100% Money Back Guarantee

Vendor: CompTIA

Exam Code:N10-009

Exam Name: CompTIA Network+ Exam

Version: Demo

QUESTION 1

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.

Correct Answer: B

TTL (Time To Live): TTL is a value in a DNS record that determines the amount of time it can be cached by DNS resolvers and other devices on the internet. When making changes to DNS records, reducing the TTL beforehand helps minimize the time it takes for the changes to propagate throughout the internet.

MX Record Change: Changing the MX (Mail Exchange) record directs email traffic to the specified mail server. However, DNS changes take time to propagate across the internet due to caching. If the TTL is set too high, old records may be cached for an extended period, leading to email delivery issues.

QUESTION 2

A network engineer wants to establish a site-o-site VPN tunnel using a protocol that allows for both data confidentially and authentication. Which of the following is the best choice?

A. IKE

B. AH

C. ESP

D. IPSec

Correct Answer: C

QUESTION 3

Which of the following is the correct order of components in a bottom-up approach for the three-tier hierarchical model?

A. Access, distribution, and core

B. Core, root, and distribution

C. Core, spine, and leaf

D. Access, core, and roof

Correct Answer: A

The three-tier hierarchical model in network design consists of three layers: access, distribution, and core. The access layer is where devices like PCs and printers connect to the network. The distribution layer aggregates the data received

from the access layer switches before it is transmitted to the core layer, which is responsible for high-speed data transfer and routing. This approach improves scalability and performance in larger networks.

References: CompTIA Network+ Exam Objectives and official study guides.

QUESTION 4

Early in the morning, an administrator installs a new DHCP server. In the afternoon, some users report they are experiencing network outages. Which of the following is the most likely issue?

A. Theadministrator didnot provisionenough IP addresses.

B. Theadministrator configured an incorrect default gateway.

C. Theadministrator didnot provisionenough routes.

D. Theadministrator didnot provisionenough MAC addresses.

Correct Answer: A

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.

QUESTION 5

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

A. Too much wireless reflection

B. Too much wireless absorption

C. Too many wireless repeaters

D. Too many client connections

Correct Answer: A

Reference: CompTIA Network+ Certification Exam Objectives - Wireless Networks section.

QUESTION 6

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

A. Implementingenterprise authentication

B. Requiring theuse of PSKs

C. Configuring acaptive portal for users

D. Enforcing wired equivalent protection

Correct Answer: A

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.

QUESTION 7

Which of the following ports is used for secure email?

A. 25

B. 110

C. 143

D. 587

Correct Answer: D

Port 587 is used for secure email submission. This port is designated for message submission by mail clients to mail servers using the SMTP protocol, typically with STARTTLS for encryption. Port 25: Traditionally used for SMTP relay, but

not secure and often blocked by ISPs for outgoing mail due to spam concerns. Port 110: Used for POP3 (Post Office Protocol version 3), not typically secured. Port 143: Used for IMAP (Internet Message Access Protocol), which can be

secured with STARTTLS or SSL/TLS. Port 587: Specifically used for authenticated email submission (SMTP) with encryption, ensuring secure transmission of email from clients to servers.

Network References:

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

ports.

Network+ Certification All-in-One uide: Explains email protocols, ports, and security considerations for email transmission.

QUESTION 8

A network administrator is working to configure a new device to provide Layer 2 connectivity to various endpoints including several WAPs. Which of the following devices will the administrator MOST likely configure?

A. WLAN controller

B. Cable modem

C. Load balancer

D. Switch

E. Hub

Correct Answer: D

A switch is a device that provides Layer 2 connectivity to various endpoints by forwarding frames based on MAC addresses. A switch can also connect to several WAPs (wireless access points) to provide wireless connectivity to wireless devices.

QUESTION 9

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

Correct Answer: A

Role of NTP (Network Time Protocol):

uk.co.certification.simulator.questionpool.PList@73015a56 Importance for SIEM Systems:

Comparison with Other Protocols:

Implementation:

References:

CompTIA Network+ study materials on network protocols and SIEM systems.

QUESTION 10

A network technician wants to identify which DNS servers a computer is configured to use. Which of the following commands should the technician use?

A. nbtstat

B. arp

C. nslookup

D. netstat

Correct Answer: C

QUESTION 11

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

A. Geofencing

B. Honeynet

C. Jumpbox

D. Screened subnet

Correct Answer: B

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

QUESTION 12

A network administrator received 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 switch port speed limits.

D. Enforce 802. IQ tagging.

Correct Answer: A

Spanning tree is a protocol that prevents network loops by dynamically disabling or enabling switch ports based on the network topology. Network loops can cause intermittent connectivity issues, such as broadcast storms, MAC address

table instability, and multiple frame transmission. By enabling spanning tree, the network administrator can ensure that there is only one active path between any two network devices at any given time.

References:

CompTIA Network+ N10-008 Certification Exam Objectives, page 91 CompTIA Network+ Cert Guide: Switching and Virtual LANs, page 172