6.2.16 Lesson Review

Date: 11/29/2025, 7:55:44 PM

Time Spent: 36:43

Score: 93%

Passing Score: 80%

Question 1 ✓ Correct

Which layer of the TCP/IP model is responsible for putting frames onto the physical network?

- Internet Layer
- Application Layer
- Link or Network Interface Layer ✓ Correct
- Transport Layer

Explanation

The Link or Network Interface Layer is responsible for putting frames onto the physical network. This layer handles communication on a local network segment and uses technologies like Ethernet or Wi-Fi. It also identifies node interfaces using MAC addresses.

The Internet Layer is responsible for packet addressing and routing within a network of networks. It does not deal with frames or physical network communication but instead focuses on forwarding data between different networks using IP addresses.

The Transport Layer manages how hosts handle multiple connections for different application protocols. It ensures reliable or unreliable data delivery using protocols like TCP and UDP, but it does not deal with frames or physical network communication.

The Application Layer contains protocols that perform high-level functions, such as web browsing or email. It operates at a much higher level than the Link Layer and does not interact with the physical network or frames.

Related Content

resources\questions\q_tcp_ip_01.question.xml

Question 2 ✓ Correct

Your Windows workstation has Automatic Private IP Addressing (APIPA) implemented with default settings. Which of the following TCP/IP addresses could you automatically assign to the system should your DHCP server go down or become inaccessible?

- 168.254.10.25
- 10.0.0.65
- 192.168.1.22
- 172.16.1.26
- 169.198.1.23
- 169.254.1.26 ✓ Correct

Explanation

In the event that a DHCP server is not available, Windows workstations can use APIPA to automatically provide themselves with an IP address. The default address range used by APIPA is 169.254.0.1 to 169.254.255.254. Of the options presented, only 169.254.1.26 falls within this range.

Related Content

6.2.12 Static Versus Dynamic Host Address Configuration
resources\questions\q_static_versus_dynamic_host_address_configuration_01.question.xml

Question 3 Correct

Which of the following BEST describes an IP address class?

- The class is the version of the IP addressing standard that the address uses.
- The class defines the type of device that the address is assigned to (server, printer, workstation, etc.).
- The class refers to the range of IP addresses that a DHCP server has been authorized to assign.
- The class defines the IP address's default network address portion. ✓ Correct

Explanation

The address class defines the IP address's default network address portion. For example, a Class A address uses the first octet as the network address and the remaining octets as the available host addresses.

Related Content

6.2.10 Public and Private Addressing

resources\questions\q_public_and_private_addressing_04.question.xml

Question 4 ✓ Correct

Which of the following BEST describes the function of the Application Layer in the TCP/IP model?

- It ensures reliable, connection-oriented forwarding of packets between hosts.
- It is responsible for addressing hosts and routing packets between networks.
- It manages multiple connections for different application layer protocols simultaneously.
- It contains protocols that perform high-level functions, such as configuring and managing network hosts. ✓ Correct

Explanation

The Application Layer is responsible for high-level functions in the TCP/IP model. It includes protocols that allow users to interact with network services, such as web browsing, email, and file transfers.

The Internet Layer handles addressing and routing, ensuring data packets are sent to the correct destination across networks.

Managing multiple connections for different application layer protocols simultaneously is the role of the Transport Layer, which manages multiple connections using protocols like TCP and UDP. It ensures that data from different applications is transmitted correctly and efficiently.

Ensuring reliable, connection-oriented forwarding of packets between hosts is a function of the Transmission Control Protocol (TCP) at the Transport Layer, not the Application Layer. TCP ensures reliable communication by recovering lost or out-of-order packets.

Related Content

resources\questions\q_application_layer_01.question.xml

Question 5 ✓ Correct

An application developer wants to ensure packets arrive at the destination in the correct order and none are lost when an application communicates across the network.

Which protocol will the application developer use?

- ○ UDP
- ○ DNS
- ○ IP
- ◉ TCP ✓ Correct

Explanation

The Transmission Control Protocol (TCP) can identify and recover from lost or out-of-order packets. Failing to receive a packet or incorrectly processing it can cause serious data errors.

The User Datagram Protocol (UDP) is faster than TCP and comes with less of a transmission overhead because it does not need to send extra information to establish reliable connections.

The Internet Protocol (IP) provides packet addressing and routing within a network of networks. For data to travel from one IP network to another, an intermediate system must forward it.

The Domain Name System (DNS) is a service that maps fully qualified domain name labels to IP addresses on most TCP/IP networks, including the internet.

Related Content

resources\questions\q_internet_layer_01.question.xml

Question 6 ✓ Correct

While setting up a home office, a technician disables the DHCP service on the office router but does not want to rely on link-local addressing.

Which of the following IP addressing methods should they use?

- ○ Alternate
- ○ APIPA
- ◉ Static ✓ Correct
- ○ Dynamic

Explanation

Without DCHP, many network hosts assign their own non-routable link-local IP address. To avoid link-local addresses when DHCP addressing is unavailable, you can assign static addresses to all devices that communicate on the local network.

Dynamic addressing automatically assigns IP addresses using DHCP.

Automatic Private IP Addressing (APIPA) is Microsoft's name for auto-configuring link-local addresses.

Alternate IP addressing is a way to assign a second IP address to a host.

Related Content

6.2.12 Static Versus Dynamic Host Address Configuration
resources\questions\q_static_versus_dynamic_host_address_configuration_05.question.xml

Question 7 Correct

What is the primary function of the Link or Network Interface layer in the TCP/IP model?

- To perform high-level functions like web and email services.
- To put frames onto the physical network. ✓ Correct
- To manage multiple connections for different application layer protocols.
- To provide packet addressing and routing within a network of networks.

Explanation

The Link or Network Interface layer is responsible for placing frames onto the physical network. It operates at the local network segment level and handles the encapsulation of data into frames for transmission over Ethernet, Wi-Fi, or other local networking media.

The Internet layer is responsible for addressing and routing packets between different networks, which is beyond the scope of the Link layer's local network operations.

The Transport layer ensures that multiple connections for different application protocols can operate simultaneously. It is unrelated to the Link layer's role in handling frames on the physical network.

The Application layer deals with high-level protocols and services such as HTTP for web browsing and SMTP for email. The Link layer does not handle these types of functions.

Related Content

resources\questions\q_link_or_network_interface_01.question.xml

Question 8

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.

Question 9 Correct

Which of the following IP addresses belong to the 114.0.0.0 Class A network? Assume that the network is indicated by the default Class A portion of the IP address. (Select three.)

- [x] 114.58.12.0 ✓ Correct
- [ ] 115.0.0.66
- [ ] 115.88.0.55
- [x] 114.122.66.12 ✓ Correct
- [ ] 115.77.89.4
- [x] 114.0.0.15 ✓ Correct

Explanation

With a Class A network, the first octet indicates the network address. All hosts on the network must have the same value in the first octet (114).

Related Content

6.2.10 Public and Private Addressing
resources\questions\q_public_and_private_addressing_01.question.xml

Question 10 ✓ Correct

You are troubleshooting a network issue where a computer on your local network cannot communicate with a server on a different network. You suspect the issue lies at the Internet Layer of the TCP/IP model.

After running a packet capture, you notice that the computer is sending packets, but they are not reaching the server.

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

- The application protocol used by the server is not supported by the client.
- The router responsible for forwarding packets to the server is misconfigured. ✓ Correct
- The computer's IP address is not assigned to the correct subnet mask.
- The MAC address of the server is incorrectly configured.

Explanation

The Internet Layer is responsible for packet addressing and routing between networks. If the router, which acts as an intermediate system for forwarding packets, is misconfigured, the packets will not reach their intended destination. This aligns with the Internet Layer's function, making this the correct answer.

The MAC address operates at the Link Layer, not the Internet Layer. While MAC addresses are used for local communication within the same network segment, they are not relevant for routing packets between different networks. Therefore, this is not the correct answer.

Application protocols operate at the Application Layer, which is above the Internet Layer. While mismatched application protocols can cause communication issues, they do not prevent packets from being routed between networks. Therefore, this is not the correct answer.

While an incorrect subnet mask can cause local communication issues, it does not directly impact the Internet Layer's ability to route packets between networks. This issue would more likely manifest at the Link Layer or during local network configuration. Hence, this is not the correct answer.

Related Content

resources\questions\q_internet_layer_03.question.xml

Question 11 ✓ Correct

A company is experiencing issues with its file transfer application. Files are often incomplete or corrupted during transmission, and users report delays when trying to resend the files.

After analyzing the situation, you suspect the issue is related to the Transport Layer protocol being used.

Which protocol is MOST likely causing these issues, and why?

- Transmission Control Protocol (TCP), because it introduces delays due to retransmissions
- Address Resolution Protocol (ARP), because it fails to resolve MAC addresses correctly
- User Datagram Protocol (UDP), because it does not guarantee reliable delivery ✓ Correct
- Internet Protocol (IP), because it cannot handle large file transfers

Explanation

UDP is the correct answer because it is a connectionless, unreliable protocol that does not guarantee the delivery or order of packets. This lack of reliability can lead to incomplete or corrupted files during transmission, as UDP does not retransmit lost packets. While UDP is faster, it is not suitable for applications like file transfers that require data integrity and reliability.

TCP is incorrect because, while it may introduce delays due to its retransmission mechanism, it ensures reliable delivery of data. The issue described in the scenario—corrupted or incomplete files—is not consistent with the behavior of TCP, which is designed to prevent such problems.

IP is incorrect because it operates at the Internet Layer, not the Transport Layer. IP is responsible for addressing and routing packets but does not handle the reliability of data transmission. The issue described in the scenario is related to the Transport Layer, not the Internet Layer.

ARP is incorrect because it operates at the Internet Layer and is used to resolve IP addresses to MAC addresses on a local network. It does not affect the reliability of file transfers or the choice of Transport Layer protocol. The described issue is unrelated to ARP's functionality.

Related Content

resources\questions\q_transport_layer_03.question.xml

Question 12 ✕ Incorrect

Which of the following describes the part of the IPv6 address that identifies the subnet?

- ◉ The first quartet in the IPv6 address prefix ✕ Incorrect
- ○ The IPv6 address interface ID
- ○ The IPv6 address network ID ✓ Correct
- ○ The last quartet in the IPv6 address network ID

Explanation

The IPv6 address network ID identifies the subnet.

For example, in the address FEC0:1319:7700:F631:446A:5511:CC40:25AB, the first 64 bits (FEC0:1319:7700:F631) represent the network ID, and the prefix length identifies the subnet.

Related Content

6.2.15 IPv6 Addressing
resources\questions\q_ipv6_addressing_04.question.xml

Question 13 ✓ Correct

Which of the following components of an IPv4 address will be unique for each network device?

- (●) Host ID ✓ Correct
- ( ) Subnet mask
- ( ) Network ID
- ( ) Network protocol

Explanation

The IPv4 address is split into two components. The host ID is a unique value that will be different for each network device.

The network ID defines the network address. Every network device will have the same network ID.

The subnet mask defines which octets belong to the network ID and which octets belong to the host ID.

The network protocol defines how data is formatted and how network hosts will communicate. It is not a part of the IPv4 address.

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_network_prefixes_03.question.xml

Question 14 ✓ Correct

You are setting up a SOHO router for a small office. The office has multiple devices that need internet access, and you want to ensure that each device receives an IP address automatically without manual configuration.

Additionally, you need to allow remote workers to securely access the office network.

Which of the following configurations should you implement?

- Configure the router to use only public IP addresses for all devices.
- Enable port forwarding for all devices on the network.
- Disable DHCP and assign static IP addresses to all devices manually.
- Enable DHCP on the router and configure a VPN for remote access. ✓ Correct

Explanation

Enabling DHCP allows the router to automatically assign private IP addresses to devices on the local network, simplifying the setup process. Configuring a VPN (Virtual Private Network) ensures that remote workers can securely access the office network over the internet, meeting both requirements of the scenario.

Manually assigning static IP addresses to all devices is time-consuming and prone to errors. It also does not address the need for secure remote access, as no VPN or similar solution is mentioned in this option.

Port forwarding is used to direct specific types of traffic to a particular device on the network, such as hosting a server. It does not automate IP address assignment or provide secure remote access for workers.

Assigning public IP addresses to all devices is not practical or secure in a SOHO environment. Public IPs are limited in availability and expose devices directly to the internet, increasing the risk of unauthorized access. This option also does not address the need for secure remote access.

Related Content

6.1.9 Routers

6.2.14 SOHO Router Configuration

resources\questions\q_soho_router_configuration_02.question.xml

Question 15 Correct

Which of the following are not valid IPv4 addresses? (Select three.)

- [ ] 1.55.254.3
- [x] 45.22.156.256 ✓ Correct
- [ ] 116.0.0.116
- [x] 257.0.122.55 ✓ Correct
- [ ] 122.0.0.0
- [x] 145.8.260.7 ✓ Correct
- [ ] 132.64.32.8

Explanation

IP addresses have a value between 0 and 255 within each octet. In this list, 45.22.156.256, 145.8.260.7, and 257.0.122.55 are not valid IP addresses.

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_03.question.xml