examunion

Certified IT Exam Material Authority

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.examunion.com

Exam : **N10-009**

Title : CompTIA Network+ Certification

Version : DEMO

1.A network administrator is notified that a user cannot access resources on the network. The network administrator checks the physical connections to the workstation labeled User 3 and sees the Ethernet is properly connected. However, the network interface’s indicator lights are not blinking on either the computer or the switch.
Which of the following Is the most likely cause?
A. The switch failed.
B. The default gateway is wrong.
C. The port Is shut down.
D. The VLAN assignment is incorrect.
Answer: C
Explanation:
When a network interface's indicator lights are not blinking on either the computer or the switch, it suggests a physical layer issue.
Here is the detailed reasoning:
Ethernet Properly Connected: The Ethernet cable is correctly connected, eliminating issues related to a loose or faulty cable.
No Indicator Lights: The absence of blinking indicator lights on both the computer and the switch typically points to the port being administratively shut down.
Switch Port Shut Down: In networking, a switch port can be administratively shut down, disabling it from passing any traffic. This state is configured by network administrators and can be verified and changed using the command-line interface (CLI) of the switch.
Command to Check and Enable Port:
bash
Copy code
Switch> enable
Switch# configure terminal
Switch(config)# interface [interface id]
Switch(config-if)# no shutdown
The command no shutdown re-enables the interface if it was previously disabled. This will restore the link and the indicator lights should start blinking, showing activity.
Reference: Basic Configuration Commands PDF, sections on interface configuration (e.g., shutdown, no shutdown).

2.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
Explanation:
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).
Reference: CompTIA Network+ materials discussing SNMP and MIB functionality.

3.Which of the following best explains the role of confidentiality with regard to data at rest?
A. DHCP relay device
B. Policy enforcement point
C. Definition file for event translation
D. Network access controller
Answer: C
Explanation:
Confidentiality with Data at Rest: Confidentiality is a core principle of data security, ensuring that data stored (at rest) is only accessible to authorized individuals. This protection is achieved through mechanisms such as encryption, access controls, and permissions.
Privileged Access: The statement "Data can be accessed after privileged access is granted" aligns with the confidentiality principle, as it restricts data access to users who have been granted specific permissions or roles. Only those with the appropriate credentials or permissions can access the data.
Incorrect Options:
A. "Data can be accessed by anyone on the administrative network." This violates the principle of confidentiality by allowing unrestricted access.
B. "Data can be accessed remotely with proper training." This focuses on remote access rather than restricting access based on privileges.
D. "Data can be accessed after verifying the hash." This option relates more to data integrity rather than confidentiality.
Reference: CompTIA Network+ materials on data security principles, particularly sections on confidentiality and access control mechanisms.

4.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
Explanation:
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.
Reference: CompTIA Network+ study materials and DNS best practices.

5.Which of the following IP transmission types encrypts all of the transmitted data?
A. ESP
B. AH
C. GRE
D. UDP
E. TCP
Answer: A
Explanation:
Definition of ESP (Encapsulating Security Payload):
ESP is a part of the IPsec protocol suite used to provide confidentiality, integrity, and authenticity of data. ESP encrypts the payload and optional ESP trailer, providing data confidentiality.
ESP Functionality:
ESP can encrypt the entire IP packet, ensuring that the data within the packet is secure from interception or eavesdropping. It also provides options for data integrity and authentication.
ESP operates in two modes: transport mode (encrypts only the payload of the IP packet) and tunnel mode (encrypts the entire IP packet).
Comparison with Other Protocols:
AH (Authentication Header): Provides data integrity and authentication but does not encrypt the payload.
GRE (Generic Routing Encapsulation): A tunneling protocol that does not provide encryption.
UDP (User Datagram Protocol) and TCP (Transmission Control Protocol): These are transport layer protocols that do not inherently provide encryption. Encryption must be provided by additional protocols like TLS/SSL.
Use Cases:

ESP is widely used in VPNs (Virtual Private Networks) to ensure secure communication over untrusted networks like the internet.
Reference: CompTIA Network+ study materials on IPsec and encryption.