6.3.7 Lesson Review

Date: 11/30/2025, 12:42:57 AM

Time Spent: 09:49

Score: 90%

Passing Score: 80%

Question 1 ✓ 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- The client's application is using an outdated version of the protocol, which does not support the three-way handshake.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 There is no "outdated version" of TCP that lacks this feature.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 2 ✓ Correct

Which of the following best describes the primary reason why Transmission Control Protocol (TCP) is considered a "connection-oriented" protocol?

- It prioritizes speed over reliability, making it suitable for time-sensitive applications like video streaming.
- It assigns random port numbers to ensure that multiple applications can communicate simultaneously.
- It uses encryption to secure data transmissions and prevent unauthorized access.
- It establishes a connection using a three-way handshake and ensures reliable data delivery. ✓ Correct

Explanation

TCP is a "connection-oriented" protocol due to its ability to establish a connection using a three-way handshake (SYN, SYN/ACK, ACK). It ensures reliable data delivery by assigning sequence numbers, allowing acknowledgments (ACK), and retransmitting missing or damaged packets. These features make TCP reliable for applications that cannot tolerate missing or corrupted data.

Encryption is not a defining feature of TCP itself. While some application protocols that use TCP (e.g., HTTPS, SSH) implement encryption, TCP's primary role is to ensure reliable data delivery, not to secure the data. Encryption is an additional layer provided by specific application protocols.

TCP prioritizes reliability over speed. It ensures that all data packets are delivered in the correct order and retransmits missing packets, which introduces overhead and delays. Time-sensitive applications like video streaming typically use UDP, which sacrifices reliability for speed.

While TCP does assign random source port numbers for client communication, this is not the primary reason TCP is considered "connection-oriented." The random port assignment is a feature of the Transport layer but does not define the connection-oriented nature of TCP.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_transmission_control_protocol_02.question.xml

Question 3 ✓ Correct

A company has built a video streaming service that supplies training videos. Quickly transmitting video data to customers is more important than guaranteed delivery.

Which of the following Transport layer IP suite protocols is MOST likely used for this service?

- File Transfer Protocol (FTP)
- Internet Control Message Protocol (ICMP)
- User Datagram Protocol (UDP) ✓ Correct
- Transport Layer Protocol (TCP)

Explanation

User Datagram Protocol (UDP) is a Transport layer protocol that uses a simple connectionless communication model with a minimal protocol mechanism. This makes it suitable for streaming video or sound. Guaranteed data delivery is not as important as fast transmissions.

Transport Layer Protocol (TCP) is a Transport layer protocol that provides reliable, ordered, and error-checked data delivery. Guaranteed data delivery is more important than fast transmissions.

Internet Control Message Protocol (ICMP) is an Internet layer protocol used by network devices, including routers, to send error messages and operational information. For example, ICMP may state that a service is unavailable or a host can't be reached.

File Transfer Protocol (FTP) is an Application layer protocol used to transfer computer files between hosts.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_user_datagram_protocol_03.question.xml

Question 4 ✓ 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

Question 5 Correct

A user configures an email client application and decides to use a TCP/IP suite protocol that stores all messages on the email server so that they can be synchronized across a laptop, a smartphone, and a web email client. In addition, this protocol stores the email messages on the email server until the user explicitly deletes them.

Which of the following TCP/IP port numbers will the client application typically access while using this protocol to contact the email server?

- 21
- 80
- 110
- 143 ✓ Correct

Explanation

The TCP/IP suite protocol that stores email messages on a server so they can be synchronized across multiple devices is Internet Message Access Protocol (IMAP). IMAP typically uses port 143.

FTP uses port 21.

HTTP uses port 80.

POP3 uses port 110.

Related Content

6.3.6 Well-Known Ports
resources\questions\q_well_known_ports_05.question.xml

Question 6 ✕ Incorrect

You've just installed the DNS service on a Windows server. Which port must be opened on the server's firewall to allow clients to access the service?

- ◯ 123
- ◯ 110
- ◯ 53 ✓ Correct
- ◯ 143

Explanation

The DNS service runs on port 53 by default.

POP3 uses port 110.

IMAP uses port 143.

NTP uses port 123.

Related Content

6.3.6 Well-Known Ports
resources\questions\q_well_known_ports_01.question.xml

Question 7 ✓ Correct

Which of the following scenarios best demonstrates the appropriate use of the User Datagram Protocol (UDP)?

- (●) A video streaming service that prioritizes speed over guaranteed delivery of every data packet. ✓ Correct
- ( ) A file transfer process where missing packets would result in corrupted files.
- ( ) A remote server login session requiring authentication and reliable data transmission.
- ( ) A secure online banking transaction requiring encryption and acknowledgment of data delivery.

Explanation

UDP is a connectionless protocol that prioritizes speed over reliability. It is suitable for applications like video streaming, where occasional missing or out-of-order packets manifest as minor glitches rather than critical errors. This makes UDP ideal for time-sensitive data transmission, where speed is more important than ensuring every packet is delivered.

Online banking requires a reliable, connection-oriented protocol like TCP. Online banking transactions cannot tolerate missing or corrupted packets, as they could compromise data integrity and security. UDP is not suitable for such applications.

File transfers require all data packets to be delivered accurately and in order. Missing packets would corrupt the file, making TCP the appropriate protocol for this scenario. UDP does not guarantee delivery or sequencing, so it is not suitable here.

Remote server login sessions, such as those using Secure Shell (SSH), require reliable data transmission and encryption to ensure secure communication. TCP is used in such cases because it provides acknowledgment and sequencing, which UDP lacks.

Related Content

6.3.2 Transmission Control Protocol

6.3.4 User Datagram Protocol

resources\questions\q_user_datagram_protocol_04.question.xml

Question 8 ✓ 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 9 Correct

Why does the Transport layer use port numbers in network communication?

- (●) To distinguish between applications communicating on the same device ✓ Correct
- ( ) To encrypt data for secure transmission
- ( ) To identify the physical address of the destination device
- ( ) To ensure data is routed to the correct network

Explanation

The Transport layer uses port numbers to identify and distinguish between multiple applications running on the same device. For example, a device might be running a web browser (using port 80 for HTTP) and an email client (using port 25 for SMTP) simultaneously. Port numbers ensure that data is delivered to the correct application.

Identifying the physical address (e.g., MAC address) is the responsibility of the Link layer, not the Transport layer. The Transport layer focuses on managing communication between applications, not physical devices.

Routing data to the correct network is the responsibility of the Internet layer, which uses IP addresses for this purpose. The Transport layer works at a higher level, focusing on application-specific communication.

Encryption is not a function of the Transport layer. While some protocols that operate at the Transport layer (e.g., HTTPS) use encryption, the encryption itself is handled by the application layer or security protocols, not by the Transport layer.

Related Content

resources\questions\q_protocols_and_ports_02.question.xml

Question 10 ✓ Correct

Which layer of the TCP/IP protocol stack is responsible for assigning port numbers to network applications?

- (●) Transport Layer ✓ Correct
- ( ) Internet Layer
- ( ) Application Layer
- ( ) Link Layer

Explanation

The Transport layer is responsible for assigning port numbers to network applications. This layer ensures that data is sent and received by the correct application by using port numbers, which range from 0 to 65535. For example, HTTP uses port 80, and email services like SMTP use port 25.

The Link layer is responsible for moving frames of data between hosts using MAC addresses. It does not deal with port numbers or application-level communication. This layer operates at a lower level than the Transport layer and is concerned with physical and data link communication.

The Internet layer is responsible for addressing and routing data packets across networks using IP addresses. It does not assign port numbers, as its primary function is to ensure packets are delivered to the correct host, not the correct application.

The Application layer is where network applications operate, such as web browsers or email clients. While applications use port numbers to communicate, the actual assignment and management of port numbers are handled by the Transport layer, not the Application layer.

Related Content

resources\questions\q_protocols_and_ports_01.question.xml