CompTIA.N10-009.v2026-08-20.q241

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	241
Version:	v2026-08-20
# of views:	109
# of Questions views:	2611
https://www.freecram.net/torrent/CompTIA.N10-009.v2026-08-20.q241.html	

NEW QUESTION: 1
Which of the following requires network devices to be managed using a different set of IP addresses?
A. Console
B. Split tunnel
C. Jump box
D. Out of band
Answer: (SHOW ANSWER)
Out-of-band (OOB) management refers to using a dedicated management network that is physically separate from the regular data network. This management network uses a different set of IP addresses to ensure that management traffic is isolated from user data traffic, providing a secure way to manage network devices even if the main network is down or compromised.References:CompTIA Network+ study materials.

NEW QUESTION: 2
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: 3

A company is concerned that the public can use network wall jacks in publicly available conference rooms to access company servers. Which of the following is the best way to mitigate the vulnerability?

A. Create a trusted zone.

B. Disable unused services.

C. Use MAC filtering.

D. Implement 802.1X.

Answer: D (LEAVE A REPLY)

The best mitigation is implementing 802.1X, which provides port-based Network Access Control (NAC).

With 802.1X enabled on access switch ports, a device plugged into a wall jack cannot gain normal network access until it successfully authenticates using credentials/certificates via an authentication server (commonly RADIUS). This directly addresses the threat of unauthorized users plugging into publicly accessible conference room jacks, because the switch keeps the port in an unauthenticated state (or places it into a restricted/guest VLAN) until authentication succeeds. This aligns with Network+ security objectives that emphasize controlling access at the edge, enforcing authentication, and reducing the risk of rogue or unmanaged devices on internal networks.

MAC filtering is weaker because MAC addresses can be spoofed and managing allow-lists at scale is error- prone. Creating a trusted zone is vague and does not prevent initial port access; segmentation helps limit blast radius but doesn't enforce authentication at the jack. Disabling unused services is a general hardening practice, but it does not stop someone from connecting physically to an active switch port and attempting access. 802.1X is purpose-built for this exact scenario.

NEW QUESTION: 4

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: D (LEAVE A REPLY)

* 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: 5
A network engineer is deploying switches at a new remote office. The switches have been preconfigured with hostnames and STP priority values. Based on the following table:
Switch Name
Priority
core-sw01
24576
access-sw01
28672
distribution-sw01
32768
access-sw02
36864
Which of the following switches will become the root bridge?
A. core-sw01
B. access-sw01
C. distribution-sw01
D. access-sw02
Answer: (SHOW ANSWER)
The switch with the lowest STP priority becomes the root bridge.In the given table, core-sw01 has the lowest priority value of 24576. Therefore, it will be elected as the root bridge in the Spanning Tree Protocol topology.
Reference:Section 2.2 - Switching Technologies and Features - "Spanning Tree Protocol (STP)"

NEW QUESTION: 6
A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses (one for a computer and one for a phone). Which of the following classful IPv4 address ranges will be best-suited for the network?
A. Class D
B. Class B
C. Class A
D. Class C
Answer: (SHOW ANSWER)
*The total number of devices = (150 + 10) users × 2 IPs per user = 320 devices
*Class C (D) supports a maximum of 254 hosts (2^8 - 2), which is too small.
*Class B (B) supports 65,534 hosts (2^16 - 2), making it the best choice.
*Why not the other options?
*Class A (C): Supports millions of addresses, which is overkill for 320 devices.
*Class D (A): Used for multicast, not for device addressing.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 7

Developers want to create a mobile application that requires a runtime environment, developer tools, and databases. The developers will not be responsible for security patches and updates. Which of the following models meets these requirements?

A. Container as a service

B. Infrastructure as a service

C. Platform as a service

D. Software as a service

Answer: (SHOW ANSWER)

The correct answer is Platform as a Service (PaaS). PaaS provides developers with a ready-to-use platform that includes runtime environments, developer tools, middleware, and database services. Developers can focus on writing code while the provider handles security patches, updates, and infrastructure management.

A). CaaS (Containers as a Service) focuses on deploying and managing containerized applications, not providing full developer platforms.

B). IaaS delivers virtual machines, storage, and networking, but administrators must install and maintain the OS, middleware, and updates.

D). SaaS provides end-user applications (e.g., email, CRM), not platforms for development.

By using PaaS, the developers can build applications quickly and cost-effectively without worrying about underlying infrastructure or system maintenance.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Cloud service models (IaaS, PaaS, SaaS, CaaS).

NEW QUESTION: 8

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: 9

A technician needs to quickly set up a network with five wireless devices. Which of the following network types should the technician configure to accomplish this task?

A. Ad hoc

B. Spine and leaf

C. Point to point

D. Mesh

Answer: (SHOW ANSWER)

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

NEW QUESTION: 10

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?

Freecram.net

A. The PoE power budget is exceeded.
B. Port security is violated.
C. The signal is degraded
D. The Ethernet cable is not working
Answer: (SHOW ANSWER)
Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data.
If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 11
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: 12
A network engineer is troubleshooting connectivity for a newly installed server on an existing VLAN. The engineer reviews the following output:

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

NEW QUESTION: 13
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: 14
A network administrator is managing network traffic so that classified services and applications are prioritized. Which of the following technologies should the network administrator use?
A. Load balancing
B. Time to live
C. Quality of service
D. Content delivery network
Answer: (SHOW ANSWER)
Quality of Service (QoS) is used to prioritize certain types of traffic to ensure critical applications receive the bandwidth, low latency, and low jitter they need-especially during congestion. Network+ objectives cover QoS concepts such as classification, marking, queuing, and policing/shaping to manage how traffic is handled on interfaces and across links. If the requirement is to prioritize "classified services and applications," QoS policies can match traffic using ports, protocols, DSCP markings, VLAN tags, or application identifiers and then place that traffic into higher-priority queues or reserve bandwidth for it. Load balancing distributes traffic across multiple servers/paths but does not inherently prioritize one class of traffic over another on congested links. TTL (time to live) is an IP header field used to prevent routing loops and is unrelated to prioritization. A CDN improves content delivery and caching for distributed users, but it is not a traffic-prioritization mechanism within an organization's network. Therefore, QoS is the correct technology for prioritizing specific services and applications.

NEW QUESTION: 15
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: 16
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."

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17
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: 18
After installing a new wireless access point, an engineer tests the device and sees that it is not performing at the rated speeds. Which of the following should the engineer do to troubleshoot the issue? (Select two.)

A. Ensure a bottleneck is not coming from other devices on the network.
B. Install the latest firmware for the device.
C. Create a new VLAN for the access point.
D. Make sure the SSID is not longer than 16 characters.
E. Configure the AP in autonomous mode.
F. Install a wireless LAN controller.
Answer: (SHOW ANSWER)
Troubleshooting poor performance of a newly installed access point involves multiple steps. Checking for network bottlenecks and ensuring the device firmware is up to date are crucial first steps. The document confirms:"Network bottlenecks can severely limit the performance of even the fastest wireless access points, so it's essential to verify that no other devices are causing a slowdown. In addition, keeping firmware updated ensures optimal performance and security."

NEW QUESTION: 19
A company recently rearranged some users' workspaces and moved several users to previously used workspaces. The network administrator receives a report that all of the users who were moved are having connectivity issues. Which of the following is the MOST likely reason?
A. Ports are error-disabled.
B. Ports have an incorrect native VLAN.
C. Ports are having an MDIX issue.
D. Ports are trunk ports.
Answer: B (LEAVE A REPLY)
The most likely cause is that the switch ports were previously configured for a different VLAN than the one the users' computers are on. If the native VLAN on the port doesn't match the end device's VLAN, communication fails.
A). Ports are error-disabled: Would result in no link at all, not common across multiple ports unless a violation occurred.
C). MDIX issue: Auto-MDIX eliminates most crossover problems on modern switches.
D). Ports are trunk ports: While possible, typical user devices should be on access ports, but if the port is incorrectly trunked, it can cause similar issues. However, "incorrect VLAN" is more precise here.
Reference:
CompTIA Network+ N10-009 Official Objectives: 2.3 - Given a scenario, configure and verify VLANs.

NEW QUESTION: 20
Which of the following should a network engineer check to verify that updates are still being released for a device?
Freecram.net
A. Baseline configuration
B. EOL documentation
C. Asset inventory licensing
D. Software development life cycle
Answer: (SHOW ANSWER)
The correct answer is B. EOL documentation. If a network engineer wants to confirm whether a device is still receiving updates, patches, or vendor support, the first thing to review is the vendor's End-of-Life (EOL) and often related End-of-Support (EOS) documentation. These documents show whether the device is still actively supported, whether firmware and security updates are still being issued, and when that support is scheduled to stop.
This is important in network operations because devices that are no longer supported can become security risks and operational liabilities. Once a vendor declares a product end-of-life or end-of-support, future bug fixes, feature releases, and security updates may no longer be available. That directly affects patch management, lifecycle planning, and risk assessment.

The other choices do not answer the question as directly. A baseline configuration shows the intended device settings, not the support status. Asset inventory licensing helps track ownership, software entitlements, or subscriptions, but it does not prove that updates are still being released. Software development life cycle refers to the process of building software, not the support state of a deployed network device.
For Network+ exam purposes, when the question asks whether updates are still being released, the best source is the vendor's EOL documentation.

NEW QUESTION: 21
Which of the following best describes a characteristic of a DNS poisoning attack?
A. DNS address records are edited and changed on a DNS server.
B. An attacker sets up a malicious DNS server in place of a legitimate server.
C. DNS client requests are intercepted and false responses are returned.
D. False DNS records are injected into cache on a DNS server.
Answer: (SHOW ANSWER)
DNS poisoning (also commonly called DNS cache poisoning) is characterized by inserting fraudulent DNS data into a resolver's cache so that subsequent queries return incorrect IP mappings. Option D describes this precisely: false DNS records are injected into a DNS server's cache, causing users to be redirected to attacker- controlled destinations even when they request a legitimate hostname. This aligns with Network+ security objectives covering common network attacks targeting name resolution and trust relationships. Editing authoritative DNS records on a DNS server (A) implies direct compromise or unauthorized administrative change, which is a different scenario than cache poisoning. Setting up a malicious DNS server in place of a legitimate server (B) is closer to DNS hijacking or rogue DNS configuration rather than cache poisoning.
Intercepting client requests and returning false responses (C) describes man-in-the-middle style spoofing on the wire; while related, the defining "poisoning" trait is the persistence created by corrupting the cache so the bad answer continues to be served. For defensive relevance in Network+ scope, cache poisoning highlights the importance of DNS security controls such as source port randomization, transaction ID entropy, and DNSSEC validation where applicable.

NEW QUESTION: 22
A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?
A. Reverse the fibers.
B. Reterminate the fibers.
C. Verify the fiber size.
D. Examine the cable runs for visual faults.
Answer: (SHOW ANSWER)
When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.References:CompTIA Network+ study materials.

NEW QUESTION: 23
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: D (LEAVE A REPLY)

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: 24
Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?
A. Access, distribution, and core
B. Core, root, and distribution
C. Core, spine, and leaf
D. Access, core, and roof
Answer: (SHOW ANSWER)
The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 25
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. nmap
B. arp
C. tracert
D. ipconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 26
A government entity wants to implement technology that can block websites based on country code. Which of the following will best enable this requirement?
A. URL filtering
B. Content filtering
C. DNS poisoning
D. MAC filtering
Answer: (SHOW ANSWER)
URL filtering can block access to websites based on their domain or country code TLDs (e.g., .cn, .ru). This is the correct method to block by location identifiers in URLs.
B). Content filtering blocks based on keywords or categories within websites, not country code.
C). DNS poisoning is an attack, not a control mechanism.
D). MAC filtering restricts devices, not websites.

References (CompTIA Network+ N10-009):
Domain: Network Security - Filtering technologies, URL vs content filtering.

NEW QUESTION: 27
Which of the following steps in the troubleshooting methodology would be next after putting preventive measures in place?
A. Implement the solution.
B. Verify system functionality.
C. Establish a plan of action.
D. Test the theory to determine cause.
Answer: (SHOW ANSWER)
After implementing a solution and putting preventive measures in place, the next step is to verify that the system is functioning correctly. This ensures that the issue has been fully resolved.

NEW QUESTION: 28
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: 29
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: 30
A network administrator is developing a method of device monitoring with the following requirements:
*Allows for explicit, by user, privilege management
*Includes centralized logging of changes
*Offers widely accessible remote management
*Provides support of service accounts
Which of the following will most closely meet these requirements?
Freecram.net
A. SNMP
B. API
C. SIEM
D. SSO
Answer: (SHOW ANSWER)
*API (Application Programming Interface) enables secure and granular access control, remote management, and logging, making it ideal for network monitoring.
*SNMP (A) is mainly used for device monitoring but lacks centralized logging and user-based privilege control.
*SIEM (C) is a security monitoring tool focused on log collection, not device management.
*SSO (D) is related to authentication, not monitoring.
#Reference: CompTIA Network+ N10-009 Official Documentation - Network Monitoring & Management Technologies.

NEW QUESTION: 31
A network administrator is implementing security zones for each department. Which of the following should the administrator use to accomplish this task?
A. ACLs
B. Port security
C. Content filtering
D. NAC
Answer: (SHOW ANSWER)
* Understanding ACLs:
* Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.
* Implementing Security Zones:
* Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.
* Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.
* Comparison with Other Options:
* Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.
* Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.
* NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.
* Implementation Steps:
* Define ACL rules based on the requirements of each department.
* Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.
References:

* CompTIA Network+ study materials on network security and access control methods.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
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: 33
Which of the following is the most cost-effective way for a network administrator to establish a persistent, secure connection between two facilities?
A. Site-to-site VPN
B. GRE tunnel
C. VXLAN
D. Dedicated line
Answer: (SHOW ANSWER)
A Site-to-site VPN (Virtual Private Network) is the most cost-effective solution for establishing a persistent, secure connection between two facilities. It uses the public internet to create an encrypted tunnel, leveraging existing internet connections without requiring expensive dedicated infrastructure. This makes it ideal for organizations looking to securely connect remote sites while minimizing costs.

Why not GRE tunnel? Generic Routing Encapsulation (GRE) tunnels encapsulate traffic but do not provide encryption natively, requiring additional protocols (e.g., IPsec) for security. This adds complexity and is less cost-effective than a site-to-site VPN, which integrates encryption.
Why not VXLAN? Virtual Extensible LAN (VXLAN) is used for overlay networks in data centers to extend Layer 2 networks, not for secure site-to-site connectivity.
Why not Dedicated line? A dedicated line (e.g., leased line or MPLS) provides high reliability but is significantly more expensive due to the need for dedicated infrastructure.
Reference:CompTIA Network+ N10-009 Objective 1.7: Explain the use cases for virtual private networks (VPNs) and tunneling protocols. The CompTIA Network+ Study Guide (e.g., Chapter 12: Network Security) explains that site-to-site VPNs are a cost-effective, secure method for connecting geographically separate networks over the internet.

NEW QUESTION: 34
A network technician needs to install patch cords from the UTP patch panel to the access switch for a newly occupied set of offices. The patch panel is not labeled for easy jack identification. Which of the following tools provides the easiest way to identify the appropriate patch panel port?
A. Toner
B. Laptop
C. Cable tester
D. Visual fault locator
Answer: (SHOW ANSWER)
A toner probe, often referred to as a toner and probe kit, is the easiest and most effective tool for identifying individual cables in a bundle, especially in situations where the patch panel is not labeled. The toner sends an audible tone through the cable, and the probe detects the tone at the other end, allowing the technician to quickly identify the correct cable.
* Functionality: The toner generates a tone that travels along the cable. When the probe is placed near the correct cable, it detects the tone and emits a sound.
* Ease of Use: Toner probes are straightforward to use, even in environments with many cables, making them ideal for identifying cables in unlabeled patch panels.
* Efficiency: This method is much faster and more reliable than manual tracing, especially in complex setups.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Details tools used for cable identification and troubleshooting.
* Cisco Networking Academy: Provides training on using toner probes and other cable testing tools.
* Network+ Certification All-in-One Exam Guide: Explains the use of different tools for network cable identification and management.

NEW QUESTION: 35
A network engineer wants to implement a new IDS between the switch and a router connected to the LAN.
The engineer does not want to introduce any latency by placing the IDS in line with the gateway. The engineer does want to ensure that the IDS sees all packets without any loss. Which of the following is the best way for the engineer to implement the IDS?
A. Use a network tap.
B. Use Nmap software.
C. Use a protocol analyzer.
D. Use a port mirror.
Answer: D (LEAVE A REPLY)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

NEW QUESTION: 36
A customer wants to cache commonly used content to reduce the number of full page downloads from the internet. Which of the following should the network administrator recommend?
A. Proxy server
B. Load balancer
C. Open relay

D. Code repository
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
A proxy server (specifically a caching HTTP/HTTPS proxy) stores frequently accessed web objects and serves them locally to clients, reducing external bandwidth consumption and improving response times.
B). Load balancer distributes traffic across servers but does not inherently cache internet content.
C). Open relay is a misconfigured mail server that permits unauthorized relaying-this is a security issue, not a caching solution.
D). Code repository (e.g., for source control) isn't related to web content caching.
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Application-layer services (HTTP/HTTPS), proxies and caching behavior, performance optimization.

NEW QUESTION: 37
A network administrator is configuring a network for a new site that will have 150 users. Within the next year, the site is expected to grow by ten users. Each user will have two IP addresses, one for a computer and one for a phone connected to the network. Which of the following classful IPv4 address ranges will be best- suited for the network?
A. Class D
B. Class B
C. Class A
D. Class C
Answer: (SHOW ANSWER)
IPv4 addresses are divided into classes:
Class A: Supports 16,777,214 hosts (large enterprises).
Class B: Supports 65,534 hosts (medium to large networks).
Class C: Supports 254 hosts (small to medium networks).
Class D: Used for multicast, not for assigning IPs to hosts.
Step-by-step Calculation:
The network will have 150 users initially, with a projected growth of 10 users, totaling 160 users.
Each user has two devices, so 160 × 2 = 320 IP addresses needed.
A Class C subnet has 254 usable IPs by default, which is not sufficient.
A Class B subnet can support thousands of hosts, making it the most appropriate option.
Incorrect Options:
A). Class D: Reserved for multicast, not for host assignments.
C). Class A: Overkill for a network of this size.
D). Class C: Cannot support 320 hosts without subnetting, making Class B the best choice.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on IP Addressing and Subnetting

NEW QUESTION: 38
A network engineer configures a new switch and connects it to an existing switch for expansion and redundancy. Users immediately lose connectivity to the network. The network engineer notes the following spanning tree information from both switches:
Switch 1
Port State Cost

1 Forward 2
2 Forward 2
Switch 2
Port State Cost
1 Forward 2
2 Forward 2
Which of the following best describes the issue?
A. The port cost should not be equal.
B. The ports should use link aggregation.
C. A root bridge needs to be identified.
D. The switch should be configured for RSTP.
Answer: (SHOW ANSWER)
The issue is that no root bridge has been identified. In STP, a root bridge is necessary to manage redundant paths and avoid loops in the network. Without a root bridge, all switches will assume they can forward traffic, causing a network loop and connectivity problems.

NEW QUESTION: 39
A network administrator notices interference with industrial equipment in the 2.4GHz range. Which of the following technologies would most likely mitigate this issue? (Select two).
A. Mesh network
B. 5GHz frequency
C. Omnidirectional antenna
D. Non-overlapping channel
E. Captive portal
F. Ad hoc network
Answer: B (LEAVE A REPLY)
* Understanding 2.4GHz Interference:
* The 2.4GHz frequency range is commonly used by many devices, including Wi-Fi, Bluetooth, and various industrial equipment. This can lead to interference and degraded performance.
* Mitigation Strategies:
* 5GHz Frequency:
* The 5GHz frequency band offers more channels and less interference compared to the 2.4 GHz band. Devices operating on 5GHz are less likely to encounter interference from other devices, including industrial equipment.
* Non-overlapping Channels:
* In the 2.4GHz band, using non-overlapping channels (such as channels 1, 6, and 11) can help reduce interference. Non-overlapping channels do not interfere with each other, providing clearer communication paths for Wi-Fi signals.
* Why Other Options are Less Effective:
* Mesh Network: While useful for extending network coverage, a mesh network does not inherently address interference issues.
* Omnidirectional Antenna: This type of antenna broadcasts signals in all directions but does not mitigate interference.
* Captive Portal: A web page that users must view and interact with before accessing a network, unrelated to frequency interference.
* Ad Hoc Network: A decentralized wireless network that does not address interference issues directly.
* Implementation:
* Switch Wi-Fi devices to the 5GHz band if supported by the network infrastructure and client devices.
* Configure Wi-Fi access points to use non-overlapping channels within the 2.4GHz band to minimize interference.

References:
* CompTIA Network+ study materials on wireless networking and interference mitigation.

NEW QUESTION: 40
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: 41
Which of the following best describes a group of devices that is used to lure unsuspecting attackers and to study the attackers' activities?
A. Geofencing
B. Honeynet
C. Jumpbox
D. Screened subnet
Answer: (SHOW ANSWER)
A honeynet is a network of honeypots designed to attract and study attackers. Honeypots are decoy systems set up to lure cyber attackers and analyze their activities. A honeynet, being a collection of these systems, provides a broader view of attack methods and patterns, helping organizations improve their security measures. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 42
Which of the following is the best use case of a site-to-site VPN?
A. Securing access across an untrusted network
B. Encrypting data at rest
C. Filtering traffic between two internal subnets
D. Hosting public-facing applications that contain company resources
Answer: (SHOW ANSWER)
A site-to-site VPN is used to securely connect two networks over an untrusted network, most commonly the public internet. In Network+ (N10-009) objectives, VPNs are described as providing confidentiality and integrity for data in transit by creating an encrypted tunnel between sites (for example, headquarters and a branch office). This allows systems at both locations to communicate as if on the same private WAN, while preventing eavesdropping or tampering by intermediate networks. Typical implementations use IPsec tunneling and rely on negotiated encryption/authentication parameters to protect traffic end-to-end between VPN gateways.

Encrypting data at rest refers to storage encryption (disk/database), not VPN tunneling. Filtering traffic between two internal subnets is usually handled by ACLs, firewalls, or segmentation controls, not a site-to- site VPN. Hosting public-facing applications is a DMZ / reverse proxy / WAF design concern; a VPN is not the primary control for exposing public services (and generally you would not require the public to use a VPN to reach a public website). Therefore, securing site connectivity across an untrusted network is the best match.

NEW QUESTION: 43
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: 44
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: 45

A user tries to visit www.abc.com, but the website that displays is www.cba.com. Which of the following should be done in order to reach the correct website?
A. Modify the CNAME record.
B. Update the PTR record.
C. Change the NTP settings.
D. Delete the TXT record.
Answer: (SHOW ANSWER)
The correct answer is Modify the CNAME record because a CNAME (Canonical Name) record maps one domain name (alias) to another domain name. If a user enters www.abc.com but is redirected to www.cba.
com, it is likely that the DNS configuration includes an incorrect CNAME entry pointing abc.com to cba.com.
Updating or correcting the CNAME record ensures the alias resolves to the intended host.
According to CompTIA Network+ (N10-009) objectives covering DNS record types, a CNAME record is used to alias one domain name to another, commonly for load balancing, CDN services, or website redirection.
A PTR record (Option B) is used for reverse DNS lookups (IP address to hostname) and does not control forward name resolution for websites. NTP settings (Option C) are used for time synchronization and have no impact on DNS resolution. A TXT record (Option D) stores descriptive text information (such as SPF, DKIM, or domain verification data) and does not affect website redirection.
Therefore, correcting the CNAME record resolves the issue and ensures users reach the correct website.

NEW QUESTION: 46
A network engineer is configuring network ports in a public office. To increase security, the engineer wants the ports to allow network connections only after authentication. Which of the following security features should the engineer use?
A. Port security
B. 802.1X
C. MAC filtering
D. Access control list
Answer: (SHOW ANSWER)
802.1X provides port-based Network Access Control (NAC). Ports remain in a blocked state until a device authenticates (usually with RADIUS). This is ideal for public or semi-public areas where ports should not be
"always on."
A). Port security restricts by MAC addresses but does not authenticate users.
C). MAC filtering is easily spoofed and weaker than 802.1X.
D). ACLs filter traffic but do not enforce port-based authentication.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, port-based security.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47

Which of the following is associated with avoidance, acceptance, mitigation, and transfer?
A. Risk
B. Vulnerability
C. Threat
D. Exploit
Answer: (SHOW ANSWER)

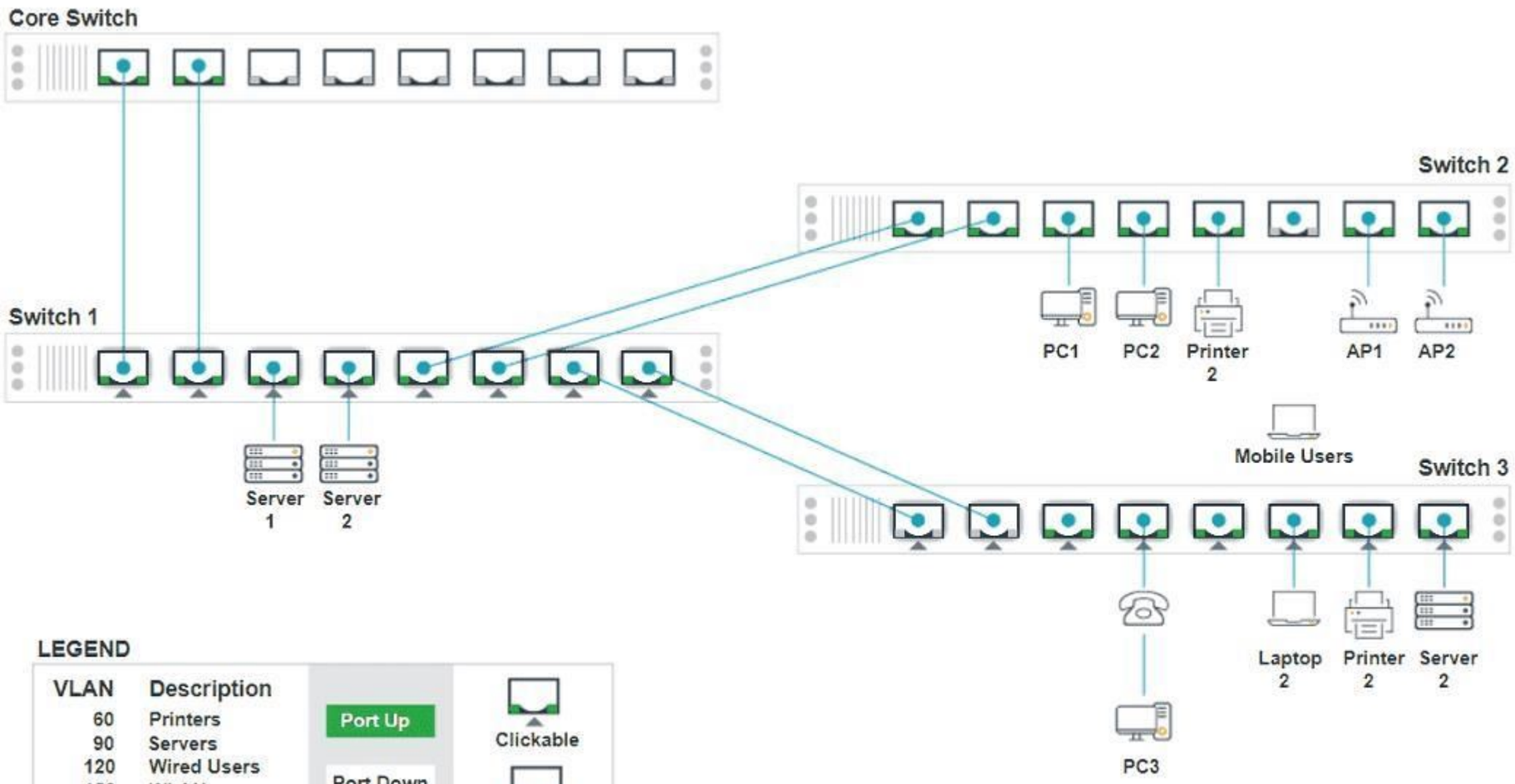
NEW QUESTION: 48
Before using a guest network, an administrator requires users to accept the terms of use Which of the following is the best way to accomplish this goal?
A. Pre-shared key
B. Autonomous access point
C. Captive portal
D. WPA2 encryption
Answer: (SHOW ANSWER)
A captive portal is a web page that users must view and interact with before being granted access to a network. It is commonly used in guest networks to enforce terms of use agreements. When a user connects to the network, they are redirected to this portal where they must accept the terms of use before proceeding. This method ensures that users are aware of and agree to the network's policies, making it the best choice for this scenario. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 49
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: 50
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: 51
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

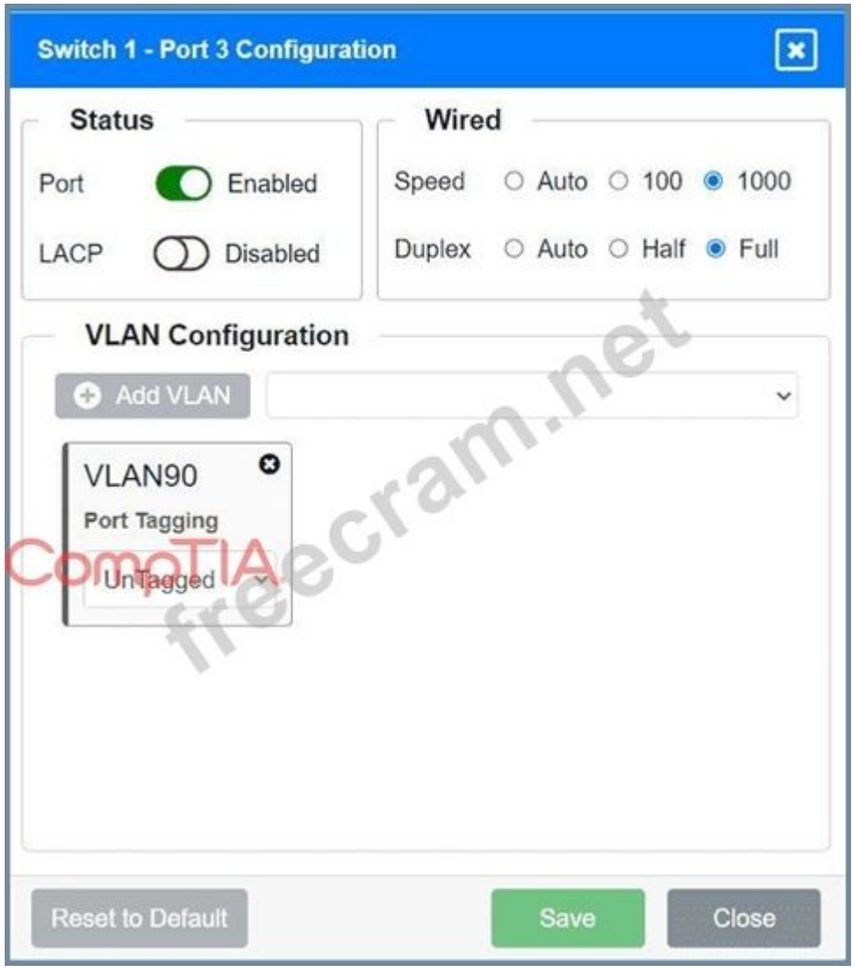
VLAN	Description
60	Printers
90	Servers
120	Wired Users
150	WLAN
220	Voice

Port Up

Port Down

Clickable

Not Clickable

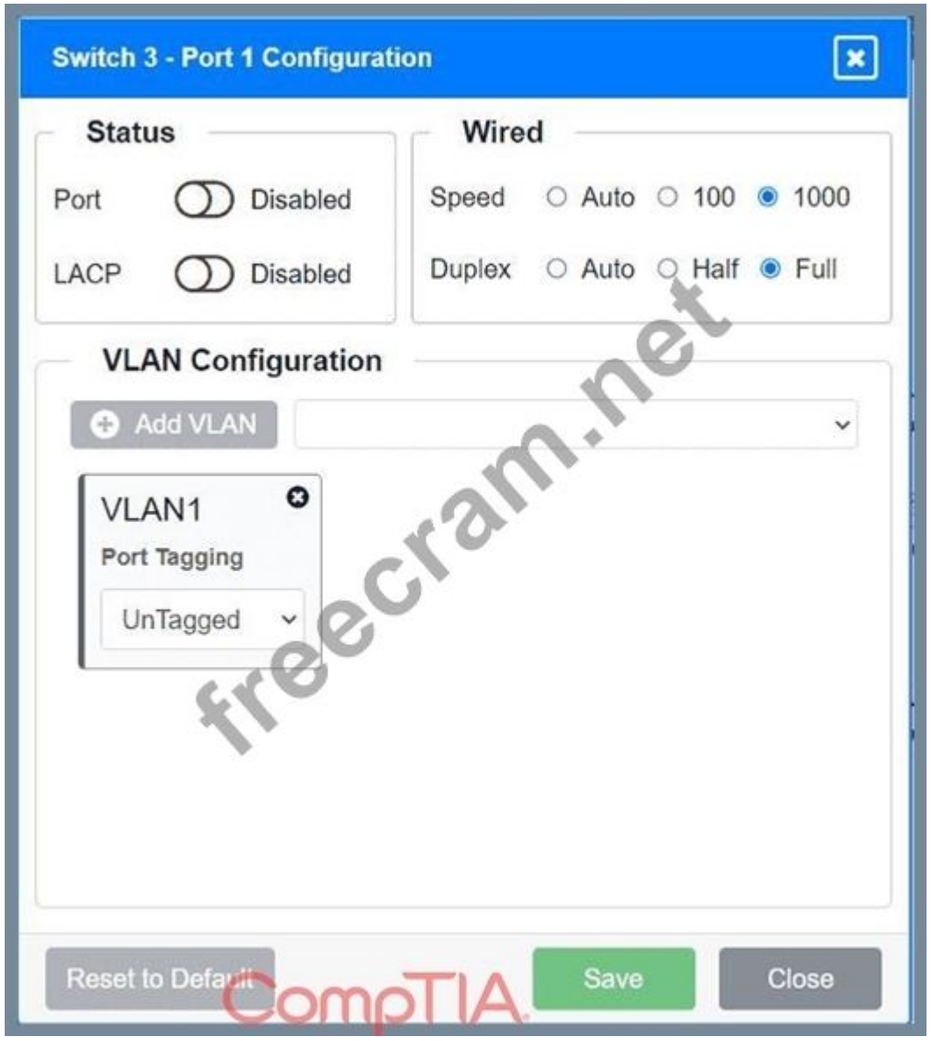


CompTIA
freecram.net

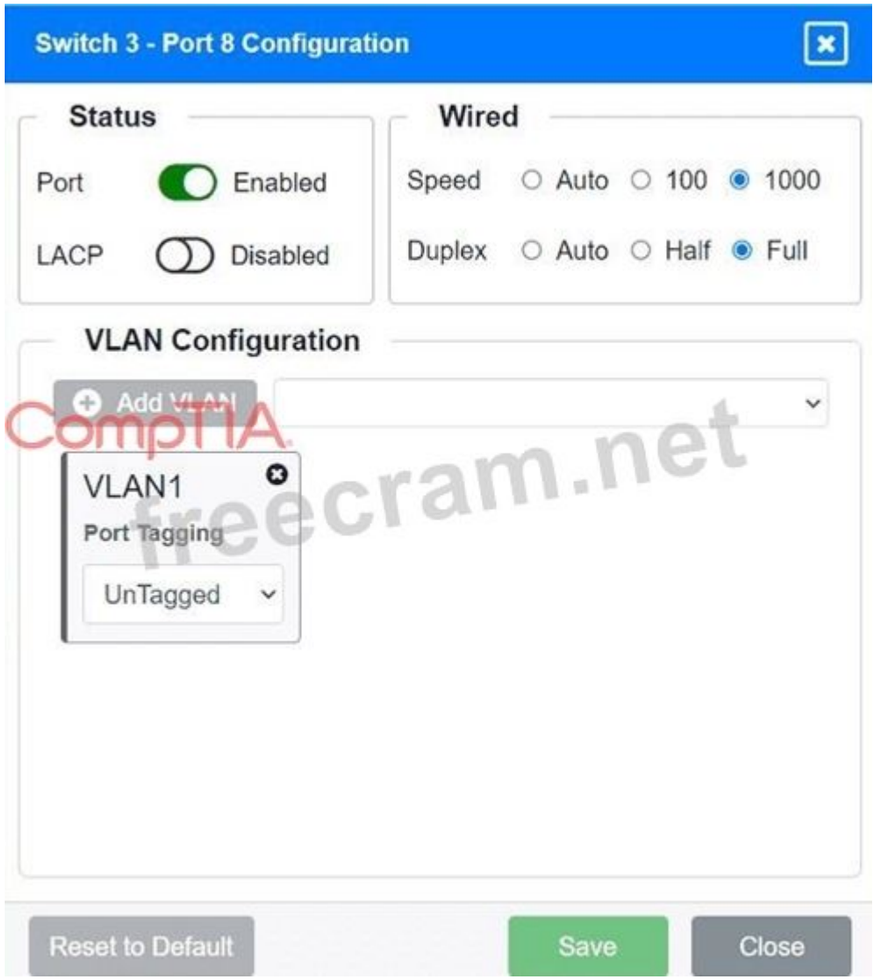
freecram.net

CompTIA
freecram.net

CompTIA
freecram.net



freecram.net
CompTIA.



CompTIA
freecram.net

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: 52
An IT department asks a newly hired employee to use a personal laptop until the company can provide one.
Which of the following policies is most applicable to this situation?
A. IAM
B. BYOD
C. DLP
D. AUP
Answer: (SHOW ANSWER)
BYOD (Bring Your Own Device) policies define rules for using personal devices on the company network.
Since the new employee is using a personal laptop, this policy applies.
Breakdown of Options:
A). IAM (Identity and Access Management) - Governs user permissions, not device policies.
B). BYOD (Bring Your Own Device) - # Correct answer. Covers using personal devices for work.
C). DLP (Data Loss Prevention) - Focuses on preventing sensitive data leaks, not device usage policies.
D). AUP (Acceptable Use Policy) - Covers internet and system usage, but not personal device rules.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.6: Explain security policies and best practices.

NEW QUESTION: 53
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: 54
A storage network requires reduced overhead and increased efficiency for the amout of data being sent.
Which of the following should an engineer likely configure to meet these requirements>?
A. Link speed
B. Jumbo frames
C. QoS
D. 802.1q tagging
Answer: (SHOW ANSWER)
Jumbo frames are Ethernet frames with a payload greater than the standard maximum transmission unit (MTU) of 1500 bytes. Configuring jumbo frames can reduce overhead and increase efficiency in storage networks by allowing more data to be sent in each frame, thus reducing the number of frames needed to transmit the same amount of data.
* Reduced Overhead: By sending larger frames, the relative overhead for headers and acknowledgments is reduced.
* Increased Efficiency: Larger frames mean fewer packets to process, leading to better utilization of network bandwidth and improved performance in high-throughput environments like storage networks.
* Configuration: Requires support from all devices in the network path, including switches and network interface cards (NICs).
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Explains jumbo frames and their benefits in reducing network overhead.
* Cisco Networking Academy: Provides training on network optimization techniques, including the use of jumbo frames.
* Network+ Certification All-in-One Exam Guide: Covers advanced Ethernet features, including jumbo frames and their configuration for improved network performance.

NEW QUESTION: 55
Users are unable to access files on their department share located on file server 2.
The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.
INSTRUCTIONS
Click on each router to review output, identify any issues, and configure the appropriate solution.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Router A

Routing Table | Routing Configuration

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, GigabitEthernet3
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.4.0/22 is directly connected, GigabitEthernet2
C        10.0.6.0/24 is directly connected, GigabitEthernet2
L        10.0.6.1/32 is directly connected, GigabitEthernet2
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet3
L        172.16.27.1/32 is directly connected, GigabitEthernet3
```

Reset to Default | Save | Close

CompTIA freecram.net

Router C

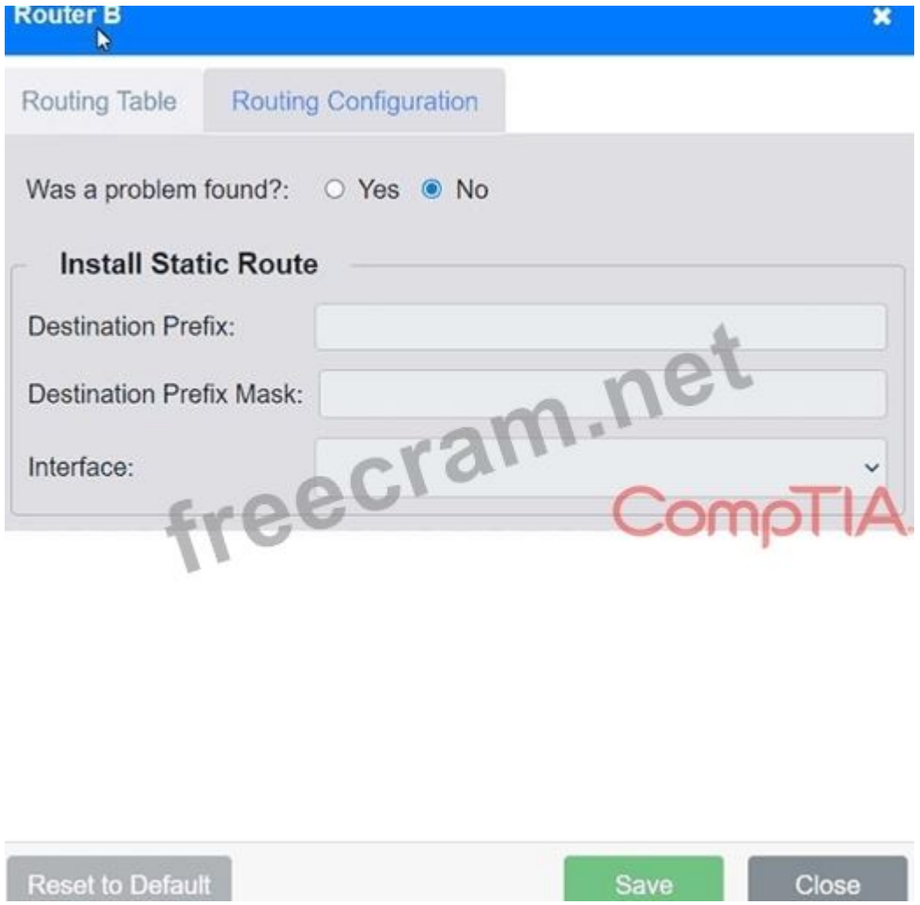
Routing Table | Routing Configuration

CompTIA

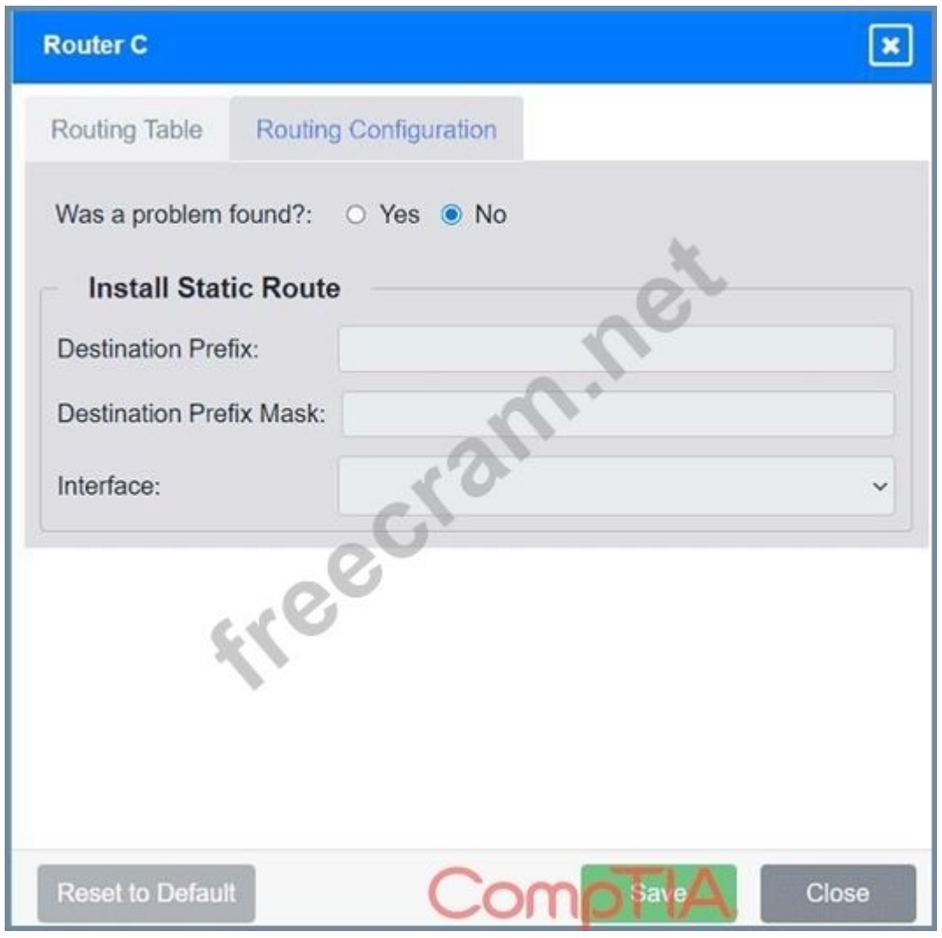
```
Router-C# show ip route

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

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.0.0.0/22 [1/0] via GigabitEthernet1
S        10.0.4.0/22 [1/0] via GigabitEthernet2
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.27.0/30 is directly connected, GigabitEthernet2
L        172.16.27.2/32 is directly connected, GigabitEthernet2
C        172.16.27.4/30 is directly connected, GigabitEthernet1
L        172.16.27.6/32 is directly connected, GigabitEthernet1
```

freecram.net

Reset to Default | Save | Close



freecram.net
CompTIA



freecram.net
CompTIA

Answer:

See the solution in Explanation.

Explanation:

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

Review Routing Tables:

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

Identify Missing Routes:

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

Add Static Routes:

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

Routing Table:

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, GigabitEthernet3

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

C 10.0.4.0/22 is directly connected, GigabitEthernet2

C 10.0.6.0/24 is directly connected, GigabitEthernet2

L 10.0.6.1/32 is directly connected, GigabitEthernet2

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

C 172.16.27.0/30 is directly connected, GigabitEthernet3

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

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

NEW QUESTION: 56
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: 57
Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?
A. Fire suppression
B. Power budget
C. Temperature
D. Humidity
Answer: (SHOW ANSWER)
Switches in sealed enclosures are at risk of overheating because airflow is restricted. The temperature factor is critical since heat buildup can damage components, shorten device lifespan, and cause outages. Proper cooling or ventilation must be ensured.
A). Fire suppression is important for data centers but not the primary concern in a sealed box.
B). Power budget applies to PoE allocations, not environmental safety.
D). Humidity matters, but overheating is far more immediate in sealed environments.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Environmental considerations, switch installation, temperature control.

NEW QUESTION: 58
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: 59
Which of the following allows a standard user to log in to multiple resources with one account?
A. RADIUS
B. MFA
C. TACACS+
D. SSO
Answer: D (LEAVE A REPLY)
Single Sign-On (SSO) enables a user to access multiple resources or applications with one set of credentials, improving usability and security. The document confirms:
"Single Sign-On (SSO) allows a user to authenticate once and gain access to multiple resources or applications without needing to log in again for each. It streamlines the login process and improves security by reducing the number of passwords that need to be managed."

NEW QUESTION: 60
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
Freecram.net
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: 61
A network technician is examining the configuration on an access port and notices more than one VLAN has been set. Which of the following best describes how the port is configured?
A. With a voice VLAN
B. With too many VLANs
C. With a default VLAN
D. With a native VLAN
Answer: (SHOW ANSWER)
It is common for an access port to have both a voice VLAN and a data VLAN. A voice VLAN separates voice traffic from regular data traffic, ensuring better quality and security for voice communications.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
Which of the following is a characteristic of the application layer?
A. It relies upon other layers for packet delivery.
B. It checks independently for packet loss.
C. It encrypts data in transit.
D. It performs address translation.
Answer: (SHOW ANSWER)
Introduction to OSI Model:
The OSI model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
Application Layer:

The application layer (Layer 7) is the topmost layer in the OSI model. It provides network services directly to end-user applications. This layer facilitates communication between software applications and lower layers of the network protocol stack.
Reliance on Other Layers:
The application layer relies on the transport layer (Layer 4) for data transfer across the network. The transport layer ensures reliable data delivery through protocols like TCP and UDP.
The network layer (Layer 3) is responsible for routing packets to their destination.
The data link layer (Layer 2) handles node-to-node data transfer and error detection.
The physical layer (Layer 1) deals with the physical connection between devices.
Explanation of the Options:
A). It relies upon other layers for packet delivery: This is correct. The application layer depends on the lower layers (transport, network, data link, and physical) for the actual delivery of data packets.
B). It checks independently for packet loss: This is incorrect. Packet loss detection is typically handled by the transport layer (e.g., TCP).
C). It encrypts data in transit: This is incorrect. Encryption is typically handled by the presentation layer or at the transport layer (e.g., TLS/SSL).
D). It performs address translation: This is incorrect. Address translation is performed by the network layer (e.
g., NAT).
Conclusion:
The application layer's primary role is to interface with the end-user applications and ensure that data is correctly presented to the user. It relies on the underlying layers to manage the actual data transport and delivery processes.
References:
CompTIA Network+ guide covering the OSI model and the specific roles and functions of each layer (see page Ref 10 How to Use Cisco Packet Tracer).

NEW QUESTION: 63
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: C (LEAVE A REPLY)
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: 64
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: 65
Which of the following is the most likely benefit of installing server equipment in a rack?
A. Simplified troubleshooting process
B. Decreased power consumption
C. Improved network performance
D. Increased compute density
Answer: (SHOW ANSWER)
Installing server equipment in a rack increases compute density by allowing multiple servers to be organized efficiently in a vertical configuration, saving space while housing more devices in a smaller footprint. This is critical for data centers and businesses with high hardware demands.
Simplified troubleshooting process (A): While racks can aid in organizing equipment, this is a secondary benefit, not the primary purpose.
Decreased power consumption (B): Rack installation does not directly reduce power usage; equipment power consumption remains the same.
Improved network performance (C): Racking servers does not inherently improve network performance; that depends on network configurations.
Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Rack Installations).

NEW QUESTION: 66
A network architect of a stock exchange broker is implementing a disaster recovery (DR), high-availability plan. Which of the following approaches would be the best fit?
A. Warm site
B. Active-active
C. Full mesh
D. In-band
Answer: B (LEAVE A REPLY)
The correct answer is Active-active because a stock exchange broker requires extremely high availability, minimal downtime, and near-zero data loss. According to CompTIA Network+ (N10-009) objectives under high availability and disaster recovery concepts, an active-active configuration involves multiple systems or sites operating simultaneously and sharing the workload. If one system fails, the other continues processing traffic without service interruption.
This model provides the lowest Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which is critical in financial trading environments where even seconds of downtime can result in major financial loss. Active-active architectures also support load balancing, redundancy, and continuous synchronization between systems.

A warm site (Option A) contains preconfigured hardware but may require data restoration and configuration before becoming fully operational, resulting in some downtime. A full mesh (Option C) is a network topology design and does not specifically address disaster recovery at the service level. In-band (Option D) refers to management traffic sharing the production network and is unrelated to DR strategy.
Therefore, an active-active approach is the most suitable solution for mission-critical financial operations.

NEW QUESTION: 67
Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?
A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO
Answer: (SHOW ANSWER)
The correct answer is 802.1X, which is an identity-based Network Access Control (NAC) framework emphasized in the CompTIA Network+ N10-009 objectives under network security and access control. 802.1 X uses a policy-driven authentication process to determine whether a user or device is allowed network access based on verified credentials, such as usernames, passwords, or digital certificates.
802.1X operates using three main components: the supplicant (the client requesting access), the authenticator (the network device such as a switch or wireless access point), and the authentication server (typically a RADIUS server). Once the user's identity is authenticated, predefined policies determine the level of access granted-full access, limited access, or denial. This makes 802.1X a cornerstone of zero trust and enterprise- grade NAC implementations.
A standard ACL controls traffic based on IP addresses and ports, not user identity. MAC filtering allows or denies access based on device MAC addresses, which can be easily spoofed and does not verify user identity.
SSO (Single Sign-On) simplifies authentication across multiple systems but does not control network-layer access.
Network+ highlights 802.1X as a secure, scalable solution for enforcing identity-based network access policies in both wired and wireless environments.

NEW QUESTION: 68
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: 69
Which of the following can be used when a server at a remote site is physically unreachable?
A. OOB management
B. Crash cart
C. Jump box
D. Console
Answer: (SHOW ANSWER)
Out-of-band (OOB) managementallows administrators to manage devices remotely even if the primary network is down. This is especially useful when physical access to the server is not possible. OOB management often uses a separate management interface, ensuring access regardless of the server's operational state.
Reference:Section 3.5 - Network Access and Management Methods - "OOB Management"

NEW QUESTION: 70
Which of the following connection methods allows a network engineer to automate configuration deployment for network devices across the environment?
Freecram.net
A. RDP
B. Telnet
C. SSH
D. GUI
Answer: (SHOW ANSWER)
Comprehensive and Detailed Explanation (paraphrased, aligned to N10-009):
SSH provides secure, scriptable remote access used by automation/orchestration tools (e.g., leveraging CLI, NETCONF over SSH, or Ansible modules) to push configurations at scale.
* A. RDP is primarily for Windows GUI sessions and is not commonly used for network device automation.
* B. Telnet can be scripted but is insecure (plaintext); modern best practice is to use SSH.
* D. GUI access is typically manual and not ideal for scalable, repeatable automation.
References (CompTIA Network+ N10-009):
* Domain: Network Operations - Configuration management, automation/orchestration, secure management protocols (SSH vs. Telnet), change at scale.

NEW QUESTION: 71
Which of the following is used to estimate the average life span of a device?
A. RTO
B. RPO
C. MTBF
D. MTTR
Answer: (SHOW ANSWER)

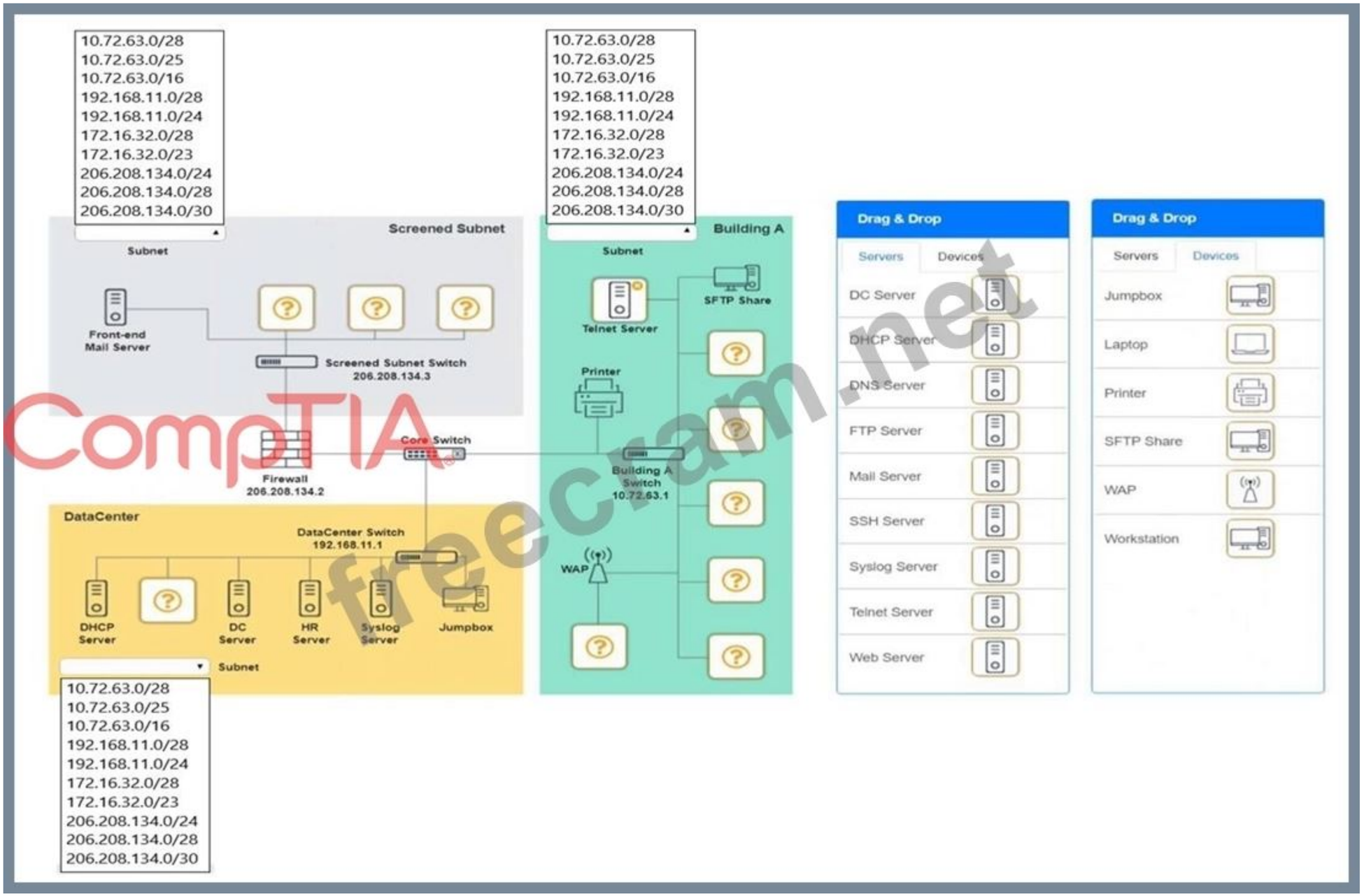
* Understanding MTBF:
* Mean Time Between Failures (MTBF):A reliability metric that estimates the average time between successive failures of a device or system.
* Calculation and Importance:
* Calculation:MTBF is calculated as the total operational time divided by the number of failures during that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

NEW QUESTION: 72
Users at a satellite office are experiencing issues when using videoconferencing. Which of the following should a technician focus on first to rectify these issues?
A. Quality of service
B. Network signal
C. Time to live
D. Load balancing
Answer: (SHOW ANSWER)
Quality of Service (QoS) is crucial for real-time services like video conferencing. It prioritizes voice and video packets over less critical traffic (like file downloads), reducing latency, jitter, and packet loss.
B). Network signal may apply to wireless, but it's not specific to video issues.
C). Time to live (TTL) affects packet lifespan, not performance or quality.
D). Load balancing manages traffic across multiple paths but doesn't prioritize real-time traffic like QoS does.
Reference:
CompTIA Network+ N10-009 Official Objectives: 3.6 - Explain the characteristics of network topologies and types.

NEW QUESTION: 73
A network architect needs to create a wireless field network to provide reliable service to public safety vehicles. Which of the following types of networks is the best solution?
A. Mesh
B. Ad hoc
C. Point-to-point
D. Infrastructure
Answer: (SHOW ANSWER)
A mesh network is the best solution for providing reliable wireless service to public safety vehicles. In a mesh network, each node (vehicle) can connect to multiple other nodes, providing multiple paths for data to travel.
This enhances reliability and redundancy, ensuring continuous connectivity even if one or more nodes fail.
Mesh networks are highly resilient and are well-suited for dynamic and mobile environments such as public safety operations.References:CompTIA Network+ study materials.

NEW QUESTION: 74
Which of the following are environmental factors that should be considered when installing equipment in a building? (Select two).
A. Fire suppression system
B. UPS location
C. Humidity control
D. Power load
E. Floor construction type
F. Proximity to nearest MDF
Answer: A (LEAVE A REPLY)
When installing equipment in a building, environmental factors are critical to ensure the safety and longevity of the equipment. A fire suppression system is essential to protect the equipment from fire hazards. Humidity control is crucial to prevent moisture-related damage, such as corrosion and short circuits, which can adversely affect electronic components. Both factors are vital for maintaining an optimal environment for networking equipment.References:CompTIA Network+ study materials.

NEW QUESTION: 75
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.

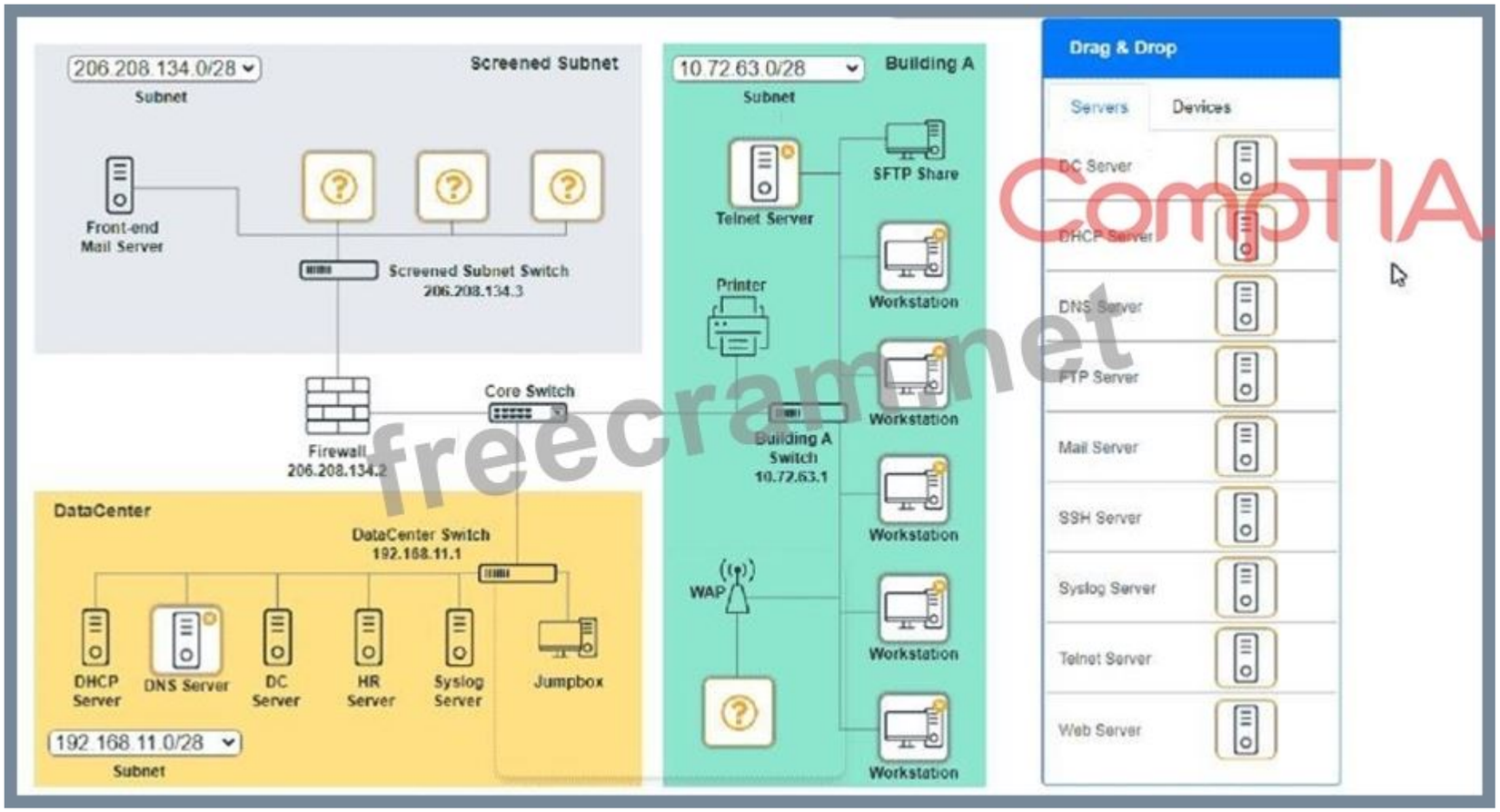
Explanation:

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.

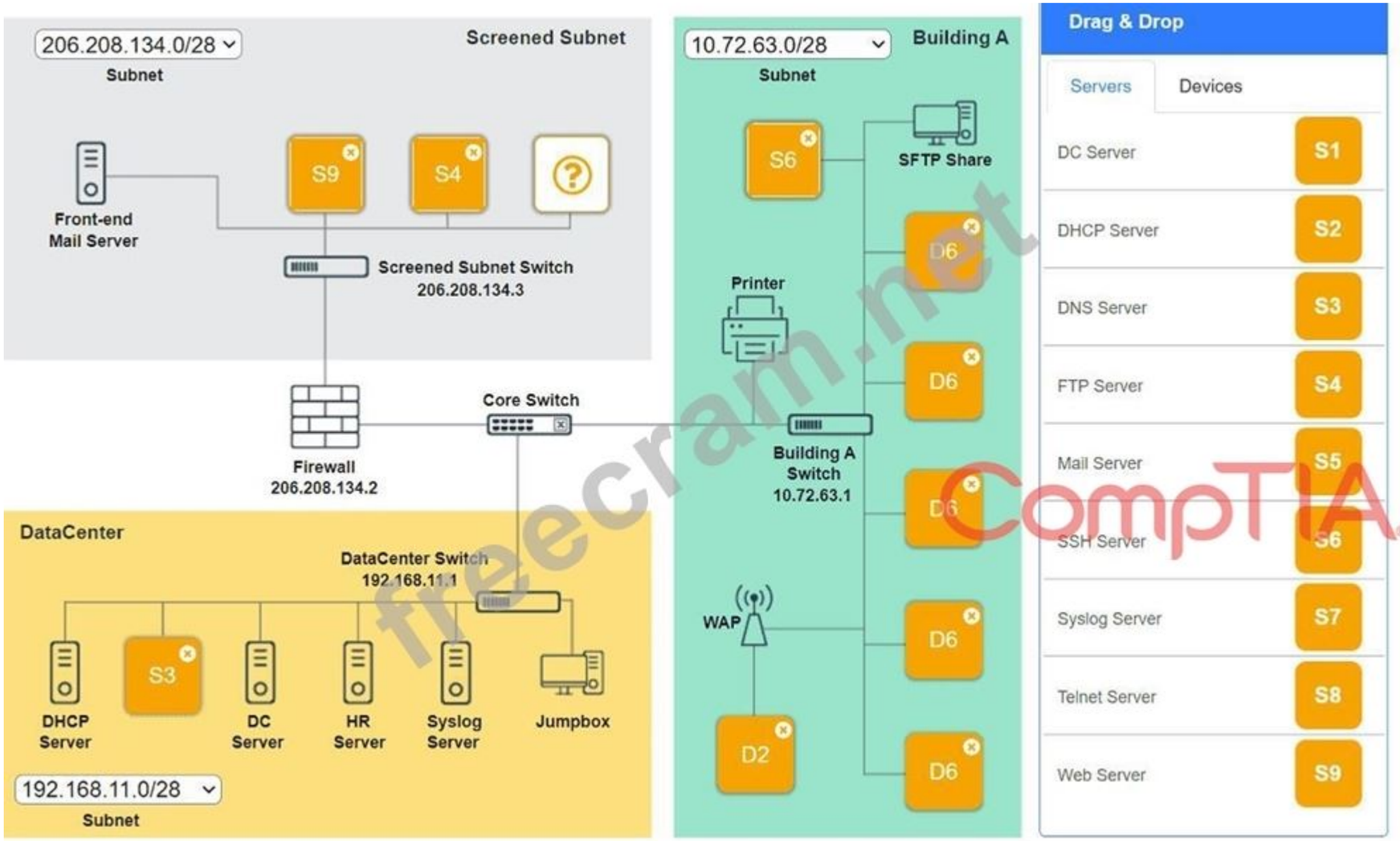
A screenshot of a computer AI-generated content may be incorrect.

CompTIA freecram.net



freecram.net
CompTIA

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



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

NEW QUESTION: 76

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.

freecram.net
CompTIA

* 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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
Which of the following cloud platform technology characteristics would a quantum computing host most likely prioritize?
A. Scalability
B. Elasticity
C. Multitenancy
D. Cost
Answer: (SHOW ANSWER)
The best answer is B. Elasticity . Quantum computing workloads are highly specialized and often require access to extremely expensive, limited, and on-demand processing resources. In cloud terms, elasticity is the ability to rapidly allocate and release resources as demand changes. That makes it a strong fit for environments where usage may spike for short periods and then drop off again.
A quantum host would not usually be designed around ordinary shared-office priorities. Instead, it would favor the ability to obtain powerful compute capacity exactly when needed, without keeping that level of capacity permanently assigned. That is the practical value of elasticity in a cloud model.
Scalability is close, but it usually describes the broader ability to increase capacity over time or as demand grows. Elasticity is more specific to dynamic, responsive adjustment of resources, which matches specialized compute workloads much better. Multitenancy refers to multiple customers sharing underlying infrastructure, and cost is always important, but neither is the main technical characteristic being highlighted here.
For exam purposes, when a scenario describes advanced or highly variable compute demand in the cloud, elasticity is usually the strongest answer because it focuses on rapid resource expansion and reduction as needed.

NEW QUESTION: 78
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: 79
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: C (LEAVE A REPLY)
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: 80
A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?
Freecram.net
A. Coaxial cable
B. 9.8ft (3m) cable
C. Plenum cable
D. STP cable
Answer: (SHOW ANSWER)
The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.
A). Coaxial is not used for modern Ethernet server-switch links.

B). Shorter UTP cable does not solve EMI issues.
C). Plenum cable refers to cable jacket type for fire safety, not electrical shielding.
STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

NEW QUESTION: 81
A network security administrator needs to monitor the contents of data sent between a secure network and the rest of the company. Which of the following monitoring methods will accomplish this task?
A. Port mirroring
B. Flow data
C. Syslog entries
D. SNMP traps
Answer: (SHOW ANSWER)
To monitor the contents of data (i.e., inspect the actual packets/frames and their payloads) moving between networks, the administrator should use port mirroring (also called SPAN on some platforms). Port mirroring copies traffic from one or more switch ports (or VLANs) to a designated monitoring port where a packet analyzer/IDS sensor can capture and inspect the traffic in detail. This aligns with Network+ (N10-009) security and monitoring concepts that distinguish between packet-level visibility and higher-level summaries or logs. If the requirement is explicitly to monitor "contents," you need a method that provides full packet capture capability, not just metadata.
Flow data (e.g., NetFlow) provides summarized metadata-who talked to whom, how much, ports, and timestamps-but not full payload contents. Syslog entries are device/application-generated logs and only show events a device chooses to report; they don't provide full data content visibility. SNMP traps are alerts about status changes (interfaces, thresholds, etc.) and similarly do not include traffic contents. Therefore, port mirroring is the correct monitoring method for inspecting data contents in transit.

NEW QUESTION: 82
Which of the following physical installation factors is the most important when a network switch is installed in a sealed enclosure?
A. Fire suppression
B. Power budget
C. Temperature
D. Humidity
Answer: (SHOW ANSWER)
The correct answer is Temperature because a sealed enclosure restricts airflow, which can cause heat to accumulate rapidly. According to CompTIA Network+ (N10-009) objectives under physical installations and environmental factors, maintaining proper temperature control is critical for network equipment reliability and longevity.
Network switches generate heat during operation, particularly models with high port density or Power over Ethernet (PoE) capabilities. In a sealed enclosure without proper ventilation or cooling mechanisms, excessive heat buildup can lead to thermal throttling, unexpected shutdowns, hardware degradation, or permanent equipment failure. Manufacturers specify operating temperature ranges, and exceeding these limits significantly reduces device lifespan and performance.
While humidity (Option D) is important to prevent condensation and corrosion, temperature fluctuations pose a more immediate risk in a sealed environment. Power budget (Option B) is relevant when calculating PoE load capacity but does not directly address environmental installation conditions. Fire suppression (Option A) is important in data centers but is not the primary concern specific to a sealed enclosure scenario.
Therefore, ensuring proper temperature management is the most critical installation factor.

NEW QUESTION: 83
Which of the following disaster recovery concepts is calculated by dividing the total hours of operation by the total number of units?

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

NEW QUESTION: 84
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: 85
Which of the following is a major difference between an IPS and IDS?
A. An IPS needs to be installed in line with traffic and an IDS does not.
B. An IPS is signature-based and an IDS is not.
C. An IPS is less susceptible to false positives than an IDS.
D. An IPS requires less administrative overhead than an IDS.
Answer: A (LEAVE A REPLY)
The key difference is that an Intrusion Prevention System (IPS) is installed in line with network traffic, allowing it to actively block threats. In contrast, an Intrusion Detection System (IDS) only monitors and alerts without actively blocking traffic.
Breakdown of Options:
A). An IPS needs to be installed in line with traffic and an IDS does not. # Correct answer. IPS actively prevents threats, while IDS only detects them.
B). An IPS is signature-based and an IDS is not. - False, both can use signature-based detection.
C). An IPS is less susceptible to false positives than an IDS. - False, both can produce false positives, depending on configurations.
D). An IPS requires less administrative overhead than an IDS. - False, IPS requires more administrative effort due to real-time blocking decisions.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Explain network security devices.

NEW QUESTION: 86
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: 87
Network administrators are using the Telnet protocol to administer network devices that are on the 192.168.1.0
/24 subnet. Which of the following tools should the administrator use to best identify the devices?
A. dig
B. nmap
C. tracert
D. telnet
Answer: (SHOW ANSWER)

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

NEW QUESTION: 88
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: 89
A network administrator installs new cabling to connect new computers and access points. After deploying the equipment, the administrator notices a few of the devices are not connecting properly. The administrator moves the devices to a different port, but it does not resolve the issue. Which of the following should the administrator verify next?
A. Power budget
B. Device requirements
C. Port status
D. Cable termination
Answer: D (LEAVE A REPLY)
*Cable termination issues (e.g., improper crimping, loose connectors) can cause connectivity failures.
*Power budget (A) applies to PoE devices, not general cabling issues.
*Device requirements (B) relate to software/hardware compatibility, not wiring faults.
*Port status (C) would help if the issue was switch-related, but since moving devices didn't help, it's likely a cabling issue.
#Reference: CompTIA Network+ N10-009 Official Documentation - Cabling & Physical Layer Troubleshooting.

NEW QUESTION: 90
A user recently moved a workstation to a different part of the office. The user is able to access the internet and print but is unable to access server resources. Which of the following is the most likely cause of the issue?
Freecramnet
A. Incorrect default gateway
B. Wrong VLAN assignment
C. Error-disabled port
D. Duplicate IP address
Answer: (SHOW ANSWER)

If a workstation can access the internet and printers (likely in another VLAN) but not internal servers, the port was likely placed into the wrong VLAN after the move. VLAN assignment controls Layer 2 segmentation, restricting access to resources on different VLANs.
A). A wrong default gateway would prevent internet access.
C). An error-disabled port would block all connectivity.
D). A duplicate IP would cause general network issues, not just missing server access.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - VLAN misconfiguration, connectivity issues.

NEW QUESTION: 91
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).

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
A network administrator is trying to troubleshoot an issue with a newly installed switch that is not connecting to the network. The administrator logs on to the switch and observes collisions on the interface. Which of the following is most likely the issue?
A. Wrong speed
B. Jumbo frames enabled
C. Incorrect VLAN
D. Duplex mismatch
Answer: (SHOW ANSWER)
The most likely issue is a duplex mismatch, which is a well-documented cause of collisions and poor network performance, as outlined in the CompTIA Network+ N10-009 troubleshooting objectives. A duplex mismatch occurs when one end of a network link is configured for full duplex while the other end is operating in half duplex. In half-duplex mode, devices must take turns transmitting and receiving data, which inherently allows for collisions. When paired with a full-duplex device-which expects simultaneous send and receive- collisions and retransmissions occur frequently.
The presence of collisions on a switch interface is a key diagnostic clue. Modern Ethernet switches operating correctly in full duplex should not experience collisions at all. When collisions are observed, it almost always points to a duplex configuration issue, often caused by manual speed/duplex settings on one device and auto- negotiation on the other.
A wrong speed setting may prevent link establishment entirely or cause errors, but it does not typically result in collisions. Jumbo frames can cause packet drops or fragmentation issues, not collisions. An incorrect VLAN configuration affects logical segmentation and connectivity but operates at Layer 2 and does not generate collisions.
CompTIA Network+ emphasizes duplex mismatch as a classic and frequently tested troubleshooting scenario.
Correcting it-usually by enabling auto-negotiation on both ends-restores normal, collision-free communication.

NEW QUESTION: 93
A network administrator is troubleshooting a connectivity issue between two devices on two different subnets.
The administrator verifies that both devices can successfully ping other devices on the same subnet. Which of the following is the most likely cause of the connectivity issue?
A. Incorrect default gateway
B. Faulty Ethernet cable
C. Wrong duplex settings
D. VLAN mismatch
Answer: (SHOW ANSWER)
When two devices on different subnets are unable to communicate, but can communicate with other devices on their own subnet, the issue is most often related to routing. Devices on different subnets require a default gateway to route traffic between networks.
If the default gateway is incorrectly configured, the device won't know how to reach other subnets.
Faulty cables (Option B) or duplex mismatches (Option C) would likely cause connectivity issues even within the local subnet, which is not the case here.
VLAN mismatches (Option D) are typically issues with switch port configurations and would likely cause total loss of connectivity, including within the same subnet.
So, the most probable and logical cause is an incorrect default gateway.

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

NEW QUESTION: 94
An organization wants better network visibility. The organization's requirements include:
Multivendor/OS-monitoring capabilities
Real-time collection
Data correlation
Which of the following meets these requirements?
A. SNMP
B. SIEM
C. Nmap
D. Syslog
Answer: (SHOW ANSWER)
A Security Information and Event Management (SIEM) system collects, correlates, and analyzes logs from multiple sources in real-time, providing enhanced visibility across multivendor environments.
Breakdown of Options:
A). SNMP - SNMP is used for network device monitoring, but it lacks real-time correlation across multiple vendors.
B). SIEM - Correct answer. SIEM aggregates, analyzes, and correlates logs from multiple sources, providing real-time visibility.
C). Nmap - Nmap is a network scanning tool used for mapping hosts and detecting open ports but does not provide log correlation.
D). Syslog - Syslog collects logs but does not correlate or analyze them in real-time.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.3: Explain network security concepts.
NIST Special Publication 800-92: Guide to Computer Security Log Management

NEW QUESTION: 95
Which of the following is used to stage copies of a website closer to geographically dispersed users?
A. VPN
B. CDN
C. SAN
D. SDN
Answer: (SHOW ANSWER)
A Content Delivery Network (CDN) caches website content across multiple geographically distributed servers to reduce latency and improve load times for users worldwide.
Breakdown of Options:
A). VPN - Encrypts network connections, does not distribute website content.
B). CDN - # Correct answer. A network of caching servers that delivers web content faster.
C). SAN - Storage Area Network, not related to web content distribution.
D). SDN - Software-defined networking, which controls network flows but does not stage website content.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.5: Compare and contrast different networking services.

NEW QUESTION: 96

Which of the following panels would be best to facilitate a central termination point for all network cables on the floor of a company building?
A. Patch
B. UPS
C. MDF
D. Rack
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Installation section.

NEW QUESTION: 97
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: 98
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: 99
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: 100
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?
Freecram.net
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: 101
A network administrator recently updated configurations on a Layer 3 switch. Following the updates, users report being unable to reach a specific file server. Which of the following is the most likely cause?
A. Incorrect ACLs
B. Switching loop
C. Duplicate IP addresses
D. Wrong default route
Answer: A (LEAVE A REPLY)
*Since this issue occurred after a configuration change on a Layer 3 switch, the most likely cause is misconfigured ACLs (Access Control Lists).
*ACLs control which traffic is allowed or denied, so an incorrect ACL may be blocking access to the file server.
*Why not the other options?
*Switching loop (B): A switching loop occurs at Layer 2 (not Layer 3) and causes network-wide broadcast storms, not just loss of access to a file server.
*Duplicate IP addresses (C): This would cause connectivity issues for the devices with the conflict, but not necessarily prevent all users from accessing the file server.
*Wrong default route (D): The default route is used for traffic leaving the local network. If users are unable to access an internal file server, this is unlikely to be the issue.
Reference:
CompTIA Network+ (N10-009) Official Guide - Chapter 8: Network Access Control and ACLs

NEW QUESTION: 102
Which of the following allows a user to connect to an isolated device on a stand-alone network?
A. Jump box
B. API gateway
C. Secure Shell (SSH)
D. Clientless VPN
Answer: (SHOW ANSWER)
A jump box is a hardened system that provides secure access to isolated or sensitive devices on a separate network.
Breakdown of Options:
A). Jump box - # Correct answer. Acts as a middle point for secure remote access.
B). API gateway - Used for managing API calls, not remote access to isolated devices.
C). Secure Shell (SSH) - Requires direct connectivity, which may not be available for an isolated device.
D). Clientless VPN - Allows web-based VPN access, but does not guarantee access to isolated devices.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Implement secure remote access methods.

NEW QUESTION: 103
A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?
A. 802.1X
B. Access control list
C. Port security
D. MAC filtering

Answer: A (LEAVE A REPLY)
802.1X is a port-based network access control (PNAC) protocol that provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. It is widely used for secure network access, ensuring that only authenticated devices can access the network, whether they are connecting via wired or wireless means.
802.1X works in conjunction with an authentication server, such as RADIUS, to validate the credentials of devices trying to connect.References:CompTIA Network+ study materials.

NEW QUESTION: 104
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: 105
As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?
A. ARP spoofing
B. Evil twin
C. MAC flooding
D. DNS poisoning
Answer: (SHOW ANSWER)
* Definition of MAC Flooding:
* MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.
* Impact of MAC Flooding:
* CAM Table Overflow:When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.
* Switch Behavior:The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.
* Comparison with Other Attacks:
* ARP Spoofing:Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.
* Evil Twin:Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.
* DNS Poisoning:Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.
* Preventive Measures:
* Port Security:Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
* Network Segmentation:Use VLANs to segment network traffic and limit the impact of such attacks.
References:
* CompTIA Network+ study materials on network security threats and mitigation techniques.

NEW QUESTION: 106
Which of the following is the most likely reason an insurance brokerage would enforce VPN usage?
A. To encrypt sensitive data in transit
B. To secure the endpoint
C. To maintain contractual agreements
D. To comply with data retentin requirements
Answer: (SHOW ANSWER)
The most likely reason an insurance brokerage would enforce VPN usage is to encrypt sensitive data in transit. VPNs (Virtual Private Networks) create a secure tunnel between the user's device and the corporate network, ensuring that data is encrypted and protected from interception.
* Encryption: VPNs encrypt data, preventing unauthorized access and ensuring data privacy during transmission over public or unsecured networks.
* Data Protection: Essential for industries handling sensitive information, such as insurance brokerages, to protect customer data and comply with regulatory requirements.
* Security: Enhances overall network security by providing secure remote access for employees.
Network References:
* CompTIA Network+ N10-007 Official Certification Guide: Discusses the role of VPNs in securing data in transit.
* Cisco Networking Academy: Provides training on VPN technologies and their importance in data security.
* Network+ Certification All-in-One Exam Guide: Explains VPN usage and its benefits in protecting sensitive information.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 107
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: 108

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

NEW QUESTION: 109
Which of the following connectors provides console access to a switch?
A. ST
B. RJ45
C. BNC
D. SFP
Answer: (SHOW ANSWER)
Console Access:
Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.
RJ45 Connector:
Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.
Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).
Comparison with Other Connectors:
ST (Straight Tip): A fiber optic connector used for networking, not for console access.
BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.
SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.
Practical Application:
Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).
References:
CompTIA Network+ study materials on network devices and connectors.

NEW QUESTION: 110
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: 111
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: D (LEAVE A REPLY)
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: 112
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: 113
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: 114
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: (SHOW ANSWER)
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: 115
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.

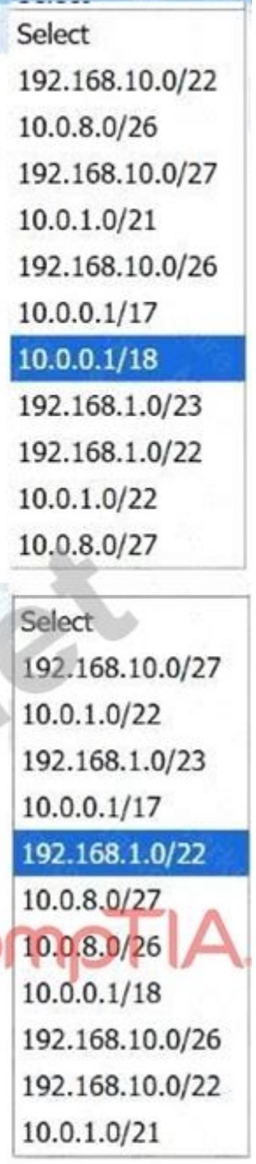
NEW QUESTION: 116

Company C is acquiring Company A and Company B. Company C needs to merge all three networks into one Class B network. Additionally, the network capacity of each company needs to grow by 20%. Company C also requires segmentation of Company A and Company B to account for unknown security vulnerabilities within each.

Instructions:

Select the correct subnet range to meet Company C ' s requirements.

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select
B	100	192.168.1.1/22	Select
C	10,000	10.0.0.1/8	Select



freecram.net
CompTIA

192.168.10.0/26
192.168.10.0/22
10.0.1.0/21

Answer:

freecram.net

Explanation:
A = 192.168.10.0/26
B = 192.168.1.0/23
C = 10.0.0.1/18
Using the choices shown in the screenshot, the best-fit subnet selections are based on host growth requirements first, then segmentation .
For Company A , the current device count is 32 . With 20% growth , that becomes about 39 devices . A /27 only supports 30 usable hosts , so it is too small. A /26 supports 62 usable hosts , so 192.168.10.0/26 is the correct choice.
For Company B , the current device count is 100 . With 20% growth , that becomes 120 devices . The smallest correct subnet would normally be a /25 with 126 usable hosts , but that option is not shown. From the available choices, 192.168.1.0/23 is the smallest subnet that still supports more than 120 hosts, so that is the best answer.
For Company C , the current device count is 10,000 . With 20% growth , it needs space for 12,000 hosts . A
/18 provides 16,382 usable hosts , while a /19 is not available and a /21 or /22 would be far too small.
Therefore, 10.0.0.1/18 is the correct selection.
One important note: the dropdown choices shown do not actually let all three companies be placed into a single true Class B network block. So these answers are the best valid selections from the provided options .

NEW QUESTION: 117
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: 118
A network administrator recently configured an autonomous wireless AP and performed a throughput test via comptiaspeedtester.com. The result was 75 Mbps. When connected to other APs, the results reached 500 Mbps. Which of the following is most likely the reason for this difference?
A. Channel width configuration
B. DNS server issues
C. Authentication failure
D. Incorrect DHCP settings
Answer: (SHOW ANSWER)

The channel width (20 MHz vs. 40 MHz vs. 80 MHz) directly impacts Wi-Fi throughput. If the AP is configured with a narrow channel width (e.g., 20 MHz), maximum data rates will be significantly lower than other APs using wider channels (e.g., 80 MHz). This matches the scenario where one AP achieves only ~75 Mbps, while others reach 500 Mbps.

* B. DNS issues affect name resolution, not raw throughput.
* C. Authentication failure would prevent connection, not reduce throughput.
* D. DHCP issues would prevent obtaining an IP, not cause slower speeds.

References (CompTIA Network+ N10-009):

* Domain: Network Troubleshooting - Wireless throughput issues, channel width configuration.

NEW QUESTION: 119

A network consultant needs to decide between running an ethernet uplink or using the built-in 5GHz-to-point functionality on a WAP. Which of the following documents provides the best information to assist the consultant with this decision?

A. Service-level agreement

B. Site survey results

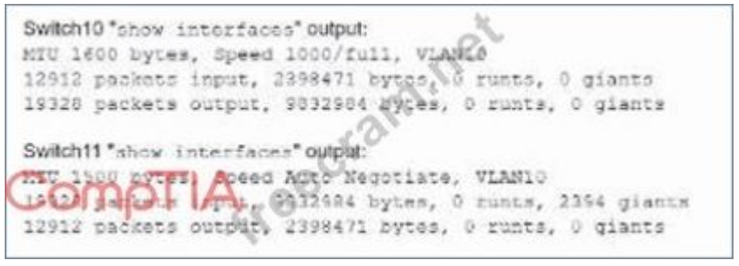
C. Physical diagram

D. Logical diagram

Answer: (SHOW ANSWER)

NEW QUESTION: 120

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. Configure STP on both switches.

B. Change the native VLAN on the ports.

C. Disable automatic negotiation on Switch11.

D. Modify Switch10 MTU value to 1500.

Answer: (SHOW ANSWER)

NEW QUESTION: 121

Which of the following would allow a network administrator to analyze attacks coming from the internet without affecting latency?

A. IPS

B. IDS

C. Load balancer

D. Firewall

Answer: (SHOW ANSWER)

An Intrusion Detection System (IDS) monitors and analyzes traffic to detect suspicious activity but does not sit in the traffic path, meaning it doesn't affect latency. In contrast, an IPS is in-

line and can introduce delay.
From Andrew Ramdayal's guide:
"IDS monitors and alerts on malicious activity but does not block traffic, making it suitable for environments where low latency is critical."

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 122
Which of the following types of routes takes precedence when building a routing table for a given subnet?
A. Static
B. BGP
C. OSPF
D. Default
Answer: A (LEAVE A REPLY)
The correct answer is Static because static routes have a lower administrative distance (AD) than most dynamic routing protocols, giving them higher priority when a router selects routes for the same destination network. According to CompTIA Network+ (N10-009) routing objectives, administrative distance is used to determine the trustworthiness of a route source when multiple routing protocols provide a path to the same subnet. The lower the administrative distance, the more preferred the route.
By default, a static route has an administrative distance of 1, which is lower than OSPF (110) and BGP (20 for eBGP, 200 for iBGP). Because of this, when identical routes to a subnet exist from both static and dynamic sources, the router installs the static route in the routing table.
A default route (0.0.0.0/0) is only used when no more specific route exists and does not take precedence over specific static or dynamic routes.
Therefore, when building the routing table for a given subnet and comparing route sources, static routes take precedence due to their lower administrative distance.

NEW QUESTION: 123
Which of the following is a type of NAC that uses a set of policies to allow or deny access to the network based on the user's identity?
A. Standard ACL
B. MAC filtering
C. 802.1X
D. SSO
Answer: (SHOW ANSWER)
802.1X is a port-based Network Access Control (NAC) method that enforces authentication before allowing access to the network. It uses a RADIUS server for identity verification and policy enforcement, ensuring only authorized users/devices gain access.
A). Standard ACL filters traffic by IP, not identity.
B). MAC filtering controls devices by hardware address but can be spoofed.
D). SSO (Single Sign-On) provides user convenience across services, not network-level access control.
References (CompTIA Network+ N10-009):
Domain: Network Security - NAC, 802.1X authentication, identity-based access.

NEW QUESTION: 124

Which of the following would describe a data recovery goal?
C. BCP
A. MTBF
D. MTTR
B. RPO
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: 125
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: 126
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: 127
Which of the following should be configured so users can authenticate to a wireless network using company credentials?
A. SSO
B. SAML
C. MFA
D. RADIUS
Answer: (SHOW ANSWER)
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.References:CompTIA Network+ study materials.

NEW QUESTION: 128
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: 129
A network engineer needs to deploy an access point at a remote office so that it will not communicate back to the wireless LAN controller. Which of the following deployment methods must the engineer use to accomplish this task?
A. Lightweight
B. Autonomous
C. Mesh
D. Ad hoc

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

NEW QUESTION: 130
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: 131
Which of the following is a use case for a PaaS environment?
A. Mobile access
B. E-commerce site
C. Application development
D. Cloud-native software
Answer: (SHOW ANSWER)
PaaS (Platform as a Service) is best suited for application development because it provides a managed platform that includes the runtime environment, development frameworks, middleware, databases (often), and build/deployment tooling. In a PaaS model, the cloud provider manages the underlying infrastructure (servers, storage, networking, OS patching, and often the application runtime), allowing developers to focus on writing code, testing, and releasing applications quickly. This aligns with Network+ cloud concepts where service models are compared by responsibility: PaaS reduces operational overhead for the customer and accelerates development through standardized environments and automation.
Mobile access is a use case for remote access solutions (VPN, zero trust access, MDM), not specifically PaaS.

An e-commerce site could be hosted using many models (IaaS, PaaS, SaaS), so it's not the most specific match. Cloud-native software describes an architectural style (microservices, containers, managed services) and can be built using PaaS components, but it is broader than a single "use case" and is not as directly tied to the PaaS definition as application development is. Therefore, application development is the clearest and most accurate PaaS use case.

NEW QUESTION: 132
Three access points have Ethernet that runs through the ceiling. One of the access points cannot reach the internet. Which of the following tools can help identify the issue?
A. Network tap
B. Cable tester
C. Visual fault locator
D. Toner and probe
Answer: (SHOW ANSWER)
A cable tester is a tool that can help identify issues with the physical cabling, such as breaks or improper terminations, which may prevent the access point from reaching the internet.

NEW QUESTION: 133
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: 134
An attacker gained access to the hosts file on an endpoint and modified it. Now, a user is redirected from the company's home page to a fraudulent website. Which of the following most likely happened?
A. DNS spoofing
B. Phishing
C. VLAN hopping
D. ARP poisoning

Answer: (SHOW ANSWER)
When the hosts file is altered, local name resolution is compromised, and domain queries are redirected to malicious IP addresses. This is a form of DNS spoofing/poisoning, where false mappings trick users into visiting fraudulent websites.
B). Phishing typically uses emails or messages to trick users, not local file modification.
C). VLAN hopping is a Layer 2 attack to gain unauthorized network access, unrelated to DNS.
D). ARP poisoning manipulates ARP tables on a LAN to reroute traffic, not name resolution.
References (CompTIA Network+ N10-009):
Domain: Network Security - DNS poisoning/spoofing, host file manipulation, endpoint attacks.

NEW QUESTION: 135
Which of the following protocols is used to route traffic on the public internet?
A. BGP
B. OSPF
C. EIGRP
D. RIP
Answer: (SHOW ANSWER)
Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).
Breakdown of Options:
A). BGP - Correct answer. Used for internet routing and exchanges routing information between ISPs.
B). OSPF - An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).
C). EIGRP - Cisco's proprietary IGP, used within private networks, not the public internet.
D). RIP - An older distance-vector protocol, not scalable for the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Explain routing technologies.
RFC 4271: Border Gateway Protocol 4 (BGP-4)

NEW QUESTION: 136
Which of the following facilities is the best example of a warm site in the event of information system disruption?
A. A combination of public and private cloud services to restore data
B. A partial infrastructure, software, and data on site
C. A full electrical infrastructure in place, but no customer devices on site
D. A full infrastructure in place, but no current data on site
Answer: (SHOW ANSWER)
A warm site typically has a full infrastructure ready, but it lacks the most up-to-date data or is not immediately operational. It requires some configuration or data restoration to become fully functional.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137
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: 138
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: 139
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: 140

A network administrator is troubleshooting issues with a DHCP server at a university. More students have recently arrived on campus, and the users are unable to obtain an IP address. Which of the following should the administrator do to address the issue?

Freecram.net

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

NEW QUESTION: 141
A network administrator needs to divide 192.168.1.0/24 into two equal halves. Which of the following subnet masks should the administrator use?
A. 255.255.0.0
B. 255.255.254.0
C. 255.255.255.0
D. 255.255.255.128
Answer: (SHOW ANSWER)
* Understanding Subnetting:
* Original Network: 192.168.1.0/24 has a subnet mask of 255.255.255.0, which allows for 256 IP addresses (including network and broadcast addresses).
* Objective: Divide this network into two equal subnets.
* Calculating Subnet Mask:
* New Subnet Mask: To divide 192.168.1.0/24 into two equal halves, we need to borrow one bit from the host portion of the address, changing the subnet mask to 255.255.255.128 (/25).
* Subnet Breakdown:
* First Subnet: 192.168.1.0/25 (192.168.1.0 - 192.168.1.127)
* Second Subnet: 192.168.1.128/25 (192.168.1.128 - 192.168.1.255)
* Verification:
* Each subnet now has 128 IP addresses (126 usable IP addresses, excluding the network and broadcast addresses).

* Comparison with Other Options:
* 255.255.0.0 (/16): Provides a much larger network, not dividing the original /24 network.
* 255.255.254.0 (/23): Also creates a larger subnet, encompassing more than the original /24 network.
* 255.255.255.0 (/24): Maintains the original subnet size, not dividing it.
References:
* CompTIA Network+ study materials on subnetting and IP addressing.

NEW QUESTION: 142
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: 143
A network administrator upgrades the wireless access points and wants to implement a configuration that gives users higher speed and less channel overlap based on device compatibility. Which of the following accomplishes this goal?
A. 802.1X
B. MIMO
C. ESSID
D. Band steering
Answer: (SHOW ANSWER)
The best solution here is band steering. Band steering allows modern wireless access points to automatically direct dual-band capable clients toward the 5 GHz band instead of the crowded 2.4 GHz band. The 5 GHz band has more available non-overlapping channels and can provide faster speeds with less interference, especially in dense environments. Devices that only support 2.4 GHz will remain on that band, while compatible devices enjoy the improved performance of 5 GHz.
A). 802.1X is a port-based network access control method for authentication. While important for security, it does not affect wireless channel utilization or client throughput.
B). MIMO (Multiple Input, Multiple Output) is a technology that improves throughput by using multiple antennas to send/receive simultaneously, but it does not actively steer clients between frequency bands.
C). ESSID (Extended Service Set Identifier) is just the network name for a set of APs in the same WLAN; it has no role in optimizing performance by band.
By implementing band steering, administrators reduce channel overlap on the 2.4 GHz band, improve spectral efficiency, and provide higher performance to capable devices, directly meeting the requirements described in the scenario.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - Wireless optimization, band steering, dual-band client management.

NEW QUESTION: 144
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: 145
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: 146
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: D (LEAVE A REPLY)
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: 147
Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?
A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.
Answer: A (LEAVE A REPLY)
To confirm a theory in the troubleshooting process, the technician should duplicate (replicate) the problem under controlled conditions. In the Network+ (N10-009) methodology, confirming a theory means validating that the suspected cause actually produces the observed symptoms. Replicating the issue helps ensure the technician is not chasing a coincidence, and it allows changes to be tested safely (for example, reproducing the issue with a specific user account, endpoint, cable, port, SSID, or configuration). If the problem can be duplicated, the technician can then try targeted actions to see whether the symptoms change in predictable ways-strengthening or disproving the hypothesis.
The other choices occur earlier as part of forming the theory. Identify the symptoms is an initial step to define the problem clearly. Gather information is part of the discovery phase-collect logs, error messages, topology details, and user observations. Determine any changes is also an early step used to correlate recent modifications (patches, new devices, config changes) with the onset of the issue. Those steps help create a theory; duplication helps confirm it before implementing a full fix.

NEW QUESTION: 148
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: 149
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: 150

A help desk technician receives a report that users cannot access Internet URLs. The technician performs ping tests and finds that sites fail when a URL is used but succeed when an IP is used. Which of the following tools should the technician utilize next?

Freecram.net

A. tcpdump

B. tracert

C. nmap

D. dig

Answer: (SHOW ANSWER)

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

* D. dig(Domain Information Groper) is a DNS lookup tool used to troubleshoot DNS problems by querying name servers directly.

Other tools are less relevant here:

* A. tcpdumpis a packet analyzer and is more advanced for deeper traffic analysis.

* B. tracertis used to trace the route to a destination, not ideal for DNS issues.

* C. nmapis a port scanner and network mapper, not for resolving DNS problems.

#Reference:

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

NEW QUESTION: 151

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

A. Security Service Edge

B. Data center interconnect

C. Infrastructure as code

D. Zero Trust architecture

Answer: (SHOW ANSWER)

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

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

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

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

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

References (CompTIA Network+ N10-009):

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

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
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: 153
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: 154
A network administrator has been tasked with configuring a network for a new corporate office. The office consists of two buildings, separated by 50 feet with no physical connectivity. The configuration must meet the following requirements:

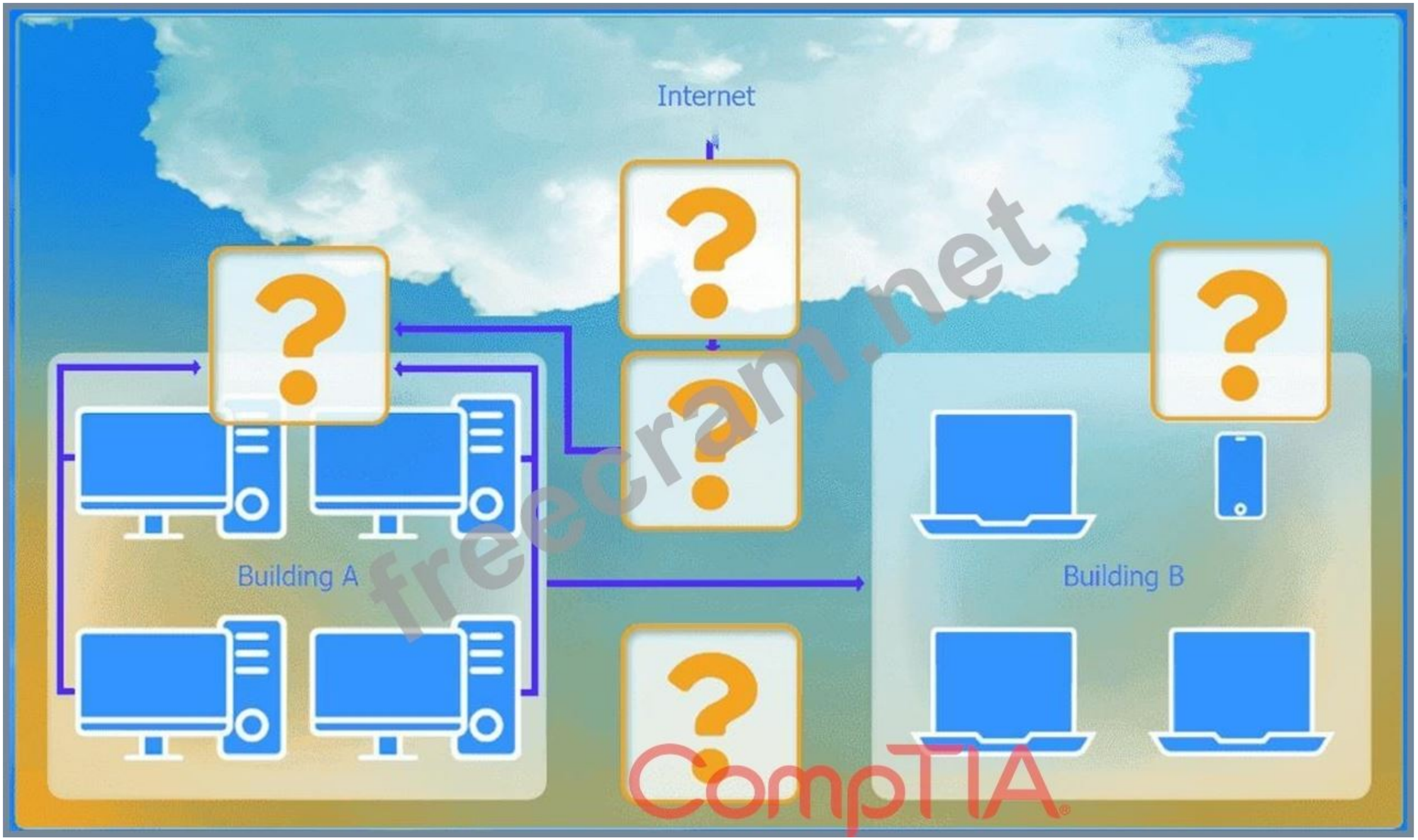
. Devices in both buildings should be
able to access the Internet.
. Security insists that all Internet traffic
be inspected before entering the
network.
. Desktops should not see traffic
destined for other devices.

INSTRUCTIONS

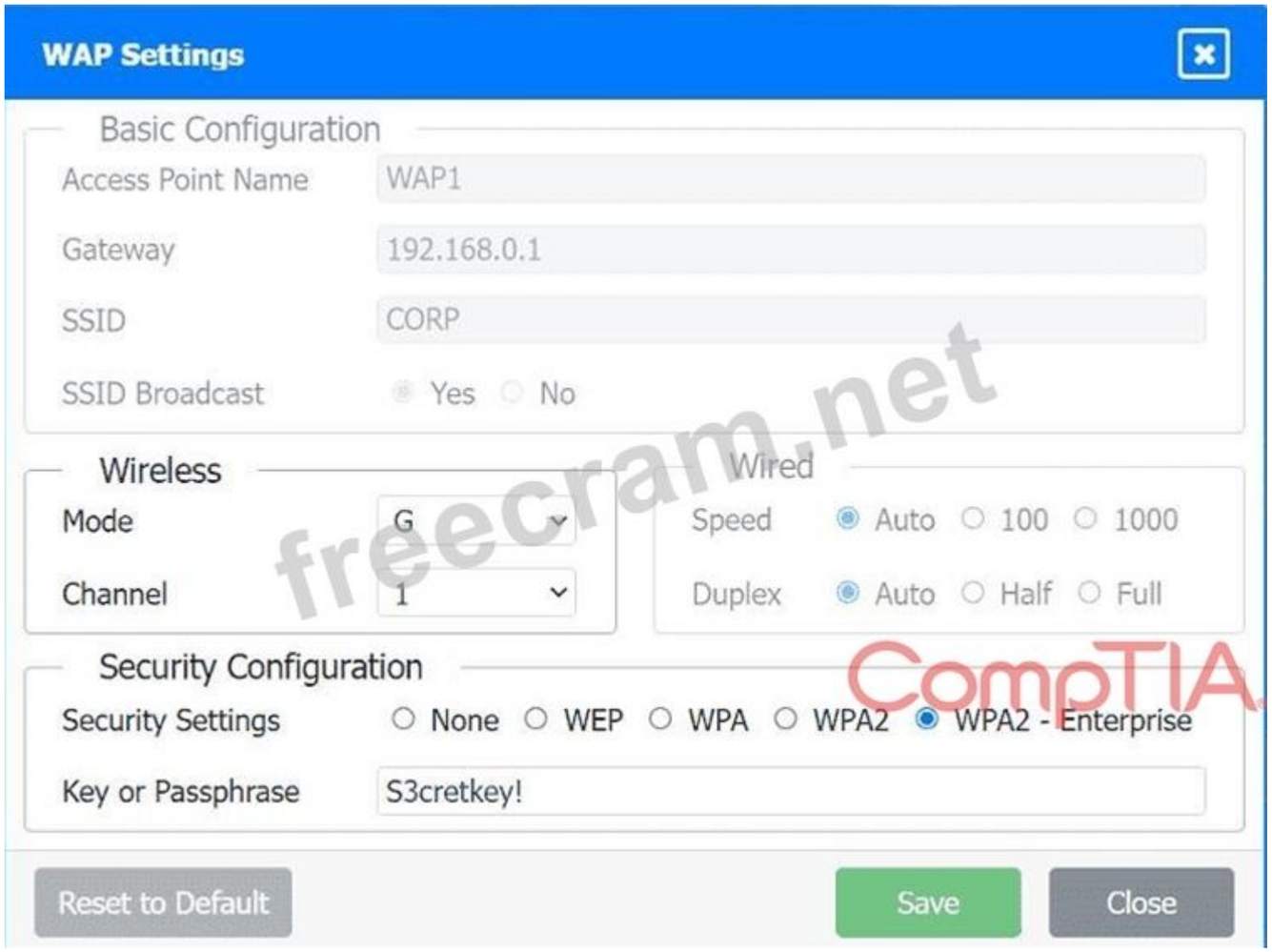
Select the appropriate network device for each location. If applicable, click on the magnifying glass next to any device which may require configuration updates and make any necessary changes.

Not all devices will be used, but all locations should be filled.

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


Internet
Building A
Building B

freecram.net
CompTIA
CompTIA
freecram.net



freecram.net
CompTIA

Answer:

See the step by step complete solution below.

Explanation:

Devices in both buildings should be able to access the Internet.

Security insists that all Internet traffic be inspected before entering the network.

Desktops should not see traffic destined for other devices.

Here is the corrected layout with explanation:

Building A:

Switch: Correctly placed to connect all desktops.

Firewall: Correctly placed to inspect all incoming and outgoing traffic.

Building B:

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

Between Buildings:

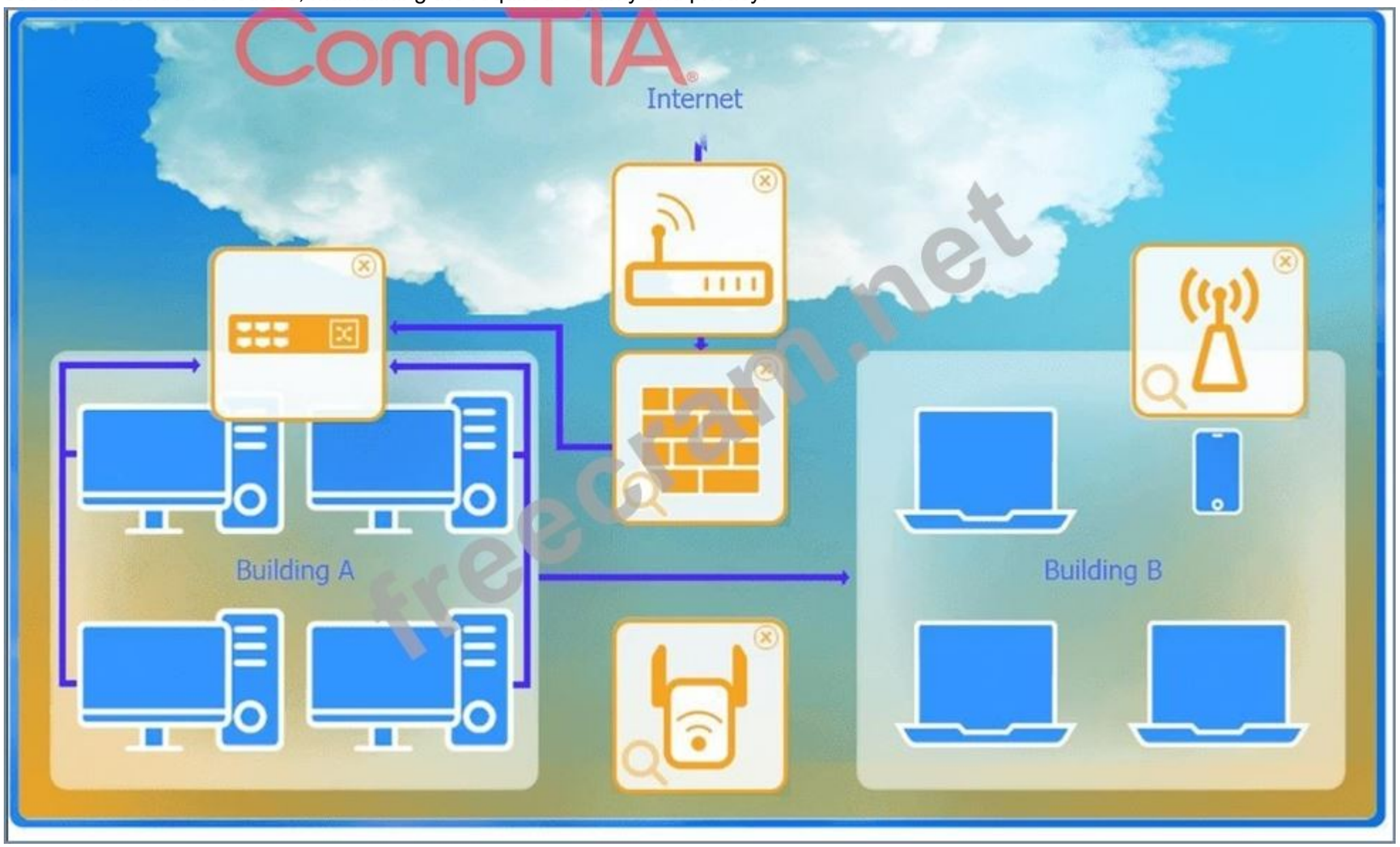
Wireless Range Extender: Correctly placed to provide connectivity between the buildings wirelessly.

Connection to the Internet:

Router: Correctly placed to connect to the Internet and route traffic between the buildings and the Internet.

Firewall: The firewall should be placed between the router and the internal network to inspect all traffic before it enters the network.

Corrected Setup:
Top-left (Building A): Switch
Bottom-left (Building A): Firewall (inspect traffic before it enters the network) Top-middle (Internet connection): Router Bottom-middle (between buildings): Wireless Range Extender Top-right (Building B): Wireless Access Point (WAP) In this corrected setup, the WAP in Building B will connect wirelessly to the Wireless Range Extender, which is connected to the Router. The Router is connected to the Firewall to ensure all traffic is inspected before it enters the network.
Configuration for Wireless Range Extender:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
With these settings, both buildings will have secure access to the Internet, and all traffic will be inspected by the firewall before entering the network. Desktops and other devices will not see traffic intended for others, maintaining the required security and privacy.



To configure the wireless range extender for security, follow these steps:
SSID (Service Set Identifier):

Ensure the SSID is set to " CORP " as shown in the exhibit.
Security Settings:
WPA2 or WPA2 - Enterprise: Choose one of these options for stronger security. WPA2-Enterprise provides more robust security with centralized authentication, which is ideal for a corporate environment.
Key or Passphrase:
If you select WPA2, enter a strong passphrase in the " Key or Passphrase " field.
If you select WPA2 - Enterprise, you will need to configure additional settings for authentication servers, such as RADIUS, which is not shown in the exhibit.
Wireless Mode and Channel:
Set the appropriate mode and channel based on your network design and the environment to avoid interference. These settings are not specified in the exhibit, so set them according to your network plan.
Wired Speed and Duplex:
Set the speed to " Auto " unless you have specific requirements for 100 or 1000 Mbps.
Set the duplex to " Auto " unless you need to specify half or full duplex based on your network equipment.
Save Configuration:
After making the necessary changes, click the " Save " button to apply the settings.
Here is how the configuration should look after adjustments:
SSID: CORP
Security Settings: WPA2 or WPA2 - Enterprise
Key or Passphrase: [Enter a strong passphrase]
Mode: [Set based on your network plan]
Channel: [Set based on your network plan]
Speed: Auto
Duplex: Auto
Once these settings are configured, your wireless range extender will provide secure connectivity for devices in both buildings.
Firewall setting to to ensure complete compliance with the requirements and best security practices, consider the following adjustments and additions:
DNS Rule: This rule allows DNS traffic from the internal network to any destination, which is fine.
HTTPS Outbound: This rule allows HTTPS traffic from the internal network (assuming 192.169.0.1/24 is a typo and should be 192.168.0.1/24) to any destination, which is also good for secure web browsing.
Management: This rule allows SSH access to the firewall for management purposes, which is necessary for administrative tasks.
HTTPS Inbound: This rule denies inbound HTTPS traffic to the internal network, which is good unless you have a web server that needs to be accessible from the internet.
HTTP Inbound: This rule denies inbound HTTP traffic to the internal network, which is correct for security purposes.
Suggested Additional Settings:
Permit General Outbound Traffic: Allow general outbound traffic for web access, email, etc.
Block All Other Traffic: Ensure that all other traffic is blocked to prevent unauthorized access.
Firewall Configuration Adjustments:
Correct the Network Typo:
Ensure that the subnet 192.169.0.1/24 is corrected to 192.168.0.1/24.
Permit General Outbound Traffic:
Rule Name: General Outbound
Source: 192.168.0.1/24
Destination: ANY

Service: ANY
Action: PERMIT
Deny All Other Traffic:
Rule Name: Block All
Source: ANY
Destination: ANY
Service: ANY
Action: DENY
Here is how your updated firewall settings should look:
Rule Name
Source
Destination
Service
Action
DNS Rule
192.168.0.1/24
ANY
DNS
PERMIT
HTTPS Outbound
192.168.0.1/24
ANY
HTTPS
PERMIT
Management
ANY
192.168.0.1/24
SSH
PERMIT
HTTPS Inbound
ANY
192.168.0.1/24
HTTPS
DENY
HTTP Inbound
ANY
192.168.0.1/24
HTTP
DENY
General Outbound
192.168.0.1/24

ANY
ANY
PERMIT
Block All
ANY
ANY
ANY
DENY
These settings ensure that:
Internal devices can access DNS and HTTPS services externally.
Management access via SSH is permitted.
Inbound HTTP and HTTPS traffic is denied unless otherwise specified.
General outbound traffic is allowed.
All other traffic is blocked by default, ensuring a secure environment.
Make sure to save the settings after making these adjustments.

NEW QUESTION: 155
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: 156
A network technician is installing a new switch that does not support STP at the access layer of a network.
The technician wants a redundant connection to the distribution switch. Which of the following should the technician use?
A. Link aggregation
B. Subinterfaces
C. Switch virtual interfaces
D. Half-duplex connections
Answer: (SHOW ANSWER)
Link aggregation(also known as port channeling or EtherChannel) allows multiple physical connections to act as one logical connection. This avoids loops that would typically be prevented by STP and provides redundancy and increased bandwidth. It's ideal when STP is not available or desirable.

Reference:Section 2.2 - Switching Technologies and Features - "Link Aggregation"

NEW QUESTION: 157
A network engineer queries a hostname using dig, and a valid IP address is returned. However, when the engineer queries that same IP address using dig, no hostname is returned. Which of the following DNS records is missing?
A. MX
B. CNAME
C. AAAA
D. PTR
Answer: (SHOW ANSWER)
This scenario describes a successful forward DNS lookup (hostname # IP address) but a failed reverse DNS lookup (IP address # hostname). Reverse lookups rely on a PTR (Pointer) record, which is stored in a reverse lookup zone (in-addr.arpa for IPv4, ip6.arpa for IPv6). If the engineer can resolve the hostname to an IP, that indicates an A record (or possibly AAAA for IPv6) exists and is functioning. But when querying the IP directly and receiving no hostname, the most likely issue is that the reverse mapping is not configured- meaning the PTR record is missing.
An MX record is used for mail exchange routing, not hostname resolution. A CNAME provides an alias from one hostname to another and does not create reverse mappings. An AAAA record maps a hostname to an IPv6 address; it is not used for reverse lookups of an IP to a name. Network+ objectives emphasize understanding common DNS record types and the difference between forward and reverse resolution, making PTR the correct missing record here.

NEW QUESTION: 158
Which of the following is most commonly associated with many systems sharing one IP address in the public IP-addressing space?
A. PAT
B. NAT
C. VIP
D. NAT64
Answer: (SHOW ANSWER)
Port Address Translation (PAT) allows multiple internal devices to share a single public IP address by assigning each device a unique port number. This is the most common method used in environments where many systems need internet access but there are limited public IP addresses.

NEW QUESTION: 159
A new SQL server is identified as allowing FTP access to all users. Which of the following would a systems administrator most likely do to ensure only the required services are allowed?
A. Disable unused ports on the server.
B. Change default passwords on all servers.
C. Delete the NGFW rules that allow all FTP traffic.
D. Configure server ACLs on the switches that the SQL traffic traverses.
Answer: (SHOW ANSWER)
If a SQL server is allowing FTP access to all users, the most direct and best practice action is to disable unused services/ports on the server itself. Network+ (N10-009) security objectives emphasize host hardening and the principle of least functionality: only required services should be running and listening. If FTP is not required for the SQL server's role, stopping and disabling the FTP service (and closing the associated ports on the host firewall) reduces the attack surface regardless of network firewall rules. This approach ensures the server cannot be reached via FTP even if it is placed on a different network segment or if upstream controls are misconfigured later.
Changing default passwords is important, but it does not address the unnecessary exposure of an unneeded service. Deleting NGFW rules that allow all FTP traffic could help at the perimeter, but it may unintentionally break legitimate FTP usage elsewhere and still doesn't guarantee the server isn't reachable from internal networks. Switch ACLs along SQL traffic

paths are indirect and easy to misapply; they also add operational complexity and may not cover all access paths. The best "only required services are allowed" control is to disable the unused service/ports on the server.

NEW QUESTION: 160

Pdfcram.net

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: 161

A network administrator needs to limit devices that can connect to a small wireless network. The network consists of less than ten unique laptops, and no network changes are anticipated. Which of the following is the simplest way to accomplish this task?

A. ACLs
B. MAC filtering
C. NAC
D. Trusted zones
Answer: (SHOW ANSWER)

The correct answer is B. MAC filtering. MAC filtering is a straightforward method of restricting network access by allowing only specific device MAC (Media Access Control) addresses to connect to a wireless network. In a small, stable environment with fewer than ten devices and no expected changes, this approach is simple to implement and manage.
Each network interface card (NIC) has a unique MAC address, and wireless access points can be configured with a whitelist of approved addresses. Devices not on the list are denied access, effectively limiting connectivity to only authorized laptops. This aligns with CompTIA Network+ guidance for basic access control mechanisms in small or low-complexity networks.
Other options are less suitable in this scenario. ACLs (Access Control Lists) are typically used on routers and switches to control traffic flow based on IP addresses or protocols, not specifically device access to a wireless network. NAC (Network Access Control) provides more advanced authentication and posture assessment but is more complex and unnecessary for a small, static environment. Trusted zones refer to network segmentation concepts rather than device-level access control.
Thus, MAC filtering provides the simplest and most appropriate solution.

NEW QUESTION: 162

After changes were made to a firewall, users are no longer able to access a web server. A network administrator wants to ensure that ports 80 and 443 on the web server are still accessible from the user IP space. Which of the following commands is best suited to perfom this testing?

A. Ping
B. Dig
C. nmap
D. Ifconfig
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following allows a standard user to log in to multiple resources with one account?
A. RADIUS
B. TACACS+
C. MFA
D. SSO
Answer: (SHOW ANSWER)

NEW QUESTION: 164
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: 165
A company's network is experiencing high levels of suspicious network traffic. The security team finds that the traffic is coming from an unknown, foreign IP address. Which of the following is the most cost-efficient way to mitigate this threat?
A. ACL
B. IDS
C. NAT
D. DoS prevention
Answer: (SHOW ANSWER)
The correct answer is ACL (Access Control List). According to the CompTIA Network+ N10-009 objectives, ACLs are a fundamental and cost-effective method for controlling traffic flow at routers and firewalls. An ACL allows administrators to permit or deny traffic based on source IP address, destination IP address, protocol, or port number.
In this scenario, the suspicious traffic is identified as originating from a specific unknown foreign IP address.
The most direct and economical mitigation strategy is to configure an ACL rule that denies traffic from that specific IP address (or subnet) at the network perimeter. This approach leverages existing network infrastructure without requiring additional hardware or licensing costs.
An IDS (Intrusion Detection System) monitors and alerts on malicious activity but does not actively block traffic unless paired with IPS functionality, and it may involve additional cost and complexity. NAT is used for address translation and does not provide traffic filtering based on threat intelligence. DoS prevention solutions are typically more advanced, specialized, and costly, often intended for large-scale distributed denial-of-service attacks rather than blocking traffic from a single suspicious IP.
The Network+ objectives emphasize implementing layered security controls, starting with simple and effective measures. In this case, applying an ACL at the firewall or router is the most cost-efficient and immediate method to mitigate the identified threat.

NEW QUESTION: 166
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167
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: 168
Which of the following is the most closely associated with segmenting compute resources within a single cloud account?
A. Network security group
B. IaaS
C. VPC
D. Hybrid cloud
Answer: (SHOW ANSWER)

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

NEW QUESTION: 169
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: 170
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?
Freecram.net
A. ping 127.0.0.1
B. ping 169.254.1.1
C. ping 172.16.1.1
D. ping 192.168.1.1
Answer: (SHOW ANSWER)
The loopback address 127.0.0.1 is used to test the TCP/IP stack of the local machine. Pinging this address confirms whether the local system's networking stack is functioning correctly.

NEW QUESTION: 171
Which of the following network topologies contains a direct connection between every node in the network?
A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point
Answer: (SHOW ANSWER)
In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.References:CompTIA Network+ study materials.

NEW QUESTION: 172
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: 173
A customer needs six usable IP addresses. Which of the following best meets this requirement?
A. 255.255.255.128
B. 255.255.255.192
C. 255.255.255.224
D. 255.255.255.240
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - IP Addressing section.

NEW QUESTION: 174
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: 175
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: 176
A network engineer needs to correlate findings and receive alerts if there are brute force attacks, DDoS attacks, or port scanning happening within their network. Which of the following network monitoring technologies should the engineer implement?
A. Packet capture
B. SNMPv3
C. SIEM
D. Syslog collector
Answer: (SHOW ANSWER)
A SIEM (Security Information and Event Management) platform is built to collect, correlate, and alert on security-relevant events across many sources, which is exactly what's needed to identify patterns such as brute force attempts, port scanning, and DDoS indicators. In Network+ (N10-009) security operations concepts, correlation is key: a SIEM can ingest logs from firewalls, IDS/IPS, servers, authentication systems, endpoint agents, and network devices, then apply rules/analytics to detect suspicious behavior that might not be obvious from a single log source. It can also generate real-time alerts, dashboards, and incident timelines-helping the engineer respond quickly and prioritize threats.
Packet capture provides deep visibility into traffic but is not inherently designed for enterprise-wide correlation and alerting without significant additional tooling and expertise. SNMPv3 is used for secure device monitoring (status, counters, performance) rather than detecting coordinated attack patterns. A syslog collector centralizes logs but generally does not provide the same level of correlation, enrichment, and automated alerting capabilities as a SIEM. Therefore, SIEM is the best answer.

NEW QUESTION: 177
Which of the following is the part of a disaster recovery (DR) plan that identifies the critical systems that should be recovered first after an incident?
A. RTO
B. SLA
C. MTBF
D. SIEM
Answer: (SHOW ANSWER)
RTO stands for Recovery Time Objective, which defines the maximum acceptable amount of time that a system, application, or function can be down after a failure or disaster. It helps prioritize which systems need to be recovered first based on their importance to business operations.
SLA (Service Level Agreement) refers to an agreement between a service provider and a customer regarding expected performance and availability, but it does not dictate recovery order.
MTBF (Mean Time Between Failures) is a measure of reliability and time between hardware or system failures.
SIEM (Security Information and Event Management) is a centralized tool for logging and alerting but not relevant to DR recovery prioritization.
Reference:
CompTIA Network+ N10-009 Official Objectives: 4.4 - Summarize business continuity and disaster recovery concepts.
NEW QUESTION: 178
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: 179
Users at an organization report that the wireless network is not working in some areas of the building. Users report that other wireless network SSIDs are visible when searching for the network, but the organization's network is not displayed. Which of the following is the most likely cause?
A. Interference or channel overlap
B. Insufficient wireless coverage
C. Roaming misconfiguration
D. Client disassociation issues
Answer: (SHOW ANSWER)
If the company's SSID is not visible in some areas while other networks are still visible, the most likely cause is insufficient wireless coverage. The wireless signal does not reach those areas, meaning additional access points or signal boosters may be required.
Breakdown of Options:
A: Interference or channel overlap - Would cause slow or unstable connections, but the SSID should still be visible.
B: Insufficient wireless coverage - # Correct answer. If the SSID is not appearing, the signal is too weak in that area.
C: Roaming misconfiguration - Would cause devices to stay on weaker APs instead of switching, but the SSID should still be visible.
D: Client disassociation issues - This would disconnect users, but they should still see the network.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 1.6: Explain wireless concepts and technologies.

NEW QUESTION: 180
Which of the following should be used to obtain remote access to a network appliance that has failed to start up properly?
FreeCram.net
A. Crash cart
B. Jump box
C. Secure Shell (SSH)
D. Out-of-band management
Answer: (SHOW ANSWER)
If a network appliance fails to start, standard remote access methods like SSH won't work. Instead, Out-of- Band (OOB) management provides a dedicated access path (e.g., a console port or iDRAC/iLO), allowing administrators to troubleshoot devices even when the network is down.
Breakdown of Options:
A). Crash cart - A physical monitor/keyboard setup, not a remote solution.
B). Jump box - A hardened system used for secure remote access but requires the device to be operational.
C). Secure Shell (SSH) - Requires the device to be fully booted and network-connected.
D). Out-of-band management - # Correct answer. Provides independent access for troubleshooting failed network devices.

Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network device management concepts.

NEW QUESTION: 181
A company wants to implement data loss prevention by restricting user access to social media platforms and personal cloud storage on workstations. Which of the following types of filtering should the company deploy to achieve these goals?
A. Port
B. DNS
C. MAC
D. Content
Answer: (SHOW ANSWER)
Reference: CompTIA Network+ Certification Exam Objectives - Network Security section.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182
A secure communication link needs to be configured between data centers via the internet. The data centers are located in different regions. Which of the following is the best protocol for the network administrator to use?
A. DCI
B. GRE
C. VXLAN
D. IPSec
Answer: (SHOW ANSWER)
IPSec (Internet Protocol Security) is the best choice for secure communication over the internet, as it provides encryption, authentication, and data integrity. It is widely used in VPNs and site-to-site secure tunnels.
Breakdown of Options:
A). DCI (Data Center Interconnect) - A general term for linking data centers, but it doesn't specify a secure tunneling protocol.
B). GRE (Generic Routing Encapsulation) - Encapsulates traffic but lacks encryption, making it less secure than IPSec.
C). VXLAN (Virtual Extensible LAN) - Used for Layer 2 network overlays, not for securing communication over the internet.
D). IPSec - # Correct answer. Provides encryption, authentication, and integrity for data over the internet.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 3.5: Implement secure remote access methods.
RFC 4301: Security Architecture for the Internet Protocol

NEW QUESTION: 183
Which of the following would most likely be utilized to implement encryption in transit when using HTTPS?
A. SSH

B. TLS
C. SCADA
D. RADIUS
Answer: (SHOW ANSWER)
TLS (Transport Layer Security)is the protocol that providesencryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.
* A. SSHis used for secure terminal access, not HTTPS.
* C. SCADArefers to control systems, not encryption protocols.
* D. RADIUSis an authentication protocol, not for encrypting HTTPS traffic.
#Reference:
CompTIA Network+ N10-009 Official Objectives: 4.2 - Identify common security threats and vulnerabilities.
CompTIA Network+ N10-009 Official Objectives: 4.6 - Explain authentication and access controls.

NEW QUESTION: 184
A client with a 2.4GHz wireless network has stated that the entire office is experiencing intermittent issues with laptops after the WAP was moved. Which of the following is the most likely reason for these issues?
A. The network uses a non-overlapping channel.
B. The signal is reflecting too much.
C. The network has excessive noise.
D. A microwave is in the office.
Answer: D (LEAVE A REPLY)
Microwaves are known to interfere with the 2.4GHz frequency, which is the same frequency used by many wireless networks. This can cause signal degradation and intermittent connectivity issues, especially if the WAP is placed near such devices.

NEW QUESTION: 185
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: 186
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: 187
A network engineer deploys ten new virtual servers and configures the NICs. Which of the following should the engineer update?
A. Asset inventory
B. Warranty support
C. Rack diagrams
D. IP address management
Answer: (SHOW ANSWER)
The correct answer is D. IP address management . In the CompTIA Network+ N10-009 objectives, network documentation and operational procedures include maintaining accurate records for addressing, device configurations, and infrastructure changes. When a network engineer deploys new virtual servers and configures their NICs, the most directly affected documentation is the IP address management , often called IPAM. IPAM tracks assigned IP addresses, subnets, gateways, DNS settings, DHCP reservations, static assignments, and address availability.
Because the scenario specifically states that the engineer configured the NICs , the key networking detail is that each virtual server's network interface likely received IP addressing information. Updating IP address management prevents duplicate IP assignments, supports troubleshooting, and helps administrators understand which addresses are in use across the environment.
The other options are less appropriate. Asset inventory may need updating when new servers are created, but the question emphasizes NIC configuration, making IPAM the better answer. Warranty support applies mainly to physical hardware and vendor support contracts, which is not the main concern for virtual servers.
Rack diagrams document physical rack placement, power, and cabling, but virtual servers do not occupy rack space individually. Therefore, the best documentation to update after configuring NICs on new virtual servers is IP address management .

NEW QUESTION: 188
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: 189
Which of the following should a company implement in order to share a single IP address among all the employees in the office?
A. STP
B. BGP
C. PAT
D. VXLAN
Answer: (SHOW ANSWER)
PAT (Port Address Translation) allows multiple devices on a local network to share a single public IP address when accessing the internet. It translates the private IP addresses to a single public IP with different port numbers for each session. The document states:
"PAT (Port Address Translation) allows multiple devices on a LAN to share a single public IP address by assigning unique port numbers to each session, enabling internet connectivity for all devices."

NEW QUESTION: 190
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?
Freecram.net
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: 191
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: 192
Which of the following protocols is commonly associated with TCP port 443?
A. Telnet
B. SMTP
C. HTTPS
D. SNMP
Answer: C (LEAVE A REPLY)
TCP port 443 is reserved for HTTPS (Hypertext Transfer Protocol Secure), which uses TLS encryption to secure web traffic. It is the standard port for encrypted web communications.
A). Telnet uses TCP port 23.
B). SMTP commonly uses TCP ports 25, 465, or 587.
D). SNMP typically uses UDP ports 161 (queries) and 162 (traps).
References (CompTIA Network+ N10-009):
Domain: Network Standards, Protocols, and Implementations - Common ports and services.

NEW QUESTION: 193
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: 194
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: A (LEAVE A REPLY)
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: 195
A firewall administrator is mapping a server's internal IP address to an external IP address for public use.
Which of the following is the name of this function?
A. NAT
B. VIP
C. PAT
D. BGP
Answer: (SHOW ANSWER)
Network Address Translation (NAT) is a process that allows a device, typically a firewall or router, to map private IP addresses to public IP addresses. This enables internal network devices to communicate over the internet using a single or a limited number of public IP addresses.
Static NAT (One-to-One Mapping): Maps a single private IP address to a single public IP address, commonly used for servers that need to be accessible from the internet.
Dynamic NAT (Many-to-Many Mapping): Dynamically assigns a public IP from a pool to internal devices.
PAT (Port Address Translation): A type of NAT where multiple private IPs share a single public IP using different port numbers.
Incorrect Options:
B). VIP (Virtual IP Address): Used in load balancing and high-availability configurations, not for NAT.
C). PAT (Port Address Translation): A specific form of NAT, but the question refers to general NAT, making option A the best choice.
D). BGP (Border Gateway Protocol): A routing protocol used to exchange information between different networks, not related to NAT.
Reference:
CompTIA Network+ N10-009 Official Study Guide - Chapter on Network Address Translation (NAT)

NEW QUESTION: 196
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.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 197
A company recently implemented a videoconferencing system that utilizes large amounts of bandwidth. Users start reporting slow internet speeds and an overall decrease in network performance. Which of the following are most likely the causes of the network performance issues? (Select two)
A. DNS misconfiguration
B. Inadequate network security
C. Malware or a virus
D. Outdated software
E. Incorrect QoS settings
F. Network congestion
Answer: (SHOW ANSWER)
When high-bandwidth services like videoconferencing are introduced, two primary factors may degrade performance:
Incorrect QoS Settings (E):QoS (Quality of Service) is used to prioritize traffic. If not configured correctly, critical services like video may not get the necessary bandwidth and prioritization.
Network Congestion (F):Video services consume large amounts of data. If the network doesn't have sufficient bandwidth or is not segmented properly, congestion will slow down all services.
DNS misconfiguration (A) would affect name resolution, not bandwidth.
Malware (C) could degrade performance, but is not tied to the described scenario.
Outdated software (D) may affect performance in some cases, but not directly linked to network congestion in this case.
Inadequate network security (B) isn't likely to cause general slowness related to video traffic.
So, the most likely culprits are E. Incorrect QoS settings and F. Network congestion.
Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 2.5: "Explain common performance concepts and issues."

NEW QUESTION: 198
A data center interconnect using a VXLAN was recently implemented. A network engineer observes slow performance and fragmentation on the interconnect. Which of the following technologies will resolve the issue?
A. 802.1Q tagging
B. Spanning tree
C. Link aggregation
D. Jumbo frames
Answer: (SHOW ANSWER)
VXLAN (Virtual Extensible LAN) encapsulates Ethernet frames inside UDP packets, increasing packet size.
This can lead to fragmentation and performance degradation unless Jumbo Frames are enabled.
Breakdown of Options:
A). 802.1Q tagging - VLAN tagging enables segmentation but does not address fragmentation issues.

B). Spanning tree - STP prevents loops but does not improve performance for VXLAN traffic.
C). Link aggregation - LACP combines links for higher bandwidth but does not prevent fragmentation.
D). Jumbo frames - Correct answer. Enabling Jumbo Frames allows larger packet sizes, reducing fragmentation and improving VXLAN performance.
Reference:
CompTIA Network+ (N10-009) Official Study Guide - Domain 2.3: Explain network performance concepts.
RFC 7348: VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks

NEW QUESTION: 199
Which of the following cable types allows the use of QSFP ports without requiring transceivers?
A. Multimode
B. Twinaxial
C. RG11
D. Category 6
Answer: B (LEAVE A REPLY)
Twinaxial (Direct Attach Copper / DAC) cables can plug directly into QSFP ports without needing separate optical transceivers. They are cost-effective for short-distance, high-speed connections (commonly in data centers).
A). Multimode fiber requires SFP/QSFP transceivers to convert electrical signals to optical.
C). RG11 is coaxial cable for broadband/cable TV, not used in QSFP ports.
D). Category 6 is twisted-pair Ethernet cabling, not directly compatible with QSFP ports.
References (CompTIA Network+ N10-009):
Domain: Network Infrastructure - Cable types, QSFP, DAC (Twinaxial), transceiver requirements.

NEW QUESTION: 200
A network technician sets up a computer on the accounting department floor for a user from the marketing department. The user reports that they cannot access the marketing department's shared drives but can access the internet. Which of the following is the most likely cause of this issue?
Freecram.net
A. Mismatched switchport duplex
B. Misconfigured gateway settings
C. Incorrect VLAN assignment
D. SVI is assigned to the wrong IP address
Answer: (SHOW ANSWER)
The user's inability to access the marketing department's shared drives, despite having internet access, suggests a network segmentation issue. The most likely cause is an incorrect VLAN assignment. The computer is physically located on the accounting department floor, and the switchport is likely configured for the accounting VLAN, not the marketing VLAN. VLANs segment network traffic, and if the computer is in the wrong VLAN, it cannot communicate with the marketing department's resources.
Why not Mismatched switchport duplex? Duplex mismatches cause performance issues (e.g., packet loss) but not specific access denials to shared drives.
Why not Misconfigured gateway settings? Incorrect gateway settings would prevent internet access, which the user has.
Why not SVI is assigned to the wrong IP address? A Switch Virtual Interface (SVI) with an incorrect IP address affects inter-VLAN routing, but this would likely impact multiple users, not just one.
Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) explains that VLANs isolate traffic, and incorrect VLAN assignments prevent access to resources on other VLANs.

NEW QUESTION: 201

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: 202
Which of the following VPN configurations forces a remote user to access internet resources through the corporate network?
A. Clientless
B. Site-to-site
C. SSE
D. Full-tunnel
Answer: (SHOW ANSWER)
A full-tunnel VPN forces a remote user's traffic-including access to public internet resources-to traverse the corporate VPN tunnel and egress from the organization's network. This is commonly required to ensure consistent enforcement of corporate security controls such as web filtering, IDS/IPS inspection, DLP policies, logging, and access control. In Network+ terms, full-tunnel VPNing routes the user's default gateway through the VPN, meaning both internal traffic (to corporate subnets) and external traffic (to internet destinations) is sent through the encrypted tunnel.
By contrast, a split-tunnel VPN (not listed) would send only corporate-bound traffic through the VPN while allowing internet traffic to go directly out the user's local ISP-reducing corporate bandwidth usage but also reducing centralized inspection and control. Clientless VPN usually refers to browser-based access to specific internal applications without a full network tunnel for all traffic. Site-to-site VPN connects entire networks to each other (e.g., branch office to HQ) rather than an individual remote user. SSE (Security Service Edge) is a cloud security framework/service model, not the classic VPN configuration described in the question. Hence, full-tunnel is the correct answer.

NEW QUESTION: 203
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: 204
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: 205
A network engineer connects a business to a new ISP. A simple ping test to 8.8.8.8 is successful. However, users complain of extreme slowness to any website and periods of no connectivity. Which of the following is the most likely cause?
A. Incorrect default gateway
B. VLAN mismatch
C. Subnet mask configuration
D. Duplicate ISP IP address
Answer: D (LEAVE A REPLY)
If the business shares or duplicates the ISP-assigned public IP address, routing instability and conflicts will occur. Pinging a public IP like 8.8.8.8 may work (since ICMP can bypass certain conflicts), but browsing websites (which requires stable sessions and return traffic) will fail intermittently.
A). If the default gateway were incorrect, no external connectivity would work at all.
B). VLAN mismatch is an internal issue, not affecting ISP routing.
C). Subnet mask misconfiguration would prevent consistent routing but usually blocks ping too.

References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Internet connectivity issues, ISP IP conflicts.

NEW QUESTION: 206
Users report that they cannot print to a specific IPv4-enabled printer after an extended power outage. Which of the following should a technician configure?
A. DoH
B. SLAAC
C. APIPA
D. DHCP reservation
Answer: (SHOW ANSWER)
The correct answer is D. DHCP reservation. In a network environment, printers are typically configured to use a consistent IP address so that client devices can reliably locate them. After a power outage, network devices such as printers may reboot and request a new IP address from the DHCP server. If the printer was previously assigned a dynamic IP address, it may now receive a different address, causing users' systems to lose connectivity because they are still trying to print to the old IP.
A DHCP reservation ensures that a specific device (identified by its MAC address) always receives the same IP address from the DHCP server. This combines the convenience of DHCP with the stability of static addressing, which is ideal for shared resources like printers.
The other options are incorrect for this scenario. DoH (DNS over HTTPS) secures DNS queries and is unrelated to IP address assignment. SLAAC (Stateless Address Autoconfiguration) is used for IPv6, not IPv4 environments. APIPA (Automatic Private IP Addressing) assigns a link-local address when DHCP fails, but it does not provide consistent or routable addressing suitable for shared printers.
Therefore, configuring a DHCP reservation ensures consistent network access to the printer after power disruptions.

NEW QUESTION: 207
A company's marketing team created a new application and would like to create a DNS record for newapplication.comptia.org that always resolves to the same address as www.comptia.org. Which of the following records should the administrator use?
A. SOA
B. MX
C. CNAME
D. NS
Answer: (SHOW ANSWER)
A CNAME (Canonical Name) record is used in DNS to alias one domain name to another. This means that newapplication.comptia.org can be made to resolve to the same IP address as www.comptia.org by creating a CNAME record pointing newapplication.comptia.org to www.comptia.org. SOA (Start of Authority) is used for DNS zone information, MX (Mail Exchange) is for mail server records, and NS (Name Server) is for specifying authoritative DNS servers.
Reference:
The DNS section of the CompTIA Network+ materials describes the use of CNAME records for creating domain aliases.

NEW QUESTION: 208
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: 209

A network engineer is implementing a new connection between core switches. The engineer deploys the following configurations:

Core-SW01
vlan 100
name
interface Ethernet 1/1
channel-group 1 mode active
interface Ethernet 1/2
channel-group 1 mode active
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100

Core-SW02
vlan 100
name
interface Ethernet 1/1
switchport mode trunk
switchport trunk allow vlan 100
interface Ethernet 1/2
switchport mode trunk
switchport trunk allow vlan 100
interface port-channel 1
switchport mode trunk
switchport trunk allow vlan 100

Which of the following is the state of the Core-SW01 port-channel interfaces?

A. Incrementing CRC errors
B. Error disabled
C. Administratively down
D. Suspended

Answer: (SHOW ANSWER)

On Core-SW01, the ports are configured with LACP (mode active) for link aggregation. On Core-SW02, the ports are configured as independent trunks, not as part of an LACP group.

Because of this mismatch, LACP cannot form the bundle, and the aggregated ports on SW01 will go into a suspended state.

A). CRC errors suggest cabling or signal integrity issues, not config mismatch.

B). Error disabled occurs when a violation (like BPDU guard or port security) disables the port, not LACP mismatch.
C). Administratively down indicates a shutdown command, not the case here.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port-channel/LACP configuration issues, interface states.

NEW QUESTION: 210

Freecram.net

A company upgrades its network and PCs to gigabit speeds. After the upgrade, users are not getting the expected performance. Technicians discover that the speeds of the endpoint NICs are inconsistent. Which of the following should be checked first to troubleshoot the issue?

A. Speed mismatches
B. Load balancer settings
C. Flow control settings
D. Infrastructure cabling grade
Answer: (SHOW ANSWER)
Speed Mismatches: If NICs are set to different speeds (e.g., 100 Mbps on one side and 1 Gbps on the other), performance will degrade. Ensuring consistent speed settings between devices is crucial for optimal performance.
Load balancer settings (B): Applies to server load distribution, not endpoint speed.
Flow control settings (C): Can affect performance but is secondary to speed mismatches.
Infrastructure cabling grade (D): Relevant if the cables are unsuitable for gigabit speeds, but speed settings should be checked first.
Reference: CompTIA Network+ Official Study Guide, Domain 2.5 (Troubleshooting Network Issues).

NEW QUESTION: 211
A company recently converted most of the office laptops to connect wirelessly to the corporate network. After a high-traffic malware attack, narrowing the event to a specific user was difficult because of the wireless configuration.
Which of the following actions should the company take?
A. Restrict users to the 5GHz frequency.
B. Upgrade to a mesh network.
C. Migrate from PSK to Enterprise.
D. Implement WPA2 encryption.
Answer: (SHOW ANSWER)
Using Pre-Shared Key (PSK) authentication means that all users share the same Wi-Fi password, making it difficult to identify individual users when security incidents occur.
Migrating to WPA2-Enterprise (or WPA3-Enterprise) replaces PSK authentication with individual user credentials using 802.1X authentication and a RADIUS server. This allows the organization to:
Track and log specific user activity
Enforce per-user authentication policies
Improve network security
Breakdown of Options:
A). Restrict users to the 5GHz frequency - Improves performance but does not enhance user tracking or security.
B). Upgrade to a mesh network - A mesh network improves coverage, not security tracking.
C). Migrate from PSK to Enterprise - # Correct answer. WPA2-Enterprise or WPA3-Enterprise uses individual user authentication, allowing per-user tracking.
D). Implement WPA2 encryption - WPA2 is already widely used; it does not resolve the tracking issue.
Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.4: Given a scenario, implement wireless security measures.
IEEE 802.1X: Authentication framework for network access control

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 212
Which of the following allows an organization to map multiple internal devices to a single external-facing IP address?
A. NAT
B. BGP
C. OSPF
D. FHRP
Answer: A (LEAVE A REPLY)
NAT (Network Address Translation) allows multiple private IP addresses to share a single public IP when accessing the internet. This conserves public IPs and provides basic security by hiding internal addresses.
B). BGP is a routing protocol.
C). OSPF is a link-state IGP.
D). FHRP provides redundant gateways, not IP sharing.
References (CompTIA Network+ N10-009):
Domain: Networking Concepts - NAT, PAT, private-to-public IP mapping.

NEW QUESTION: 213
Which of the following most likely determines the size of a rack for installation? (Select two).
A. KVM size
B. Switch depth
C. Hard drive size
D. Cooling fan speed
E. Outlet amperage
F. Server height
Answer: (SHOW ANSWER)
Understanding Rack Size Determination:
The size of a rack for installation is determined by the dimensions of the equipment to be housed in it, primarily focusing on the depth and height of the devices.
Switch Depth:
Depth of Equipment: The depth of network switches and other rack-mounted devices directly influences the depth of the rack. If the equipment is deeper, a deeper rack is required to accommodate it.
Industry Standards: Most racks come in standard depths, but it is essential to match the depth of the rack to the deepest piece of equipment to ensure proper fit and airflow.
Server Height:
Height of Equipment: The height of servers and other devices is measured in rack units (U), where 1U equals

1.75 inches. The total height of all equipment determines the overall height requirement of the rack.
Rack Units: A rack's height is typically described in terms of the number of rack units it can accommodate, such as 42U, 48U, etc.
Why Other Options are Less Relevant:
KVM Size: While important for management, KVM (Keyboard, Video, Mouse) switches do not typically determine rack size.
Hard Drive Size: Individual hard drives are installed within servers or storage devices, not directly influencing rack dimensions.
Cooling Fan Speed: Fan speed affects cooling but not the physical size of the rack.
Outlet Amperage: Power requirements do not determine rack dimensions but rather the electrical infrastructure supporting the rack.
References:
CompTIA Network+ study materials on rack installation and equipment sizing.

NEW QUESTION: 214
A network administrator is troubleshooting a connection issue and needs to determine the path that a packet will take. Which of the following commands accomplishes this task?
A. netstat
B. traceroute
C. ping
D. nslookup
E. ipconfig
Answer: (SHOW ANSWER)
The correct answer is traceroute, which is the diagnostic command specifically designed to determine the path a packet takes across a network. According to the CompTIA Network+ N10-009 objectives, traceroute is a key network troubleshooting tool used to identify routing paths, hop counts, and points of latency or failure between a source and a destination. Traceroute works by sending packets with incrementally increasing Time to Live (TTL) values. Each router along the path decrements the TTL by one, and when it reaches zero, the router returns an ICMP Time Exceeded message. This process allows the administrator to see each intermediate hop, its response time, and where packets may be delayed or dropped.
The other options do not fulfill this purpose. Ping only verifies basic connectivity and round-trip time but does not show the route taken. Netstat displays active connections, ports, and routing tables but does not trace packet paths. Nslookup is used to resolve DNS names to IP addresses, and ipconfig displays local network configuration information.
The Network+ objectives emphasize traceroute (or tracert on Windows systems) as the primary tool for diagnosing routing issues, asymmetric paths, and network congestion, making it the correct and most appropriate choice in this scenario.
NEW QUESTION: 215
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: 216
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: 217
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: 218
Which of the following is the most secure way to provide site-to-site connectivity?
A. VXLAN
B. IKE
C. GRE
D. IPsec
Answer: (SHOW ANSWER)
IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, ensuring that data sent across the network is protected from interception and tampering. Unlike other options, IPsec operates at the network layer and can secure all traffic that crosses the IP network, making it the most comprehensive and secure choice for site-to-site VPNs.References: CompTIA Network+ study materials and NIST Special Publication 800-77.

NEW QUESTION: 219
A network administrator manages multiple computers and notices that three computers are no longer communicating with the network. Which of the following commands best identifies whether other devices are restricting packet traffic?
A. ipconfig
B. traceroute
C. nmap
D. ping
Answer: (SHOW ANSWER)
The correct answer is B. traceroute. Traceroute is a diagnostic command used to track the path that packets take from a source device to a destination across an IP network. It identifies each hop (router or intermediary device) along the route and measures the time it takes for packets to travel between them. This makes it particularly useful for determining where communication is failing or being restricted.
In this scenario, the administrator suspects that other network devices may be restricting traffic, such as routers, firewalls, or access control devices. Traceroute helps pinpoint exactly where packets stop or experience delays, indicating a potential filtering or blocking point in the network path.
The other options are less appropriate. ipconfig is used to view or manage a device's local IP configuration and does not test packet flow across the network. Nmap is a scanning tool used to identify open ports and services, not to trace packet paths. Ping verifies basic connectivity but does not provide insight into intermediate devices or where traffic may be blocked.
According to CompTIA Network+ objectives, traceroute is the best tool for identifying routing issues and determining whether network devices are restricting traffic.

NEW QUESTION: 220
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?
Freecram.net
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: 221
A network technician needs to configure IP addressing in a Class C network with eight subnets total:
Three subnets for 60 hosts
Three subnets for 15 hosts
Two subnets for seven hosts
Which of the following solutions should the technician use to accomplish this task?
A. CIDR
B. APIPA
C. VLSM
D. RFC 1918
Answer: (SHOW ANSWER)
The correct answer is VLSM (Variable Length Subnet Masking). According to the CompTIA Network+ N10-
009 objectives, VLSM allows a network administrator to create subnets of different sizes within the same network, making it ideal for environments where subnet host requirements vary. In this scenario, the technician must support multiple subnet sizes-60 hosts, 15 hosts, and seven hosts- within a single Class C network. Using a single subnet mask for all eight subnets would either waste a large number of IP addresses or fail to meet host requirements. VLSM solves this problem by allowing each subnet to be assigned a custom subnet mask that closely matches its host needs, maximizing address efficiency.
CIDR enables classless addressing and route aggregation but does not, by itself, describe creating multiple subnet sizes within a single address block. APIPA is a self-assigned addressing mechanism used when DHCP fails and has no relevance to subnet design. RFC 1918 defines private IP address ranges but does not address subnetting strategies.
The Network+ objectives emphasize VLSM as a best practice for efficient IP address management, especially in enterprise environments where conserving address space and meeting diverse departmental requirements are critical. In this case, VLSM is the only solution capable of meeting all stated constraints.

NEW QUESTION: 222
A user reports having intermittent connectivity issues to the company network. The network configuration for the user reveals the following:
IP address: 192.168.1.10
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.254
The network switch shows the following ARP table:

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

CompTIA
freeram.net

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

A. A port with incorrect VLAN assigned

B. A switch with spanning tree conflict

C. Another PC with manually configured IP

D. A router with overlapping route tables

Answer: (SHOW ANSWER)

This scenario describes a duplicate IP address. The ARP table shows two different MAC addresses (0c00.
1134.0001 and 0c00.1298.d239) associated with the same IP address (192.168.1.10), which leads to ARP table conflicts and intermittent connectivity.

From Andrew Ramdayal's guide:

"Duplicate IP addresses occur when two devices on the same network are assigned the same IP address, causing network conflicts. Common issues include manual configuration errors or DHCP lease issues.

Resolution includes using IP management tools and avoiding overlaps in DHCP and static IP assignments."

NEW QUESTION: 223

In an environment with one router, which of the following will allow a network engineer to communicate between VLANs without purchasing additional hardware?

A. Subinterfaces

B. VXLAN

C. Layer 3 switch

D. VIR

Answer: (SHOW ANSWER)

A subinterface is a logical interface created on a single physical router interface that allows routing between VLANs (known as Router-on-a-Stick (ROAS)). This method is commonly used when only one physical router is available, allowing inter-VLAN communication without additional hardware.

*Why not the other options?

*VXLAN (B) - This is used for extending Layer 2 networks over a Layer 3 infrastructure, primarily in data centers. It does not directly enable inter-VLAN communication.

*Layer 3 switch (C) - A Layer 3 switch can route between VLANs, but the scenario states that purchasing additional hardware is not an option.

*VIR (D) - This is not a standard networking term in the context of VLAN communication.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 8: VLANs and Inter-VLAN Routing

NEW QUESTION: 224

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: 225
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: 226
A firewall receives traffic on port 80 and forwards it to an internal server on port 88. Which of the following technologies is being leveraged?
A. TLS
B. FHRP
C. SSL
D. PAT
Answer: (SHOW ANSWER)
The correct answer is PAT (Port Address Translation). According to the CompTIA Network+ N10-009 objectives, PAT is a form of Network Address Translation (NAT) that allows multiple internal hosts-or services-to be mapped to a single public IP address using different port numbers. PAT can also translate destination port numbers, which is exactly what is occurring in this scenario.
In this case, the firewall receives incoming traffic on port 80 (commonly used for HTTP) and forwards it to an internal server listening on port 88. This process is often referred to as port forwarding, which is a practical implementation of PAT. The firewall rewrites the destination port and potentially the destination IP address so that external clients can access internal services without exposing internal addressing schemes.
The other options do not apply. TLS and SSL are encryption protocols used to secure data in transit; they do not perform port translation. FHRP (First Hop Redundancy Protocol), such as HSRP or VRRP, provides gateway redundancy and high availability, not traffic forwarding or port remapping.

The Network+ objectives emphasize understanding how firewalls and NAT technologies manipulate IP addresses and ports to enable secure access to internal resources. PAT is the technology that enables this functionality, making it the correct answer.

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
Which of the following network cables involves bounding light off of protective cladding?
A. Twinaxial
B. Coaxial
C. Single-mode
D. Multimode
Answer: (SHOW ANSWER)
Multimode fiber optic cables involve the transmission of light signals that bounce off the core's cladding as they travel down the fiber. This characteristic differentiates it from single-mode fiber, where the light travels directly down the fiber without reflecting off the cladding.
Here are some detailed points about multimode fiber cables:
Construction: Multimode fibers have a larger core diameter, typically 50 or 62.5 microns, compared to single- mode fibers, which have a core diameter of about 9 microns.
Light Propagation: The larger core of multimode fiber allows multiple light modes to propagate. These modes travel at different angles, leading to reflections off the core-cladding boundary.
Distance and Bandwidth: Due to modal dispersion, where different light modes arrive at the receiver at different times, multimode fibers are suited for shorter distance applications compared to single-mode fibers.
Typical distances are up to 550 meters for 10 Gbps Ethernet using OM4 multimode fiber.
Applications: Multimode fibers are commonly used in LANs (Local Area Networks), data centers, and for shorter distance data transmission due to their cost-effectiveness and ease of installation.
Network References:
CompTIA Network+ N10-007 Official Certification Guide, which covers fiber optic technologies, including the differences between multimode and single-mode fibers.
Cisco Networking Academy: Provides training materials and reference guides on the properties of different fiber optic cables.
Fiber Optic Association (FOA): A professional society dedicated to fiber optics, offering extensive information and certification on fiber optic technologies.
Multimode fibers are specifically designed for short-range communication with higher data rates and are typically used in environments like data centers, where high bandwidth over shorter distances is crucial. The reflections off the cladding, inherent to multimode fiber, facilitate this high-capacity communication.

NEW QUESTION: 228
Which of the following is enforced through legislation?
A. AUP
B. GDPR
C. Code of conduct
D. EULA
Answer: B (LEAVE A REPLY)

GDPR (General Data Protection Regulation)is alegal frameworkenforced by the European Union to protect personal data and privacy. Unlike internal organizational policies such as AUPs or codes of conduct, GDPR is alegislated regulation, and organizations must comply or face legal consequences.
Reference:Section 4.1 - Basic Network Security Concepts - "GDPR and Compliance Regulations"

NEW QUESTION: 229
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: 230
A network engineer adds a tunnel for a new branch network. Which of the following ensures that all data is encrypted inside the tunnel?
Freecram.net
A. ESP
B. SSH
C. GRE
D. IKE
Answer: (SHOW ANSWER)
ESP (Encapsulating Security Payload) is an IPsec protocol that provides encryption, integrity, and authentication for data inside a VPN tunnel. It ensures that all tunneled traffic is encrypted.
B). SSH secures remote terminal sessions, not site-to-site VPN tunnels.
C). GRE (Generic Routing Encapsulation) provides encapsulation but does not encrypt data.
D). IKE (Internet Key Exchange) negotiates keys and establishes the IPsec tunnel but does not encrypt the payload itself.
References (CompTIA Network+ N10-009):
Domain: Network Security - VPN protocols, IPsec (AH vs. ESP), encryption in transit.

NEW QUESTION: 231
Which of the following can also provide a security feature when implemented?
A. NAT

B. BGP
C. FHRP
D. EIGRP
Answer: A (LEAVE A REPLY)
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: 232
A network administrator needs to configure the core switches where multiple connections between data centers are used. Given the following requirements:
* Fault tolerance and redundancy
* Vendor interoperability
* Increased bandwidth
* Cost effectiveness
* Simplified management
Which of the following should the administrator configure?
A. Spanning tree
B. Interface speeds to 10GB
C. Link aggregation
D. Jumbo frames
Answer: (SHOW ANSWER)
The best answer is C. Link aggregation. The requirements point directly to combining multiple physical links into one logical connection. Link aggregation provides higher total bandwidth, supports redundancy if one member link fails, and simplifies administration because the bundle is managed as a single logical interface instead of several separate ones.
Another important clue is vendor interoperability. Standards-based link aggregation, such as LACP, is designed to work across different vendors when supported properly. That makes it a strong match for inter- data-center switch environments where equipment may not all come from the same manufacturer.
The other choices do not satisfy the full requirement list. Spanning tree helps prevent loops, but it can block redundant links instead of actively using them for extra bandwidth. Setting interface speeds to 10GB increases speed per port, but it does not by itself provide the logical bundling, simplified management, or redundancy benefits described. Jumbo frames can improve efficiency for some traffic types, but they are not the right answer for bandwidth aggregation and resilient uplinks.
Because the question asks for a solution that improves throughput, keeps redundancy, remains cost effective, and is easier to manage, link aggregation is the strongest fit.

NEW QUESTION: 233
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: 234
A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?
A. Trunk all VLANs on the port.
B. Configure the native VLAN.
C. Tag the traffic to voice VLAN.
D. Disable VLANs.
Answer: (SHOW ANSWER)
* Understanding VoIP and VLANs:
* VoIP (Voice over IP) phones often use VLANs (Virtual Local Area Networks) to separate voice traffic from data traffic for improved performance and security.
* Tagging Traffic to Voice VLAN:
* Voice VLAN Configuration:The port on the switch needs to be configured to tag traffic for the specific voice VLAN. This ensures that voice packets are prioritized and handled correctly.
* VLAN Tagging:VLAN tagging allows the switch to identify and separate voice traffic from other types of traffic on the network, reducing latency and jitter for VoIP communications.
* Comparison with Other Options:
* Trunk all VLANs on the port:Trunking all VLANs is typically used for links between switches, not for individual device ports.
* Configure the native VLAN:The native VLAN is for untagged traffic and does not address the need for separating and prioritizing voice traffic.
* Disable VLANs:Disabling VLANs would mix voice and data traffic, leading to potential performance issues and lack of traffic separation.
* Implementation:
* Configure the switch port connected to the VoIP phone to tag the traffic for the designated voice VLAN, ensuring proper network segmentation and quality of service.
References:
* CompTIA Network+ study materials on VLAN configuration and VoIP implementation.

NEW QUESTION: 235
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: 236

A wireless technician wants to implement a technology that will allow user devices to automatically navigate to the best available frequency standard. Which of the following technologies should the technician use?

A. Band steering

B. Wireless LAN controller

C. Directional antenna

D. Autonomous access point

Answer: (SHOW ANSWER)

Band Steering: This technology enables wireless devices to connect to the most optimal frequency band (2.4 GHz or 5 GHz) by encouraging capable devices to switch to the less congested 5 GHz band. This improves overall network performance and prevents overcrowding on the 2.4 GHz band.

Wireless LAN controller (B): This manages multiple access points in a network but does not handle frequency optimization.

Directional antenna (C): This focuses the signal in a specific direction but does not affect frequency selection.

Autonomous access point (D): This operates independently but lacks advanced features like band steering.

Reference: CompTIA Network+ Official Study Guide, Domain 1.6 (Wireless Standards and Technologies).

NEW QUESTION: 237

A technician is planning an equipement installation into a rack in a data center that practices hot aisle/cold aise ventilation. Which of the following directions should the equipement exhaust face when installed in the rack?

A. Sides

B. Top

C. Front

D. Rear

Answer: (SHOW ANSWER)

In a data center that practices hot aisle/cold aisle ventilation, equipment should be installed so that the exhaust faces the rear of the rack. This setup ensures that hot air is expelled into the hot aisle, maintaining proper airflow and cooling efficiency.

* Hot Aisle/Cold Aisle Configuration: Equipment intake should face the cold aisle where cool air is supplied, and exhaust should face the hot aisle where hot air is expelled.

* Cooling Efficiency: Proper orientation of equipment helps maintain an efficient cooling environment by segregating hot and cold air, preventing overheating and improving energy efficiency.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses data center design principles, including hot aisle/cold aisle configurations.

* Cisco Data Center Design Guide: Provides best practices for data center layout and equipment installation.

* Network+ Certification All-in-One Exam Guide: Covers data center environmental controls and ventilation strategies.

NEW QUESTION: 238

A company ' s Chief Information Security Officer requires that servers and firewalls have accurate time stamps when creating log files so that security analysts can correlate events during incident investigations.

Which of the following should be implemented?

A. Syslog server

B. SMTP

C. NTP

D. SNMP

Answer: (SHOW ANSWER)

The correct solution is NTP (Network Time Protocol). Accurate timestamps across servers, firewalls, and network devices are critical for correlating logs during incident response. NTP synchronizes device clocks to a trusted time source, ensuring consistency across the network.
A). Syslog centralizes logs but does not synchronize time.
B). SMTP is email transfer, unrelated to time.
D). SNMP monitors devices but does not correct time discrepancies.
By implementing NTP, analysts can ensure that logs from different devices are time-aligned, which is essential for reconstructing attack timelines and detecting anomalies.
References (CompTIA Network+ N10-009):
Domain: Network Operations - Time synchronization, NTP, log correlation.

NEW QUESTION: 239
A junior network administrator is auditing the company network and notices incrementing input errors on a long-range microwave interface. Which of the following is the most likely reason for the errors?
A. The parabolic signal is misaligned.
B. The omnidirectional signal is being jammed.
C. The omnidirectional signal is not strong enough to receive properly.
D. The parabolic signal uses improper routing protocols.
Answer: A (LEAVE A REPLY)
A misaligned parabolic antenna can cause a significant increase in input errors because the signal is not properly focused or directed towards the receiving antenna, resulting in poor reception and data corruption.
The document confirms:
"Misalignment of parabolic microwave antennas can lead to weak or incorrect signal reception, causing an increase in input errors and connectivity issues on the link."

NEW QUESTION: 240
A network technician is working on a PC with a faulty NIC. The host is connected to a switch with secured ports. After testing the connection cables and using a known-good NIC, the host is still unable to connect to the network. Which of the following is causing the connection issue?
Freecram.net
A. MAC address of the new card
B. BPDU guard settings
C. Link aggregation settings
D. PoE power budget
Answer: (SHOW ANSWER)
If a switch has port security enabled (such as sticky MAC or a configured allowed MAC), the port will only allow the original NIC's MAC address. When a new NIC with a different MAC address is installed, the port rejects traffic, preventing network connectivity.
B). BPDU guard protects against rogue switches, not end hosts.
C). Link aggregation applies when bundling multiple uplinks, not a single PC connection.
D). PoE budget applies to powered devices like APs, not PCs.
References (CompTIA Network+ N10-009):
Domain: Network Troubleshooting - Port security, MAC address filtering, switch security features.

NEW QUESTION: 241
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."

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

Valid N10-009 Dumps shared by EduDump.com for Helping Passing N10-009 Exam! EduDump.com now offer the **newest N10-009 exam dumps**, the EduDump.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com N10-009 dumps with Test Engine here:
https://www.edudump.com/exams/CompTIA/N10-009/premium/ (**792** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)