Thank You for your purchase

CompTIA N10-009 Exam Question & Answers

CompTIA Network+ Certification Exam

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.

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

Explanation:

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.
Reference:
CompTIA Network+ study materials and structured cabling installation guides.

Question: 13

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

Explanation:

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.
Reference:
CompTIA Network+ study materials on rack installation and equipment sizing.

Question: 14

A VoIP phone is plugged in to a port but cannot receive calls. Which of the following needs to be done on the port to address the issue?

A. Trunk all VLANs on the port.
B. Configure the native VLAN.
C. Tag the traffic to voice VLAN.
D. Disable VLANs.

Answer: C

Explanation:

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

Question: 15

As part of an attack, a threat actor purposefully overflows the content-addressable memory (CAM) table on a switch. Which of the following types of attacks is this scenario an example of?

A. ARP spoofing
B. Evil twin
C. MAC flooding
D. DNS poisoning

Answer: C

Explanation:

Definition of MAC Flooding:
MAC flooding is an attack where a malicious actor sends numerous fake MAC addresses to a switch, overwhelming its CAM table. The CAM table stores MAC addresses and their associated ports for efficient traffic forwarding.
Impact of MAC Flooding:

CAM Table Overflow: When the CAM table is full, the switch cannot learn new MAC addresses and is forced to broadcast traffic to all ports, leading to a degraded network performance and potential data interception.
Switch Behavior: The switch operates in a fail-open mode, treating the network as a hub, which can be exploited for eavesdropping on traffic.
Comparison with Other Attacks:
ARP Spoofing: Involves sending false ARP (Address Resolution Protocol) messages to associate the attacker's MAC address with the IP address of another device.
Evil Twin: Involves creating a rogue wireless access point that mimics a legitimate one to intercept data.
DNS Poisoning: Involves corrupting the DNS cache with false information to redirect traffic to malicious sites.
Preventive Measures:
Port Security: Configure port security on switches to limit the number of MAC addresses per port, preventing CAM table overflow.
Network Segmentation: Use VLANs to segment network traffic and limit the impact of such attacks.
Reference:
CompTIA Network+ study materials on network security threats and mitigation techniques.

Question: 16

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: A

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

Question: 17

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

Explanation:
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.
Reference:
CompTIA Network+ study materials on IPsec and secure communication protocols.

Question: 18

Which of the following routing protocols uses an autonomous system number?

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

Answer: D

Explanation:

BGP (Border Gateway Protocol) uses an Autonomous System (AS) number for its operations. An AS is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the Internet. BGP is used to exchange routing information between different ASes on the Internet, making it the only protocol among the listed options that uses an AS number.
Reference: CompTIA Network+ study materials and RFC 4271.

Question: 19

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

Explanation:
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.
Reference: CompTIA Network+ study materials and NIST Special Publication 800-77.

Question: 20

A network administrator needs to connect two routers in a point-to-point configuration and conserve IP space. Which of the following subnets should the administrator use?

A. /24
B. /26
C. /28
D. /30

Answer: D

Explanation:

Using a /30 subnet mask is the most efficient way to conserve IP space for a point-to-point connection between two routers. A /30 subnet provides four IP addresses, two of which can be assigned to the router interfaces, one for the network address, and one for the broadcast address. This makes it ideal for point-to-point links where only two usable IP addresses are needed.
Reference: CompTIA Network+ study materials and subnetting principles.

Question: 21

To reduce costs and increase mobility, a Chief Technology Officer (CTO) wants to adopt cloud services for the organization and its affiliates. To reduce the impact for users, the CTO wants key services to run from the on-site data center and enterprise services to run in the cloud. Which of the following deployment models is the best choice for the organization?

A. Public
B. Hybrid
C. SaaS
D. Private

Answer: B

Explanation:

A hybrid cloud deployment model is the best choice for the CTO's requirements. It allows the organization to run key services from the on-site data center while leveraging the cloud for enterprise services. This approach provides flexibility, scalability, and cost savings, while also minimizing disruptions to users by keeping critical services local. The hybrid model integrates both private and public cloud environments, offering the benefits of both.
Reference: CompTIA Network+ study materials and cloud computing principles.

Question: 22

A technician is troubleshooting a user's laptop that is unable to connect to a corporate server. The technician thinks the issue pertains to routing. Which of the following commands should the technician use to identify the issue?

A. tcpdump
B. dig
C. tracert
D. arp

Answer: C

Explanation:
The tracert (Traceroute) command is used to determine the path packets take from the source to the destination. It helps in identifying routing issues by showing each hop the packets pass through, along with the time taken for each hop. This command can pinpoint where the connection is failing or experiencing delays, making it an essential tool for troubleshooting routing issues.
Reference: CompTIA Network+ study materials and common network troubleshooting commands.

Question: 23

Which of the following fiber connector types is the most likely to be used on a network interface card?

A. LC
B. SC
C. ST

D. MPO

Answer: A

Explanation:

Definition of Fiber Connector Types:
LC (Lucent Connector): A small form-factor fiber optic connector with a push-pull latching mechanism, commonly used for high-density applications.
SC (Subscriber Connector or Standard Connector): A larger form-factor connector with a push-pull latching mechanism, often used in datacom and telecom applications.
ST (Straight Tip): A bayonet-style connector, typically used in multimode fiber optic networks.
MPO (Multi-fiber Push On): A connector designed to support multiple fibers (typically 12 or 24 fibers), used in high-density cabling environments.
Common Usage:
LC Connectors: Due to their small size, LC connectors are widely used in network interface cards (NICs) and high-density environments such as data centers. They allow for more connections in a smaller space compared to SC and ST connectors.
SC and ST Connectors: These are larger and more commonly used in patch panels and older fiber installations but are less suitable for high-density applications.
MPO Connectors: Primarily used for trunk cables in data centers and high-density applications but not typically on individual network interface cards.
Selection Criteria:
The small form-factor and high-density capabilities of LC connectors make them the preferred choice for network interface cards, where space and connection density are critical considerations.
Reference:
CompTIA Network+ study materials on fiber optics and connector types.

Question: 24

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

Explanation:

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.
Reference:
CompTIA Network+ study materials on network security and device management.

Question: 25

A virtual machine has the following configuration:

- IPv4 address: 169.254.10.10
- Subnet mask: 255.255.0.0

The virtual machine can reach colocated systems but cannot reach external addresses on the Internet. Which of the following Is most likely the root cause?

A. The subnet mask is incorrect.
B. The DHCP server is offline.
C. The IP address is an RFC1918 private address.
D. The DNS server is unreachable.

Answer: B

Explanation:
Understanding the 169.254.x.x Address:
An IPv4 address in the range of 169.254.x.x is an Automatic Private IP Addressing (APIPA) address,

assigned when a DHCP server is unavailable.
DHCP Server Offline:
APIPA Assignment: When a device cannot obtain an IP address from a DHCP server, it assigns itself an APIPA address to enable local network communication. This allows communication with other devices on the same local subnet but not with external networks.
Resolution: Ensure the DHCP server is operational. Check for connectivity issues between the virtual machine and the DHCP server, and verify the DHCP server settings.
Comparison with Other Options:
The subnet mask is incorrect: The subnet mask 255.255.0.0 is appropriate for the 169.254.x.x range and does not prevent external access by itself.
The IP address is an RFC1918 private address: RFC1918 addresses are private IP ranges (10.x.x.x, 172.16.x.x-172.31.x.x, 192.168.x.x) but 169.254.x.x is not one of them.
The DNS server is unreachable: While this could affect name resolution, it would not prevent the assignment of a non-APIPA address or local network communication.
Troubleshooting Steps:
Verify the DHCP server’s status and connectivity.
Restart the DHCP service if necessary.
Renew the IP lease on the virtual machine using commands such as ipconfig /renew (Windows) or dhclient (Linux).
Reference:
CompTIA Network+ study materials on IP addressing and DHCP troubleshooting.

Question: 26

A network technician is troubleshooting a web application's poor performance. The office has two internet links that share the traffic load. Which of the following tools should the technician use to determine which link is being used for the web application?

A. netstat
B. nslookup
C. ping
D. tracert

Answer: D

Explanation:
Understanding Tracert:
Traceroute Tool: tracert (Windows) or traceroute (Linux) is a network diagnostic tool used to trace the path that packets take from a source to a destination. It lists all the intermediate routers the packets traverse.
Determining Traffic Path:
Path Identification: By running tracert to the web application's destination IP address, the technician can identify which route the traffic is taking and thereby determine which internet link is being used.

Load Balancing Insight: If the office uses load balancing for its internet links, tracert can help verify which link is currently handling the traffic for the web application.
Comparison with Other Tools:
netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace the path of packets.
nslookup: Used for querying DNS to obtain domain name or IP address mapping, not for tracing packet routes.
ping: Tests connectivity and measures round-trip time but does not provide path information.
Implementation:
Open a command prompt or terminal.
Execute tracert [destination IP] to trace the route.
Analyze the output to determine the path and the link being used.
Reference:
CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 27

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

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

Question: 28

Which of the following does a full-tunnel VPN provide?

A. Lower bandwidth requirements
B. The ability to reset local computer passwords
C. Corporate Inspection of all network traffic
D. Access to blocked sites

Answer: C

Explanation:
A full-tunnel VPN routes all of a user's network traffic through the corporate network. This means that the organization can inspect all network traffic for security and compliance purposes, as all data is tunneled through the VPN, allowing for comprehensive monitoring and inspection.
Reference: CompTIA Network+ study materials.

Question: 29

A customer is adding fiber connectivity between adjacent buildings. A technician terminates the multimode cable to the fiber patch panel. After the technician connects the fiber patch cable, the indicator light does not turn on. Which of the following should a technician try first to troubleshoot this issue?

A. Reverse the fibers.
B. Reterminate the fibers.
C. Verify the fiber size.
D. Examine the cable runs for visual faults.

Answer: A

Explanation:
When working with fiber optic cables, one common issue is that the transmit (TX) and receive (RX) fibers might be reversed. The first step in troubleshooting should be to reverse the fibers at one end to ensure they are correctly aligned (TX to RX and RX to TX). This is a simple and quick step to rule out a common issue before moving on to more complex troubleshooting.
Reference: CompTIA Network+ study materials.

Question: 30

Which of the following protocols has a default administrative distance value of 90?

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

Answer: B

Explanation:
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.
Reference: CompTIA Network+ study materials.

Question: 31

Which of the following is a cost-effective advantage of a split-tunnel VPN?

A. Web traffic is filtered through a web filter.
B. More bandwidth is required on the company's internet connection.
C. Monitoring detects insecure machines on the company’s network.
D. Cloud-based traffic flows outside of the company's network.

Answer: D

Explanation:

A split-tunnel VPN allows certain traffic (e.g., cloud-based services) to bypass the VPN and go directly to the Internet. This reduces the amount of traffic that needs to traverse the company's VPN and Internet connection, conserving bandwidth and reducing costs. It also means that not all traffic is subject to the same level of inspection or filtering, which can improve performance for cloud-based services.
Reference: CompTIA Network+ study materials.

Question: 32

Which of the following should be configured so users can authenticate to a wireless network using company credentials?

A. SSO
B. SAML
C. MFA
D. RADIUS

Answer: D

Explanation:
RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS is often used to manage access to wireless networks, enabling users to authenticate with their company credentials, ensuring secure access to the network.
Reference: CompTIA Network+ study materials.

Question: 33

Which of the following is most likely responsible for the security and handling of personal data in Europe?

A. GDPR
B. SCADA

C. SAML
D. PCI DSS

Answer: A

Explanation:
Definition of GDPR:
General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
Scope and Objectives:
GDPR aims to give individuals control over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
It enforces rules about data protection, requiring companies to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.
Comparison with Other Options:
SCADA (Supervisory Control and Data Acquisition): Refers to control systems used in industrial and infrastructure processes, not related to personal data protection.
SAML (Security Assertion Markup Language): A standard for exchanging authentication and authorization data between parties, not specifically for personal data protection.
PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment, not specific to personal data protection in Europe.
Key Provisions:
GDPR includes provisions for data processing, data subject rights, obligations of data controllers and processors, and penalties for non-compliance.
Reference:
CompTIA Network+ study materials on regulatory and compliance standards.

Question: 34

Users cannot connect to an internal website with an IP address 10.249.3.76. A network administrator runs a command and receives the following output:

```
1 3ms 2ms 3ms 192.168.25.234
2 2ms 3ms 1ms 192.168.3.100
3 4ms 5ms 2ms 10.249.3.1
4 *
5 ’
6 *
7 •
```

Which of the following command-line tools is the network administrator using?

A. tracert

B. netstat
C. tcpdump
D. nmap

Answer: A

Explanation:

Understanding Tracert:
tracert (Traceroute in Windows) is a command-line tool used to trace the path that packets take from the source to the destination. It records the route (the specific gateways at each hop) and measures transit delays of packets across an IP network.
Output Analysis:
The output shows a series of IP addresses with corresponding round-trip times (RTTs) in milliseconds. The asterisks (*) indicate that no response was received from those hops, which is typical for routers or firewalls that block ICMP packets used by tracert.
Comparison with Other Tools:
netstat: Displays network connections, routing tables, interface statistics, and more, but does not trace packet routes.
tcpdump: Captures network packets for analysis, used for detailed network traffic inspection.
nmap: A network scanning tool used to discover hosts and services on a network, not for tracing packet routes.
Usage:
tracert helps identify the path to a destination and locate points of failure or congestion in the network.
Reference:
CompTIA Network+ study materials on network troubleshooting and diagnostic tools.

Question: 35

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

^p
Explanation:

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

Question: 36

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. 4096
B. 8192
C. 32768
D. 36684

Answer: C

Explanation:

Understanding Spanning Tree Protocol (STP):
STP is used to prevent network loops in Ethernet networks by creating a spanning tree that selectively blocks some redundant paths.
Default Priority Value:
Bridge Priority: STP uses bridge priority to determine which switch becomes the root bridge. The default bridge priority value for most switches is 32768.
Priority Range: The bridge priority can be set in increments of 4096, ranging from 0 to 61440.
Configuration and Verification:
When deploying a new switch, the network administrator can verify the bridge priority using commands such as show spanning-tree to ensure it is set to the default value of 32768.
Comparison with Other Values:

4096 and 8192: Lower than the default priority, indicating these would be manually configured for higher preference.
36684: A non-standard value, likely a result of specific configuration changes.
Reference:
CompTIA Network+ study materials on Spanning Tree Protocol and network configuration.

Question: 37

Which of the following steps of the troubleshooting methodology should a technician take to confirm a theory?

A. Duplicate the problem.
B. Identify the symptoms.
C. Gather information.
D. Determine any changes.

Answer: A

Explanation:

Troubleshooting Methodology:
Troubleshooting involves a systematic approach to diagnosing and resolving issues. It typically includes steps such as identifying symptoms, gathering information, formulating and testing theories, and implementing solutions.
Confirming a Theory:
Duplicate the Problem: To confirm a theory, the technician should reproduce the problem in a controlled environment. This helps verify that the identified cause actually leads to the observed issue.
Verification: By duplicating the problem, the technician can observe the issue firsthand, validate the hypothesis, and rule out other potential causes.
Comparison with Other Steps:
Identify the Symptoms: Initial step to understand what the problem is, not specifically for confirming a theory.
Gather Information: Involves collecting data and details about the issue, usually done before formulating a theory.
Determine Any Changes: Involves checking for recent changes that could have caused the issue, a part of the information-gathering phase.
Implementation:
Use similar equipment or software in a test environment to recreate the issue.
Observe the results to see if they match the original problem, thereby confirming the theory.
Reference:
CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 38

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

Explanation:

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.
Reference: CompTIA Network+ study materials.

Question: 39

Which of the following network topologies contains a direct connection between every node in the network?

A. Mesh
B. Hub-and-spoke
C. Star
D. Point-to-point

Answer: A

Explanation:

In a mesh topology, every node is directly connected to every other node. This provides high redundancy and reliability, as there are multiple paths for data to travel between nodes. This topology is often used in networks where high availability is crucial.
Reference: CompTIA Network+ study materials.

Question: 40

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

Explanation:

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.
Reference: CompTIA Network+ study materials.

Question: 41

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

Explanation:
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.
Reference: CompTIA Network+ study materials.

Question: 42

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

Explanation:

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.
Reference: CompTIA Network+ study materials.

Question: 43

Which of the following devices can operate in multiple layers of the OSI model?

A. Hub
B. Switch
C. Transceiver
D. Modem

Answer: B

Explanation:
Understanding Switches:
Layer 2 (Data Link Layer): Traditional switches operate primarily at Layer 2, where they use MAC addresses to forward frames within a local network.
Layer 3 (Network Layer): Layer 3 switches, also known as multilayer switches, can perform routing functions using IP addresses to forward packets between different networks.
Capabilities of Multilayer Switches:
VLANs and Inter-VLAN Routing: Multilayer switches can handle VLAN (Virtual Local Area Network) configurations and perform inter-VLAN routing, enabling communication between different VLANs.
Routing Protocols: They can run routing protocols like OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol) to manage traffic between networks.
Comparison with Other Devices:
Hub: Operates only at Layer 1 (Physical Layer) and simply repeats incoming signals to all ports.
Transceiver: Also operates at Layer 1, converting electrical signals to optical signals and vice versa.
Modem: Primarily operates at Layer 1 and Layer 2, modulating and demodulating signals for transmission over different types of media.
Practical Application:
Multilayer switches are commonly used in enterprise networks to optimize performance and manage complex routing and switching requirements within a single device.
Reference:
CompTIA Network+ study materials on network devices and the OSI model.

Question: 44

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

Explanation:

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.
Reference:
CompTIA Network+ study materials on network maintenance and security best practices.

Question: 45

Which of the following is the next step to take after successfully testing a root cause theory?

A. Determine resolution steps.
B. Duplicate the problem in a lab.
C. Present the theory for approval.
D. Implement the solution to the problem.

Answer: A

Explanation:

Troubleshooting Methodology:
Confirming the Root Cause: After testing and confirming the theory, the next logical step is to address the issue by implementing a solution.
Implementation of the Solution:
Resolve the Issue: Implement the identified solution to rectify the problem. This step involves making necessary changes to the network configuration, replacing faulty hardware, or applying software patches.
Documentation: Document the solution and the steps taken to resolve the issue to provide a reference for future troubleshooting.
Comparison with Other Steps:
Determine Resolution Steps: This is part of the implementation process where specific actions are outlined, but the actual next step after testing is to implement those steps.
Duplicate the Problem in a Lab: This step is typically done earlier in the troubleshooting process to understand the problem, not after confirming the root cause.
Present the Theory for Approval: In some scenarios, presenting the theory might be necessary for major changes, but generally, once the root cause is confirmed, the solution should be implemented.
Final Verification:
After implementing the solution, it is important to verify that the issue is resolved and that normal operations are restored. This may involve monitoring the network and testing to ensure no further issues arise.
Reference:
CompTIA Network+ study materials on troubleshooting methodologies and best practices.

Question: 46

Which of the following network devices converts wireless signals to electronic signals?

A. Router
B. Firewall
C. Access point
D. Load balancer

Answer: C

Explanation:

Role of an Access Point (AP):
Wireless to Wired Conversion: An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi. It converts wireless signals (radio waves) into electronic signals that can be understood by wired network devices.
Functionality:
Signal Conversion: The AP receives wireless signals from devices such as laptops, smartphones, and tablets, converts them into electronic signals, and transmits them over the wired network.
Connectivity: APs provide a bridge between wireless and wired segments of the network, enabling seamless communication.
Comparison with Other Devices:
Router: Directs traffic between different networks and may include built-in AP functionality but is not

primarily responsible for converting wireless to electronic signals.
Firewall: Protects the network by controlling incoming and outgoing traffic based on security rules, not involved in signal conversion.
Load Balancer: Distributes network or application traffic across multiple servers to ensure reliability and performance, not involved in signal conversion.
Deployment:
APs are commonly used in environments where wireless connectivity is needed, such as offices, homes, and public spaces. They enhance mobility and provide flexible network access.
Reference:
CompTIA Network+ study materials on wireless networking and access points.

Question: 47

Which of the following connectors provides console access to a switch?

A. ST
B. RJ45
C. BNC
D. SFP

Answer: B

Explanation:

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).
Reference:
CompTIA Network+ study materials on network devices and connectors.

Question: 48

A network administrator wants users to be able to authenticate to the corporate network using a port-based authentication framework when accessing both wired and wireless devices. Which of the following is the best security feature to accomplish this task?

A. 802.1X
B. Access control list
C. Port security
D. MAC filtering

Answer: A

Explanation:

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

Question: 49

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

Explanation:

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.
Reference: CompTIA Network+ study materials.

Question: 50

Which of the following should a network administrator configure when adding OT devices to an