6.7 Module Quiz

Date: 11/30/2025, 11:26:23 AM

Time Spent: 29:54

Score: 95%

Passing Score: 80%

Question 1 ✓ Correct

A network administrator is troubleshooting an issue where a client device cannot access a web server. The administrator uses a packet analyzer and observes that the client is sending packets to the server on port 80, but the server is not responding.

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

- ○ The server's MAC address is not configured correctly.
- ○ The Transport layer protocol being used is UDP instead of TCP.
- ○ The client device has an incorrect IP address.
- ◉ The server is using a different port for HTTP communication. ✓ Correct

Explanation

If the client is sending packets to port 80 (the default port for HTTP) but the server is not responding, it is possible that the server is configured to use a different port for HTTP communication. For example, the server might be using port 8080 instead of port 80.

If the client had an incorrect IP address, it would not be able to send packets to the server at all. The scenario specifies that packets are being sent to the server, so the IP address is not the issue.

HTTP communication requires the use of TCP, not UDP. If UDP were being used, the client would not be able to establish a connection with the server in the first place. The issue described in the scenario is related to the port number, not the protocol.

MAC addresses are used at the Link layer for local network communication. If there were an issue with the server's MAC address, the client would not be able to send packets to the server at all. The scenario specifies that packets are being sent, so the MAC address is not the problem.

Related Content

- 6.3.1 Protocols and Ports
- 6.3.2 Transmission Control Protocol
- 6.3.4 User Datagram Protocol
- 6.3.6 Well-Known Ports

6.3.7 Lesson Review
resources\questions\q_protocols_and_ports_03.question.xml

Question 2 ✓ Correct

Which of the following are options for connecting a computing device, such as a notebook computer or tablet, to a cellular network? (Select four.)

- [x] Use an integrated cellular antenna to connect the device directly to the cellular network. ✓ Correct
- [ ] Use an integrated transmitter to connect the device directly to the cellular network through a satellite.
- [x] Use a USB cable to connect the device to the network through a smartphone. ✓ Correct
- [x] Use a USB cellular adapter to connect the device directly to the cellular network. ✓ Correct
- [ ] Use a USB transmitter to connect the device directly to the cellular network through a satellite.
- [x] Use the device's Wi-Fi to connect to the network through a cellular Wi-Fi hotspot. ✓ Correct
- [ ] Use a USB cable to connect the device to the cellular network through a cable modem.
- [ ] Use the device's Wi-Fi to connect to the cellular network through a cable modem's Wi-Fi antenna.

Explanation

You can connect a computing device, such as a notebook computer or tablet, to a cellular network by using any of these four options:

- Use a USB cable to connect the device to the network through a smartphone.
- Use the device's Wi-Fi to connect to the network through a cellular Wi-Fi hotspot.
- Use a USB cellular adapter to connect the device directly to the cellular network.
- Use an integrated cellular antenna to connect the device directly to the cellular network.

A transmitter antenna, or dish, connects you to a satellite network, not a cellular network.

Connecting to the cable service does not connect you to a cellular network (cable is a separate type of networking service).

Related Content

6.1.8 Cellular Radio Internet Connections

resources\questions\q_cellular_radio_internet_connections_03.question.xml

Question 3 ✓ Correct

A network administrator notices that several devices on the network are unable to connect to the internet. Upon investigation, they find that the affected devices have IP addresses in the 169.254.x.x range.

The DHCP server appears to be running, and other devices on the network are functioning correctly.

What is the MOST likely cause of the issue?

- The affected devices are using static IP addresses that conflict with the DHCP scope.
- The DHCP server is configured with an incorrect subnet mask for the network.
- **The DHCP scope does not have enough available IP addresses to assign to new devices.** ✓ Correct
- The DNS server is misconfigured, preventing devices from resolving domain names.

Explanation

Devices receiving an IP address in the 169.254.x.x range indicate that they could not obtain an IP address from the DHCP server. If the DHCP scope has run out of available IP addresses, the server cannot assign new addresses to devices, causing them to self-assign an APIPA address. This scenario matches the symptoms described.

The issue described is related to IP address assignment, not domain name resolution. A misconfigured DNS server would cause problems with resolving domain names (e.g., accessing websites), but devices would still have valid IP addresses assigned by the DHCP server.

Devices with static IP addresses would not attempt to contact the DHCP server for an address. Additionally, a conflict with the DHCP scope would not result in the devices receiving an APIPA address (169.254.x.x).

An incorrect subnet mask on the DHCP server would typically cause connectivity issues for all devices on the network, not just a subset. The scenario specifies that other devices are functioning correctly, which rules out this possibility.

Related Content

6.4.1 DHCP Functions

resources\questions\q_dhcp_functions_04.question.xml

Question 4 ✓ Correct

Which of the following are valid IP addresses? (Select two.)

- [ ] 1.254.1.1024
- [ ] 10.384.0.3
- [x] 172.16.1.26 ✓ Correct
- [x] 2.2.2.2 ✓ Correct
- [ ] 254.7.1.417
- [ ] 192.168.1.512
- [ ] 256.0.0.1

Explanation

A valid IPv4 address consists of four 8-bit (1-byte) numbers separated by periods. For example, 10.0.0.65 is a valid IP address. Because they are 8 bits long, these numbers are frequently called octets.

Even though we typically express these numbers using decimal notation, it is important to remember that these numbers are binary numbers. The lowest value one of these numbers can have is 00000000. The decimal equivalent for this number is simply 0. The highest value one of these numbers can take is 11111111. The decimal equivalent of this number is 255. So, in decimal notation, each octet must contain a number between 0 and 255.

Related Content

6.2.6 IPv4 Addressing

6.2.8 Network Prefixes

6.2.9 IPv4 Forwarding

6.2.14 SOHO Router Configuration

resources\questions\q_ipv4_addressing_04.question.xml

Question 5 ✓ Correct

An IT administrator is troubleshooting a file transfer issue between a client and a server.

Using a protocol analyzer, the administrator observes that the client sends a SYN packet to the server, and the server responds with a SYN/ACK packet, but the client does not send the final ACK packet.

Based on this observation, what is the MOST likely cause of the issue?

- The server's port number is incorrectly configured, causing the client to fail to respond.
- The client's application is using an outdated version of the protocol, which does not support the three-way handshake.
- **The client's TCP connection is being blocked by a firewall, preventing the completion of the three-way handshake.** ✓ Correct
- The server is using UDP instead of TCP, which does not require a three-way handshake.

Explanation

The three-way handshake (SYN, SYN/ACK, ACK) is a fundamental part of establishing a TCP connection. If the client does not send the final ACK packet, it is likely that something is blocking the connection, such as a firewall or security rule. TCP requires this handshake to establish a reliable connection, and any interruption in this process will prevent the connection from being established.

The scenario explicitly describes the SYN and SYN/ACK packets, which are part of the TCP handshake process. UDP does not use a three-way handshake, so the presence of SYN and SYN/ACK packets confirms that TCP is being used.

The server has already responded with a SYN/ACK packet, indicating that the port configuration is correct and the server is listening for connections. The issue lies with the client's failure to send the final ACK packet, not the server's port configuration.

The three-way handshake is a fundamental feature of TCP and has been part of the protocol since its inception. There is no "outdated version" of TCP that lacks this feature. The issue is more likely related to network interference, such as a firewall blocking the connection.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_transmission_control_protocol_04.question.xml

Question 6 Correct

Which protocol at the Transport Layer guarantees connection-oriented forwarding of packets?

- Address Resolution Protocol (ARP)
- Transmission Control Protocol (TCP) ✓ Correct
- Internet Protocol (IP)
- User Datagram Protocol (UDP)

Explanation

TCP is the correct answer because it is the protocol at the Transport Layer that guarantees connection-oriented forwarding of packets. It ensures reliable communication by identifying and recovering from lost or out-of-order packets, making it suitable for most application protocols that require data integrity.

UDP is incorrect because, while it is also a Transport Layer protocol, it provides unreliable, connectionless forwarding. It does not guarantee delivery or order of packets, making it faster but less reliable than TCP. UDP is typically used for time-sensitive applications like video or voice streaming.

ARP is incorrect because it operates at the Internet Layer, not the Transport Layer. Its purpose is to resolve IP addresses to MAC addresses, enabling communication between devices on the same local network.

IP is incorrect because it operates at the Internet Layer, not the Transport Layer. It is responsible for addressing and routing packets between networks but does not manage connections or guarantee reliable delivery.

Related Content

resources\questions\q_transport_layer_01.question.xml

Question 7 ✓ Correct

A company is setting up a secure web server to handle sensitive customer transactions.

During testing, the IT team notices that some packets are occasionally lost due to network congestion.

Which protocol should the team use to ensure reliable delivery of data and prevent transaction failures?

- (●) TCP, because it ensures reliable delivery through acknowledgments, retransmissions, and sequence numbers. ✓ Correct
- ( ) TFTP, because it uses its own acknowledgment messaging and is suitable for secure transactions.
- ( ) DHCP, because it is designed to handle network configuration and can recover from packet loss.
- ( ) UDP, because it prioritizes speed and can handle packet loss without retransmissions.

Explanation

TCP is specifically designed to handle scenarios where reliable delivery is critical. As described in the document, TCP uses mechanisms like sequence numbers, acknowledgments (ACK), and retransmissions to ensure that all packets are delivered correctly and in order. This makes it ideal for secure web servers handling sensitive transactions, where missing or corrupted packets could cause failures.

UDP is a connectionless protocol that does not guarantee reliable delivery. It does not retransmit lost packets or ensure that packets are received in order. While UDP is faster, it is unsuitable for scenarios where reliability is critical, such as secure web transactions.

DHCP is not a transport protocol like TCP or UDP. It is used to assign IP configuration information to devices on a network. While DHCP can handle packet loss by restarting the process, it is not designed for reliable data delivery in application-level communications.

TFTP (Trivial File Transfer Protocol) is a simple protocol used for transferring files, often in network device configurations. While it uses its own acknowledgment messaging, it does not provide the robust reliability features of TCP, nor is it suitable for secure transactions.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_transmission_control_protocol_03.question.xml

Question 8 Correct

A small business is experiencing intermittent internet connectivity issues with their cable modem. Upon investigation, you find that the coaxial cable is securely connected, the RJ45 cable is properly attached to the router, and the modem's power light is on.

However, the modem's connection light is blinking instead of staying solid.

What is the MOST likely cause of the issue?

- The F-type connector on the coaxial cable is overtightened, causing signal interference.
- The modem is incompatible with the router being used.
- The RJ45 cable is faulty and needs to be replaced.
- The cable modem termination system (CMTS) at the service provider's end is experiencing issues. ✓ Correct

Explanation

The CMTS forwards data traffic from the coaxial cable to the ISP's point of presence. A blinking connection light on the modem typically indicates that the modem is unable to establish a stable connection with the service provider's network, which could be due to issues with the CMTS. This is the most logical explanation based on the scenario.

While it is advised not to overtighten the F-type connector, overtightening is unlikely to cause intermittent connectivity issues. The blinking connection light suggests a problem beyond the physical connection, making this answer incorrect.

The RJ45 cable connects the modem to the router, not to the service provider's network. Since the issue is with the modem's connection to the service provider, the RJ45 cable is not the likely cause of the problem.

If the modem were incompatible with the router, the issue would manifest as a failure to connect the local network to the modem, not as a blinking connection light. The problem described in the scenario points to the modem's connection with the service provider, not the router.

Related Content

6.1.3 Cable Modems

resources\questions\q_cable_modems_03.question.xml

Question 9 ✕ Incorrect

How does a Virtual LAN (VLAN) improve network performance and security?

- By replacing the need for firewalls and other security measures in a network ✕ Incorrect
- By reducing the size of broadcast domains and isolating traffic between groups of devices ✓ Correct
- By automatically assigning IP addresses to devices in the network
- By physically separating devices into different networks to prevent unauthorized access

Explanation

VLANs logically segment a network into smaller broadcast domains. This reduces unnecessary traffic and isolates communication between groups of devices, improving both performance and security.

VLANs do not handle IP address assignment. That function is typically performed by a DHCP server. VLANs focus on logical segmentation and traffic isolation, not IP management.

VLANs do not involve physical separation. They achieve logical separation, allowing devices on the same physical switch to be grouped into different logical networks.

VLANs do not replace firewalls or other security measures. While VLANs enhance security by isolating traffic, they are not a substitute for comprehensive network security tools like firewalls.

Related Content

6.4.6 Virtual LANs

resources\questions\q_virtual_lans_02.question.xml

Question 10 ✓ Correct

How do DNS Spam Management Records, such as SPF records, help reduce email spam?

- By blocking all incoming emails from unknown domains
- By redirecting email traffic to a secure server
- By encrypting all email messages sent from a domain
- By specifying which mail servers are authorized to send emails on behalf of a domain ✓ Correct

Explanation

DNS Spam Management Records, such as SPF (Sender Policy Framework) records, help reduce email spam by allowing domain owners to specify which mail servers are authorized to send emails on their behalf. This helps receiving mail servers verify the authenticity of the sender and prevents email spoofing.

DNS Spam Management Records do not deal with encryption. Encryption is handled by other protocols, such as TLS, and is not related to the function of SPF records.

DNS Spam Management Records do not redirect email traffic. Their purpose is to validate the sender's domain, not to manage the routing of email traffic.

DNS Spam Management Records do not block emails outright. Instead, they provide a mechanism for verifying the legitimacy of the sender's domain, allowing mail servers to make informed decisions about accepting or rejecting emails.

Related Content

6.4.5 DNS Spam Management Records

resources\questions\q_dns_spam_management_records_02.question.xml

Question 11 Correct

What is the primary purpose of a Virtual LAN (VLAN)?

- To physically separate devices on a network
- To logically segment a network into smaller, isolated broadcast domains ✓ Correct
- To assign static IP addresses to devices on a network
- To replace the need for a Domain Name System (DNS)

Explanation

VLANs are designed to logically divide a network into separate broadcast domains, even if the devices are connected to the same physical switch. This helps improve network performance and security by isolating traffic.

VLANs do not involve physical separation of devices. Instead, VLANs achieve logical separation, allowing devices to communicate as if they are on separate physical networks without requiring additional hardware.

VLANs are not responsible for assigning IP addresses. Assigning static or dynamic IP addresses is typically managed by DHCP or manual configuration, not VLANs.

VLANs and DNS serve entirely different purposes. DNS resolves hostnames to IP addresses, while VLANs are used for network segmentation and traffic isolation.

Related Content

6.4.6 Virtual LANs
resources\questions\q_virtual_lans_01.question.xml

Question 12 ✓ Correct

You are working as a junior technician for a small consulting firm. You have been tasked with installing a new computer on the network. You have performed this task and connected the computer to the network.

To verify network connectivity, you decide to ping the network server. Before this can happen, the new device needs to know the MAC address of the network server so it can match it to the IP address.

The computer sends a broadcast message, asking who has the IP address. The network server responds with its MAC address, and now the computer can communicate with the server.

Which protocol is being used when sending the broadcast message to match the MAC address to the IP address?

- ICMP
- ARP ✓ Correct
- IP
- HTTP

Explanation

Address Resolution Protocol (ARP) is used to match a device's IP address to its MAC address. Some network devices, such as switches, will build tables to match MAC addresses with IP addresses in order to always know where to send packets. When a host wants to send some data, it uses ARP to send a broadcast message out on the network, requesting that the host with a specific IP address respond with its MAC address. When the sending host gets the response, it can then match up the MAC address and IP address.

Internet Control Message Protocol (ICMP) is used when sending ping packets, but it is not used to match a MAC address to an IP address.

HyperText Transfer Protocol (HTTP) defines how pages with hyperlinks (web pages) are designed. It is not used to match a MAC address to an IP address.

Internet Protocol (IP) defines how data moves across a network. IP is not used to match the MAC address to an IP address.

Related Content

resources\questions\q_internet_layer_02.question.xml

Question 13 Correct

An organization has implemented VLANs to separate traffic for its Sales, Finance, and IT departments. However, the IT team notices that devices in the Sales VLAN cannot communicate with devices in the Finance VLAN, even though some applications require inter-department communication.

What is the MOST likely cause of this issue, and how can it be resolved?

- (●) The switch is not configured with a router or Layer 3 device to enable inter-VLAN communication. ✓ Correct
- ( ) VLANs are designed to block all inter-VLAN communication, and the network must be reconfigured to use a single VLAN.
- ( ) The VLANs are misconfigured, and all devices should be assigned to the same VLAN to allow communication.
- ( ) The devices in the Sales VLAN and Finance VLAN are using different IP address ranges, which prevents communication.

Explanation

VLANs inherently isolate traffic between different VLANs. To enable communication between VLANs, a router or Layer 3 switch must be configured to route traffic between them. Without this configuration, devices in separate VLANs cannot communicate.

VLANs do not block inter-VLAN communication permanently. Inter-VLAN communication is possible with the proper configuration of a router or Layer 3 switch. Reconfiguring the network to use a single VLAN would negate the benefits of VLANs, such as traffic isolation and improved security.

Different IP address ranges are expected in separate VLANs. The issue is not the IP address ranges but the lack of a routing mechanism to enable communication between the VLANs.

Assigning all devices to the same VLAN would eliminate the logical segmentation provided by VLANs. The problem is not a misconfiguration of VLANs but the absence of a routing solution for inter-VLAN communication.

Related Content

6.4.6 Virtual LANs

resources\questions\q_virtual_lans_04.question.xml

Question 14 Correct

Which of the following BEST describes the role of a digital modem in an Internet connection?

- It manages the routing of data packets between different networks.
- It acts as a firewall to protect the local network from external threats.
- It establishes the physical connection to the WAN interface. ✓ Correct
- It assigns IP addresses to devices on the local network.

Explanation

A digital modem is responsible for creating the physical connection between the local network and the ISP's network, enabling access to the Internet. A modem is the device that connects the local network to the ISP's network for Internet access.

Assigning IP addresses is the role of a DHCP server, which is often a function of a router, not the modem. The modem's primary function is to establish the physical connection to the WAN interface.

Firewalls are separate devices or software that monitor and control incoming and outgoing network traffic. A modem does not perform this function.

Routing is the responsibility of a router, not the modem. The modem's role is limited to establishing the physical connection to the ISP's network.

Related Content

resources\questions\q_internet_connection_types_and_modems_01.question.xml

Question 15

Correct

A network administrator is troubleshooting a connectivity issue in a corporate network. Devices in one subnet (192.168.1.0/24) cannot communicate with devices in another subnet (192.168.2.0/24). Both subnets are connected to a router, and the router has been configured with the correct IP addresses for each subnet.

Upon further investigation, the administrator discovers that IPv4 forwarding is disabled on the router.

What conclusion can the administrator draw from this information to resolve the issue?

- The router's NAT (Network Address Translation) configuration is incorrect.
- The devices in the 192.168.1.0/24 subnet are using an incorrect default gateway.
- The subnet masks for both subnets are misconfigured, preventing communication.
- The router cannot route packets between the two subnets because IPv4 forwarding is disabled. ✓ Correct

Explanation

IPv4 forwarding is a critical function that allows a router to forward packets between different subnets. If IPv4 forwarding is disabled, the router will not route traffic between the 192.168.1.0/24 and 192.168.2.0/24 subnets, even if the IP addresses and subnet configurations are correct. Enabling IPv4 forwarding will resolve the issue by allowing the router to forward packets between the subnets.

While an incorrect default gateway can cause communication issues, the scenario specifies that the router is correctly configured with the appropriate IP addresses for each subnet. The issue lies with the router's inability to forward packets, not with the devices' default gateway settings.

Misconfigured subnet masks can cause communication issues within or between subnets. However, the scenario specifies that the subnets are correctly defined as 192.168.1.0/24 and 192.168.2.0/24. The problem is not related to subnet mask configuration but to the router's disabled IPv4 forwarding feature.

NAT is used to translate private IP addresses to public IP addresses for internet access. In this scenario, the issue is related to communication between two private subnets within the same network. NAT is not required for this type of communication, so its configuration is irrelevant to the problem described.

Related Content

6.2.8 Network Prefixes

6.2.9 IPv4 Forwarding

resources\questions\q_ipv4_forwarding_03.question.xml

Question 16 Correct

A SOHO's connection to the internet is through an antenna that sends and receives a microwave signal to the ISP's antenna. There can be no obstacles on the direct path between the two antennae.

Which of the following internet connection types is this?

- Fiber
- Satellite
- WISP ✓ Correct
- DSL

Explanation

A wireless internet service provider (WISP) uses microwave or radio frequency signals between two antennae. The direct path between the antennae cannot be blocked.

A fiber internet connection uses fiber cabling. Transmitted light pulses are carried by the fiber.

Digital subscriber line (DSL) uses a modem that connects to copper telephone lines, allows the use of the internet and phone calls at the same time, and has average download speeds of 3 to 7 Mbps.

Satellite internet connections are made through satellites orbiting the Earth in a geosynchronous orbit. Typically, a roof-mounted satellite dish is aimed at the target satellite, and a transceiver sends and receives data.

Related Content

6.1.7 Fixed Wireless Internet Access
resources\questions\q_fixed_wireless_internet_access_03.question.xml

Question 17

Correct

A network administrator troubleshoots a video conferencing application that occasionally experiences minor glitches, such as dropped video frames or slight audio delays.

After analyzing the network traffic, the administrator observes that the application uses a connectionless protocol with minimal overhead.

Based on this information, which conclusion can the administrator make about the protocol being used and its suitability for the application?

- The application uses TCP, which is unsuitable because it prioritizes reliability over speed.
- The application uses UDP, which is suitable because it prioritizes speed and can tolerate minor data loss. ✓ Correct
- The application uses SSH, which is unsuitable because it is designed for secure remote access, not real-time communication.
- The application uses HTTPS, which is unsuitable because it is designed for secure web browsing, not video conferencing.

Explanation

UDP is a connectionless protocol with minimal overhead, making it ideal for time-sensitive applications like video conferencing. While it does not guarantee the delivery or sequencing of packets, it allows for faster communication, and minor glitches (e.g., dropped frames) are acceptable in this context. The administrator's observation of a connectionless protocol aligns with UDP's characteristics, confirming its suitability for the application.

TCP is a connection-oriented protocol that ensures reliable delivery of data through acknowledgments and retransmissions. This adds overhead and latency, making it unsuitable for real-time applications like video conferencing. The administrator's observation of a connectionless protocol rules out TCP.

HTTPS is an application-layer protocol used for secure communication over the web. It relies on TCP for reliable data delivery and is not designed for real-time communication. The administrator's observation of minimal overhead and a connectionless protocol does not align with HTTPS.

SSH is a protocol used for secure remote access to servers and devices. It relies on TCP for reliable and encrypted communication, making it unsuitable for video conferencing. The administrator's observation of a connectionless protocol rules out SSH as a possibility.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_user_datagram_protocol_06.question.xml

Question 18 ✓ Correct

You are setting up a small office network and need to ensure that devices on your local network can communicate with external networks, such as the Internet. You already have a modem connected to your ISP.

What device should you configure next, and what is its primary role?

- ○ A cable modem, to establish a physical connection to the ISP's network
- ◉ A router, to forward data packets between your local network and external networks using IP ✓ Correct
- ○ A switch, to connect multiple devices within the local network
- ○ A DSL splitter, to separate voice and data signals for better communication

Explanation

A router is responsible for forwarding data packets between your local network and external networks, such as the Internet. It uses the Internet Protocol (IP) to distinguish between logical networks and ensure proper communication.

A switch is used to connect multiple devices within the same local network, but it does not handle communication with external networks. A router is required to manage data flow between local and external networks.

A DSL splitter is used to separate voice and data signals on a telephone line, which is unrelated to the router's role of managing network communication.

The cable modem is already in place to establish the physical connection to the ISP. However, the modem alone cannot manage data routing between the local network and external networks; this is the router's job.

Related Content

6.1.9 Routers

6.2.14 SOHO Router Configuration

resources\questions\q_routers_03.question.xml

Question 19

Correct

A network administrator is analyzing a connectivity issue between two devices on different networks. The administrator observes the following during troubleshooting:

- The source device successfully sends packets to its default gateway.
- The default gateway forwards the packets to the next router in the path.
- The packets are dropped at an intermediate router, and no response is sent back to the source device.

Based on this information, which of the following is the MOST likely cause of the issue?

- The source device is using an incorrect subnet mask for its IP address configuration.
- The Address Resolution Protocol (ARP) is failing to resolve the MAC address of the destination device.
- The destination device is not running a compatible application protocol.
- The intermediate router does not have a route to the destination network in its routing table. ✓ Correct

Explanation

The Internet Layer is responsible for packet addressing and routing between networks. If an intermediate router does not have a route to the destination network in its routing table, it will drop the packets because it cannot determine where to forward them. This directly aligns with the Internet Layer's function, making this the correct answer.

Question 20 Correct

Which protocol is used to send email messages from a mail client to a mail server?

- SNMP
- IMAP
- POP3
- FTP
- SMTP ✓ Correct

Explanation

SMTP sends email from a mail client to a mail server.

FTP provides a generic method for transferring files.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

POP3 and IMAP are email protocols used by mail clients to retrieve email from a mail server. However, they can't be used to send mail from the client to the server.

Related Content

6.3.6 Well-Known Ports
resources\questions\q_well_known_ports_04.question.xml