TCS 332, Fundamental of Information Security and Blockchain

B. Tech CSE III Semester

Topic: TCP 3 way handshake

Instructor:

Dr Mohammad Wazid

Professor, Department of CSE

Graphic Era (Deemed to be University), Dehradun, India

Email: wazidkec2005@gmail.com

Homepage: https://sites.google.com/site/mwazidiiith/home

Topic: TCP 3 way handshake

Transmission Control Protocol (TCP)

- Transmission Control Protocol (TCP) is a connection-oriented communications protocol that facilitates the exchange of messages between computing devices in a network.
- It is the most common protocol in networks which is used for connection oriented and reliable network service.
- TCP takes messages from an application/server and divides them into packets, which can then be forwarded by the devices in the network for example, routers, security gateways to the destination.

Transmission Control Protocol (TCP)

- For example, when an email (using SMTP) is sent from an email server, the TCP layer in that server will divide the message **into multiple packets, number them and then forward them to the IP layer for transport**.
- At the IP layer, each packet will be transported to the destination email server.
- While each packet is going to the same place, the route they take to get there may be different.
- When it arrives, the IP layer hands it back to the TCP layer, which reassembles the packets (by the help of assigned number) into the message.

Transmission Control Protocol (TCP)

- In TCP/IP sender sends messages to receiver via a network of routers.
- But there are certain limitation related to the size of those messages.
- It is because of the physical limitations of the internet's infrastructure (i.e., **available bandwidth limitation**).
- That’s why computers split those messages into multiple small packets.
- Many things could go wrong once a single message is divided into multiple packets.

Transmission Control Protocol (TCP)

- For example,

- Packets can be lost, due to problems in the physical layer or in routers' forwarding tables.

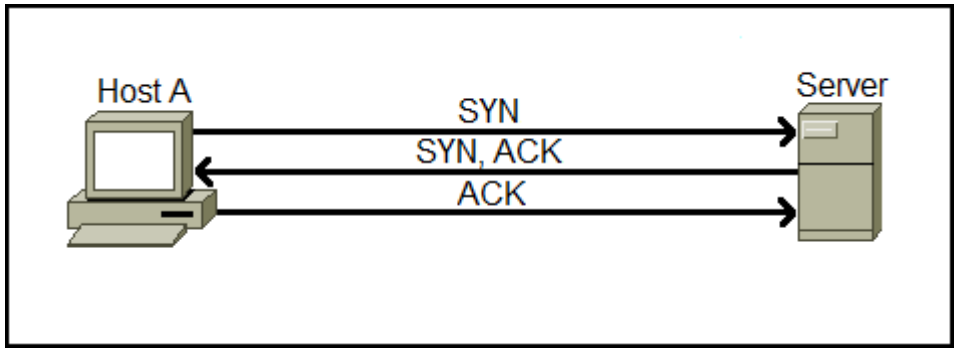
- Packets can arrive out of order. That can happen especially if two packets follow different paths to the destination.

- A computer might send multiple messages to a destination, and the destination needs to identify which packet belongs to which message.

- TCP is used to recover from such kind of problems. TCP is always used alongside the IP in order to ensure reliable transmission of packets.

TCP three-way handshake

- Since TCP is a connection-oriented protocol, a connection needs to be established before two devices can communicate.
- TCP uses a process called three-way handshake to negotiate the sequence and acknowledgment fields and start the session. A graphical representation of the process is as follows:



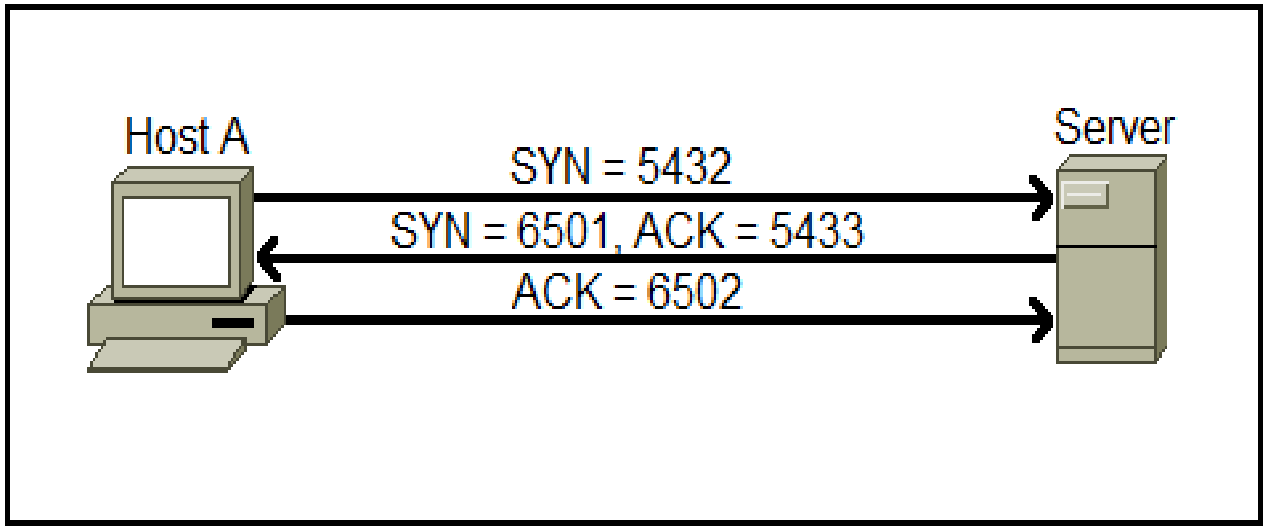
- As the name implies, the three way handshake process consists of three steps:

TCP three-way handshake

- **Host A** initiates the connection by sending the TCP SYN packet to the destination host.
- The packet contains the random sequence number (e.g. 5432) which marks the beginning of the sequence numbers for data that the Host A will transmit.
- The **Server** receives the packet and responds with its own sequence number. The response also includes the acknowledgment number, which is Host A's sequence number incremented by 1 (in our case, that would be 5433).
- Host A acknowledges the response of the Server by sending the acknowledgment number, which is the Server's sequence number incremented by 1.

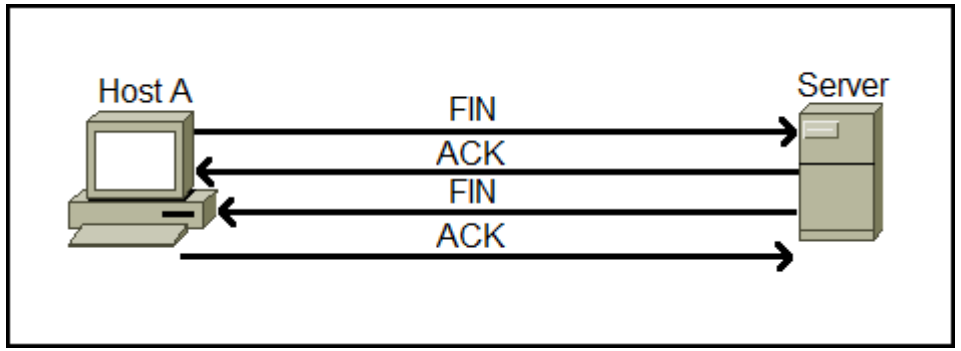
TCP three-way handshake

- For example,



TCP three-way handshake

- After the data transmission process is finished, TCP will terminate the connection between two endpoints.
- This four-step process is illustrated below:



TCP three-way handshake

- The client application that wants to close the connection sends a TCP segment with the FIN (Finished) flag set to 1.
- The server receives the TCP segment and acknowledges it with the ACK segment.
- Server sends its own TCP segment with the FIN flag set to 1 to the client in order to terminate the connection.
- The client acknowledges the server’s FIN segment and closes the connection.

List of TCP flags (there are six types)

- Each TCP flag corresponds to 1 bit in size. The list below describes each flag:
- SYN-The SYN, or Synchronization flag, is used as a first step in establishing a 3-way handshake between two hosts. Only the first packet from both the sender and receiver should have this flag set.
- ACK-The ACK flag, which stands for "Acknowledgment", is used to acknowledge the successful receipt of a packet.
- FIN-The FIN flag, which stands for "Finished", means there is no more data from the sender. Therefore, it is used in the last packet sent from the sender.

List of TCP flags (there are six types)

- URG-The URG flag is used to notify the receiver to process the urgent packets before processing all other packets. The receiver will be notified when all known urgent data has been received.
- PSH-The PSH flag, which stands for "Push", is somewhat similar to the URG flag and tells the receiver to process these packets as they are received instead of buffering them.
- RST-The RST flag, which stands for "Reset". It is used for connection reset purpose.

References

2. Data Communications and Networking Textbook by Behrouz A. Forouzan