

Chapter 04:

TCP/IP Protocol suite

A series of horizontal lines in teal and light blue colors, with varying lengths and slight offsets, creating a modern, layered effect across the width of the slide.

TCP & UDP

Overview

- IP key characteristics ?
 - *Connectionless, Unreliable and Unacknowledged.*
- Fixing this problem: let the network layer (IP) take care of basic data movement on the internetwork, and define two protocols at the transport layer.

TCP vs. UDP

- The *Transmission Control Protocol (TCP)* is a full-featured, connection-oriented protocol that provides acknowledged delivery of data while managing traffic flow and handling issues such as congestion and transmission loss.
- The *User Datagram Protocol (UDP)* is a much simpler protocol that concentrates only on delivering data, to maximize the speed of communication when the features of TCP are not required.

Applications of TCP & UDP

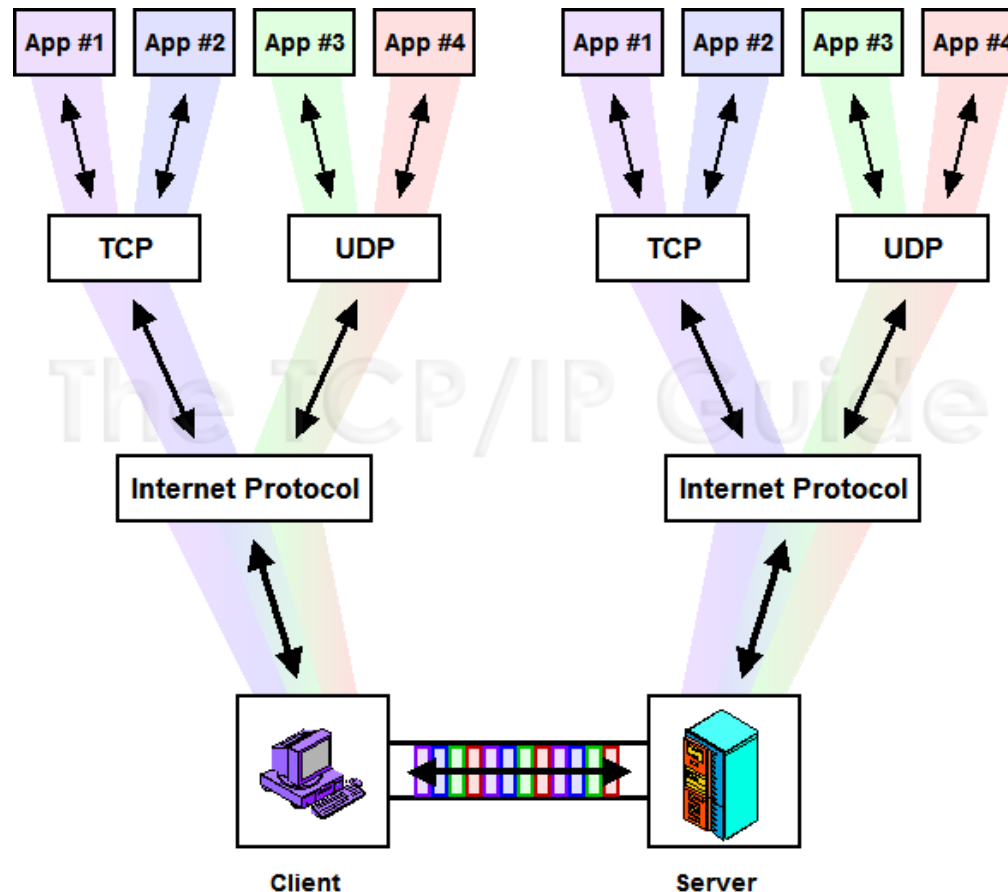
- **TCP Applications:**

- Most “typical” applications need the reliability and other services provided by TCP, and don't care about loss of a small amount of performance to overhead (HTTP, FTP, SMTP...)

- **UDP Applications:**

- The application doesn't really care if some of the data gets lost (streaming video or multimedia)
- Applications that send very small amounts of data.

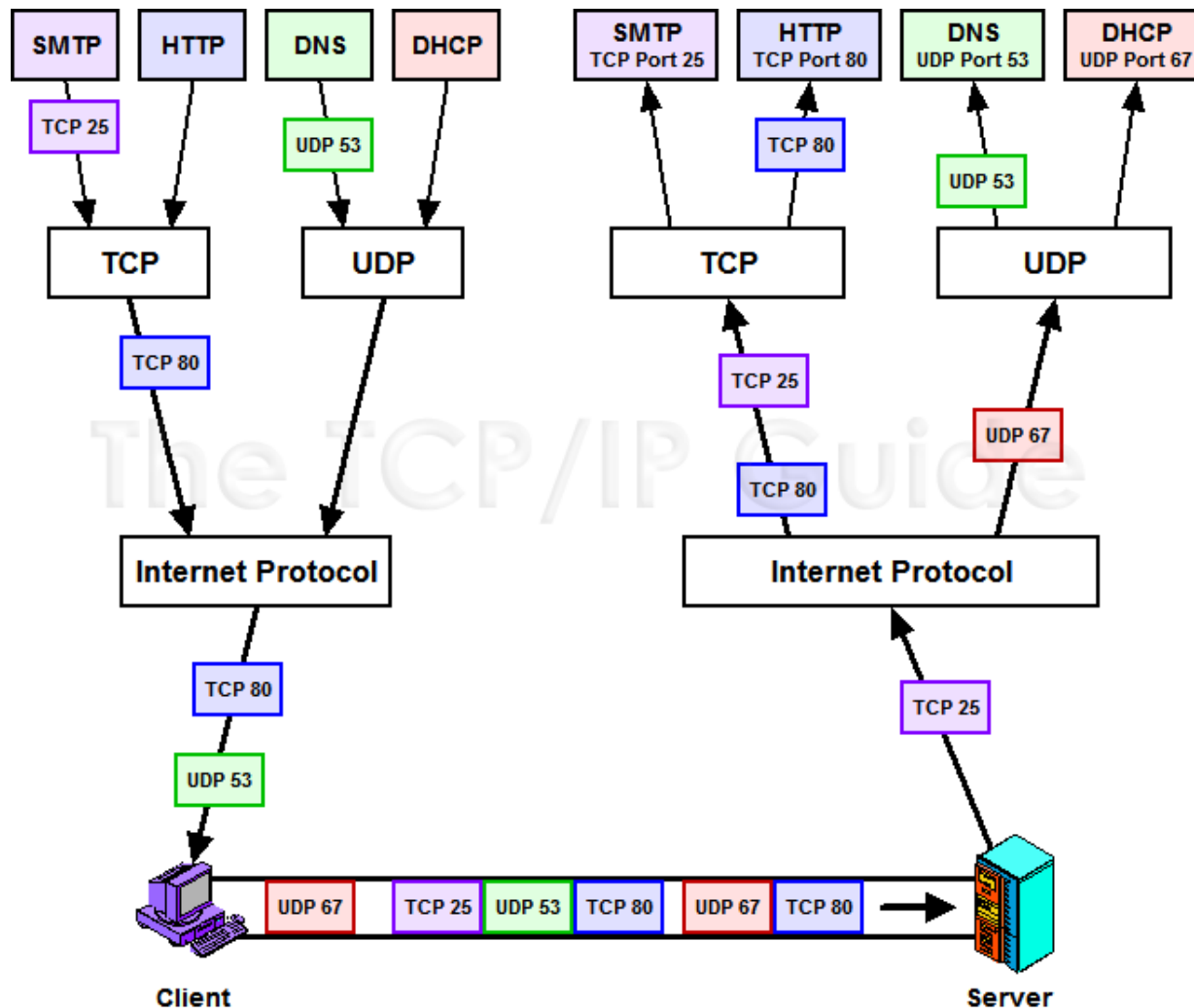
Multiplexing & Demultiplexing in TCP/IP



Transport Layer Addressing

- TCP/IP transport layer addressing is accomplished using TCP and UDP *ports*. Each port number within a particular IP device identifies a particular software process.
- TCP and UDP port numbers are 16 bits → values from 0 to 65,535.
- There are Source Ports and Destination Ports.

Source Ports and Destination Ports



TCP & UDP Port Number Ranges

Port Range Name	Port Number Range	Description
Well-Known (Privileged) Port Numbers	0 to 1,023	These port numbers are managed by IANA and reserved for only the most universal TCP/IP applications such as Web servers, FTP servers... http: 80, ftp: 21, DNS: 53, Telnet: 23
Registered (User) Port Numbers	1,024 to 49,151	To ensure that these various applications do not conflict with each other, IANA uses the bulk of the overall port number range for registered port numbers
Private/Dynamic Port Numbers	49,152 to 65,535	These ports are neither reserved nor maintained by IANA. They can be used for any purpose without registration, so they are appropriate for a private protocol used only by a particular organization

Ephemeral Ports

Client/Server applications:

- Server processes listens on port in well-known or registered port numbers range. They are used as the destination port number in requests sent by clients.
- Client processes don't use well-known or registered ports. Instead, each client process is assigned a temporary port number for its use. This is commonly called an *ephemeral port number*.

TCP/IP Sockets

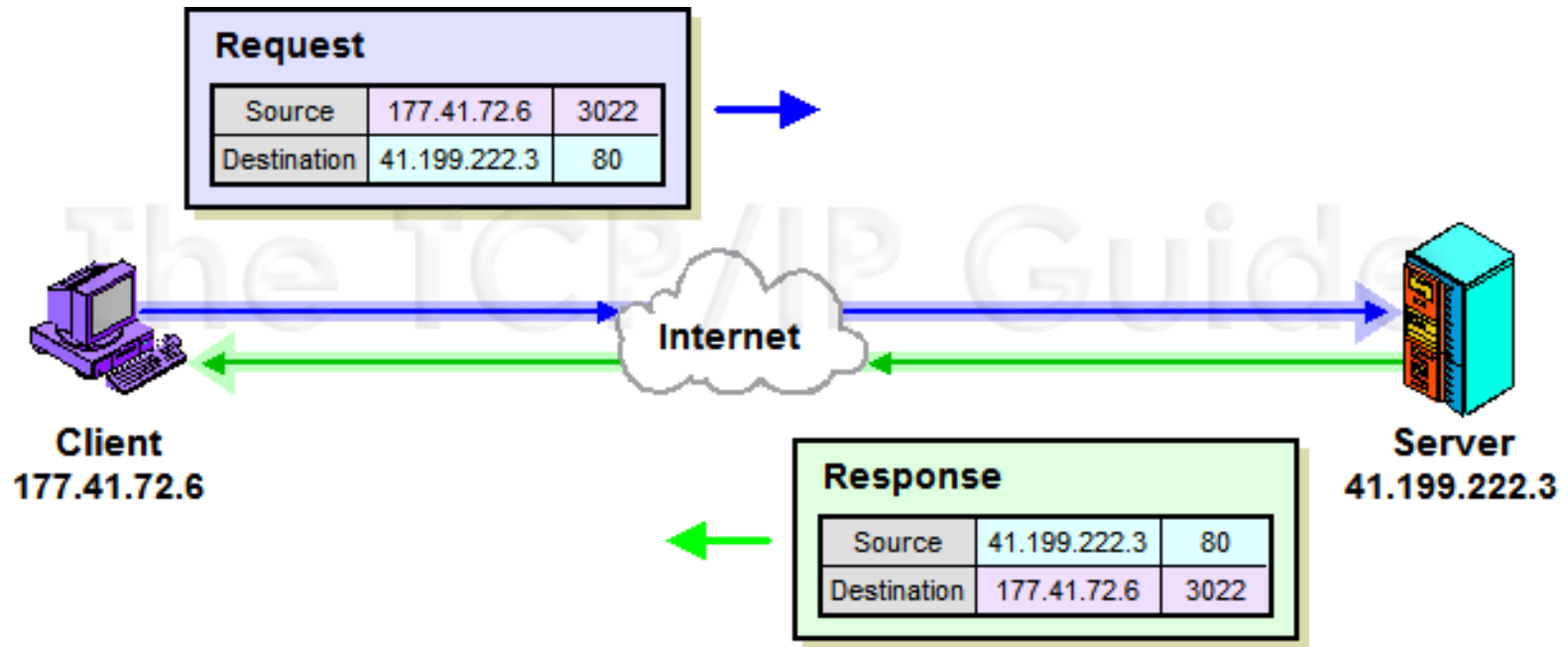
- The overall identifier of a TCP/IP application process on a device is the combination of its IP address and port number, which is called a *socket*.

<Host Name>:<Port Number>

Ex: <http://10.0.0.1:3128>

- This API for Windows is called *Windows Sockets* or *WinSock*

Client/Server Application Port use



Socket Pair: (41.199.222.3:80, 177.41.72.6:3022)

Common TCP/IP Well-Known Port Numbers

Port #	TCP / UDP	Keyword	Protocol Abbreviation	Application or Protocol Name / Comments
7	TCP + UDP	echo	—	Echo Protocol
9	TCP + UDP	discard	—	Discard Protocol
11	TCP + UDP	systat	—	Active Users Protocol
13	TCP + UDP	daytime	—	Daytime Protocol
17	TCP + UDP	qotd	QOTD	Quote Of The Day Protocol
19	TCP + UDP	chargen	—	Character Generator Protocol
20	TCP	ftp-data	FTP (data)	File Transfer Protocol (default data port)
21	TCP	ftp	FTP (control)	File Transfer Protocol (control / commands)
23	TCP	telnet	—	Telnet Protocol
25	TCP	smtp	SMTP	Simple Mail Transfer Protocol
43	TCP	nicname	—	Whois Protocol (also called “Nickname”)

Common TCP/IP Well-Known Port Numbers

Port #	TCP / UDP	Keyword	Protocol Abbreviation	Application or Protocol Name / Comments
53	TCP + UDP	domain	DNS	Domain Name Server (Domain Name System)
67	UDP	bootps	BOOTP / DHCP	Bootstrap Protocol / Dynamic Host Configuration Protocol (Server)
68	UDP	bootpc	BOOTP / DHCP	Bootstrap Protocol / Dynamic Host Configuration Protocol (Client)
69	UDP	tftp	TFTP	Trivial File Transfer Protocol
80	TCP	http	HTTP	Hypertext Transfer Protocol (World Wide Web)
110	TCP	pop3	POP	Post Office Protocol (version 3)
119	TCP	nntp	NNTP	Network News Transfer Protocol
123	UDP	ntp	NTP	Network Time Protocol
143	TCP	imap	IMAP	Internet Message Access Protocol
161	UDP	snmp	SNMP	Simple Network Management Protocol
194	TCP	irc	IRC	Internet Relay Chat
443	TCP	https	HTTP over SSL	Hypertext Transfer Protocol over Secure Sockets Layer
500	UDP	isakmp	IKE	IPSec Internet Key Exchange
520	UDP	router	RIP	Routing Information Protocol (RIP-1 and RIP-2)

User Datagram Protocol (UDP)

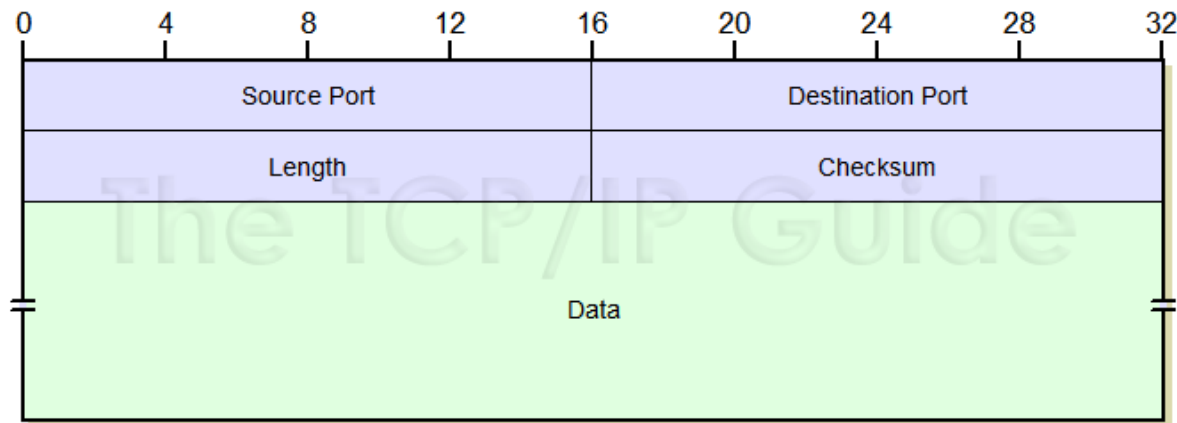
The User Datagram Protocol (UDP) was developed for use by application protocols that do not require reliability, acknowledgment or flow control features at the transport layer.

UDP does not

- Establish connections before sending data,
- Provide acknowledgments to show that data was received,
- Provide any guarantees that its messages will arrive.
- Detect lost messages and retransmit them,
- Ensure that data is received in the same order that they were sent,
- Provide any mechanism to manage the flow of data between devices, or handle congestion.

UDP Message format

- 8 bytes long



- Length: The length of the entire UDP datagram, including both header and *Data* fields.
- Checksum: An optional 16-bit checksum computed over the entire UDP datagram

Common UDP Applications and Server Port Assignments

Port #	Keyword	Protocol	Comments
53	domain	Domain Name Server (DNS)	Uses a simple request/reply messaging system for most exchanges
67 and 68	bootps / bootpc	Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP)	Host configuration protocols that consist of short request and reply exchanges.
69	tftp	Trivial File Transfer Protocol (TFTP)	TFTP is designed for the quick and easy transfer of small files. It includes simple versions of some of TCP's features, such as acknowledgments, to avoid file corruption.
161 and 162	snmp	Simple Network Management Protocol	An administrative protocol that uses relatively short messages.
2049	nfs	Network File System	A file sharing protocol was originally designed to use UDP for performance reasons.

Transmission Control Protocol (TCP)

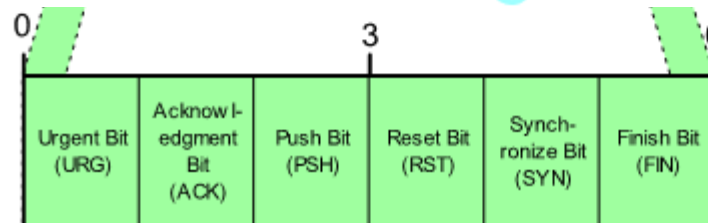
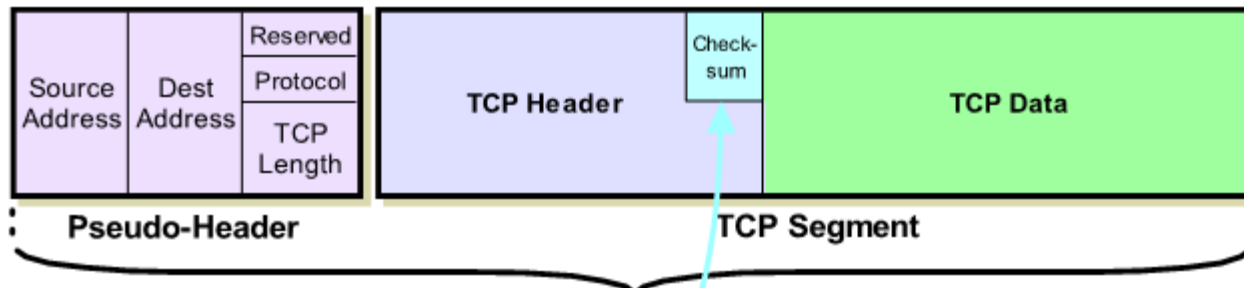
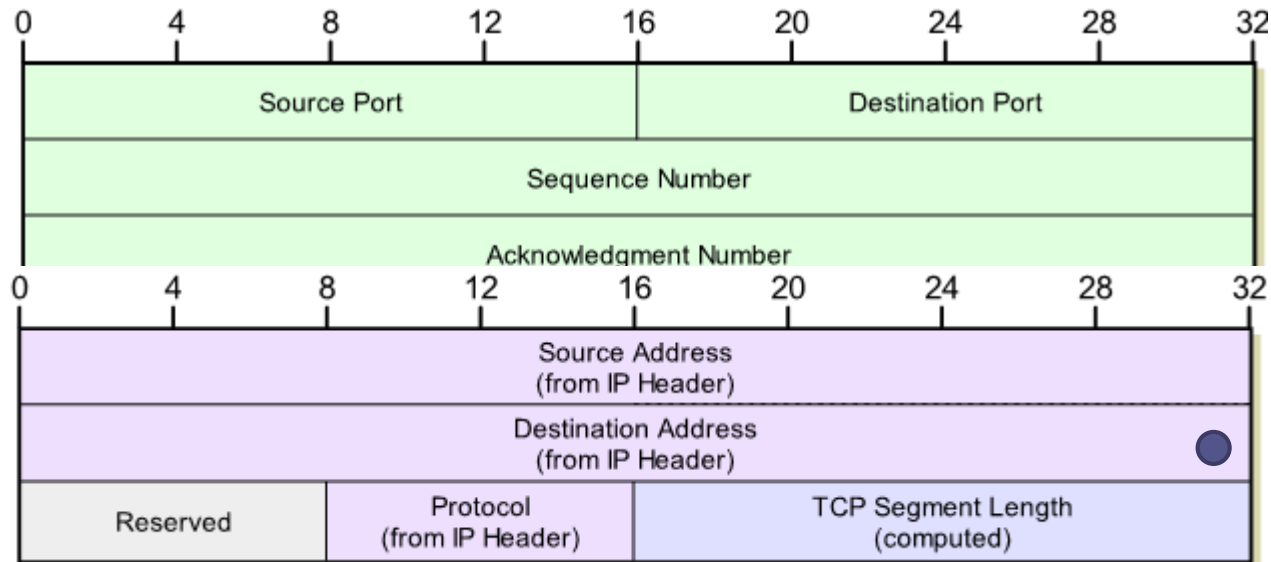
TCP Functions

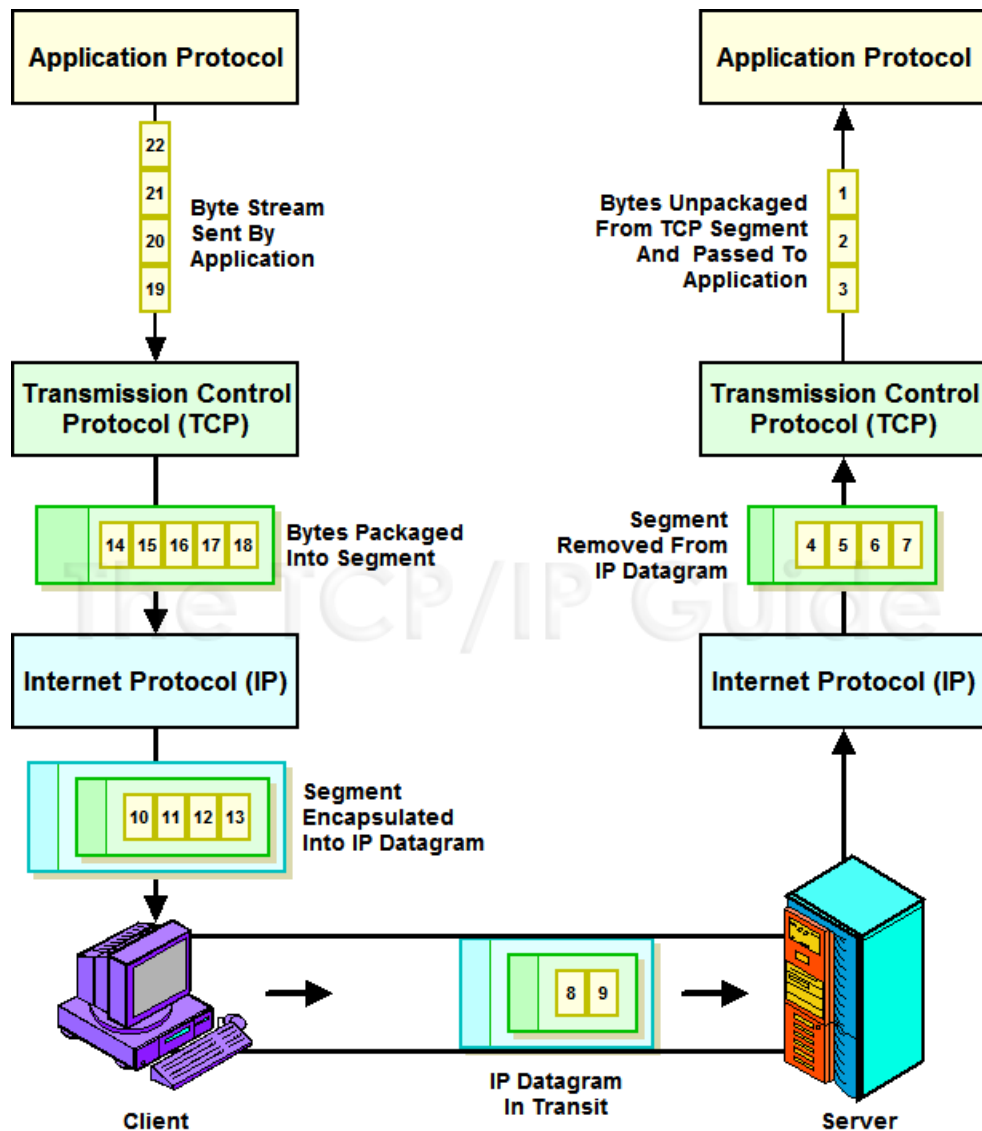
- Addressing/Multiplexing
- Connection Establishment, Management and Termination
- Data Handling and Packaging
- Data Transfer
- Providing Reliability and Transmission Quality Services
- Providing Flow Control and Congestion Avoidance Features

TCP Characteristics

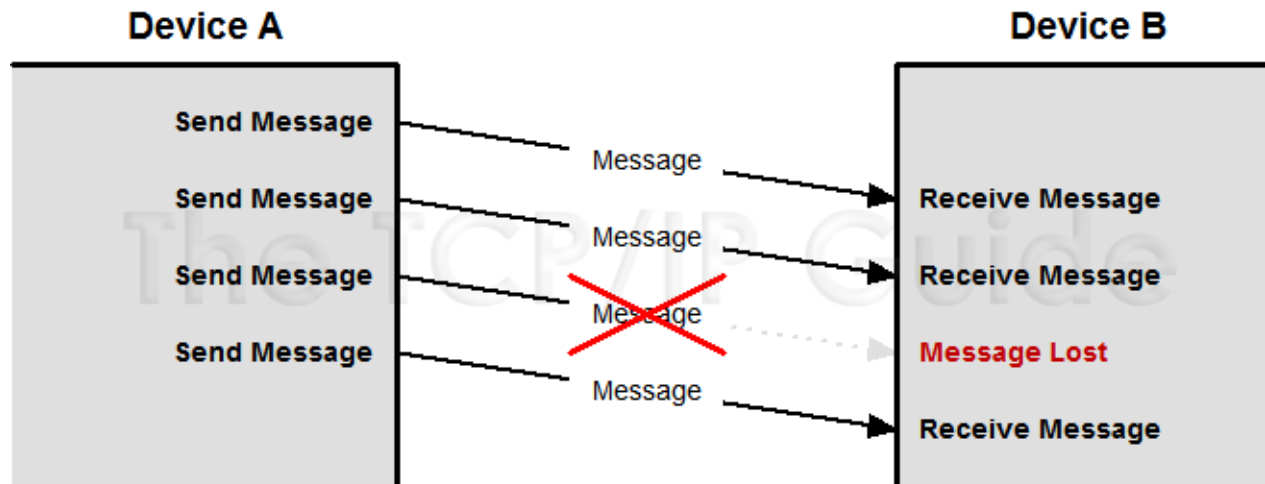
- Connection-oriented,
- Bidirectional,
- Reliable,
- Acknowledged,
- Stream-oriented,
- Flow-managed.

TCP Message format

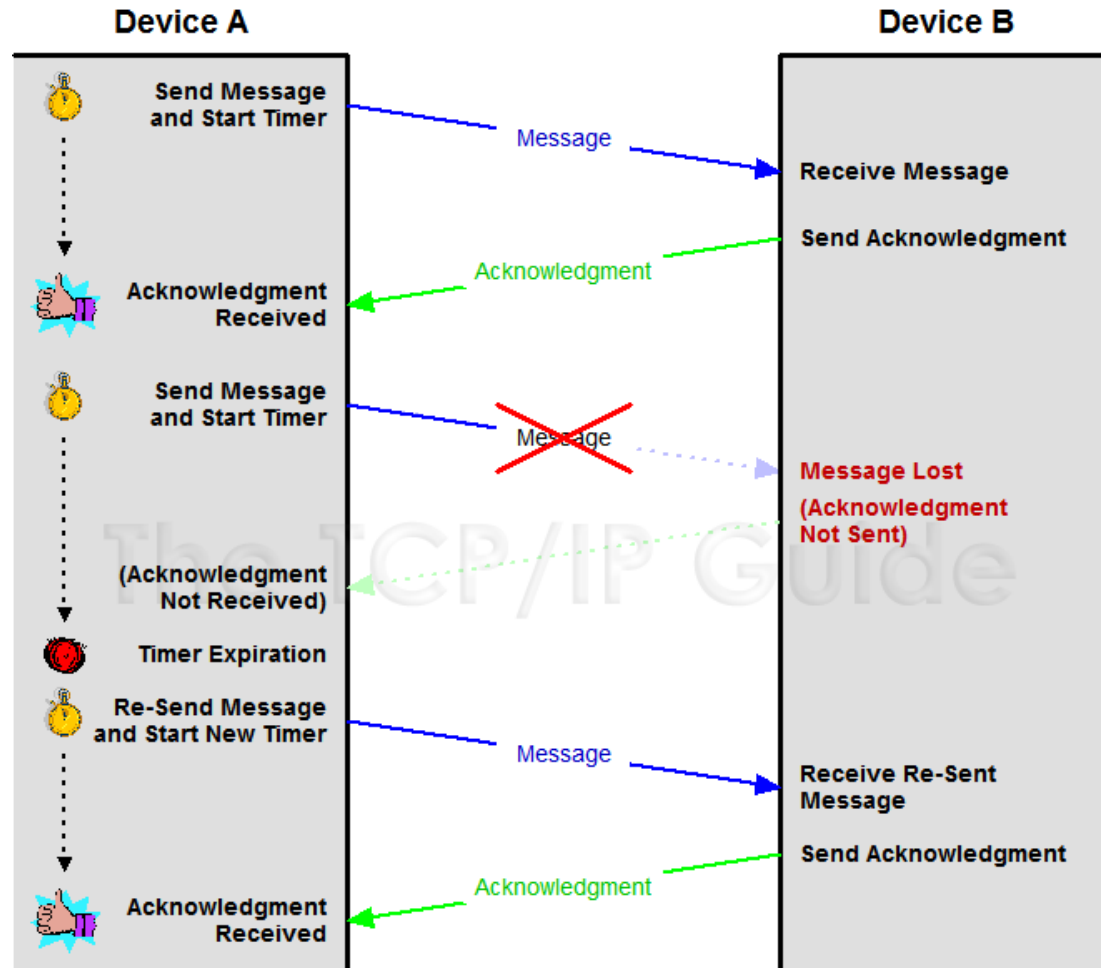




Unreliable Protocol



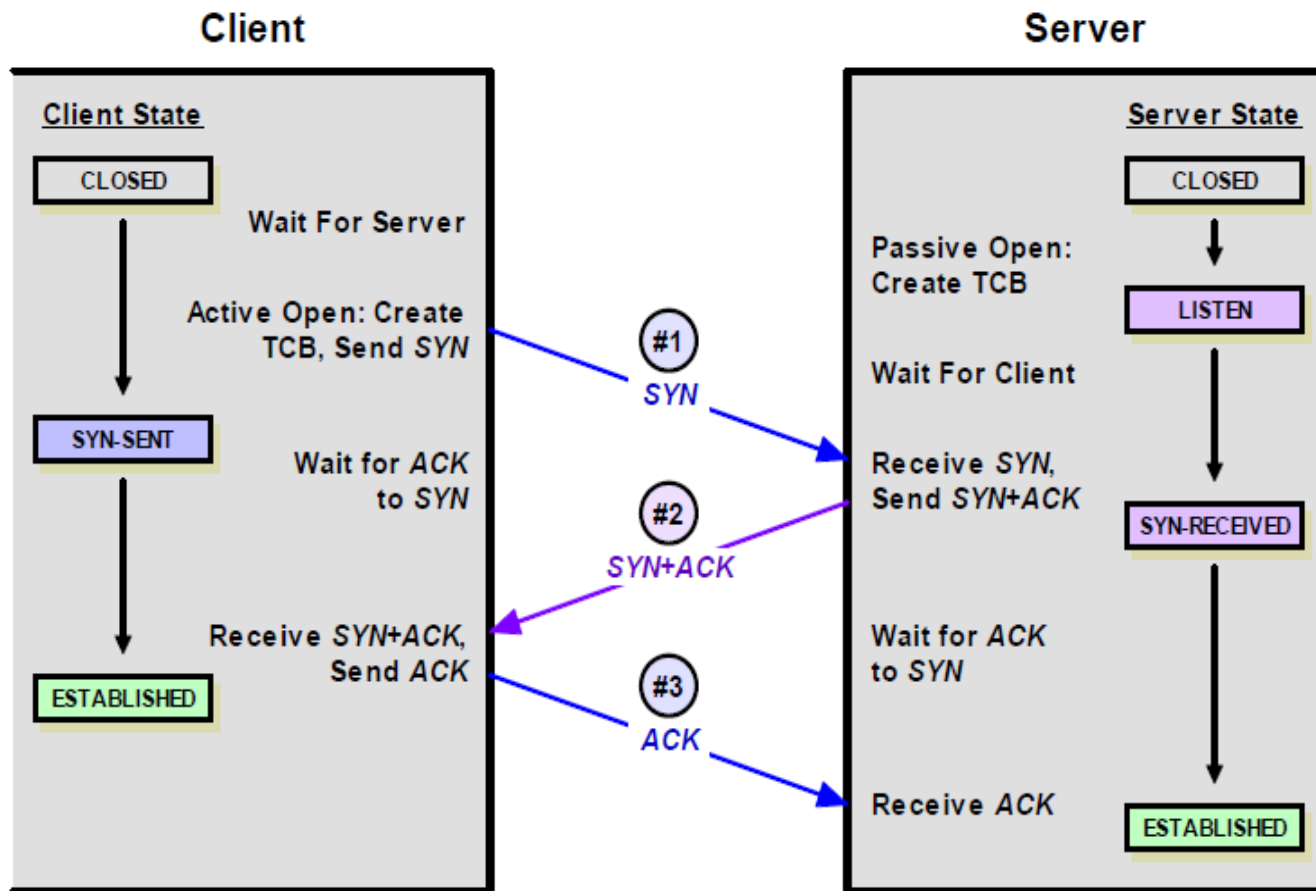
Positive Acknowledgement with Retransmission (PAR)



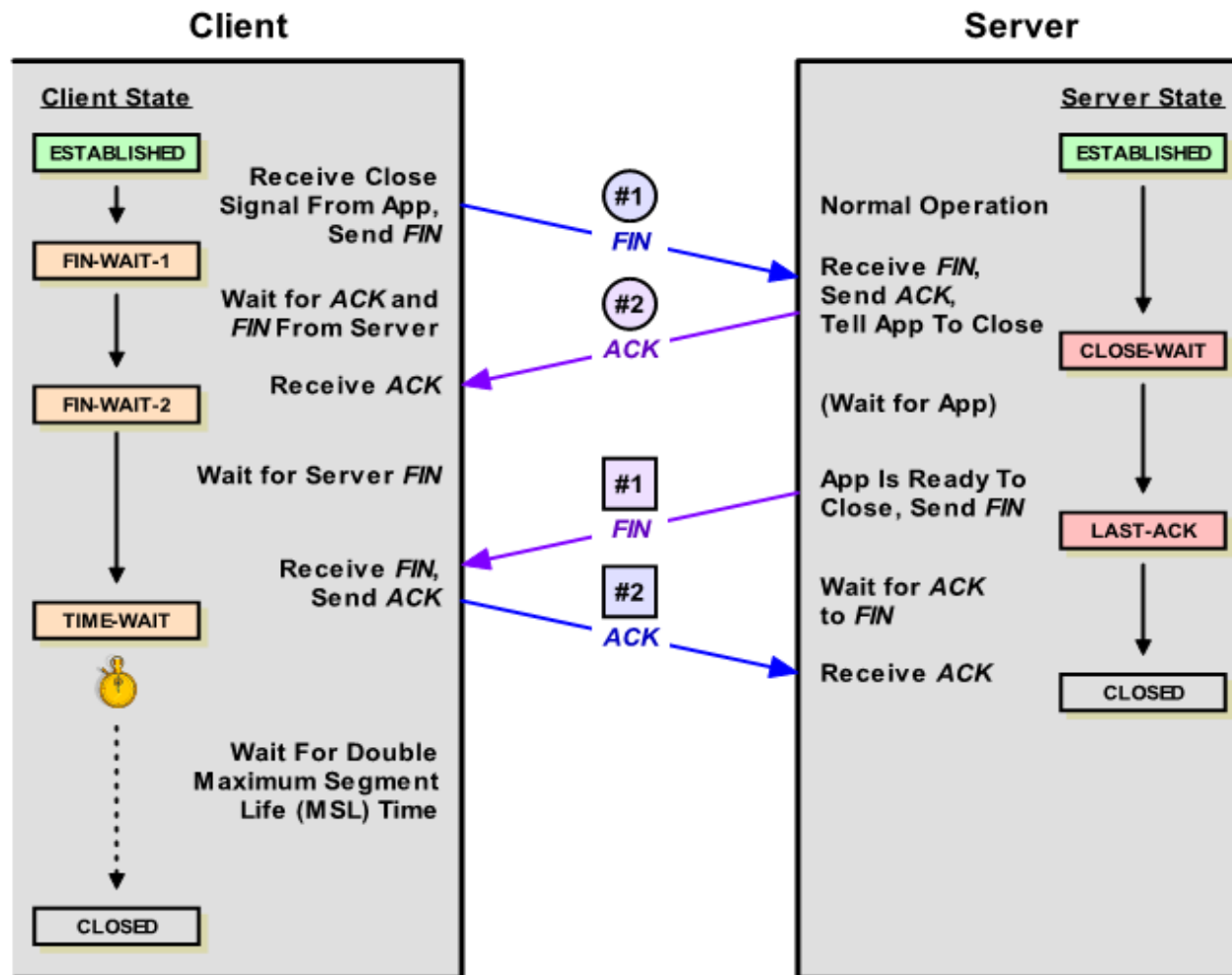
TCP basic operation

- Connection Establishment
 - Three-way Handshake (SYN, SYN+ACK, ACK)
- Management
 - The sliding windows scheme will be used to control segment size and to provide flow control, congestion handling and retransmissions as needed
- Termination
 - (FIN-ACK, FIN-ACK)

Three-way Handshake



Termination



Common TCP Port and Applications

Port #	Keyword	Protocol	Comments
20 and 21	ftp-data / ftp	File Transfer Protocol (FTP, data and control)	Used to send large files, so ideally suited for TCP.
23	telnet	Telnet Protocol	Interactive session-based protocol. Requires the connection-based nature of TCP.
25	smtp	Simple Mail Transfer Protocol (SMTP)	Uses an exchange of commands, and sends possibly large files between devices.
53	domain	Domain Name Server (DNS)	An example of a protocol that uses both UDP and TCP. For simple requests and replies, DNS uses UDP. For larger messages, especially zone transfers, TCP is used.
70	gopher	Gopher Protocol	A messaging protocol that has been largely replaced by the WWW.
80	http	Hypertext Transfer Protocol (HTTP / World Wide Web)	The classic example of a TCP-based messaging protocol.
110	pop3	Post Office Protocol (POP version 3)	E-mail message retrieval protocols; use TCP to exchange commands and data.
119	nntp	Network News Transfer Protocol (NNTP)	Used for transferring NetNews (USEnet) messages, which can be lengthy.
139	netbios-ssn	NetBIOS Session Service	A session protocol, clearly better suited to TCP than UDP.
143	imap	Internet Message Access Protocol (IMAP)	Another e-mail message retrieval protocol.