

Transport Layer

- Responsible for logical communications between apps running on hosts:

- (1) Tracking individual conversations
- (2) Segmenting data / Reassembling segments
- (3) Adds header info
- (4) Identify, manage and separate multiple conversations
- (5) Uses segmentation and multiplexing
(for different communications to be interleaved on network)

IP: unreliable, best effort delivery

Layer 4 protocols: (1) TCP (2) UDP

Transmission Control Protocol (TCP)

- Provides reliability and flow control / Connection-oriented

Basic Operations

- (1) Number / Track data segments transmitted to a certain host from a specific app
- (2) Acknowledge received data
- (3) Retransmit any unacknowledged data after a certain amount of time
- (4) Sequence data in the right order
- (5) Efficient rate of sending data acceptable by receiver

User Datagram Protocol (UDP)

- Very little overhead / data checking : Connectionless
Best-effort delivery

TCP Overview

- Features :
- (1) Establishes a session
 - (2) Ensures Reliable Delivery
 - (3) Provides Same-Order Delivery
 - (4) Supports Flow Control

- Stateful / Connection-Oriented Protocol

TCP Header Length = 20 Bytes



(1) Source Port	= 16 bits
(2) Destination Port	= 16 bits
(3) Sequence Number	= 32 bits
(4) Acknowledgement Number	= 32 bits
(5) Header Length	= 4 bits
(6) Reserved	= 6 bits
(7) Control Bits	= 6 bits
(8) Window	= 16 bits
(9) Checksum	= 16 bits
(10) Urgent	= 16 bits

Total = 160 bits

Applications that use TCP

- (1) HTTP
- (2) FTP
- (3) SMTP
- (4) SSH

Applications that use UDP

- (1) DHCP
- (2) DNS
- (3) SNMP
- (4) TFTP
- (5) VoIP

UDP Overview

(6) Video Conferencing

UDP Header Length = 8 Bytes * Layer 4 protocols use port numbers to manage multiple, simultaneous conversations.

- (1) Source Port = 16 bits
- (2) Destination Port = 16 bits
- (3) Length = 16 bits
- (4) Checksum = 16 bits

Total = 64 bits

Socket Pairs

- Combination of source IP / Port number or destination IP / Port number

E.g. 192.168.1.1:80
172.16.0.254:443

* Sockets enable multiple processes running on a client

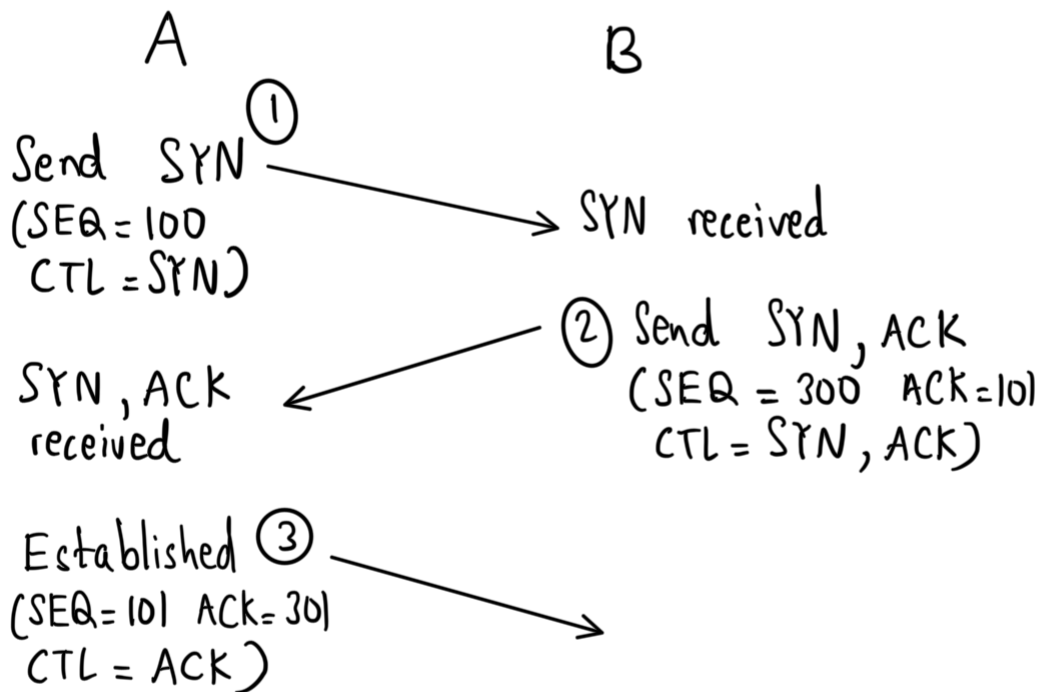
Port Number Groups : (1) Well-known (0 to 1023)
(2) Registered (1024 to 49,151)
(3) Private / Dynamic (49,152 to 65,535)

Port	Protocol	Application
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	FTP - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP	Domain Name System (DNS)
	TCP	
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server

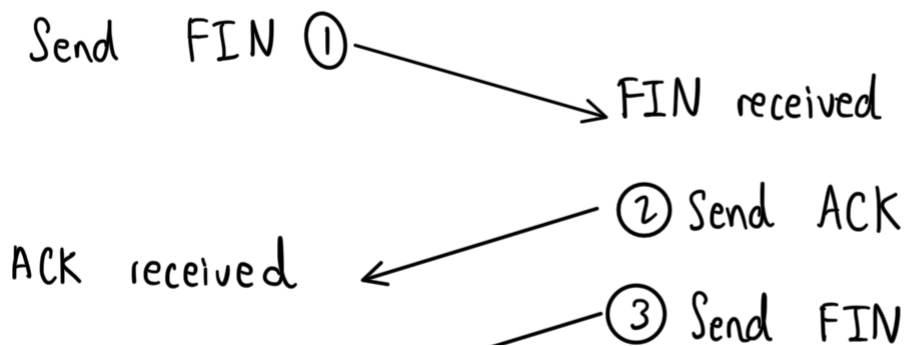
68	UDP	DHCP - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

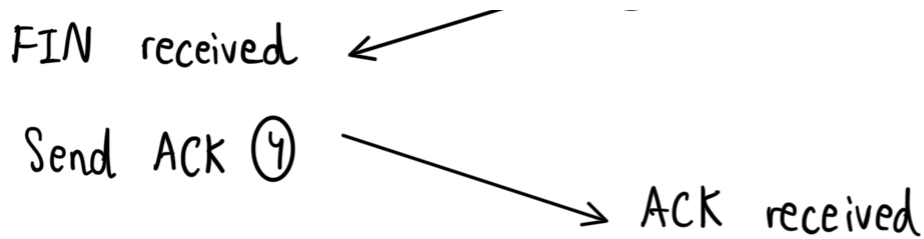
* An individual server cannot have 2 services assigned to the same port number

TCP Connection Establishment (3-way handshake)



Session Termination





3-way Handshake Analysis

Six control bit flags :

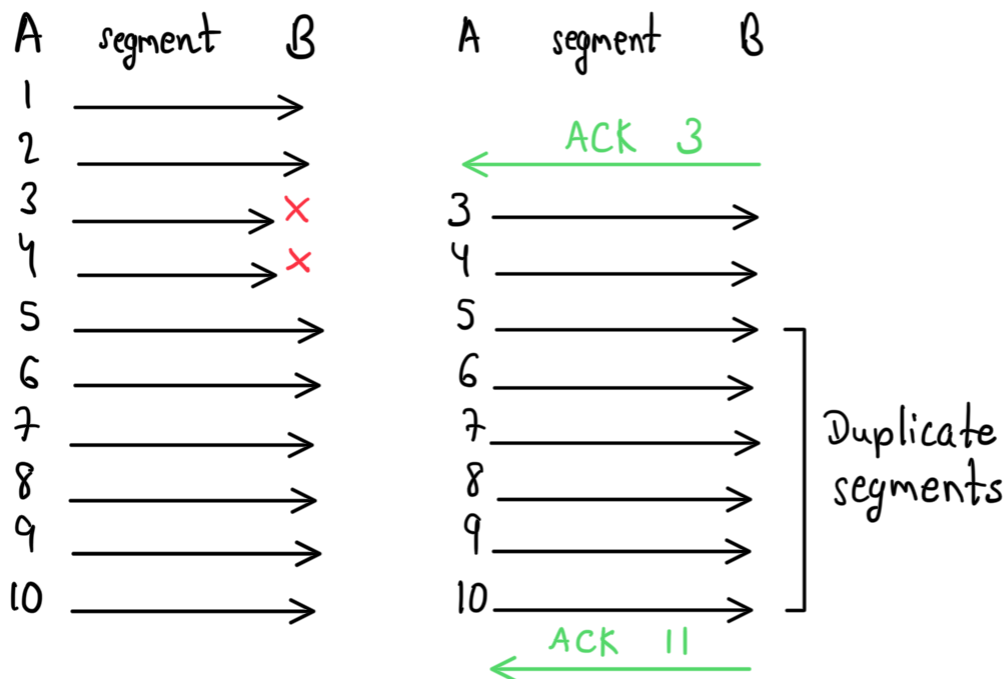
- (1) URG
- (2) ACK
- (3) PSH
- (4) RST
- (5) SYN
- (6) FIN

Reliability and Flow Control

- TCP maintain the flow of packets
- all data must be received
- the segments must be reassembled into the original order

* Different segments may take different routes

TCP Reliability - Data Loss and Retransmission



An optional TCP feature : Selective Acknowledgement (SACK)

- Can explicitly acknowledge segments
- No duplicate segments