

CompTIA.N10-009.v2026-07-20.q260

Exam Code:	N10-009
Exam Name:	CompTIA Network+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	260
Version:	v2026-07-20
# of views:	115
# of Questions views:	2600
https://www.freepdfdumps.com/CompTIA.N10-009.v2026-07-20.q260.html	

NEW QUESTION: 1

Several users in an organization report connectivity issues and lag during a video meeting. The network administrator performs a tcpdump and observes increased retransmissions for other non-video applications on the network. Which of the following symptoms describes the users' reported issues?

- A. Latency
- B. Packet loss
- C. Bottlenecking
- D. Jitter

Answer: B (LEAVE A REPLY)

Packet loss occurs when network packets fail to reach their destination, leading to disruptions in connectivity and performance issues. In this scenario:

Users report connectivity issues and lag during video meetings.

The administrator detects increased retransmissions in tcpdump, which is a strong indicator of lost packets that must be resent.

Video meetings are particularly sensitive to packet loss, leading to buffering, frozen screens, and dropped calls.

Latency (Option A) refers to delayed data transmission but does not necessarily cause retransmissions.

Bottlenecking (Option C) happens when a network component (e.g., router, switch) cannot handle the traffic load, but packet retransmissions are more directly related to packet loss.

Jitter (Option D) affects the consistency of packet arrival times, but the symptoms described here are more aligned with packet loss rather than timing variations.

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

NEW QUESTION: 2

A network engineer must determine which ports are currently established from a client device. Given the following:

Active Connections

Proto Local Address Foreign Address State

TCP 10.203.10.11:3389 207.141.201.10:65278 ESTABLISHED

TCP 10.203.10.11:49678 168.63.129.16:32526 ESTABLISHED

TCP 10.203.10.11:49688 168.63.129.16:http ESTABLISHED

TCP 10.203.10.11:49701 168.63.129.16:32526 ESTABLISHED

TCP 10.203.10.11:52502 20.190.135.17:https TIME_WAIT

TCP 10.203.10.11:52554 168.63.129.16:http TIME_WAIT

Which of the following commands was used to produce the output?

- A. nslookup
- B. dig
- C. nmap
- D. netstat

Answer: D ([LEAVE A REPLY](#))

The correct choice is D. netstat because the display shown is a classic list of active TCP sessions, including the protocol, local address, remote address, and the connection state such as ESTABLISHED and TIME_WAIT. That is exactly the kind of information a technician checks when trying to see what connections a workstation currently has open.

The distractors do different jobs. nslookup and dig are DNS utilities. They help query name resolution records, but they do not list active client sessions. nmap is mainly used to scan hosts and ports across the network, usually to discover services or assess exposure on target systems. It does not normally produce a local session table in this format.

For Network+ purposes, this falls under troubleshooting with command-line tools. When the goal is to inspect current sessions on the local device and confirm whether a port is open, listening, or already connected, netstat is the expected command. The wording "currently established from a client device" is the clue that matters most. The question is not asking what ports exist on a remote server; it is asking what active connections are present on the machine itself. That makes netstat the best fit.

NEW QUESTION: 3

A company is implementing a new wireless network in its office building and wants to ensure maximum coverage and signal strength. Which of the following factors should a technician consider to meet these requirements? Select two.

- A. Building materials
- B. Electrical interference
- C. Distance from the server room
- D. Type of encryption being used
- E. Power over Ethernet
- F. Type of client devices

Answer: ([SHOW ANSWER](#)**)**

Building materials and electrical interference are the two best factors to consider when designing a wireless network for maximum coverage and signal strength. Wireless signals can be weakened or blocked by concrete, brick, metal, glass, insulation, elevator shafts, walls, and other structural materials. These materials can absorb, reflect, or scatter radio frequency signals, creating weak coverage areas or dead zones.

Electrical interference is also important because wireless networks can be affected by devices that generate electromagnetic or radio frequency interference. Examples include microwaves, motors, fluorescent lighting, cordless devices, industrial equipment, and neighboring wireless networks. Interference can reduce signal quality, increase retransmissions, and cause unstable connectivity.

The CompTIA Network+ N10-009 objectives include wireless site surveys, signal strength, antenna placement, interference, and environmental factors. These considerations are central to proper wireless design.

Distance from the server room does not directly determine wireless signal coverage. Encryption affects security, not radio signal strength. Power over Ethernet affects how APs receive power but not coverage by itself. Client device type can affect performance, but the best design factors for coverage and signal strength are building materials and electrical interference.

NEW QUESTION: 4

Which of the following ports is a secure protocol?

- A. 20
- B. 23
- C. 443
- D. 445

Answer: ([SHOW ANSWER](#)**)**

Port 443 is used by HTTPS (Hypertext Transfer Protocol Secure), a secure version of HTTP that uses SSL/TLS to encrypt the communication between a client and server. This ensures confidentiality and integrity of data in transit. The document states:
"Port 443 is the default port for HTTPS, which secures HTTP traffic using SSL/TLS, providing encryption and secure identification of web servers."

NEW QUESTION: 5

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: 6

A new backup system takes too long to copy files to the new SAN each night. A network administrator makes a simple change to the network and the devices to decrease backup times. Which of the following does the network administrator change?

- A. QoS
- B. SDN
- C. MTU
- D. VXLAN
- E. TTL

Answer: C ([LEAVE A REPLY](#))

Increasing the MTU (Maximum Transmission Unit) size allows larger frames to be transmitted, reducing overhead and improving throughput - especially for large file transfers like backups.

A). QoS prioritizes traffic but doesn't reduce backup times directly.

B). SDN is a network management model, not a parameter change.

D). VXLAN encapsulates VLANs, not relevant to backup speeds.

E). TTL is for packet lifetime, not throughput.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - MTU, jumbo frames, performance tuning.

NEW QUESTION: 7

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

- A. Identify the problem
- B. Test in the theory
- C. Establish a plan of action
- D. Verify full system functionality

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 8

An ongoing mail server migration is in progress. The current system does not use encrypted mail protocols, but the new system does. Which of the following port can the administrator close to deny non-encrypted mail protocols without interrupting the migration?

- A. 22
- B. 23
- C. 25
- D. 443
- E. 587

Answer: ([SHOW ANSWER](#))

Port 25 is associated with SMTP, which is traditionally used for Simple Mail Transfer Protocol traffic. In basic port-mapping questions for CompTIA Network+, SMTP on port 25 is commonly treated as the non-encrypted mail transport option. If the organization is migrating to encrypted mail protocols, closing port 25 can help deny non-encrypted SMTP access while allowing encrypted mail submission or web-based secure access to continue through other ports.

The CompTIA Network+ N10-009 objectives require candidates to recognize common protocols, port numbers, and their secure alternatives. Port 587 is commonly used for SMTP message submission with TLS support, so it should remain available when encrypted mail submission is required. Port 443 is HTTPS and may be used for secure webmail access. Port 22 is SSH, which is encrypted remote administration, not a mail protocol. Port 23 is Telnet, which is unencrypted, but it is not a mail protocol.

Because the question specifically asks about denying non-encrypted mail protocols, port 25 is the best answer among the listed options.

NEW QUESTION: 9

Which of the following protocols is used to route traffic on the public internet?

- A. BGP
- B. OSPF
- C. EIGRP
- D. RIP

Answer: A ([LEAVE A REPLY](#))

Border Gateway Protocol (BGP) is the primary protocol used to route traffic on the public internet. It allows ISPs and large networks to exchange routing information, making it an Exterior Gateway Protocol (EGP).

Breakdown of Options:

- A). BGP - Correct answer. Used for internet routing and exchanges routing information between ISPs.
- B). OSPF - An Interior Gateway Protocol (IGP) used for routing within an autonomous system (not the public internet).
- C). EIGRP - Cisco's proprietary IGP, used within private networks, not the public internet.

D). RIP - An older distance-vector protocol, not scalable for the internet.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.4: Explain routing technologies.

RFC 4271: Border Gateway Protocol 4 (BGP-4)

NEW QUESTION: 10

Which of the following network ports is used when a client accesses an SFTP server?

A. 22

B. 80

C. 443

D. 3389

Answer: (SHOW ANSWER)

SFTP (Secure File Transfer Protocol) operates over port 22, using SSH (Secure Shell) encryption for secure file transfers.

Breakdown of Options:

A). 22 - Correct answer. SFTP runs over SSH (port 22) for secure file transfers.

B). 80 - Used for HTTP, not SFTP.

C). 443 - Used for HTTPS (secure web traffic).

D). 3389 - Used for RDP (Remote Desktop Protocol).

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.

RFC 4253: SSH Transport Layer Protocol

NEW QUESTION: 11

A detective is investigating an identity theft case in which the target had an RFID-protected payment card issued and compromised in the same day. The only place the target claims to have used the card was at a local convenience store. The detective notices a video camera at the store is placed in such a way that customers' credentials can be seen when they pay. Which of the following best explains this social engineering technique?

A. Shoulder surfing

B. Impersonation

C. Vishing

D. Tailgating

Answer: A (LEAVE A REPLY)

Shoulder surfing is a social engineering attack where attackers observe someone's private information by looking over their shoulder or using tools like cameras to capture input.

From Andrew Ramdayal's guide:

"Shoulder surfing is the act of watching someone enter confidential information, such as PINs or passwords, often using direct line-of-sight or surveillance equipment."

NEW QUESTION: 12

A network technician receives a ticket from an employee who is working on PC 1 but is unable to connect to the database server. The technician pings the database server from PC 1, but the request times out.

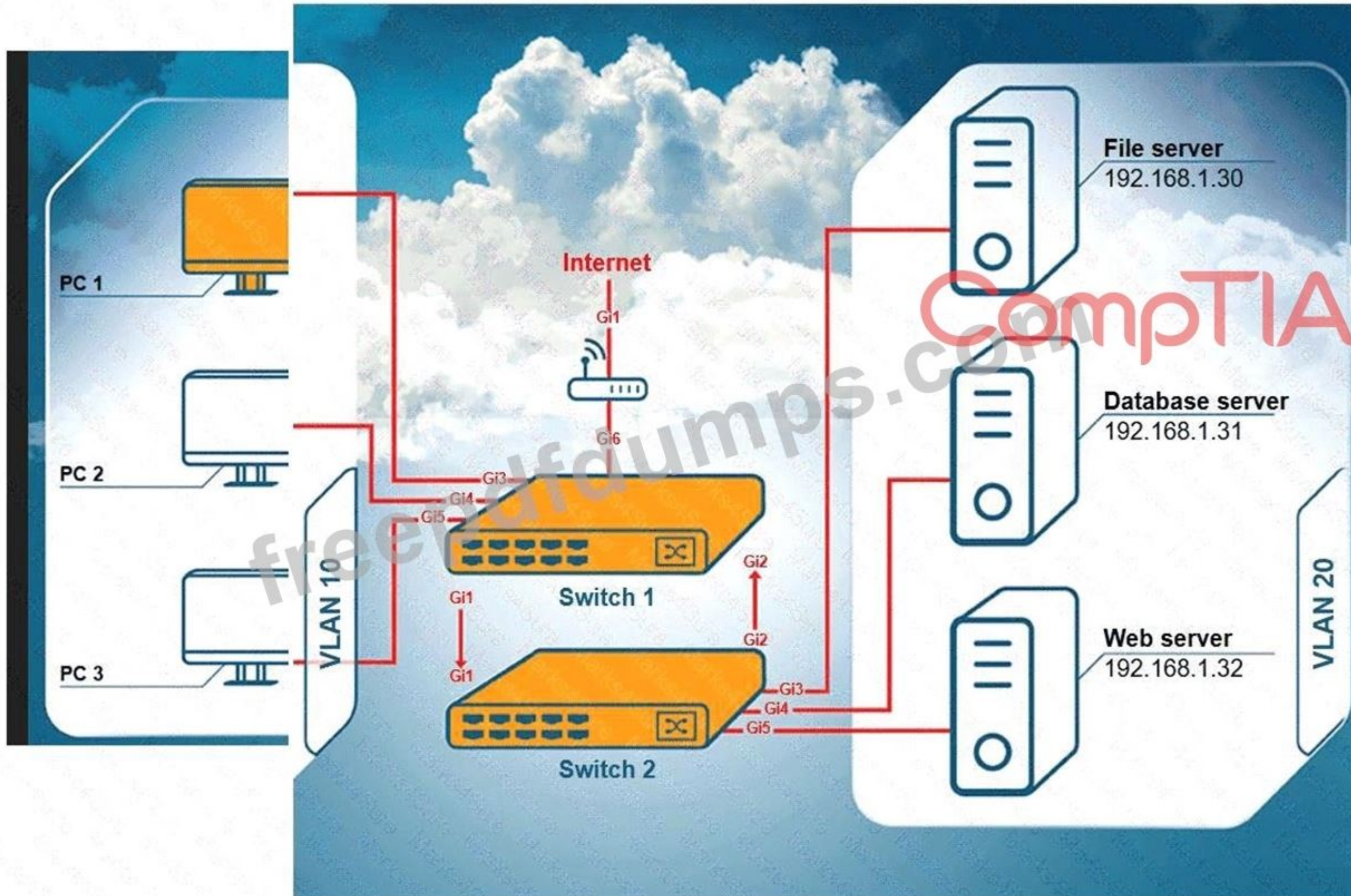
After reviewing the utilization of Switch 1 and Switch 2, the technician finds high CPU utilization and sees that the MAC table is continuously changing.

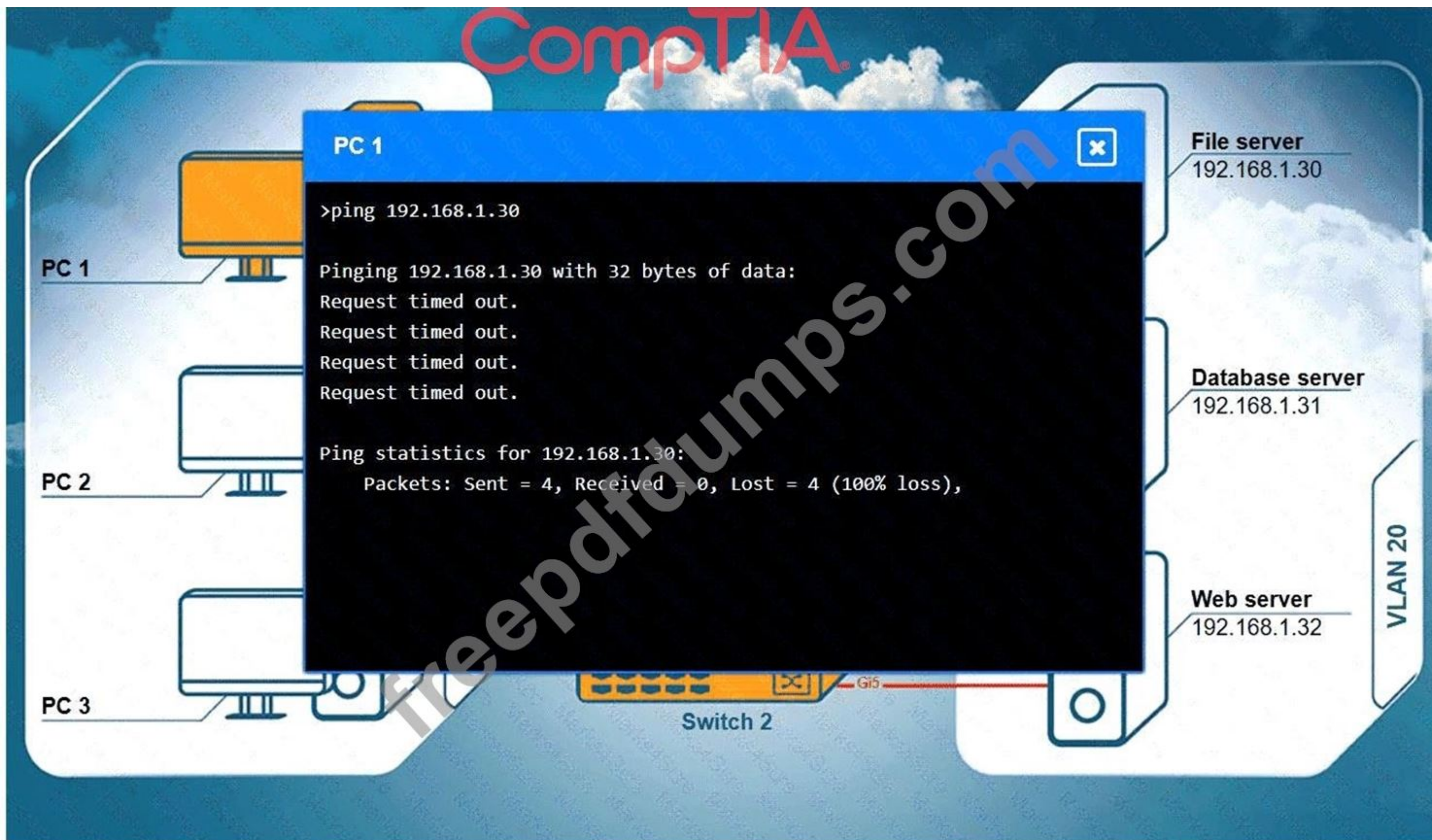
INSTRUCTIONS

Configure Switch 1 and Switch 2 to remediate the employee ' s issue. Then, validate connectivity between PC

1 and the database server.

Switch 1 and Switch 2 are already in configuration mode. Type help to view a list of available commands.







Switch 2



Switch2(config)#

freepdfdumps.com

CompTIA

Switch 1



```
Switch1(config)# interface gi2
```

```
% Invalid input detected.
```

```
Switch1(config)# ?
```

```
Available commands:
```

```
show vlan
```

```
show spanning-tree
```

```
spanning-tree vlan
```

```
Switch1(config)# spanning-tree vlan 10
```

```
Switch1(config)# spanning-tree vlan 20
```

```
Switch1(config)#
```

freepdfdumps.com

CompTIA.

```
Switch 2
Switch2(config)# ?
Available commands:
show vlan
show spanning-tree
spanning-tree vlan
Switch2(config)#
```



Answer:

See the solution in Explanation below.

Explanation:

Switch 1

spanning-tree vlan 10 root primary

spanning-tree vlan 20 root secondary

Switch 2

spanning-tree vlan 20 root primary

spanning-tree vlan 10 root secondary

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

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

A clean design is:

Switch 1 root primary for VLAN 10

Switch 2 root primary for VLAN 20

Make each opposite switch root secondary for failover

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

NEW QUESTION: 13

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

A. VLAN hopping

B. Rogue DHCP

C. Distributed DoS

D. Evil twin

Answer: B ([LEAVE A REPLY](#))

A rogue DHCP server occurs when an unauthorized or misconfigured DHCP server assigns incorrect IP addresses, default gateways, or DNS settings to clients.

*In this scenario:

*The user can ping the gateway, meaning local network communication is working.

*However, they cannot access network resources, which suggests incorrect IP configuration (likely due to a rogue DHCP server assigning the wrong gateway or DNS).

*Why not the other options?

*VLAN hopping (A): This is an attack that exploits VLAN configurations to gain access to unauthorized VLANs. It would not typically cause multiple users to lose network access.

*Distributed DoS (C): A DDoS attack floods a network or service with traffic, but this issue is more likely misconfigured IP settings than an actual attack.

*Evil twin (D): This refers to a fraudulent Wi-Fi network mimicking a legitimate one. Since the users are on a wired network (ipconfig output checked), this is not applicable.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security Threats

NEW QUESTION: 14

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

A. Identify the problem.

B. Establish a theory.

C. Document findings.

D. Create a plan of action.

Answer: A ([LEAVE A REPLY](#))

The correct answer is Identify the problem, which is always the first step in the CompTIA Network+ N10-009 troubleshooting methodology. Before forming theories, creating action plans, or documenting outcomes, technicians must clearly understand what is happening, who is affected, and what symptoms are present.

In this scenario, the symptoms-inaccessible files and a changed wallpaper-are serious and potentially indicative of a security incident such as ransomware. However, at this stage, there is disagreement between the network administrator and the security analyst regarding the nature of the issue. That reinforces the need to begin with problem identification, which includes gathering information, determining the scope of impact, identifying recent changes, and assessing whether the incident is isolated or widespread.

Establishing a theory comes after the problem has been clearly defined. Creating a plan of action and documenting findings occur later in the process, once the issue has been confirmed and remediation steps are determined. Jumping ahead without properly identifying the problem could result in delayed containment or an incorrect response-especially critical in potential security incidents.

The Network+ objectives emphasize following the structured troubleshooting process precisely to reduce risk, prevent escalation, and ensure accurate resolution-particularly when malware or ransomware may be involved.

NEW QUESTION: 15

Which of the following services runs on port 636?

- A.** SMTP
- B.** Syslog
- C.** TFTP
- D.** LDAPS

Answer: D (LEAVE A REPLY)

LDAP over SSL (LDAPS) uses port 636 to provide secure, encrypted authentication for directory services.

Breakdown of Options:

- A). SMTP (Simple Mail Transfer Protocol) - Uses port 25, not 636.
- B). Syslog - Uses port 514 (UDP), not 636.
- C). TFTP (Trivial File Transfer Protocol) - Uses port 69 (UDP), not 636.
- D). LDAPS (Lightweight Directory Access Protocol Secure) - # Correct answer. Uses port 636 for secure directory authentication.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 3.1: Compare and contrast network protocols.

RFC 4511: Lightweight Directory Access Protocol (LDAP)

NEW QUESTION: 16

Which of the following attacks would most likely cause duplicate IP addresses in a network?

- A.** Rogue DHCP server
- B.** DNS poisoning
- C.** Social engineering
- D.** Denial-of-service

Answer: A (LEAVE A REPLY)

* Definition of a Rogue DHCP Server:

* A rogue DHCP server is an unauthorized DHCP server on a network, which can assign IP addresses to devices without proper control, leading to IP address conflicts.

* Impact of a Rogue DHCP Server:

* IP Address Conflicts: Multiple devices may receive the same IP address from different DHCP servers, causing network connectivity issues.

* Network Disruption: Devices may be assigned incorrect network configuration settings, disrupting network services and connectivity.

* Comparison with Other Attacks:

* DNS poisoning: Alters DNS records to redirect traffic to malicious sites, but does not cause IP address conflicts.

* Social engineering: Involves manipulating individuals to gain unauthorized access or information, not directly related to IP address conflicts.

* Denial-of-service (DoS): Floods a network or service with excessive traffic to disrupt operations, but does not cause duplicate IP addresses.

* Prevention and Detection:

* Implement network access control measures to prevent unauthorized devices from acting as DHCP servers.

* Use DHCP snooping on switches to allow DHCP responses only from authorized DHCP servers.

References:

* CompTIA Network+ study materials on network security threats and mitigation techniques.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

Which of the following are the best device-hardening techniques for network security? (Select two).

- A. Disabling unused ports
- B. Performing regular scanning of unauthorized devices
- C. Monitoring system logs for irregularities
- D. Enabling logical security such as SSO
- E. Changing default passwords
- F. Ensuring least privilege concepts are in place

Answer: A,E (LEAVE A REPLY)

Disabling unused ports prevents unauthorized access and reduces the attack surface by ensuring that no inactive or unmonitored entry points are available for exploitation. Changing default passwords is critical for security because default credentials are widely known and can easily be exploited by attackers. These techniques are fundamental steps in hardening devices against unauthorized access and ensuring network security. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 18

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: D (LEAVE A REPLY)

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.

NEW QUESTION: 19

An organization requires the ability to send encrypted email messages to a partner from an email server that is hosted on premises. The organization prefers to use the standard default ports when creating firewall rules.

Which of the following ports should be open to satisfy the requirements?

- A. 110
- B. 143
- C. 587
- D. 636

Answer: C (LEAVE A REPLY)

Port 587 is the standard default port for sending email (SMTP) with TLS encryption, which is used to secure email transmissions between mail servers or between clients and mail servers. Allowing traffic over port 587 enables secure email sending while maintaining standard protocol usage. (Reference: CompTIA Network+ Study Guide, Chapter on Ports and Protocols)

NEW QUESTION: 20

Which of the following is used when implementing VoIP phones?

- A. VPN
- B. CDN
- C. TTL
- D. QoS

Answer: ([SHOW ANSWER](#))

Quality of Service, or QoS, is used when implementing VoIP phones because voice traffic is sensitive to delay, jitter, and packet loss. QoS allows network administrators to classify and prioritize traffic so that real-time voice packets receive preferential treatment over less time-sensitive traffic such as file downloads, backups, or general web browsing. This helps maintain call quality, reduce dropped audio, and improve the user experience during periods of network congestion.

The CompTIA Network+ N10-009 objectives include traffic management, network performance, and services that require prioritization. VoIP is one of the most common examples of a service that benefits from QoS because voice communication must be delivered consistently and in sequence.

A VPN provides secure encrypted connectivity but does not inherently prioritize voice traffic. A CDN distributes content closer to users, typically for web or media delivery, and is not specifically used to implement VoIP phones. TTL, or Time to Live, is a packet field that helps prevent packets from circulating indefinitely in a network. Therefore, QoS is the correct answer for VoIP implementation.

NEW QUESTION: 21

A Chief Information Officer wants a DR solution that runs only after a failure of the primary site and can be brought online quickly once recent backups are imported. Which of the following DR site solutions meets these requirements?

- A. Cold
- B. Warm
- C. Active
- D. Hot

Answer: B ([LEAVE A REPLY](#))

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

A warm site is partially configured with necessary infrastructure and systems, but it requires recent backups to be restored before becoming fully operational. This provides a balance between cost and recovery time.

- A). Cold site has only power and space, requiring full setup, which takes too long.
- C). Active (active-active) runs simultaneously with the primary site, not only during failure.
- D). Hot site is fully operational at all times and can take over immediately, but it's more expensive.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - Disaster recovery sites (cold, warm, hot, active).

NEW QUESTION: 22

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

- A. 10.2.2.0/23
- B. 10.2.2.0/24
- C. 10.2.2.0/25
- D. 10.2.2.0/26

Answer: C ([LEAVE A REPLY](#))

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

NEW QUESTION: 23

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: B ([LEAVE A REPLY](#))

*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: 24

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: D ([LEAVE A REPLY](#))

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: 25

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: C (LEAVE A REPLY)

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: 26

Which of the following terms describes the capability in a public cloud to add or remove compute resources based on need?

- A.** Scalability
- B.** Availability
- C.** Elasticity
- D.** Multitenancy

Answer: C (LEAVE A REPLY)

The correct answer is C. Elasticity. In cloud computing, elasticity refers to the ability to increase or decrease resources quickly based on current demand. If workloads rise, more compute resources can be allocated. If demand drops, those resources can be reduced again. That is exactly what the question is describing.

This is slightly different from scalability. Scalability is the broader idea that a system can grow to handle more workload. Elasticity focuses more on the dynamic, on-demand adjustment of resources as conditions change. In exam questions, wording like "add or remove based on need" usually points straight to elasticity.

The other answer choices do not fit. Availability is about uptime and service access. Multitenancy refers to multiple customers sharing underlying cloud infrastructure while remaining logically separated. Neither describes rapid expansion and contraction of compute resources.

From a Network+ study perspective, elasticity is one of the core cloud characteristics to remember because it explains why cloud services are useful for workloads that are unpredictable or variable. Instead of permanently building for peak demand, organizations can consume more or less compute as required. That makes elasticity the best answer.

NEW QUESTION: 27

A network administrator needs to fail over services to an off-site environment. This process will take four weeks to become fully operational. Which of the following DR (Disaster Recovery) concepts does this describe?

- A.** Hot site
- B.** Warm site
- C.** Cold site
- D.** Active-active approach

Answer: C (LEAVE A REPLY)

A cold site is a backup facility that provides infrastructure (such as power, cooling, and space) but does not have active IT resources installed. When a disaster occurs, IT teams must bring in and configure all necessary hardware and software before services can resume. This process can take weeks or longer-which matches the scenario described.

*Why not the other options?

*Hot site (A) - A hot site is a fully operational backup facility with up-to-date data and pre-configured hardware, allowing almost instant failover (minutes to hours).

*Warm site (B) - A warm site has pre-installed hardware and some software/configurations, but it requires some setup before becoming fully operational (hours to a few days).

*Active-active approach (D) - This means that multiple sites run simultaneously with load balancing, ensuring no downtime in case of a failure.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 15: Business Continuity and Disaster Recovery

NEW QUESTION: 28

A network engineer performed a migration to a new mail server. The engineer changed the MX record, verified the change was accurate, and confirmed the new mail server was reachable via the IP address in the A record. However, users are not receiving email. Which of the following should the engineer have done to prevent the issue from occurring?

- A. Change the email client configuration to match the MX record.
- B. Reduce the TTL record prior to the MX record change.
- C. Perform a DNS zone transfer prior to the MX record change.
- D. Update the NS record to reflect the IP address change.

Answer: B (LEAVE A REPLY)

Understanding TTL (Time to Live):

TTL is a value in a DNS record that tells how long that record should be cached by DNS servers and clients.

A higher TTL value means that the record will be cached longer, reducing the load on the DNS server but delaying the propagation of changes.

Impact of TTL on DNS Changes:

When an MX record change is made, it may take time for the change to propagate across all DNS servers due to the TTL setting. If the TTL is high, old DNS information might still be cached, leading to email being directed to the old server.

Best Practice Before Making DNS Changes:

To ensure that changes to DNS records propagate quickly, it is recommended to reduce the TTL value to a lower value (such as 300 seconds or 5 minutes) well in advance of making the changes. This ensures that any cached records will expire quickly, and the new records will be used sooner.

Verification of DNS Changes:

After reducing the TTL and making the change to the MX record, it is important to verify the propagation using tools like dig or nslookup.

Comparison with Other Options:

Change the email client configuration to match the MX record: Email clients generally do not need to match the MX record directly; they usually connect to a specific mail server specified in their settings.

Perform a DNS zone transfer prior to the MX record change: DNS zone transfers are used to replicate DNS records between DNS servers, but they are not related to the propagation of individual record changes.

Update the NS record to reflect the IP address change: NS records specify the DNS servers for a domain and are not related to MX record changes.

References:

CompTIA Network+ study materials and DNS best practices.

NEW QUESTION: 29

You are tasked with verifying the following requirements are met in order to ensure network security.

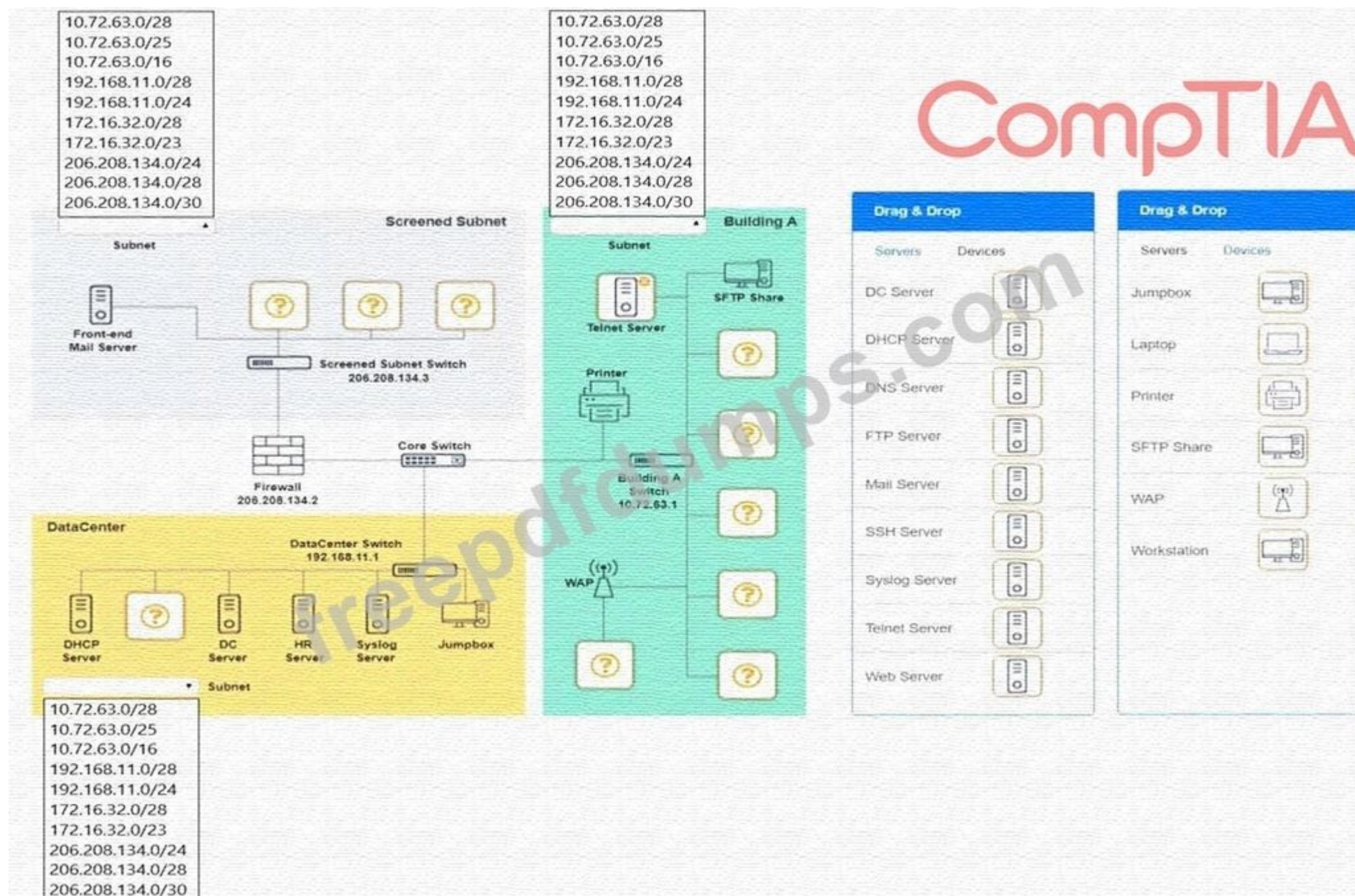
Requirements:

Datacenter

Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a dedicated server to resolve IP addresses and hostnames correctly and handle port 53 traffic Building A Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide devices to support 5 additional different office users Add an additional mobile user Replace the Telnet server with a more secure solution Screened subnet Ensure network is subnetted to allow all devices to communicate properly while minimizing address space usage Provide a server to handle external 80/443 traffic Provide a server to handle port 20/21 traffic INSTRUCTIONS Drag and drop objects onto the appropriate locations. Objects can be used multiple times and not all placeholders need to be filled.

Available objects are located in both the Servers and Devices tabs of the Drag & Drop menu.

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



Answer:

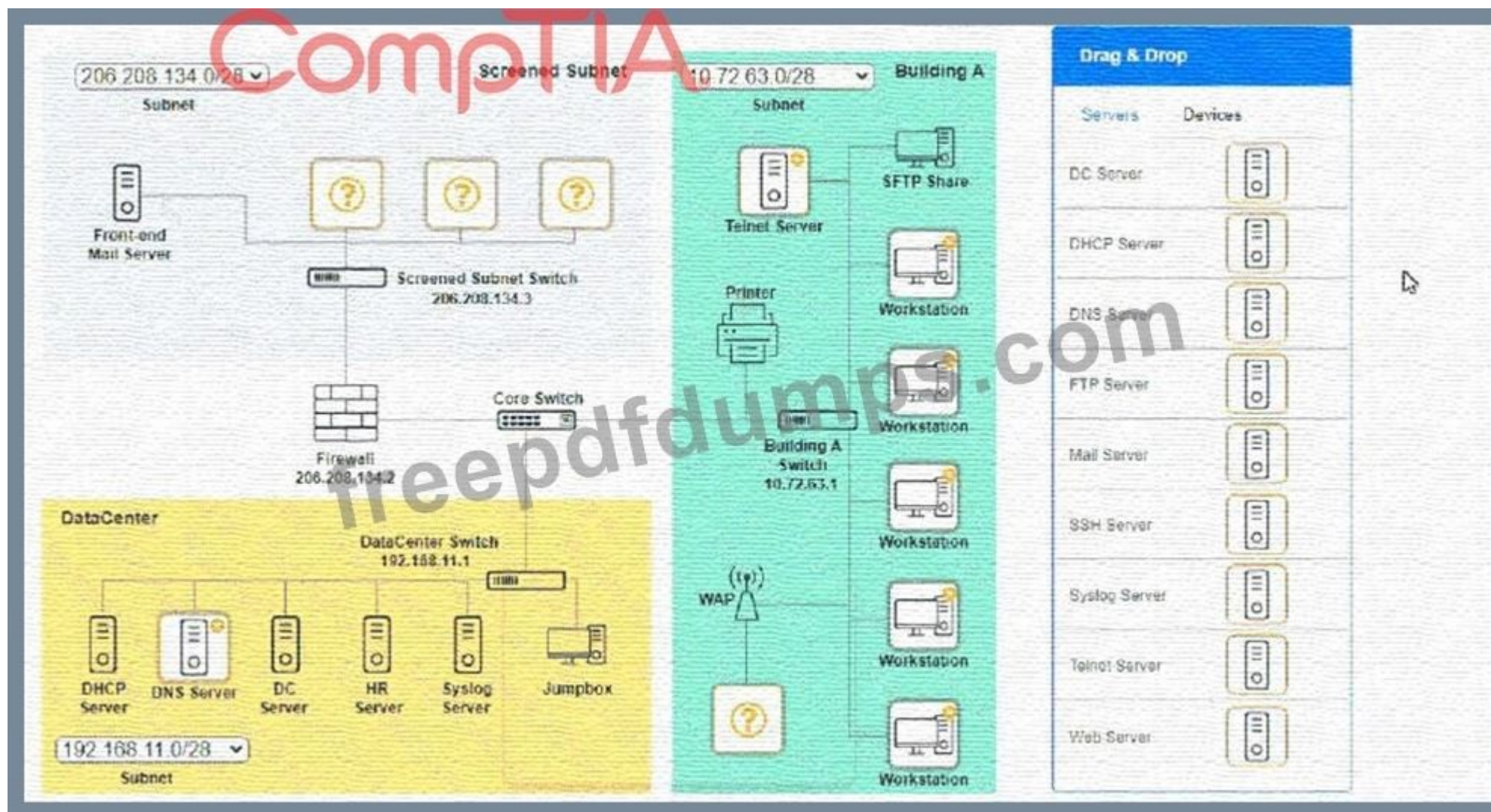
See explanation below.

Explanation:

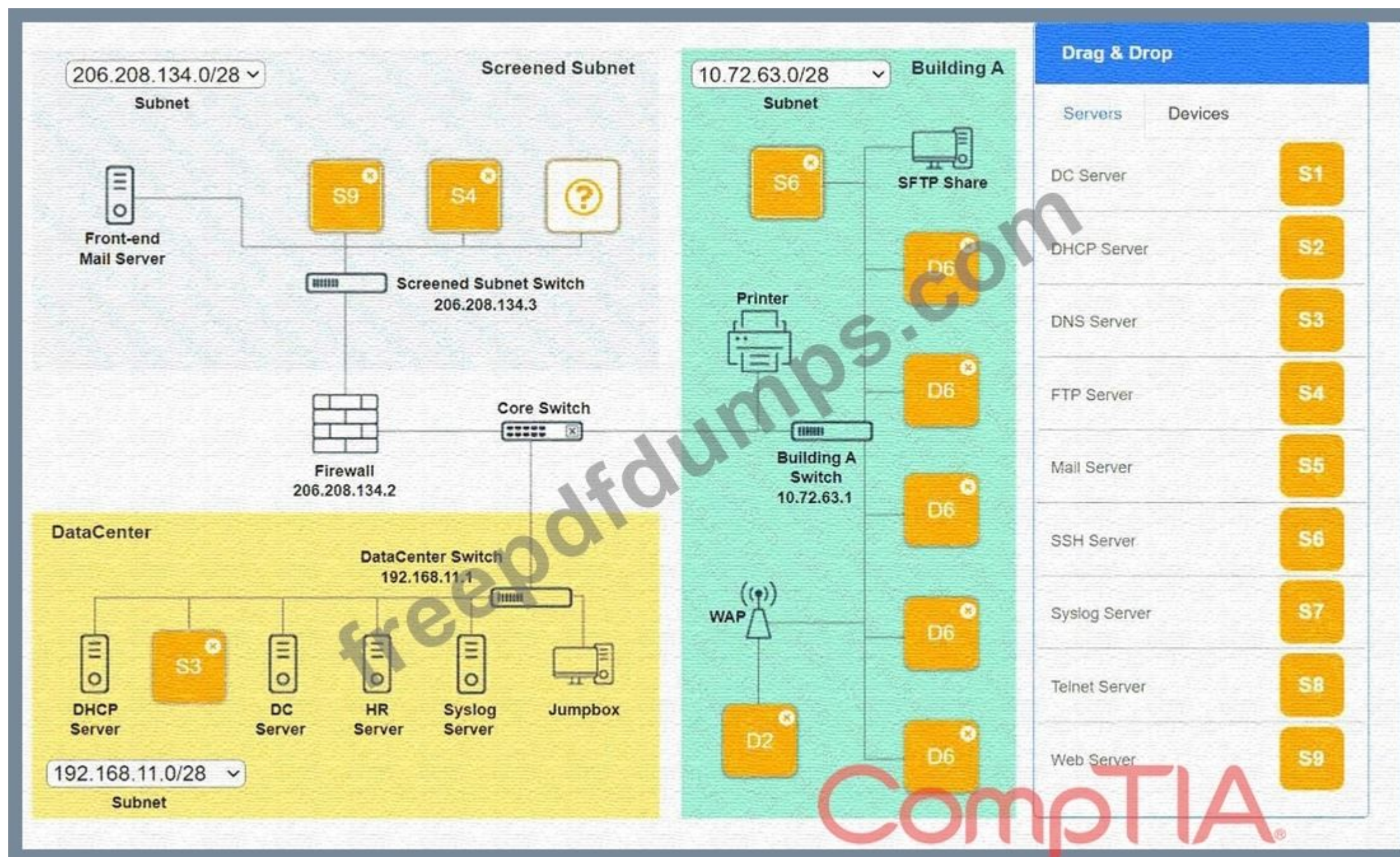
Screened Subnet devices - Web server, FTP server

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

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



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



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

NEW QUESTION: 30

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: A (LEAVE A REPLY)

* Understanding ACLs:

* Access Control Lists (ACLs): A set of rules used to control network traffic and restrict access to network resources by filtering packets based on IP addresses, protocols, or ports.

* Implementing Security Zones:

* Defining Zones: ACLs can be used to create security zones by applying specific rules to different departments, ensuring that only authorized traffic is allowed between these zones.

- * Control Traffic: ACLs control inbound and outbound traffic at network boundaries, enforcing security policies and preventing unauthorized access.
- * Comparison with Other Options:
- * Port Security: Limits the number of devices that can connect to a switch port, preventing MAC address flooding attacks, but not used for defining security zones.
- * Content Filtering: Blocks or allows access to specific content based on predefined policies, typically used for web filtering rather than network segmentation.
- * NAC (Network Access Control): Controls access to the network based on the security posture of devices but does not define security zones.
- * Implementation Steps:
- * Define ACL rules based on the requirements of each department.
- * Apply these rules to the appropriate network interfaces or firewall policies to segment the network into security zones.

References:

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

NEW QUESTION: 31

An organization recently connected a new computer to the LAN. The user is unable to ping the default gateway. The technician examines the configuration and sees a self-assigned IP address. Which of the following is the most likely cause?

- A. The DHCP server is not available
- B. An RFC1918 address is being used
- C. The TCP/IP stack is disabled
- D. A static IP is assigned

Answer: (SHOW ANSWER)

When a host fails to obtain an IP address from a DHCP server, it assigns itself an APIPA (Automatic Private IP Addressing) address in the 169.254.x.x range, commonly described as a "self-assigned IP." This prevents communication outside the local link, including reaching the default gateway.

- B). RFC1918 addresses are private ranges (10.x.x.x, 172.16-31.x.x, 192.168.x.x), but these are not self- assigned.
- C). If the TCP/IP stack were disabled, the host wouldn't have any IP at all.
- D). If a static IP were assigned, it would show a configured value, not self-assigned.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - IP addressing issues, DHCP failures, APIPA behavior.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

Users on the network are experiencing slow throughput. A technician wants to increase throughput without changing any switch hardware. Which of the following solutions should the technician implement?

- A. SVI configuration
- B. VLAN trunking
- C. 802.1Q tagging
- D. Link aggregation

Answer: D (LEAVE A REPLY)

The correct answer is D. Link aggregation. Link aggregation combines multiple physical switch links into one logical connection. This increases available bandwidth and can also add redundancy, all without replacing the switch hardware itself. If users are experiencing slow throughput and the goal is to improve capacity using existing equipment, bundling links is a common and effective solution.

The other options do not directly increase throughput. SVI configuration provides Layer 3 interfaces for VLANs, but it does not add link capacity. VLAN trunking allows multiple VLANs to traverse one connection, but that does not increase bandwidth by itself. 802.1Q tagging identifies VLAN membership on tagged frames; it is related to trunking, not throughput expansion.

In many enterprise environments, link aggregation is implemented through standards such as LACP. This lets several ports act together as one logical channel, which can help distribute traffic more efficiently across the bundled interfaces. For Network+ exam scenarios, when the requirement is to improve throughput using the current switch hardware rather than buying faster switches, link aggregation is the most appropriate answer.

NEW QUESTION: 33

A network administrator is setting up a firewall to protect the organization's network from external threats.

Which of the following should the administrator consider first when configuring the firewall?

- A. Required ports, protocols, and services
- B. Inclusion of a deny all rule
- C. VPN access
- D. Outbound access originating from customer-facing servers

Answer: A (LEAVE A REPLY)

When configuring a firewall, the first step is identifying which ports, protocols, and services are required for normal business operations. This ensures only legitimate traffic is allowed. After establishing the required rules, a default deny rule is added for security.

- B). Deny all rule is important, but it should come after defining required rules.
- C). VPN access is a service to configure, but only after determining baseline needs.
- D). Outbound traffic policies are part of refinement, not the first consideration.

References (CompTIA Network+ N10-009):

Domain: Network Security - Firewall configuration, rule order, least privilege.

NEW QUESTION: 34

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: A (LEAVE A REPLY)

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: 35

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 correct answer is C. Address pool exhaustion. The client has an address in the 169.254.x.x range, which is an APIPA address automatically assigned when a system cannot get a valid IP lease from DHCP. The absence of both a default gateway and a DHCP server entry confirms that the laptop did not receive proper network settings from the DHCP service.

Among the choices, the most likely cause is that the DHCP server has no addresses left in its scope. When the address pool is exhausted, new or renewing clients cannot obtain a lease and must self-assign an APIPA address instead. A client with that kind of address cannot normally reach internal resources such as an intranet site because it lacks the correct network configuration.

The other options do not align with the evidence shown. A short DHCP lease duration could create frequent renewals, but it does not directly explain this output. An IIS malfunction would affect the web server, not the client's IP assignment. An IDS misconfiguration would not normally cause a host to self-assign a 169.254 address.

This is a DHCP-related problem, and from the available answers, address pool exhaustion is the best explanation.

NEW QUESTION: 36

Which of the following is a company most likely enacting if an accountant for the company can only see the financial department's shared folders?

A. General Data Protection Regulation

B. Least privilege network access

C. Acceptable use policy

D. End user license agreement

Answer: B (LEAVE A REPLY)

Least privilege network access is a principle that restricts users' access rights to only what is necessary for them to perform their job functions. In this case, the accountant's access is limited to only the financial department's shared folders, ensuring that they cannot access other parts of the network unnecessarily. This reduces the risk of unauthorized access and potential data breaches. References: CompTIA Network+ Exam Objectives and official study guides.

NEW QUESTION: 37

Users are reporting issues with mobile phone connectivity after a cellular repeater was recently installed.

Users also note that the phones are rapidly losing battery charge. Which of the following should the technician check first to troubleshoot the issue?

A. WPS configuration

B. Signal strength

C. Channel frequency

D. Power budget

Answer: B (LEAVE A REPLY)

When signal strength is poor, mobile devices constantly boost their transmission power in an attempt to maintain a stable connection. This results in dropped calls/data and rapid battery drain. Since a repeater was installed, misalignment or misconfiguration could be degrading the signal strength.

A). WPS applies to Wi-Fi, not cellular repeaters.

C). Channel frequency might matter for interference, but signal strength is the most direct cause of the described symptoms.

D). Power budget applies to PoE and wired devices, not mobile phones.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Wireless/cellular troubleshooting, signal strength impact, user symptoms (battery drain, poor connectivity).

NEW QUESTION: 38

Which of the following does a router prioritize first in the route selection process?

A. Prefix length

B. Metric

C. Administrative distance

D. Default route

Answer: A ([LEAVE A REPLY](#))

In the router route selection process, the first priority is the longest prefix match, also known as prefix length.

According to CompTIA Network+ (N10-009) routing concepts, routers examine the destination IP address in the packet and compare it to entries in the routing table. When multiple routes exist, the router selects the route with the most specific match, meaning the route with the longest subnet mask (largest number of matching bits). For example, a /30 route is preferred over a /24, and a /24 is preferred over a /16 if all match the destination.

Only after the longest prefix match is determined do other factors come into play. Administrative distance (AD) is used to determine which routing source is more trustworthy when the same network is learned from different routing protocols (e.g., OSPF vs. RIP). Metric is then used within the same routing protocol to determine the best path (e.g., hop count, cost, bandwidth). A default route (0.0.0.0/0) is used only when no more specific match exists.

Therefore, prefix length is always evaluated first in route selection.

NEW QUESTION: 39

A technician is designing a cloud service solution that will accommodate the company's current size, compute capacity, and storage capacity. Which of the following cloud deployment models will fulfill these requirements?

A. SaaS

B. PaaS

C. IaaS

D. IaC

Answer: ([SHOW ANSWER](#)**)**

Infrastructure as a Service (IaaS) provides scalable compute power, storage, and networking resources on demand. It is the best choice for a company that needs to customize its cloud solution based on size, compute capacity, and storage needs.

IaaS Benefits:

Provides virtual machines, storage, and networking resources.

Scalable based on company needs.

Reduces the need for physical infrastructure.

Incorrect Options:

A: SaaS (Software as a Service): Delivers software applications (e.g., Google Docs, Microsoft 365) but does not provide compute/storage infrastructure.

B: PaaS (Platform as a Service): Provides a development environment for application deployment but not full infrastructure control.

D: IaC (Infrastructure as Code): A methodology for automating infrastructure, not a cloud deployment model.

Reference:

NEW QUESTION: 40

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: 41

A network administrator configures a new network discovery tool and is concerned that it might disrupt business operations. Which of the following scan types should the administrator configure?

- A.** Authenticated
- B.** Ad hoc
- C.** Unauthenticated
- D.** Scheduled

Answer: D (LEAVE A REPLY)

If the administrator is concerned a new discovery tool could disrupt operations, the safest option is to configure scheduled scans. Network+ (N10-009) operations guidance emphasizes minimizing impact by running potentially noisy tasks (discovery, vulnerability checks, inventory scans) during defined maintenance windows or off-peak hours. A scheduled scan allows controlled timing, predictable load, and easier coordination with change management, monitoring, and support teams. This reduces the risk of saturating links, overwhelming devices with queries, or triggering alerts during business-critical periods.

Ad hoc scanning is on-demand and may occur at any time, which increases the chance of disruption if run during peak usage. Authenticated versus unauthenticated describes whether the scanner uses credentials to log into systems for deeper visibility; that choice affects depth and accuracy, but it doesn't directly address when scanning occurs to reduce business impact. An authenticated scan can still be disruptive if run at the wrong time, and an unauthenticated scan can still generate significant traffic. Since the key concern is operational disruption, controlling scan timing via scheduled scans is the best mitigation.

NEW QUESTION: 42

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

- A.** Neighbor adjacency
- B.** Link state flooding
- C.** Administrative distance
- D.** Hop count

Answer: (SHOW ANSWER)

Introduction to Administrative Distance

Administrative distance (AD) is a value used by routers to rank routes from different routing protocols. AD represents the trustworthiness of the source of the route. Lower AD values are more preferred. If a router has multiple routes to a destination from different sources, it will choose the route with the lowest AD.

Static Routes and Backup Routes

When a dynamic routing protocol is not used, static routes can be employed. Static routes are manually configured routes. To ensure a backup route, multiple static routes to the same destination can be configured with different AD values.

Configuring Static Routes with Administrative Distance

The primary route is configured with a lower AD value, making it the preferred route. The backup route is configured with a higher AD value. In the event of the primary route failure, the router will then use the backup route.

Example Configuration:

plaintext

Copy code

```
ip route 192.168.1.0 255.255.255.0 10.0.0.1 1
```

```
ip route 192.168.1.0 255.255.255.0 10.0.0.2 10
```

In the above example, 192.168.1.0/24 is the destination network.

10.0.0.1 is the next-hop IP address for the primary route with an AD of 1.

10.0.0.2 is the next-hop IP address for the backup route with an AD of 10.

Verification:

After configuration, use the show ip route command to verify that the primary route is in use and the backup route is listed as a candidate for use if the primary route fails.

References:

CompTIA Network+ guide explains the concept of administrative distance and its use in static routing configuration (see page #Ref9 Basic Configuration Commands).

NEW QUESTION: 43

After extremely high temperatures cause a power outage, the servers automatically shut down, even though the UPSs for the servers still have hours of battery life. Which of the following should a technician recommend?

- A. Include backup power for air-conditioning units
- B. Configure door locks to automatically lock during power outages
- C. Increase UPS battery size
- D. Add an IoT-enabled thermostat

Answer: (SHOW ANSWER)

Servers shut down due to overheating, not loss of electrical power. Although UPS units had battery life, without cooling systems (HVAC/air conditioning) running on backup power, server rooms overheated.

Backup power for air-conditioning is essential in data center design.

- B). Door locks are unrelated to server shutdown.
- C). Increasing UPS capacity won't help cooling.
- D). IoT thermostats may monitor temperature but won't prevent overheating.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - Environmental controls, power redundancy, HVAC systems.

NEW QUESTION: 44

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

- A. Toner and probe
- B. Cable tester

C. Visual fault locator

D. Network tap

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 45

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

A. 802.1Q tagging

B. Full duplex

C. Link aggregation

D. QoS

Answer: (SHOW ANSWER)

Link aggregation (also known as port trunking or EtherChannel) combines multiple network connections in parallel to increase throughput and provide redundancy. When two switches are connected with multiple links without any additional configuration, a Layer 2 loop may occur. Link aggregation prevents these loops by treating the multiple connections as a single logical link, using a protocol such as LACP (Link Aggregation Control Protocol).

From Andrew Ramdayal's guide:

"Link aggregation allows you to combine multiple network connections to increase the bandwidth and provide redundancy. It helps prevent Layer 2 loops when connecting switches with multiple links by making them operate as a single logical interface."

NEW QUESTION: 46

A network technician is configuring the company's network of 100 Mbps Layer 2 switches. The technician wants increased throughput for the uplinks between switches. The technician connects multiple redundant links between the switches. Which of the following should the technician configure?

A. Spanning Tree Protocol

B. Switch Virtual Interfaces

C. Native VLAN

D. First Hop Redundancy Protocol

Answer: A (LEAVE A REPLY)

When multiple redundant links exist between switches, Spanning Tree Protocol (STP) is required to prevent switching loops. STP blocks redundant paths but can allow aggregation if configured with protocols like LACP.

B). SVIs provide Layer 3 interfaces, not loop prevention.

C). Native VLAN defines the untagged VLAN but does not manage loops.

D). FHRP (VRRP, HSRP, GLBP) provides gateway redundancy, not switch uplink management.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - STP, redundancy, loop prevention.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 47

A network technician installs a new 19.7ft (6m), Cat 6, UTP cable for the connection between a server and a switch. Communication to the server is degraded, and the NIC statistics show dropped packets and CRC errors. Which of the following cables would the technician most likely use instead to reduce the errors?

- A. Coaxial cable
- B. 9.8ft (3m) cable
- C. Plenum cable
- D. STP cable

Answer: D (LEAVE A REPLY)

The errors described - dropped packets and CRC (Cyclic Redundancy Check) errors - often indicate electromagnetic interference (EMI) on unshielded twisted pair (UTP) cabling. The correct replacement is STP (Shielded Twisted Pair), which has shielding that protects signals from external interference, ensuring better reliability in noisy environments such as data centers or near heavy electrical equipment.

A). Coaxial is not used for modern Ethernet server-switch links.

B). Shorter UTP cable does not solve EMI issues.

C). Plenum cable refers to cable jacket type for fire safety, not electrical shielding.

STP cabling reduces interference and ensures reliable gigabit+ Ethernet connections between servers and switches.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Cabling issues, UTP vs. STP, EMI.

NEW QUESTION: 48

A company implements a video streaming solution that will play on all computers that have joined a particular group, but router ACLs are blocking the traffic. Which of the following is the most appropriate IP address that will be allowed in the ACL?

- A. 127.0.0.1
- B. 172.17.1.1
- C. 224.0.0.1
- D. 240.0.0.1

Answer: (SHOW ANSWER)

224.0.0.1 is a multicast address that allows packets to be sent to all hosts within a multicast group. Since video streaming often uses multicast to efficiently distribute data to multiple clients without unnecessary duplication, this is the correct answer.

*Why not the other options?

*127.0.0.1 (A) - This is the loopback address used for internal device testing, not for multicast traffic.

*172.17.1.1 (B) - This is a private unicast address, meaning it can only send packets to one specific host.

*240.0.0.1 (D) - This falls within the reserved experimental IP address range and is not used for multicast.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 7: IP Addressing and Subnetting

NEW QUESTION: 49

A security engineer is trying to connect cameras to a 12-port PoE switch, but only eight cameras turn on.

Which of the following should the engineer check first?

- A. Ethernet cable type
- B. Voltage
- C. Transceiver compatibility
- D. DHCP addressing

Answer: ([SHOW ANSWER](#))

Power over Ethernet (PoE) allows devices such as cameras, access points, and VoIP phones to receive both power and data over the same Ethernet cable. If only eight out of twelve cameras turn on, the most likely issue is that the PoE switch has exceeded its power budget (total wattage capacity).

PoE Budget Limitation: PoE switches have a maximum power output, which can limit the number of devices they support simultaneously.

Voltage Check: Different PoE standards exist:

802.3af (PoE): Supplies up to 15.4W per port

802.3at (PoE+): Supplies up to 30W per port

802.3bt (PoE++): Supplies up to 60-100W per port

Power Draw Calculation: If each camera requires 15W and the switch can only provide 120W, then only 8 cameras ($8 \times 15W = 120W$) will turn on.

Incorrect Options:

- A). Ethernet Cable Type: Most PoE devices work with Cat5e and above. Cable type could be an issue, but power limitation is the more immediate concern.
- C). Transceiver Compatibility: Only relevant if fiber transceivers or modules are in use, but not likely the root cause for power-related issues.
- D). DHCP Addressing: DHCP issues affect network connectivity, not power delivery.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on Power over Ethernet (PoE)

NEW QUESTION: 50

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: 51

Which of the following Layer 1 devices is responsible for the termination of fiber-optic connections on an SFP-capable switch?

- A. Transceiver
- B. Modem
- C. Ethernet NIC
- D. Repeater

Answer: A ([LEAVE A REPLY](#))

A transceiver is the correct answer because it is the Layer 1 (Physical Layer) component that physically terminates and converts fiber-optic signals on an SFP-capable switch. In CompTIA Network+ N10-009 objectives, transceivers-such as SFP, SFP+, QSFP, and QSFP+ modules-are explicitly identified as physical interface components that handle signal transmission and reception. These modules convert electrical signals from the switch into optical signals for fiber cabling (and vice versa), enabling communication over different media types and distances.

A modem is also a Layer 1 device, but its purpose is to modulate and demodulate signals for WAN technologies such as DSL or cable-it does not terminate fiber connections on switches. An Ethernet NIC provides network access for end devices like computers and servers and typically terminates copper Ethernet, not modular fiber interfaces on switches. A repeater regenerates and amplifies signals to extend cable distances but does not provide fiber termination or media conversion at a switch port.

According to Network+ standards, SFP transceivers are essential for flexible network design, allowing administrators to select appropriate fiber types (single-mode or multi-mode), wavelengths, and distances while remaining compliant with physical layer requirements.

NEW QUESTION: 52

Which of the following must be implemented to securely connect a company's headquarters with a branch location?

- A. Split-tunnel VPN
- B. Clientless VPN
- C. Full-tunnel VPN
- D. Site-to-site VPN

Answer: D ([LEAVE A REPLY](#))

Site-to-Site VPN: A site-to-site VPN is used to securely connect two networks, such as a company's headquarters and a branch location, over the internet. This type of VPN creates a secure tunnel for data transmission, ensuring confidentiality and integrity.

Split-tunnel VPN (A): Allows some traffic to bypass the VPN tunnel, which may not secure all communications.

Clientless VPN (B): Used for individual users to access the network without VPN client software.

Full-tunnel VPN (C): Typically used for individual user traffic rather than connecting two networks.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Secure Network Connections).

NEW QUESTION: 53

Which of the following would be violated if an employee accidentally deleted a customer's data?

- A. Integrity
- B. Confidentiality
- C. Vulnerability
- D. Availability

Answer: (SHOW ANSWER)

Availability refers to ensuring that data is accessible when needed. If a customer's data is accidentally deleted, it impacts availability, as the data can no longer be accessed.

NEW QUESTION: 54

A network engineer receives a new router to use for WAN connectivity. Which of the following best describes the layer the network engineer should connect the new router to?

- A. Access
- B. Core
- C. Leaf
- D. Spine

Answer: C ([LEAVE A REPLY](#))

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

In a spine-leaf architecture, endpoints (including servers, firewalls, and WAN/edge routers) connect to leaf switches. Leaf switches then uplink to spine switches; spine switches do not have endpoints connected directly to them. Therefore, a WAN router (an external/edge device) should connect to the leaf layer-often specifically to a "border leaf" that handles external connectivity.

Why not B. Core or D. Spine? In spine-leaf, "core" isn't a formal layer, and spines are designed only to interconnect leafs, not to terminate endpoints.

Why not A. Access? "Access" is a term from the traditional three-tier model (access-distribution-core). In modern spine-leaf language, the analogous layer for endpoint attachment is the leaf.

References (CompTIA Network+ N10-009):

Domain: Network Infrastructure - Data center and campus architectures (spine-leaf vs. three-tier), roles of leaf/spine, WAN/edge connectivity points.

NEW QUESTION: 55

Which of the following enables an organization to leverage an identity provider to manage access across SaaS applications?

- A. PKI
- B. SSO
- C. TACACS+
- D. RADIUS

Answer: B ([LEAVE A REPLY](#))

SSO (Single Sign-On) allows an organization to use an identity provider (IdP) to centrally manage authentication and access across multiple SaaS applications. In the Network+ (N10-009) objectives, identity and access management concepts include federated authentication, centralized account control, and reducing password sprawl. With SSO, users authenticate once to the IdP, and the IdP then provides assertions/tokens to SaaS services (commonly using federation standards such as SAML or OIDC in real environments). This improves security (fewer reused passwords, easier MFA enforcement), streamlines user experience, and simplifies administration (provisioning/deprovisioning from one place).

PKI supports certificates and encryption/signing, but it is not the core mechanism for managing access across many SaaS apps via an IdP. TACACS+ is typically used for device administration (AAA) on network equipment, and RADIUS commonly supports network access (802.1X, VPN) AAA-both are important AAA protocols but do not describe the SaaS-wide "one login across many apps" capability. Therefore, SSO is the best answer.

NEW QUESTION: 56

Which of the following is used to estimate the average life span of a device?

- A. RTO
- B. RPO
- C. MTBF
- D. MTTR

Answer: C ([LEAVE A REPLY](#))

* 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: 57

Which of the following is used to describe the average duration of an outage for a specific service?

- A. RPO
- B. MTTR
- C. RTO
- D. MTBF

Answer: B ([LEAVE A REPLY](#))

MTTR (Mean Time to Repair) is the average time it takes to repair a system or service after a failure. It helps in measuring the downtime and planning recovery processes.

NEW QUESTION: 58

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: 59

Which of the following network traffic types is sent to all nodes on the network?

- A. Unicast
- B. Broadcast
- C. Multicast
- D. Anycast

Answer: B ([LEAVE A REPLY](#))

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

A broadcast message is delivered to all nodes in a broadcast domain (e.g., ARP requests).

A). Unicast is one-to-one.

C). Multicast is one-to-many but only to subscribed members.

D). Anycast is one-to-one-of-many, sending to the nearest node.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Traffic types: unicast, multicast, broadcast, anycast.

NEW QUESTION: 60

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: 61

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.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

A network administrator needs to create a way to redirect a network resource that has been on the local network but is now hosted as a SaaS solution. Which of the following records should be used to accomplish the task?

- A. TXT
- B. AAA
- C. PTR
- D. CNAME

Answer: D (LEAVE A REPLY)

To redirect a network resource that has moved from a local network to a Software-as-a-Service (SaaS) solution, the network administrator needs to configure a DNS record that maps an alias to the new canonical name (hostname) of the SaaS provider's server. The CNAME (Canonical Name) record is used to alias one domain name to another, effectively redirecting requests to the new hostname without needing to update the IP address directly. This is ideal for SaaS solutions, where the provider's server hostname is used, and the IP address may change dynamically.

Why not TXT? A TXT record is used to store arbitrary text data, such as SPF records for email authentication or verification strings, not for redirecting resources.

Why not AAA? There is no such thing as an "AAA" record in DNS. This might be a typo for AAAA (IPv6 address record), but AAAA maps a hostname to an IPv6 address, not an alias.

Why not PTR? A PTR record is used for reverse DNS lookups (mapping an IP address to a hostname), not for redirecting a resource to a new hostname.

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

NEW QUESTION: 63

A network administrator is setting up two new firewalls for redundancy and needs to implement a redundant internet connection. Which of the following routing technologies will the administrator most likely use?

- A. EIGRP
- B. RIPv2
- C. OSPF

D. BGP

Answer: D ([LEAVE A REPLY](#))

The answer is D. BGP . When a company wants a redundant internet connection , especially across more than one external path or provider, Border Gateway Protocol (BGP) is the routing technology most commonly associated with that design. BGP is used between autonomous systems and is the standard protocol for making routing decisions across the internet or between an organization and one or more ISPs.

The other options are interior routing protocols. EIGRP , RIPv2 , and OSPF are generally used inside an organization to exchange routes within a private network environment. They are not the normal answer when the question specifically says internet connection redundancy . That wording points outward, beyond the internal LAN or campus routing domain.

In practical terms, BGP gives administrators a way to influence path selection, advertise network prefixes, and maintain reachability if one outside connection fails. That is why it appears in questions involving multihoming, ISP failover, or resilient edge connectivity. Since the scenario mentions redundant firewalls and a need for a redundant internet connection, the best match is the routing technology designed for external route exchange. For Network+, that technology is BGP .

NEW QUESTION: 64

A network administrator needs to connect a department to a new network segment. They need to use a DHCP server located on another network. Which of the following can the administrator use to complete this task?

A. IP Helper

B. Reservation

C. Exclusion

D. Scope

Answer: ([SHOW ANSWER](#))

An IP Helper (IP Helper Address) allows DHCP requests to pass through routers and reach a DHCP server on another network.

* DHCP broadcasts are not forwarded across routers by default, so an IP Helper Address is needed to relay the request.

* This is crucial for large networks where a single DHCP server serves multiple subnets.

* Option B (Reservation): Ensures a specific IP address is assigned to a MAC address but does not relay DHCP across networks.

* Option C (Exclusion): Prevents specific IP addresses from being assigned, but does not help with DHCP relay.

* Option D (Scope): Defines the range of IP addresses available for DHCP clients but does not assist in cross-network communication.

? Reference: CompTIA Network+ (N10-009) Official Study Guide - Section: DHCP and IP Addressing

NEW QUESTION: 65

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

A. SSH

B. DHCP

C. NTP

D. SNMP

Answer: ([SHOW ANSWER](#))

The correct answer is SNMP (Simple Network Management Protocol) because it is specifically designed to collect and transmit network management and status information between managed devices and management systems. According to CompTIA Network+ (N10-009) objectives, SNMP is used for monitoring and managing network devices such as routers, switches, servers, and printers.

SNMP operates using a manager-agent model. The SNMP manager (such as a network monitoring server) communicates with SNMP agents installed on network devices. Agents send traps and inform messages, which are unsolicited status alerts indicating events such as device failures, high CPU usage, or link outages.

The manager can also poll agents to retrieve performance metrics and configuration details stored in the Management Information Base (MIB).

SSH (Option A) is used for secure remote administration. DHCP (Option B) dynamically assigns IP addresses. NTP (Option C) synchronizes time between devices. None of these protocols are designed for network status monitoring and alert messaging.

Therefore, SNMP is the correct protocol for sending networking status messages between devices and management systems.

Bottom of Form

NEW QUESTION: 66

Which of the following provides two switches with the most uptime if a power outage occurs?

- A. Plugging both switches into the same PDU
- B. Plugging each switch into a different circuit
- C. Plugging each switch into a different PDU
- D. Plugging each switch into a different UPS

Answer: D ([LEAVE A REPLY](#))

Plugging each switch into a different UPS provides the most uptime during a power outage. A UPS, or uninterruptible power supply, provides temporary battery power when utility power fails. Using separate UPS units also improves redundancy because a failure of one UPS does not necessarily affect both switches. This design helps maintain network availability and supports fault tolerance during electrical outages.

The CompTIA Network+ N10-009 objectives include network availability, redundancy, power management, UPS usage, and environmental considerations. Network switches are critical infrastructure devices, and loss of switch power can disconnect users, servers, wireless access points, VoIP phones, and other dependent systems. A UPS gives administrators time to maintain operations during short outages or shut systems down gracefully during longer outages.

Plugging both switches into the same PDU creates a single point of failure. Plugging each switch into a different circuit improves electrical redundancy, but it does not provide backup power if both circuits lose utility power. Plugging each switch into a different PDU can help with power distribution, but a PDU alone does not provide battery backup unless connected to a UPS. Therefore, different UPS units provide the best uptime.

NEW QUESTION: 67

Which of the following typically uses compromised systems that become part of a bot network?

- A. Evil twin attack
- B. DDoS attack
- C. XML injection
- D. Brute-force password attack

Answer: B ([LEAVE A REPLY](#))

A DDoS (Distributed Denial of Service) attack is often launched from botnets - networks of compromised systems (bots or zombies) under the control of an attacker. These devices flood the target with traffic to disrupt services.

A: Evil twin attack is a wireless spoofing method.

C: XML injection targets web applications.

D: Brute-force attacks repeatedly guess passwords but don't involve a botnet by default.

Reference:

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

NEW QUESTION: 68

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as login information and attributes, to providers?

- A. IAM
- B. MFA
- C. RADIUS
- D. SAML

Answer: D (LEAVE A REPLY)

The correct answer is SAML (Security Assertion Markup Language). SAML is an XML-based standard used for single sign-on (SSO) and identity federation. It allows identity providers (IdPs) to share authentication and authorization data with service providers (SPs), passing secure tokens containing user attributes and credentials.

A). IAM (Identity and Access Management) is the broader framework, not specifically XML-based.

B). MFA enforces multiple factors for authentication but does not involve XML assertions.

C). RADIUS is an AAA protocol, but it uses UDP, not XML assertions.

SAML is widely used in federated identity systems, enabling secure authentication across different domains and applications without requiring multiple credentials.

References (CompTIA Network+ N10-009):

Domain: Network Security - Authentication methods, SAML, SSO.

NEW QUESTION: 69

A network technician is troubleshooting a connectivity issue on a server. Which of the following commands is the most effective for checking whether the server is receiving network traffic?

A. traceroute

B. tcpdump

C. nslookup

D. arp

Answer: B (LEAVE A REPLY)

The correct answer is B. tcpdump. According to the CompTIA Network+ N10-009 objectives, troubleshooting network connectivity often requires validating whether traffic is actually reaching a device.

tcpdump is a command-line packet analyzer that captures and displays packets being transmitted or received on a network interface in real time. This makes it the most effective tool among the options for verifying whether a server is receiving network traffic.

When using tcpdump, a technician can observe incoming packets, identify source and destination IP addresses, check protocols, and determine whether expected traffic (such as HTTP, ICMP, or DNS) is reaching the server. This directly helps isolate issues such as firewall blocking, routing problems, or application-layer failures.

The other options serve different purposes. traceroute is used to identify the path packets take across a network and diagnose routing issues, but it does not confirm packet arrival at the server interface.

nslookup is used to query DNS servers for name resolution and is unrelated to packet capture. arp is used to view or manipulate the Address Resolution Protocol table, which maps IP addresses to MAC addresses, but it does not show live traffic flow.

Therefore, tcpdump is the most appropriate tool for confirming whether the server is receiving network traffic.

NEW QUESTION: 70

A storage network requires reduced overhead and increased efficiency for the amount of data being sent.

Which of the following should an engineer likely configure to meet these requirements>?

A. Link speed

B. Jumbo frames

C. QoS

D. 802.1q tagging

Answer: B (LEAVE A REPLY)

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

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

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

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

Network 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: 71

A network administrator is creating a subnet that will include 45 separate hosts on a small private network within a large network architecture. Which of the following options is the most efficient use of network addresses when assigning this network?

- A.** 10.0.50.128/25
- B.** 10.7.142.128/27
- C.** 10.152.4.192/26
- D.** 10.192.1.64/28

Answer: C ([LEAVE A REPLY](#))

For 45 hosts, the minimum subnet size must allow at least 46 usable addresses (1 each for network and broadcast addresses).

A /26 subnet provides 64 addresses, 62 usable - suitable.

A /27 subnet gives only 30 usable - insufficient.

A /25 offers 126 usable - more than needed.

A /28 provides just 14 - too small.

So, the most efficient subnet with minimal wastage is /26.

From Andrew Ramdayal's guide:

"When designing subnets, always choose the smallest subnet mask that still accommodates all hosts. A /26 provides 62 usable host addresses, suitable for networks with about 50 hosts."

NEW QUESTION: 72

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: A ([LEAVE A REPLY](#))

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: 73

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: C ([LEAVE A REPLY](#))

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: 74

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: 75

After a recent power outage, users are reporting performance issues accessing the application servers.

Wireless users are also reporting intermittent Internet issues.

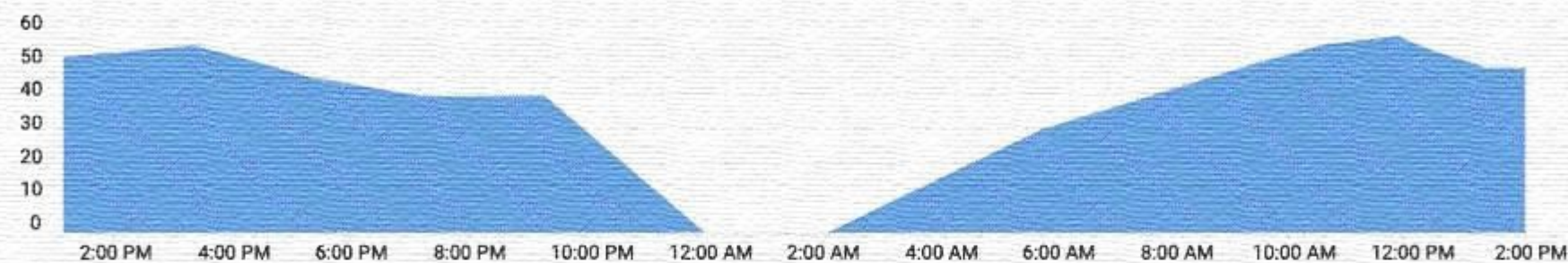
INSTRUCTIONS

Click on each tab at the top of the screen. Select a widget to view information, then use the drop-down menus to answer the associated questions. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

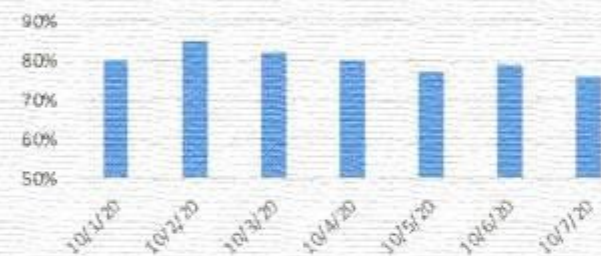
Wireless Client Distribution



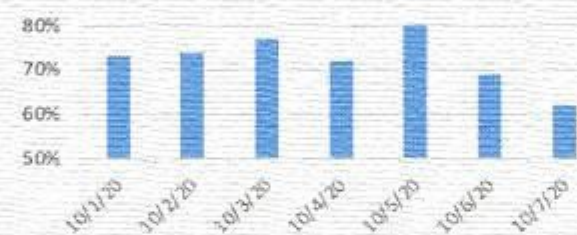
Wireless Users Connected - 24 Hours



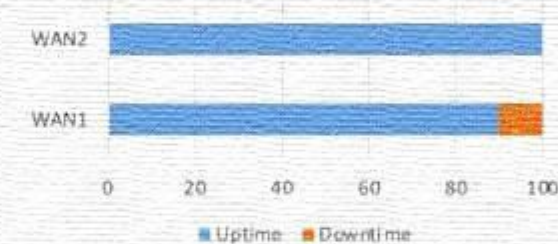
Ram Usage



Processor Usage



WAN Health



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

Which WAN station should be preferred for VoIP traffice?

WAN 1

Select WAN

WAN 1

WAN 2

Device Status



Alert (3)
Up (8)
Warning (2)
Down (1)

Top Hosts

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

Which device is experiencing connectivity issues?

Select Answer

Router A

Router B

WAP1

WAP2

WirelessController

Switch A

Switch B

DHCP Server

Web Server

APP Server

Router A

Which workstation IP is generating the MOST traffic?

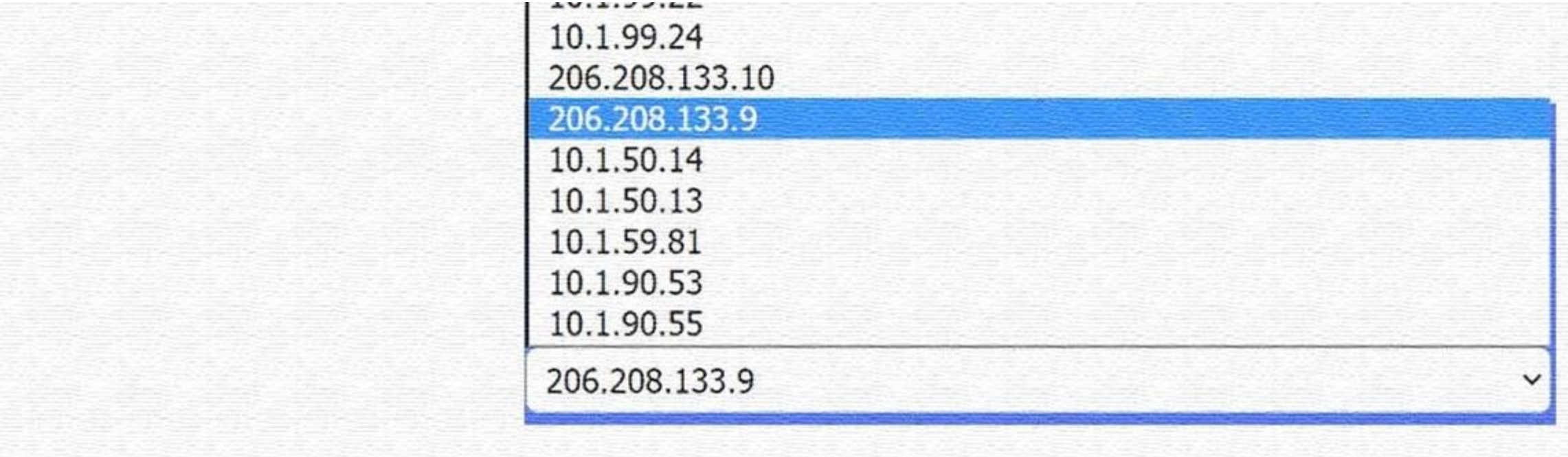
Select Answer

10.1.99.28

10.1.99.14

10.1.99.10

10.1.99.22



Answer:

See the answer and solution below.

Explanation:

Network Health:

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

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

WAN 1:

Uplink Speed: 10G

Total Usage: 26.969GB Up / 1.748GB Down

Average Throughput: 353MBps Up / 23.42MBps Down

Loss: 2.51%

Average Latency: 24ms

Jitter: 9.5ms

WAN 2:

Uplink Speed: 1G

Total Usage: 930GB Up / 138GB Down

Average Throughput: 12.21MBps Up / 1.82MBps Down

Loss: 0.01%

Average Latency: 11ms

Jitter: 3.9ms

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

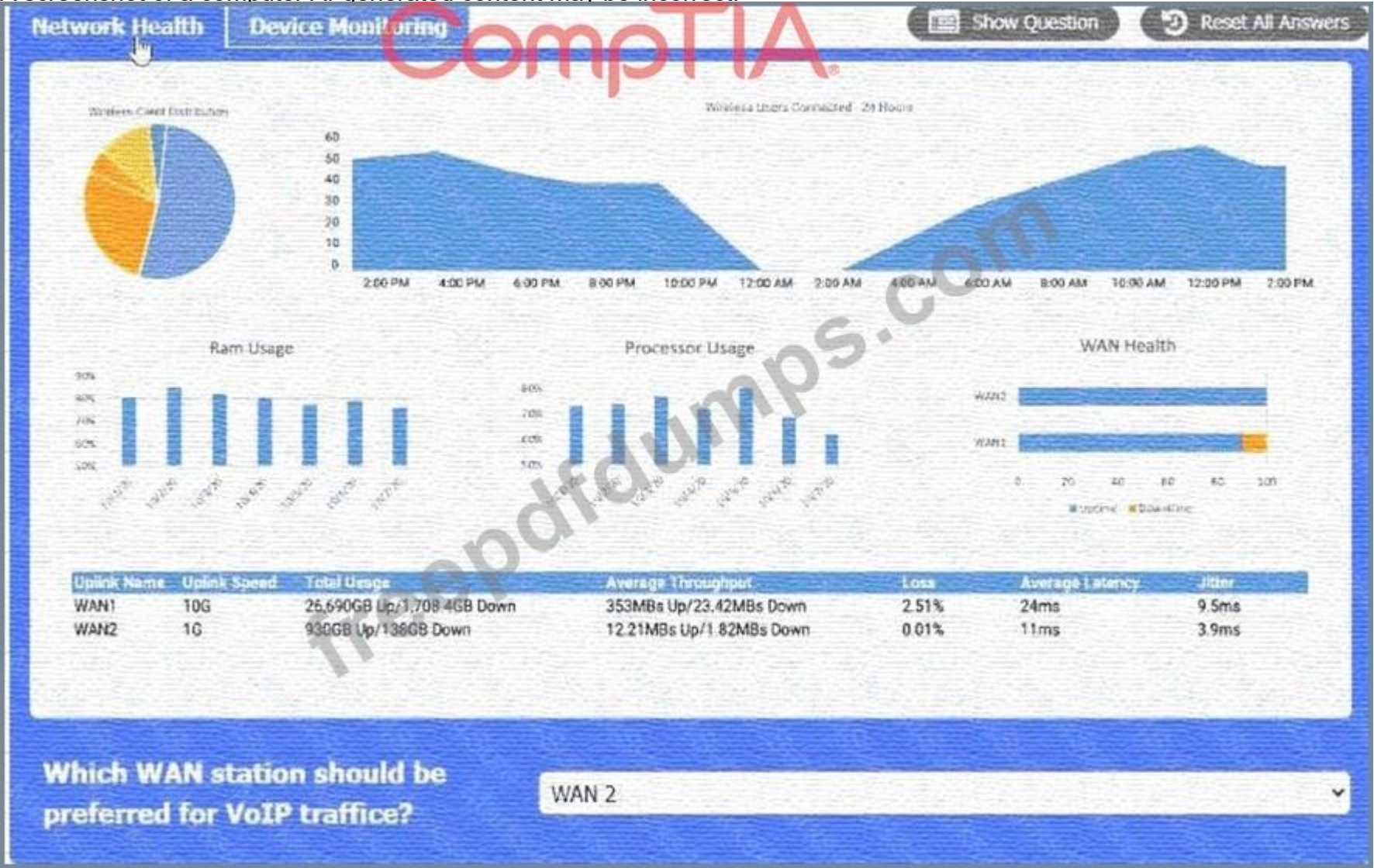
Given this information, WAN 2 would generally be preferred for VoIP traffic due to its lower latency, lower jitter, and significantly lower loss percentage, despite its lower bandwidth compared to WAN 1. The high bandwidth of WAN 1 may be more suitable for other types of traffic that are less sensitive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

Device Monitoring:

the device that is experiencing connectivity issues is the APP Server or Router 1, which has a status of Down.

This means that the server is not responding to network requests or sending any data. You may want to check the physical connection, power supply, and configuration of the APP Server to troubleshoot the problem.

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



NEW QUESTION: 76

Which of the following steps of the troubleshooting methodology comes after testing the theory to determine cause?

- A. Verify full system functionality.
- B. Document the findings and outcomes.
- C. Establish a plan of action.
- D. Identify the problem.

Answer: (SHOW ANSWER)

The CompTIA Troubleshooting Methodology states that after testing the theory, the next step is to establish a plan of action to resolve the issue.

Troubleshooting Steps:

Identify the problem.

Establish a theory of probable cause.

Test the theory to determine the cause.

Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

A: Verify full system functionality - Happens after implementing the solution.

B: Document the findings and outcomes - Final step, happens after resolving the issue.

C: Establish a plan of action - # Correct answer. Comes immediately after confirming the cause.

D: Identify the problem - First step, already completed.

Reference:

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

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 77

A client wants to increase overall security after a recent breach. Which of the following would be best to implement? (Select two.)

A. Least privilege network access

B. Dynamic inventories

C. Central policy management

D. Zero-touch provisioning

E. Configuration drift prevention

F. Subnet range limits

Answer: A,C (LEAVE A REPLY)

To increase overall security after a recent breach, implementing least privilege network access and central policy management are effective strategies.

* Least Privilege Network Access: This principle ensures that users and devices are granted only the access necessary to perform their functions, minimizing the potential for unauthorized access or breaches.

By limiting permissions, the risk of an attacker gaining access to critical parts of the network is reduced.

* Central Policy Management: Centralized management of security policies allows for consistent and streamlined implementation of security measures across the entire network. This helps in quickly responding to security incidents, ensuring compliance with security protocols, and reducing the chances of misconfigurations.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses network security principles, including least privilege and policy management.

* Cisco Networking Academy: Provides training on implementing security policies and access controls.

* Network+ Certification All-in-One Exam Guide: Covers strategies for enhancing network security and managing policies effectively.

NEW QUESTION: 78

Which of the following is used most often when implementing a secure VPN?

A. IPSec

B. GRE

C. BGP

D. SSH

Answer: A (LEAVE A REPLY)

The most common protocol for secure VPNs is IPsec (Internet Protocol Security). IPsec provides confidentiality, integrity, and authentication for VPN traffic, typically using ESP (Encapsulating Security

Payload). It is used in both site-to-site and remote access VPNs.

B). GRE encapsulates traffic but does not provide encryption.

C). BGP is a routing protocol, not a VPN technology.

D). SSH can be used for secure tunneling but is not the standard for VPN deployment.

IPsec is the industry standard because it operates at Layer 3, securing IP traffic regardless of the application, making it highly versatile.

References (CompTIA Network+ N10-009):

Domain: Network Security - VPN protocols, IPsec, ESP.

NEW QUESTION: 79

Which of the following technologies most likely increases the potential for packet loss due to timeout?

A. Load balancer

B. IDS

C. CDN

D. QoS

Answer: A (LEAVE A REPLY)

A load balancer is the best answer because it sits in the traffic path and distributes client requests across multiple backend servers. Since a load balancer tracks sessions, health checks, connection states, and response timers, incorrect timeout values or overloaded backend systems can cause client sessions to expire before the server responds. When that happens, packets or connections may be dropped, reset, or redirected, creating symptoms that appear as packet loss or failed application communication.

The CompTIA Network+ N10-009 objectives include availability concepts, load balancing, traffic management, and network performance troubleshooting. Load balancers are useful for improving scalability and fault tolerance, but they also introduce another decision point in the traffic path. If persistence, health checks, or timeout settings are misconfigured, application traffic can be interrupted.

An IDS is usually passive and monitors copied traffic, so it is less likely to directly cause packet loss. A CDN generally reduces latency and improves delivery by serving content closer to users. QoS is designed to prioritize important traffic and reduce delay, jitter, and packet loss for sensitive applications such as VoIP.

Therefore, the most likely technology to increase packet loss due to timeout is a load balancer.

NEW QUESTION: 80

A network technician was recently onboarded to a company. A manager has tasked the technician with documenting the network and has provided the technician With partial information from previous documentation.

Instructions:

Click on each switch to perform a network discovery by entering commands into the terminal. Fill in the missing information using drop-down menus provided.

Core Switch 1 Prompt



```
C:\> nmap
% Invalid input detected.
C:\> netdiscover
% Invalid input detected.
C:\> |
```

freepdfdumps.com

CompTIA®



```
Access Switch 1 Prompt
C:\> nmap
% Invalid input detected.
C:\>
```

Answer:

See the Explanation for detailed information on this simulation.

Explanation:

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

Click on each switch to open its terminal window.

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

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

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

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

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

The IP address of Core Switch 1 is 192.168.1.1.

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

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

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

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

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

NEW QUESTION: 81

A company's Chief Information Security Officer requires that servers and firewalls have accurate timestamps when creating log files so that security analysts can correlate events during incident investigations. Which of the following should be implemented?

- A. Syslog server
- B. SMTP
- C. SNMP
- D. NTP

Answer: ([SHOW ANSWER](#))

NTP (Network Time Protocol) synchronizes clocks across network devices, ensuring accurate timestamps in logs. This is critical for correlating events across different systems during investigations.

- A). Syslog collects logs but relies on accurate timestamps already present.
- B). SMTP is an email protocol, unrelated to time synchronization.
- C). SNMP is for monitoring and management, not time.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Time synchronization (NTP), log correlation, security operations.

NEW QUESTION: 82

An attack on an internal server is traced to an isolated guest network. Which of the following best describes the attack?

- A. On-path
- B. DNS poisoning
- C. VLAN hopping
- D. ARP spoofing

Answer: ([SHOW ANSWER](#))

The correct answer is VLAN hopping, which is a Layer 2 attack specifically associated with bypassing network segmentation controls. According to the CompTIA Network+ N10-009 objectives, VLANs are commonly used to isolate traffic between different network segments, such as separating a guest network from internal production systems. When an attack originates from an isolated guest network and successfully reaches an internal server, it strongly indicates a failure or exploitation of VLAN boundaries.

VLAN hopping occurs when an attacker gains access to traffic on another VLAN by exploiting misconfigured switch ports or trunking protocols. Common techniques include switch spoofing, where the attacker pretends to be a switch to negotiate a trunk link, and double-tagging, where two VLAN tags are inserted to trick switches into forwarding traffic across VLANs.

The other options do not best fit this scenario. An on-path (man-in-the-middle) attack requires interception between two communicating hosts but does not inherently bypass VLAN isolation. DNS poisoning manipulates name resolution, not network segmentation. ARP spoofing affects local Layer 2 address resolution within the same broadcast domain and typically cannot cross VLAN boundaries.

The Network+ objectives emphasize proper VLAN configuration, disabling unused trunk ports, and implementing port security to prevent VLAN hopping attacks. In this case, VLAN hopping most accurately explains how a guest network could access internal servers.

NEW QUESTION: 83

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

- A. Implementing enterprise authentication
- B. Requiring the use of PSKs
- C. Configuring a captive portal for users
- D. Enforcing wired equivalent protection

Answer: A ([LEAVE A REPLY](#))

Enterprise authentication (such as WPA2-Enterprise) utilizes unique credentials for each user, typically integrating with an authentication server like RADIUS. This allows for tracking and logging user activity, ensuring that all connections can be traced back to individual users. PSKs (Pre-Shared Keys) are shared among users and do not provide individual accountability. Captive portals can identify users but are

less secure than enterprise authentication, and Wired Equivalent Privacy (WEP) is outdated and not recommended for security purposes.

Reference:

CompTIA Network+ materials highlight enterprise authentication methods as the preferred solution for secure and accountable wireless network access.

NEW QUESTION: 84

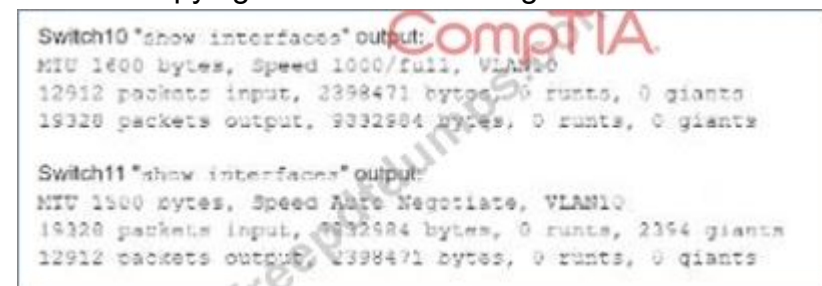
An organization is struggling to get effective coverage using the wireless network. The organization wants to implement a solution that will allow for continuous connectivity anywhere in the facility. Which of the following should the network administrator suggest to ensure the best coverage?

- A. Providing more Ethernet drops for user connections
- B. Changing the current frequency of the Wi-Fi
- C. Implementing additional ad hoc access points
- D. Deploying a mesh network in the building

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 85

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



```
Switch10 "show interfaces" output:
MTU 1600 bytes, Speed 1000/full, VLAN20
12912 packets input, 2398471 bytes, 0 runs, 0 giants
19328 packets output, 3332684 bytes, 0 runs, 0 giants

Switch11 "show interfaces" output:
MTU 1500 bytes, Speed Auto Negotiate, VLAN10
19328 packets input, 3332684 bytes, 0 runs, 2364 giants
12912 packets output, 2398471 bytes, 0 runs, 0 giants
```

Which of the following should the technician most likely do to resolve the issue?

- A. Change the native VLAN on the ports.
- B. Configure STP on both switches.
- C. Disable automatic negotiation on Switch11.
- D. Modify Switch10 MTU value to 1500.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 86

Which of the following is the most cost-efficient way to host email services?

- A. PaaS
- B. IaaS
- C. VPC
- D. SaaS

Answer: D ([LEAVE A REPLY](#))

The correct answer is SaaS (Software as a Service). According to the CompTIA Network+ N10-009 objectives, SaaS is the most cost-efficient cloud model for hosting common business applications such as email, collaboration tools, and productivity suites. With SaaS, the cloud provider manages all infrastructure, operating systems, application software, security updates, and maintenance, significantly reducing administrative overhead and operational costs.

Email services are a prime example of workloads that benefit from SaaS solutions such as Microsoft 365 or Google Workspace. Organizations pay a subscription-based fee, typically per user, and avoid expenses related to server hardware, licensing, patching, backups, redundancy, and disaster recovery. This makes SaaS far more economical than deploying and maintaining email servers internally or in

lower-level cloud models.

IaaS requires the organization to manage virtual machines, operating systems, email server software, and security configurations, which increases both cost and complexity. PaaS simplifies application development but is not designed for hosting ready-made services like email platforms. A VPC (Virtual Private Cloud) is a networking construct, not a service model, and does not inherently provide email hosting functionality.

The Network+ objectives emphasize selecting cloud service models based on cost, management responsibility, and operational efficiency. For standardized services like email, SaaS offers the lowest total cost of ownership and the least administrative burden, making it the best and most cost-effective choice.

NEW QUESTION: 87

A technician is deploying new networking hardware for company branch offices. The bridge priority must be properly set. Which of the following should the technician configure?

- A. Spanning tree protocol
- B. Jumbo frames
- C. Perimeter network
- D. Port security

Answer: A (LEAVE A REPLY)

Spanning Tree Protocol (STP) uses bridge priority values to determine the root bridge in a switched network topology. Correctly configuring bridge priority helps in maintaining a loop-free and efficient network.

The document explains:

"Spanning Tree Protocol (STP) uses bridge priority values to determine which switch will be the root bridge, ensuring loop prevention and efficient path selection within the network."

NEW QUESTION: 88

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

- A. Uninterruptible power supply
- B. Surge protector
- C. Power distribution units
- D. Temperature and humidity control

Answer: D (LEAVE A REPLY)

Temperature and humidity controls the best way to reduce the risk of electrostatic discharge (ESD). Dry environments significantly increase the likelihood of static buildup, which can discharge and damage sensitive components. By controlling humidity, the environment becomes less prone to static electricity.

Reference:Section 2.4 - Important Factors of Physical Installations - "Environmental Considerations"

NEW QUESTION: 89

Which of the following tools uses ICMP to help determine whether a network host is reachable?

- A. tcpdump
- B. netstat
- C. nslookup
- D. ping

Answer: D (LEAVE A REPLY)

Ping sends ICMP Echo Request packets and waits for Echo Replies to verify host reachability and measure round-trip time.

- A). tcpdump captures packets but does not test reachability.
- B). netstat displays open ports and network sessions.
- C). nslookup queries DNS servers for name resolution.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - ICMP operation, troubleshooting tools.

NEW QUESTION: 90

A network 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 insufficient.

Answer: C (LEAVE A REPLY)

An SVI (Switched Virtual Interface) is a logical interface on a Layer 3-capable switch used to route traffic between VLANs. This is particularly useful in environments where voice and data traffic need to be separated, as each type of traffic can be assigned to different VLANs and routed accordingly.

* SVI (Switched Virtual Interface): A virtual interface created on a switch for inter-VLAN routing.

* VLAN Routing: Enables the routing of traffic between VLANs on a Layer 3 switch, allowing for logical separation of different types of traffic, such as voice and data.

* Use Case: Commonly used in scenarios where efficient and segmented traffic management is required, such as in VoIP implementations.

Network References:

* CompTIA Network+ N10-007 Official Certification Guide: Discusses VLANs, SVIs, and their applications in network segmentation and routing.

* Cisco Networking Academy: Provides training on VLAN configuration and inter-VLAN routing using SVIs.

* Network+ Certification All-in-One Exam Guide: Covers network segmentation techniques, including the use of SVIs for VLAN routing.

NEW QUESTION: 91

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 perform this testing?

- A. Ping
- B. Dig
- C. Ifconfig
- D. nmap

Answer: D (LEAVE A REPLY)

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 92

Which of the following attacks can cause users who are attempting to access a company website to be directed to an entirely different website?

- A. DNS poisoning
- B. Denial-of-service
- C. Social engineering
- D. ARP spoofing

Answer: A (LEAVE A REPLY)

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance. References: CompTIA Network+ study materials.

NEW QUESTION: 93

A network administrator configured a router interface as 10.0.0.95 255.255.255.240. The administrator discovers that the router is not routing packets to a web server with IP 10.0.0.81/28. Which of the following is the best explanation?

- A. The web server is in a different subnet.
- B. The router interface is a broadcast address.
- C. The IP address space is a class A network.
- D. The subnet is in a private address space.

Answer: B ([LEAVE A REPLY](#))

Understanding Subnetting:

The subnet mask 255.255.255.240 (or /28) indicates that each subnet has 16 IP addresses (14 usable addresses, 1 network address, and 1 broadcast address).

Calculating the Subnet Range:

Subnet Calculation: For the IP address 10.0.0.95 with a /28 subnet mask:

Network address: 10.0.0.80

Usable IP range: 10.0.0.81 to 10.0.0.94

Broadcast address: 10.0.0.95

Router Interface Configuration:

Broadcast Address Issue: The IP address 10.0.0.95 is the broadcast address for the subnet 10.0.0.80/28.

Configuring a router interface with the broadcast address will cause routing issues as it is not a valid host address.

Comparison with Other Options:

The web server is in a different subnet: The web server (10.0.0.81) is within the same subnet range (10.0.0.80 /28).

The IP address space is a class A network: While 10.0.0.0 is a Class A network, this does not explain the routing issue caused by the broadcast address.

The subnet is in a private address space: The private address space designation (RFC 1918) does not impact the routing issue related to the broadcast address configuration.

Resolution:

Reconfigure the router interface with a valid host IP address within the usable range, such as 10.0.0.94.

References:

CompTIA Network+ study materials on subnetting and IP address configuration.

NEW QUESTION: 94

Which of the following allows an individual to access multiple websites using one set of credentials?

- A. SAML
- B. One-time password
- C. OpenID Connect
- D. SSO

Answer: D ([LEAVE A REPLY](#))

Single sign-on, or SSO, allows a user to access multiple applications, systems, or websites using one set of credentials. With SSO, the user authenticates once through an identity provider, and that authentication can then be trusted by multiple service providers. This improves user convenience, reduces password fatigue, and allows organizations to centralize authentication policies.

The CompTIA Network+ N10-009 objectives include authentication methods, identity and access management, and security concepts. SSO is commonly implemented using protocols or standards such as SAML, OAuth, or OpenID Connect, but SSO is the overall concept being described in the question. SAML is a protocol often used for browser-based federated authentication, especially in enterprise environments. OpenID Connect is an authentication layer built on OAuth 2.0 and is also commonly used for federated login. However, both are implementation methods rather than the general capability described. A one-time password is a temporary authentication code, often used as part of multifactor authentication, but it does not by itself allow access to multiple websites using one credential set. Therefore, SSO is the correct answer.

NEW QUESTION: 95

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: A (LEAVE A REPLY)

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: 96

An organization has four departments that each need access to different resources that do not overlap. Which of the following should a technician configure in order to implement and assign an ACL?

- A. VLAN
- B. DHCP
- C. VPN
- D. STP

Answer: A (LEAVE A REPLY)

VLANs (Virtual Local Area Networks) segment network traffic by department, allowing ACLs (Access Control Lists) to be applied based on VLAN membership, improving security and resource isolation.

Breakdown of Options:

- A). VLAN - Correct answer. VLANs enable logical network segmentation, allowing ACLs per department.
- B). DHCP - Assigns IP addresses but does not control access.
- C). VPN - Provides remote access, not segmentation within a network.
- D). STP - Prevents switching loops, not related to ACL implementation.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain VLANs and network segmentation.

IEEE 802.1Q: VLAN tagging standard

NEW QUESTION: 97

Which of the following types of connectors allows the transmission of network data through a coaxial cable?

- A. SC

- B. MPO
- C. BNC
- D. RJ11

Answer: C (LEAVE A REPLY)

The correct answer is BNC. A Bayonet Neill-Concelman connector, commonly called a BNC connector, is used with coaxial cable. Coaxial cabling has historically been used in Ethernet networks, cable broadband, CCTV systems, and radio frequency applications. BNC connectors use a twist-lock bayonet mechanism that provides a secure connection and helps maintain signal integrity over coaxial media. The CompTIA Network+ N10-009 objectives include recognizing common cable types and connectors used in networking. SC and MPO are fiber-optic connectors, not coaxial connectors. SC connectors are commonly used for fiber connections and have a push-pull design. MPO connectors are multi-fiber push-on connectors often used in high-density fiber environments. RJ11 is commonly associated with telephone cabling and DSL connections, not coaxial Ethernet or RF-style network cabling. Since coaxial cable uses a central conductor, insulation, shielding, and an outer jacket, it requires connectors designed specifically for coaxial signaling.

Among the listed options, BNC is the connector type associated with transmitting network data over coaxial cable.

NEW QUESTION: 98

Which of the following needs to be configured when communicating over multiple VLANs and only a single routed interface is available?

- A. Static routing
- B. NAT
- C. Full duplex
- D. SVI

Answer: D (LEAVE A REPLY)

The correct answer is D. SVI. When traffic must move between multiple VLANs, some Layer 3 function has to exist so each VLAN can have a gateway. A Switched Virtual Interface (SVI) provides a logical Layer 3 interface for a VLAN and is commonly used to support inter-VLAN communication. In exam wording, when the question points to communication across multiple VLANs, the important idea is that each VLAN needs a Layer 3 presence.

The other answer choices do not fit this requirement. Static routing is used to define network paths, but it does not by itself create the VLAN gateway interfaces needed for inter-VLAN traffic. NAT translates addresses, usually for internet access, not for switching between local VLANs. Full duplex is a link operation mode and has nothing to do with routing traffic between VLANs.

The phrase "communicating over multiple VLANs" is the key clue. VLANs are separate broadcast domains, so devices in different VLANs cannot communicate without Layer 3 intervention. Among the choices given, SVI is the only answer that provides that Layer 3 function in a switched environment. That is why D is the best answer.

NEW QUESTION: 99

Which of the following involves an attacker traversing from one part of a network to another part that should be inaccessible?

- A. MAC flooding
- B. DNS poisoning
- C. VLAN hopping
- D. ARP spoofing

Answer: C (LEAVE A REPLY)

VLAN hopping allows an attacker to send traffic into another VLAN without authorization, often by impersonating a switch and negotiating a trunk link. This lets the attacker traverse into normally inaccessible VLANs.

A). MAC flooding disrupts switch operations but does not cross VLANs.

B). DNS poisoning corrupts name resolution.

D). ARP spoofing reroutes local traffic but doesn't grant VLAN traversal.

References (CompTIA Network+ N10-009):

Domain: Network Security - VLAN attacks, unauthorized lateral movement.

NEW QUESTION: 100

A network technician is working on a PC with a faulty NIC. The host is connected to a switch with secured ports. After testing the connection cables and using a known-good NIC, the host is still unable to connect to the network. Which of the following is causing the connection issue?

- A. MAC address of the new card
- B. BPDU guard settings
- C. Link aggregation settings
- D. PoE power budget

Answer: A ([LEAVE A REPLY](#))

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: 101

A company is expanding to another floor in the same building. The network engineer configures a new switch with the same VLANs as the existing stack. When the network engineer connects the new switch to the existing stack, all users lose connectivity. Which of the following is the MOST likely reason?

- A. The new switch has unused ports disabled
- B. The new switch does not have a default gateway
- C. The new switch is connected to an access port
- D. The new switch is in a spanning tree loop

Answer: ([SHOW ANSWER](#))

This describes a Spanning Tree Protocol (STP) loop. If STP isn't correctly configured or a redundant link is added without STP protection, it causes broadcast storms and network outages.

- * A. Unused ports disabled would not affect the entire network.
- * B. Missing default gateway on a switch doesn't cause total network loss.
- * **C. Connecting a switch to an access port can cause VLAN mismatches, but not total connectivity loss unless a loop forms.

#Reference:

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

NEW QUESTION: 102

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

- A. 802.1X
- B. MIMO
- C. ESSID
- D. Band steering

Answer: D ([LEAVE A REPLY](#))

Band steering allows wireless access points to automatically direct capable devices to the 5GHz band, which typically has higher throughput and less interference than the 2.4GHz band, improving performance. The document confirms:

"Band steering helps balance wireless client loads by steering dual-band capable devices to the 5GHz band, which offers higher speeds and less channel congestion than 2.4GHz."

NEW QUESTION: 103

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 provides encryption in transit for HTTPS. It ensures data is encrypted between the client (browser) and the web server, protecting it from interception or tampering.

- * A. SSH is used for secure terminal access, not HTTPS.
- * C. SCADA refers to control systems, not encryption protocols.
- * D. RADIUS is 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: 104

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

- A. Change network translation definitions
- B. Enable 802.1Q
- C. Implement a routing protocol
- D. Set up voice VLANs
- E. Reconfigure the DNS
- F. Place devices in the perimeter network

Answer: B,D (LEAVE A REPLY)

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

- B). Enable 802.1Q: This standard supports VLAN tagging, allowing voice and data traffic to share the same port using separate VLANs.
- D). Set up voice VLANs: Separating voice traffic into its own VLAN improves QoS and manageability.

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

- A). Network translation definitions (NAT) are unrelated to switch-level VLAN configuration.
- C). Routing protocols are not necessary at the switch level for VLAN setup.
- E). DNS is not required for the switch or VLAN setup.
- F). Perimeter network (DMZ) is used for public-facing servers, not VoIP VLANs.

Reference:

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

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

NEW QUESTION: 105

Which of the following protocol ports should be used to securely transfer a file?

- A. 22
- B. 69
- C. 80
- D. 3389

Answer: ([SHOW ANSWER](#))

Port 22 is used for SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol), which encrypt file transfers using SSH (Secure Shell). This ensures data is transmitted securely over the network.

*Why not the other options?

*Port 69 (B) - TFTP (Trivial File Transfer Protocol): Transfers files but is not secure (no encryption).

*Port 80 (C) - HTTP: Used for web traffic, not for file transfer.

*Port 3389 (D) - RDP (Remote Desktop Protocol): Used for remote desktop access, not file transfer.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 5: Network Protocols and Ports

NEW QUESTION: 106

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.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 107

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 $160 \times 2 = 320$ 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: 108

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: 109

A network technician is troubleshooting the connection to the company website. The traceroute command produces the following output:

Traceroute to www.mysite.com (8.8.8.8) over a maximum of 30 hops

10.1.1.1 <1 ms 2. * <1 ms <1 ms

k k

k kTraceroute completeWhich of the following should the technician do to identify the path to the server?

- A.** Review the router's ACL.
- B.** Execute netstat.
- C.** Perform an nslookup.
- D.** Enable LLDP.

Answer: C ([**LEAVE A REPLY**](#)**)**

When traceroute shows asterisks (timeouts) instead of IP addresses or hostnames, it may indicate that intermediate routers are dropping ICMP packets. However, performing an nslookup will reveal the IP address associated with the domain name, confirming that DNS resolution is correct and helping identify the path to the target server. The document states:

"nslookup is used to query DNS servers to retrieve IP address information associated with a domain name, which helps confirm DNS resolution is working correctly even when traceroute results show timeouts."

NEW QUESTION: 110

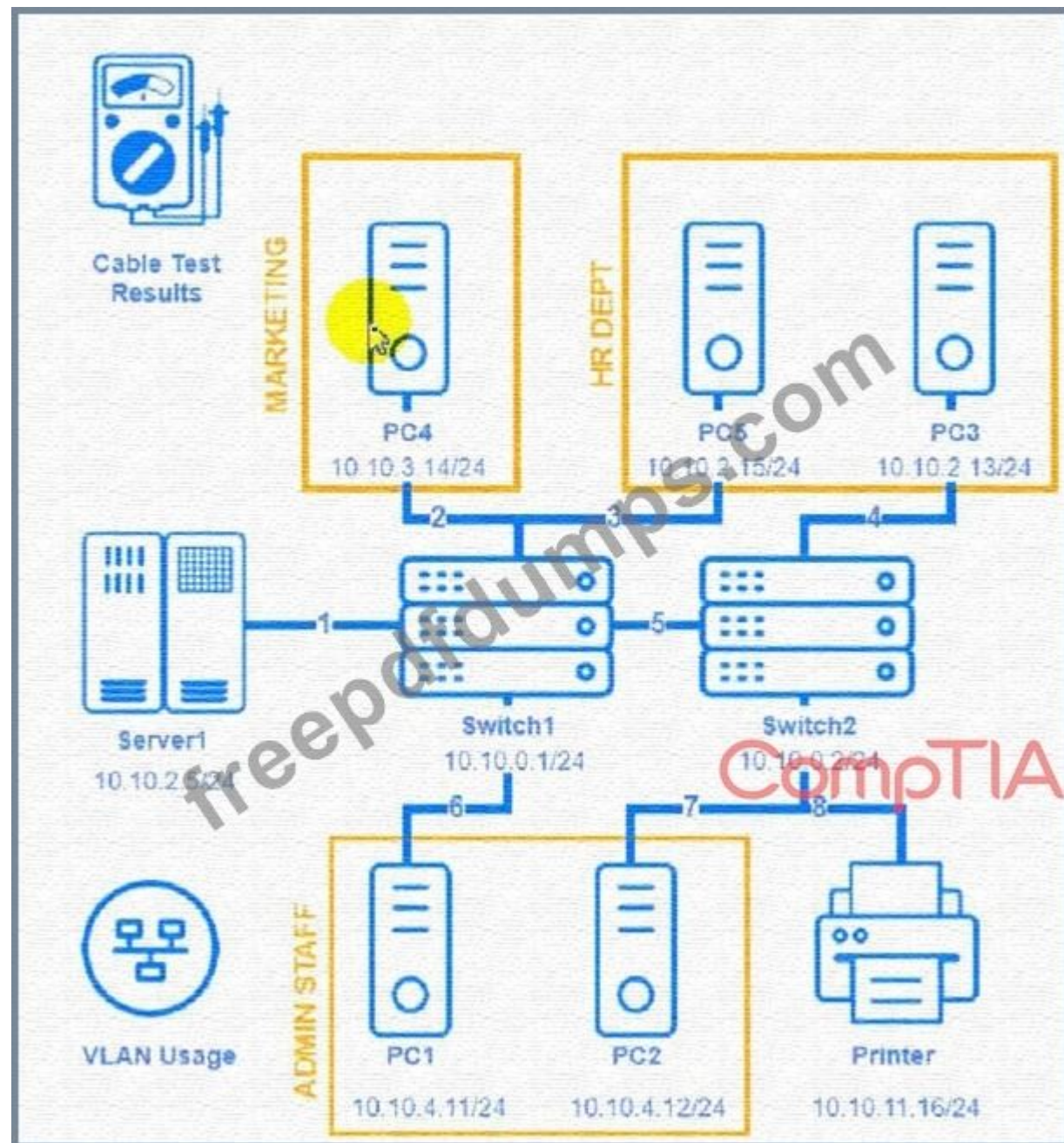
A network technician needs to resolve some issues with a customer ' s SOHO network.

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

INSTRUCTIONS

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

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





Cable Test Results:

Cable 1:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8	
Length: 22M	1	2	3	6	4	5	7	8
VLAN: VLAN 2	1	2	3	6	4	5	7	8
Speed: 1000 FDX	1	2	3	6	4	5	7	8
Port: GigabitEthernet0/1	1	2	3	6	4	5	7	8

Cable 2:

Cable 3:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8			
Length:	18M		1	2	3	6	4	5	7	8
VLAN:	VLAN 2		1	2	3	6	4	5	7	8
Speed:	1000 FDX		1	2	3	6	4	5	7	8
Port:	GigabitEthernet0/3		1	2	3	6	4	5	7	8

Cable 4:

Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 20M		1 2 3 6 4 5 7 8					
VLAN: VLAN 1		1 2 3 6 4 5 7 8					
Speed: 1000 FDX		1 2 3 6 4 5 7 8					
Port: GigabitEthernet0/2		1 2 3 6 4 5 7 8					

Cable Test Results							
Cable 1	Cable 2	Cable 3	Cable 4	Cable 5	Cable 6	Cable 7	Cable 8
Length: 16M		1 2 3 6 4 5 7 8					
VLAN: VLAN 1		1 2 3 6 4 5 7 8					
Speed: 1000 FDX		1 2 3 6 4 5 7 8					
Port: GigabitEthernet0/5		1 2 3 6 4 5 7 8					

Cable Test Results

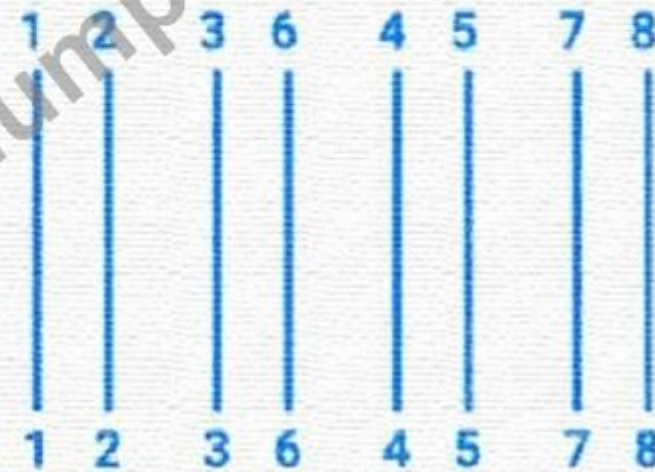
Cable 1 Cable 2 Cable 3 Cable 4 Cable 5 Cable 6 Cable 7 Cable 8

Length: 12M

VLAN: VLAN 1

Speed: 1000 FDX

Port: GigabitEthernet0/1



Printer

HP Network Configuration Page

Model: HP Officejet Pro 8610

General Information

Network Status	Ready
Active Connection Type	Wired
URL(s) for Embedded Web Server	http://HP4D30EC, http://192.168.2.9
Firmware Revision	FDP1CN1347A
Hostname	HP4D30EC
Serial Number	CN3AO1KG42
Internet	Not Connected

802.3 Wired

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

Remediation

Select Device/Cable

Select Device/Cable

- PC1
- PC2
- PC3
- PC4
- PC5
- Printer
- Server1
- Switch1
- Switch2
- Cable1
- Cable2
- Cable3
- Cable4
- Cable5
- Cable6
- Cable7
- Cable8

Answer:

See the Explanation for detailed information on this simulation.

Explanation:

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

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

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

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

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

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

The component with a problem is PC1.

The problem is Incorrect IP address.

The solution is Change the IP address to 192.168.1.10.

You can use the same steps to fill in the remediation form for other components.

To enter commands in each device, you can use the following steps:

Click on the device to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of the device, including its IP address, subnet mask, default gateway, and DNS servers.

Enter the command `ping < IP address >` to test the connectivity and reachability to another device on the network by sending and receiving echo packets. Replace `< IP address >` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Enter the command `tracert < IP address >` to trace the route and measure the latency of packets from the device to another device on the network by sending and receiving packets with increasing TTL values.

Replace `< IP address >` with the IP address of the destination device, such as 192.168.1.1 for Core Switch 1.

Here is an example of how to enter commands in PC1:

Click on PC1 to open its terminal window.

Enter the command `ipconfig /all` to display the IP configuration of PC1. You should see that PC1 has an incorrect IP address of 192.168.2.10, which belongs to VLAN 2 instead of VLAN 1.

Enter the command `ping 192.168.1.1` to test the connectivity to Core Switch 1. You should see that PC1 is unable to ping Core Switch 1 because they are on different subnets.

Enter the command `tracert 192.168.1.1` to trace the route to Core Switch 1. You should see that PC1 is unable to reach Core Switch 1 because there is no route between them.

You can use the same steps to enter commands in other devices, such as PC3, PC4, PC5, and Server 1.

NEW QUESTION: 111

Which of the following cloud deployment models is most commonly associated with multitenancy and is generally offered by a service provider?

- A. Private
- B. Community
- C. Public
- D. Hybrid

Answer: C (LEAVE A REPLY)

The correct answer is public cloud. In public cloud models, a provider (such as AWS, Azure, or Google Cloud) hosts infrastructure and services that are shared across multiple customers, known as multitenancy.

Each tenant is logically isolated, but physical infrastructure is shared, allowing providers to achieve economies of scale.

A). Private cloud is dedicated to one organization, not multitenant.

B). Community cloud is shared among organizations with common interests, but it's less common than public multitenancy.

D). Hybrid cloud combines private and public but does not define tenancy alone.

Public cloud services are the most cost-effective and scalable because they spread costs across many customers, but they require strong security and isolation to protect tenants.

References (CompTIA Network+ N10-009):

Domain: Networking Concepts - Cloud models, multitenancy, public vs private.

NEW QUESTION: 112

After a recent merger, a large number of alerts are coming in regarding extremely high utilization. Which of the following should be generated to help inform new alerting requirements?

- A. SLA
- B. Network diagram
- C. Baseline
- D. Heat map

Answer: C ([LEAVE A REPLY](#))

A baseline establishes normal performance levels for network utilization, latency, jitter, and other metrics.

After a merger, traffic patterns change, so a new baseline is needed to recalibrate monitoring thresholds and avoid excessive false alerts.

A). SLA defines performance agreements with customers but doesn't adjust alerting.

B). Network diagrams show topology, not traffic norms.

D). Heat maps show wireless coverage, not utilization baselines.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Baselines, monitoring, alerting, performance tuning.

NEW QUESTION: 113

A medical clinic recently configured a guest wireless network on the existing router. Since then, guests have been changing the music on the speaker system. Which of the following actions should the clinic take to prevent unauthorized access? (Select two).

A. Isolate smart devices to their own network segment.

B. Configure IPS to prevent guests from making changes.

C. Install a new AP on the network.

D. Set up a syslog server to log who is making changes.

E. Change the default credentials.

F. Configure GRE on the wireless router.

Answer: ([SHOW ANSWER](#))

*A. Isolate smart devices to their own network segment: Network segmentation using VLANs or separate SSIDs ensures that smart devices (like speakers) are not on the same network as guests, preventing unauthorized control.

*E. Change the default credentials: Many IoT devices (e.g., smart speakers) come with default usernames and passwords. If these are not changed, unauthorized users can easily take control.

*Why not the other options?

*B. Configure IPS: IPS (Intrusion Prevention System) detects threats but cannot block specific guest actions on an IoT device.

*C. Install a new AP: A new access point does not solve the unauthorized control issue.

*D. Set up a syslog server: Helps with logging, but does not prevent unauthorized access.

*F. Configure GRE: Generic Routing Encapsulation (GRE) is used for VPN tunneling, which is irrelevant in this case.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 11: Network Security

NEW QUESTION: 114

A research facility is expecting to see an exponential increase in global network traffic in the near future. The offices are equipped with 2.5Gbps fiber connections from the ISP, but the facility is currently only utilizing

1Gbps connections. Which of the following would need to be configured in order to use the ISP's connection speed?

A. 802.1Q tagging

B. Network address translation

C. Port duplex

D. Link aggregation

Answer: D ([LEAVE A REPLY](#))

* Understanding Link Aggregation:

* Definition: Link aggregation combines multiple network connections into a single logical link to increase bandwidth and provide redundancy.

* Usage in High-Bandwidth Scenarios:

* Combining Links: By aggregating multiple 1Gbps connections, the facility can utilize the full 2.5 Gbps bandwidth provided by the ISP.

* Benefits: Enhanced throughput, load balancing, and redundancy, ensuring better utilization of available bandwidth.

* Comparison with Other Options:

* 802.1Q Tagging: Used for VLAN tagging, which does not affect the physical bandwidth utilization.

* Network Address Translation (NAT): Used for IP address translation, not related to link speed or bandwidth aggregation.

* Port Duplex: Refers to the mode of communication (full or half duplex) on a port, not the aggregation of bandwidth.

* Implementation:

* Configure link aggregation (often referred to as LACP - Link Aggregation Control Protocol) on network devices to combine multiple physical links into one logical link.

References:

* CompTIA Network+ study materials on network configuration and link aggregation.

NEW QUESTION: 115

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

A. MAC security

B. Content filtering

C. Screened subnet

D. Perimeter network

Answer: B (LEAVE A REPLY)

Content filtering can be used to block or restrict access to websites and services that facilitate torrenting and other prohibited activities. By implementing content filtering, the company can comply with the ISP's cease- and-desist order and prevent users from accessing torrent sites and engaging in prohibited activities.

References: CompTIA Network+ study materials.

NEW QUESTION: 116

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

98469 packets input, 1681937 bytes, 0 no buffer

Received 1548 broadcasts (25285 multicasts)

65335 runs, 0 giants, 0 throttles

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

0 input packets with dribble condition detected

22781 packets output, 858040 bytes, 0 underruns

0 output errors, 89920 collisions, 0 interface resets

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

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

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

B. The switchport bandwidth needs to be increased.

C. Multicast is not configured correctly on the switch.

D. The NIC is set to half duplex.

Answer: (SHOW ANSWER)

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

The document explains:

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

NEW QUESTION: 117

Which of the following is most closely associated with having a leased line to a public cloud provider?

- A.** VPN
- B.** Direct Connect
- C.** Internet gateway
- D.** Private cloud

Answer: B (LEAVE A REPLY)

Direct Connect is the option most closely associated with having a leased line to a public cloud provider, as defined in the CompTIA Network+ N10-009 objectives under cloud connectivity and WAN technologies.

Direct Connect (or equivalent services such as Azure ExpressRoute or Google Cloud Interconnect) provides a dedicated, private physical connection between an organization's on-premises network and a public cloud provider's infrastructure. This connection bypasses the public internet, offering consistent bandwidth, lower latency, improved performance, and enhanced security.

A VPN uses encrypted tunnels over the public internet, which does not qualify as a leased line and is subject to internet congestion and variable performance. An internet gateway simply allows cloud resources to communicate with the public internet and does not imply a private or dedicated connection. A private cloud refers to a deployment model where cloud resources are dedicated to a single organization; it does not describe the connectivity method or the use of a leased circuit.

According to Network+ objectives, leased-line connectivity to cloud providers is commonly used by enterprises that require high availability, predictable throughput, regulatory compliance, or secure hybrid cloud architectures. Direct Connect is a foundational component of hybrid networking strategies, linking on- premises environments directly to public cloud services using provider-managed circuits.

NEW QUESTION: 118

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: (SHOW ANSWER)

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: 119

A company is implementing a new internal network in which all devices use IPv6 addresses. Which of the following routing protocols will be best for this setup?

- A. EIGRP
- B. OSPFv3
- C. BGP4
- D. iBGP

Answer: ([SHOW ANSWER](#))

For an internal network using IPv6, the best option listed is OSPFv3, which is the OSPF version designed to support IPv6 routing. In Network+ (N10-009) routing objectives, OSPF is a common interior gateway protocol (IGP) used within an organization (an autonomous system) to exchange routes dynamically and converge efficiently. OSPFv3 maintains the link-state approach of OSPF while adding IPv6 support, making it a strong fit for enterprise internal routing where multiple routers and subnets need dynamic path calculation and fast convergence.

BGP4 and iBGP are associated with BGP, primarily used for inter-domain routing on the internet and between large networks; while BGP can carry IPv6 (via MP-BGP), it is generally not the "best" default choice for a typical internal-only enterprise network unless there is a specific design reason. EIGRP can support IPv6 in some implementations, but Network+ typically emphasizes OSPF/OSPFv3 as the widely adopted, vendor- neutral IGP for IPv6 deployments. Given the options and the "best for this setup" wording, OSPFv3 is the most appropriate answer.

NEW QUESTION: 120

Which of the following does BGP use for loop avoidance?

- A. Autonomous system path
- B. Peer autonomous system
- C. Autonomous system length
- D. Public autonomous system

Answer: A ([LEAVE A REPLY](#))

The correct answer is Autonomous system path because BGP (Border Gateway Protocol) prevents routing loops by using the AS_PATH attribute. According to CompTIA Network+ (N10-009) objectives under routing protocols, BGP is a path vector protocol used to exchange routing information between autonomous systems (AS) on the internet.

When a BGP router advertises a route, it includes its autonomous system number (ASN) in the AS_PATH attribute. As the route passes through additional autonomous systems, each AS appends its own ASN to the path. If a BGP router receives a route advertisement that already contains its own ASN in the AS_PATH list, it recognizes this as a loop and rejects the route. This mechanism effectively prevents routing loops across large-scale networks such as the internet.

Option B (Peer autonomous system) refers to neighboring BGP routers but does not describe the loop prevention mechanism. Option C (Autonomous system length) relates to path selection metrics, as shorter AS_PATH lengths are generally preferred, but this is not the loop avoidance function itself. Option D (Public autonomous system) is not a loop prevention mechanism.

Therefore, BGP uses the AS_PATH attribute for loop avoidance.

NEW QUESTION: 121

An organization moved its DNS servers to new IP addresses. After this move, customers are no longer able to access the organization's website. Which of the following DNS entries should be updated?

- A. AAAA
- B. CNAME
- C. MX
- D. NS

Answer: D ([LEAVE A REPLY](#))

When an organization moves its DNS servers to new IP addresses, the NS (Name Server) records must be updated. The NS record defines which DNS servers are authoritative for a domain. If these records still point to the old IP addresses, clients will continue to query the outdated servers, leading to connectivity issues.

Breakdown of Options:

- A). AAAA - This record maps a domain name to an IPv6 address. Since the issue is with DNS resolution, not IP versioning, this is incorrect.
- B). CNAME - A CNAME (Canonical Name) record is used for domain aliasing, not for defining authoritative name servers.
- C). MX - Mail Exchange (MX) records direct email traffic to the correct mail server, which does not impact general website accessibility.

D). NS - Correct answer. NS records must be updated to reflect the new authoritative DNS servers.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.3: Explain the purpose and properties of DNS records.

RFC 1035: Domain Names - Implementation and Specification

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 122

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

A. RDP

B. Telnet

C. GUI

D. API

Answer: D (LEAVE A REPLY)

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

APIs (Application Programming Interfaces) allow automation tools and scripts to push configurations to network devices programmatically. Modern network automation platforms rely on APIs to ensure consistency and scalability.

A). RDP is remote desktop for Windows systems, not automation.

B). Telnet is insecure and manual.

C). GUI requires manual configuration, not automation.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Automation, orchestration, APIs in network management.

NEW QUESTION: 123

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: A (LEAVE A REPLY)

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: 124

After a networking intern plugged in a switch, a significant number of users in a building lost connectivity.

Which of the following is the most likely root cause?

- A. VTP update
- B. Port security issue
- C. LLDP misconfiguration
- D. Native VLAN mismatch

Answer: (SHOW ANSWER)

When a switch is improperly connected to a network, it can cause widespread connectivity issues, especially if there's a misconfiguration in VLAN settings. A Native VLAN mismatch occurs when two switches connected via a trunk link have different native VLANs configured for untagged traffic. This can cause traffic to be sent to the wrong VLAN or dropped, resulting in connectivity loss for users.

Scenario Analysis: The intern likely connected the switch without ensuring that the trunk port's native VLAN matched the existing network configuration. This is a common issue in Cisco-based networks when trunk links are misconfigured.

Why not VTP update? VLAN Trunking Protocol (VTP) updates propagate VLAN configurations across switches. While a VTP misconfiguration could cause issues, it's less likely to immediately disrupt connectivity for many users unless the VTP server deleted critical VLANs, which is not implied here.

Why not Port security issue? Port security restricts access based on MAC addresses, typically affecting individual ports, not causing widespread outages.

Why not LLDP misconfiguration? Link Layer Discovery Protocol (LLDP) is used for device discovery, and misconfiguration is unlikely to cause a broad loss of connectivity.

Reference:CompTIA Network+ N10-009 Objective 2.2: Explain the purpose of network segmentation and VLAN configuration. The CompTIA Network+ Study Guide (e.g., Chapter 6: Switching) discusses VLAN trunking and the importance of matching native VLANs on trunk links to prevent connectivity issues. Native VLAN mismatches are highlighted as a common cause of network disruptions.

NEW QUESTION: 125

Which of the following steps of the troubleshooting methodology would most likely involve comparing current throughput tests to a baseline?

- A. Implement the solution
- B. Verify full system functionality
- C. Document findings
- D. Test the theory

Answer: B (LEAVE A REPLY)

Verifying full system functionality occurs after implementing a fix. This step ensures the solution resolved the issue and that performance is back to expected levels. Comparing current throughput to baseline measurements is part of validation testing to confirm everything is within normal operational parameters.

A). Implement the solution applies the fix but does not confirm results.

C). Document findings happens at the end of troubleshooting.

D). Test the theory comes earlier, when trying to confirm the suspected cause.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Troubleshooting methodology steps, baselines, verification testing.

NEW QUESTION: 126

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: A (LEAVE A REPLY)

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: 127

A technician is implementing a new SD-WAN device with a default configuration. The technician receives a URL via email and connects the new device to the internet to complete the installation. Which of the following is this an example of?

- A. SASE device installation
- B. Zero-touch provisioning
- C. Infrastructure as code
- D. Configuration management

Answer: B ([LEAVE A REPLY](#))

This process describes Zero-touch provisioning (ZTP), where a device automatically pulls its configuration from a cloud controller or URL once connected to the internet. It's common in SD-WAN and modern network appliances.

- A). SASE (Secure Access Service Edge) refers to cloud-delivered network security, not a provisioning method.
- C). Infrastructure as code automates infrastructure deployment using code, but this scenario specifically fits ZTP.
- D). Configuration management tracks and maintains system configurations but doesn't describe the installation process.

Reference:

CompTIA Network+ N10-009 Official Objectives: 4.3 - Explain remote access methods and automation.

NEW QUESTION: 128

Which of the following actions should be taken as part of the first step of the troubleshooting methodology?

- A. Handle multiple problems individually
- B. Create a theory about the possible root cause
- C. Use a top-down approach
- D. Conduct tests to verify ideas

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 129

Which of the following best describes the purpose of a UPS and PDU in a network installation?

- A. To support voltage requirements for devices in an IDF
- B. To manage power consumption in the MDF
- C. To connect multiple devices to a single network connection
- D. To regulate temperature in the MDF and IDF

Answer: A ([LEAVE A REPLY](#))

The correct answer is A. To support voltage requirements for devices in an IDF. In the CompTIA Network+ N10-009 objectives, network infrastructure includes power systems such as Uninterruptible Power

Supplies (UPS) and Power Distribution Units (PDU), which are critical components in both MDF (Main Distribution Frame) and IDF (Intermediate Distribution Frame) environments.

A UPS provides temporary backup power during electrical outages and also conditions power by protecting against surges, spikes, and voltage fluctuations. This ensures that sensitive network equipment such as switches, routers, and servers can continue operating or safely shut down. A PDU, on the other hand, distributes electrical power to multiple devices within a rack, ensuring that all equipment receives the appropriate voltage and sufficient power capacity.

Option B is incorrect because while PDUs can help distribute power, they do not directly manage or optimize power consumption. Option C refers to networking devices like switches, not power equipment.

Option D relates to environmental controls such as HVAC systems, not UPS or PDU devices.

Therefore, the primary purpose of UPS and PDU systems is to ensure stable and adequate power delivery to network devices, particularly in environments like IDFs.

NEW QUESTION: 130

A network engineer added more APs to improve wireless coverage. However, users now report that the connectivity disconnects and reconnects repeatedly. Which of the following is causing the issue?

- A.** Throughput capacity
- B.** Roaming misconfiguration
- C.** Channel overlap
- D.** Packet loss

Answer: C (LEAVE A REPLY)

Adding more access points can improve coverage, but it also increases the risk of co-channel interference if APs are configured on the same or overlapping channels. Channel overlap causes contention and interference, leading to retries, unstable performance, and symptoms that feel like frequent disconnect/reconnect events- especially in dense deployments. Network+ (N10-009) wireless troubleshooting objectives highlight proper channel planning (non-overlapping channels, appropriate channel width) as critical when increasing AP density. If adjacent APs are competing on the same channel (or overlapping channels in 2.4 GHz), clients may experience poor signal-to-noise ratios and repeated reassociations as they struggle to maintain a stable link.

Roaming misconfiguration can cause sticky clients or poor handoffs, but the classic problem introduced immediately after "adding more APs" is interference from bad channel design. Throughput capacity is about available bandwidth and airtime efficiency; it can make things slow, but it doesn't inherently cause repeated disconnect/reconnect loops like interference does. Packet loss is a symptom that may occur due to interference, but the root cause in the options that best fits the scenario is channel overlap.

NEW QUESTION: 131

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: C (LEAVE A REPLY)

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: 132

A network engineer needs to prioritize traffic over a link with the goal of more effectively utilizing the connection. Which of the following should the engineer implement?

- A. CDN
- B. VPN
- C. TTL
- D. QoS

Answer: D (LEAVE A REPLY)

To prioritize traffic and utilize a constrained link more effectively, the engineer should implement QoS (Quality of Service). QoS is a set of mechanisms that classifies and marks traffic (for example, voice, video, business-critical apps) and then applies queuing and scheduling behaviors to ensure important traffic receives preferential treatment during congestion. Network+ objectives commonly connect QoS to supporting real-time applications (VoIP/video) by reducing latency, jitter, and packet loss, while preventing less critical traffic (bulk transfers, updates) from consuming all available bandwidth. Techniques can include traffic classification, DSCP marking, priority queuing, and traffic shaping/policing.

A CDN improves content delivery by caching closer to users, but it doesn't provide link-level prioritization for all traffic types. A VPN provides secure tunneling/encryption, not prioritization. TTL (Time To Live) is an IP header value used to prevent routing loops by limiting packet lifespan; it does not manage bandwidth or prioritize flows. QoS is the standard solution when the goal is to control how bandwidth is allocated under load and to ensure critical services remain performant.

NEW QUESTION: 133

Which of the following is the most likely benefit of installing server equipment in a rack?

- A. Simplified troubleshooting process
- B. Decreased power consumption
- C. Improved network performance
- D. Increased compute density

Answer: D (LEAVE A REPLY)

Installing server equipment in a rack increases compute density by allowing multiple servers to be organized efficiently in a vertical configuration, saving space while housing more devices in a smaller footprint. This is critical for data centers and businesses with high hardware demands.

Simplified troubleshooting process (A): While racks can aid in organizing equipment, this is a secondary benefit, not the primary purpose.

Decreased power consumption (B): Rack installation does not directly reduce power usage; equipment power consumption remains the same.

Improved network performance (C): Racking servers does not inherently improve network performance; that depends on network configurations.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (Rack Installations).

NEW QUESTION: 134

A user notifies a network administrator about losing access to a remote file server. The network administrator is able to ping the server and verifies the current firewall rules do not block access to the network fileshare.

Which of the following tools would help identify which ports are open on the remote file server?

- A. Dig
- B. Nmap
- C. Tracert
- D. nslookup

Answer: B (LEAVE A REPLY)

Nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a computer network. It can be used to identify which ports are open on a remote server, which can help diagnose access issues to services like a remote file server.

- * Port Scanning: Nmap can perform comprehensive port scans to determine which ports are open and what services are running on those ports.

- * Network Discovery: It provides detailed information about the host's operating system, service versions, and network configuration.

- * Security Audits: Besides troubleshooting, Nmap is also used for security auditing and identifying potential vulnerabilities.

Network References:

- * CompTIA Network+ N10-007 Official Certification Guide: Covers network scanning tools and their uses.

- * Nmap Documentation: Official documentation provides extensive details on how to use Nmap for port scanning and network diagnostics.

- * Network+ Certification All-in-One Exam Guide: Discusses various network utilities, including Nmap, and their applications in network troubleshooting.

NEW QUESTION: 135

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: B (LEAVE A REPLY)

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: 136

A user's VoIP phone and workstation are connected through an inline cable. The user reports that the VoIP phone intermittently reboots, but the workstation is not having any network-related issues Which of the following is the most likely cause?

A. The PoE power budget is exceeded.

- B. Port security is violated.
- C. The signal is degraded
- D. The Ethernet cable is not working

Answer: A ([LEAVE A REPLY](#))

Power over Ethernet (PoE) delivers power to devices such as VoIP phones over the same cables used for data.

If the total power requirement of connected devices exceeds the PoE power budget of the switch or injector, some devices may not receive adequate power and could intermittently reboot. This issue would not affect the workstation, which is likely receiving power separately. References: CompTIA Network+ Exam Objectives and official study guides.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 137

Which of the following allows a remote user to connect to the network?

- A. Command-line interface
- B. API gateway
- C. Client-to-site VPN
- D. Jump box

Answer: (SHOW ANSWER)

A Client-to-Site VPN allows a remote user to securely connect to a company's internal network, providing access as if they were physically on-site.

NEW QUESTION: 138

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: 139

A network analyst is installing a wireless network in a corporate environment. Employees are required to use their domain identities and credentials to authenticate and connect to the WLAN. Which of the following actions should the analyst perform on the AP to fulfill the requirements?

- A.** Enable MAC security.
- B.** Generate a PSK for each user.
- C.** Implement WPS.
- D.** Set up WPA3 protocol.

Answer: D (LEAVE A REPLY)

WPA3-Enterprise provides strong security and supports authentication using domain identities through a RADIUS server and 802.1X authentication. This is the best choice for a corporate environment requiring user- based authentication.

WPA3-Enterprise Benefits:

Uses 802.1X with EAP (Extensible Authentication Protocol) to authenticate users via a directory service (e.g., Active Directory).

Eliminates shared passwords (PSK) for authentication.

Provides strong encryption and resistance to brute-force attacks.

Incorrect Options:

A). Enable MAC Security:

MAC filtering is not secure because MAC addresses can be spoofed.

B). Generate a PSK for Each User:

Pre-shared keys (PSK) are used in WPA-Personal, not in an enterprise setting.

Does not scale well in corporate environments.

C). Implement WPS:

Wi-Fi Protected Setup (WPS) is a vulnerable security method meant for home users.

Not suitable for enterprise authentication.

Reference:

CompTIA Network+ N10-009 Official Study Guide - Chapter on Wireless Security and Authentication

NEW QUESTION: 140

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: 141

A customer purchases a new UTM device and wants the development team to integrate some of the device's data-reporting capabilities into the company's custom internal support software. Which of the

following features should the development team use to obtain the device's data?

- A. API
- B. SNMPv2c
- C. SIEM
- D. MIB

Answer: A (LEAVE A REPLY)

An API (Application Programming Interface) is the best choice when a development team needs to integrate a device's reporting data directly into custom software. In Network+ (N10-009) objectives, network operations commonly include device management, monitoring, and automation, and APIs are a key method for programmatic access to operational data (often via REST/HTTPS with structured formats like JSON). This enables the internal support application to pull dashboards, health metrics, events, configuration details, and reporting outputs in a controlled, developer-friendly way.

SNMPv2c is primarily used for network monitoring and polling counters/alerts, but it is less secure (community strings) and is not as flexible for modern application integration as an API. A MIB is not a data-access "feature" by itself; it's the schema/definitions SNMP uses to describe managed objects. A SIEM is a separate security analytics platform that collects and correlates logs/events-useful for security operations, but not the direct interface a custom support tool would typically call to retrieve device reporting data.

NEW QUESTION: 142

A network administrator needs to ensure that users accept internet usage rules. Which of the following will help the administrator accomplish this task?

- A. Captive portal
- B. Acceptable use policy
- C. Network access control
- D. DNS filtering

Answer: A (LEAVE A REPLY)

A captive portal is designed to present terms, conditions, or usage rules to users and require them to acknowledge/accept those rules before granting network or internet access. In Network+ (N10-009) security and access control concepts, captive portals are commonly associated with guest wireless or public access scenarios, where users are redirected to a web page that displays acceptable-use language and requires a click- through acceptance (and sometimes authentication). This provides a technical enforcement point: users must actively accept the rules to proceed, which supports organizational policy compliance and creates a recordable control in many implementations.

An Acceptable Use Policy (AUP) is the document that defines the rules, but by itself it does not technically force a user to acknowledge them at the time of access. NAC controls who/what can connect and can enforce posture and segmentation, but it does not inherently ensure users "accept" usage rules unless paired with a portal workflow. DNS filtering blocks or allows domain access categories (malware, adult content, etc.), which enforces browsing restrictions but does not guarantee user acceptance of rules. Therefore, the best answer to ensure users accept the rules is captive portal.

NEW QUESTION: 143

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: 144

A user ' s home mesh wireless network is experiencing latency issues. A technician has:

- *Performed a speed test.
- *Rebooted the devices.
- *Performed a site survey.
- *Performed a wireless packet capture.

The technician reviews the following information:

SSID	MAC	RSSI	Channel
Home	AAAAAA111112	-83dBm	11
Home	AAAAAA111113	-91dBm	11
Home	AAAAAA111114	-70dBm	11

The technician notices in the packet capture that frames were retransmitted. Which of the following is the most likely cause of the user ' s network issue?

- A. The SSIDs should not be the same.
- B. The network has too much overlap.
- C. The devices are incompatible with the mesh network.
- D. The nodes are underpowered.

Answer: (SHOW ANSWER)

- *Too much overlap on the same channel (all devices on channel 11) causes interference, leading to retransmissions and high latency.
- *Same SSIDs (A) are expected in mesh networks.
- *Device compatibility (C) would show different symptoms.
- *Node power (D) affects coverage, not congestion.

Reference: CompTIA Network+ N10-009 Official Documentation - Wireless Troubleshooting & Signal Interference.

NEW QUESTION: 145

A cloud administrator must ensure that all access to social media websites is prohibited. Which of the following should the administrator use to prevent users from accessing those websites?

- A. NAC
- B. Screened subnet
- C. VPN
- D. Content filter

Answer: D (LEAVE A REPLY)

A content filter is the correct solution because it can block access to specific categories of websites, domains, URLs, or application types, including social media. Content filtering is commonly used to enforce acceptable use policies, reduce risk, improve productivity, and prevent users from accessing prohibited or unsafe web content. In this scenario, the requirement is to stop access to social media websites, so filtering web content by category or URL is the most direct control.

The CompTIA Network+ N10-009 objectives include network security concepts, access control, filtering, and security appliances or services. A content filter may be implemented through a secure web gateway, firewall, DNS filtering platform, proxy server, cloud security platform, or endpoint security solution.

Network Access Control, or NAC, controls whether devices are allowed to connect to the network based on identity, posture, or policy. A screened subnet, also called a DMZ, is used to isolate public-facing services. A VPN provides encrypted connectivity but does not inherently block social media access. Therefore, content filtering is the most appropriate answer.

NEW QUESTION: 146

A newly opened retail shop uses a combination of new tablets, PCs, printers, and legacy card readers. Which of the following wireless encryption types is the most secure and compatible?

- A. WPA3
- B. WPA2
- C. WPA2/WPA3 mixed mode
- D. WPA/WPA2 mixed mode

Answer: C ([LEAVE A REPLY](#))

WPA2/WPA3 mixed mode provides compatibility for older devices (that only support WPA2) while allowing newer devices to take advantage of stronger WPA3 encryption. This ensures maximum compatibility and security in a mixed-device environment.

- A). WPA3 only is most secure but not compatible with legacy devices.
- B). WPA2 only is secure but does not future-proof against WPA3-capable devices.
- D). WPA/WPA2 mixed mode is weaker due to WPA (deprecated, insecure).

References (CompTIA Network+ N10-009):

Domain: Network Security - Wi-Fi encryption standards, WPA2 vs WPA3, mixed-mode compatibility.

NEW QUESTION: 147

Which of the following can be implemented to add an additional layer of security between a corporate network and network management interfaces?

- A. Jump box
- B. Console server
- C. API interface
- D. In-band management

Answer: A ([LEAVE A REPLY](#))

A jump box is a hardened, isolated system that provides secure access to critical infrastructure devices like routers and firewalls.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 4.3: Explain network security techniques.

NEW QUESTION: 148

A systems administrator is investigating why users cannot reach a Linux web server with a browser but can ping the server IP. The server is online, the web server process is running, and the link to the switch is up.

Which of the following commands should the administrator run on the server first?

- A. traceroute
- B. netstat
- C. tcpdump
- D. arp

Answer: B ([LEAVE A REPLY](#))

The `netstat` command provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Running `netstat` on the server can help the administrator verify that the web server process is listening on the expected port (e.g., port 80 for HTTP or port 443 for HTTPS) and that there are no issues with network connections. This is a crucial first step in diagnosing why the web server is not accessible via a browser. References: CompTIA Network+ study materials.

NEW QUESTION: 149

Which of the following is the MOST appropriate solution to extend the network to a building located across the street from the main facility?

- A. Multimode fiber
- B. 802.11ac wireless bridge
- C. Cat 6 copper
- D. Loopback adapter

Answer: B (LEAVE A REPLY)

An 802.11ac wireless bridge is the most practical solution to connect two nearby buildings without trenching or laying physical cable. It provides high-speed, point-to-point connectivity using directional antennas.

- * A. Multimode fiber is effective but expensive and typically limited to 500 meters or less.
- * C. Cat 6 copper is only rated for up to 100 meters - not viable for a street-wide distance.
- * D. Loopback adapter is a troubleshooting tool, not for network extension.

#Reference:

CompTIA Network+ N10-009 Official Objectives: 1.3 - Compare and contrast various network topologies, types, and technologies.

NEW QUESTION: 150

After installing a series of Cat 8 keystones, a data center architect notices higher than normal interference during tests. Which of the following steps should the architect take to troubleshoot the issue?

- A. Check to see if the end connections were wrapped in copper tape before terminating.
- B. Use passthrough modular crimping plugs instead of traditional crimping plugs.
- C. Connect the RX/TX wires to different pins.
- D. Run a speed test on a device that can only achieve 100Mbps speeds.

Answer: A (LEAVE A REPLY)

* Importance of Proper Termination:

* Cat 8 cabling requires precise termination practices to ensure signal integrity and reduce interference. One common requirement is to wrap the end connections in copper tape to maintain shielding and reduce electromagnetic interference (EMI).

* Interference Troubleshooting:

* Interference in high-frequency cables like Cat 8 can be caused by improper shielding or grounding. Checking the end connections for proper wrapping in copper tape is a crucial step.

* Why Other Options are Less Likely:

* Passthrough modular crimping plugs: Not specifically related to interference issues and are typically used for ease of cable assembly.

* Connecting RX/TX wires to different pins: Would likely result in no connection or incorrect data transmission rather than interference.

* Running a speed test on a device that can only achieve 100Mbps speeds: This would not diagnose interference and would not provide relevant information for Cat 8 cabling rated for higher speeds.

* Corrective Actions:

- * Verify that all end connections are properly wrapped with copper tape before termination.
- * Ensure that the shielding is continuous and properly grounded throughout the installation.
- * Retest the cabling for interference after making corrections.

References:

* CompTIA Network+ study materials and structured cabling installation guides.

NEW QUESTION: 151

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.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 152

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

- A. The patch panel
- B. The front of the IDF
- C. The warm aisle
- D. The administrator console

Answer: C (LEAVE A REPLY)

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

The document clarifies:

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

NEW QUESTION: 153

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

- A. 802.1Q tagging
- B. Jumbo frames
- C. Half duplex
- D. Link aggregation

Answer: D (LEAVE A REPLY)

Since the switch supports only 10Gbps per port, achieving 40Gbps throughput requires link aggregation (LACP), which combines multiple 10Gbps links into one logical interface for higher bandwidth.

Breakdown of Options:

- A). 802.1Q tagging - VLAN tagging helps segment traffic but does not increase throughput.
- B). Jumbo frames - Jumbo frames reduce overhead but do not increase bandwidth.
- C). Half duplex - Half duplex restricts communication, reducing performance instead of improving it.
- D). Link aggregation - Correct answer. LACP combines multiple 10Gbps links to provide a 40Gbps connection.

Reference:

CompTIA Network+ (N10-009) Official Study Guide - Domain 1.2: Compare and contrast network topologies and technologies.

IEEE 802.3ad: Link Aggregation Control Protocol (LACP)

NEW QUESTION: 154

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 the Voice VLAN is functioning correctly, but the Data VLAN (C) is either misconfigured or missing. The workstation typically connects through the phone, which tags voice and data traffic separately using VLANs.

- * A. Voice VLAN is for the IP phone, which is already working.
- * B. Native VLAN is for untagged traffic on trunk ports, but doesn't control access directly.
- * D. Trunk port is 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: 155

Two companies successfully merged. Following the merger, a network administrator identified a connection bottleneck. The newly formed company plans to acquire a high-end 40GB switch and redesign the network from a three-tier model to a collapsed core. Which of the following should the administrator do until the new devices are acquired?

- A. Implement the FHRP.
- B. Configure a route selection metric change.
- C. Install a load balancer.
- D. Enable link aggregation.

Answer: D (LEAVE A REPLY)

*The issue described is a network bottleneck due to increased traffic after a merger.

*A collapsed core architecture consolidates the core and distribution layers into a single layer to improve efficiency and reduce latency.

*Until the 40GB switch is acquired, Link Aggregation (LAG) (IEEE 802.3ad / LACP) can be used to combine multiple physical links into a single logical link, increasing bandwidth and reducing bottlenecks.

*FHRP (First Hop Redundancy Protocol) (A) is used for gateway redundancy, not link aggregation.

*Route selection metric changes (B) help with routing decisions but don't address physical link congestion.

*Load balancers (C) distribute traffic for applications, not network links.

#Reference: CompTIA Network+ N10-009 Official Documentation - Network Architecture and Performance Optimization.

NEW QUESTION: 156

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

- A.** Infrastructure as a service
- B.** Software as a service
- C.** Platform as a service
- D.** Network as a service

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 157

A network engineer needs to change, update, and control APs remotely, with real-time visibility over HTTPS.

Which of the following will best allow these actions?

- A.** Web interface
- B.** Command line
- C.** SNMP console
- D.** API gateway

Answer: D ([LEAVE A REPLY](#))

API gateways offer programmable control and real-time communication, commonly over HTTPS, which allows administrators to update and manage devices like access points remotely and efficiently.

From Andrew Ramdayal's guide:

"APIs enable automation and real-time interaction with network devices via secure interfaces, often using HTTPS for encrypted communication and control."

NEW QUESTION: 158

A customer migrates its phone system from analog to a new hosted VoIP/software application solution with integrated video. After installation, some users notice issues with dropped calls, broken video, and slow internet access. The issues start in the mid-morning and continue into the afternoon. However, remote users do not report the same issues. Which of the following is the most likely cause of the issues?

- A.** Roaming misconfiguration
- B.** Signal degradation
- C.** Insufficient bandwidth
- D.** Miswired cable

Answer: C ([LEAVE A REPLY](#))

The best answer is C. Insufficient bandwidth. The pattern in the question matters more than anything else. The company moved to a hosted VoIP and video solution, which means voice and video traffic now depend heavily on the site's internet connection. The problems begin mid-morning and continue into the afternoon, which strongly suggests the link becomes congested during the busiest usage period of the day.

That also explains why users see dropped calls, broken video, and slow internet access all at the same time.

Real-time applications like VoIP and video are very sensitive to delay, jitter, and packet loss. When bandwidth is limited or saturated, those services are usually the first to show noticeable symptoms. The fact that remote users do not report the same issue is another major clue. If the application platform itself were failing, remote users would likely be affected too. Since the issue seems limited to the main site, the bottleneck is most likely the local office's WAN or internet connection rather than the hosted service.

The other options are weaker. Roaming misconfiguration is more of a wireless mobility issue, signal degradation is too vague for this traffic pattern, and a miswired cable would not usually appear only during peak business hours. This points to insufficient bandwidth.

NEW QUESTION: 159

Computer A cannot reach Computer B in the following network:

Computer A: 172.16.2.10/16

Computer B: 172.16.4.10/16

Switch A:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Switch B:

Gi0/1 access VLAN 1, status up/up

Gi0/9 access VLAN 8, status up/up

Gi0/10 access VLAN 5, status administratively down

Which of the following will resolve the issue?

A. Set up link aggregation between Switch A and Switch B on Gi0/9 and Gi0/10

B. Configure spanning tree on Switch A and Switch B

C. Establish a trunk connection between Switch A and Switch B

D. Put Computer A and Computer B in the same /24 subnet

Answer: C (LEAVE A REPLY)

The correct solution is to establish a trunk connection between Switch A and Switch B. Computer A and Computer B are both connected to access VLAN 1 on their local switches. However, the inter-switch link appears to be configured as an access port in VLAN 8. Because the link between the switches is not carrying VLAN 1 traffic, devices in VLAN 1 on separate switches cannot communicate across that connection.

The CompTIA Network+ N10-009 objectives include VLANs, switching, trunking, access ports, and troubleshooting Layer 2 connectivity. Access ports carry traffic for a single VLAN. Trunk ports carry traffic for multiple VLANs between switches, usually using tagging such as IEEE 802.1Q. To allow VLAN 1 devices on both switches to communicate, the inter-switch connection must carry VLAN 1 traffic. A trunk would allow VLAN 1 and other required VLANs to pass between the switches.

Link aggregation is not the issue, and Gi0/10 is administratively down. Spanning Tree Protocol prevents loops but does not fix missing VLAN transport. Changing both hosts to a /24 would not solve the VLAN separation problem and could make IP reachability worse. Therefore, trunking is required.

NEW QUESTION: 160

Which of the following should a network engineer check to verify that updates are still being released for a device?

A. Baseline configuration

B. EOL documentation

C. Asset inventory licensing

D. Software development life cycle

Answer: B (LEAVE A REPLY)

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: 161

A network administrator installs wireless access points (APs) inside an industrial warehouse. A wireless survey shows a large amount of electromagnetic interference. Which of the following cable types should the administrator use to connect the APs to the switch?

- A. UTP
- B. STP
- C. Multimode
- D. Single-mode

Answer: B ([LEAVE A REPLY](#))

The correct answer is STP (Shielded Twisted Pair). According to the CompTIA Network+ N10-009 objectives, environments with high levels of electromagnetic interference (EMI)-such as industrial warehouses with heavy machinery, motors, and electrical equipment-require additional protection at the physical layer to maintain signal integrity.

STP cabling includes shielding around the twisted copper pairs that helps block external electromagnetic signals from interfering with data transmission. This shielding significantly reduces crosstalk and EMI, making STP far more suitable than UTP (Unshielded Twisted Pair) in electrically noisy environments. UTP lacks this shielding and is more prone to signal degradation under such conditions.

While fiber-optic cabling (multimode or single-mode) is completely immune to EMI, it is typically not used to directly connect wireless APs in most enterprise deployments. Wireless access points commonly rely on copper Ethernet connections to support Power over Ethernet (PoE), which supplies both data and electrical power over the same cable. Fiber does not natively support PoE, making it impractical for directly powering APs without additional equipment.

The Network+ objectives emphasize selecting appropriate cabling based on environmental factors and operational requirements. In this scenario, STP provides the optimal balance of EMI resistance, Ethernet compatibility, and PoE support, making it the best choice for connecting APs in an industrial warehouse.

NEW QUESTION: 162

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

- A. ACL
- B. MAC filtering
- C. Port security
- D. NAC

Answer: ([SHOW ANSWER](#)**)**

For a secure 802.1X design that includes BYOD access to a trusted wireless network, the engineer should implement NAC (Network Access Control). In the Network+ (N10-009) objectives, 802.1X provides authentication (commonly via EAP to a RADIUS server), but NAC expands this by enforcing policy-based access decisions-such as device posture checks, user/device identity validation, and dynamic assignment to the appropriate VLAN/role. With BYOD, the organization often needs to confirm whether devices meet requirements (OS version, encryption, security software) and then grant the correct level of access (full, limited, or quarantine/remediation). NAC is the architecture that ties these controls together in a scalable way for wireless networks.

An ACL can restrict traffic after a device connects, but it doesn't perform authentication/posture assessment.

MAC filtering is weak because MAC addresses can be spoofed and it does not provide strong identity assurance. Port security is mainly a wired switch control (limiting MAC addresses per port) and is not the right control set for secure BYOD wireless access. NAC best matches the requirement of secure, policy- driven 802.1X BYOD access.

NEW QUESTION: 163

A technician is plugging an Ethernet cable into a switch to bring a new device online, but the device is not showing an active network connection. Previously, another technician turned off unused switchports as part of device hardening. Which of the following describes the port status?

- A. Error disabled
- B. Idle
- C. Suspended
- D. Administratively down

Answer: ([SHOW ANSWER](#)**)**

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

NEW QUESTION: 164

Following a VoIP deployment, users report issues using the VoIP system. After further review, a network technician reports the following:

- * Dropped calls are occurring.
- * Local file transfer is successful.
- * New firewalls have recently been added.
- * Web traffic is functional.
- * Users experience audio latency.

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

- A.** Conflicting firewall rule
- B.** Spanning tree issue
- C.** Incorrect voice VLAN
- D.** Misconfigured QoS

Answer: ([SHOW ANSWER](#))

Misconfigured QoS is the most likely cause because the symptoms are specific to VoIP quality: dropped calls and audio latency. Voice traffic is highly sensitive to delay, jitter, and packet loss. Quality of Service allows administrators to classify and prioritize voice packets so they are handled ahead of less time-sensitive traffic such as file transfers or general web browsing. If QoS is missing or incorrectly configured, voice packets may compete equally with other traffic and suffer from congestion-related delay or loss.

The CompTIA Network+ N10-009 objectives include VoIP, QoS, traffic shaping, latency, jitter, and performance troubleshooting. The fact that local file transfers and web traffic are functional indicates the general network is working. The problem is with real-time traffic quality rather than total connectivity.

A conflicting firewall rule could block call setup or media streams, but the question emphasizes audio latency, which strongly points to QoS. A spanning tree issue would more likely cause broader Layer 2 instability. An incorrect voice VLAN could prevent phones from receiving proper addressing or access, but users are able to use the VoIP system with poor quality. Therefore, misconfigured QoS is correct.

NEW QUESTION: 165

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

- A.** VXLAN
- B.** IKE
- C.** GRE
- D.** IPsec

Answer: **D** ([LEAVE A REPLY](#))

IPsec (Internet Protocol Security) is the most secure way to provide site-to-site connectivity. It provides robust security services, such as data integrity, authentication, and encryption, 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: 166

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

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

- A. Incorrect default gateway
- B. Faulty Ethernet cable
- C. Wrong duplex settings
- D. VLAN mismatch

Answer: A (LEAVE A REPLY)

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

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

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

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

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

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

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 167

Which of the following protocols has a default administrative distance value of 90?

- A. RIP
- B. EIGRP
- C. OSPF
- D. BGP

Answer: (SHOW ANSWER)

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

NEW QUESTION: 168

A CDN provider needs to implement a solution that delivers services to customers using IPv4, IPv6, or both to ensure interoperability. Which of the following technologies is the most appropriate for this requirement?

- A. Quality of service
- B. Automatic Private IP Addressing
- C. Dual stack
- D. Stateless Address Autoconfiguration

Answer: (SHOW ANSWER)

Dual stack is the most appropriate technology because it allows a device, network, or service to support IPv4 and IPv6 at the same time. In a dual-stack environment, systems can communicate with IPv4-only clients, IPv6-only clients, and clients that support both protocol versions. This is especially important for a CDN provider because customers may connect from many different networks, and not all networks have fully migrated to IPv6.

The CompTIA Network+ N10-009 objectives include IPv4 and IPv6 addressing concepts, network services, and interoperability methods. Dual stack is a common transition strategy because it does not require immediate removal of IPv4. Instead, both protocol stacks operate together while networks gradually adopt IPv6.

Quality of service is used to prioritize traffic, not to provide IPv4 and IPv6 interoperability. Automatic Private IP Addressing assigns a 169.254.x.x address when DHCP fails and applies to IPv4 link-local addressing.

Stateless Address Autoconfiguration allows IPv6 hosts to create their own IPv6 addresses, but it does not provide IPv4 and IPv6 coexistence by itself. Therefore, dual stack is the correct answer.

NEW QUESTION: 169

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: A ([LEAVE A REPLY](#))

Reference: CompTIA Network+ Certification Exam Objectives - Remote Access Methods section.

NEW QUESTION: 170

A network technician needs to connect a new user to the company's Wi-Fi network called SSID: business.

When attempting to connect, two networks are listed as possible choices: SSID: business and SSID: myaccess. Which of the following attacks is occurring?

- A.** On-path
- B.** Rogue AP
- C.** Evil twin
- D.** Tailgating

Answer: C ([LEAVE A REPLY](#))

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

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

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

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

References (CompTIA Network+ N10-009):

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

NEW QUESTION: 171

Users are reporting latency on the network. The network engineer notes the following:

Confirms the only change was a new network switch

Confirms all users are experiencing latency

Thinks the issue is a network loop caused by the lower bridge ID of the new switch Which of the following describes the next step in the troubleshooting methodology?

- A. Identify the problem.
- B. Test the theory.
- C. Implement the solution.
- D. Verify full system functionality.

Answer: B ([LEAVE A REPLY](#))

The correct answer is Test the theory, which aligns directly with the CompTIA Network+ N10-009 troubleshooting methodology. According to the official troubleshooting steps, once a problem has been identified and relevant information gathered, the next step is to establish a theory of probable cause and then test that theory to determine whether it is valid.

In this scenario, the engineer has already completed the problem identification phase by confirming that all users are experiencing latency and correlating the issue with the installation of a new switch. The engineer has also formed a theory: that a network loop caused by the lower bridge ID of the new switch may be impacting Spanning Tree Protocol (STP), resulting in congestion and latency. Because this theory has already been developed, the next logical and required step is to test the theory-for example, by reviewing STP states, temporarily disabling ports, or adjusting bridge priorities.

Implementing a solution would be premature without validating the theory, and verifying full system functionality occurs only after a fix has been applied. The Network+ objectives stress following a structured methodology to avoid unnecessary changes and minimize network disruption. Testing the theory ensures accuracy before corrective action is taken, reducing risk and downtime.

NEW QUESTION: 172

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

- A. ST
- B. RJ45
- C. BNC
- D. SFP

Answer: B ([LEAVE A REPLY](#))

Console Access:

Purpose: Console access to a switch allows administrators to configure and manage the device directly. This is typically done using a terminal emulator program on a computer.

RJ45 Connector:

Common Use: The RJ45 connector is widely used for Ethernet cables and also for console connections to network devices like switches and routers.

Console Cables: Console cables often have an RJ45 connector on one end (for the switch) and a DB9 serial connector on the other end (for the computer).

Comparison with Other Connectors:

ST (Straight Tip): A fiber optic connector used for networking, not for console access.

BNC (Bayonet Neill-Concelman): A connector used for coaxial cable, typically in older network setups and not for console access.

SFP (Small Form-factor Pluggable): A modular transceiver used for network interfaces, not for console access.

Practical Application:

Connection Process: Connect the RJ45 end of the console cable to the console port of the switch. Connect the DB9 end (or USB via adapter) to the computer. Use a terminal emulator (e.g., PuTTY, Tera Term) to access the switch's command-line interface (CLI).

References:

CompTIA Network+ study materials on network devices and connectors.

NEW QUESTION: 173

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

NEW QUESTION: 174

Which of the following routing technologies uses an attribute list for path selection?

A. BGP

B. RIP

C. EIGRP

D. OSPF

Answer: A ([LEAVE A REPLY](#))

BGP (Border Gateway Protocol) uses attributes like AS path, origin, and MED (multi-exit discriminator) to determine the best path among multiple available routes.

From Andrew Ramdayal's guide:

"BGP is the protocol underlying the global routing system of the internet. It is used for routing data between autonomous systems (ASes)... BGP uses a path vector mechanism and maintains a list of attributes for route selection."

NEW QUESTION: 175

Which of the following kinds of targeted attacks uses multiple computers or bots to request the same resource repeatedly?

A. On-path

B. DDoS

C. ARP spoofing

D. MAC flooding

Answer: B ([LEAVE A REPLY](#))

A Distributed Denial of Service (DDoS) attack leverages multiple computers or bots (botnet) to flood a target system with requests, overwhelming its resources and making it unavailable to legitimate users. This is a common tactic used by attackers to disrupt services. The document explains:

"A DDoS (Distributed Denial of Service) attack involves multiple computers (often called bots) simultaneously sending requests to a single resource, overwhelming the system and causing a denial of service to legitimate users."

NEW QUESTION: 176

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: D (LEAVE A REPLY)

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: 177

Which of the following is the best way to keep devices on during a loss of power?

- A.** UPS
- B.** Power load
- C.** PDU
- D.** Voltage

Answer: A (LEAVE A REPLY)

A UPS (Uninterruptible Power Supply) provides backup power to devices during a power outage, allowing for continuous operation and protecting against sudden shutdowns that could cause data loss or equipment damage. The document confirms:

"A UPS (Uninterruptible Power Supply) is essential for maintaining power to critical devices during an outage, protecting data and ensuring continuous operation until power is restored or a safe shutdown can be performed."

NEW QUESTION: 178

Which of the following is an XML-based security concept that works by passing sensitive information about users, such as log-in information and attributes, to providers.

- A.** IAM
- B.** MFA
- C.** RADIUS
- D.** SAML

Answer: D (LEAVE A REPLY)

Security Assertion Markup Language (SAML) is an XML-based standard used for exchanging authentication and authorization data between parties, particularly between an identity provider (IdP) and a service provider (SP). SAML is commonly used in Single Sign-On (SSO) solutions to pass sensitive user information, such as login credentials and attributes, securely between the identity provider and the service provider.

* SAML (Security Assertion Markup Language): Facilitates web-based authentication and authorization, allowing users to access multiple services with a single set of credentials.

* XML-based: Uses XML to encode the authentication and authorization data, ensuring secure transmission of user information.

* Identity Federation: Enables secure sharing of identity information across different security domains, making it ideal for enterprise SSO solutions.

Network References:

- * CompTIA Network+ N10-007 Official Certification Guide: Covers authentication protocols, including SAML.
- * Cisco Networking Academy: Provides training on identity management and federation technologies.
- * Network+ Certification All-in-One Exam Guide: Explains SAML and its role in secure identity management and SSO.

NEW QUESTION: 179

A network engineer needs to order cabling to connect two buildings within the same city. Which of the following media types should the network engineer use?

- A.** Coaxial
- B.** Twinaxial
- C.** Single-mode fiber
- D.** Cat 5

Answer: C ([LEAVE A REPLY](#))

Single-mode fiber is best suited for long-distance communication, often exceeding 10 km (6.2 miles). It's immune to EMI and offers high bandwidth - making it the ideal choice for connecting buildings across a city.

Coaxial (A) and Twinaxial (B) are used for shorter distances and specific use cases (e.g., storage or legacy systems).

Cat 5 (D) is limited to 100 meters and is not suitable for city-level interconnects.

For long-distance, high-speed, and reliable communication between buildings, Single-mode fiber is the professional choice.

Reference:CompTIA Network+ N10-009 Official Study Guide - Objective 3.4: "Summarize the properties and purposes of physical network topologies and network types."

NEW QUESTION: 180

Which of the following describes a company that houses all of its critical network infrastructure configurations in one location?

- A.** Central repository
- B.** Version control
- C.** Conflict mitigation
- D.** Branching

Answer: (SHOW ANSWER)

A central repository describes a single location where critical network infrastructure configurations are stored and managed. This can include switch configurations, router configurations, firewall rules, wireless controller settings, diagrams, templates, backup files, and standard operating procedures. A central repository helps administrators maintain consistency, improve recovery time, simplify audits, and reduce the risk of losing important configuration data.

The CompTIA Network+ N10-009 objectives include network documentation, configuration management, change management, and operational best practices. Storing configurations in a central repository supports backup and recovery because administrators can quickly retrieve known-good configurations if a device fails or a change causes an outage. It also helps teams collaborate by giving authorized personnel access to the same current documentation and configuration files.

Version control is related but refers specifically to tracking changes, revisions, and rollback history over time.

Conflict mitigation involves reducing conflicts when multiple people work on the same files or configurations. Branching is a version-control feature that allows separate lines of development or change testing.

Since the question focuses on housing all configurations in one location, the best answer is central repository.

Top of Form

Bottom of Form

NEW QUESTION: 181

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: A (LEAVE A REPLY)

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.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 182

A network technician is investigating an issue in which a specific user is unable to access a server. Other users in the company, however, can access the server. After checking the switch and router logs, the technician is unable to identify any issues. Which of the following troubleshooting steps should the technician take next?

- A. Inspect the client's firewall configuration
- B. Update the network equipment's firmware
- C. Check the server's DNS configuration
- D. Check the server's event logs

Answer: A (LEAVE A REPLY)

The technician should inspect the client's firewall configuration. Since only one specific user is unable to access the server while other users can access it successfully, the issue is most likely isolated to that user's device, account, local configuration, or local security settings. After switch and router logs show no network infrastructure issue, the next logical step is to examine the affected client.

The CompTIA Network+ N10-009 troubleshooting methodology emphasizes identifying the scope of the problem, testing the most likely causes, and isolating whether the issue is client-side, server-side, or network- side. A local firewall could block outbound connections to the server, block a required application, restrict ports, or apply a profile that prevents communication.

Updating network firmware is not an appropriate next step because there is no evidence of a widespread infrastructure problem. Checking the server's DNS configuration is unlikely because other users can access the same server. Checking the server's event logs may be useful later, but the scenario points first to the single affected client. Therefore, inspecting the client's firewall configuration is the best next troubleshooting step.

NEW QUESTION: 183

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

- A. Jumbo frames
- B. 802.1Q tagging
- C. Native VLAN
- D. Link aggregation

Answer: B ([LEAVE A REPLY](#))

802.1Q tagging, also known as VLAN tagging, is used to identify VLANs on a trunk link between switches.

This allows the switches to transfer data for multiple VLANs (or networks) over a single physical connection.

This method ensures that traffic from different VLANs is properly separated and managed across the network.

References: CompTIA Network+ study materials.

NEW QUESTION: 184

Which of the following provides simple authentication to access network devices while also providing logging capabilities?

- A. TACACS+
- B. SAML
- C. SSO
- D. MFA

Answer: ([SHOW ANSWER](#)**)**

The correct answer is A. TACACS+. This protocol is commonly used for authentication, authorization, and accounting (AAA) when administrators need to access network infrastructure devices such as routers, switches, and firewalls. The key part of the question is not just authentication, but also logging capabilities.

TACACS+ supports accounting functions, which means it can record administrative actions and login events.

That makes it especially useful when organizations want traceability for device access and configuration changes.

The other options do not fit as well. SAML is primarily used for federated identity and web-based authentication between identity providers and service providers. SSO is a general authentication convenience feature that allows one login to access multiple systems, but it does not itself provide detailed device-level accounting. MFA strengthens authentication by requiring multiple factors, but it is not the protocol best known for centralized access control and activity logging on network devices.

For Network+ exam purposes, TACACS+ is strongly associated with administrative access to network equipment and with maintaining an audit trail of who accessed devices and what actions were performed.

Because the question asks for both simple authentication and logging, TACACS+ is the best match.

NEW QUESTION: 185

Which of the following offers the ability to manage access at the cloud VM instance?

- A. Security group
- B. Internet gateway
- C. Direct Connect
- D. Network ACL

Answer: A ([LEAVE A REPLY](#))

Security groups in cloud environments act as virtual firewalls for VM instances, controlling inbound and outbound traffic based on specified rules.

From Andrew Ramdayal's guide:

"Network security groups are used to control inbound and outbound traffic to cloud resources within a VPC.

They act as a virtual firewall for associated instances..."

NEW QUESTION: 186

Which of the following is the step that a troubleshooter should take immediately after implementing a solution?

- A. Review lessons learned during the process.
- B. Establish a plan of action.
- C. Verify full system functionality.
- D. Document actions and outcomes.

Answer: C (LEAVE A REPLY)

After implementing the solution, the immediate next step is to verify full system functionality. This confirms that the problem has been resolved and helps ensure no new issues have been introduced.

From Andrew Ramdayal's guide:

"After the solution is implemented, test the system to ensure that it is fully operational, and the original problem has been resolved. Also, put in place any measures that could prevent the issue from recurring."

NEW QUESTION: 187

A systems administrator is looking for operating system information, running services, and network ports that are available on a server. Which of the following software tools should the administrator use to accomplish this task?

- A. Nmap
- B. Traceroute
- C. Netstat
- D. Ping

Answer: A (LEAVE A REPLY)

The correct answer is A. Nmap. Nmap (Network Mapper) is a powerful network scanning and reconnaissance tool specifically designed to gather detailed information about hosts on a network. According to CompTIA Network+ N10-009 objectives, Nmap can be used to identify open ports, running services, and even the operating system of a target device through techniques such as TCP/UDP scanning and OS fingerprinting.

This makes Nmap the best choice when a systems administrator needs a comprehensive view of a server's exposure and configuration. It can enumerate services (e.g., HTTP, SSH), detect service versions, and determine which ports are open, closed, or filtered.

The other options are more limited in scope. Traceroute is used to map the path packets take across a network and identify latency or routing issues, but it does not provide service or OS details. Netstat shows active connections and listening ports on a local machine but does not perform remote OS detection or full service enumeration. Ping simply tests connectivity and reachability using ICMP and does not provide detailed system information.

Therefore, Nmap is the most appropriate and comprehensive tool for this requirement.

NEW QUESTION: 188

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: B (LEAVE A REPLY)

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: 189

Which of the following does a hash provide?

- A. Non-repudiation
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: B (LEAVE A REPLY)

The correct answer is Integrity because a hashing algorithm ensures that data has not been altered. According to CompTIA Network+ (N10-009) security objectives, hashing is a cryptographic process that takes input data of any size and produces a fixed-length output known as a hash value or digest. If even a single bit of the original data changes, the resulting hash value will be significantly different.

Hashing is commonly used to verify file integrity, validate message authenticity, and securely store passwords. For example, when downloading software, the vendor may publish a hash value so users can calculate the hash of the downloaded file and confirm it matches, ensuring the file was not tampered with.

Non-repudiation (Option A) typically requires digital signatures that combine hashing with asymmetric encryption to verify the sender's identity. Confidentiality (Option C) is achieved through encryption, which protects data from unauthorized access. Availability (Option D) refers to ensuring systems and data are accessible when needed and is not related to hashing functions.

Therefore, hashing primarily provides data integrity verification.

NEW QUESTION: 190

A company implements a new network utilizing only IPv6 addressing and needs to connect to the internet.

Which of the following must be enabled in order for the internal network to contact servers on the internet?

- A. MPLS
- B. NAT64
- C. GRE
- D. Static routing

Answer: B (LEAVE A REPLY)

The correct answer is B. NAT64 . This scenario says the internal network is using only IPv6 . In the real world, many internet services still rely on IPv4, so an IPv6-only client may need a translation mechanism to reach IPv4-based servers. That is exactly where NAT64 is used. It allows communication between IPv6-only clients and IPv4 resources by translating between the two protocols.

The other options do not solve that requirement. MPLS is used for traffic forwarding across provider networks and has nothing to do with IPv4/IPv6 protocol translation. GRE creates tunnels, but it does not automatically translate one IP version into another. Static routing can direct traffic, but it cannot make IPv6- only hosts speak to IPv4-only internet destinations.

From a Network+ perspective, this question is testing knowledge of IPv6 transition and interoperability mechanisms . If the network is entirely IPv6 internally, but still needs access to parts of the internet that may be IPv4, some translation service has to exist at the boundary. Among the choices given, NAT64 is the only technology that fits that role. That is why B is the best answer.

NEW QUESTION: 191

A company discovers on video surveillance recordings that an unauthorized person installed a rogue access point in its secure facility. Which of the following allowed the unauthorized person to do this?

- A. Evil twin
- B. Honeytrap
- C. Wardriving
- D. Tailgating

Answer: D (LEAVE A REPLY)

Tailgating is a physical security breach where someone follows an authorized person into a restricted area without proper credentials. Once inside, the attacker can install rogue devices like unauthorized APs.

- * A. Evil twin is a wireless attack where an attacker sets up a fake AP.
- * B. Honeytrap is used to attract attackers for analysis.
- * C. Wardriving involves scanning for unsecured Wi-Fi networks while driving, not physical intrusion.

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

NEW QUESTION: 192

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 192.168.10.0/22 10.0.8.0/26 192.168.10.0/27 10.0.1.0/21 192.168.10.0/26 10.0.0.1/17 10.0.0.1/18 192.168.1.0/23 192.168.1.0/22 10.0.1.0/22 10.0.8.0/27
B	100	192.168.1.1/22	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22

			10.0.1.0/21
C	10,000	10.0.0.1/8	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21

Answer:

Company	Current number of devices	Current subnet range	New subnet range
A	32	192.168.10.1/27	Select 192.168.10.0/22 10.0.8.0/26 192.168.10.0/27 10.0.1.0/21 192.168.10.0/26 10.0.0.1/17 10.0.0.1/18 192.168.1.0/23 192.168.1.0/22 10.0.1.0/22 10.0.8.0/27
B	100	192.168.1.1/22	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21
C	10,000	10.0.0.1/8	Select 192.168.10.0/27 10.0.1.0/22 192.168.1.0/23 10.0.0.1/17 192.168.1.0/22 10.0.8.0/27 10.0.8.0/26 10.0.0.1/18 192.168.10.0/26 192.168.10.0/22 10.0.1.0/21

CompTIA

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: 193

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

- A. Apply the latest patches and bug fixes.
- B. Decommission and replace the switch.
- C. Ensure the current firmware has no issues.
- D. Isolate the switch from the network.

Answer: B (LEAVE A REPLY)

* Understanding End-of-Support:

* End-of-Support Status: When a vendor declares a device as end-of-support, it means the device will no longer receive updates, patches, or technical support. This poses a security risk as new vulnerabilities will not be addressed.

* Risks of Keeping an End-of-Support Device:

* Security Vulnerabilities: Without updates, the switch becomes susceptible to new security threats.

* Compliance Issues: Many regulatory frameworks require that critical infrastructure be maintained with supported and secure hardware.

* Best Next Step - Replacement:

* Decommission and Replace: The most secure approach is to replace the end-of-support switch with a new, supported model. This ensures the infrastructure remains secure and compliant with current standards.

* Planning and Execution: Plan for the replacement by evaluating the network's needs, selecting a suitable replacement switch, and scheduling downtime for the hardware swap.

* Comparison with Other Options:

* Apply the Latest Patches: While helpful, this does not address future vulnerabilities since no further patches will be provided.

* Ensure the Current Firmware Has No Issues: This is only a temporary measure and does not mitigate future risks.

* Isolate the Switch from the Network: Isolating the switch may disrupt network operations and is not a viable long-term solution.

References:

* CompTIA Network+ study materials on network maintenance and security best practices.

NEW QUESTION: 194

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: D (LEAVE A REPLY)

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: 195

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: C ([LEAVE A REPLY](#))

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: 196

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

- A. Sides
- B. Top
- C. Front
- D. Rear

Answer: D ([LEAVE A REPLY](#))

In a data center that uses hot aisle/cold aisle ventilation, equipment is typically installed so that cool air enters from the cold aisle (front) and hot air is exhausted to the hot aisle (rear). This configuration maximizes cooling efficiency.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 197

Which of the following should a network technician do to maintain remote administrative redundancy if a switch becomes unresponsive through SSH?

- A. Deploy a jump host

- B.** Use an out-of-band management solution
- C.** Enable an administrative GUI
- D.** Connect a physical console cable

Answer: B ([LEAVE A REPLY](#))

An out-of-band management solution is the best answer because it provides an alternate administrative path to network equipment when the normal production network path is unavailable. If a switch becomes unresponsive through SSH, the technician needs a separate management method that does not depend on the same in-band network connectivity. Out-of-band management can use a dedicated management network, console server, cellular connection, modem, or management interface to reach devices during outages or configuration failures.

The CompTIA Network+ N10-009 objectives include network operations, device management, availability, and remote access methods. SSH is an in-band management method when accessed over the production network. If routing, VLANs, ACLs, management services, or switch control-plane functions are affected, SSH may fail. Out-of-band access improves administrative redundancy and supports recovery.

A jump host can centralize administrative access, but it still depends on network connectivity to the switch.

An administrative GUI may also fail if management access is unavailable. A physical console cable can work locally, but the question specifically asks for remote administrative redundancy. Therefore, an out-of-band management solution is the best answer.

NEW QUESTION: 198

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: B ([LEAVE A REPLY](#))

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: 199

Which of the following layers of the OSI model is responsible for end-to-end encryption?

- A.** Presentation
- B.** Application
- C.** Session
- D.** Transport

Answer: ([SHOW ANSWER](#)**)**

The correct answer is Presentation, which is Layer 6 of the OSI model. According to the CompTIA Network+ N10-009 objectives, the Presentation layer is responsible for data formatting, compression, and encryption, ensuring that data sent from the application layer of one system can be properly interpreted by the receiving system.

End-to-end encryption refers to encrypting data before transmission and decrypting it only at the final destination, preventing intermediaries from accessing the plaintext data. In the OSI model, this encryption and decryption function is logically placed at the Presentation layer, which sits between the Application and Session layers. This layer transforms data into a standardized format and applies security mechanisms such as encryption algorithms.

While modern implementations like TLS/SSL often operate across multiple layers in real-world networking stacks, the Network+ exam adheres to the conceptual OSI model when testing knowledge. From an OSI perspective, encryption is explicitly associated with the Presentation layer.

The Application layer provides network services to end-user applications, the Session layer manages session establishment and teardown, and the Transport layer focuses on segmentation, flow control, and reliability.

None of these layers are primarily responsible for encryption within the OSI framework.

CompTIA emphasizes understanding these conceptual responsibilities, making Presentation the correct and expected answer.

NEW QUESTION: 200

A network engineer runs ipconfig and notices that the default gateway is 0.0.0.0. Which of the following address types is in use?

- A. APIPA
- B. Multicast
- C. Class C
- D. Experimental

Answer: ([SHOW ANSWER](#))

APIPA (Automatic Private IP Addressing) assigns an IP address in the range 169.254.x.x when a DHCP server cannot be contacted, and it sets the default gateway to 0.0.0.0 because APIPA is designed only for local communication within the same subnet. The document states:

"APIPA allows for automatic, ad hoc network communication within a single subnet when a DHCP server is not available. In this state, the default gateway is typically set to 0.0.0.0 because APIPA does not provide routing to other networks."

NEW QUESTION: 201

A network administrator needs to add 255 useable IP addresses to the network. A /24 is currently in use. Which of the following prefixes would fulfill this need?

- A. /23
- B. /25
- C. /29
- D. /32

Answer: ([SHOW ANSWER](#))

A /23 subnet provides 512 total addresses, of which 510 are usable (subtracting 2 for network and broadcast addresses). This would satisfy the need for 255 additional addresses.

NEW QUESTION: 202

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: D ([LEAVE A REPLY](#))

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: 203

A network technician is adding a security camera with an enhancer to a network closet in an organization's office building. When plugged in, the camera does not respond. Given the following information:

* Switch: 24 ports, 124W PoE capable, maximum 16W per port

* Access point: 12W PoE

* Camera: 14W

* Enhancer: 4W

Which of the following is the most likely reason the camera is not working?

A. The cable is experiencing too much crosstalk.

B. The switch is beyond the PoE budget.

C. The cable is improperly terminated.

D. The single connection surpasses the power allowed.

Answer: D ([LEAVE A REPLY](#))

The most likely reason the camera is not working is that the single PoE connection exceeds the maximum power allowed per port. The switch supports a total PoE budget of 124W, but each port has a maximum output of 16W. The camera requires 14W, and the enhancer requires 4W. Together, they require 18W on one connection. Since 18W exceeds the switch's maximum of 16W per port, the device may fail to power on or operate correctly.

The CompTIA Network+ N10-009 objectives include understanding network devices, cabling, power delivery, and Power over Ethernet limitations. PoE design requires checking both the total switch PoE budget and the per-port wattage limit. The total budget is not the issue here because the listed devices do not exceed

124W overall. Crosstalk and improper termination could cause connectivity or performance issues, but the provided wattage values strongly point to a power limitation. Since the camera and enhancer together require more power than the port can deliver, option D is the correct answer.

NEW QUESTION: 204

Which of the following is the best use case for PAT?

A. Using BGP for internet routing

B. Using a single public IP

C. Using redundant internet service providers

D. Using a dual-stack IP scheme

Answer: B ([LEAVE A REPLY](#))

The correct choice is B. Using a single public IP. PAT (Port Address Translation) is a form of NAT that allows many internal private IP addresses to share one public IP address by tracking sessions with port numbers. This is one of the most common edge-network designs for homes, small offices, and many enterprise branch environments.

The reason PAT is so useful is that it conserves public IPv4 addresses. Internal hosts keep their private addressing, and when they access external resources, the firewall or router translates those connections so they appear to come from one public address, while still keeping each session unique through port mapping.

The other options are unrelated to PAT's primary purpose. BGP is a routing protocol for route exchange between networks. Redundant ISPs deal with resiliency and multihoming, not port-based address

translation.

A dual-stack IP scheme means running IPv4 and IPv6 together, which is separate from the NAT/PAT function.

This question is really asking what situation most naturally calls for PAT. When an organization wants multiple internal devices to reach the internet without assigning each device its own public IPv4 address, PAT is the standard solution. That makes using a single public IP the best answer.

NEW QUESTION: 205

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

- 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: 206

Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

- A. The administrator did not provision enough IP addresses.
- B. The administrator configured an incorrect default gateway.
- C. The administrator did not provision enough routes.
- D. The administrator did not provision enough MAC addresses.

Answer: A ([LEAVE A REPLY](#))

When a DHCP server is installed and not enough IP addresses are provisioned, users may start experiencing network outages once the available IP addresses are exhausted. DHCP servers assign IP addresses to devices on the network, and if the pool of addresses is too small, new devices or those renewing their lease may fail to obtain an IP address, resulting in network connectivity issues. References: CompTIA Network+ study materials.

NEW QUESTION: 207

A network administrator is configuring a wireless network with an ESSID. Which of the following is a user benefit of ESSID compared to SSID?

- A. Stronger wireless connection
- B. Roaming between access points
- C. Advanced security
- D. Increased throughput

Answer: B ([LEAVE A REPLY](#))

An Extended Service Set Identifier (ESSID) allows multiple access points to share the same SSID, enabling seamless roaming for users. This means that users can move between different access points within the same ESSID without losing connection or having to reauthenticate. This provides a better user experience, especially in large environments such as office buildings or campuses. References: CompTIA Network+ study materials.

NEW QUESTION: 208

A customer calls the help desk to report that resources are no longer reachable. The resources were available before network changes were made. The technician verifies the report, investigates, and discovers that a new logical layout is segmenting the network using tagging. Which of the following appliances most likely needs to be reviewed to restore the connections?

- A. Access point
- B. Firewall
- C. Switch
- D. Load balancer

Answer: C ([LEAVE A REPLY](#))

The correct answer is Switch because the question references a new logical layout segmenting the network using tagging, which indicates VLAN (Virtual Local Area Network) configuration. VLAN tagging (IEEE 802.1Q) is performed on switches to logically separate broadcast domains within the same physical infrastructure.

According to CompTIA Network+ (N10-009) objectives under switching technologies, VLANs are used to improve security, reduce broadcast traffic, and logically segment network traffic. When VLAN tagging is misconfigured-such as incorrect trunk ports, access port assignments, or mismatched VLAN IDs-devices may lose connectivity to required network resources.

Since the issue began after changes involving tagging, the most likely cause is an incorrect switch configuration, such as improper VLAN assignments or trunking settings.

An access point (Option A) may use VLANs for SSID segmentation, but core tagging configuration is handled at the switch. A firewall (Option B) filters traffic but does not control VLAN tagging at Layer 2 in typical deployments. A load balancer (Option D) distributes traffic among servers and is unrelated to VLAN segmentation.

Therefore, reviewing the switch configuration is the appropriate action to restore connectivity.

NEW QUESTION: 209

Some newly installed wireless access points are not broadcasting. Which of the following is the most likely cause of the issue?

- A. PoE power budget exceeded
- B. Improper VLAN assignment
- C. Limited signal strength/degradation
- D. Uplink transceiver incorrectly configured

Answer: ([SHOW ANSWER](#)**)**

The most likely cause is that the PoE power budget has been exceeded. Wireless access points commonly receive power through Power over Ethernet. If newly installed APs are not broadcasting at all, one of the first things to verify is whether the switch has enough available PoE capacity to power them. A switch can have enough physical ports available but still lack sufficient PoE wattage. When the total PoE budget is exhausted, some APs may fail to power on, partially boot, reboot repeatedly, or never begin broadcasting an SSID.

The CompTIA Network+ N10-009 objectives include network devices, wireless infrastructure, PoE, power budgets, and troubleshooting physical connectivity. Wireless APs must have both data connectivity and sufficient power before they can operate normally. An improper VLAN assignment could prevent clients from reaching network resources or receiving DHCP addresses, but the AP would usually still power on and broadcast. Limited signal strength would affect coverage, not prevent broadcasting entirely. An uplink transceiver issue applies more to fiber or modular uplink connections and is less likely for newly installed APs. Therefore, the best answer is PoE power budget exceeded.

NEW QUESTION: 210

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: 211

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

- A. LLDP
- B. IKE
- C. VLAN
- D. netstat

Answer: A (LEAVE A REPLY)

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

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

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

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 212

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

- A. MFA
- B. Screened subnet
- C. Captive portal
- D. Honeypot

Answer: D (LEAVE A REPLY)

A honeypot is specifically designed to attract, isolate, and observe malicious activity so defenders can learn how an attacker is operating and determine attack techniques. In the context of Network+ (N10-009) security objectives, honeypots (and broader deception technologies) are defensive controls used to detect reconnaissance and exploitation attempts by presenting a decoy system or service that appears legitimate.

Because a honeypot should not receive normal production traffic, any interaction is suspicious, making it valuable for identifying threat actors, collecting indicators of compromise, and analyzing the attacker's tools, commands, and behavior patterns. This supports the goal of understanding the type of attack used (for example, credential stuffing, exploitation attempts, lateral movement probes) while keeping the attacker away from real assets.

MFA strengthens authentication but does not provide a controlled environment to observe attacker techniques.

A screened subnet (DMZ) is for segmentation of public-facing services and reducing exposure of internal systems, but it is not primarily used to "bait" and analyze attackers. A captive portal enforces user acknowledgement/authentication for network access; it is not a deception/analysis system. Therefore, honeypot is the best match.

NEW QUESTION: 213

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

- A. BNC
- B. SFP
- C. MPO
- D. RJ45

Answer: A (LEAVE A REPLY)

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

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

NEW QUESTION: 214

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

- A. Sides
- B. Top
- C. Front
- D. Rear

Answer: C (LEAVE A REPLY)

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: 215

A network administrator changed an external DNS to point customers to a new server. Which of the following tools should the administrator use to test the new server's configuration?

- A. ping
- B. tracet
- C. tcpdump
- D. nslookup

Answer: (SHOW ANSWER)

*nslookup allows querying DNS records to verify if the new server is correctly resolving domain names.

*ping (A) tests basic connectivity, not DNS configuration.

*tracert (B) shows network path latency but doesn't test DNS.

*tcpdump (C) captures packets but isn't ideal for DNS verification.

#Reference: CompTIA Network+ N10-009 Official Documentation - DNS Testing Tools.

NEW QUESTION: 216

Which of the following protocols uses the Dijkstra's Link State Algorithm to establish routes inside its routing table?

- A. OSPF
- B. EIGRP
- C. BGP
- D. RIP

Answer: A ([LEAVE A REPLY](#))

OSPF (Open Shortest Path First) is a link-state routing protocol that uses the Dijkstra algorithm, also known as the shortest path first (SPF) algorithm, to determine the most efficient routes.

From Andrew Ramdayal's guide:

"OSPF is a link-state routing protocol that provides fast, efficient path selection using the shortest path first (SPF) algorithm."

NEW QUESTION: 217

Which of the following layers in the OSI model is responsible for establishing, maintaining, and terminating connections between nodes?

- A. Physical
- B. Network
- C. Session
- D. Transport

Answer: ([SHOW ANSWER](#)**)**

TheSession Layer(Layer 5 of the OSI Model) is responsible for setting up, managing, and tearing down sessions between applications. It maintains dialog control and synchronizes data exchange between systems.

Reference:Section 1.1 - OSI Reference Model Concepts - "Layer 5 - Session"

NEW QUESTION: 218

A network engineer is installing new PoE wireless APs. The first five APs deploy successfully, but the sixth one fails to start. Which of the following should the engineer investigate first?

- A. Signal strength
- B. Duplex mismatch
- C. Power budget
- D. CRC

Answer: C ([LEAVE A REPLY](#))

When deploying multiple Power over Ethernet (PoE) devices, the switch's power budget can be exhausted. If the available wattage on the switch cannot supply the additional AP, it will fail to power on. This is the most likely cause when previous APs worked fine but a new one does not.

A). Signal strength affects wireless connectivity, not whether the AP powers up.

B). Duplex mismatch causes poor throughput, not power failure.

D). CRC errors point to cabling issues but do not prevent booting if no power is available.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - PoE power budget considerations, device startup issues.

NEW QUESTION: 219

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: 220

A network architect is implementing an off-premises computing facility and needs to ensure that operations will not be impacted by major outages. Which of the following should the architect consider?

- A. Hot site
- B. DCI
- C. Direct Connect
- D. Active-passive approach

Answer: ([SHOW ANSWER](#))

A hot site is a fully operational backup facility with hardware, network, and data synchronization already in place. It allows for immediate failover in the event of a disaster, minimizing downtime.

* B. DCI (Data Center Interconnect) connects data centers but doesn't guarantee availability unless built redundantly.

* C. Direct Connect refers to a private link to cloud providers, not disaster recovery.

* D. Active-passive can help with failover but may involve delay unless combined with hot site principles.

#Reference:

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

NEW QUESTION: 221

An administrator is setting up an SNMP server for use in the enterprise network and needs to create device IDs within a MIB. Which of the following describes the function of a MIB?

- A. DHCP relay device
- B. Policy enforcement point
- C. Definition file for event translation
- D. Network access controller

Answer: C ([LEAVE A REPLY](#))

* MIB (Management Information Base): A MIB is a database used for managing the entities in a communication network. The MIB is used by Simple Network Management Protocol (SNMP) to translate events into a readable format, enabling network administrators to manage and monitor network devices effectively.

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

CompTIA Network+ materials discussing SNMP and MIB functionality.

NEW QUESTION: 222

Which of the following is a difference between EOL and EOS?

- A.** EOL discontinues the product but may offer support.
- B.** EOS replaces free support with a subscription model.
- C.** EOS only applies to physical products.
- D.** EOL still guarantees warranty service.

Answer: (SHOW ANSWER)

The correct answer is EOL discontinues the product but may offer support. According to CompTIA Network+ (N10-009) objectives related to lifecycle management and vendor support policies, End of Life (EOL) indicates that a product is no longer being manufactured or sold by the vendor. However, after EOL is declared, the vendor may continue to provide limited support, updates, or warranty services for a defined period.

In contrast, End of Support (EOS) means the vendor has stopped providing technical assistance, patches, firmware updates, and security fixes for the product. Once a product reaches EOS, organizations are responsible for maintaining it without vendor assistance, which can introduce operational and security risks.

Option B is incorrect because EOS does not typically convert support into a subscription model-it signifies the termination of support. Option C is incorrect because EOS applies to both hardware and software products. Option D is incorrect because warranty terms depend on vendor policy and are not guaranteed after EOL status.

Therefore, the key distinction is that EOL ends product sales, while EOS ends vendor support.

NEW QUESTION: 223

Two network switches at different locations are connected via fiber-optic cable at a distance of 10 miles (16 km). The duplex fiber-optic patch cord between the patch panel and switch is accidentally pinched, stopping connectivity between the two switches. A network technician replaces the broken cable with a new, single- mode patch cord. However, connectivity between both switches is still down and the link lights are still off.

Which of the following actions should the technician perform first?

- A.** Replace the fiber-optic transceiver in the switch
- B.** Log in to the switch to shut down and re-enable the switchport
- C.** Transpose the two fiber connectors at one end of the new patch cord
- D.** Swap the single-mode fiber patch cord with a multimode fiber patch cord

Answer: C (LEAVE A REPLY)

Fiber connections require Tx on one end to connect to Rx on the other end. If the patch cord is replaced and link lights remain off, the most common cause is that the connectors are reversed. Swapping (transposing) the connectors ensures proper transmit/receive alignment.

- A). Replacing the transceiver may eventually be necessary, but only after verifying correct connections.
- B). Restarting the switchport won't resolve a physical misconnection.
- D). Using multimode fiber would be incorrect here, as the link was designed for single-mode (10 miles/16 km requires SMF).

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Fiber connectivity, Tx/Rx alignment, link light diagnostics.

NEW QUESTION: 224

Which of the following should a network administrator configure when adding OT devices to an organization's architecture?

- A.** Honeynet
- B.** Data-at-rest encryption
- C.** Time-based authentication

D. Network segmentation

Answer: D (LEAVE A REPLY)

Network segmentation involves dividing a network into smaller segments or subnets. This is particularly important when integrating OT (Operational Technology) devices to ensure that these devices are isolated from other parts of the network. Segmentation helps protect the OT devices from potential threats and minimizes the impact of any security incidents. It also helps manage traffic and improves overall network performance. References: CompTIA Network+ study materials.

NEW QUESTION: 225

A user reports issues connecting to the wireless network. A network technician notices the following:

- * Several wireless networks are available externally from other businesses
 - * APs configured in the building are set to use the maximum amount of power
 - * Signal strength:
 - * First floor lobby: -55 dBm
 - * Break room: -78 dBm
 - * Conference room: -67 dBm
 - * Office area: -61 dBm
 - * Walking path around the building: -80 dBm
- * Channels in use: 1, 5, 44, 32 Which of the following is causing the user's wireless issues?

- A. AP power settings
- B. Channel overlap
- C. Rogue devices
- D. Interference outside the lobby

Answer: (SHOW ANSWER)

Channel overlap is the most likely cause of the wireless issues. In the 2.4 GHz band, the commonly recommended non-overlapping channels are 1, 6, and 11. The listed channels include 1 and 5, which overlap.

When nearby access points use overlapping channels, their transmissions can interfere with each other, causing retransmissions, reduced throughput, connection instability, and poor roaming behavior.

The CompTIA Network+ N10-009 objectives include wireless standards, frequency bands, channel planning, signal strength, interference, and troubleshooting wireless connectivity. Proper channel planning is essential in environments where multiple APs and neighboring wireless networks are present. Since the question specifically lists external wireless networks and internal channel usage, channel overlap is the strongest answer.

Maximum AP power can contribute to excessive coverage and co-channel interference, but the clearest technical issue shown in the data is the use of overlapping channels. Rogue devices are not identified in the scenario. Interference outside the lobby is not supported by the signal readings, and the lobby signal is actually strong at -55 dBm. Therefore, channel overlap is the best answer.

NEW QUESTION: 226

The leadership team is updated on the results of an approved change request after a breach. Which of the following troubleshooting methodology steps is described in this example?

- A. Establishing a theory of probable cause
- B. Implementing the solution or escalating as necessary
- C. Establishing a plan of action to resolve the problem and identifying potential effects
- D. Documenting findings, actions, outcomes, and lessons learned throughout the process

Answer: C (LEAVE A REPLY)

The correct answer is C. Documenting findings, actions, outcomes, and lessons learned throughout the process. According to the CompTIA Network+ N10-009 troubleshooting methodology, the final step in the structured troubleshooting process involves documenting everything that occurred during the incident. This includes the root cause, actions taken, changes implemented (such as approved change requests), outcomes of those actions, and any lessons learned.

In the scenario, the key phrase is that leadership is being updated on the results after a breach and an approved change request. This clearly aligns with post-resolution communication and documentation, where technical teams report findings and outcomes to stakeholders. This step is critical for organizational knowledge, audit requirements, compliance, and improving future incident response.

The other options represent earlier steps in the troubleshooting process. Establishing a theory of probable cause occurs early when diagnosing the issue. Establishing a plan of action comes before implementing changes. Implementing the solution happens during remediation. However, none of these involve summarizing and communicating results after the fact. Therefore, updating leadership on results corresponds directly to the documentation and lessons-learned phase of the troubleshooting methodology.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 227

A network technician is troubleshooting a faulty NIC and tests the theory. Which of the following should the technician do next?

- A. Develop a theory.
- B. Establish a plan of action.
- C. Implement the solution.
- D. Document the findings.

Answer: C (LEAVE A REPLY)

Once the theory has been tested and confirmed, the next step is to implement the solution based on the CompTIA troubleshooting model.

CompTIA Troubleshooting Model:

Identify the problem.

Establish a theory of probable cause.

Test the theory.

Establish a plan of action and implement the solution. # (Correct step) Verify full system functionality.

Document findings, actions, and outcomes.

Breakdown of Options:

- A). Develop a theory - The theory has already been developed and tested.
- 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: 228

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: 229

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: 230

Which of the following is the best example of implementing role-based access control?

A. Granting data center access only to server and network administrators

B. Providing the entire IT department access to an application development server

C. Requiring all employees to use multifactor authentication when accessing the network

D. Allowing the human resources director to determine who can access human resources files

Answer: A (LEAVE A REPLY)

Role-based access control, or RBAC, assigns permissions according to a user's job role or responsibility within the organization. In this question, granting data center access only to server and network administrators is the best example because the permission is tied directly to the users' operational roles. Server administrators and network administrators typically require physical or logical access to data center infrastructure to perform maintenance, troubleshooting, configuration, and support tasks. This aligns with the CompTIA Network+ N10-009 security objectives related to authentication, authorization, and access control.

Option B is too broad because giving the entire IT department access to an application development server may violate least privilege. Not every IT employee needs that access. Option C describes multifactor authentication, which strengthens authentication but does not define authorization by role. Option D is closer to discretionary access control because the HR director is deciding who can access files. RBAC is centrally defined by roles, not by an individual data owner's discretion. Therefore, option A is the strongest RBAC example.

NEW QUESTION: 231

A network administrator installs a node that requires a media converter to connect Ethernet to fiber but sees no link light on the node. The administrator notices the following:

- * Both terminating points are properly seated.
- * Both the fiber and Ethernet cables have been successfully tested.
- * The media converter is turned on.
- * The switch port is configured as half duplex and enabled.

Which of the following is the reason the link light is not on?

- A.** The TX/RX connection is transposed.
- B.** The switch port is misconfigured.
- C.** One of the cables has a short.
- D.** The switch port interface has errors.

Answer: B (LEAVE A REPLY)

The most likely reason is that the switch port is misconfigured. The scenario states that the switch port is configured for half duplex. In modern Ethernet environments, especially when connecting through fiber media converters or higher-speed switch links, duplex and speed settings must be compatible between devices. A mismatch or unsupported duplex setting can prevent the link from establishing correctly or cause serious connectivity problems. Since the cables have already been successfully tested, the connectors are seated properly, and the media converter is powered on, the configuration of the switch port becomes the most likely cause.

The CompTIA Network+ N10-009 objectives include troubleshooting physical connectivity, interface configuration, speed and duplex mismatch, and media converter issues. A transposed TX/RX fiber pair can also cause a no-link condition, but the question provides a specific suspicious configuration detail: the switch port is set to half duplex. One of the cables having a short is unlikely because both cables tested successfully.

Interface errors usually occur after a link is established and traffic is passing; they would not be the best explanation for no link light. Therefore, the switch port misconfiguration is the best answer.

NEW QUESTION: 232

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

- A.** Service-level agreement
- B.** Physical diagram
- C.** Site survey results
- D.** Logical diagram

Answer: C (LEAVE A REPLY)

NEW QUESTION: 233

In the troubleshooting methodology, which of the following actions comes after verifying that the initial problem has been resolved?

- A.** If necessary, escalating the issue

- B. Attempting to replicate the problem
- C. Documenting findings
- D. Implementing the plan

Answer: C ([LEAVE A REPLY](#))

In the CompTIA Network+ (N10-009) troubleshooting methodology, the step that follows verifying full system functionality (confirming the issue is resolved and validating with the user/requirements) is documenting findings, actions, and outcomes. Documentation is a required closing step because it captures what the original symptoms were, what troubleshooting steps were performed, what root cause was identified (if found), what remediation was applied, and what validation confirmed success. This record supports operational continuity by enabling faster resolution if the issue recurs, improving knowledge transfer across teams, and meeting organizational change-control or compliance requirements.

The other options fall in different parts of the methodology. Attempting to replicate the problem is typically performed earlier-after identifying symptoms and before or during isolation-to confirm the issue and help narrow scope. Implementing the plan occurs before verification; you implement the selected solution or escalation plan and then test/verify. Escalating the issue occurs when the technician lacks access, expertise, time, or evidence to proceed, and it can happen during troubleshooting-but it is not the standard step that comes after verifying resolution.

NEW QUESTION: 234

During a security audit, a consulting firm notices inconsistencies between the documentation and the actual environment. Which of the following can keep a record of who made the changes and what the changes are?

- A. Network access control
- B. Configuration monitoring
- C. Zero Trust
- D. Syslog

Answer: ([SHOW ANSWER](#))

Configuration monitoring and management tools (often part of network management systems) maintain version-controlled records of device configurations, track changes, and log who made them. This provides accountability and supports compliance audits.

- A). Network access control (NAC) manages endpoint access policies but does not track device config changes.
- C). Zero Trust is a security framework requiring strict identity verification, not a configuration tracking tool.
- D). Syslog collects system logs, but without a config monitoring system, it does not directly compare documentation to device state.

References (CompTIA Network+ N10-009):

Domain: Network Operations - Change management, configuration management, auditing.

NEW QUESTION: 235

During a VoIP call, a user notices inconsistent audio and logs an incident ticket. A network administrator notices inconsistent delays in arrival of the RTP packets. Which of the following troubleshooting tools should the network administrator use to determine the issue?

- A. Toner and probe
- B. Protocol analyzer
- C. Cable tester
- D. Spectrum reader

Answer: B ([LEAVE A REPLY](#))

Inconsistent arrival of RTP (Real-Time Protocol) packets indicates jitter or latency variation. A protocol analyzer (packet sniffer, e.g., Wireshark) can capture and analyze RTP streams, showing delay, jitter, and packet loss statistics.

- A). Toner and probe locates cable runs, not packet analysis.
- C). Cable tester checks wiring faults, not packet timing.
- D). Spectrum reader is for identifying wireless interference, not analyzing RTP traffic.

References (CompTIA Network+ N10-009):

Domain: Network Troubleshooting - Protocol analyzers, VoIP troubleshooting, jitter analysis.

NEW QUESTION: 236

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.

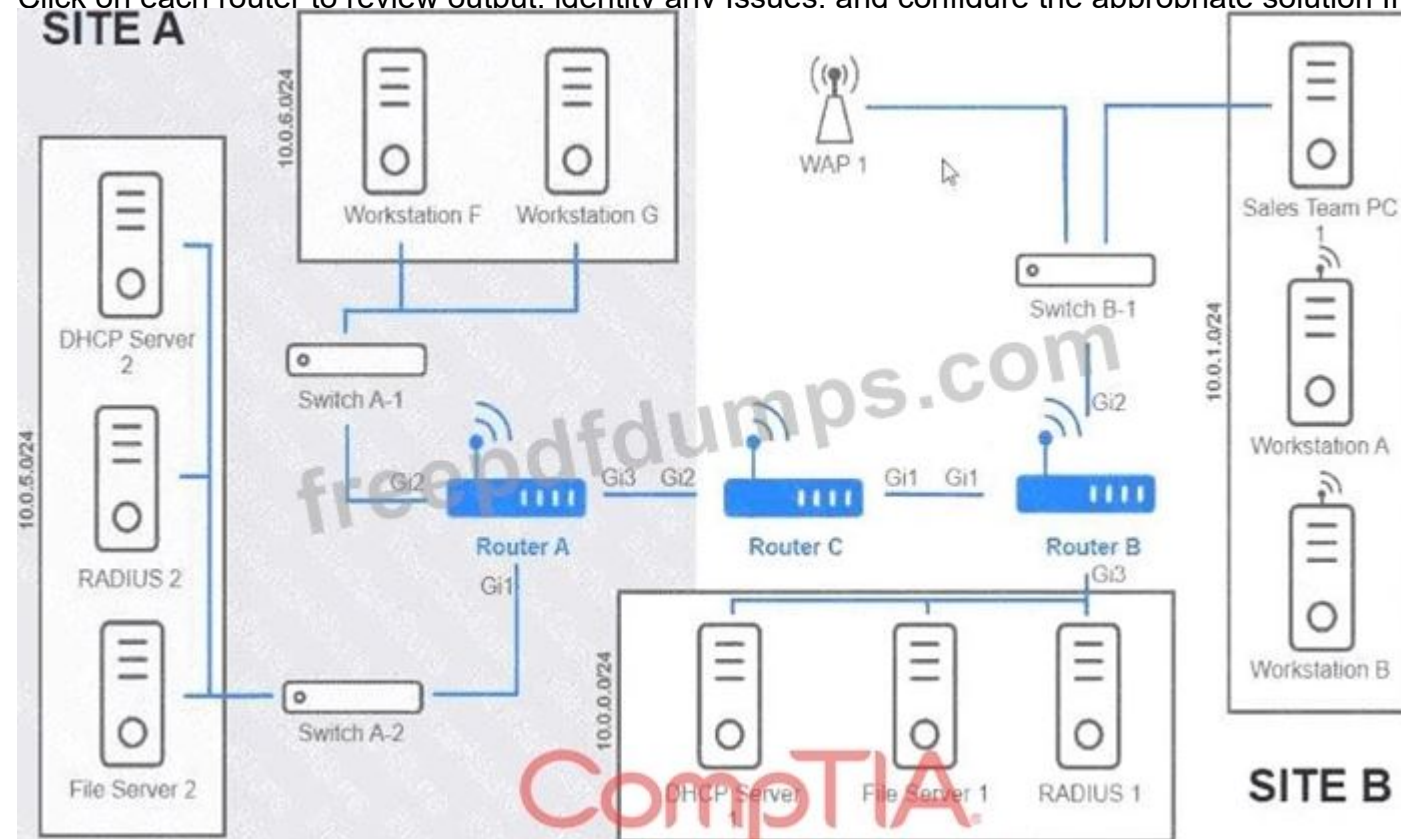
For exam purposes, when a scenario describes advanced or highly variable compute demand in the cloud, elasticity is usually the strongest answer because it focuses on rapid resource expansion and reduction as needed.

NEW QUESTION: 237

Users are unable to access files on their department share located on file_server 2. The network administrator has been tasked with validating routing between networks hosting workstation A and file server 2.

INSTRUCTIONS

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



Router-B# 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

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, GigabitEthernet3
L 10.0.0.1/32 is directly connected, GigabitEthernet3
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

Answer:

See the solution configuration below in Explanation.

Explanation:

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

Router A

Routing Table Routing Configuration

Was a problem found? ☒ Yes ☐ No

Install Static Route

Destination Prefix: 10.0.5.0

Destination Prefix Mask: 255.255.255.0

Interface: G1/1

Reset to Default Save Close

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

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



NEW QUESTION: 238

Which of the following is used to store and deliver content to clients in a geographically distributed manner using edge servers?

- A. Load balancer
- B. CDN
- C. DNS server
- D. SAN

Answer: B (LEAVE A REPLY)

A Content Delivery Network (CDN) stores cached versions of content in edge locations to deliver data faster and more reliably to users based on geographical proximity.

From Andrew Ramdayal's guide:

"CDNs distribute content to multiple, geographically dispersed servers. This enhances performance and reliability for end-users by reducing latency and load times."

NEW QUESTION: 239

A company reports that their facsimile machine no longer has a dial tone when trying to send a fax. The phone cable is damaged on one end. Which of the following types of connectors should a technician replace?

- A. F-type
- B. RJ45
- C. SC
- D. RJ11

Answer: D (LEAVE A REPLY)

Fax machines use analog phone lines, which are connected using RJ11 connectors. These are standard telephone connectors with 4 or 6 positions and are used for POTS (Plain Old Telephone Service) lines.

F-type is used for coaxial cables (e.g., TV and cable modems).

RJ45 is used for Ethernet network connections.

SC (Subscriber Connector) is used for fiber optic connections, not analog telephone lines.

Reference:

CompTIA Network+ N10-009 Official Objectives: 2.4 - Compare and contrast common network connectors.

NEW QUESTION: 240

A network administrator receives a ticket from a user. The user reports that they cannot access any websites and that they have already checked everything on their computer. Which of the following is the first action the administrator should take?

A. Divide and conquer.

B. Establish a theory of probable cause.

C. Question the user.

D. Document the findings.

Answer: C (LEAVE A REPLY)

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: 241

A customer calls the help desk to report issues connection to the internet. The customer can reach a local database server. A technician goes to the site and examines the configuration:

Which of the following is causing the user's issue?

A. Incorrect DNS

B. Unreachable gateway

C. Failed root bridge

D. Poor upstream routing

Answer: B (LEAVE A REPLY)

The customer can access local resources (a database server), which means local networking is working.

However, the inability to reach the internet suggests an issue with the default gateway. If the default gateway is unreachable, packets will not be routed outside the local network.

Breakdown of Options:

A). Incorrect DNS - DNS issues would cause problems resolving domain names, but the user should still be able to access external resources via IP addresses.

B). Unreachable gateway - # Correct answer. If the default gateway is incorrect or unreachable, the device cannot route traffic to the internet.

C). Failed root bridge - STP (Spanning Tree Protocol) failures cause switching issues, but the user can still access local devices, meaning STP is not the problem.

D). Poor upstream routing - Would affect the entire network, not just one user.

Reference:

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 242

A network administrator is deploying a new switch and wants to make sure that the default priority value was set for a spanning tree. Which of the following values would the network administrator expect to see?

- A. 36684
- B. 4096
- C. 8192
- D. 32768

Answer: (SHOW ANSWER)

NEW QUESTION: 243

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: D (LEAVE A REPLY)

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: 244

Which of the following routing protocols is most commonly used to interconnect WANs?

- A. IGP
- B. EIGRP
- C. BGP
- D. OSPF

Answer: C (LEAVE A REPLY)

Border Gateway Protocol (BGP): BGP is the most commonly used routing protocol for interconnecting WANs, especially across the internet. It is used for exchanging routing information between autonomous systems (AS), making it the backbone protocol for large-scale WANs.

IGP (A): Interior Gateway Protocols like OSPF and EIGRP are typically used within a single AS, not between them.

EIGRP (B): While it is efficient, EIGRP is primarily used for intra-domain routing and not ideal for WAN interconnection.

OSPF (D): While OSPF can be used for WANs, it is not as common as BGP for inter-AS communication.

Reference: CompTIA Network+ Official Study Guide, Domain 1.3 (WAN Concepts), Domain 2.5 (Routing Protocols).

NEW QUESTION: 245

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: 246

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: C ([LEAVE A REPLY](#))

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: 247

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: C ([LEAVE A REPLY](#))

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: 248

A junior network administrator gets a text message from a number posing as the domain registrar of the firm.

The administrator is tricked into providing global administrator credentials. Which of the following attacks is taking place?

A. DNS poisoning

B. ARP spoofing

C. Vishing

D. Smishing

Answer: D ([LEAVE A REPLY](#))

Smishing (SMS phishing) occurs when attackers send fraudulent text messages pretending to be a trusted source, tricking the victim into giving up sensitive credentials. Since this came via text message, it qualifies as smishing.

A). DNS poisoning corrupts name resolution.

B). ARP spoofing manipulates MAC-to-IP mappings.

C). Vishing is phishing via voice calls, not text.

References (CompTIA Network+ N10-009):

Domain: Network Security - Social engineering, phishing types (smishing, vishing, spear phishing).

NEW QUESTION: 249

A network administrator needs to set up a network monitoring solution. It must have the following features:

* Ability to define read-only users

* Community strings for authentication

* Availability as free open-source software

* Ability to feed a dashboard

Which of the following should the administrator do to complete this task?

A. Configure SNMP

B. Enable TACACS+

C. Set up LLDP

D. Implement a SIEM

Answer: ([SHOW ANSWER](#))

The correct answer is SNMP because Simple Network Management Protocol is commonly used to monitor network devices such as switches, routers, firewalls, servers, and wireless access points. SNMP supports community strings, especially in SNMPv1 and SNMPv2c, which function as basic authentication values. A read-only community string allows monitoring systems to collect device information without allowing configuration changes. This directly matches the requirement for read-only users and community-string-based authentication.

CompTIA Network+ N10-009 includes monitoring, management protocols, and operational tools as part of network operations. SNMP data can be collected by open-source monitoring platforms and displayed in dashboards for visibility into bandwidth usage, interface status, errors, CPU utilization, memory usage, and device availability.

TACACS+ is used for centralized authentication, authorization, and accounting, especially for administrative access to network devices. LLDP is a discovery protocol that helps identify neighboring devices but does not provide full monitoring dashboards. A SIEM collects and correlates security events, but community strings are not a SIEM feature. Therefore, configuring SNMP is the best answer.

NEW QUESTION: 250

A network engineer is designing a secure communication link between two sites. The entire data stream needs to remain confidential. Which of the following will achieve this goal?

- A.** GRE
- B.** IKE
- C.** ESP
- D.** AH

Answer: C ([LEAVE A REPLY](#))

* Definition of ESP (Encapsulating Security Payload):

* ESP is a part of the IPsec protocol suite designed to provide confidentiality, integrity, and authenticity of data by encrypting the payload and optional ESP trailer.

* Ensuring Confidentiality:

* Encryption: ESP encrypts the payload, ensuring that the data remains confidential during transmission. Only authorized parties with the correct decryption keys can access the data.

* Modes of Operation: ESP can operate in transport mode (encrypts only the payload) or tunnel mode (encrypts the entire IP packet), both providing strong encryption to secure data between sites.

* Comparison with Other Protocols:

* GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption or security features.

* IKE (Internet Key Exchange): A protocol used to set up a secure, authenticated communications channel, but it does not encrypt the data itself.

* AH (Authentication Header): Provides integrity and authentication for IP packets but does not encrypt the payload.

* Implementation:

* Use ESP as part of an IPsec VPN configuration to encrypt and secure communication between two sites. This involves setting up IPsec policies and ensuring both endpoints are configured to use ESP for data encryption.

References:

* CompTIA Network+ study materials on IPsec and secure communication protocols.

NEW QUESTION: 251

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

Location	Speed Down	Speed Up
Wireless laptop	4.8 Mbps	47.1 Mbps
Wired desktop	5.2 Mbps	49.3 Mbps
Firewall	48.8 Mbps	49.5 Mbps

Which of the following is the most likely issue?

- A.** Packet loss
- B.** Bottlenecking
- C.** Channel overlap
- D.** Network congestion

Answer: B ([LEAVE A REPLY](#))

Bottlenecking occurs when a device in the network (such as an IPS) cannot process traffic efficiently, resulting in a dramatic drop in throughput. The significant difference between the firewall's speed (48.8

Mbps down) and the end-user devices' speeds (4.8 - 5.2 Mbps down) indicates a bottleneck caused by the IPS.

*Why not the other options?

*Packet loss (A) - Would typically cause connection timeouts, not just slow speeds.

*Channel overlap (C) - Affects only wireless networks, but the wired desktop is also experiencing slow speeds.

*Network congestion (D) - Would show fluctuations in both upload and download speeds, but upload speeds remain unaffected.

Reference:

CompTIA Network+ (N10-009) Official Guide - Chapter 13: Network Performance Optimization

NEW QUESTION: 252

A customer wants to separate the finance department from the marketing department. The network administrator suggests segmenting the existing Class C network into two sections and readdressing all devices appropriately. Which of the following subnet masks should the network administrator use?

A. /24

B. /25

C. /26

D. /27

Answer: B (LEAVE A REPLY)

The correct answer is /25, which is the appropriate subnet mask for dividing an existing Class C network into two equal subnets. According to the CompTIA Network+ N10-009 objectives, subnetting is a core networking concept used to improve network segmentation, performance, and security.

A Class C network uses a default subnet mask of /24 (255.255.255.0), which provides 256 total addresses (254 usable). To split this network into two sections, the administrator must borrow one host bit from the last octet. Borrowing one bit results in a /25 subnet mask (255.255.255.128). This creates two subnets, each with 128 total addresses (126 usable)-an ideal solution for separating two departments such as finance and marketing.

A /24 would not create any segmentation, as it represents the original single network. A /26 would create four subnets, and a /27 would create eight subnets, both of which exceed the requirement of only two sections and unnecessarily reduce the number of available host addresses per subnet.

The Network+ objectives emphasize selecting subnet masks based on organizational requirements, balancing the number of subnets with sufficient host capacity. In this scenario, /25 is the most efficient and correct choice.

NEW QUESTION: 253

Which of the following is most likely affected when executing a successful DoS attack?

A. Bandwidth

B. NAT pool

C. ACL

D. Storage availability

Answer: A (LEAVE A REPLY)

Bandwidth is most likely affected during a successful denial-of-service attack. A DoS attack attempts to make a system, service, or network unavailable to legitimate users. One common method is flooding the target with excessive traffic, which consumes bandwidth, processing resources, or connection capacity. When bandwidth is overwhelmed, legitimate users may experience slow connections, dropped sessions, failed requests, or complete service unavailability.

The CompTIA Network+ N10-009 objectives include identifying common attacks and understanding their effect on network availability. DoS and DDoS attacks primarily target availability, one of the three core security goals in the CIA triad: confidentiality, integrity, and availability. Network-based DoS attacks often generate large amounts of traffic, making bandwidth a primary resource under attack.

A NAT pool could be exhausted in certain attack scenarios, but it is not the most general or most likely answer. An ACL is a rule set used to permit or deny traffic; it may help mitigate an attack but is not usually the resource being consumed. Storage availability could be affected in some application-specific attacks, but bandwidth is the best answer for a typical DoS attack.

NEW QUESTION: 254

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

- A.** MTTR
- B.** RTO
- C.** RPO
- D.** MTBF

Answer: C ([LEAVE A REPLY](#))

* Definition of RPO:

* Recovery Point Objective (RPO) is a disaster recovery metric that describes the maximum acceptable amount of data loss measured in time. It indicates the point in time to which data must be recovered to resume normal operations after a disaster.

* For example, if the RPO is set to 24 hours, then the business could tolerate losing up to 24 hours' worth of data in the event of a disruption.

* Why RPO is Important:

* RPO is critical for determining backup frequency and helps businesses decide how often they need to back up their data. A lower RPO means more frequent backups and less potential data loss.

* Comparison with Other Metrics:

* MTTR (Mean Time to Repair): Refers to the average time required to repair a system or component and return it to normal operation.

* RTO (Recovery Time Objective): The maximum acceptable length of time that a computer, system, network, or application can be down after a failure or disaster occurs.

* MTBF (Mean Time Between Failures): The predicted elapsed time between inherent failures of a system during operation.

* How RPO is Used in Disaster Recovery:

* Organizations establish RPOs to ensure that they can recover data within a timeframe that is acceptable to business operations. This involves creating a backup plan that meets the RPO requirements.

References:

* CompTIA Network+ study materials and certification guides.

NEW QUESTION: 255

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: 256

- A.** Self-signed certificate
- B.** VLAN hopping

C. On-path attack

D. Phishing

Answer: C (LEAVE A REPLY)

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

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 257

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: A (LEAVE A REPLY)

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: 258

Which of the following is the best example of a networking appliance that connects different network segments and directs allowed traffic between specific segments?

A. Firewall

B. IDS

C. Unmanaged switch

D. (Not provided)

Answer: A (LEAVE A REPLY)

A firewall is the best example of an appliance that can sit between network segments and permit or deny traffic flows based on security policy. In Network+ terms, firewalls enforce segmentation controls by applying rules that match on items such as source/destination IP, ports, protocols, and (with next-generation firewalls) even applications. This makes a firewall a common choice for directing allowed traffic between specific segments (for example, allowing users in a workstation VLAN to reach only certain ports on a server VLAN, while blocking everything else). This function is core to network security architecture and is frequently paired with concepts like network segmentation, ACL-style rule sets, and creating security zones.

An IDS (intrusion detection system) primarily monitors traffic and generates alerts on suspicious activity; it does not typically control or "direct allowed traffic" unless it is specifically an IPS (prevention) with inline blocking. An unmanaged switch operates at Layer 2 and forwards frames within a broadcast domain; it does not provide policy-based filtering between security segments. Therefore, the correct answer is Firewall.

NEW QUESTION: 259

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

- A. SSH
- B. TLS
- C. SCADA
- D. RADIUS

Answer: B (LEAVE A REPLY)

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

HTTPS is HTTP encapsulated in TLS (the successor to SSL), which provides confidentiality, integrity, and server authentication for web traffic.

- * A. SSH secures remote shell and tunnels, not HTTPS.
- * C. SCADA refers to industrial control systems, not a transport security protocol.
- * D. RADIUS is an AAA protocol for authentication/authorization/accounting, not the web encryption layer.

References (CompTIA Network+ N10-009):

* Domain: Network Standards, Protocols, and Implementations - Web protocols (HTTP/HTTPS), TLS handshake and purpose, encryption in transit.

NEW QUESTION: 260

A network administrator needs to implement a solution to filter access to the internet. Which of the following should the administrator most likely implement?

- A. Router
- B. Cloud gateway
- C. Proxy
- D. Intrusion detection system

Answer: C (LEAVE A REPLY)

A proxy server can filter internet access by controlling which websites or services users can reach. It enforces content policies and can provide caching and monitoring.

- A). A router directs traffic but doesn't filter internet sites by itself.
- B). A cloud gateway could also filter, but the most direct answer is proxy.
- D). An IDS detects suspicious activity but doesn't filter browsing access.

References (CompTIA Network+ N10-009):

Domain: Network Security - Proxy servers, filtering, access control.

Valid N10-009 Dumps shared by Actual4test.com for Helping Passing N10-009 Exam! Actual4test.com now offer the **newest N10-009 exam dumps**, the Actual4test.com N10-009 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com N10-009 dumps with Test Engine here: https://www.actual4test.com/N10-009_examcollection.html (792 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)