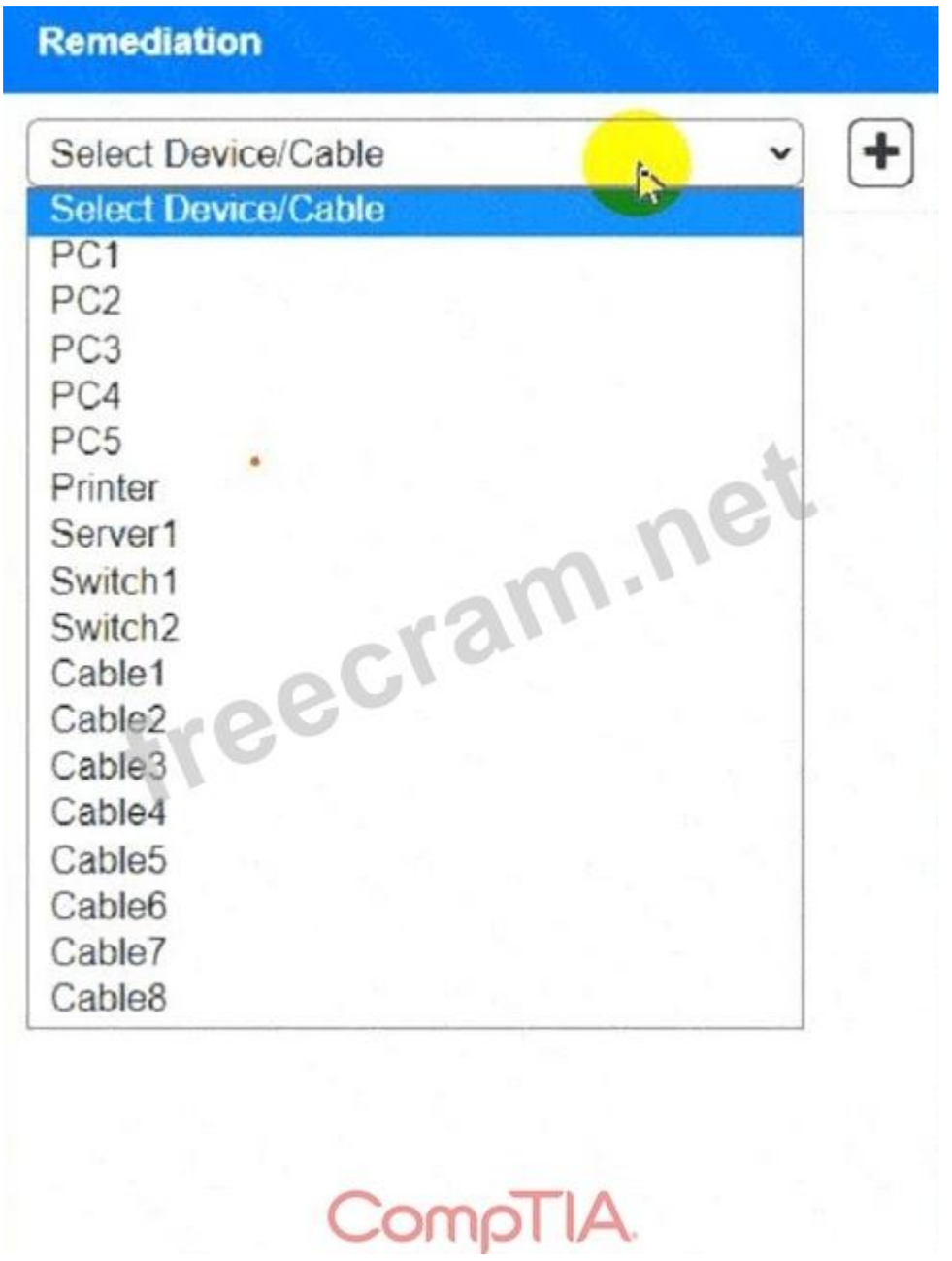


Cable 4:









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: 88
An administrator is configuring a switch that will be placed in an area of the office that is accessible to customers. Which of the following is the best way for the administrator to mitigate unknown devices from connecting to the network?
A. SSE
B. ACL
C. Perimeter network
D. 802.1x
Answer: (SHOW ANSWER)
802.1x is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. This ensures that only authorized devices can access the network, making it ideal for mitigating the risk of unknown devices connecting to the network, especially in accessible areas.
* 802.1x Authentication: Requires devices to authenticate using credentials (e.g., username and password, certificates) before gaining network access.

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

NEW QUESTION: 89
A network administrator changed an external DNS to point customers to a new server. Which of the following tools should the administrator use to test the new server's configuration?
A. ping
B. tracert
C. tcpdump
D. nslookup
Answer: (SHOW ANSWER)
*nslookup allows querying DNS records to verify if the new server is correctly resolving domain names.
*ping (A) tests basic connectivity, not DNS configuration.
*tracert (B) shows network path latency but doesn't test DNS.
*tcpdump (C) captures packets but isn't ideal for DNS verification.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Testing Tools.

NEW QUESTION: 90
A storage network requires reduced overhead and increased efficiency for the amout of data being sent. Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
* Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.

* Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
* Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.
* Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.
* Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

NEW QUESTION: 91
A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?
A. Port
B. DNS
C. MAC
D. Content
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 92
A network administrator installs new cabling to connect new computers and access points. After deploying the equipment, the administrator notices a few of the devices are not connecting properly. The administrator moves the devices to a different port, but it does not resolve the issue. Which of the following should the administrator verify next?
A. Power budget
B. Device requirements
C. Port status

D. Cable termination

Answer: (SHOW ANSWER)

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

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

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

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

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

NEW QUESTION: 93

While troubleshooting a VoIP handset connection, a technician's laptop is able to successfully connect to network resources using the same port. The technician needs to identify the port on the switch. Which of the following should the technician use to determine the switch and port?

A. LLDP

B. IKE

C. VLAN

D. netstat

Answer: (SHOW ANSWER)

Link Layer Discovery Protocol (LLDP) is a network protocol used for discovering devices and their capabilities on a local area network, primarily at the data link layer (Layer 2). It helps in identifying the connected switch and the specific port to which a device is connected. When troubleshooting a VoIP handset connection, the technician can use LLDP to determine the exact switch and port where the handset is connected. This protocol is widely used in network management to facilitate the discovery of network topology and simplify troubleshooting.

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

Reference: CompTIA Network+ Certification Exam Objectives - Network Troubleshooting and Tools section.

NEW QUESTION: 94

Which of the following is used to stage copies of a website closer to geographically dispersed users?

A. VPN

B. CDN

C. SAN

D. SDN

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

NEW QUESTION: 95
A network engineer is testing a website to ensure it is compatible with IPv6. After attempting to ping the website by its IPv6 address, the engineer determines that the DNS has not been set up properly. Which of the following should the network engineer complete to resolve this issue?
A. Enable a PTR record.
B. Update the existing TXT record.
C. Add a new AAAA record.
D. Configure a secondary NS record.
Answer: (SHOW ANSWER)
*AAAA records map domain names to IPv6 addresses, enabling proper resolution.
*PTR records (A) are for reverse DNS lookups.
*TXT records (B) store text-based information, not IP addresses.
*NS records (D) define authoritative name servers but don't directly affect IPv6 resolution.
#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Configuration & IPv6.

NEW QUESTION: 96
Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).
A. Fire suppression system
B. UPS location
C. Humidity control
D. Power load
E. Floor construction type
F. Proximity to nearest MDF
Answer: (SHOW ANSWER)
When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as

corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.References:CompTIA Network+ study materials.

NEW QUESTION: 97
A network engineer wants to implement a new IDS between the switch and a router connected to the LAN.
The engineer does not want to introduce any latency by placing the IDS in line with the gateway.
The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?
A. Use a network tap.
B. Use Nmap software.
C. Use a protocol analyzer.
D. Use a port mirror.
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 98
Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?
A. Site-to-site VPN
B. GRE tunnel
C. VXLAN
D. Dedicated line
Answer: (SHOW ANSWER)
A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.
Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.
Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.
Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.
Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

NEW QUESTION: 99
Which of the following must be implemented to securely connect a company's headquarters with a branch location?
A. Split-tunnel VPN
B. Clientless VPN
C. Full-tunnel VPN
D. Site-to-site VPN
Answer: (SHOW ANSWER)
Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.
Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.
Clientless VPN (B): Used for individual users to access the network without VPN client software.
Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Secure Network Connections).

NEW QUESTION: 100
A company is purchasing a 40Gbps broadband connection service from an ISP. Which of the following should most likely be configured on the 10G switch to take advantage of the new service?

A. 802.1Q tagging
B. Jumbo frames
C. Half duplex
D. Link aggregation
Answer: (SHOW ANSWER)
Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.
IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

NEW QUESTION: 101
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. Point-to-point
C. Infrastructure
D. Ad hoc
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following should be configured so users can authenticate to a wireless network using company credentials?
A. SSO
B. SAML
C. MFA
D. RADIUS
Answer: (SHOW ANSWER)
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.References:CompTIA Network+ study materials.

NEW QUESTION: 103
Which of the following ports is used for secure email?
A. 25
B. 110
C. 143
D. 587
Answer: (SHOW ANSWER)
Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption.
Port 25: Traditionally used for SMTP relay, but not secure and often blocked by ISPs for outgoing mail due to spam concerns.
Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured.
Port 143: Used for IMAP (Internet Message Access Protocol), which can be secured with STARTTLS or SSL
/TLS.
Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.
Network References:

CompTIA Network+ N10-007 Official Certification Guide: Discusses email protocols and ports, including secure email transmission.
Cisco Networking Academy: Provides training on securing email communications and the use of appropriate ports.
Network+ Certification All-in-One Exam Guide: Explains email protocols, ports, and security considerations for email transmission.

NEW QUESTION: 104
A network engineer needs to add a boundary network to isolate and separate the internal network from the public-facing internet. Which of the following security defense solutions would best accomplish this task?
A. Trusted zones
B. URL filtering
C. ACLs
D. Screened subnet
Answer: (SHOW ANSWER)
Ascreened subnet, also known as aDMZ (Demilitarized Zone), is aboundary networkthat separates an organization's internal network from external-facing systems. It is used to host public services like web or email servers while protecting internal systems from exposure.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "Screened Subnet (DMZ)"

NEW QUESTION: 105
Which of the following could provide a lightweight and private connection to a remote box?
A. Site-to-site VPN
B. Telnet
C. Console
D. Secure Shell
Answer: (SHOW ANSWER)
Secure Shell (SSH)is a protocol used tosecurely access remote devices over an unsecured network. It provides encrypted command-line access and is a lightweight and secure method of remote administration.
* A. Site-to-site VPNconnects entire networks, not just a single host.
* B. Telnetis not secure; it transmits data (including credentials) in plaintext.
* C. Consoleaccess is direct via serial cable, not remote.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 2.6 - Configure and troubleshoot remote access.

NEW QUESTION: 106
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: (SHOW ANSWER)

Quality of Service (QoS)is the best cost-effective solution. It prioritizes traffic based on application criticality.

If the bandwidth is limited and only a few users are affected, prioritizing that application traffic can improve performance without needing costly bandwidth upgrades or direct connections.

Reference:Section 1.2 - Networking Appliances, Applications, and Functions - "Quality of Service (QoS)"

NEW QUESTION: 107

Three access points have Ethernet that runs through the ceiling. One of the access points cannot reach the internet. Which of the following tools can help identify the issue?

A. Network tap

B. Cable tester

C. Visual fault locator

D. Toner and probe

Answer: (SHOW ANSWER)

A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

NEW QUESTION: 108

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

A. ST

B. RJ45

C. BNC

D. SFP

Answer: (SHOW ANSWER)

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

NEW QUESTION: 109
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: 110

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: 111

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

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

Answer: (SHOW ANSWER)

A system has reachedend-of-supportwhen thevendor no longer provides patches, updates, or bug fixes. This significantly increases the risk of security vulnerabilities and is a major operational concern.
Reference:Section 3.3 - Disaster Recovery Concepts - "End-of-Support Considerations"

NEW QUESTION: 112

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

NEW QUESTION: 113
A network administrator is configuring access points for installation in a dense environment where coverage is often overlapping. Which of the following channel widths should the administrator choose to help minimize interference in the 2.4GHz spectrum?
A. 11MHz
B. 20MHz
C. 40MHz
D. 80MHz
E. 160MHz
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

NEW QUESTION: 114
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: C (LEAVE A REPLY)
* Understanding Multicast:
* Multicast IP Address Range:The multicast address range is from 224.0.0.0 to 239.255.255.255, designated for multicast traffic.
* Multicast Applications:

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

NEW QUESTION: 115
Which of the following is a major difference between an IPS and IDS?
A. An IPS needs to be installed in line with traffic and an IDS does not.
B. An IPS is signature-based and an IDS is not.
C. An IPS is less susceptible to false positives than an IDS.
D. An IPS requires less administrative overhead than an IDS.
Answer: A (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: 116
Which of the following most likely determines the size of a rack for installation? (Select two).
A. KVM size
B. Switch depth
C. Hard drive size

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

NEW QUESTION: 117
Which of the following is a cost-effective advantage of a split-tunnel VPN?
A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company's network.
D. Cloud-based traffic flows outside of the company's network.
Answer: (SHOW ANSWER)
A split-tunnel VPN allows some traffic to be routed through the VPN while other traffic goes directly to the internet. This setup offers several advantages, with a primary one being cost-effectiveness due to cloud-based traffic not consuming company bandwidth.

* Bandwidth Utilization: Split-tunnel VPNs reduce the amount of traffic passing through the company's network, freeing up bandwidth for other uses.
* Performance: By allowing internet-bound traffic to bypass the VPN, it can reduce latency and improve the performance for users accessing cloud services directly.
* Cost Savings: Reduced load on the company's VPN infrastructure can lead to lower costs in terms of both hardware and bandwidth.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers VPN types, including split-tunnel configurations and their advantages.
* Cisco Networking Academy: Discusses VPN technologies and the benefits of split-tunneling.
* Network+ Certification All-in-One Exam Guide: Provides detailed information on VPN setups, including the cost-effectiveness of split-tunnel VPNs.
By allowing cloud-based traffic to flow outside the company's network, a split-tunnel VPN optimizes resource usage and enhances the overall network performance without incurring extra costs for bandwidth.

NEW QUESTION: 118
A network engineer is now in charge of all SNMP management in the organization. The engineer must use a SNMP version that does not utilize plaintext data. Which of the following is the minimum version of SNMP that supports this requirement?
A. v1
B. v2c
C. v2u
D. v3
Answer: (SHOW ANSWER)
SNMPv3 is the version of the Simple Network Management Protocol that introduces security enhancements, including message integrity, authentication, and encryption. Unlike previous versions (v1 and v2c), SNMPv3 supports encrypted communication, ensuring that data is not transmitted in plaintext. This provides confidentiality and protects against eavesdropping and unauthorized access.References:CompTIA Network+ study materials.

NEW QUESTION: 119
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: 120

Which of the following is the best way to reduce the likelihood of electrostatic discharge?

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

NEW QUESTION: 121
Which of the following is the next step to take after successfully testing a root cause theory?
A. Determine resolution steps.
B. Duplicate the problem in a lab.
C. Present the theory for approval.
D. Implement the solution to the problem.
Answer: (SHOW ANSWER)
* Troubleshooting Methodology:
* Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.
* Implementation of the Solution:
* Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.

* Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.
* Comparison with Other Steps:
* Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.
* Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.
* Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.
* Final Verification:
* After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.
References:
* CompTIA Network+ study materials on troubleshooting methodologies and best practices.

NEW QUESTION: 122
Which of the following network cables involves bounding light off of protective cladding?
A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode
Answer: (SHOW ANSWER)
Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.
Here are some detailed points about multimode fiber cables:
Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single- mode fibers, which have a core diameter of about 9 microns.
Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.

Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers.
Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.
Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.
Network References:
CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.
Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.
Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.
Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

NEW QUESTION: 123
A company receives a cease-and-desist order from its ISP regarding prohibited torrent activity.
Which of the following should be implemented to comply with the cease-and-desist order?
A. MAC security
B. Content filtering
C. Screened subnet
D. Perimeter network
Answer: (SHOW ANSWER)
Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease- and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.
References: CompTIA Network+ study materials.

NEW QUESTION: 124
Which of the following is enforced through legislation?
A. AUP
B. GDPR
C. Code of conduct
D. EULA
Answer: (SHOW ANSWER)
GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or

codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences.
Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

NEW QUESTION: 125
A company is implementing a wireless solution in a high-density environment. Which of the following 802.11 standards is used when a company is concerned about device saturation and converage?
A. 802.11ac
B. 802.11ax
C. 802.11g
D. 802.11n
Answer: (SHOW ANSWER)
802.11ax, also known as Wi-Fi 6, is designed for high-density environments and improves device saturation and coverage compared to previous standards.
802.11ac: While it offers high throughput, it is not optimized for high-density environments as effectively as
802.11ax.
802.11ax (Wi-Fi 6): Introduces features like OFDMA, MU-MIMO, and BSS Coloring, which enhance performance in crowded environments, reduce latency, and increase the number of devices that can be connected simultaneously.
802.11g and 802.11n: Older standards that do not offer the same level of efficiency or support for high device density as 802.11ax.
Network References:
CompTIA Network+ N10-007 Official Certification Guide: Covers the 802.11 standards and their capabilities.
Cisco Networking Academy: Provides training on Wi-Fi technologies and best practices for high-density deployments.
Network+ Certification All-in-One Exam Guide: Discusses the various 802.11 standards and their applications in different environments.

NEW QUESTION: 126
Newly crimped 26ft (8m) STP Cat 6 patch cables were recently installed in one room to replace cables that were damaged by a vacuum cleaner. Now, users in that room are unable to connect to the network. A network technician tests the existing cables first. The 177ft (54m) cable that runs from the core switch to the access switch on the floor is working, as is the 115ft (35m) cable run from the access switch to the wall jack in the office. Which of the following is the most likely reason the users cannot connect to the network?
A. Mixed UTP and STP cables are being used.
B. The patch cables are not plenum rated.
C. The cable distance is exceeded.

D. An incorrect pinout on the patch cable is being used.

Answer: (SHOW ANSWER)

An incorrect pinout on the patch cable could prevent network connectivity due to mismatched wiring. Even if the cables are the correct length and type, a pinout issue can cause continuity problems and prevent data transmission. Proper crimping with the correct pinout is essential for network cables to function. (Reference:
CompTIA Network+ Study Guide, Chapter on Network Media and Topologies)

NEW QUESTION: 127

A network administrator is troubleshooting a connectivity issue between two devices on two different subnets.

The administrator verifies that both devices can successfully ping other devices on the same subnet. Which of the following is the most likely cause of the connectivity issue?

A. Incorrect default gateway

B. Faulty Ethernet cable

C. Wrong duplex settings

D. VLAN mismatch

Answer: (SHOW ANSWER)

When two devices on different subnets are unable to communicate, but can communicate with other devices on their own subnet, the issue is most often related to routing. Devices on different subnets require a default gateway to route traffic between networks.

If the default gateway is incorrectly configured, the device won't know how to reach other subnets.

Faulty cables (Option B) or duplex mismatches (Option C) would likely cause connectivity issues even within the local subnet, which is not the case here.

VLAN mismatches (Option D) are typically issues with switch port configurations and would likely cause total loss of connectivity, including within the same subnet.

So, the most probable and logical cause is an incorrect default gateway.

Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.4: "Compare and contrast routing technologies."

NEW QUESTION: 128

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: (SHOW ANSWER)

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 References:
* 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: 129
An investment bank is seeking a DR backup solution. Which of the following provides the most cost-effective backup site?
A. Hot
B. Cold
C. Cluster
D. Warm
Answer: (SHOW ANSWER)
*Cold sites are the most cost-effective disaster recovery (DR) option since they require the least infrastructure investment. They provide space and power but no pre-configured systems.
*Hot sites (A) are fully operational and very expensive.
*Warm sites (D) offer some pre-configured hardware but still require setup, making them more costly than cold sites.
*Clusters (C) are active failover systems, not DR sites.
#Reference: CompTIA Network+ N10-009 Official Documentation - Disaster Recovery & Business Continuity Planning.

NEW QUESTION: 130
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: 131
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: 132
Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?
A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.
Answer: (SHOW ANSWER)
After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

NEW QUESTION: 133
Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?
A. To encrypt sensitive data in transit
B. To secure the endpoint
C. To maintain contractual agreements
D. To comply with data retentin requirements
Answer: (SHOW ANSWER)
The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
* Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
* Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
* Security: Enhances overall network security by providing secure remote access for employees.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.
* Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.
* Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

NEW QUESTION: 134
A user's VoIP phone and workstation are connected through an inline cable. The user reports that the VoIP phone intermittently reboots, but the workstation is not having any network-related issues Which of the following is the most likely cause?
A. The PoE power budget is exceeded.
B. Port security is violated.
C. The signal is degraded
D. The Ethernet cable is not working
Answer: (SHOW ANSWER)
Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data.
If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 135
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)

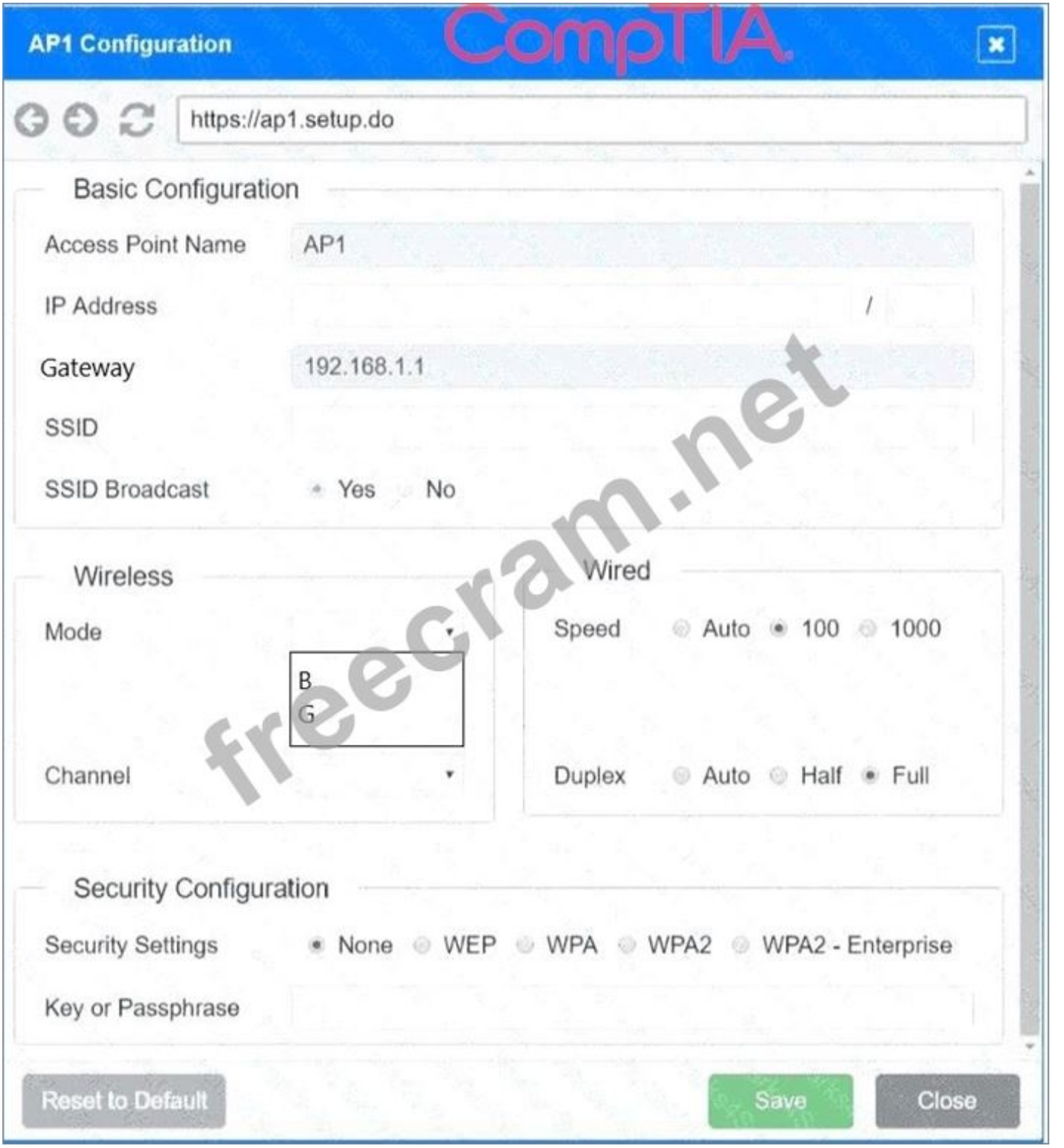
NEW QUESTION: 136
Which of the following does a full-tunnel VPN provide?
A. Lower bandwidth requirements
B. The ability to reset local computer passwords
C. Corporate Inspection of all networktraffic
D. Access to blocked sites
Answer: (SHOW ANSWER)
A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.References:CompTIA Network+ study materials.

NEW QUESTION: 137
Which of the following would be violated if an employee accidentally deleted a customer's data?
A. Integrity
B. Confidentiality
C. Vulnerability
D. Availability
Answer: (SHOW ANSWER)
Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

NEW QUESTION: 138
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: 139
SIMULATION
You have been tasked with setting up a wireless network in an office. The network will consist of 3 Access Points and a single switch. The network must meet the following parameters:
The SSIDs need to be configured as CorpNet with a key of S3cr3t!
The wireless signals should not interfere with each other

The subnet the Access Points and switch are on should only support 30 devices maximum The Access Points should be configured to only support TKIP clients at a maximum speed INSTRUCTONS Click on the wireless devices and review their information and adjust the settings of the access points to meet the given requirements.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

See explanation below.

Explanation:

On the first exhibit, the layout should be as follows

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

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

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

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

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

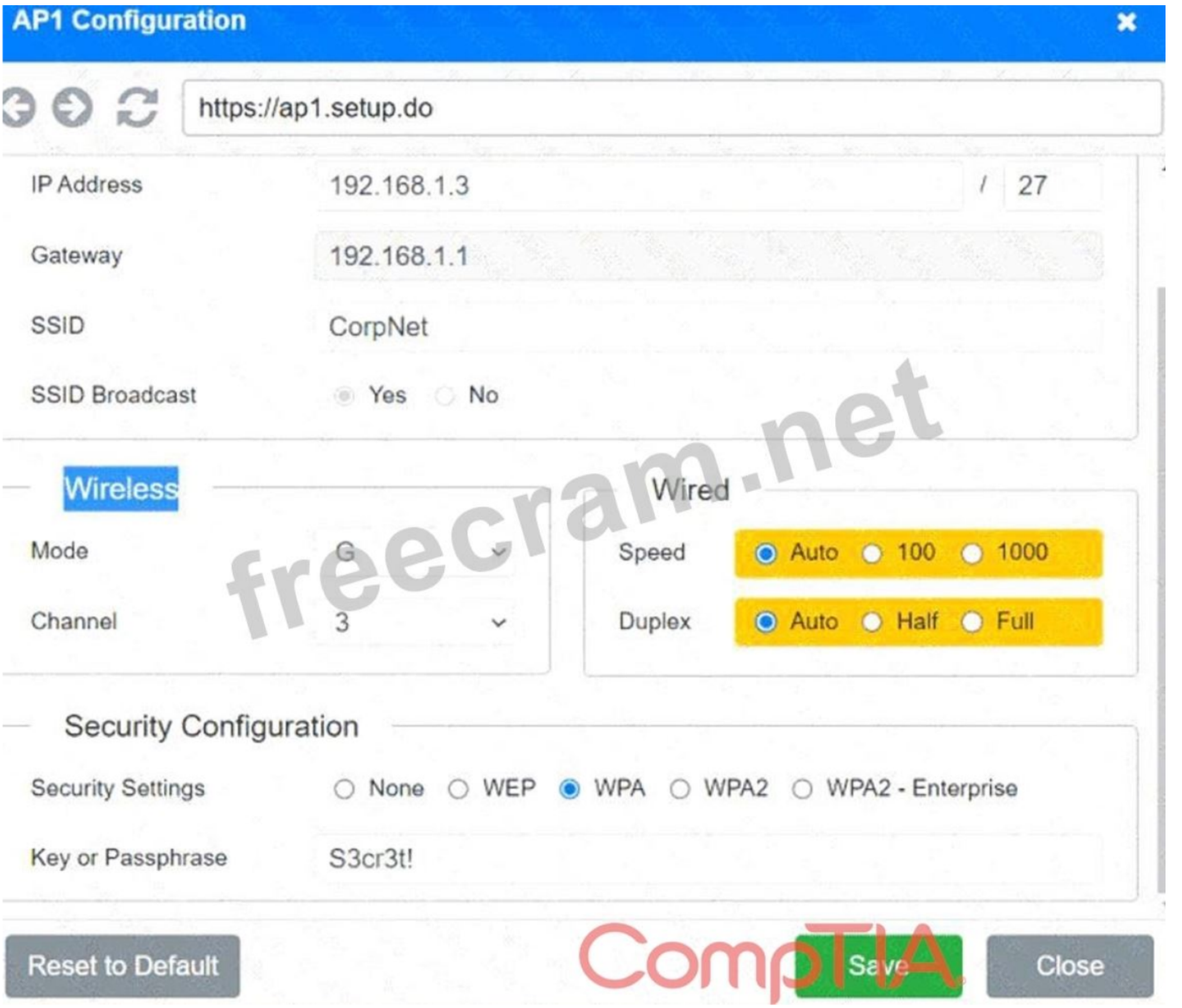
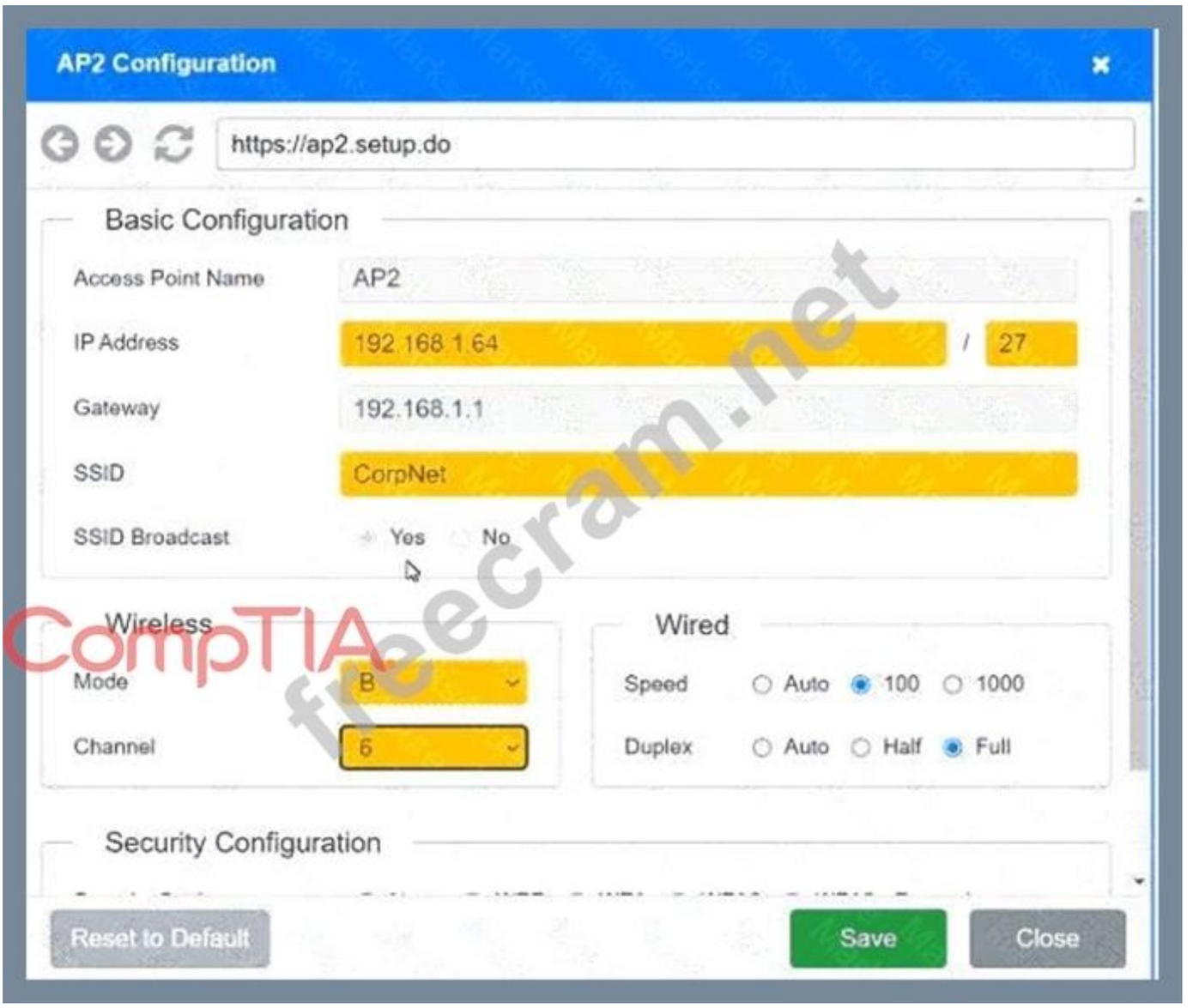


Exhibit 2 as follows

Access Point Name AP2

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



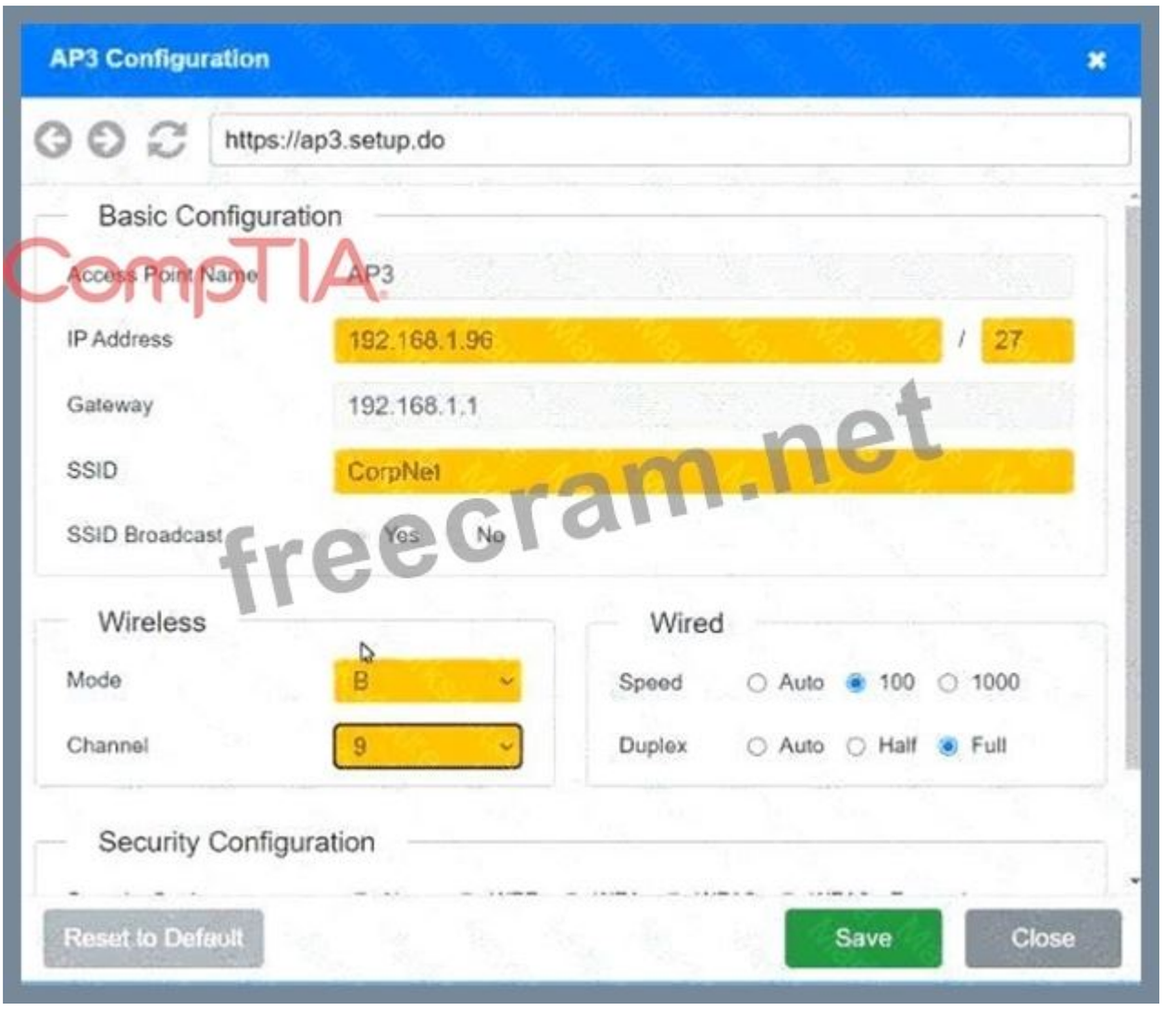
A screenshot of a computer AI-generated content may be incorrect.

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

Exhibit 3 as follows

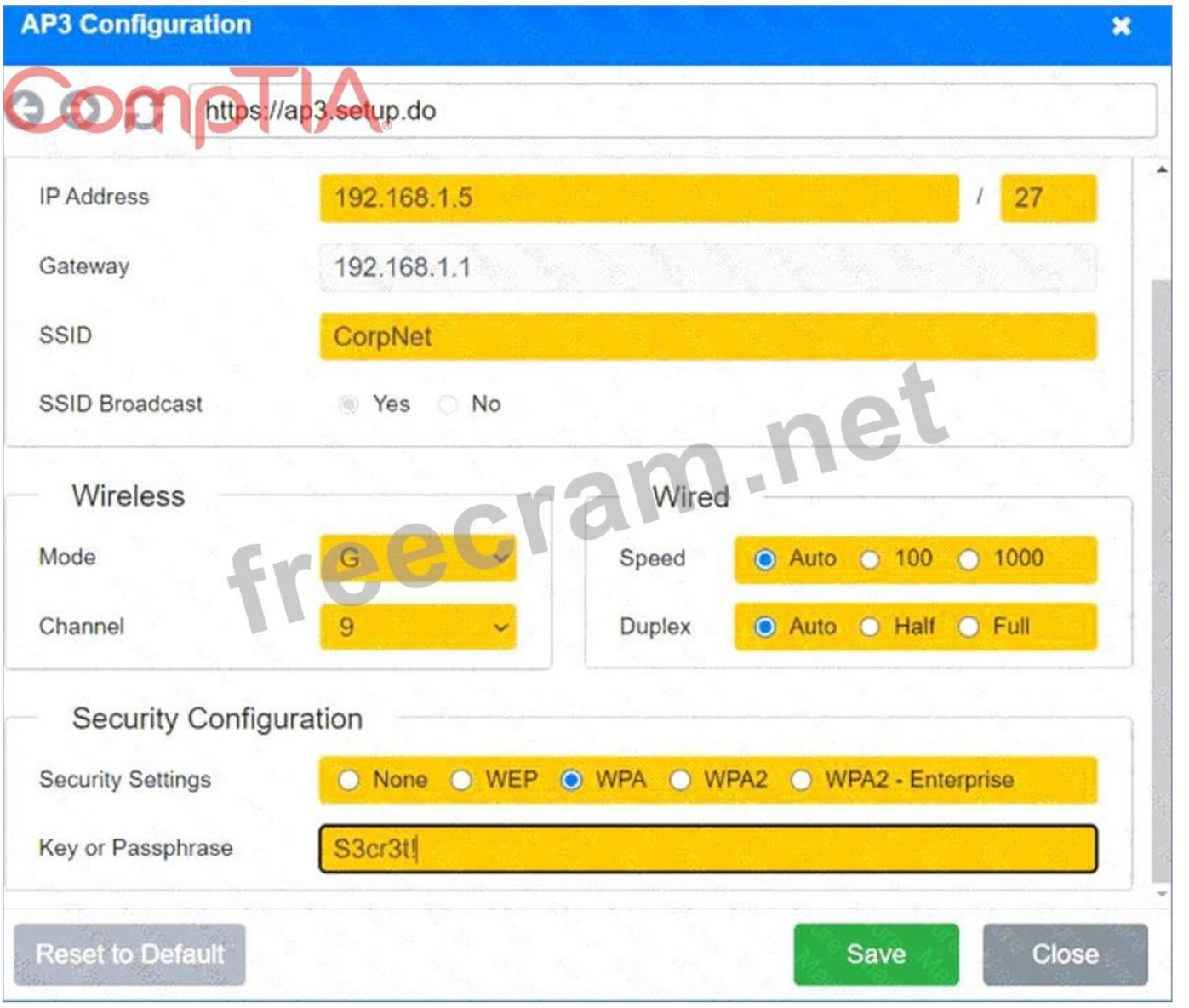
Access Point Name AP3

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



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

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



NEW QUESTION: 140

Which of the following is the most closely associated with segmenting compute resources within a single cloud account?

A. Network security group

B. IaaS

C. VPC

D. Hybrid cloud

Answer: (SHOW ANSWER)

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

NEW QUESTION: 141

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

A. Exclusions

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

NEW QUESTION: 142
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: 143
An organization wants better network visibility. The organization's requirements include:
Multivendor/OS-monitoring capabilities
Real-time collection
Data correlation

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

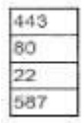
NEW QUESTION: 144
A network administrator wants to implement security zones in the corporate network to control access to only individuals inside of the corporation. Which of the following security zones is the best solution?
A. Extranet
B. Trusted
C. VPN
D. Public
Answer: (SHOW ANSWER)
Introduction to Security Zones:
Security zones are logical segments within a network designed to enforce security policies and control access.
They help in segregating and securing different parts of the network.
Types of Security Zones:
Trusted Zone: This is the most secure zone, typically used for internal corporate networks where only trusted users have access.
Extranet: This zone allows controlled access to external partners, vendors, or customers.
VPN (Virtual Private Network): While VPNs are used to create secure connections over the internet, they are not a security zone themselves.

Public Zone: This zone is the least secure and is typically used for public-facing services accessible by anyone.
Trusted Zone Implementation:
The trusted zone is configured to include internal corporate users and resources. Access controls, firewalls, and other security measures ensure that only authorized personnel can access this zone.
Internal network segments, such as the finance department, HR, and other critical functions, are usually placed in the trusted zone.
Example Configuration:
Firewall Rules: Set up rules to allow traffic only from internal IP addresses.
Access Control Lists (ACLs): Implement ACLs on routers and switches to restrict access based on IP addresses and other criteria.
Segmentation: Use VLANs and subnetting to segment and isolate the trusted zone from other zones.
Explanation of the Options:
A). Extranet: Suitable for external partners, not for internal-only access.
B). Trusted: The correct answer, as it provides controlled access to internal corporate users.
C). VPN: A method for secure remote access, not a security zone itself.
D). Public: Suitable for public access, not for internal corporate users.
Conclusion:
Implementing a trusted zone is the best solution for controlling access within a corporate network. It ensures that only trusted internal users can access sensitive resources, enhancing network security.
References:
CompTIA Network+ guide detailing security zones and their implementation in a corporate network (see page Ref 9 Basic Configuration Commands).

NEW QUESTION: 145
An IT department asks a newly hired employee to use a personal laptop until the company can provide one.
Which of the following policies is most applicable to this situation?
A. IAM
B. BYOD
C. DLP
D. AUP
Answer: (SHOW ANSWER)
BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network.
Since the new employee is using a personal laptop, this policy applies.
Breakdown of Options:
A). IAM (Identity and Access Management) - Governs user permissions, not device policies.

B). BYOD (Bring Your Own Device) - # Correct answer. Covers using personal devices for work.
C). DLP (Data Loss Prevention) - Focuses on preventing sensitive data leaks, not device usage policies.
D). AUP (Acceptable Use Policy) - Covers internet and system usage, but not personal device rules.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.6: Explain security policies and best practices.

NEW QUESTION: 146
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server. The following ports on the web server are open:



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

NEW QUESTION: 147

Which of the following troubleshooting steps would provide a change advisory board with the information needed to make a decision?

A. Identify the problem.

B. Develop a theory of probable cause.

C. Test the theory to determine cause.

D. Establish a plan of action.

Answer: (SHOW ANSWER)

A Change Advisory Board (CAB) reviews and approves network changes. Before approval, they need a detailed action plan outlining the change, potential impacts, and mitigation strategies.

* A Plan of Action includes risk assessments, rollback procedures, and deployment steps, which are critical for decision-making.

? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: Network Troubleshooting Methodologies

NEW QUESTION: 148

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing

B. Evil twin

C. MAC flooding

D. DNS poisoning

Answer: (SHOW ANSWER)

* Definition of MAC Flooding:

* MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.

* Impact of MAC Flooding:

* CAM Table Overflow:When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.

* Switch Behavior:The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.

* Comparison with Other Attacks:

* ARP Spoofing:Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.

* Evil Twin:Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.

* DNS Poisoning:Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.

* Preventive Measures:

* Port Security:Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
* Network Segmentation:Use VLANs to segment network traffic and limit the impact of such attacks.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 149
A technician is implementing a new SD-WAN device with a default configuration. The technician receives a URL via email and connects the new device to the internet to complete the installation. Which of the following is this an example of?
A. SASE device installation
B. Zero-touch provisioning
C. Infrastructure as code
D. Configuration management
Answer: B (LEAVE A REPLY)
This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN and modern network appliances.
A). SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.
C). Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits ZTP.
D). Configuration management tracks and maintains system configurations but doesn't describe the installation process.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.3 - Explain remote access methods and automation.

NEW QUESTION: 150
Due to concerns around single points of failure, a company decided to add an additional WAN to the network.
The company added a second MPLS vendor to the current MPLS WAN and deployed an additional WAN router at each site. Both MPLS providers use OSPF on the WAN network, and EIGRP is run internally. The first site to go live with the new WAN is successful, but when the second site is activated, significant network issues occur. Which of the following is the most likely cause for the WAN instability?

A. A changed CDP neighbor
B. Asymmetrical routing
C. A switching loop
D. An incorrect IP address
Answer: (SHOW ANSWER)

Asymmetrical routing occurs when packets take different paths to and from the destination, leading to instability in network communication. The use of two different MPLS providers with OSPF can lead to this type of routing issue, especially if the paths aren't carefully configured and managed. This can cause unexpected routing behaviors and instability in a dual-WAN setup. (Reference: CompTIA Network+ Study Guide, Chapter on Network Routing)

NEW QUESTION: 151
A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?
A. The parabolic signal is misaligned.
B. The omnidirectional signal is being jammed.
C. The omnidirectional signal is not strong enough to receive properly.
D. The parabolic signal uses improper routing protocols.
Answer: (SHOW ANSWER)
A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.
The document confirms:
"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

NEW QUESTION: 152
Which of the following is most closely associated with a dedicated link to a cloud environment and may not include encryption?
A. Direct Connect
B. Internet gateway
C. Captive portal
D. VPN
Answer: (SHOW ANSWER)
Direct Connect refers to a dedicated network connection between an on-premises network and a cloud service provider (such as AWS Direct Connect). This link bypasses the public internet,

providing a more reliable and higher-bandwidth connection. It may not inherently include encryption because it relies on the security measures of the dedicated physical connection itself. In contrast, other options like VPN typically involve encryption as they traverse the public internet.
Reference:
CompTIA Network+ full course material indicates that Direct Connect type services offer dedicated, private connections which might not include encryption due to the dedicated and secure nature of the link itself.

NEW QUESTION: 153
A small business is deploying new phones, and some of the phones have full HD videoconferencing features.
The Chief Information Officer (CIO) is concerned that the network might not be able to handle the traffic if it reaches a certain threshold. Which of the following can the network engineer configure to help ease these concerns?
A. A VLAN with 100Mbps speed limits
B. An IP helper to direct VoIP traffic
C. A smaller subnet mask
D. Full duplex on all user ports
Answer: (SHOW ANSWER)
Full duplex mode allows devices to send and receive data simultaneously, improving network performance and reducing congestion, which is critical for VoIP and video conferencing.
Breakdown of Options:
A). A VLAN with 100Mbps speed limits - VLANs segment traffic but limiting speeds to 100Mbps would worsen video performance.
B). An IP helper to direct VoIP traffic - IP helper is used for DHCP relay, not for VoIP optimization.
C). A smaller subnet mask - A smaller subnet reduces IP address availability but does not improve network performance.
D). Full duplex on all user ports - Correct answer. Full duplex eliminates collisions, allowing better VoIP and video performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.2: Compare and contrast various networking devices.
IEEE 802.3: Ethernet Full Duplex Operation

NEW QUESTION: 154
Which of the following connectors allows a singular QSFP transceiver to have several physical connections?
A. RJ45
B. ST
C. LC
D. MPO

Answer: (SHOW ANSWER)

The MPO (Multi-fiber Push On) connector is designed to handle multiple fiber strands in a single connector, and it is commonly used with high-density transceivers like QSFP (Quad Small Form-factor Pluggable).

QSFP can support up to four channels (hence "quad"), and MPO connectors can interface multiple fibers (e.g.,

8, 12, 24), making them ideal for 40Gbps or 100Gbps deployments.

RJ45 (A) is used for Ethernet over copper.

ST (B) and LC (C) are single-fiber connectors - they don't support the multi-fiber needs of QSFP setups.

Therefore, MPO is the correct connector type for this use case.

Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.1: "Compare and contrast different types of connectors and transceivers."