CompTIA.N10-009.v2026-07-13.q237

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	237
Version:	v2026-07-13
# of views:	103
# of Questions views:	2370
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-07-13.q237.html	

NEW QUESTION: 1
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: 2
After a recent security awareness phishing campaign, the cybersecurity team discovers that additional security measures need to be set up when users access potentially malicious websites. Which of the following security measures will best address this concern?
A. Implement DNS filtering.
B. Update ACLs to only allow HTTPS.
C. Configure new IPS hardware.
D. Deploy 802.1X security features.
Answer: (SHOW ANSWER)
DNS filtering blocks access to known malicious websites by comparing domain requests against a list of allowed or blocked URLs. It is an effective defense against phishing and other web-based attacks.
From Andrew Ramdayal's guide:

"URL filtering restricts access to specific websites or web content by comparing URLs against a predefined list of allowed or blocked sites...commonly used to prevent users from accessing malicious sites."

NEW QUESTION: 3
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: 4
A network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?
A. Access
B. Core
C. Leaf
D. Spine
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
In a spine-leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer-often specifically to a "border leaf" that handles external connectivity.
Why not B. Core or D. Spine? In spine-leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.
Why not A. Access? "Access" is a term from the traditional three-tier model (access-distribution-core). In modern spine-leaf language, the analogous layer for endpoint attachment is the leaf.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Data center and campus architectures (spine-leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

NEW QUESTION: 5
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: 6
Which of the following is an XML-based security concept that works by passing sensitive information about users, such as login information and attributes, to providers?
A. IAM
B. MFA
C. RADIUS
D. SAML
Answer: (SHOW ANSWER)
The correct answer is SAML (Security Assertion Markup Language). SAML is an XML-based standard used for single sign-on (SSO) and identity federation. It allows identity providers (IdPs) to share authentication and authorization data with service providers (SPs), passing secure tokens containing user attributes and credentials.
A). IAM (Identity and Access Management) is the broader framework, not specifically XML-based.
B). MFA enforces multiple factors for authentication but does not involve XML assertions.
C). RADIUS is an AAA protocol, but it uses UDP, not XML assertions.
SAML is widely used in federated identity systems, enabling secure authentication across different domains and applications without requiring multiple credentials.
References (CompTIA Network+ N10-009):
Domain: Network Security - Authentication methods, SAML, SSO.

NEW QUESTION: 7
A company's Chief Information Security Officer requires that servers and firewalls have accurate timestamps when creating log files so that security analysts can correlate events during incident investigations. Which of the following should be implemented?
A. Syslog server
B. SMTP
C. SNMP
D. NTP
Answer: (SHOW ANSWER)
NTP (Network Time Protocol) synchronizes clocks across network devices, ensuring accurate timestamps in logs. This is critical for correlating events across different systems during investigations.
A). Syslog collects logs but relies on accurate timestamps already present.
B). SMTP is an email protocol, unrelated to time synchronization.

C). SNMP is for monitoring and management, not time.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Time synchronization (NTP), log correlation, security operations.

NEW QUESTION: 8
A network technician is designing a LAN for a new facility. The company is expecting more than 300 devices to connect to the network. Which of the following masks will provide the most efficient subnet?
A. 255.255.0.0
B. 255.255.192.0
C. 255.255.254.0
D. 255.255.255.254
Answer: C (LEAVE A REPLY)
The requirement is to support over 300 hosts. The subnet mask 255.255.254.0 (or /23) provides 512 addresses, 510 of which are usable - ideal for around 300 devices.
* 255.255.0.0 (/16) provides too many addresses.
* 255.255.192.0 (/18) gives 16384 addresses - overkill.
* 255.255.255.254 is invalid for host assignments (only 2 addresses, 0 usable).
From Andrew Ramdayal's guide:
"To support 300 hosts, a /23 subnet (255.255.254.0) offers 510 usable addresses - the most efficient choice without excessive overhead."

NEW QUESTION: 9
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: 10
Which of the following best describes the amount of time between a disruptive event and the point that affected resources need to be back to fully functional status?

A. RTO
B. MTBF
C. RPO
D. MTTR
Answer: (SHOW ANSWER)

The correct metric is RTO (Recovery Time Objective). RTO defines the maximum acceptable time to restore services after a disruption, ensuring business continuity. For example, if the RTO is 4 hours, systems must be back online within that timeframe after an outage.
B). MTBF (Mean Time Between Failures) measures reliability by calculating the average time between hardware failures.
C). RPO (Recovery Point Objective) defines how much data loss (in terms of time, such as last backup point) is acceptable.
D). MTTR (Mean Time to Repair) measures the average time taken to fix a failure but is not a predefined business requirement like RTO.
Organizations define RTOs during disaster recovery planning to align IT recovery capabilities with business needs.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Business continuity metrics (RTO, RPO, MTBF, MTTR).

NEW QUESTION: 11
A network administrator receives a ticket from a user. The user reports that they cannot access any websites and that they have already checked everything on their computer. Which of the following is the first action the administrator should take?
A. Divide and conquer.
B. Establish a theory of probable cause.
C. Question the user.
D. Document the findings.
Answer: (SHOW ANSWER)
The correct answer is Question the user because the first step in the CompTIA Network+ (N10-009) troubleshooting methodology is to identify the problem. Identifying the problem involves gathering information, asking clarifying questions, determining if anything has changed, and establishing the scope of the issue.
Even though the user states they have "checked everything," the administrator should not assume that all relevant troubleshooting steps were properly performed. The technician must ask specific questions such as:
Are other users affected? Is the issue limited to certain websites? Are there any error messages? When did the issue start? Were there recent updates or configuration changes?
Only after gathering sufficient information should the administrator move to the next steps, such as establishing a theory of probable cause (Option B) or using divide-and-conquer methods (Option A).
Documentation (Option D) occurs after resolving and verifying the issue.
Therefore, questioning the user to clearly define and scope the problem is the correct first action according to the structured troubleshooting process.

NEW QUESTION: 12
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).

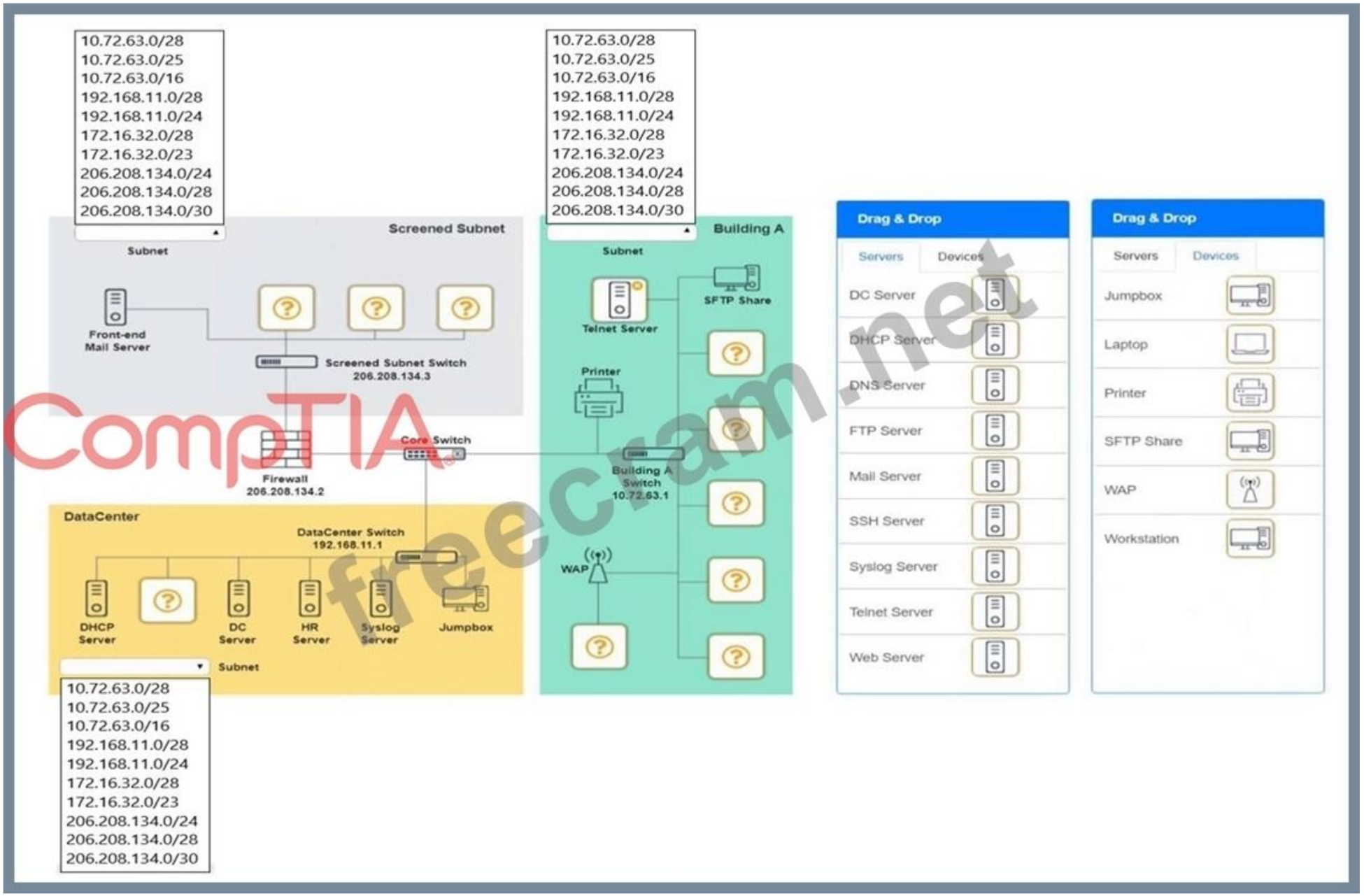
NEW QUESTION: 13
A company is opening a new site that needs to be divided into subnets that accommodate 75 hosts each.
Which of the following is the most efficient subnet?
A. 192.168.13.0/25
B. 192.168.13.0/26
C. 192.168.13.0/27
D. 192.168.13.0/28
Answer: (SHOW ANSWER)
To support 75 hosts per subnet, you must choose a subnet size that provides at least 75 usable IP addresses. In IPv4, usable hosts per subnet equals 2^(host bits) # 2 (subtracting network and broadcast). A /25 leaves 7 host bits (32-25 = 7), giving 2^7 # 2 = 128 # 2 = 126 usable hosts, which meets the requirement and is the smallest (most efficient) option listed that does so. A /26 leaves 6 host bits, giving 62 usable hosts, which is insufficient. A /27 gives 30 usable, and a /28 gives 14 usable, both far below 75. Network+ subnetting objectives emphasize selecting the smallest subnet that satisfies the host requirement to conserve address space while meeting growth and design constraints. Therefore, 192.168.13.0/25 is the most efficient option that accommodates at least 75 hosts per subnet.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 15
Which of the following tools uses ICMP to help determine whether a network host is reachable?
A. tcpdump
B. netstat
C. nslookup
D. ping
Answer: (SHOW ANSWER)
Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.
A). tcpdump captures packets but does not test reachability.
B). netstat displays open ports and network sessions.
C). nslookup queries DNS servers for name resolution.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - ICMP operation, troubleshooting tools.

NEW QUESTION: 16
You are tasked with verifying the following requirements are met in order to ensure network security.
Requirements:
Datacenter
Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.
Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Answer:

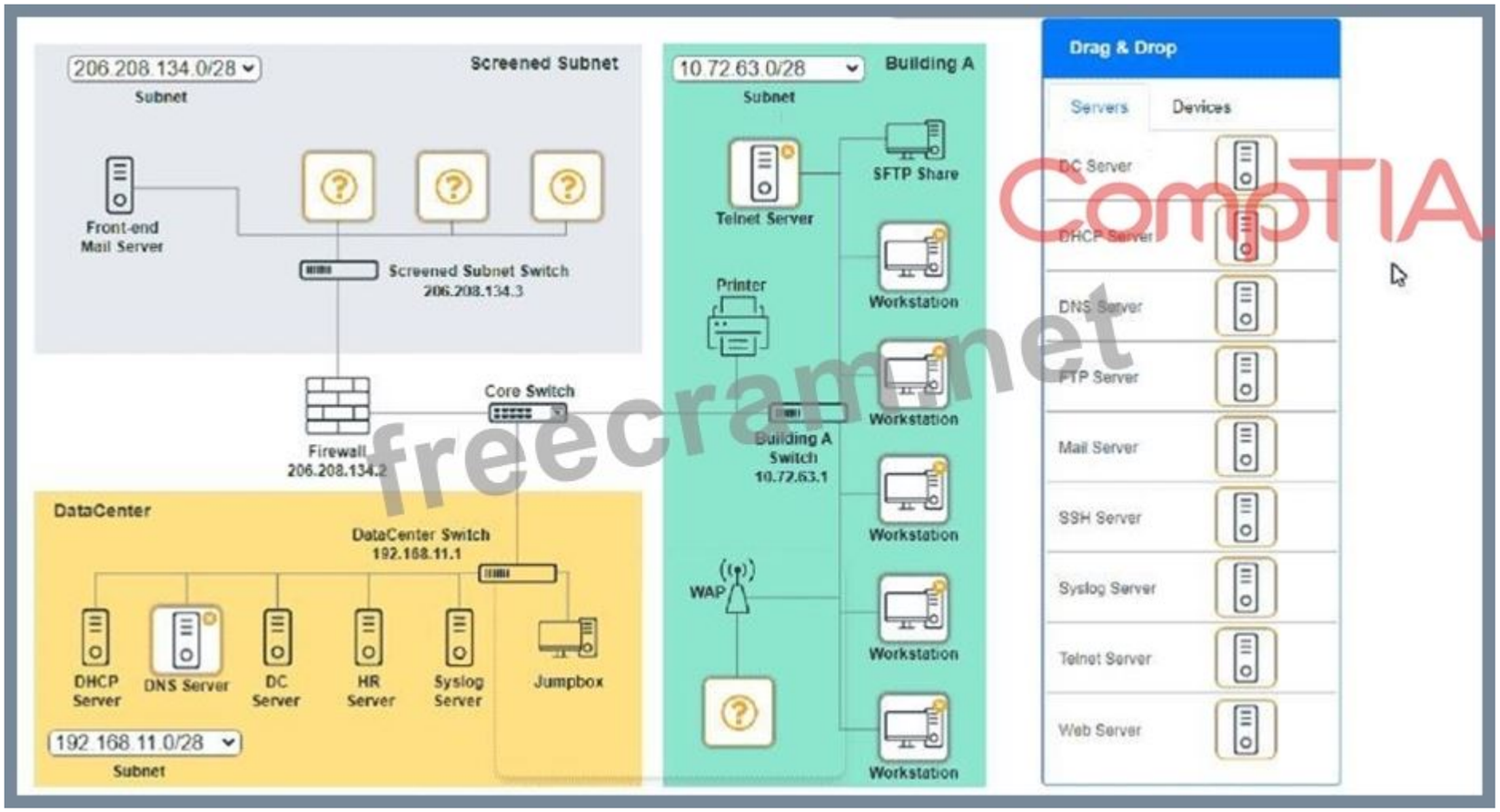
See explanation below.

Explanation:

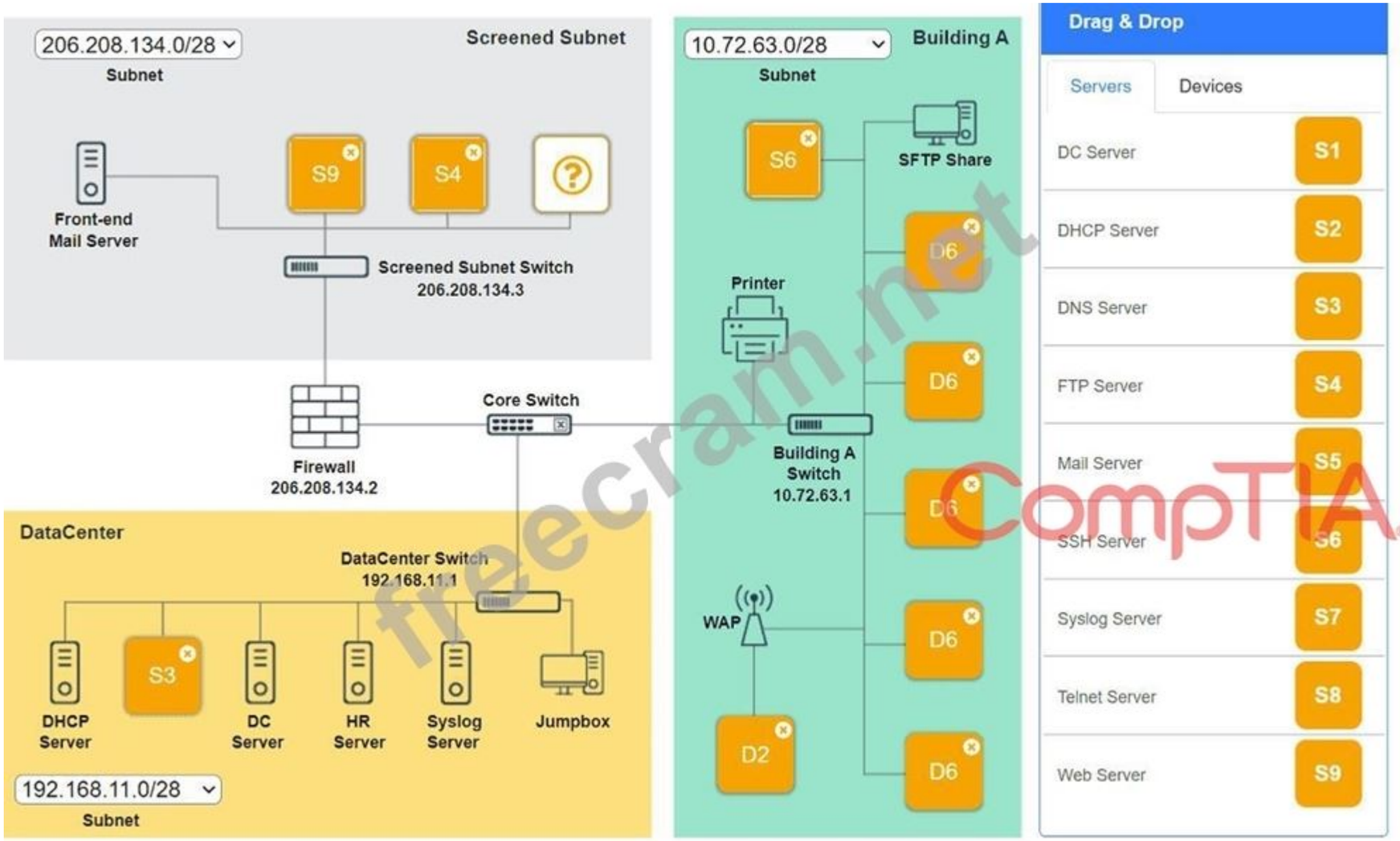
Screened Subnet devices - Web server, FTP server

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

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



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



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

NEW QUESTION: 17

Users usually use RDP to connect to a terminal server with hostname TS19 that points to 10.0.100.19.

However, users recently have been unable to connect to TS19. The technician pings 10.0.100.19 and gets an unreachable error. Which of the following is the most likely cause?

A. The users are on the wrong subnet.

B. The DHCP server renewed the lease.

C. The IP address was not reserved.

D. The hostname was changed.

Answer: (SHOW ANSWER)

If a ping to 10.0.100.19 is unreachable, the most likely issue is that users are on the wrong subnet and cannot communicate with the server.
Breakdown of Options:
A: The users are on the wrong subnet. # Correct answer. If users are on a different subnet without proper routing, they won't reach the server.
B: The DHCP server renewed the lease. - Would change the client's IP, but the server's static IP should remain unchanged.
C: The IP address was not reserved. - DHCP reservations matter for dynamic IPs, but RDP servers typically have static IPs.
D: The hostname was changed. - Would affect DNS resolution, but pinging the IP directly would still work.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.4: Explain subnetting concepts.

NEW QUESTION: 18
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: 19
A network engineer needs to change, update, and control APs remotely, with real-time visibility over HTTPS.
Which of the following will best allow these actions?
A. Web interface

B. Command line
C. SNMP console
D. API gateway
Answer: (SHOW ANSWER)
API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.
From Andrew Ramdayal's guide:
"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

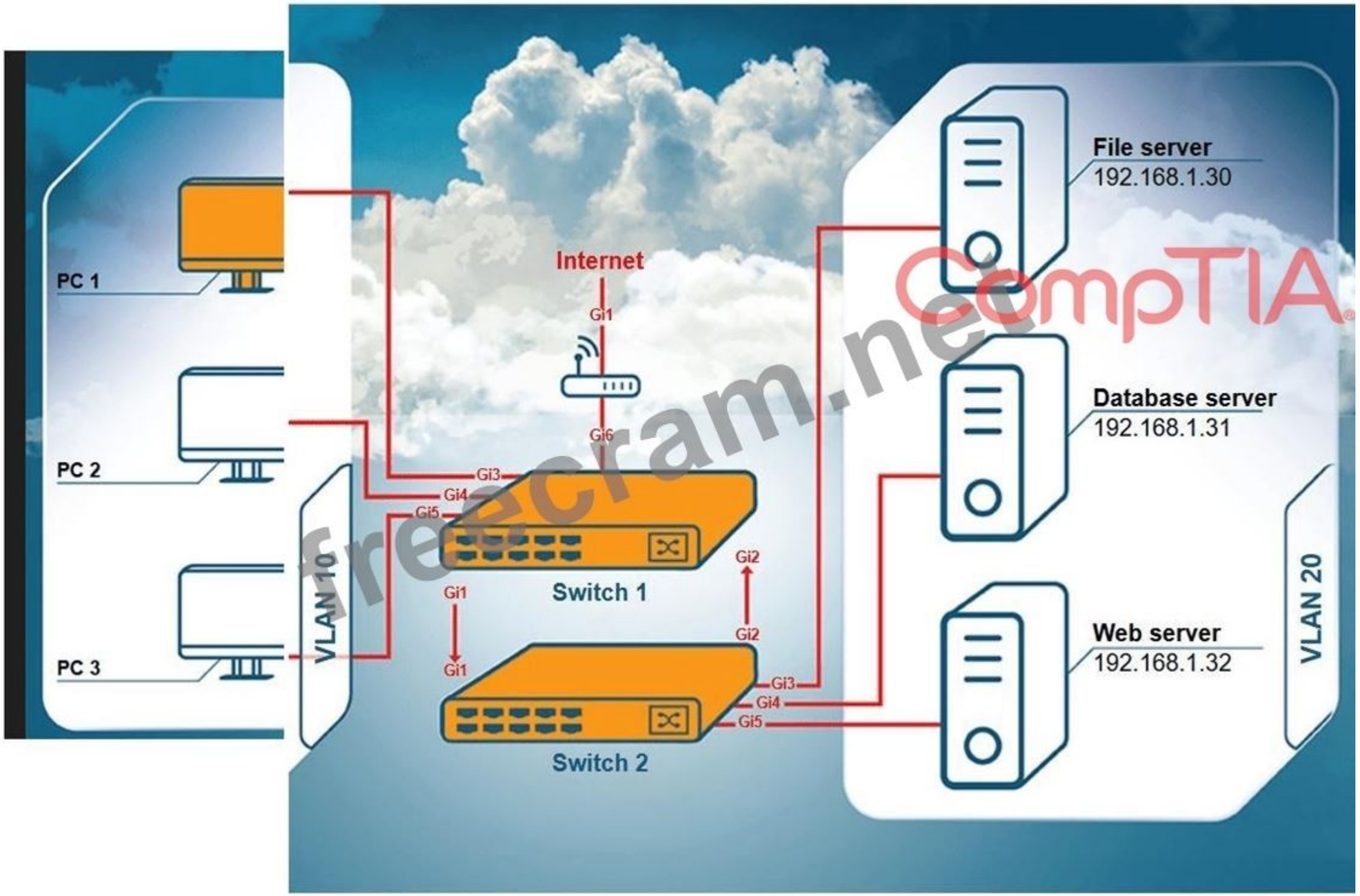
NEW QUESTION: 20
A group of users cannot connect to network resources. The technician runs ipconfig from one user's device and is able to ping the gateway shown from the command. Which of the following is most likely preventing the users from accessing network resources?

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

NEW QUESTION: 21
A technician is plugging an Ethernet cable into a switch to bring a new device online, but the device is not showing an active network connection. Previously, another technician turned off unused switchports as part of device hardening. Which of the following describes the port status?
A. Error disabled
B. Idle
C. Suspended
D. Administratively down
Answer: (SHOW ANSWER)
The correct answer is D. Administratively down . The question states that another technician had already turned off unused switchports as part of hardening. When a port is intentionally disabled by configuration, its status is described as administratively down . In other words, the switchport is not broken and has not failed on its own; it has simply been shut down by an administrator.

This is a common security practice. Unused ports are often disabled so unauthorized devices cannot be plugged in and gain access to the network. If a legitimate device later needs that port, the administrator must re-enable it before the link can come up.
The other answer choices do not line up as well with the scenario. Error disabled usually points to a protective shutdown caused by a violation or fault, such as port security or BPDU guard. Idle is not the standard description for a manually shut switchport in this context. Suspended can appear with certain switch features, but it is not the normal label for a port deliberately turned off as part of hardening.
The phrase "turned off unused switchports" is the key detail. That clearly indicates a manual administrative shutdown, so administratively down is the best answer.

NEW QUESTION: 22
A network technician receives a ticket from an employee who is working on PC 1 but is unable to connect to the database server. The technician pings the database server from PC 1, but the request times out. After reviewing the utilization of Switch 1 and Switch 2, the technician finds high CPU utilization and sees that the MAC table is continuously changing.
INSTRUCTIONS
Configure Switch 1 and Switch 2 to remediate the employee ' s issue. Then, validate connectivity between PC
1 and the database server.
Switch 1 and Switch 2 are already in configuration mode. Type help to view a list of available commands.




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


Switch 1
Switch1(config)#
freecram.net
CompTIA

Switch 1

```
switch1(config)# interface gi2
  % Invalid input detected.
switch1(config)# ?
Available commands:

show vlan
show spanning-tree
spanning-tree vlan

switch1(config)# spanning-tree vlan 10
switch1(config)# spanning-tree vlan 20
switch1(config)#
```

Answer:

See the solution in Explanation below.

Explanation:

Switch 1

spanning-tree vlan 10 root primary

spanning-tree vlan 20 root secondary

Switch 2

spanning-tree vlan 20 root primary

spanning-tree vlan 10 root secondary

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

The available commands shown in the screenshots are limited to spanning-tree vlan , so this is not an interface shutdown question. The fix is to use STP per VLAN and make one switch the preferred root for one VLAN and the other switch the preferred root for the other VLAN. That prevents both uplinks from forwarding in an uncontrolled loop while still giving redundancy.

A clean design is:

* Switch 1 root primary for VLAN 10
* Switch 2 root primary for VLAN 20
* Make each opposite switch root secondary for failover

That stabilizes Layer 2 forwarding, stops MAC address flapping, reduces CPU load, and restores normal connectivity. After applying the STP root settings, the user should be able to ping 192.168.1.31 from PC 1 successfully. If your simulator asks for validation, run the ping again from PC 1 to the database server.

NEW QUESTION: 23
Which of the following is the best VPN to use for reducing data bandwidth requirements of the corporate network?
A. Split-tunnel
B. Site-to-site
C. Full-tunnel client
D. GRE tunnel
Answer: (SHOW ANSWER)
A split-tunnel VPN allows a device to route some traffic through the VPN (typically corporate traffic) while sending other traffic (like general internet browsing) directly over the local internet connection. This reduces the load on the corporate network because not all traffic is routed through the VPN tunnel.
Site-to-site VPNs are for permanent links between locations.
Full-tunnel VPNs route all traffic through the VPN, increasing the bandwidth usage on the corporate network.
GRE (Generic Routing Encapsulation) is a tunneling protocol that doesn't encrypt and doesn't reduce bandwidth usage by itself.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.3 - Given a scenario, configure and deploy common VPN technologies.

NEW QUESTION: 24
Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?
A. General Data Protection Regulation
B. Least privilege network access
C. Acceptable use policy
D. End user license agreement
Answer: (SHOW ANSWER)
Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 25
A network technician is terminating a cable to a fiber patch panel in the MDF. Which of the following connector types is most likely in use?
A. F-type
B. RJ11
C. BNC
D. SC
Answer: (SHOW ANSWER)
In a fiber patch panel, the SC (Subscriber Connector or Standard Connector) is commonly used because of its push-pull design and reliability in enterprise environments.
Breakdown of Options:

A). F-type - Used for coaxial cables (e.g., cable TV), not fiber.
B). RJ11 - Used for telephone lines, not fiber.
C). BNC - Used for coaxial connections, not fiber.
D). SC - # Correct answer. A standard fiber optic connector used in patch panels.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.1: Compare and contrast physical network connectors.

NEW QUESTION: 26
A customer purchases a new UTM device and wants the development team to integrate some of the device's data-reporting capabilities into the company's custom internal support software. Which of the following features should the development team use to obtain the device's data?
A. API
B. SNMPv2c
C. SIEM
D. MIB
Answer: (SHOW ANSWER)
An API (Application Programming Interface) is the best choice when a development team needs to integrate a device's reporting data directly into custom software. In Network+ (N10-009) objectives, network operations commonly include device management, monitoring, and automation, and APIs are a key method for programmatic access to operational data (often via REST/HTTPS with structured formats like JSON). This enables the internal support application to pull dashboards, health metrics, events, configuration details, and reporting outputs in a controlled, developer-friendly way.
SNMPv2c is primarily used for network monitoring and polling counters/alerts, but it is less secure (community strings) and is not as flexible for modern application integration as an API. A MIB is not a data- access "feature" by itself; it's the schema/definitions SNMP uses to describe managed objects. A SIEM is a separate security analytics platform that collects and correlates logs/events-useful for security operations, but not the direct interface a custom support tool would typically call to retrieve device reporting data.

NEW QUESTION: 27
Which of the following routing protocols needs to have an autonomous system set in order to establish communication with neighbor devices?
A. OSPF
B. EIGRP
C. FHRP
D. RIP
Answer: (SHOW ANSWER)
EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco proprietary advanced distance-vector routing protocol. While it operates within an Autonomous System (AS), it requires the AS number to be configured for routers to recognize each other as EIGRP neighbors.
OSPF (Open Shortest Path First) uses areas and routers must be in the same area to form adjacencies, but it doesn ' t require AS numbers in the same way.
FHRP (First Hop Redundancy Protocol) is not a routing protocol but a group of protocols (e.g., HSRP, VRRP) to ensure high availability at the default gateway level.
RIP (Routing Information Protocol) does not use autonomous system numbers.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.1 - Compare and contrast various routing technologies.
==========

NEW QUESTION: 28
Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP
B. AH
C. GRE
D. UDP
E. TCP
Answer: (SHOW ANSWER)
Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data.
ESP encrypts the payload and optional ESP trailer, providing data confidentiality.
ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.
ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).
Comparison with Other Protocols:
AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.
GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.
UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.
Use Cases:
ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.
References:
CompTIA Network+ study materials on IPsec and encryption.

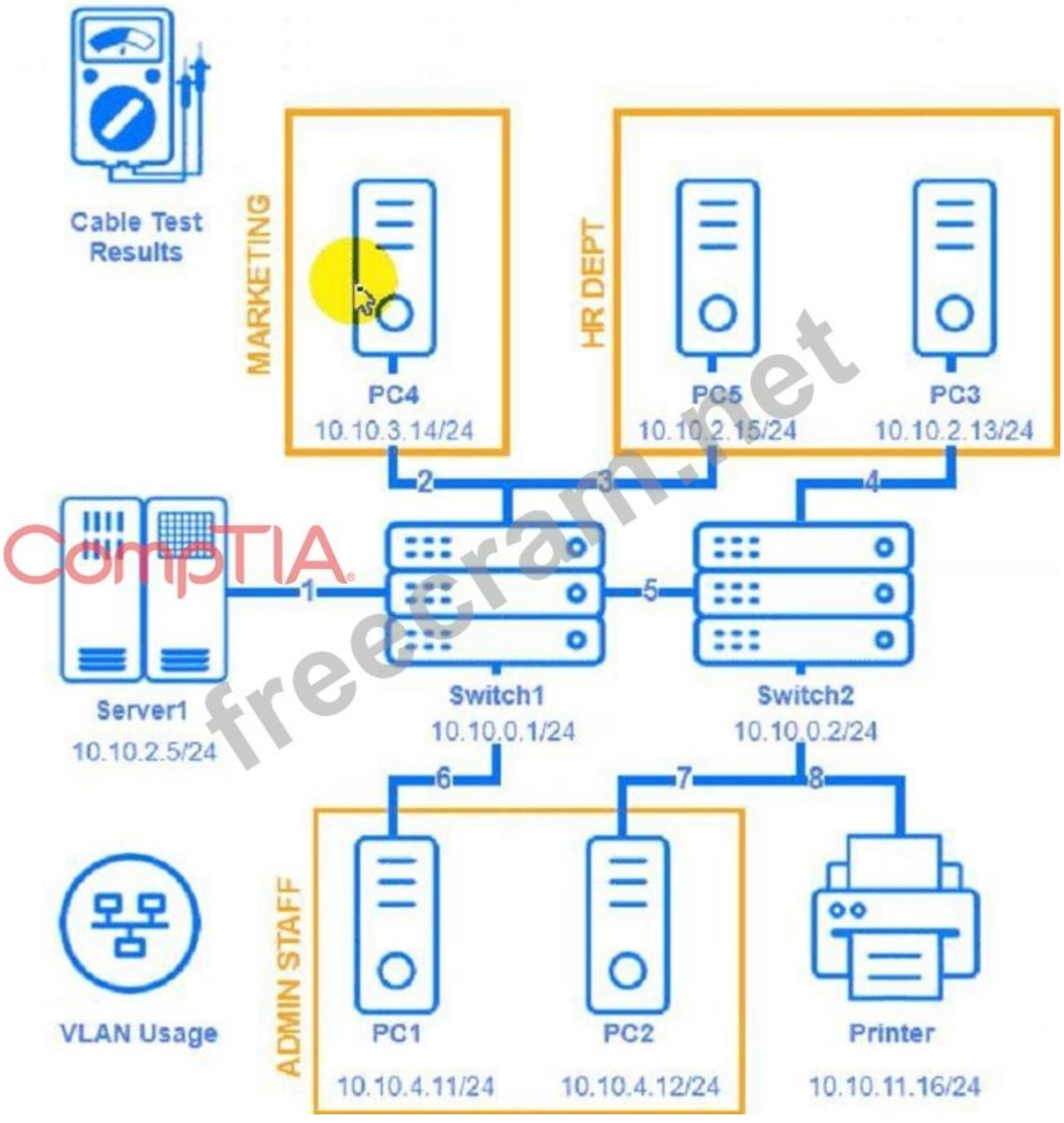
NEW QUESTION: 29
A network administrator is unable to ping a remote server from a newly connected workstation that has been added to the network. Ping to 127.0.0.1 on the workstation is failing. Which of the following should the administrator perform to diagnose the problem?
A. Verify the NIC interface status.
B. Verify the network is not congested.
C. Verify the router is not dropping packets.
D. Verify that DNS is resolving correctly.
Answer: (SHOW ANSWER)
The failure of a ping to 127.0.0.1 (the loopback address) indicates a problem with the workstation's TCP/IP stack or network interface card (NIC). Since 127.0.0.1 is a local address, the issue is not related to the network, router, or DNS. The first step in diagnosing this issue is to verify the NIC interface status to ensure the network adapter is functioning and properly configured.
Why not Verify the network is not congested? Network congestion affects external connectivity, not the loopback address.
Why not Verify the router is not dropping packets? Router issues are irrelevant since the loopback ping fails locally.
Why not Verify that DNS is resolving correctly? DNS resolution is not involved in pinging 127.0.0.1, which uses a direct IP address.
Reference:CompTIA Network+ N10-009 Objective 5.2: Explain the troubleshooting methodology. The CompTIA Network+ Study Guide (e.g., Chapter 13: Network Troubleshooting) emphasizes that a failed loopback ping indicates a local TCP/IP stack or NIC issue, and checking the NIC status is the first diagnostic step.

NEW QUESTION: 30

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

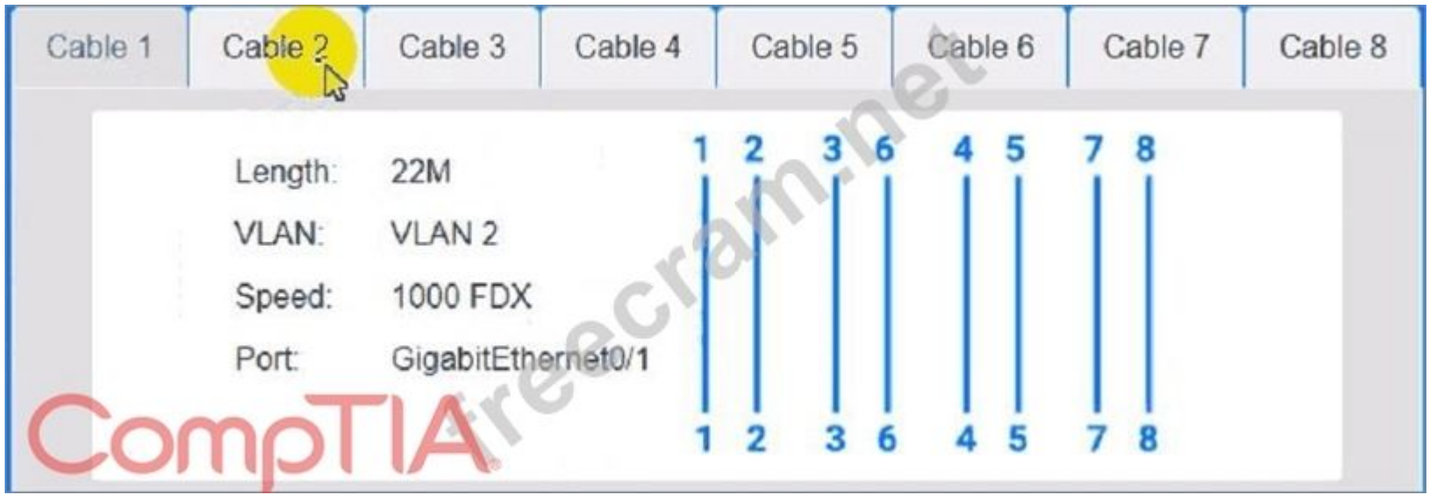
A. SSH
B. DHCP
C. NTP
D. SNMP
Answer: (SHOW ANSWER)
The correct answer is SNMP (Simple Network Management Protocol) because it is specifically designed to collect and transmit network management and status information between managed devices and management systems. According to CompTIA Network+ (N10-009) objectives, SNMP is used for monitoring and managing network devices such as routers, switches, servers, and printers.
SNMP operates using a manager-agent model. The SNMP manager (such as a network monitoring server) communicates with SNMP agents installed on network devices. Agents send traps and inform messages, which are unsolicited status alerts indicating events such as device failures, high CPU usage, or link outages.
The manager can also poll agents to retrieve performance metrics and configuration details stored in the Management Information Base (MIB).
SSH (Option A) is used for secure remote administration. DHCP (Option B) dynamically assigns IP addresses. NTP (Option C) synchronizes time between devices. None of these protocols are designed for network status monitoring and alert messaging.
Therefore, SNMP is the correct protocol for sending networking status messages between devices and management systems.
Bottom of Form

NEW QUESTION: 31
A network technician needs to resolve some issues with a customer ' s SOHO network.
The customer reports that some of the devices are not connecting to the network, while others appear to work as intended.
INSTRUCTIONS
Troubleshoot all the network components and review the cable test results by Clicking on each device and cable.
Diagnose the appropriate component(s) by identifying any components with a problem and recommend a solution to correct each problem.



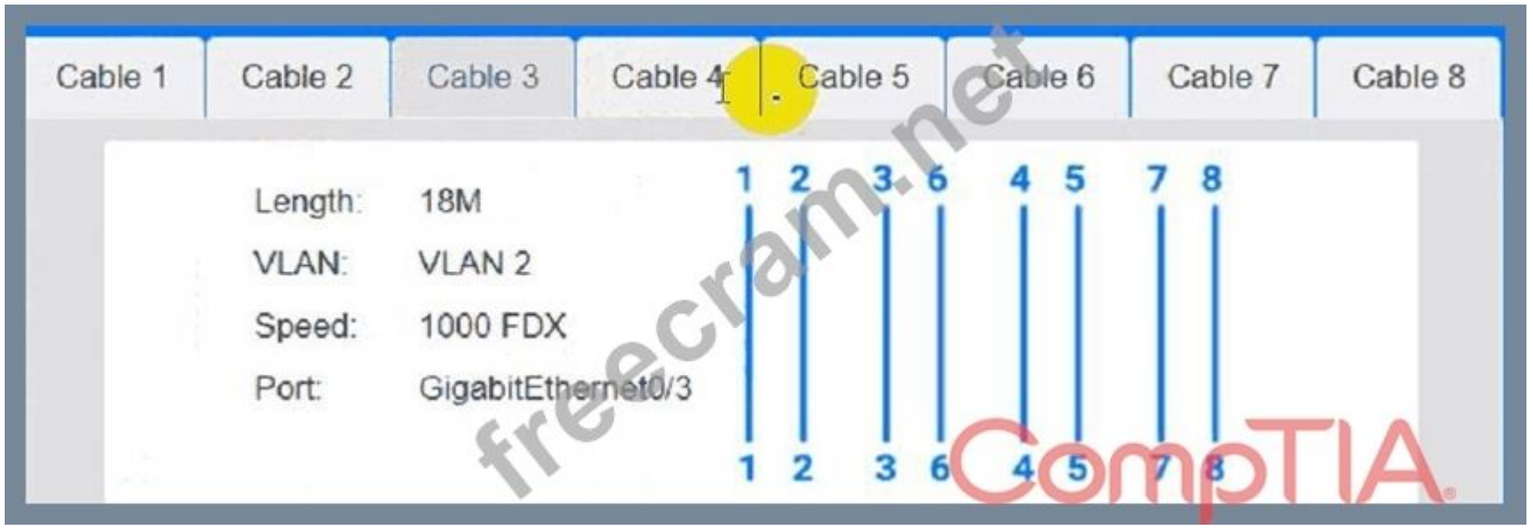
Cable Test Results:

Cable 1:



Cable 2:

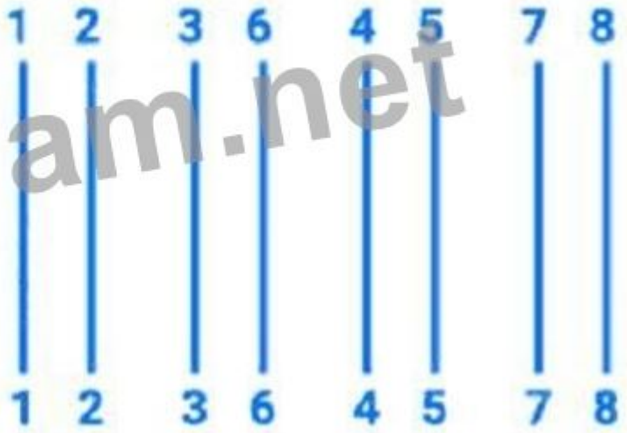
Cable 3:



Cable 4:

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

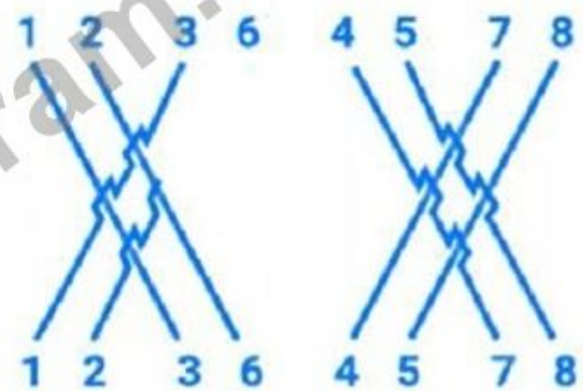
Length: 20M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/2

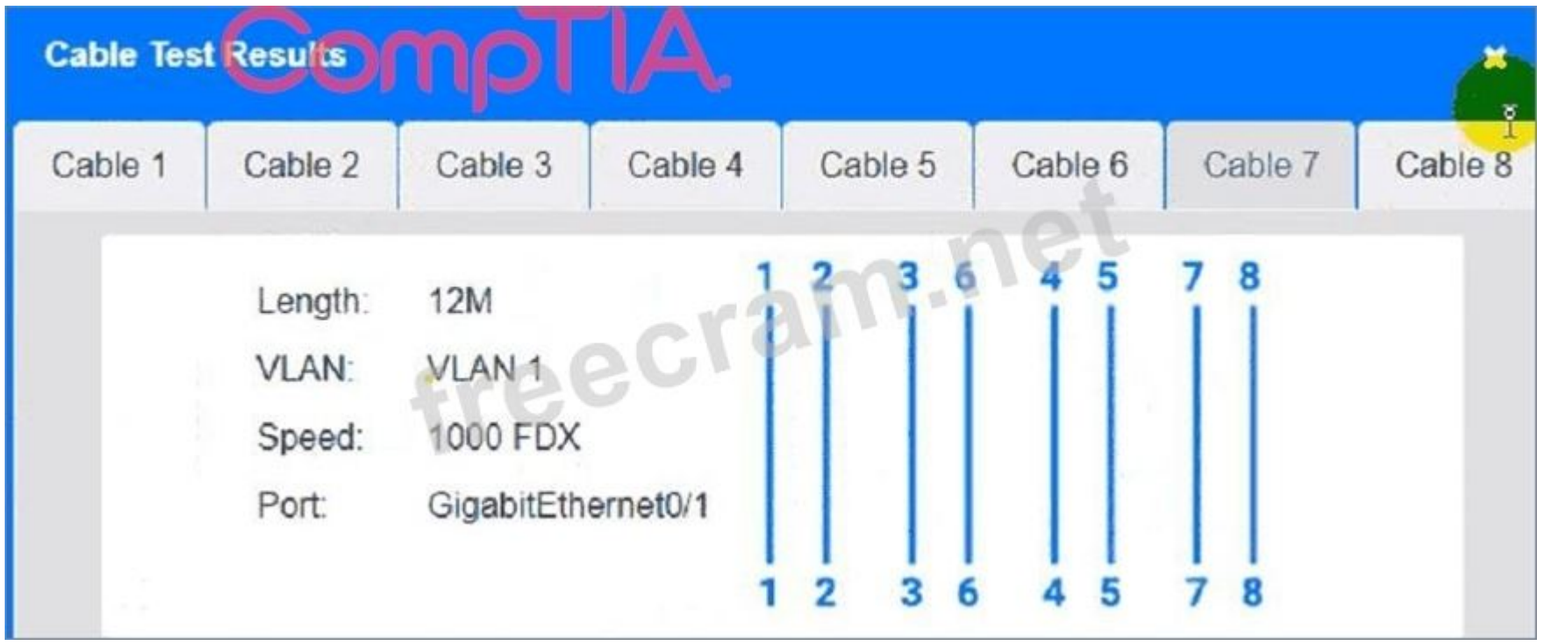


Cable Test Results

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

Length: 16M
VLAN: VLAN 1
Speed: 1000 FDX
Port: GigabitEthernet0/5





Printer

HP Network Configuration Page

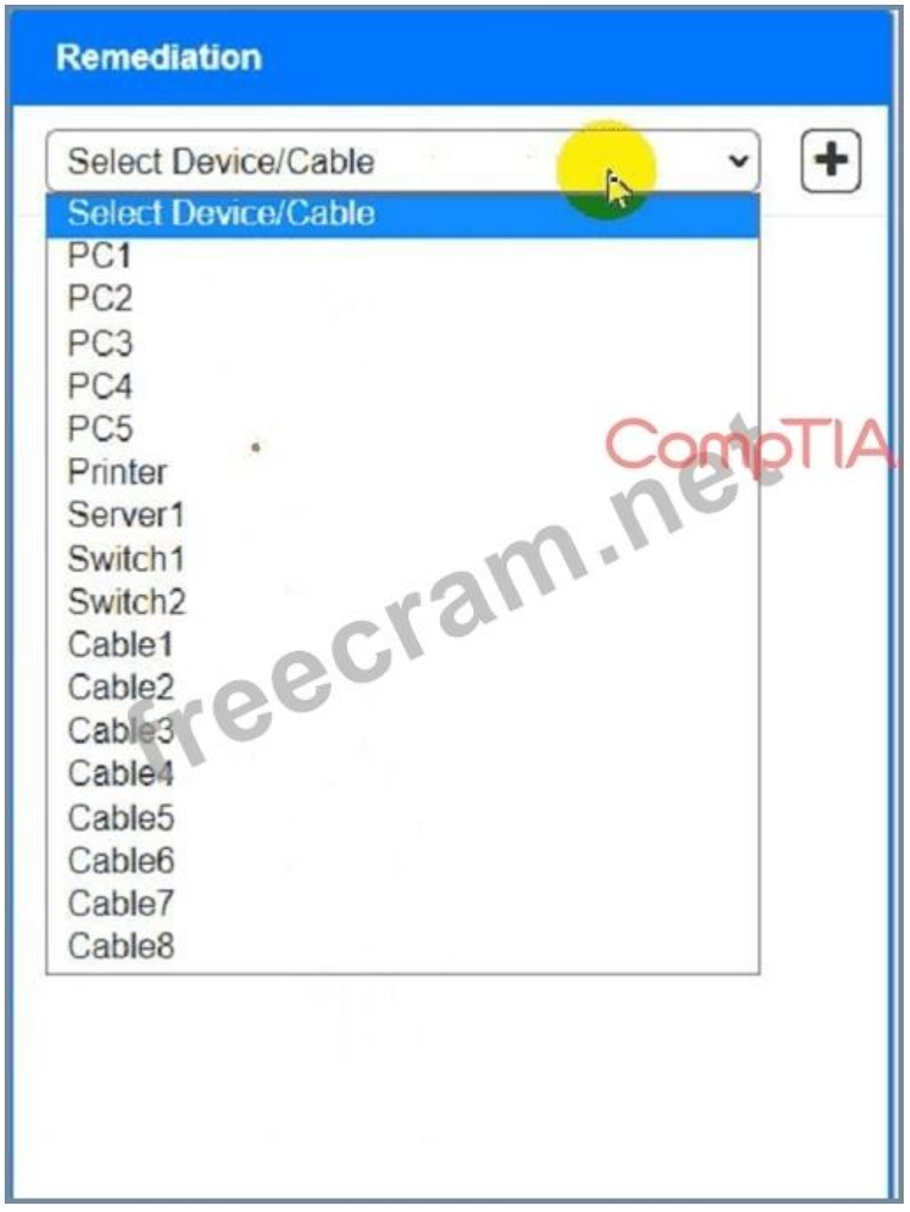
Model: HP Officejet Pro 8610

General Information

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

802.3 Wired

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



Answer:

See the Explanation for detailed information on this simulation.

Explanation:

(Note: Ips will be change on each simulation task, so we have given example answer for the understanding) To troubleshoot all the network components and review the cable test results, you can use the following steps:

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

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

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

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

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

The component with a problem is PC1.

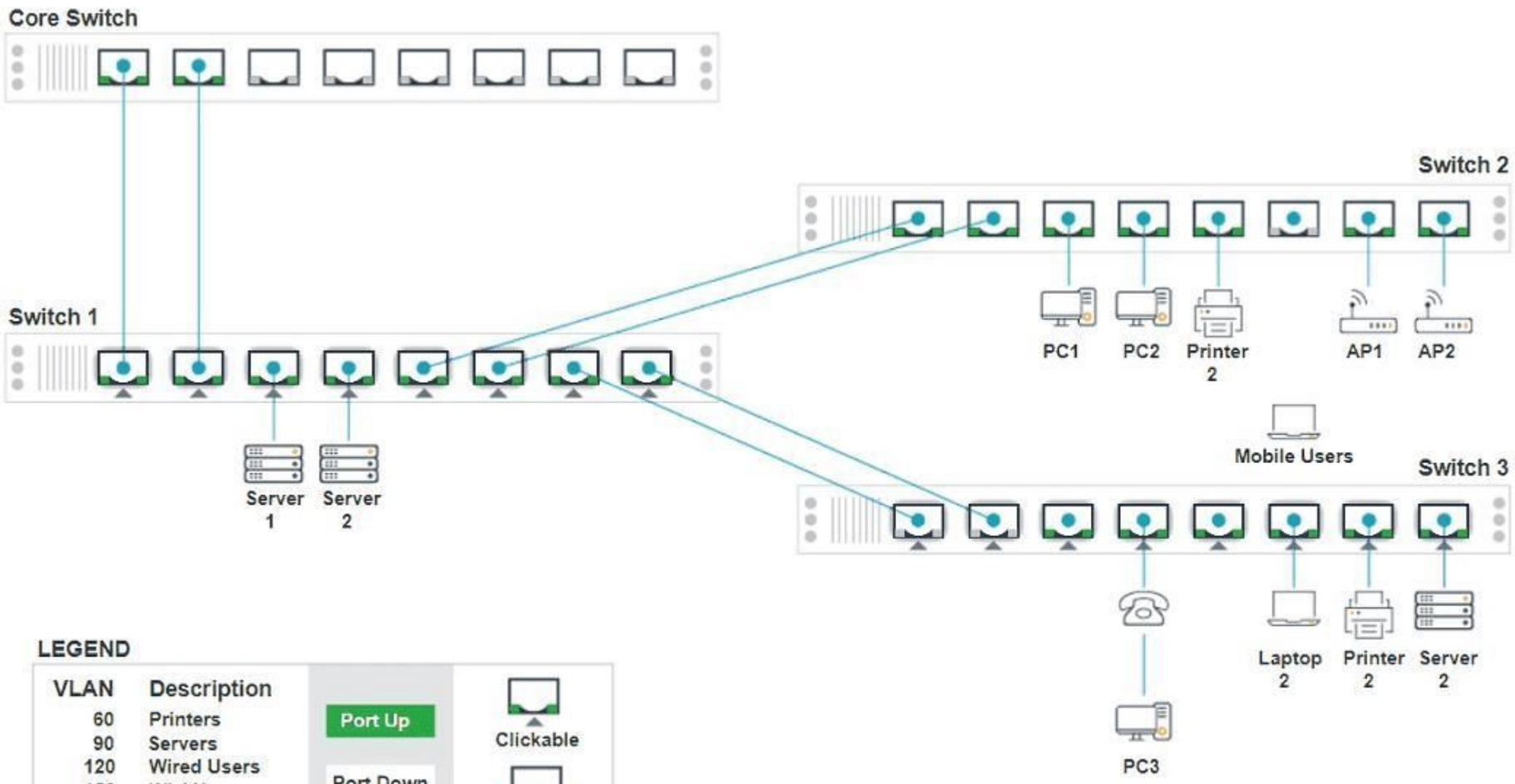
The problem is Incorrect IP address.

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

NEW QUESTION: 32
Which of the following most likely requires the use of subinterfaces?
A. A router with only one available LAN port
B. A firewall performing deep packet inspection
C. A hub utilizing jumbo frames
D. A switch using Spanning Tree Protocol
Answer: (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: 33
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.



LEGEND

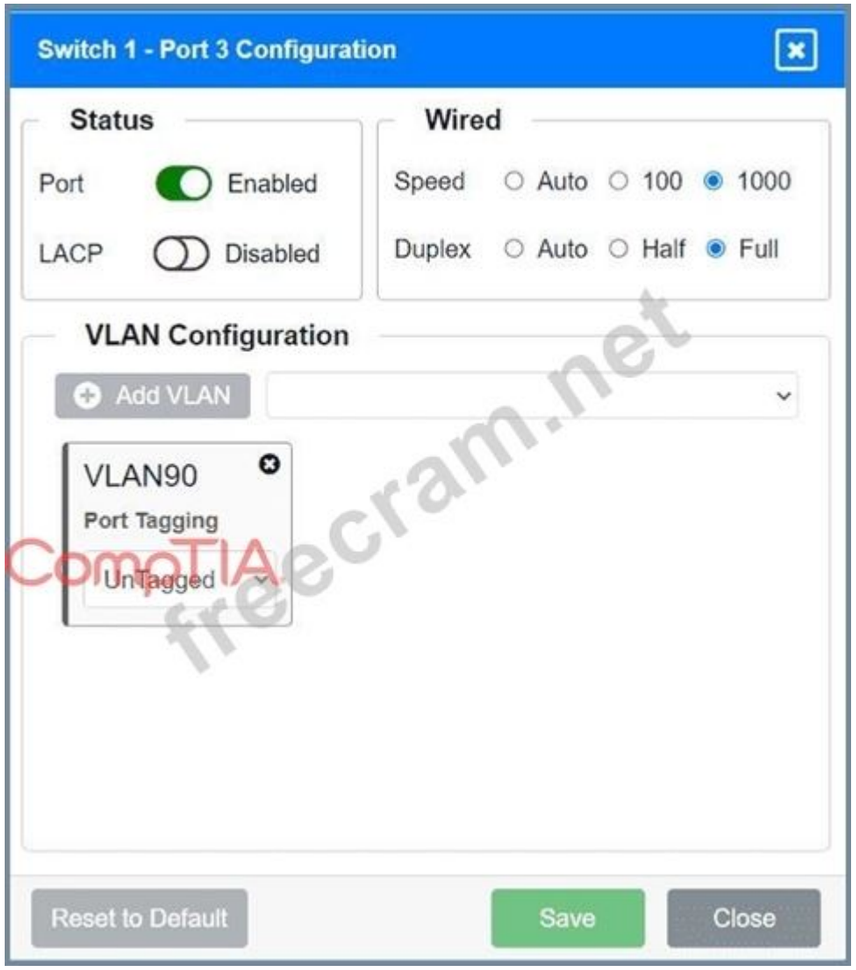
VLAN	Description
60	Printers
90	Servers
120	Wired Users
150	WLAN
220	Voice

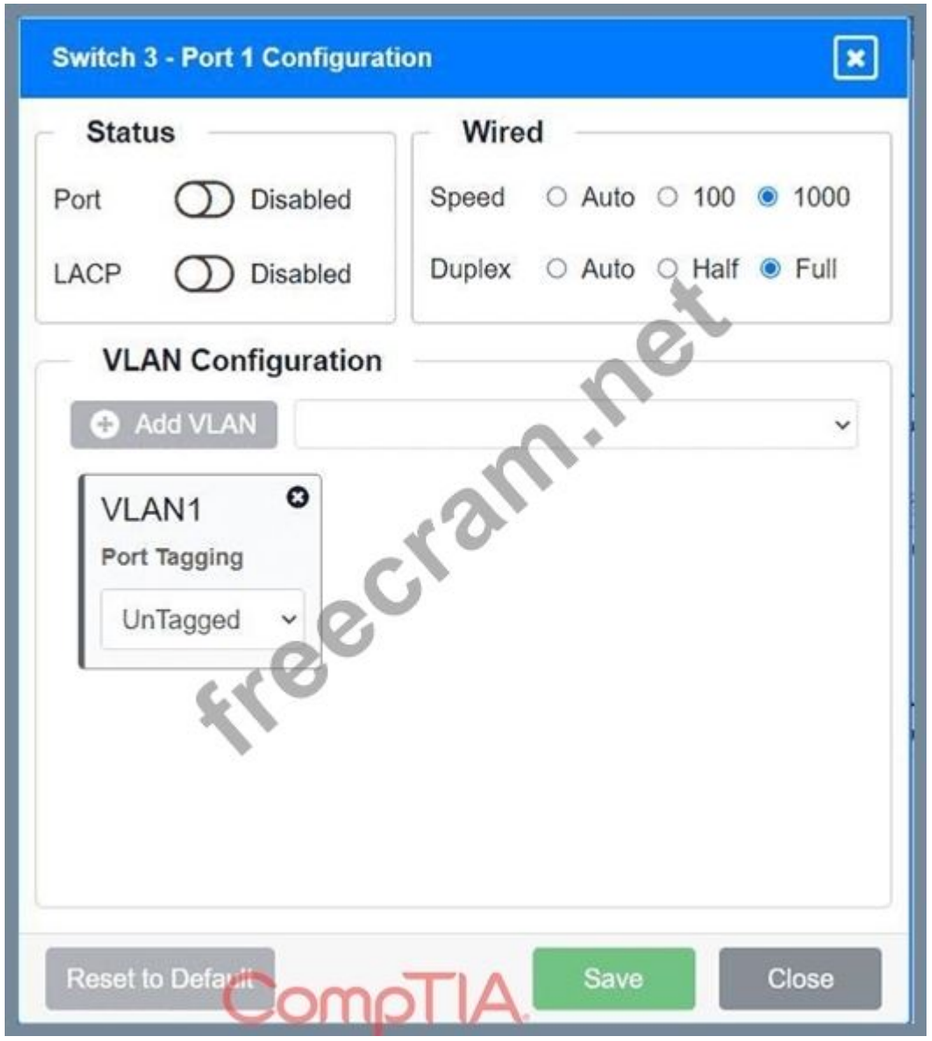
Port Up

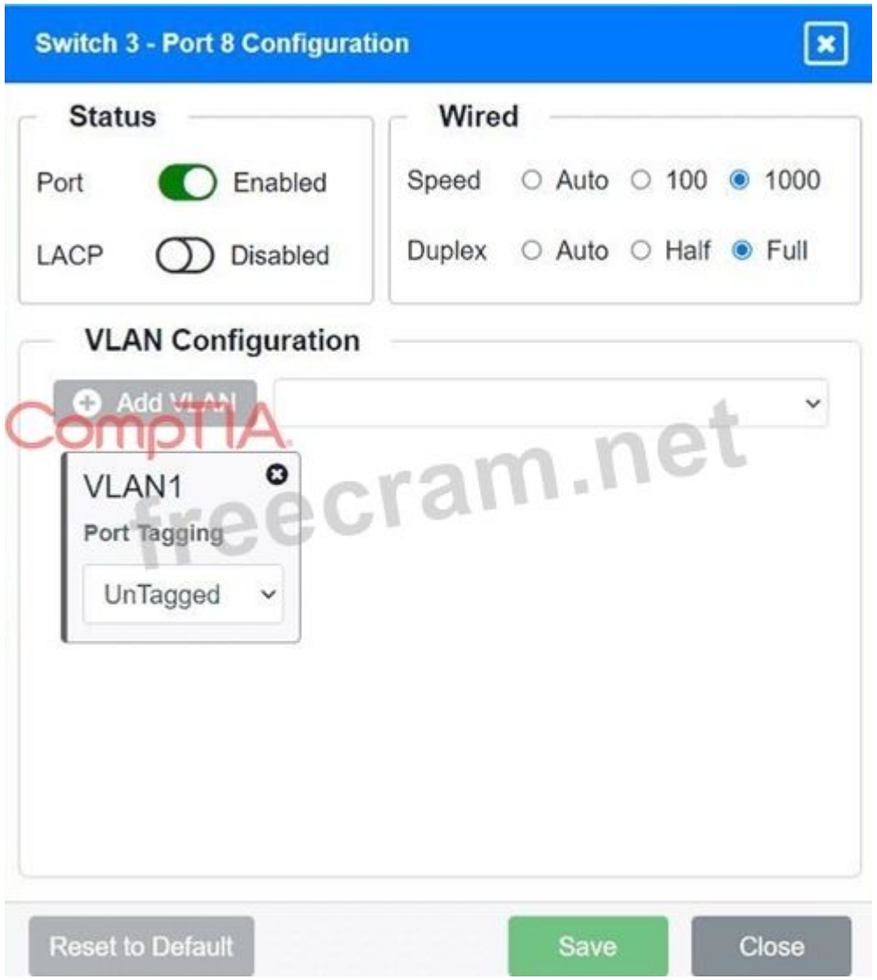
Port Down

Clickable

Not Clickable







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: 34
Which of the following troubleshooting steps provides a change advisory board with the information needed to make a decision?
A. Identify the problem
B. Develop a theory of probable cause
C. Test the theory to determine cause
D. Establish a plan of action
Answer: (SHOW ANSWER)
When dealing with troubleshooting and change management, the plan of action outlines the steps, risks, and mitigation strategies. A change advisory board (CAB) uses this documented plan to decide whether to approve the change.
A). Identify the problem is the first step in troubleshooting, not decision-making for CAB.
B). Develop a theory is diagnostic work, not planning.
C). Test the theory confirms causes but doesn't provide actionable planning information.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Change management, troubleshooting methodology, CAB processes.

NEW QUESTION: 35
A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)
A. Least privilege network access
B. Dynamic inventeries
C. Central policy management
D. Zero-touch provisioning
E. Configuration drift prevention
F. Subnet range limits
Answer: A,C (LEAVE A REPLY)
To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.

* Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches. By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.
* Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.
* Cisco Networking Academy: Provides training on implementing security policies and access controls.
* Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

NEW QUESTION: 36
Which of the following ports is used to transfer data between mail exchange servers?
A. 21
B. 25
C. 53
D. 69
Answer: (SHOW ANSWER)
The correct answer is 25, which is the default port used by SMTP (Simple Mail Transfer Protocol) for communication between mail servers. According to CompTIA Network+ (N10-009) objectives under common port numbers and protocols, SMTP operates over TCP port 25 for server-to-server email transmission.
When an email is sent from one domain to another, the sending mail server queries DNS for the recipient domain's MX (Mail Exchange) record and then establishes an SMTP session over TCP port 25 to deliver the message. This port is specifically designated for mail relay between mail transfer agents (MTAs).
Port 21 is used for FTP (File Transfer Protocol), 53 is used for DNS (Domain Name System), and 69 is used for TFTP (Trivial File Transfer Protocol). None of these are responsible for transferring email between mail servers.
While SMTP can also use ports 587 (submission) and 465 (SMTPS) for client-to-server communication, port
25 remains the standard for mail server-to-mail server communication.
Therefore, TCP port 25 is the correct answer.

NEW QUESTION: 37
A network administrator installed a new VLAN to the network after a company added an additional floor to the office. Users are unable to obtain an IP address on the new VLAN, but ports on existing VLANs are working properly. Which of the following configurations should the administrator update?
A. Scope size
B. Address reservations
C. Lease time
D. IP helper
Answer: (SHOW ANSWER)
When a new VLAN is created, it typically exists on a different subnet. If DHCP servers are on a different VLAN, the network needs an IP helper address to forward DHCP requests correctly. Without it, clients in the new VLAN won't receive an IP address.
Breakdown of Options:
A: Scope size - Increasing the DHCP scope would not resolve the issue if requests aren't reaching the server.
B: Address reservations - Reservations only assign specific addresses to devices; they do not fix DHCP communication issues.
C: Lease time - Changing the lease time does not impact DHCP functionality across VLANs.
D: IP helper - Correct answer. This forwards DHCP requests across VLANs to the DHCP server.

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

NEW QUESTION: 38
A network administrator is setting up a firewall to protect the organization's network from external threats.
Which of the following should the administrator consider first when configuring the firewall?
A. Required ports, protocols, and services
B. Inclusion of a deny all rule
C. VPN access
D. Outbound access originating from customer-facing servers
Answer: (SHOW ANSWER)
When configuring a firewall, the first step is identifying which ports, protocols, and services are required for normal business operations. This ensures only legitimate traffic is allowed.
After establishing the required rules, a default deny rule is added for security.
B). Deny all rule is important, but it should come after defining required rules.
C). VPN access is a service to configure, but only after determining baseline needs.
D). Outbound traffic policies are part of refinement, not the first consideration.
References (CompTIA Network+ N10-009):
Domain: Network Security - Firewall configuration, rule order, least privilege.

NEW QUESTION: 39
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: 40

A new network is being created to support 126 users. Which of the following CIDR ranges provides the most efficient use of space?

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

NEW QUESTION: 41
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: 42
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: 43
Which of the following should an installer orient a port-side exhaust to when installing equipment?
A. The patch panel
B. The front of the IDF
C. The warm aisle
D. The administrator console
Answer: C (LEAVE A REPLY)
In data centers, hot aisle/cold aisle configurations are used to manage airflow and cooling efficiency. Port-side exhausts should be oriented towards the warm aisle to expel hot air and maintain optimal cooling. The document clarifies:
"Equipment with port-side exhausts should be oriented towards the warm aisle to ensure that hot air is properly directed away from the cold air intake areas. This alignment supports effective cooling in data center environments."

NEW QUESTION: 44
A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration:
Which of the following is causing the user's issue?
A. Incorrect DNS
B. Unreachable gateway

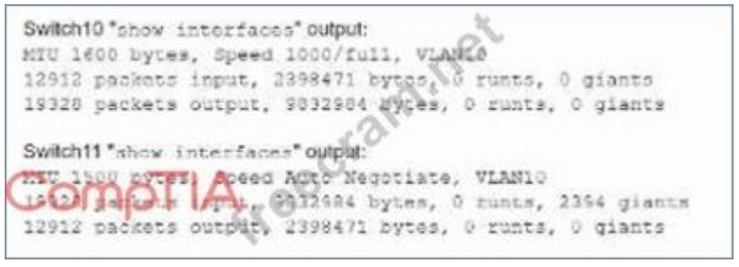
C. Failed root bridge
D. Poor upstream routing
Answer: (SHOW ANSWER)
The customer can access local resources (a database server), which means local networking is working.
However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets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

NEW QUESTION: 45
A network rack has four servers and four switches with dual power supplies. Only one intelligent PDU is installed in the rack. Which of the following is the reason to add a second PDU?
A. Power redundancy
B. Failed PSU monitoring
C. Surge protection
D. Electricity conservation
Answer: (SHOW ANSWER)
The correct answer is Power redundancy because the devices in the rack are equipped with dual power supplies, which are specifically designed to support redundant power sources.
According to CompTIA Network+ (N10-009) objectives under high availability and physical infrastructure concepts, redundancy is a key strategy to eliminate single points of failure.
If only one PDU (Power Distribution Unit) is installed, both power supplies from each device may ultimately rely on the same power source. This creates a single point of failure-if the PDU fails or loses upstream power, all connected equipment will shut down despite having dual power supplies.
By installing a second PDU connected to a separate power circuit (and ideally a separate UPS or power feed), each power supply in the servers and switches can connect to different PDUs. If one PDU fails, the other continues delivering power, ensuring uninterrupted operation.
Option B (Failed PSU monitoring) is not the primary reason for adding another PDU. Option C (Surge protection) can be provided by a single PDU. Option D (Electricity conservation) is unrelated to redundancy design.
Therefore, adding a second PDU provides true power redundancy.

NEW QUESTION: 46
Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?
A. Verify full system functionality.
B. Document the findings and outcomes.
C. Establish a plan of action.
D. Identify the problem.
Answer: (SHOW ANSWER)
The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.
Troubleshooting Steps:
Identify the problem.
Establish a theory of probable cause.

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

NEW QUESTION: 47
A network technician is troubleshooting network latency and has determined the issue to be occuring two network switches(Switch10 and Switch11). Symptoms reported included poor video performance and slow file copying. Given the following informtion:



Which of the following should the technician most likely do to resolve the issue?
A. Modify Switch10 MTU value to 1500.
B. Configure STP on both switches.
C. Change the native VLAN on the ports.
D. Disable automatic negotiation on Switch11.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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: 49
A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?
A. Change the email client configuration to match the MX record.
B. Reduce the TTL record prior to the MX record change.
C. Perform a DNS zone transfer prior to the MX record change.
D. Update the NS record to reflect the IP address change.
Answer: (SHOW ANSWER)
Understanding TTL (Time to Live):
TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients.
A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.
Impact of TTL on DNS Changes:
When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.
Best Practice Before Making DNS Changes:
To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making thechanges. This ensures that any cached records will expire quickly, and the new records will be used sooner.
Verification of DNS Changes:
After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.
Comparison with Other Options:
Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.
Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.
Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.
References:
CompTIA Network+ study materials and DNS best practices.

NEW QUESTION: 50
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: 51
A network technician is troubleshooting the connection to the company website. The traceroute command produces the following output:
Traceroute towww.mysite.com(8.8.8.8) over a maximum of 30 hops
10.1.1.1 <1 ms 2. * <1 ms <1 ms
k k
k kTraceroute completeWhich of the following should the technician do to identify the path to the server?
A. Review the router's ACL.
B. Execute netstat.
C. Perform an nslookup.
D. Enable LLDP.
Answer: (SHOW ANSWER)
When traceroute shows asterisks (timeouts) instead of IP addresses or hostnames, it may indicate that intermediate routers are dropping ICMP packets. However, performing an nslookup will reveal the IP address associated with the domain name, confirming that DNS resolution is correct and helping identify the path to the target server. The document states: "nslookup is used to query DNS servers to retrieve IP address information associated with a domain name, which helps confirm DNS resolution is working correctly even when traceroute results show timeouts."

NEW QUESTION: 52
A small business is choosing between static and dynamic routing for its network. Which of the following is the best reason to use dynamic routing in a growing network?
A. Easier to configure compared to using manually entered routes
B. Does not require additional network security controls
C. Features enhanced network monitoring and visibility
D. Includes automatic changes and updates in network topology
Answer: (SHOW ANSWER)
Dynamic routing is most beneficial in a growing/changing network because it can automatically learn, adapt, and update routes as the topology changes. In Network+ (N10-009) routing objectives, dynamic routing protocols exchange routing information between routers and recalculate paths when links go down, new networks are added, or metrics change. This reduces the operational burden and the risk of human error that increases as the environment scales. With dynamic routing, adding a new subnet or branch often requires far fewer manual updates because routers propagate new route information automatically, and convergence mechanisms help restore connectivity after failures.

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

NEW QUESTION: 53
Which of the following helps a network administrator understand security risk from external malicious actors and offers insights on which threats to mitigate?
A. Compliance benchmarks
B. CIA triad
C. SAML
D. Honeypot
Answer: (SHOW ANSWER)
The CIA triad (Confidentiality, Integrity, Availability) is a foundational security model used in Network+ (N10-009) to evaluate risk and guide prioritization of mitigations. By categorizing assets and threats based on how they could impact confidentiality (data exposure), integrity (unauthorized alteration), or availability (service disruption), administrators can better understand which attacks from external actors matter most to the business and which controls to apply first. For example, a public-facing portal might prioritize availability protections (DDoS mitigation, redundancy), while sensitive customer records demand strong confidentiality controls (encryption, access control), and financial systems require integrity controls (logging, validation, change control). This model helps translate "threats" into business impact, which is central to deciding what to mitigate.
Compliance benchmarks support meeting regulatory/industry requirements, but they don't inherently provide a conceptual lens for analyzing external attacker impact across all systems.
SAML is a federation
/authentication standard, not a risk model. A honeypot can provide insight into attacker behavior, but it doesn' t broadly structure risk prioritization the way CIA does. Therefore, CIA triad is the best answer.

NEW QUESTION: 54
Voice traffic is experiencing excessive jitter. A network engineer wants to improve call performance and clarity. Which of the following features should the engineer configure?
A. QoS
B. STP
Answer: (SHOW ANSWER)
Quality of Service (QoS) prioritizes delay-sensitive traffic such as VoIP by assigning higher priority in queues, reducing jitter, latency, and packet loss. Implementing QoS policies ensures stable and clear voice communication.
B). STP (Spanning Tree Protocol) prevents switching loops, but it does not address jitter or real-time traffic performance.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - QoS, traffic shaping, prioritization of voice/video.

NEW QUESTION: 55
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: 56
Which of the following cloud service models most likely requires the greatest up-front expense by the customer when migrating a data center to the cloud?
A. Infrastructure as a service
B. Software as a service
C. Platform as a service
D. Network as a service
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Cloud Models section.

NEW QUESTION: 57
A network engineer is designing an internal network that needs to support both IPv4 and IPv6 routing. Which of the following routing protocols is capable of supporting both IPv4 and IPv6?
A. OSPFv3
B. RIPv2
C. BGP
D. EIGRP
Answer: (SHOW ANSWER)
EIGRP(Enhanced Interior Gateway Routing Protocol) supports bothIPv4 and IPv6. While OSPFv3 is specific to IPv6 and RIPv2 only supports IPv4, EIGRP was extended to handle dual-stack environments efficiently.
Reference:Section 2.1 - Characteristics of Routing Technologies - "EIGRP"

NEW QUESTION: 58
Which of the following does a router use to determine the preferred route?
A. Shortest prefix match
B. Routes learned from EIGRP
C. Longest prefix match
D. Routes learned from OSPF
Answer: (SHOW ANSWER)
Routers determine the best route to a destination using longest prefix match. This means the router chooses the route entry with the most specific matching network prefix for the destination IP address. For example, if a routing table contains 10.1.0.0/16 and 10.1.2.0/24, a packet destined to 10.1.2.50 matches both entries, but the router prefers /24 because it is more specific (longer mask). Network+ (N10-009) routing fundamentals emphasize that route selection begins with prefix length specificity before considering other factors within the same prefix length (such as administrative distance and metric, depending on the platform).

"Shortest prefix match" is the opposite of correct behavior. "Routes learned from EIGRP" and "routes learned from OSPF" describe sources of routes, not the general selection rule routers use when multiple matching routes exist. Even if routes come from different protocols, the router still applies selection logic; the universal rule for matching destination networks is longest prefix match. Hence, option C is correct.

NEW QUESTION: 59
A user tries to visit a website, but instead of the intended site, the page displays vmw.cba.com. Which of the following should be done to reach the correct website?
A. Modify the CNAME record
B. Update the PTR record
C. Change the NTP settings
D. Delete the TXT record
Answer: (SHOW ANSWER)
A CNAME (Canonical Name) record maps an alias to the correct fully qualified domain name (FQDN). If a user is redirected to the wrong hostname, correcting or updating the CNAME ensures the alias points to the proper domain.
B). PTR record maps IP to hostname (reverse DNS), not forward website resolution.
C). NTP relates to time sync, irrelevant to DNS resolution.
D). TXT record stores metadata like SPF or DKIM info, not used for hostname aliasing.
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - DNS record types (A, AAAA, CNAME, PTR, TXT).

NEW QUESTION: 60
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: 61
A company's network is experiencing high latency and packet loss during peak hours. Network monitoring tools show increased traffic on a switch. Which of the following should a network technician implement to reduce the network congestion and improve performance?
A. Load balancing
B. Port mirroring
C. Quality of Service
D. Spanning Tree Protocol
Answer: (SHOW ANSWER)
Quality of Service (QoS): This is a feature used in networking to prioritize certain types of traffic. By configuring QoS, network administrators can allocate higher bandwidth to time-sensitive applications like VoIP, video conferencing, or critical business applications during peak usage times. This helps to reduce latency and packet loss, which are often caused by congestion.
Load Balancing (A): While load balancing is useful in distributing traffic across multiple servers or paths, it does not address congestion on a single switch.
Port Mirroring (B): This is used for monitoring network traffic for troubleshooting and diagnostics but does not alleviate congestion.
Spanning Tree Protocol (D): STP prevents switching loops in redundant network topologies, but it is not designed to handle traffic prioritization or congestion issues.
Reference: CompTIA Network+ Official Study Guide, Domain 1.5 (Network Optimization), Domain 2.1 (Network Management).

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

NEW QUESTION: 63
A company security policy requires all network traffic from remote employees ' corporate laptops to use the company's VPN. Which of the following network access methods best describes this scenario?
A. Clientless VPN
B. Full-tunnel
C. Site-to-site tunnel
D. Split-tunnel
Answer: (SHOW ANSWER)
The correct answer is Full-tunnel because the policy requires all network traffic from remote corporate laptops to pass through the company's VPN. In a full-tunnel VPN configuration, once the VPN connection is established, all traffic-including internet-bound traffic-is routed through the corporate network before reaching its destination. This ensures centralized monitoring, content filtering, logging, and enforcement of security controls such as IDS/IPS and firewalls.
According to CompTIA Network+ (N10-009) security objectives, full-tunnel VPNs enhance security by preventing users from directly accessing the internet from their local connection, thereby reducing exposure to local network threats (e.g., public Wi-Fi attacks).
A split-tunnel VPN (Option D) allows users to access the internet directly while only sending corporate- bound traffic through the VPN, which does not meet the "all traffic" requirement. A site-to-site tunnel (Option C) connects entire networks rather than individual remote users. A clientless VPN (Option A) typically provides web-based access without a full network tunnel and does not necessarily route all traffic.
Therefore, full-tunnel best matches the policy requirement.

NEW QUESTION: 64
A data center administrator is evaluating the use of jumbo frames within a storage environment. Which of the following describes the best reason to use jumbo frames in the storage environment?
A. To reduce device overhead
B. To report on the current root switch in the STP
C. To improve routing convergence
D. To increase drive throughput
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard 1,500 bytes. Using jumbo frames reduces the number of frames transmitted over the network, thereby reducing the overhead associated with frame headers and processing. The document explains:
"Jumbo frames are used in storage networks to reduce device overhead by lowering the number of frames required for data transfer, which can increase overall throughput and performance."

NEW QUESTION: 65
Which of the following types of attacks is most likely to occur after an attacker sets up an evil twin?
A. On-path
B. DDoS
C. ARP spoofing
D. Phishing
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):

An evil twin is a malicious wireless access point that impersonates a legitimate SSID. Once victims connect, the attacker can intercept and manipulate traffic, performing an on-path (man-in-the-middle) attack- capturing credentials, injecting content, or downgrading encryption.
B). DDoS overwhelms services with traffic; it's not the typical follow-on from clients joining a rogue AP.
C). ARP spoofing is another way to become on-path on wired segments, but with an evil twin, the wireless association itself enables the on-path position.
D). Phishing is social engineering; while an evil twin could be used to present fake portals, the primary technical posture after connection is on-path.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs/evil twins), traffic interception, on-path attacks.

NEW QUESTION: 66
A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?
A. 802.1Q tagging
B. Spanning tree
C. Link aggregation
D. Jumbo frames
Answer: D (LEAVE A REPLY)
VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size.
This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging enables segmentation but does not address fragmentation issues.
B). Spanning tree - STP prevents loops but does not improve performance for VXLAN traffic.
C). Link aggregation - LACP combines links for higher bandwidth but does not prevent fragmentation.
D). Jumbo frames - Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network performance concepts.
RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

NEW QUESTION: 67
After a security incident, a technician reveals that company data was stolen. During the investigation, it is discovered that a host disguised itself as a switch. Which of the following best describes the attack that occurred?
A. VLAN hopping
B. Evil twin
C. DNS poisoning
D. ARP spoofing
Answer: (SHOW ANSWER)
VLAN hopping occurs when an attacker tricks a switch into believing the host is another switch by generating tagged frames or exploiting trunk negotiation (DTP). This allows the attacker to access traffic from multiple VLANs, potentially stealing sensitive data.
B). Evil twin is a rogue wireless AP attack, unrelated to switch impersonation.
C). DNS poisoning corrupts name resolution, not VLAN access.
D). ARP spoofing is a Layer 2 on-path attack, not masquerading as a switch.
References (CompTIA Network+ N10-009):

Domain: Network Security - VLAN hopping attacks, switch spoofing techniques.

NEW QUESTION: 68
A network technician is adding a new switch to increase capacity on the network. The technician connects the two switches using a single cable. Several hosts are moved to the new switch, but none of the hosts can access the network or internet. Which of the following should the technician do to resolve the issue?
A. Configure the connecting ports as trunk ports
B. Install STP cables between the switches
C. Increase the PoE budget for the switches
D. Set up link aggregation on the uplink ports
Answer: (SHOW ANSWER)
The correct solution is to configure the connecting ports as trunk ports. When connecting switches, the uplink ports must be configured to carry traffic for multiple VLANs (trunking), not just a single access VLAN.
Without trunking, VLAN tags may be dropped, and traffic from hosts will not reach the rest of the network or internet.
B). STP cables is a misnomer - STP refers to Spanning Tree Protocol or Shielded Twisted Pair cables, neither of which solves this logical configuration issue.
C). PoE budget is irrelevant because switches and hosts in this context don't require PoE.
D). Link aggregation (LACP, EtherChannel) is for increasing bandwidth/redundancy across multiple links, not required with a single cable.
By enabling trunking on the uplink ports, the switches can pass VLAN-tagged traffic, ensuring hosts connected to the new switch have access to the same resources as those on the existing switch.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN trunking, inter-switch connectivity.

NEW QUESTION: 69
A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?
A. EIGRP
B. OSPFv3
C. BGP4
D. iBGP
Answer: (SHOW ANSWER)
For an internal network using IPv6, the best option listed is OSPFv3, which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence. BGP4 and iBGP are associated with BGP, primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor- neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.

NEW QUESTION: 70
After installing a new 6E wireless router in a small office, a technician notices that some wireless devices are not able to achieve the rated speeds.
Which of the following should the technician check to troubleshoot the issue? (Select two)

A. Voltage source requirements

B. Back-end cabling
C. Weather phenomena
D. Client device compatibility
E. Processing power
F. Interference levels
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 71
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: 72
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: 73
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: A (LEAVE A REPLY)
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: 74
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: 75
A company is hosting a secure that requires all connections to the server to be encrypted. A junior administrator needs to harded the web server. The following ports on the web server.
The following ports on the web server are open:

443
80
22
587

Which of the following ports should be disabled?
A. 22
B. 80
C. 443
D. 587
Answer: (SHOW ANSWER)
For a web server that requires all connections to be encrypted, port 80 (HTTP) should be disabled. Port 80 is used for unencrypted web traffic, whereas port 443 is used for HTTPS, which provides encrypted communication.
Port 80 (HTTP): This port is used for unsecured web traffic. Disabling this port ensures that all web traffic must use HTTPS, which encrypts the data in transit.
Port 443 (HTTPS): This port is used for secure web traffic via SSL/TLS encryption. Keeping this port open ensures that secure connections can be made to the web server.
Other Ports:
Port 22: Used for SSH, providing secure remote access and file transfers.
Port 587: Used for secure email submission (SMTP) with encryption.

Network References:
CompTIA Network+ N10-007 Official Certification Guide: Discusses the roles and security implications of various ports and protocols.
Cisco Networking Academy: Provides training on secure web server configuration and port management.
Network+ Certification All-in-One Exam Guide: Covers port security and best practices for securing web servers.

NEW QUESTION: 76
A network administrator needs to divide a Class B network into four equal subnets, each with a host range of
1,000 hosts. Which of the following subnet masks should the administrator use?
A. 255.255.0.0
B. 255.255.252.0
C. 255.255.255.0
D. 255.255.255.128
Answer: (SHOW ANSWER)
The best answer is B. 255.255.252.0 , which is a /22 mask. A Class B network starts with a default mask of
255.255.0.0 or /16 . The question says the administrator wants four equal subnets , which means borrowing 2 bits from the host portion, since 2 borrowed bits gives $2^2 = 4$ subnets . That moves the mask from /16 to /18 if subnetting is based only on splitting the Class B into four equal parts.
However, the answer choices point toward the host requirement as the deciding factor. Each subnet needs to support about 1,000 hosts . A /22 leaves 10 host bits , which gives 2^{1}# = 1024 total addresses , or 1022 usable hosts after subtracting the network and broadcast addresses. That fits the requirement. Among the options provided, 255.255.252.0 is the only mask that supports around 1,000 hosts per subnet.
The smaller masks, /24 and /25 , do not allow enough hosts. The default Class B mask, /16 , does not subnet the network at all. Based on the available choices and the host-capacity requirement, 255.255.252.0 is the correct exam answer.

NEW QUESTION: 77
Which of the following is associated with avoidance, acceptance, mitigation, and transfer?
A. Risk
B. Exploit
C. Threat
D. Vulnerability
Answer: (SHOW ANSWER)
These four terms-avoidance, acceptance, mitigation, and transfer-are strategies used in risk management.
From Andrew Ramdayal's guide:
"Risk in security refers to the potential for loss, damage, or destruction of assets or data due to a threat exploiting a vulnerability. Risk management strategies include avoidance, acceptance, mitigation, and transfer."

NEW QUESTION: 78

In the troubleshooting methodology, which of the following actions comes after verifying that the initial problem has been resolved?
A. If necessary, escalating the issue
B. Attempting to replicate the problem
C. Documenting findings
D. Implementing the plan
Answer: C (LEAVE A REPLY)
In the CompTIA Network+ (N10-009) troubleshooting methodology, the step that follows verifying full system functionality (confirming the issue is resolved and validating with the user/requirements) is documenting findings, actions, and outcomes. Documentation is a required closing step because it captures what the original symptoms were, what troubleshooting steps were performed, what root cause was identified (if found), what remediation was applied, and what validation confirmed success. This record supports operational continuity by enabling faster resolution if the issue recurs, improving knowledge transfer across teams, and meeting organizational change-control or compliance requirements.
The other options fall in different parts of the methodology. Attempting to replicate the problem is typically performed earlier-after identifying symptoms and before or during isolation-to confirm the issue and help narrow scope. Implementing the plan occurs before verification; you implement the selected solution or escalation plan and then test/verify. Escalating the issue occurs when the technician lacks access, expertise, time, or evidence to proceed, and it can happen during troubleshooting-but it is not the standard step that comes after verifying resolution.

NEW QUESTION: 79
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: 80
Which of the following routing protocols is most commonly used to interconnect WANs?
A. IGP
B. EIGRP
C. BGP
D. OSPF
Answer: (SHOW ANSWER)

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

NEW QUESTION: 81
A network administrator for a small office is adding a passive IDS to its network switch for the purpose of inspecting network traffic. Which of the following should the administrator use?
A. SNMP trap
B. Port mirroring
C. Syslog collection
D. API integration
Answer: (SHOW ANSWER)
Port mirroring, also known as SPAN (Switched Port Analyzer), is used to send a copy of network packets seen on one switch port (or an entire VLAN) to another port where the IDS is connected. This allows the IDS to passively inspect network traffic without interfering with the actual traffic flow. Port mirroring is an essential feature for implementing IDS in a network for traffic analysis and security monitoring.References:
CompTIA Network+ study materials.

NEW QUESTION: 82
Which of the following routing protocols uses an autonomous system number?
A. IS-IS
B. EIGRP
C. OSPF
D. BGP
Answer: (SHOW ANSWER)
BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.References:CompTIA Network+ study materials and RFC 4271.

NEW QUESTION: 83
A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?
A. Develop a theory.
B. Establish a plan of action.
C. Implement the solution.
D. Document the findings.
Answer: (SHOW ANSWER)
Once the theory has been tested and confirmed, the next step is to implement the solution based on the CompTIA troubleshooting model.
CompTIA Troubleshooting Model:
Identify the problem.
Establish a theory of probable cause.

Test the theory.
Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.
Document findings, actions, and outcomes.
Breakdown of Options:
A). Develop a theory - The theory has already been developed and tested.
B). Establish a plan of action - This happens before implementation, but since the issue is confirmed, it's time to act.
C). Implement the solution - Correct answer. The problem is confirmed, so the fix should be applied.
D). Document the findings - Documentation is the final step, not the next one.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 5.1: Explain network troubleshooting methodology.

NEW QUESTION: 84
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: 85
Which of the following devices functions mainly at the data link layer of the OSI model and is used to connect a fiber-optic cable to a network interface?
A. SC
B. DAC
C. SFP transceiver
D. Twinaxial cable
Answer: (SHOW ANSWER)
An SFP (Small Form-factor Pluggable) transceiver is a modular device that provides the interface between fiber-optic or copper cabling and the networking equipment (e.g., switch or router). It operates primarily at Layer 2 (Data Link), converting optical or electrical signals into frames usable by the network device.
A). SC is a fiber connector type, not the transceiver.
B). DAC (Direct Attach Copper) is a passive copper cable assembly with fixed transceivers, not a general- purpose module.
D). Twinaxial cable is a copper medium, not an interface device.

References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Transceivers (SFP, GBIC, QSFP), fiber connectivity, OSI model mapping.

NEW QUESTION: 86
A network engineer configures a NIC that has an IP address of 192.168.123.232. Which of the following classes is this address an example of?
A. Class A
B. Class B
C. Class C
D. Class D
Answer: (SHOW ANSWER)
The IPv4 address 192.168.123.232 falls within the Class C range under classful addressing. In classful terms, Class C addresses have a first octet from 192 to 223, which makes any address starting with 192.x.x.x a Class C address. Network+ (N10-009) networking concepts cover IPv4 addressing fundamentals and commonly reference class ranges as foundational knowledge, even though modern networks primarily use CIDR (classless) subnetting rather than strict classful boundaries.
This address is also within a well-known private IPv4 block: 192.168.0.0/16 (RFC1918 private addressing), which is frequently used for internal networks and NIC configurations where addresses are not routable on the public internet.
To eliminate the distractors: Class A uses first octet 1-126, Class B uses 128-191, and Class D (224-239) is reserved for multicast. Since the first octet here is 192, it maps to Class C, making option C correct.

NEW QUESTION: 87
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: 88
Which of the following can support a jumbo frame?
A. Access point
B. Bridge
C. Hub
D. Switch
Answer: (SHOW ANSWER)
* Definition of Jumbo Frames:
* Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.
* Why Switches Support Jumbo Frames:

* Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.
* Incompatibility of Other Devices:
* Access Point: Primarily handles wireless communications and does not typically support jumbo frames.
* Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.
* Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.
* Practical Application:
* Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.
References:
* CompTIA Network+ course materials and networking hardware documentation.

NEW QUESTION: 89
Which of the following standards enables the use of an enterprise authentication for network access control?
A. 802.1Q
B. 802.1X
C. 802.3bt
D. 802.11h
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
802.1X provides port-based Network Access Control (NAC), requiring authentication (often through RADIUS) before granting access. This is the standard for enterprise authentication on both wired and wireless networks.
A). 802.1Q defines VLAN trunking.
C). 802.3bt defines higher-power PoE.
D). 802.11h deals with spectrum management in wireless.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication.

NEW QUESTION: 90
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: 91
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: 92
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: 93
A security administrator is creating a new firewall object for a device with IP address 192.168.100.1/25.
However, the firewall software only uses dotted decimal notation in configuration fields. Which of the following is the correct subnet mask to use?
A. 255.255.254.0
B. 255.255.255.1
C. 255.255.255.128
D. 255.255.255.192
Answer: (SHOW ANSWER)
A /25 subnet mask means 25 bits are reserved for the network portion, leaving 7 bits for host addresses. In dotted decimal, that is:
11111111.11111111.11111111.10000000
Decimal equivalent: 255.255.255.128
A). 255.255.254.0 corresponds to /23.
B). 255.255.255.1 is invalid as a subnet mask.
D). 255.255.255.192 corresponds to /26.
Thus, the correct subnet mask for a /25 network is 255.255.255.128.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Subnetting, CIDR notation, dotted decimal.

NEW QUESTION: 94
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: 95
A network manager connects two switches together and uses two connecting links. Which of the following configurations will prevent Layer 2 loops?

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

NEW QUESTION: 96
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: 97
A newtwork administrator needs to create an SVI on a Layer 3-capable device to separate voice and data traffic. Which of the following best explains this use case?
A. A physical interface used for trunking logical ports
B. A physical interface used for management access
C. A logical interface used for the routing of VLANs
D. A logical interface used when the number of physical ports is insufficent.
Answer: (SHOW ANSWER)
An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.
* SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.
* VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.
* Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.

* Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.
* Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

NEW QUESTION: 98
Which of the following protocols uses the Dijkstra's Link State Algorithm to establish routes inside its routing table?
A. OSPF
B. EIGRP
C. BGP
D. RIP
Answer: (SHOW ANSWER)
OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.
From Andrew Ramdayal's guide:
"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

NEW QUESTION: 99
A network administrator wants an automatic alert to be sent when a switch ' s link status changes, administered through SNMP. Which of the following SNMP technologies will allow for this alert?
A. Trap
B. Object identifier
C. String
D. MIB
Answer: (SHOW ANSWER)
The right answer is A. Trap . In SNMP, a trap is an unsolicited notification sent from a managed device to the management system when a significant event happens. A switch detecting that an interface has gone up or down is a textbook example of the kind of event that can trigger this kind of message.
That is different from normal SNMP polling, where the monitoring server asks the device for status information on a schedule. With a trap, the device does not wait to be asked. It sends the alert immediately, which makes it useful for link failures, threshold violations, and other time-sensitive conditions.
The other choices are related to SNMP, but not in the same way. An object identifier (OID) points to a specific managed value. A string is commonly associated with SNMP community information in older versions. A MIB is the structured database of manageable objects. None of those are the actual alerting mechanism.
Because the question asks for an automatic alert when link status changes, the feature being described is clearly an SNMP trap .

NEW QUESTION: 100
Which of the following does BGP use for loop avoidance?
A. Autonomous system path
B. Peer autonomous system
C. Autonomous system length
D. Public autonomous system
Answer: (SHOW ANSWER)
The correct answer is Autonomous system path because BGP (Border Gateway Protocol) prevents routing loops by using the AS_PATH attribute. According to CompTIA Network+ (N10-009) objectives under routing protocols, BGP is a path vector protocol used to exchange routing information between autonomous systems (AS) on the internet.

When a BGP router advertises a route, it includes its autonomous system number (ASN) in the AS_PATH attribute. As the route passes through additional autonomous systems, each AS appends its own ASN to the path. If a BGP router receives a route advertisement that already contains its own ASN in the AS_PATH list, it recognizes this as a loop and rejects the route. This mechanism effectively prevents routing loops across large-scale networks such as the internet.
Option B (Peer autonomous system) refers to neighboring BGP routers but does not describe the loop prevention mechanism. Option C (Autonomous system length) relates to path selection metrics, as shorter AS_PATH lengths are generally preferred, but this is not the loop avoidance function itself. Option D (Public autonomous system) is not a loop prevention mechanism.
Therefore, BGP uses the AS_PATH attribute for loop avoidance.

NEW QUESTION: 101
Which of the following steps of the troubleshooting methodology would most likely involve comparing current throughput tests to a baseline?
A. Implement the solution
B. Verify full system functionality
C. Document findings
D. Test the theory
Answer: (SHOW ANSWER)
Verifying full system functionality occurs after implementing a fix. This step ensures the solution resolved the issue and that performance is back to expected levels. Comparing current throughput to baseline measurements is part of validation testing to confirm everything is within normal operational parameters.
A). Implement the solution applies the fix but does not confirm results.
C). Document findings happens at the end of troubleshooting.
D). Test the theory comes earlier, when trying to confirm the suspected cause.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Troubleshooting methodology steps, baselines, verification testing.

NEW QUESTION: 102
A network administrator is creating a subnet that will include 45 separate hosts on a small private network within a large network architecture. Which of the following options is the most efficient use of network addresses when assigning this network?
A. 10.0.50.128/25
B. 10.7.142.128/27
C. 10.152.4.192/26
D. 10.192.1.64/28
Answer: (SHOW ANSWER)
For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).
A /26 subnet provides 64 addresses, 62 usable - suitable.
A /27 subnet gives only 30 usable - insufficient.
A /25 offers 126 usable - more than needed.
A /28 provides just 14 - too small.
So, the most efficient subnet with minimal wastage is /26.
From Andrew Ramdayal's guide:
"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts. A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."

NEW QUESTION: 103
A network administrator wants to restrict inbound traffic to allow only HTTPS to the company website, denying all other inbound traffic from the internet. Which of the following would best accomplish this goal?
A. ACL on the edge firewall
B. Port security on an access switch
C. Content filtering on a web gateway
D. URL filtering on an outbound proxy
Answer: (SHOW ANSWER)
AnAccess Control List (ACL)configured on theedge firewallis the correct and most effective solution tofilter inbound traffic. The administrator can allow TCP port 443 (HTTPS) and deny all other traffic. This is a classic firewall configuration for securing public-facing servers.
Reference:Section 4.3 - Network Security Features, Defense Techniques, and Solutions - "ACLs (Access Control Lists)"

NEW QUESTION: 104
Which of the following technologies are X.509 certificates most commonly associated with?
A. PKI
B. VLAN tagging
C. LDAP
D. MFA
Answer: (SHOW ANSWER)
X.509 certificates are most commonly associated with Public Key Infrastructure (PKI). These certificates are used for a variety of security functions, including digital signatures, encryption, and authentication.
* PKI: X.509 certificates are a fundamental component of PKI, used to manage encryption keys and authenticate users and devices.
* Digital Certificates: They are used to establish secure communications over networks, such as SSL/TLS for websites and secure email communication.
* Authentication and Encryption: X.509 certificates provide the means to securely exchange keys and verify identities in various applications, ensuring data integrity and confidentiality.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers PKI and the role of X.509 certificates in network security.
* Cisco Networking Academy: Provides training on PKI, certificates, and secure communications.
* Network+ Certification All-in-One Exam Guide: Explains PKI, X.509 certificates, and their applications in securing network communications.

NEW QUESTION: 105
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: 106
A network administrator needs to locate a specific AP using a spectrum analyzer to complete an 802.11ax device migration. Which of the following should display on the analyzer to locate the AP?
A. SSID
B. RSSI
C. Channel number
D. BSSID
Answer: (SHOW ANSWER)
To locate a specific access point (AP), the most reliable identifier to view is the BSSID. In 802.11 networks, the BSSID is the radio interface identifier for the AP (typically the AP radio's MAC address). Unlike an SSID, which can be shared across many APs in the same wireless network (especially in an enterprise deployment using the same SSID across multiple APs), the BSSID uniquely distinguishes one AP radio from another. This is critical during an 802.11ax (Wi-Fi 6) migration, where multiple APs may broadcast identical SSIDs and operate on the same channels in different areas.
While RSSI is useful for physically walking toward the strongest signal (a technique used in locating RF sources), RSSI alone does not confirm you are tracking the correct AP-only that you are near an RF transmitter. Channel number also does not uniquely identify the AP because multiple APs can share the same channel (and channels may overlap depending on band and width). SSID similarly is not unique. Therefore, viewing the BSSID on the analyzer (or Wi-Fi analyzer mode) allows the administrator to confirm the exact AP being measured and located.

NEW QUESTION: 107
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: 108
Which of the following actions should be taken as part of the first step of the troubleshooting methodology?
A. Create a theory about the possible root cause
B. Use a top-down approach
C. Conduct tests to verify ideas
D. Handle multiple problems individually
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
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: 110
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: 111
A network administrator has been monitoring the company's servers to ensure that they are available. Which of the following should the administrator use for this task?
A. Packet capture
B. Data usage reports
C. SNMP traps
D. Configuration monitoring
Answer: (SHOW ANSWER)
To monitor server availability, SNMP traps are the best choice. SNMP (Simple Network Management Protocol) allows devices to send alerts (traps) when certain conditions are met, such as server downtime or high resource usage.
Breakdown of Options:
A). Packet capture - Capturing packets provides insights into network traffic but does not actively monitor server availability.
B). Data usage reports - These analyze network traffic consumption but do not indicate whether a server is available or not.
C). SNMP traps - Correct answer. SNMP traps notify administrators of server issues in real time.
D). Configuration monitoring - This tracks configuration changes rather than availability.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network monitoring concepts.
RFC 1157: Simple Network Management Protocol (SNMP)

NEW QUESTION: 112
A Linux server is running a log collector that needs to be hardened. A network administrator executes netstat to find open ports on the server. Which of the following ports should be disabled?
A. 22
B. 80
C. 162
D. 514
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
For a log collector server, the primary needed service is Syslog, which typically uses UDP port 514. Other ports may be open for management (e.g., 22 for SSH) or SNMP traps (162) if integrated. However, port 80 (HTTP) should not be open unless required, as it increases attack surface and does not directly serve the log collection purpose. Disabling it hardens the server.
A). 22 (SSH) is needed for secure management.
C). 162 (SNMP trap) may be required for monitoring/log correlation.
D). 514 (Syslog) is essential for log collection.
References (CompTIA Network+ N10-009):
Domain: Network Security - Hardening servers, disabling unnecessary services and ports.

NEW QUESTION: 113
A network administrator is connecting two Layer 2 switches in a network. These switches must transfer data in multiple networks. Which of the following would fulfill this requirement?
A. Jumbo frames

B. 802.1Q tagging
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.
This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.
This method ensures that traffic from different VLANs is properly separated and managed across the network.
References: CompTIA Network+ study materials.

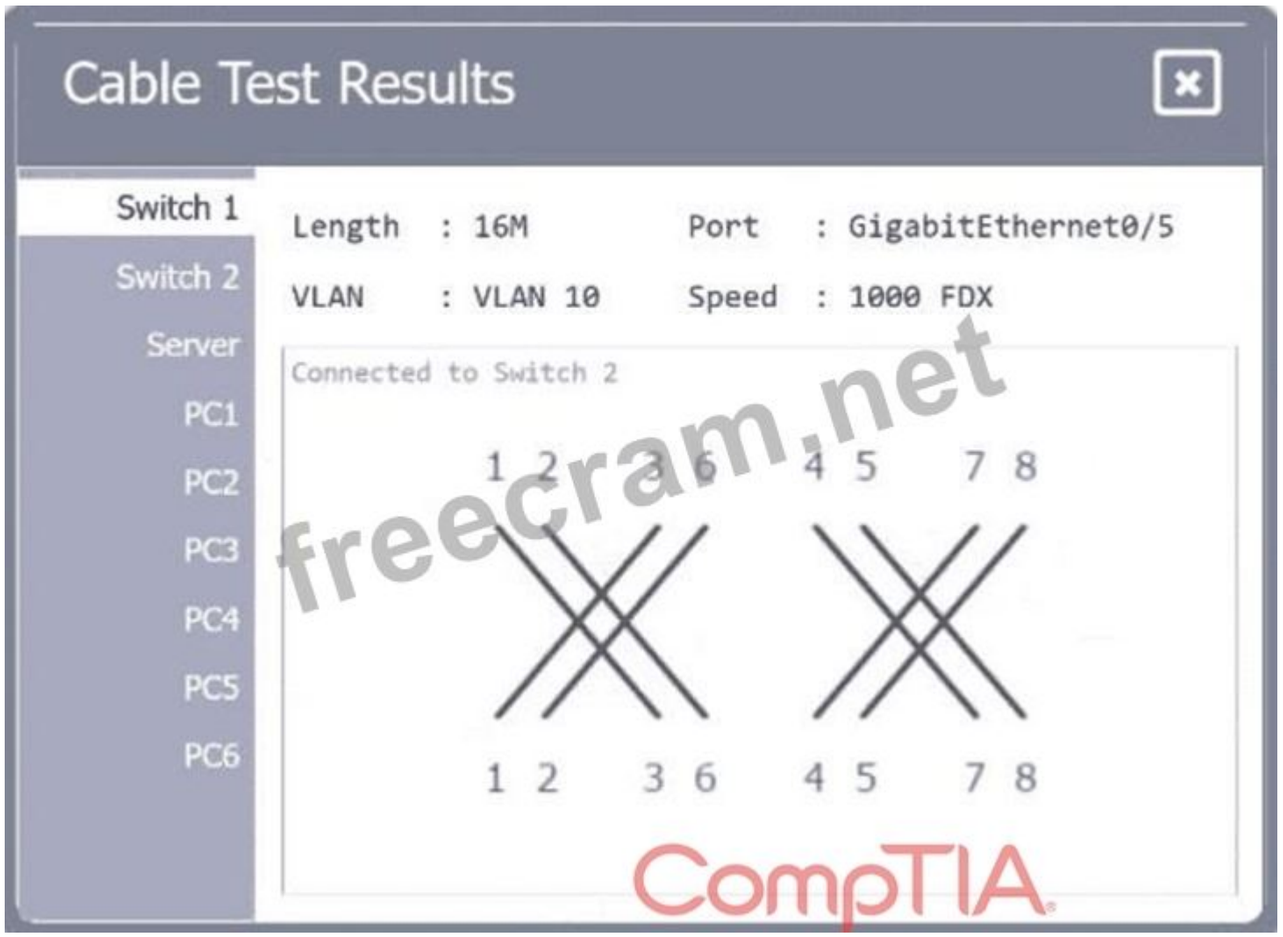
NEW QUESTION: 114
After running a Cat 8 cable using passthrough plugs, an electrician notices that connected cables are experiencing a lot of cross talk. Which of the following troubleshooting steps should the electrician take first?
A. Inspect the connectors for any wires that are touching or exposed.
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.

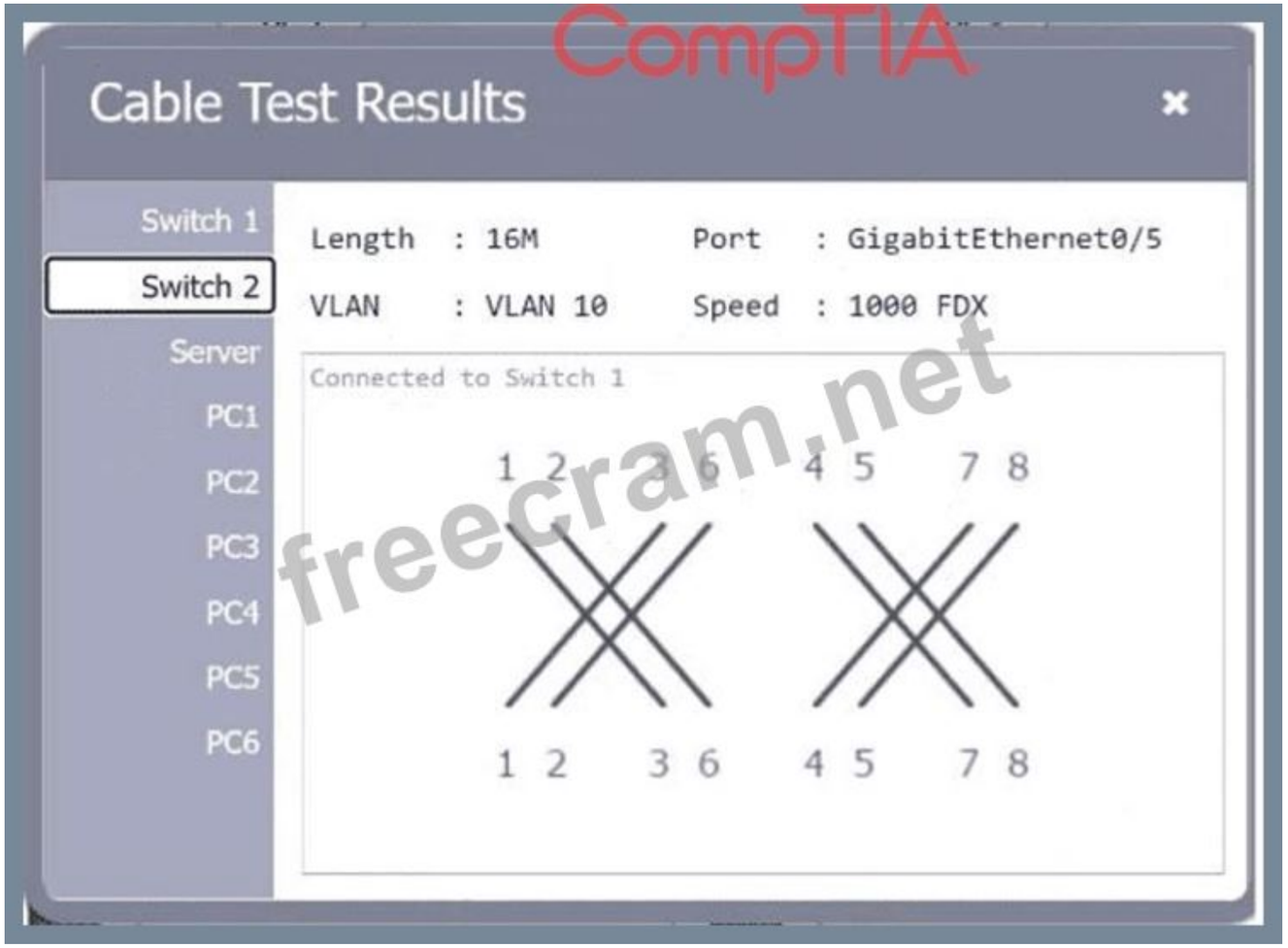
NEW QUESTION: 115
Which of the following allows an organization to map multiple internal devices to a single external-facing IP address?
A. NAT
B. BGP
C. OSPF
D. FHRP
Answer: (SHOW ANSWER)
NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.
B). BGP is a routing protocol.
C). OSPF is a link-state IGP.
D). FHRP provides redundant gateways, not IP sharing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - NAT, PAT, private-to-public IP mapping.

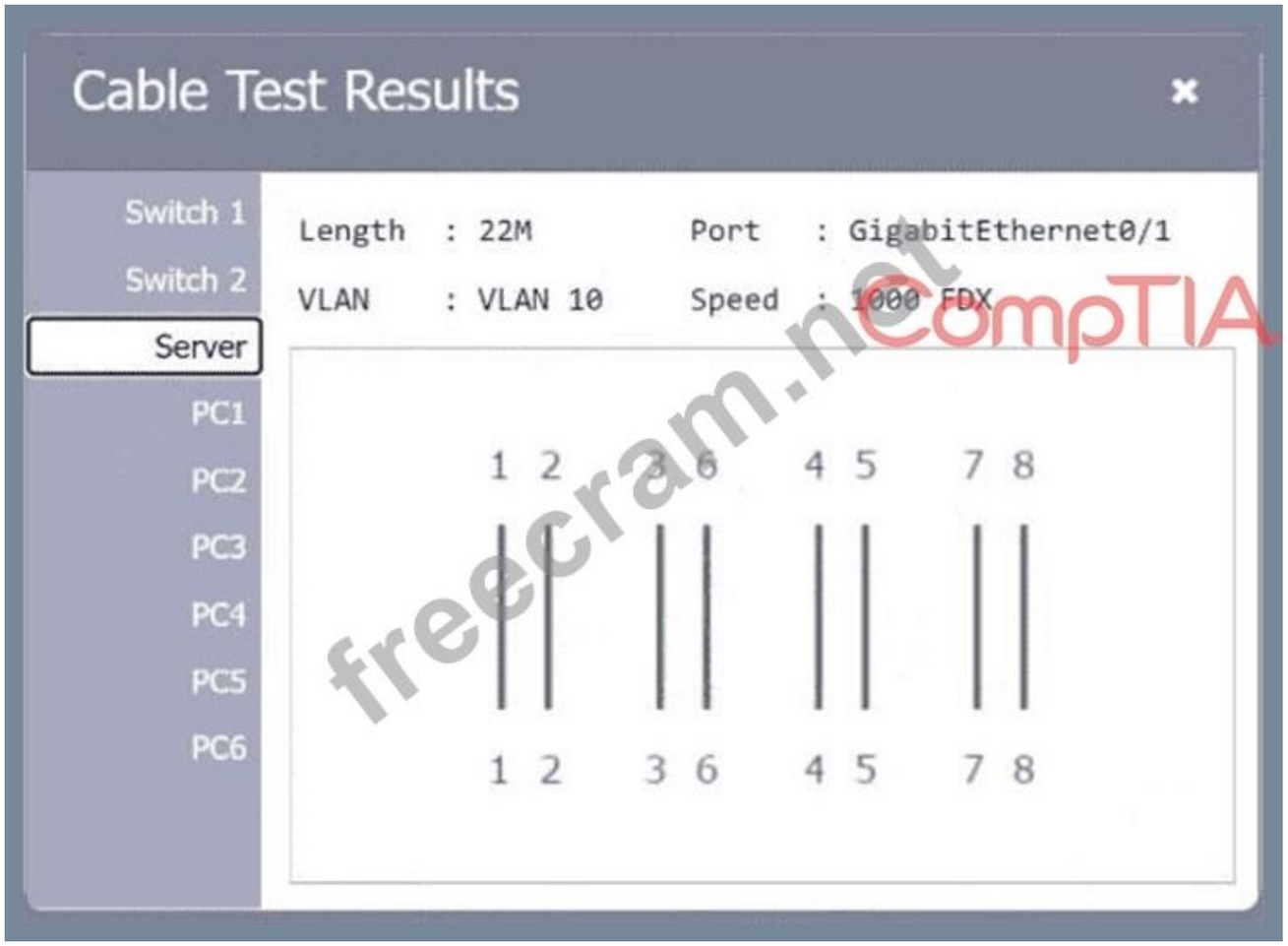
NEW QUESTION: 116
A network administrator upgraded the wireless access points and wants to implement a configuration that will give users higher speed and less channel overlap based on device compatibility. Which of the following will accomplish this goal?
A. 802.1X

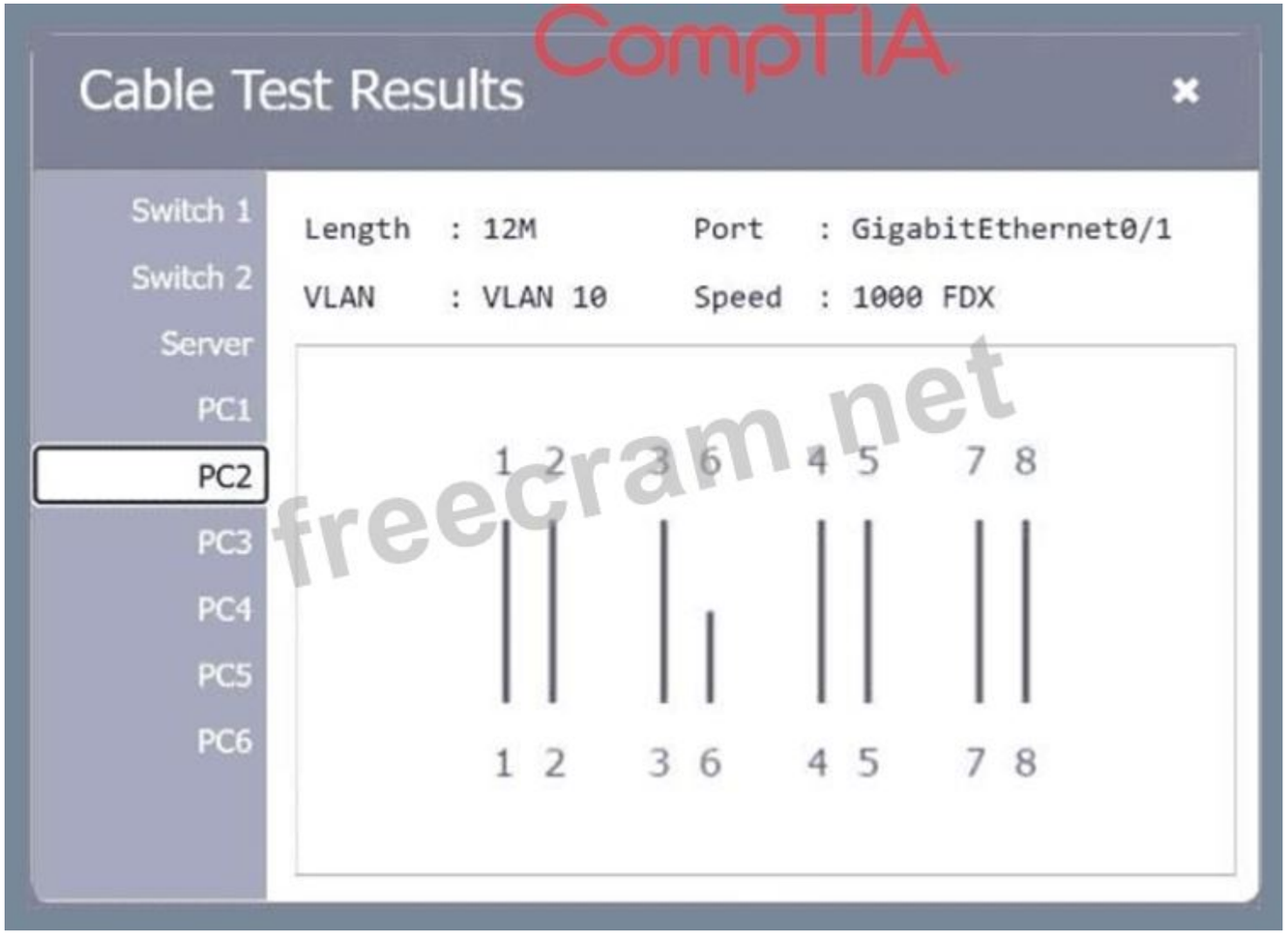
B. MIMO
C. ESSID
D. Band steering
Answer: (SHOW ANSWER)
Band steering allows wireless access points to automatically direct capable devices to the 5GHz band, which typically has higher throughput and less interference than the 2.4GHz band, improving performance. The document confirms:
"Band steering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

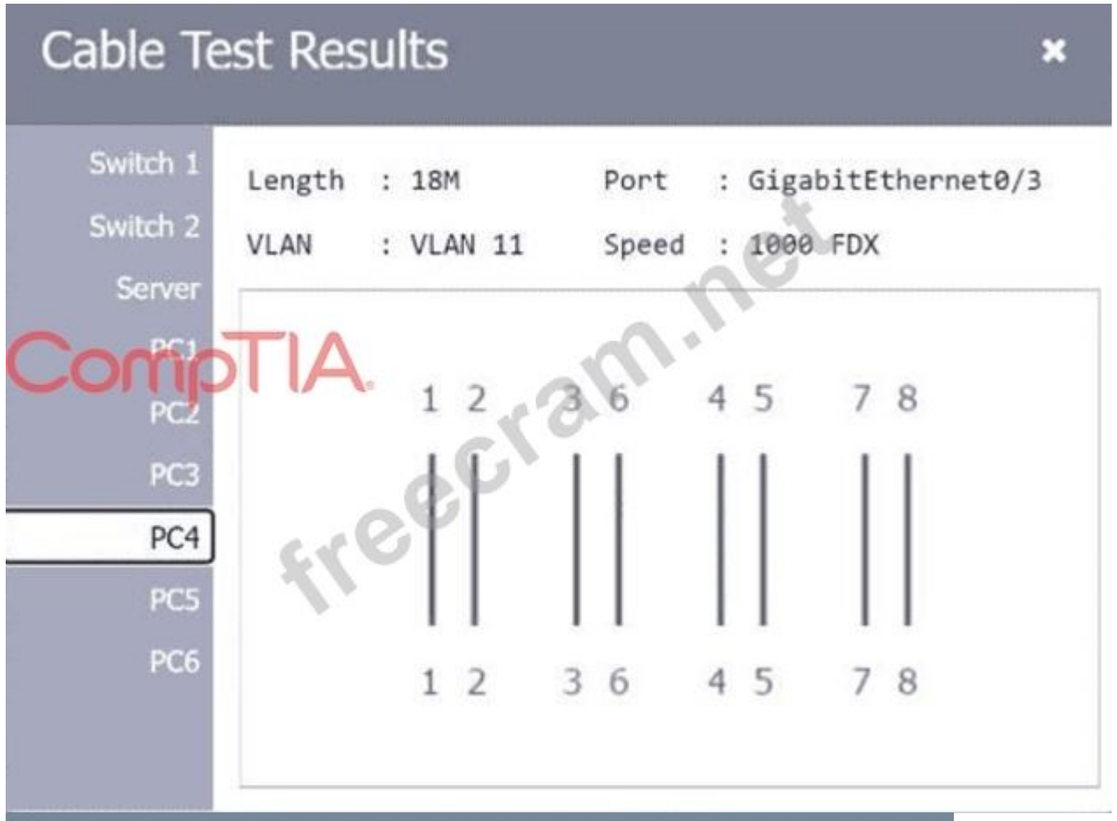
NEW QUESTION: 117
A network technician needs to resolve some issues with a customer ' s SOHO network. The customer reports that some of the PCs are not connecting to the network, while others appear to be working as intended.
INSTRUCTIONS
Troubleshoot all the network components.
Review the cable test results first, then diagnose by clicking on the appropriate PC, server, and Layer 2 switch.
Identify any components with a problem and recommend a solution to correct each problem.
If at any time you would like to bring back
the initial state of the simulation, please
click the Reset All button.

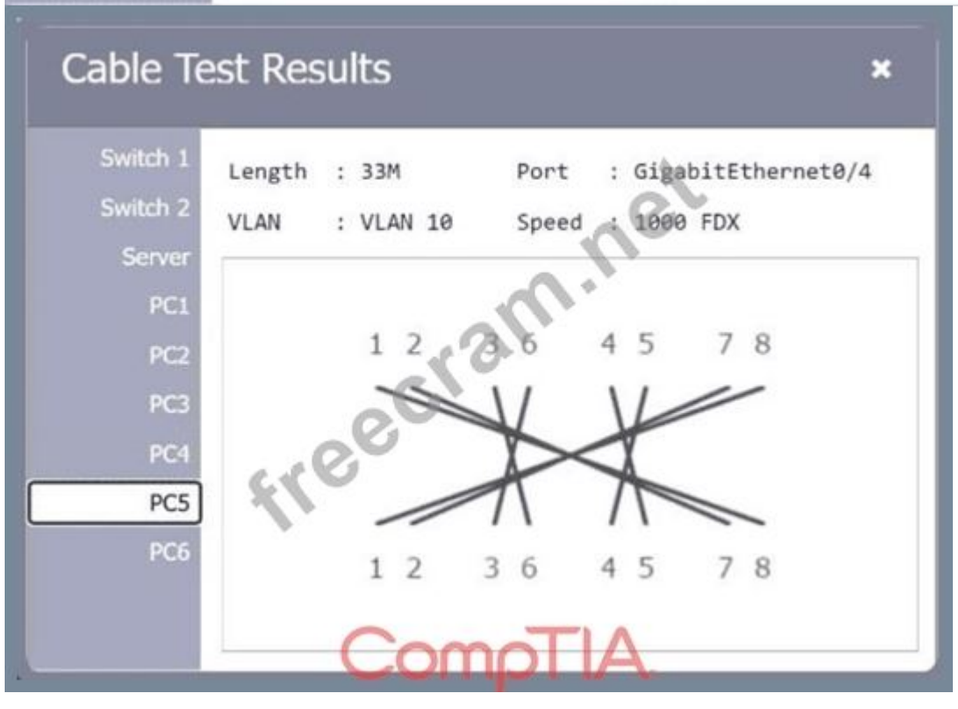


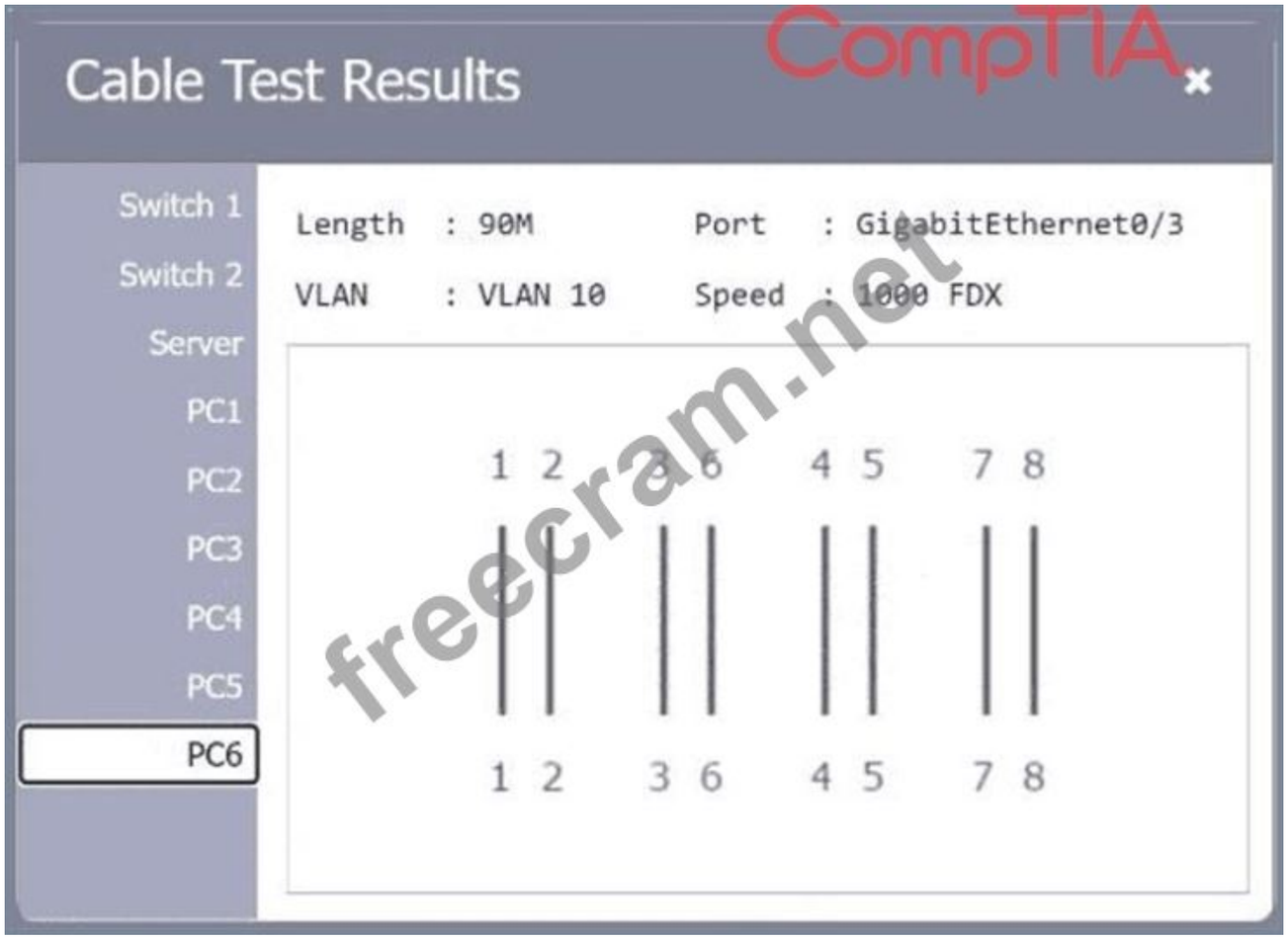










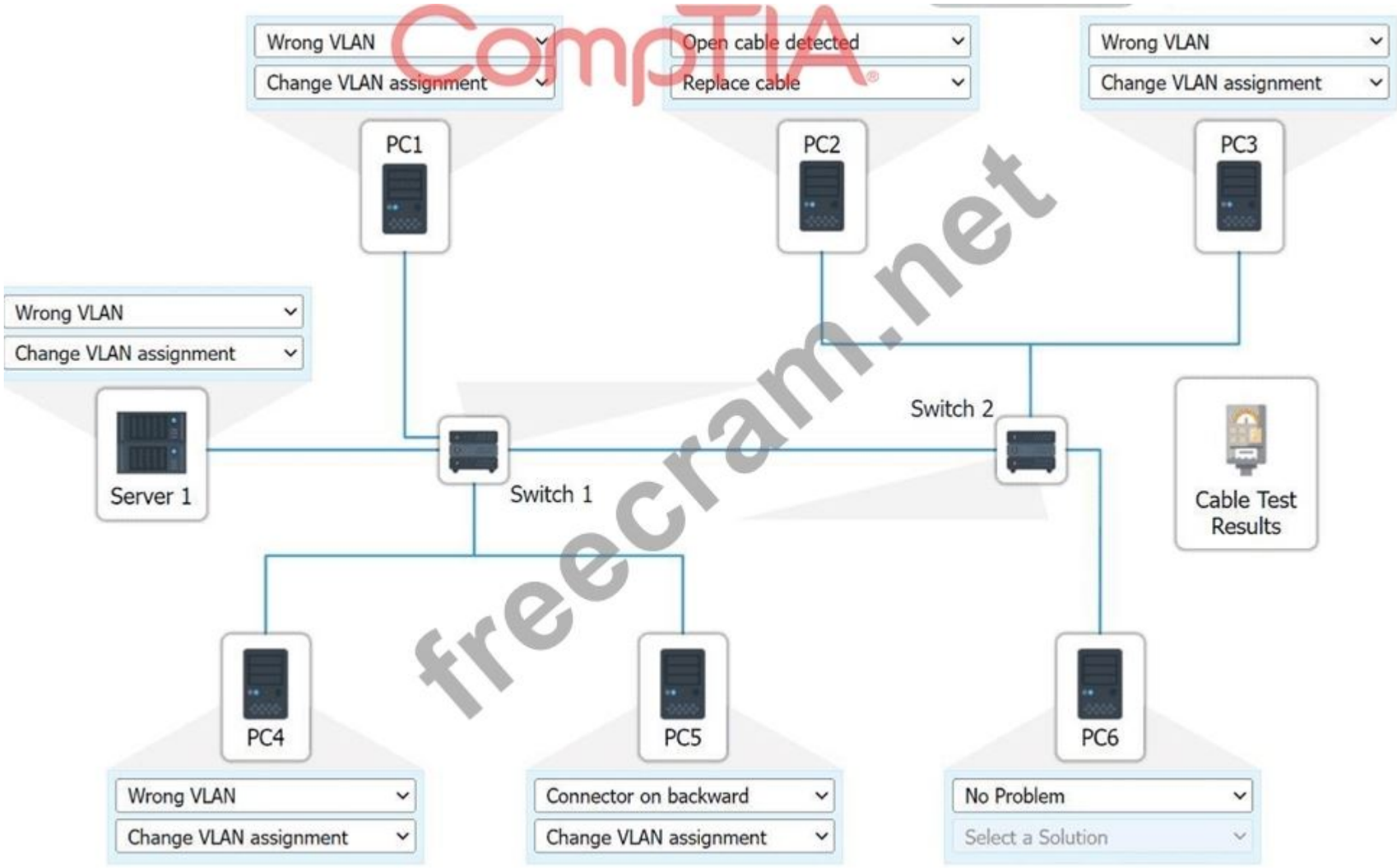


Answer:

See the answer and solution below:

Explanation:

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



NEW QUESTION: 118
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: 119
Which of the following appliances provides users with an extended footprint that allows connections from multiple devices within a designated WLAN?
A. Router
B. Switch
C. Access point

D. Firewall

Answer: (SHOW ANSWER)

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

* Router: Typically used to connect different networks, not specifically for extending wireless coverage.
* Switch: Used to connect devices within a wired network, not for providing wireless access.
* Access Point (AP): Extends wireless network coverage, allowing multiple wireless devices to connect to the network.
* Firewall: Primarily used for network security, controlling incoming and outgoing traffic based on security rules, not for providing wireless connectivity.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Explains the roles and functions of network appliances, including access points.
* Cisco Networking Academy: Provides training on deploying and managing wireless networks with access points.
* Network+ Certification All-in-One Exam Guide: Covers network devices and their roles in creating and managing networks.

NEW QUESTION: 120

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: 121

An organizatin is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that will allow for continous connectivity anywhere in the facility. Which of the following should the network administ rator suggest to ensure the best coverage?

A. nl Changing the current frequency of the WI-FI

B. Implementing additional ad hoc access points

C. Deploying a mesh network in the building

D. Providing more Ethernet drops for user connections

Answer: (SHOW ANSWER)

NEW QUESTION: 122
A customer wants to separate the finance department from the marketing department. The network administrator suggests segmenting the existing Class C network into two sections and readdressing all devices appropriately. Which of the following subnet masks should the network administrator use?
A. /24
B. /25
C. /26
D. /27
Answer: (SHOW ANSWER)
The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.
A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128). This creates two subnets, each with
128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.
A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.
The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

NEW QUESTION: 123
Which of the following types of network architecture typically uses leased lines to provide dedicated, private connections between multiple satellite offices and a head office?
A. Mesh
B. Point to point
C. Hub and spoke
D. Star
Answer: (SHOW ANSWER)
The correct answer is hub-and-spoke. In this design, the head office serves as the hub, and all satellite or branch offices (the spokes) connect directly to the hub using leased lines or VPNs. Communication between spokes typically passes through the hub, which centralizes connectivity and simplifies management.
A). Mesh involves every site connecting to every other site, which is more redundant but costly.
B). Point-to-point describes a single dedicated link between two sites, not a multi-site topology.
D). Star is often used in LAN switching, with all devices connecting to a central switch, but it's not the WAN architecture typically used here.
Hub-and-spoke is a cost-effective WAN design, as fewer circuits are needed compared to full mesh. However, its main disadvantage is reliance on the hub site: if the hub goes down, inter-spoke communication fails.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - WAN topologies (hub-and-spoke, mesh, point-to-point).

NEW QUESTION: 124

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

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

NEW QUESTION: 127
A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.
Instructions:
Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Answer:

See the Explanation for detailed information on this simulation.

Explanation:

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

Click on each switch to open its terminal window.

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

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

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

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

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

The IP address of Core Switch 1 is 192.168.1.1.

The VLAN configuration of Core Switch 1 is VLAN 1: 192.168.1.0/24, VLAN 2: 192.168.2.0/24, VLAN 3: 192.168.3.0/24.

The neighboring devices of Core Switch 1 are Access Switch 1 and Access Switch 2.

The interfaces that connect Core Switch 1 to Access Switch 1 are GigabitEthernet0/1 and GigabitEthernet0/2.

The interfaces that connect Core Switch 1 to Access Switch 2 are GigabitEthernet0/3 and GigabitEthernet0/4.

You can use the same steps to fill in the missing information for Access Switch 1 and Access Switch 2.

NEW QUESTION: 128
Which of the following offers the ability to manage access at the cloud VM instance?
A. Security group
B. Internet gateway
C. Direct Connect
D. Network ACL
Answer: (SHOW ANSWER)
Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.
From Andrew Ramdayal's guide:
"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC.
They act as a virtual firewall for associated instances..."

NEW QUESTION: 129
A network administrator determines that some switch ports have more errors present than expected. The administrator traces the cabling associated with these ports. Which of the following would most likely be causing the errors?
A. arp
B. tracert
C. nmap
D. ipconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 130
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: 131
A user's desk has a workstation and an IP phone. The user is unable to browse the internet on the workstation, but the phone works. Which of the following configurations is required?
A. Voice VLAN
B. Native VLAN
C. Data VLAN

D. Trunk port
Answer: (SHOW ANSWER)
If the IP phone works but the workstation doesn't, it indicates that theVoice VLAN is functioningcorrectly, but theData VLAN (C)is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately usingVLANs.
* A. Voice VLANis for the IP phone, which is already working.
* B. Native VLANis for untagged traffic on trunk ports, but doesn't control access directly.
* D. Trunk portis more relevant to switch interconnections than individual workstation ports.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 132
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: 133
A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare.
Which of the following tools wold help identify which ports are open on the remote file server?
A. Dig
B. Nmap
C. Tracert
D. nslookup
Answer: (SHOW ANSWER)
Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.
* Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.
* Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.
* Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.
* Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.
* Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

NEW QUESTION: 134
Users are reporting latency on the network. The network engineer notes the following:
Confirms the only change was a new network switch

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

NEW QUESTION: 135
A technician needs to set up a wireless connection that utilizes MIMO on non-overlapping channels. Which of the following would be the best choice?
A. 802.11a
B. 802.11b
C. 802.11g
D. 802.11n
Answer: (SHOW ANSWER)
The 802.11n standard supports MIMO (Multiple Input Multiple Output), which allows multiple antennas to increase data throughput and improve reliability. Additionally, it uses non-overlapping channels in the 5 GHz band (and optionally the 2.4 GHz band), making it a good choice for high-speed, interference-resistant wireless connections. (Reference: CompTIA Network+ Study Guide, Chapter on Wireless Technologies)

NEW QUESTION: 136
Which of the following allows a user to authenticate to multiple resources without requiring additional passwords?
A. SSO
B. MFA
C. SAML
D. RADIUS
Answer: (SHOW ANSWER)
The correct answer is SSO (Single Sign-On) because it enables a user to authenticate once and gain access to multiple systems or resources without being prompted to log in again. According to CompTIA Network+ (N10-009) security objectives, SSO improves usability and productivity while maintaining centralized authentication control. After the initial authentication, a trust relationship between systems allows the user to access additional applications seamlessly.
MFA (Multi-Factor Authentication) enhances security by requiring two or more authentication factors (something you know, have, or are), but it does not inherently provide access to multiple systems without repeated authentication events.

SAML (Security Assertion Markup Language) is an authentication and authorization protocol commonly used to implement SSO in web-based environments. While SAML supports SSO functionality, it is the underlying protocol rather than the access method itself.
RADIUS is a centralized authentication, authorization, and accounting (AAA) protocol used for network access control but does not specifically provide seamless multi-resource authentication without additional logins.
Therefore, SSO best describes authentication to multiple resources without requiring additional passwords.

NEW QUESTION: 137
A university is implementing a new campus wireless network. A network administrator needs to configure the network to support a large number of devices and high-bandwidth demands from students.
Which of the following wireless technologies should the administrator consider for this scenario?
A. Bluetooth
B. Wi-Fi 6E
C. 5G
D. LTE
Answer: (SHOW ANSWER)
Wi-Fi 6E is the best choice for high-density environments, such as a university campus. It:
Supports more devices with OFDMA (Orthogonal Frequency-Division Multiple Access) Uses the 6GHz band, reducing congestion Provides faster speeds and lower latency This makes Wi-Fi 6E ideal for large networks with high-bandwidth demands, like those in a university setting.
Breakdown of Options:
A). Bluetooth - Used for short-range, low-power connections, not large-scale wireless networks.
B). Wi-Fi 6E - # Correct answer. Designed for high-density environments, improving speed and efficiency.
C). 5G - Used for mobile networks, but not ideal for campus-wide local wireless infrastructure.
D). LTE - Used for cellular data, not for campus-wide Wi-Fi.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Compare and contrast wireless networking technologies.
IEEE 802.11ax (Wi-Fi 6E): Enhancements for high-efficiency wireless networking

NEW QUESTION: 138
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: 139
During a VoIP call, a user notices inconsistent audio and logs an incident ticket. A network administrator notices inconsistent delays in arrival of the RTP packets. Which of the following troubleshooting tools should the network administrator use to determine the issue?
A. Toner and probe
B. Protocol analyzer
C. Cable tester
D. Spectrum reader
Answer: (SHOW ANSWER)
Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.
A). Toner and probe locates cable runs, not packet analysis.
C). Cable tester checks wiring faults, not packet timing.
D). Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Protocol analyzers, VoIP troubleshooting, jitter analysis.

NEW QUESTION: 140
Which of the following is created to illustrate the effectiveness of wireless networking coverage in a building?

A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map
Answer: (SHOW ANSWER)
* Definition of Heat Maps:
* A heat map is a graphical representation of data where individual values are represented by colors. In the context of wireless networking, a heat map shows the wireless signal strength in different areas of a building.
* Purpose of a Heat Map:
* Heat maps are used to illustrate the effectiveness of wireless networking coverage, identify dead zones, and optimize the placement of access points (APs) to ensure adequate coverage and performance.
* Comparison with Other Options:
* Logical Diagram: Represents the logical connections and relationships within the network.
* Layer 3 Network Diagram: Focuses on the routing and IP addressing within the network.
* Service-Level Agreement (SLA): A contract that specifies the expected service levels between a service provider and a customer.
* Creation and Use:

* Heat maps are created using specialized software or tools that measure wireless signal strength throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
References:
* CompTIA Network+ certification materials and wireless network planning guides.

NEW QUESTION: 141
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: 142
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: 143
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: 144
A network administrator receives complaints of intermittent network connectivity issues. The administrator investigates and finds that the network design contains potential loop scenarios. Which of the following should the administrator do?
A. Enable spanning tree
B. Configure port security
C. Change switchport speed limits
D. Enforce 802.1Q tagging
Answer: (SHOW ANSWER)
Spanning Tree Protocol (STP) is designed to detect and prevent Layer 2 loops by blocking redundant paths. If loops are possible in the design, enabling STP ensures network stability.
B). Port security controls endpoint MAC addresses, not loops.
C). Speed limits address bandwidth, not loop prevention.
D). 802.1Q tagging allows VLAN separation but does not resolve loops.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Loop prevention, spanning tree, switch design.

NEW QUESTION: 145
Which of the following is the final step in the ticket management process?
A. Escalating to senior management
B. Performing functional and non-functional testing
C. Documenting findings, outcomes, and lessons learned
D. Establishing a detailed action plan
Answer: (SHOW ANSWER)
The correct answer is Documenting findings, outcomes, and lessons learned because proper documentation and closure are the final steps in the ticket management and troubleshooting process. According to CompTIA Network+ (N10-009) objectives under network operations and troubleshooting methodology, once an issue is resolved, technicians must verify full system functionality, implement preventive measures if needed, and document the entire process before closing the ticket.
Documentation ensures that all relevant information-such as the root cause, corrective actions taken, configuration changes made, and lessons learned-is recorded for future reference. This supports knowledge base updates, trend analysis, compliance requirements, and improved response times for similar incidents.

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

NEW QUESTION: 146
Users report latency with a SaaS application. Which of the following should a technician adjust to fix the issue?
A. Server hardware specifications
B. Data-at-rest encryption settings
C. Network bandwidth and utilization
D. Virtual machine configurations
Answer: (SHOW ANSWER)
The correct answer is Network bandwidth and utilization because latency issues with a SaaS (Software as a Service) application are most commonly related to network performance constraints, not local server hardware or virtualization settings. According to CompTIA Network+ (N10-009) troubleshooting objectives, technicians should evaluate bandwidth capacity, throughput, congestion, packet loss, and overall utilization when diagnosing performance issues affecting cloud-based applications.
Since SaaS applications are hosted externally by a service provider, the organization typically does not control the underlying server hardware or virtual machine configurations (Options A and D). Therefore, adjusting internal server specifications would not resolve user-side latency.
Option B, data-at-rest encryption, applies to stored data security and does not impact real-time application responsiveness.
High network utilization, insufficient bandwidth, QoS misconfiguration, or WAN congestion can significantly increase latency. Technicians should review network monitoring tools, check interface statistics, analyze traffic patterns, and verify Quality of Service (QoS) policies to ensure SaaS traffic is prioritized appropriately.
Thus, optimizing bandwidth and reducing network congestion is the most appropriate corrective action.

NEW QUESTION: 147
After providing a username and password, a user must input a passcode from a phone application. Which of the following authentication technologies is used in this example?
A. SSO
B. LDAP
C. MFA
D. SAML
Answer: (SHOW ANSWER)
This is an example of Multi-Factor Authentication (MFA) because it requires:
Something you know (username/password)
Something you have (a phone-generated passcode)
Breakdown of Options:
A: SSO (Single Sign-On) - Allows one login for multiple services, but does not add a second authentication factor.
B: LDAP (Lightweight Directory Access Protocol) - Used for directory authentication, not MFA.
C: MFA (Multi-Factor Authentication) - # Correct answer. Uses multiple authentication factors for better security.
D: SAML (Security Assertion Markup Language) - Used for federated identity management, not multi-factor authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement authentication and authorization methods.

NEW QUESTION: 148

A network administrator is in the process of installing 35 PoE security cameras. After the administrator installed and tested the new cables, the administrator installed the cameras. However, a small number of the cameras do not work. Which of the following is the most reason?

A. Incorrect wiring standard

B. Power budget exceeded

C. Signal attenuation

D. Wrong voltage

Answer: (SHOW ANSWER)

When installing multiple Power over Ethernet (PoE) devices like security cameras, it is crucial to ensure that the total power requirement does not exceed the power budget of the PoE switch. Each PoE switch has a maximum power capacity, and exceeding this capacity can cause some devices to fail to receive power.

* PoE Standards: PoE switches conform to standards such as IEEE 802.3af (PoE) and 802.3at (PoE+), each with specific power limits per port and total power capacity.
* Power Calculation: Adding up the power requirements of all connected PoE devices can help determine if the total power budget of the switch is exceeded.
* Symptoms: When the power budget is exceeded, some devices, typically those farthest from the switch or connected last, may not power up or function correctly.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Covers PoE standards and troubleshooting power issues.
* Cisco Networking Academy: Discusses PoE technologies, power budgeting, and managing PoE devices.
* Network+ Certification All-in-One Exam Guide: Provides information on PoE setup, including power budget considerations.

NEW QUESTION: 149

Which of the following would describe a data recovery goal?

A. MTBF

B. RPO

C. BCP

D. MTTR

Answer: (SHOW ANSWER)

RPO (Recovery Point Objective) describes a data recovery goal by defining the maximum acceptable amount of data loss measured in time. For example, an RPO of 4 hours means the organization must be able to restore data to a point no more than four hours before the outage-so backups, replication, or snapshots must occur frequently enough to meet that target. In Network+ (N10-009) operations objectives, disaster recovery and business continuity concepts include understanding recovery metrics and how they influence backup strategies, replication design, and service resilience planning. RPO specifically answers: "How much data can we afford to lose?" By contrast, MTBF (Mean Time Between Failures) is a reliability metric describing how often failures occur.

MTTR (Mean Time To Repair/Recover) measures how long it takes to restore a system after failure, which is more aligned with service restoration time rather than data loss. BCP (Business Continuity Plan) is the overall plan/process for keeping critical business functions running during disruptions; it is not a single data recovery metric. Therefore, RPO is the correct term for a data recovery goal.

NEW QUESTION: 150

An organization is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that allows for continuous connectivity anywhere in the facility. Which of the following should the network administrator suggest to ensure the best coverage?

A. Implementing additional ad hoc access points

B. Providing more Ethernet drops for user connections

C. Deploying a mesh network in the building

D. Changing the current frequency of the Wi-Fi

Answer: (SHOW ANSWER)
The correct answer is deploying a mesh network. A mesh wireless network uses multiple interconnected access points that automatically route traffic through the best available path. This ensures seamless coverage throughout a facility, even when users move between APs. Mesh APs can extend coverage without requiring each AP to be directly wired, making them ideal for large or hard-to-wire environments.
A). Ad hoc access points are peer-to-peer connections and cannot provide enterprise-grade continuous coverage.
B). Ethernet drops provide wired connectivity but do not solve wireless coverage issues.
D). Changing the frequency (from 2.4 GHz to 5 GHz or vice versa) may reduce interference but will not guarantee building-wide seamless connectivity.
Mesh networks are particularly effective in environments with roaming devices (smartphones, tablets, handheld scanners) and ensure that there are no dead spots, thereby delivering continuous wireless access.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Wireless architectures, mesh networking, seamless connectivity.

NEW QUESTION: 151
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: 152
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: 153
Which of the following protocols has a default administrative distance value of 90?
A. RIP
B. EIGRP
C. OSPF
D. BGP
Answer: (SHOW ANSWER)
EIGRP (Enhanced Interior Gateway Routing Protocol) has a default administrative distance (AD) value of 90 for internal routes. The administrative distance is used to rate the trustworthiness of routing information received from different routing protocols. EIGRP, developed by Cisco, has an AD of 90, which is lower than that of RIP (120) and OSPF (110), making it more preferred if multiple protocols provide a route to the same destination.References:CompTIA Network+ study materials.

NEW QUESTION: 154
A network administrator needs to add 255 useable IP addresses to the network. A /24 is currently in use.
Which of the following prefixes would fulfill this need?
A. /23
B. /25
C. /29
D. /32
Answer: (SHOW ANSWER)
A /23 subnet provides 512 total addresses, of which 510 are usable (subtracting 2 for network and broadcast addresses). This would satisfy the need for 255 additional addresses.

NEW QUESTION: 155
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: 156
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: 157
A technician is troubleshooting a computer issue for a user who works in a new annex of an office building.
The user is reporting slow speeds and intermittent connectivity. The computer is connected via a Cat 6 cable to a distribution switch that is 492ft (150m) away. Which of the following should the technician implement to correct the issue?
A. Increase the bandwidth allocation to the computer.
B. Install an access switch in the annex and run fiber to the distribution switch.
C. Run a Cat 7 cable from the computer to the distribution switch.
D. Enable the computer to support jumbo frames.
Answer: (SHOW ANSWER)
The maximum recommended length for Ethernet cable runs is 100 meters (328 feet). At 150 meters, the Cat 6 cable is too long, causing signal degradation and connectivity issues. Running fiber from the distribution switch to an access switch in the annex will allow for reliable connectivity over longer distances, as fiber can cover greater distances without signal loss.
(Reference: CompTIA Network+ Study Guide, Chapter on Network Cable Standards)

NEW QUESTION: 158
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: 159
A network engineer configures the network settings in a new server as follows:
IP address = 192.163.1.15
Subnet mask = 255.255.255.0
Gateway = 192.163.1.255
The server can reach other hosts on the same subnet successfully, but it cannot reach hosts on different subnets. Which of the following is most likely configured incorrectly?
A. Subnet mask
B. Gateway
C. Default route
D. IP address
Answer: (SHOW ANSWER)
The default gateway for a network should be an IP address within the subnet, but not the broadcast address. In this case:
IP: 192.163.1.15
Subnet Mask: 255.255.255.0
This means the network range is: 192.163.1.0 - 192.163.1.255
192.163.1.255 is the broadcast address for this subnet, so it cannot be used as a gateway.
Hence, the device fails to communicate outside its subnet because it's trying to use a broadcast address as its gateway.
The issue is clearly with the gateway configuration.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 1.4: "Given a scenario, configure and deploy common Ethernet switching features."

NEW QUESTION: 160
A network administrator needs to connect a multimode fiber cable from the MDF to the server room. The administrator connects the cable to Switch 2, but there is no link light. The administrator tests the fiber and finds it does not have any issues. Swapping the connection to Switch 1 in a working port is successful, but the swapped connection does not work on Switch 2. Which of the following should the administrator verify next?

A. Fiber length
B. Transceiver model
C. Connector type
D. Port speed
Answer: (SHOW ANSWER)
The most probable issue is with thetransceiver model. Not all transceivers are compatible with multimode fiber, and the specific type (e.g., SFP, SFP+) and its wavelength must match the fiber cable type. If a port works on one switch but not the other with the same cable, this is a strong indicator of incompatible or faulty transceiver hardware.
Reference:Section 1.5 - Transmission Media and Transceivers - "Transceivers and Compatibility"

NEW QUESTION: 161
Which of the following services runs on port 636?
A. SMTP
B. Syslog
C. TFTP
D. LDAPS
Answer: (SHOW ANSWER)

LDAP over SSL (LDAPS) uses port 636 to provide secure, encrypted authentication for directory services.
Breakdown of Options:
A). SMTP (Simple Mail Transfer Protocol) - Uses port 25, not 636.
B). Syslog - Uses port 514 (UDP), not 636.
C). TFTP (Trivial File Transfer Protocol) - Uses port 69 (UDP), not 636.
D). LDAPS (Lightweight Directory Access Protocol Secure) - # Correct answer. Uses port 636 for secure directory authentication.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.
RFC 4511: Lightweight Directory Access Protocol (LDAP)

NEW QUESTION: 162
Which of the following protocol ports should be used to securely transfer a file?
A. 22
B. 69
C. 80
D. 3389
Answer: (SHOW ANSWER)
Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.
*Why not the other options?
*Port 69 (B) - TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).
*Port 80 (C) - HTTP: Used for web traffic, not for file transfer.
*Port 3389 (D) - RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 5: Network Protocols and Ports

NEW QUESTION: 163
After a recent merger, a large number of alerts are coming in regarding extremely high utilization. Which of the following should be generated to help inform new alerting requirements?
A. SLA
B. Network diagram
C. Baseline
D. Heat map
Answer: (SHOW ANSWER)
A baseline establishes normal performance levels for network utilization, latency, jitter, and other metrics.
After a merger, traffic patterns change, so a new baseline is needed to recalibrate monitoring thresholds and avoid excessive false alerts.
A). SLA defines performance agreements with customers but doesn't adjust alerting.
B). Network diagrams show topology, not traffic norms.
D). Heat maps show wireless coverage, not utilization baselines.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Baselines, monitoring, alerting, performance tuning.

NEW QUESTION: 164
A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?
A. APIPA
B. Multicast
C. Class C
D. Experimental
Answer: (SHOW ANSWER)
APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:
"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

NEW QUESTION: 165
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: 166
Which of the following concepts describes the idea of housing different customers in the same public cloud data center?
A. Elasticity
B. Hybrid cloud
C. Scalability
D. Multitenancy
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
Multitenancy is a cloud concept where multiple customers share the same physical resources (servers, storage, and networks) but remain logically separated for security and privacy.
A). Elasticity is auto-scaling resources.
B). Hybrid cloud combines private and public resources.
C). Scalability is the ability to grow resources but doesn't imply multiple customers.

References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing models, multitenancy in public cloud.

NEW QUESTION: 167
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: 168
A company's VoIP phone connection is cutting in and out. A senior network engineer is recommending the implementation of a voice VLAN. Which of the following should be configured?
A. 802.1Q tagging
B. Jumbo frames
C. Native VLAN
D. Link aggregation
Answer: (SHOW ANSWER)
Voice VLANs rely on 802.1Q tagging to separate voice traffic from data traffic on the same physical link.
This separation allows QoS policies to prioritize VoIP, reducing jitter and packet loss.
B). Jumbo frames improve throughput for large data transfers, not voice.
C). Native VLAN is the untagged VLAN, not specifically for voice.
D). Link aggregation bundles links for bandwidth/redundancy, not QoS.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - VLANs, voice VLANs, 802.1Q tagging, QoS.

NEW QUESTION: 169
A company recently experienced outages of one of its critical, customer-facing applications. The root cause was an overutilized network router, but the Chief Technology Officer is concerned that the support staff was unaware of the issue until notified by customers. Which of the following is the best way to address this issue in the future?
A. Packet capture
B. SNMP

C. Syslog collector
D. SIEM
Answer: (SHOW ANSWER)
The best answer is SNMP (Simple Network Management Protocol). SNMP enables monitoring of network devices (routers, switches, firewalls, servers) and provides performance data such as CPU usage, bandwidth utilization, and interface status. In this scenario, if SNMP monitoring had been in place, administrators would have received alerts that the router was overutilized before customers noticed outages.
A). Packet capture (e.g., Wireshark) is useful for deep troubleshooting but is reactive, not proactive, and not scalable for continuous monitoring.
C). Syslog collects log messages but generally does not provide proactive resource utilization metrics. It is complementary but not the best fit for this problem.
D). SIEM aggregates logs and security events for analysis, but the primary requirement here is performance and availability monitoring.
By implementing SNMP monitoring (and potentially integrating it with a network monitoring tool such as Nagios, PRTG, or SolarWinds), the organization can track utilization trends, set thresholds, and automatically generate alerts, thereby preventing downtime from going unnoticed.
References (CompTIA Network+ N10-009):
Domain: Network Operations - SNMP monitoring, proactive network performance management.

NEW QUESTION: 170
Which of the following disaster recovery metrics is used to describe the amount of data that is lost since the last backup?

A. MTTR
B. RTO
C. RPO
D. MTBF
Answer: (SHOW ANSWER)
* Definition of RPO:
* Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.
* For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.
* Why RPO is Important:
* RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.
* Comparison with Other Metrics:
* MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.
* RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.
* MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.
* How RPO is Used in Disaster Recovery:
* Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.
References:
* CompTIA Network+ study materials and certification guides.

NEW QUESTION: 171
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: 172
A media company is implementing a global streaming service. Which of the following should the company apply to each regional point of presence in order to comply with local laws?
A. ACL
B. Port security
C. Key management
D. Content filtering
Answer: (SHOW ANSWER)
For a global streaming service, different countries and regions often have specific legal requirements about what content can be accessed (for example, age restrictions, prohibited material, censorship rules, or licensing constraints). To comply with these local laws at each regional point of presence (PoP), the company should implement content filtering. In Network + security objectives, content filtering is a control used to allow, block, or restrict access to specific categories of content, URLs, applications, or media based on policy.
Applied regionally, it supports geo-policy enforcement by ensuring that users served by a given PoP receive only content permitted in that jurisdiction.
An ACL primarily controls network traffic flows (permit/deny based on IPs, ports, and protocols). While ACLs can help block certain services, they are not designed to classify and regulate streaming media content in a way that aligns with legal content rules. Port security is a switch feature to restrict which devices can connect to a port (MAC-based controls) and is unrelated to regional compliance for streamed media. Key management concerns encryption key handling and protects confidentiality/integrity, but it does not determine which content is allowed in a region. Therefore, regional content filtering is the best match for meeting local legal requirements.

NEW QUESTION: 173
A network engineer configures an application server so that it automatically adjusts resource allocation as demand changes. This server will host a new application and demand is not predictable. Which of the following concepts does this scenario demonstrate?
A. Scalability
B. Software as a Service
C. Hybrid cloud
D. Elasticity
Answer: (SHOW ANSWER)
Elasticity is the ability of a system (often in cloud environments) to automatically scale resources up or down in real time based on demand.
A). Scalability means the ability to grow over time but not necessarily dynamically.
B). SaaS is a service model, not a resource-allocation concept.
C). Hybrid cloud is a deployment model, not a performance behavior.

References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Cloud computing, elasticity vs. scalability.

NEW QUESTION: 174
A laptop user gets an error when trying to access the company ' s intranet site. A technician runs ipconfig /all with the following results:
Autoconfiguration IPv4 Address: 169.254.0.5 (Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCP Server . . . . . :
Which of the following is most likely causing the issue?
A. Short DHCP lease duration
B. IIS server malfunction
C. Address pool exhaustion
D. IDS misconfiguration
Answer: (SHOW ANSWER)
The giveaway here is the 169.254.x.x address. That is an APIPA address, which Windows assigns to itself when it asks for an IP address from DHCP and does not get one. Since there is also no default gateway and no DHCP server listed, the laptop clearly failed to obtain normal network settings.
Out of the choices, address pool exhaustion makes the most sense. If the DHCP scope has run out of available addresses, the client cannot lease one, so it falls back to an automatic private address. At that point, the device may still think its network adapter is working, but it will not be able to reach internal resources like the company intranet because it does not have valid Layer 3 settings for that network.
The other answers do not fit the output. A short lease duration could cause frequent renewals, but it would not normally explain an APIPA address by itself. An IIS problem would affect the web server, not the client's local IP configuration. An IDS issue also would not cause the workstation to self-assign 169.254.0.5. This is a DHCP addressing problem, and the best answer is C .

NEW QUESTION: 175
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: 176
A network technician is configuring the company's network of 100 Mbps Layer 2 switches. The technician wants increased throughput for the uplinks between switches. The technician connects multiple redundant links between the switches. Which of the following should the technician configure?
A. Spanning Tree Protocol
B. Switch Virtual Interfaces
C. Native VLAN

D. First Hop Redundancy Protocol
Answer: (SHOW ANSWER)
When multiple redundant links exist between switches, Spanning Tree Protocol (STP) is required to prevent switching loops. STP blocks redundant paths but can allow aggregation if configured with protocols like LACP.
B). SVIs provide Layer 3 interfaces, not loop prevention.
C). Native VLAN defines the untagged VLAN but does not manage loops.
D). FHRP (VRRP, HSRP, GLBP) provides gateway redundancy, not switch uplink management.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - STP, redundancy, loop prevention.

NEW QUESTION: 177
A network administrator prepares a VLAN for a new office while planning for minimal IP address waste. The new office will have approximately 800 workstations. Which of the following network schemes meets the requirements?
A. 10.0.100.0/22
B. 172.16.8.0/23
C. 172.16.15.0/20
D. 192.168.4.0/21
Answer: (SHOW ANSWER)
To support about 800 workstations with minimal IP waste, you choose the smallest subnet that provides at least 800 usable host addresses. In IPv4, usable hosts per subnet are calculated as 2^(host bits) # 2 (subtracting network and broadcast addresses). A /22 leaves 10 host bits (32 # 22 = 10), providing 2^10 # 2 = 1024 # 2 = 1022 usable addresses-enough for 800 devices with relatively low waste.
Check the other options: /23 leaves 9 host bits, giving 2^9 # 2 = 512 # 2 = 510 usable addresses, which is not enough. A /21 provides 2^11 # 2 = 2048 # 2 = 2046 usable addresses-enough, but wastes more than /22. A
/20 provides 2^12 # 2 = 4096 # 2 = 4094 usable addresses-much more waste.
Therefore, 10.0.100.0/22 is the best choice that meets the workstation requirement while minimizing unused addresses.

NEW QUESTION: 178
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: 179
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: 180
A network administrator is migrating a domain to a different provider. As part of the onboarding process, the new provider requests domain ownership proof. Which of the following records would the administrator most likely need to create?
A. A
B. CNAME
C. PTR

D. TXT
Answer: (SHOW ANSWER)
The best answer is D. TXT . When a provider asks an administrator to prove ownership of a domain, the most common method is to have the administrator place a specific verification value inside a DNS TXT record .
The provider then checks public DNS for that value. If the expected text is present, it confirms that the person managing the migration has control over the domain's DNS settings.
This matches how TXT records are commonly used in real network environments. They are flexible and can store readable text strings for verification, policy, and security-related purposes. In Network+ study material, TXT records are frequently associated with things like domain validation and email-related configurations such as SPF and other verification mechanisms.
The other record types do not fit this task. An A record maps a hostname to an IPv4 address. A CNAME points one name to another name. A PTR record is used for reverse DNS, mapping an IP address back to a hostname. None of those are typically created just to prove domain ownership during provider onboarding.
The key clue is the phrase "domain ownership proof" , which strongly points to a TXT record .

NEW QUESTION: 181
A company has been added to an unapproved list because of spam. The network administrator confirmed that a workstation was infected by malware. Which of the following processes did the administrator use to identify the root cause?
A. Traffic analysis
B. Availability monitoring
C. Baseline metrics
D. Network discovery
Answer: (SHOW ANSWER)
Traffic analysis involves monitoring and inspecting network traffic flows to detect unusual patterns, such as a workstation sending large volumes of outbound SMTP (spam). This process enables identification of malware as the root cause.
B). Availability monitoring checks uptime but doesn't diagnose spam traffic.
C). Baseline metrics show normal usage but don't pinpoint infected hosts.
D). Network discovery identifies devices, not malicious traffic flows.
References (CompTIA Network+ N10-009):
Domain: Network Security - Traffic analysis, malware detection, identifying compromised hosts.

NEW QUESTION: 182
While troubleshooting connectivity issues, a junior network administrator is given explicit instructions to test the host's TCP/IP stack first. Which of the following commands should the network administrator run?
A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1

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

NEW QUESTION: 183
While deploying a new fleet of computers on a DHCP network, a network administrator notices that new computers cannot connect to the internet. Which of the following is most likely the problem?
A. Incorrect default gateway
B. Address pool exhaustion
C. Duplicate IP address
D. Incorrect subnet mask
Answer: B (LEAVE A REPLY)
The best answer is B. Address pool exhaustion . The key detail is that this started happening while deploying a new fleet of computers on a DHCP network . That strongly suggests the number of available leases in the DHCP scope has been used up. When no more addresses are available, new devices cannot obtain valid network settings and will fail to connect properly.
This is a common issue when many systems are added at once. Existing devices may already be consuming most or all of the available leases, and the new clients are left without an address assignment. Without a valid IP configuration from DHCP, the computers will not be able to reach the local network or the internet in the normal way.
The other choices are possible network problems in general, but they are less likely in this exact scenario. An incorrect default gateway or incorrect subnet mask would more often reflect a bad DHCP option or a misconfiguration affecting many clients in a different way. A duplicate IP address can affect connectivity, but it does not naturally match the clue about many new devices being added at once on a DHCP scope.
When a question combines DHCP, many new clients, and sudden inability for new systems to connect, address pool exhaustion is the most likely cause.

NEW QUESTION: 184
After a company installed a new IPS, the network is experiencing speed degradation. A network administrator is troubleshooting the issue and runs a speed test. The results from the different network locations are as follows:
LocationSpeed DownSpeed Up
Wireless laptop4.8 Mbps47.1 Mbps
Wired desktop5.2 Mbps49.3 Mbps
Firewall48.8 Mbps49.5 Mbps
Which of the following is the most likely issue?
A. Packet loss
B. Bottlenecking
C. Channel overlap
D. Network congestion
Answer: (SHOW ANSWER)
Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8 Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.

*Why not the other options?
*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.
*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.
*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

NEW QUESTION: 185
A company implements a new network utilizing only IPv6 addressing and needs to connect to the internet.
Which of the following must be enabled in order for the internal network to contact servers on the internet?
A. MPLS
B. NAT64
C. GRE
D. Static routing
Answer: (SHOW ANSWER)
The correct answer is B. NAT64 . This scenario says the internal network is using only IPv6 . In the real world, many internet services still rely on IPv4, so an IPv6-only client may need a translation mechanism to reach IPv4-based servers. That is exactly where NAT64 is used. It allows communication between IPv6-only clients and IPv4 resources by translating between the two protocols.
The other options do not solve that requirement. MPLS is used for traffic forwarding across provider networks and has nothing to do with IPv4/IPv6 protocol translation. GRE creates tunnels, but it does not automatically translate one IP version into another. Static routing can direct traffic, but it cannot make IPv6- only hosts speak to IPv4-only internet destinations.
From a Network+ perspective, this question is testing knowledge of IPv6 transition and interoperability mechanisms . If the network is entirely IPv6 internally, but still needs access to parts of the internet that may be IPv4, some translation service has to exist at the boundary. Among the choices given, NAT64 is the only technology that fits that role. That is why B is the best answer.

NEW QUESTION: 186
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: 187

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

A. Toner and probe

B. Cable tester

C. Visual fault locator

D. Network tap

Answer: (SHOW ANSWER)

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

NEW QUESTION: 188

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: 189

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: 190

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

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

NEW QUESTION: 191
A server administrator needs to add a record to the company's DNS server to verify ownership of a web domain. The administrator has the record's name and value. Which of the following record types should the administrator use to add the record to the DNS server?
A. TXT
B. A
C. PTR
D. CNAME
Answer: (SHOW ANSWER)
To verify ownership of a domain, providers commonly require adding a TXT record to DNS containing a specific validation token (a name/value pair). A TXT (text) record is designed to store arbitrary text data associated with a domain or hostname, which makes it ideal for domain verification workflows used by certificate authorities, email security (SPF/DKIM/DMARC-related entries), and third-party services that need proof of administrative control over DNS. This fits Network+ DNS objectives that cover common record types and their practical purposes in real deployments.

An A record maps a hostname to an IPv4 address and is used for name-to-address resolution, not ownership verification. A PTR record provides reverse DNS mapping (IP address to hostname) and is stored in reverse lookup zones, not typically used for validating web domain ownership. A CNAME record creates an alias from one hostname to another canonical hostname; while sometimes used in service integrations, the classic
"record name + token value" ownership verification is most directly and universally satisfied by a TXT record. Therefore, TXT is the correct choice given the requirement and the provided record name and value.

NEW QUESTION: 192
A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business.
When attempting to connect, two networks are listed as possible choices: SSID: business and SSID:
myaccess. Which of the following attacks is occurring?
A. On-path
B. Rogue AP
C. Evil twin
D. Tailgating
Answer: (SHOW ANSWER)
An evil twin attack occurs when an attacker creates a fraudulent AP with an SSID very similar (or identical) to the legitimate one. Users may accidentally connect, allowing the attacker to capture traffic and credentials.
A). On-path is the consequence of connecting to the evil twin, not the initial attack itself.
B). Rogue AP is any unauthorized access point, but the key here is the malicious mimicry of a legitimate SSID
- specifically an evil twin.
D). Tailgating is a physical social engineering attack, unrelated to Wi-Fi.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless threats (rogue APs, evil twins).

NEW QUESTION: 193
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: 194
A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?
A. Stronger wireless connection
B. Roaming between access points
C. Advanced security
D. Increased throughput
Answer: (SHOW ANSWER)
An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses.References:CompTIA Network+ study materials.

NEW QUESTION: 195
A network administrator is planning to host a company application in the cloud, making the application available for all internal and third-party users. Which of the following concepts describes this arrangement?
A. Multitenancy
B. VPC
C. NFV
D. SaaS
Answer: (SHOW ANSWER)
Multitenancy is a cloud computing architecture where a single instance of software serves multiple customers or tenants. Each tenant's data is isolated and remains invisible to other tenants. Hosting a company application in the cloud to be available for both internal and third-party users fits this concept, as it allows shared resources and infrastructure while maintaining data separation and security. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 196
A network administrator needs to deploy a subnet using an IP address range that can support at least 260 devices with the fewest wasted addresses. Which of the following subnets should the administrator use?
A. 172.16.0.0/24
B. 172.25.2.0/23
C. 172.30.1.0/22
D. 172.33.0.0/21
Answer: (SHOW ANSWER)
To support at least 260 hosts, you need at least 512 total IP addresses (accounting for network/broadcast overhead).

/23 (255.255.254.0) gives 510 usable IPs, ideal for 260 devices with minimal waste.
/24 (255.255.255.0) gives only 254 usable - not enough.
/22 (1022 usable) and /21 (2046 usable) would work but result in significant address waste.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.1 - Given a scenario, configure and apply IP addressing schemes.

NEW QUESTION: 197
A network administrator is conducting an assessment and finds network devices that do not meet standards.
Which of the following configurations is considered a set of rules that devices should adhere to?
A. Production
B. Backup
C. Candidate
D. Golden
Answer: (SHOW ANSWER)
The correct answer is golden configuration. This is a reference standard or baseline that defines the approved settings and rules devices should follow. Any deviation from the golden configuration indicates drift or misconfiguration that must be remediated.
A). Production refers to the live environment but doesn't define a standard.
B). Backup configurations are stored copies, not the standard rules.
C). Candidate configuration is a proposed change being tested, not the final baseline.
By enforcing golden configurations, administrators ensure compliance, maintain security standards, and improve consistency across the enterprise.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Configuration standards, golden images/configs.

NEW QUESTION: 198
Which of the following provides an opportunity for an on-path attack?
A. Phishing
B. Dumpster diving
C. Evil twin
D. Tailgating
Answer: (SHOW ANSWER)
An evil twin is a rogue Wi-Fi access point that mimics a legitimate network. Attackers use it to intercept and manipulate traffic, making it an on-path (formerly MITM) attack opportunity.
Breakdown of Options:
A: Phishing - Tries to steal credentials through fake emails/websites but does not intercept network traffic.
B: Dumpster diving - Involves physical security breaches, not network interception.
C: Evil twin - # Correct answer. A rogue Wi-Fi AP impersonates a real network, allowing traffic interception.

D: Tailgating - Involves physical access security, not network interception.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain common network security threats.

NEW QUESTION: 199
Which of the following steps in the troubleshooting methodology includes checking logs for recent changes?
A. Identify the problem.
B. Document the findings and outcomes.
C. Test the theory to determine cause.
D. Establish a plan of action.
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Troubleshooting section.

NEW QUESTION: 200
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: 201
A company has observed increased user traffic to gambling websites and wants to limit this behavior on work computers. Which of the following should the company most likely implement?
A. ACLs
B. Content filter
C. Port security
D. Screened subnet
Answer: (SHOW ANSWER)
A content filter blocks access to specific websites based on category, URL, or keywords. This is the best solution to restrict gambling websites.
Breakdown of Options:
A). ACLs - Control network access, not specific web content.
B). Content filter - # Correct answer. Used to block access to unwanted websites.
C). Port security - Prevents unauthorized device connections, not web traffic filtering.
D). Screened subnet - A DMZ isolates public-facing servers, not user restrictions.
Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Given a scenario, implement network security measures.

NEW QUESTION: 202
Which of the following uses the longest prefix match to determine an exit interface?
A. ARP table
B. MAC address table
C. Routing table
D. Netstat table
Answer: (SHOW ANSWER)
The longest prefix match is a routing concept used to find the most specific route to a destination IP address.
The routing table performs this calculation to determine the exit interface for a packet, ensuring the most accurate delivery. The document explains:
"Routers use the longest prefix match when searching the routing table to determine the best path for an IP packet. This ensures that the most specific (and thus optimal) route is chosen, based on the destination IP address."

NEW QUESTION: 203
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: 204
A technician is planning an equipment installation into a rack in a data center that practices hot aisle/cold aisle ventilation. Which of the following directions should the equipment exhaust face when installed in the rack?
A. Sides
B. Top
C. Front
D. Rear
Answer: (SHOW ANSWER)
In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

NEW QUESTION: 205
An ISP provided a company with a pre-configured modem and five public static IP addresses. Which of the following does the company's firewall require to access the internet? (Select TWO).

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

NEW QUESTION: 206
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: 207
A company experiences an incident involving a user who connects an unmanaged switch to the network.
Which of the following technologies should the company implement to help avoid similar incidents without conducting an asset inventory?
A. Screened subnet
B. 802.1X
C. MAC filtering
D. Port security
Answer: (SHOW ANSWER)

Port security is a Layer 2 security feature that restricts the number of devices connecting to a network switch port. It helps prevent unauthorized devices, such as an unmanaged switch, from being connected to the network.
How Port Security Works:
Limits the number of MAC addresses that can connect to a port.
Can shut down or restrict the port if an unauthorized device is detected.
Prevents users from plugging in unauthorized networking equipment (e.g., unmanaged switches, hubs).
Incorrect Options:
A). Screened Subnet: A screened subnet (DMZ) is used for isolating external-facing servers, not for controlling unauthorized network connections.
B). 802.1X: Provides authentication for devices but requires a RADIUS server, which is a more complex solution than port security.
C). MAC Filtering: Controls which MAC addresses can connect but is difficult to manage and can be spoofed.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Security Controls

NEW QUESTION: 208
An administrator is troubleshooting a Layer 3 communication issue between the web server and the database server. The administrator finds the following information:
Device
IP
Subnet
Gateway
Firewall
192.168.1.1
255.255.255.0
1.2.3.4
Web server
192.168.1.50
255.255.255.0
192.168.1.1
Database server
192.168.1.201
255.255.255.128
192.168.1.1
Which of the following corrects the communication issue?
A. Changing the subnet on the database server to 255.255.255.0
B. Changing the subnet on the firewall to 255.255.255.128
C. Changing the default gateway on the database server to 1.2.3.4
D. Changing the IP address on the database server to 192.168.1.150
E. Changing the gateway on the firewall to 192.168.1.1
Answer: (SHOW ANSWER)
The problem is a subnet mismatch . The web server is using 255.255.255.0 , which places it in the
192.168.1.0/24 network. The database server is using 255.255.255.128 , which places 192.168.1.201 in the
192.168.1.128/25 network. So even though both addresses begin with 192.168.1, the two systems are not treating the network boundaries the same way.

That creates a Layer 3 communication issue because one host may believe the other device is local while the other host may treat traffic differently based on its smaller subnet. In a normal server segment like this, both systems should agree on the same mask if they are intended to be on the same network.
Changing the database server's subnet mask to 255.255.255.0 fixes that inconsistency immediately. Then both servers and the firewall interface are using the same local network definition, and traffic can be handled properly.
The other options do not solve the real issue. Changing the firewall to /25 would break consistency for the rest of the segment. Pointing the database server to 1.2.3.4 is incorrect because that is outside the local subnet and appears to be an upstream route. Changing the IP to 192.168.1.150 still leaves the wrong mask in place. The clean fix is A .

NEW QUESTION: 209
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: 210
An organization has a security requirement that all network connections can be traced back to a user. A network administrator needs to identify a solution to implement on the wireless network. Which of the following is the best solution?

A. Implementingenterprise authentication
B. Requiring theuse of PSKs
C. Configuring acaptive portal for users
D. Enforcing wired equivalent protection
Answer: (SHOW ANSWER)
Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual accountability. Captive portals can identify users but are less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.
Reference:
CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

NEW QUESTION: 211

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

NEW QUESTION: 212
As part of a recovery strategy, a network administrator needs to make sure no more than eight hours of data loss occurs. Which of the following DR metrics describes this requirement?
A. RPO
B. MTTR
C. RTO
D. MTBF
Answer: (SHOW ANSWER)
Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. If leadership states "no more than eight hours of data loss," they are describing how far back the organization is willing to roll data after an outage or disaster-meaning backups, replication, snapshots, or journaling must ensure recoverable data is no older than eight hours. In Network+ terms, this is a core availability and resiliency planning concept: you choose an RPO based on business impact, then implement backup frequency /replication strategy to meet it. By contrast, Recovery Time Objective (RTO) is about how quickly services must be restored (downtime duration), not how much data can be lost. MTTR (Mean Time to Repair/Recover) is an operational reliability metric describing typical time to restore a system, and MTBF (Mean Time Between Failures) indicates expected time between failures-neither directly states acceptable data loss.
Therefore, the metric matching "eight hours of data loss" is RPO.

NEW QUESTION: 213
A user called the help desk after business hours to complain that files on a device are inaccessible and the wallpaper was changed. The network administrator thinks that this issue is an isolated incident, but the security analyst thinks the issue might be a ransomware attack. Which of the following troubleshooting steps should be taken first?

A. Identify the problem
B. Establish a theory
C. Document findings
D. Create a plan of action
Answer: (SHOW ANSWER)
The first step in any troubleshooting process is to identify the problem. This includes gathering information from the user, reviewing logs, and observing the symptoms. In this case, identifying the scope and nature of the issue (e.g., signs of ransomware) is critical before forming any theories or plans.
From Andrew Ramdayal's guide:
"The troubleshooting methodology begins with identifying the problem. This step involves questioning users, identifying user changes, and determining the symptoms."

NEW QUESTION: 214
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: 215
A company is concerned that the public can use network wall jacks in publicly available conference rooms to access company servers. Which of the following is the best way to mitigate the vulnerability?
A. Create a trusted zone.
B. Disable unused services.
C. Use MAC filtering.
D. Implement 802.1X.
Answer: (SHOW ANSWER)
The best mitigation is implementing 802.1X, which provides port-based Network Access Control (NAC).
With 802.1X enabled on access switch ports, a device plugged into a wall jack cannot gain normal network access until it successfully authenticates using credentials/certificates via an authentication server (commonly RADIUS). This directly addresses the threat of unauthorized users plugging into publicly accessible conference room jacks, because the switch keeps the port in an unauthenticated state (or places it into a restricted/guest VLAN) until authentication succeeds. This aligns with Network+ security objectives that emphasize controlling access at the edge, enforcing authentication, and reducing the risk of rogue or unmanaged devices on internal networks.
MAC filtering is weaker because MAC addresses can be spoofed and managing allow-lists at scale is error- prone. Creating a trusted zone is vague and does not prevent initial port access; segmentation helps limit blast radius but doesn't enforce authentication at the jack. Disabling unused services is a general hardening practice, but it does not stop someone from connecting physically to an active switch port and attempting access. 802.1X is purpose-built for this exact scenario.

NEW QUESTION: 216
A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?
A. tcpdump
B. dig
C. tracert
D. arp
Answer: (SHOW ANSWER)
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.References: CompTIA Network+ study materials and common network troubleshooting commands.

NEW QUESTION: 217
An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?
A. SD-WAN
B. VXLAN
C. VPN
D. NFV
Answer: (SHOW ANSWER)
* Definition of SD-WAN:
* Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.
* Benefits of SD-WAN:
* Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
* Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
* Scalability: Easily scales to accommodate additional sites and bandwidth requirements.
* Comparison with Other Technologies:
* VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.
* VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.
* NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.
* Implementation:
* SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.
References:
* CompTIA Network+ course materials and networking solution guides.

NEW QUESTION: 218
Which of the following is used to redistribute traffic between one source and multiple servers that run the same service?
A. Router
B. Switch

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

NEW QUESTION: 219
Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed.
Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?
A. WPS configuration
B. Signal strength
C. Channel frequency
D. Power budget
Answer: (SHOW ANSWER)
When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.
A). WPS applies to Wi-Fi, not cellular repeaters.
C). Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.
D). Power budget applies to PoE and wired devices, not mobile phones.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

NEW QUESTION: 220
Which of the following network traffic type is sent to all nodes on the network?
A. Unicast
B. Broadcast
C. Multicast
D. Anycast
Answer: (SHOW ANSWER)
Broadcast traffic is sent to all nodes on the network. In a broadcast, a single packet is transmitted to all devices in the network segment. This is commonly used for tasks like ARP (Address Resolution Protocol) requests.
* Broadcast Domain: All devices within the same broadcast domain will receive broadcast traffic.
* Network Types: Ethernet networks commonly use broadcast traffic for certain functions, including network discovery and addressing.
* IPv4 Broadcast: An IPv4 broadcast address (e.g., 255.255.255.255) ensures the packet is sent to all devices on the network.

Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains network traffic types, including broadcast, unicast, and multicast.
* Cisco Networking Academy: Provides training on network communication methods and traffic types.
* Network+ Certification All-in-One Exam Guide: Discusses different types of network traffic and their uses in various network scenarios.
Broadcast traffic is essential for network operations that require communication with all nodes, such as ARP requests or DHCP discovery messages.

NEW QUESTION: 221
Which of the following objectives does an evil twin achieve?
A. DNS poisoning
B. Login credentials
C. ARP spoofing
D. Denial of service
Answer: (SHOW ANSWER)
An evil twin attack is when an attacker sets up a rogue access point (AP) with the same SSID as a legitimate one to trick users into connecting. Once users connect, attackers often present fake login pages or capture unencrypted session data to steal login credentials.
A). DNS poisoning manipulates DNS resolution but is not inherent to evil twin.
C). ARP spoofing is a Layer 2 attack involving MAC/IP mapping manipulation.
D). Denial of service can be a side effect but is not the primary objective of evil twin attacks.
The main purpose of an evil twin is credential theft, enabling further unauthorized access to networks or systems.
References (CompTIA Network+ N10-009):
Domain: Network Security - Wireless attacks, rogue APs, evil twins.

NEW QUESTION: 222
A company wants to implement a disaster recovery site or non-critical applicance, which can tolerance a short period of downltime. Which of the followig type of sites should the company impelement to achive this goal?
A. Hot
B. Cold
C. Warm
D. Passive
Answer: (SHOW ANSWER)
A warm site is a compromise between a hot site and a cold site, providing a balance between cost and recovery time. It is partially equipped with the necessary hardware, software, and infrastructure, allowing for a quicker recovery compared to a cold site but at a lower cost than a hot site.
* Recovery Time: Warm sites can be operational within hours to a day, making them suitable for non- critical applications that can tolerate short downtimes.
* Cost-Effectiveness: Warm sites are more economical than hot sites as they do not require all systems to be fully operational at all times.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses disaster recovery strategies and the different types of recovery sites.
* Cisco Networking Academy: Provides training on disaster recovery planning and site selection.
* Network+ Certification All-in-One Exam Guide: Explains the characteristics of hot, warm, and cold sites and their use cases in disaster recovery planning.
Warm sites offer a practical solution for maintaining business continuity for non-critical applications, balancing the need for availability with cost considerations.

NEW QUESTION: 223

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: 224

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: 225

A network administrator is troubleshooting a connection issue and needs to determine the path that a packet will take. Which of the following commands accomplishes this task?

A. netstat

B. traceroute

C. ping

D. nslookup

E. ipconfig

Answer: B (LEAVE A REPLY)

The correct answer is traceroute, which is the diagnostic command specifically designed to determine the path a packet takes across a network. According to the CompTIA Network+ N10-009 objectives, traceroute is a key network troubleshooting tool used to identify routing paths, hop counts, and points of latency or failure between a source and a destination.

Traceroute works by sending packets with incrementally increasing Time to Live (TTL) values. Each router along the path decrements the TTL by one, and when it reaches zero, the router returns an ICMP Time Exceeded message. This process allows the administrator to see each intermediate hop, its response time, and where packets may be delayed or dropped. The other options do not fulfill this purpose. Ping only verifies basic connectivity and round-trip time but does not show the route taken. Netstat displays active connections, ports, and routing tables but does not trace packet paths. Nslookup is used to resolve DNS names to IP addresses, and ipconfig displays local network configuration information.
The Network+ objectives emphasize traceroute (or tracert on Windows systems) as the primary tool for diagnosing routing issues, asymmetric paths, and network congestion, making it the correct and most appropriate choice in this scenario.

NEW QUESTION: 226
A newly opened retail shop uses a combination of new tablets, PCs, printers, and legacy card readers. Which of the following wireless encryption types is the most secure and compatible?
A. WPA3
B. WPA2
C. WPA2/WPA3 mixed mode
D. WPA/WPA2 mixed mode
Answer: (SHOW ANSWER)
WPA2/WPA3 mixed mode provides compatibility for older devices (that only support WPA2) while allowing newer devices to take advantage of stronger WPA3 encryption. This ensures maximum compatibility and security in a mixed-device environment.
A). WPA3 only is most secure but not compatible with legacy devices.
B). WPA2 only is secure but does not future-proof against WPA3-capable devices.
D). WPA/WPA2 mixed mode is weaker due to WPA (deprecated, insecure).
References (CompTIA Network+ N10-009):
Domain: Network Security - Wi-Fi encryption standards, WPA2 vs WPA3, mixed-mode compatibility.

NEW QUESTION: 227
A user connects to a corporate VPN via a web browser and is able to use TLS to access the internal financial system to input a time card. Which of the following best describes how the VPN is being used?
A. Clientless
B. Client-to-site
C. Full tunnel
D. Site-to-site
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

NEW QUESTION: 228
A network administrator is extending a network beyond the primary equipment location. Which of the following is where the administrator should install additional network switches?

A. MDF
B. VPC
C. VXLAN
D. IDF
Answer: (SHOW ANSWER)
When extending a network beyond the primary equipment location, additional access/distribution switches are typically placed in an IDF (Intermediate Distribution Frame). Network+ (N10-009) infrastructure objectives differentiate between the MDF and IDF: the MDF is the main, central wiring/equipment location (often where core switches, routers, WAN demarcation, and main cross-connects reside). As a building grows or spans multiple floors/areas, an IDF is used as a secondary wiring closet to reduce cable runs, provide local switching, and aggregate user access connections back to the MDF using backbone cabling (often fiber). This supports scalability, cable management, and performance by keeping horizontal runs within recommended distance limits.
VPC (Virtual Private Cloud) is a cloud networking construct, not a physical wiring location. VXLAN is an overlay tunneling technology used in virtualized/data center networks, not where you physically install switches. The question specifically references extending the network beyond the primary equipment location, which is a classic use case for deploying an IDF to host additional switches closer to endpoint areas while uplinking back to the MDF.

NEW QUESTION: 229
A network engineer receives a vendor alert regarding a vulnerability in a router CPU. Which of the following should the engineer do to resolve the issue?
A. Update the firmware.
B. Replace the system board.
C. Patch the OS.
D. Isolate the system.
Answer: (SHOW ANSWER)
Understanding the Vulnerability:
Vulnerabilities in the router CPU can be exploited to cause performance degradation, unauthorized access, or other security issues.
Firmware Update:
Firmware Role: The firmware is low-level software that controls the hardware of a device. Updating the firmware can address vulnerabilities by providing patches and enhancements from the manufacturer.
Procedure: Download the latest firmware from the vendor's website, follow the manufacturer's instructions to apply the update, and verify that the update resolves the vulnerability.
Comparison with Other Options:
Replace the System Board: This is a costly and often unnecessary step if the issue can be resolved with a firmware update.
Patch the OS: Patching the OS is relevant for devices with a full operating system but not directly applicable to addressing a CPU vulnerability on a router.
Isolate the System: Temporarily isolating the system can mitigate immediate risk but does not resolve the underlying vulnerability.
Best Practice:
Regularly check for and apply firmware updates to ensure that network devices are protected against known vulnerabilities.
References:
CompTIA Network+ study materials on network security and device management.

NEW QUESTION: 230
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: 231
A systems administrator needs to connect two laptops to a printer via Wi-Fi. The office does not have access points and cannot purchase any. Which of the following wireless network types best fulfills this requirement?
A. Mesh
B. Infrastructure
C. Ad hoc
D. Point-to-point
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (aligned to N10-009):
An ad hoc wireless network allows devices to connect directly to each other without an access point. This is suitable for small, temporary setups like two laptops and a printer.
A). Mesh requires multiple nodes forming a larger distributed network.
B). Infrastructure requires an AP, which is not available here.
D). Point-to-point is typically for long-distance wireless links between two fixed endpoints.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Wireless network types: infrastructure, ad hoc, mesh.

NEW QUESTION: 232
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: 233
A network administrator needs to change where the outside DNS records are hosted. Which of the following records should the administrator change the registrar to accomplish this task?
A. NS
B. SOA
C. PTR
D. CNAME

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

NEW QUESTION: 234
Which of the following impacts the availability of a web-based customer portal?
A. MAC flooding
B. ARP spoofing
C. DoS
D. Rogue devices
Answer: (SHOW ANSWER)
A DoS (Denial of Service) attack directly targets availability, one of the core security goals (CIA triad) emphasized in Network+ (N10-009) security objectives. A web-based customer portal depends on reachable services (web servers, load balancers, DNS, upstream bandwidth). In a DoS, an attacker attempts to overwhelm the portal or its supporting infrastructure-consuming bandwidth, exhausting server resources, or saturating state tables-so legitimate users cannot connect or experience severe degradation. This is the most direct and common scenario where "availability" is impacted for a public web service.
MAC flooding aims to overflow a switch's CAM table and can lead to traffic being broadcast out ports, which is more commonly associated with enabling sniffing or disruption within a local switched network segment- not typically the primary attack described for a web portal's availability. ARP spoofing is a local network man-in-the-middle/redirection technique affecting integrity/confidentiality and potentially availability for local hosts, but it is not the best match for a public portal availability impact. Rogue devices can introduce risk, but the option is broad and indirect; DoS is the clearest availability-focused threat.

NEW QUESTION: 235
An employee has a new laptop and reports slow performance when using the wireless network. Switch firmware was updated the previous night. A network administrator logs in to the switch and sees the following statistics on the switch interface for that employee:
98469 packets input, 1681937 bytes, 0 no buffer
Received 1548 broadcasts (25285 multicasts)
65335 runts, 0 giants, 0 throttles
11546 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
22781 packets output, 858040 bytes, 0 underruns
0 output errors, 89920 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier

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

NEW QUESTION: 236
A company is migrating a data center from on premises to the cloud. Which of the following tools will help maintain consistency, reliability, and efficiency of provisioning and management?
A. IaC
B. CDN
C. SASE
D. ZTA
Answer: (SHOW ANSWER)
The correct answer is A. IaC . Infrastructure as Code is used to define and deploy infrastructure through templates, configuration files, or code rather than building everything manually. During a cloud migration, that approach helps keep deployments consistent across environments and reduces the chance of human error.
This fits the question especially well because it mentions consistency, reliability, and efficiency in both provisioning and management. Those are exactly the kinds of benefits IaC is meant to provide. Instead of configuring servers, networks, and services one by one, administrators can reuse tested deployment definitions and apply the same settings repeatedly. That makes rollouts faster and easier to audit.
The other options do not match the task. A CDN improves content delivery performance. SASE is a networking and security architecture. ZTA focuses on access control and trust decisions. All of those are important in the right context, but none is primarily a provisioning and management automation tool.
In a cloud migration, the organization usually wants repeatable builds, standardization, and faster recovery if something has to be recreated. That is why IaC is the strongest answer here. It directly supports automated, dependable, and scalable infrastructure deployment.

NEW QUESTION: 237
Which of the following network ports is used when a client accesses an SFTP server?
A. 22
B. 80
C. 443
D. 3389
Answer: A (LEAVE A REPLY)
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