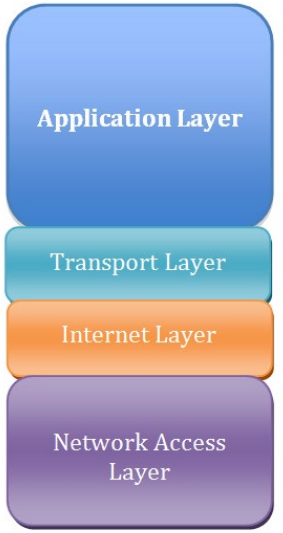
Attacks on TCP

(Some slides based on SEED LAB)

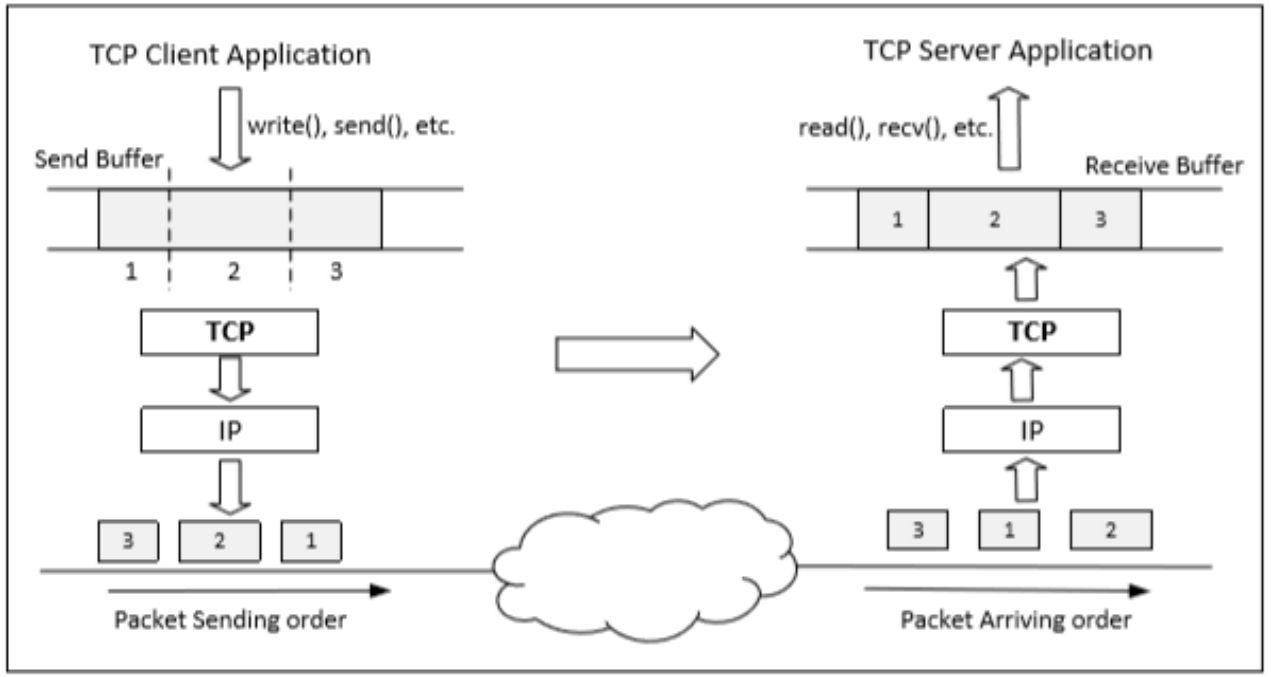
TCP



- Transmission Control Protocol (TCP) is a core protocol of the Internet protocol suite.
- Sits on the top of the IP layer; transport layer.
- Provide host-to-host communication services for applications.
- Two transport Layer protocols
  - **TCP**: provides a reliable and ordered communication channel between applications.
  - **UDP**: lightweight protocol with lower overhead and can be used for applications that do not require reliability or communication order.

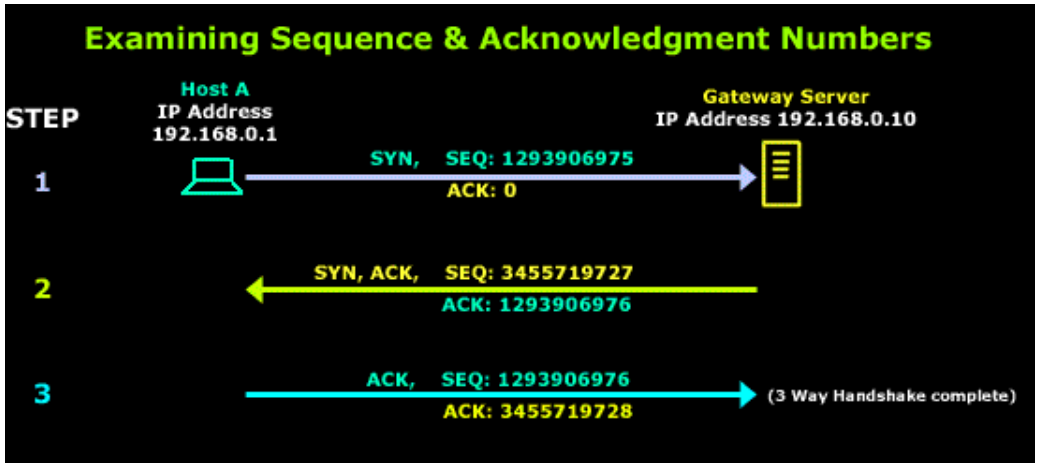
Data Transmission over TCP

- Maintaining the order
  - Packets are arrived at the same order as they sent.
- Reliability
  - Can detect a packet is lost.
- Flow Control
  - The sender and receiver will work at almost the same rate.



The data will be in send buffer until when it is decided that it can be sent. Depending on time (time-out happened), size (enough data is given)

Sequence/Ackonowledgment Number



Send Buffer

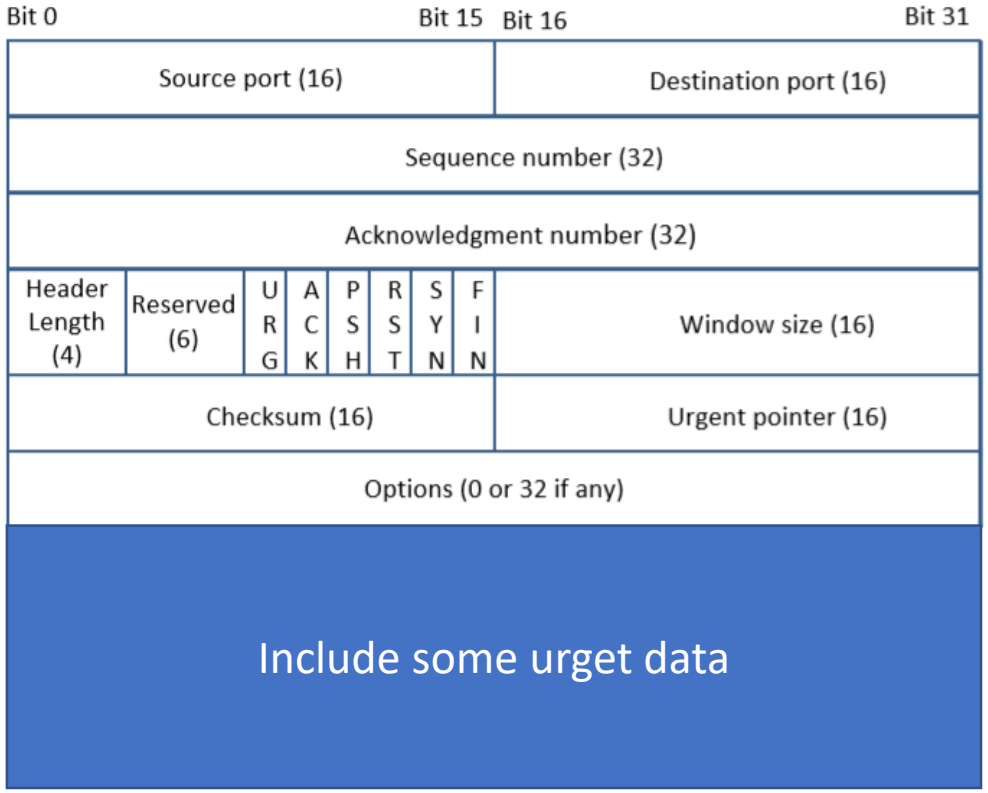
Receive Buffer

Receive Buffer

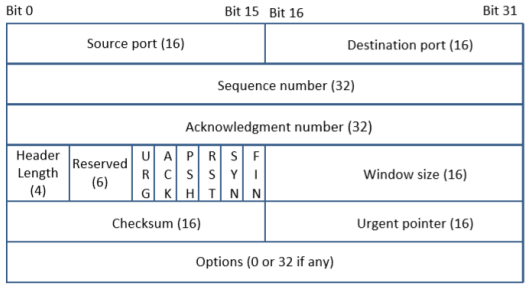
Send Buffer

TCP header

- Ack Number: Only valid if ACK flag is set.
- Window Size: Window advertisement.
- Urgent Pointer: If URG flag is set, the first part of data is urgent. The urgent pointer, points to the end of that data.



TCP 3-way Handshake Protocol



SYN Packet

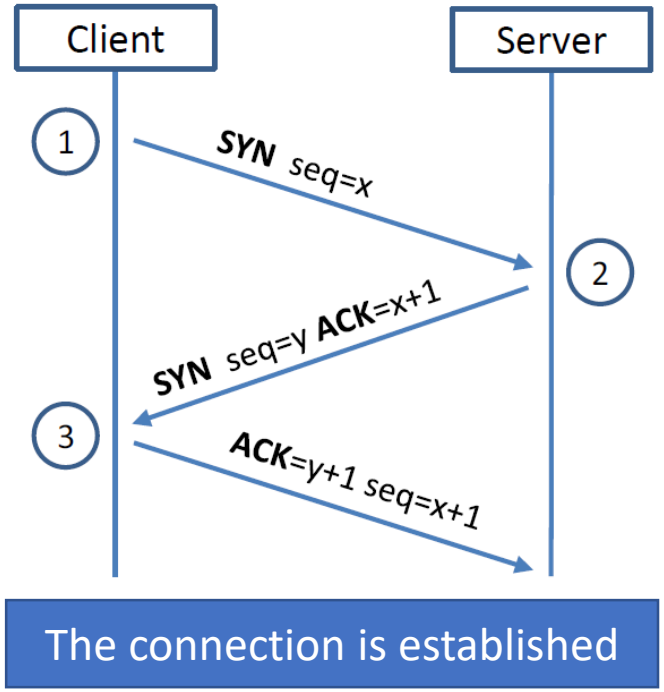
- The client sends a special packet called SYN packet to the server using a randomly generated number x as its sequence number.

SYN-ACK Packet

- On receiving it, the server sends a reply packet using its own randomly generated number y as its sequence number.

ACK Packet

- Client sends out ACK packet to conclude the handshake



What about future packets?

Client increments its SEQ number based on the number of bytes sent

Client increments its ACK number based on the number of bytes received