

TCP Handshake Handout

The TCP (Transmission Control Protocol) handshake, also known as the three-way handshake, is a crucial process in establishing a reliable connection between two devices over a network. It is the foundation of TCP's reliability, error-checking, and sequencing mechanisms. The TCP handshake consists of three steps, and it works as follows:

Step 1: SYN (Synchronize)

1. The process starts with the initiating device, often referred to as the client, sending a TCP packet with the SYN (synchronize) flag set to the target device, which is the server. This packet is also known as the SYN packet.
2. The client randomly selects an initial sequence number (ISN) for the connection and includes it in the SYN packet.
3. The server receives the SYN packet and responds by sending its own TCP packet back to the client. This packet is known as the SYN-ACK packet.
4. The server selects its own initial sequence number (ISN) and acknowledges the client's sequence number. The server also sets the SYN and ACK flags in the packet.

Step 2: SYN-ACK (Synchronize-Acknowledge)

5. The client receives the SYN-ACK packet from the server. It acknowledges the server's ISN by incrementing it by 1 and sends back an ACK packet.
6. The client sets the ACK flag in the packet and increments its own sequence number by 1.

Step 3: ACK (Acknowledge)

7. The server receives the ACK packet from the client. It acknowledges the client's ISN by incrementing it by 1.
8. The client has now received an acknowledgment of its SYN packet from the server, and the connection is established. Both devices can start sending data to each other, and the communication is considered reliable.

The TCP handshake is complete, and both the client and server know that the other party is ready to communicate. This process ensures that both devices are in sync and ready to exchange data. The initial sequence numbers (ISNs) are used to order and verify the data exchanged during the session, making TCP a reliable and connection-oriented protocol.

The handshake process also serves as a form of error checking, as it verifies that both parties are reachable and responsive. If any of the steps fail or a packet is lost, the connection is not established, and the devices will retry the handshake until a successful connection is achieved.