Product Questions: 171
Version: 5.0

Question: 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).

Question: 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.

Question: 3

Which of the following best explains the role of confidentiality with regard to data at rest?

A. Data can be accessed by anyone on the administrative network.
B. Data can be accessed remotely with proper training.
C. Data can be accessed after privileged access Is granted.
D. Data can be accessed after verifying the hash.

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.

Question: 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.

Question: 5

Which of the following IP transmission types encrypts all of the transmitted data?

A. ESP
B. AH
C. GRE
D. UDP
E. TC
P

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.

Question: 6

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

Explanation:
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 2.4GHz 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.
Reference:
CompTIA Network+ study materials on wireless networking and interference mitigation.

Question: 7

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

Explanation:
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.
Reference:
CompTIA Network+ study materials and certification guides.

Question: 8

Which of the following can support a jumbo frame?

A. Access point
B. Bridge
C. Hub
D. Switch

Answer: D

Explanation:

Definition of Jumbo Frames:
Jumbo frames are Ethernet frames with more than 1500 bytes of payload, typically up to 9000 bytes. They are used to improve network performance by reducing the overhead caused by smaller frames.
Why Switches Support Jumbo Frames:
Switches are network devices designed to manage data packets and can be configured to support jumbo frames. This capability enhances throughput and efficiency, particularly in high-performance networks and data centers.
Incompatibility of Other Devices:
Access Point: Primarily handles wireless communications and does not typically support jumbo frames.
Bridge: Connects different network segments but usually operates at standard Ethernet frame sizes.
Hub: A simple network device that transmits packets to all ports without distinguishing between devices, incapable of handling jumbo frames.
Practical Application:
Enabling jumbo frames on switches helps in environments where large data transfers are common, such as in storage area networks (SANs) or large-scale virtualized environments.
Reference:
CompTIA Network+ course materials and networking hardware documentation.

Question: 9

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

A. Logical diagram
B. Layer 3 network diagram
C. Service-level agreement
D. Heat map

Answer: D

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

throughout the building. The data collected is then used to generate a visual map, guiding network administrators in optimizing wireless coverage.
Reference:
CompTIA Network+ certification materials and wireless network planning guides.

Question: 10

A user is unable to navigate to a website because the provided URL is not resolving to the correct IP address. Other users are able to navigate to the intended website without issue. Which of the following is most likely causing this issue?

A. Hosts file
B. Self-signed certificate
C. Nameserver record
D. IP helper
ANS

Answer: A

Explanation:
Role of the Hosts File:
The hosts file is a local file on a computer that maps hostnames to IP addresses. It can be used to override DNS resolution by providing a static mapping of a hostname to an IP address.
Common Issues with the Hosts File:
If an incorrect IP address is mapped to a hostname in the hosts file, it can cause the computer to resolve the hostname to the wrong IP address. This can lead to navigation issues for specific websites while other users, relying on DNS, do not face the same problem.
Why Other Options are Less Likely:
Self-signed certificate: Relates to SSL/TLS and would cause a security warning, not a navigation failure.
Nameserver record: Affects all users, not just one.
IP helper: Used to forward DHCP requests and is unrelated to DNS resolution issues.
Troubleshooting Steps:
Check the hosts file on the affected user's computer (C:\Windows\System32\drivers\etc\hosts on Windows or /etc/hosts on Unix/Linux).
Look for entries that map the problematic hostname to an incorrect IP address and correct or remove them.
Reference:
CompTIA Network+ study materials and system administration documentation.

Question: 11

An IT manager needs to connect ten sites in a mesh network. Each needs to be secured with reduced provisioning time. Which of the following technologies will best meet this requirement?

A. SD-WAN
B. VXLAN
C. VPN
D. NFV

Answer: A

Explanation:
Definition of SD-WAN:
Software-Defined Wide Area Network (SD-WAN) is a technology that simplifies the management and operation of a WAN by decoupling the networking hardware from its control mechanism. It allows for centralized management and enhanced security.
Benefits of SD-WAN:
Reduced Provisioning Time: SD-WAN enables quick and easy deployment of new sites with centralized control and automation.
Security: Incorporates advanced security features such as encryption, secure tunneling, and integrated firewalls.
Scalability: Easily scales to accommodate additional sites and bandwidth requirements.
Comparison with Other Technologies:
VXLAN (Virtual Extensible LAN): Primarily used for network virtualization within data centers.
VPN (Virtual Private Network): Provides secure connections but does not offer the centralized management and provisioning efficiency of SD-WAN.
NFV (Network Functions Virtualization): Virtualizes network services but does not specifically address WAN management and provisioning.
Implementation:
SD-WAN solutions are implemented by deploying edge devices at each site and connecting them to a central controller. This allows for dynamic routing, traffic management, and security policy enforcement.
Reference:
CompTIA Network+ course materials and networking solution guides.

Question: 12

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.