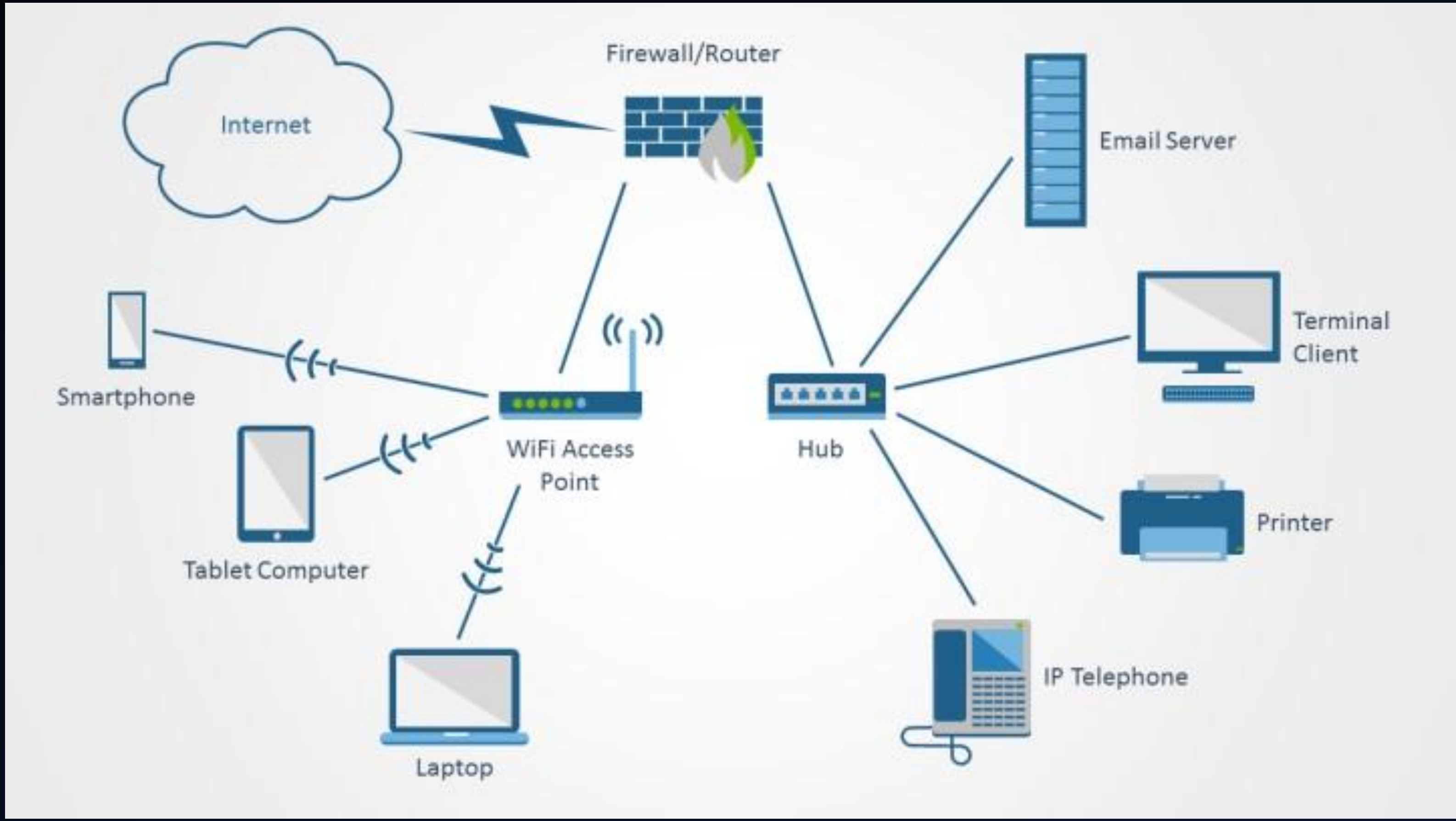
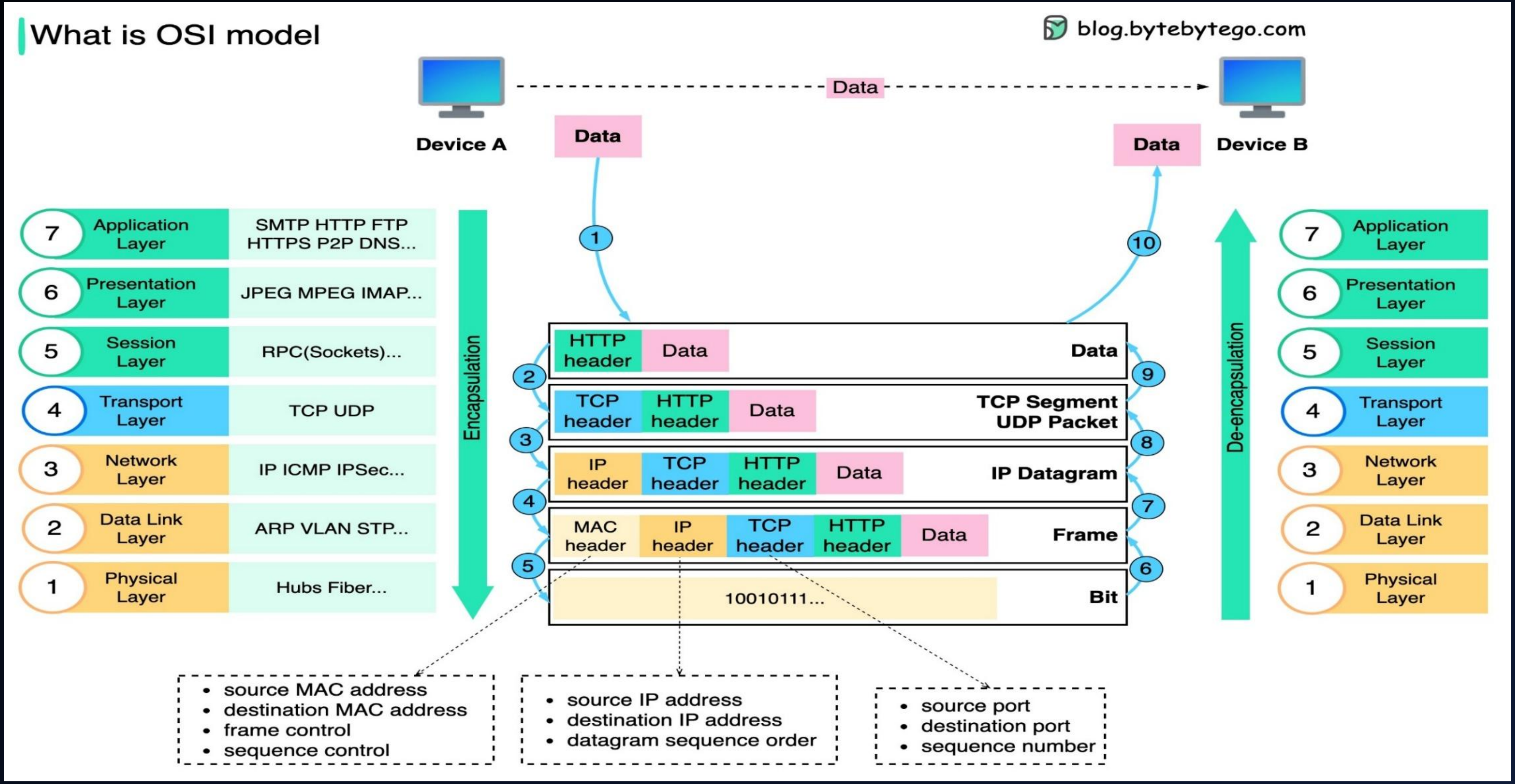
Computer Network

FROM BITS TO BANDWIDTH

Your First Thought on Computer Network



How it actually looks…

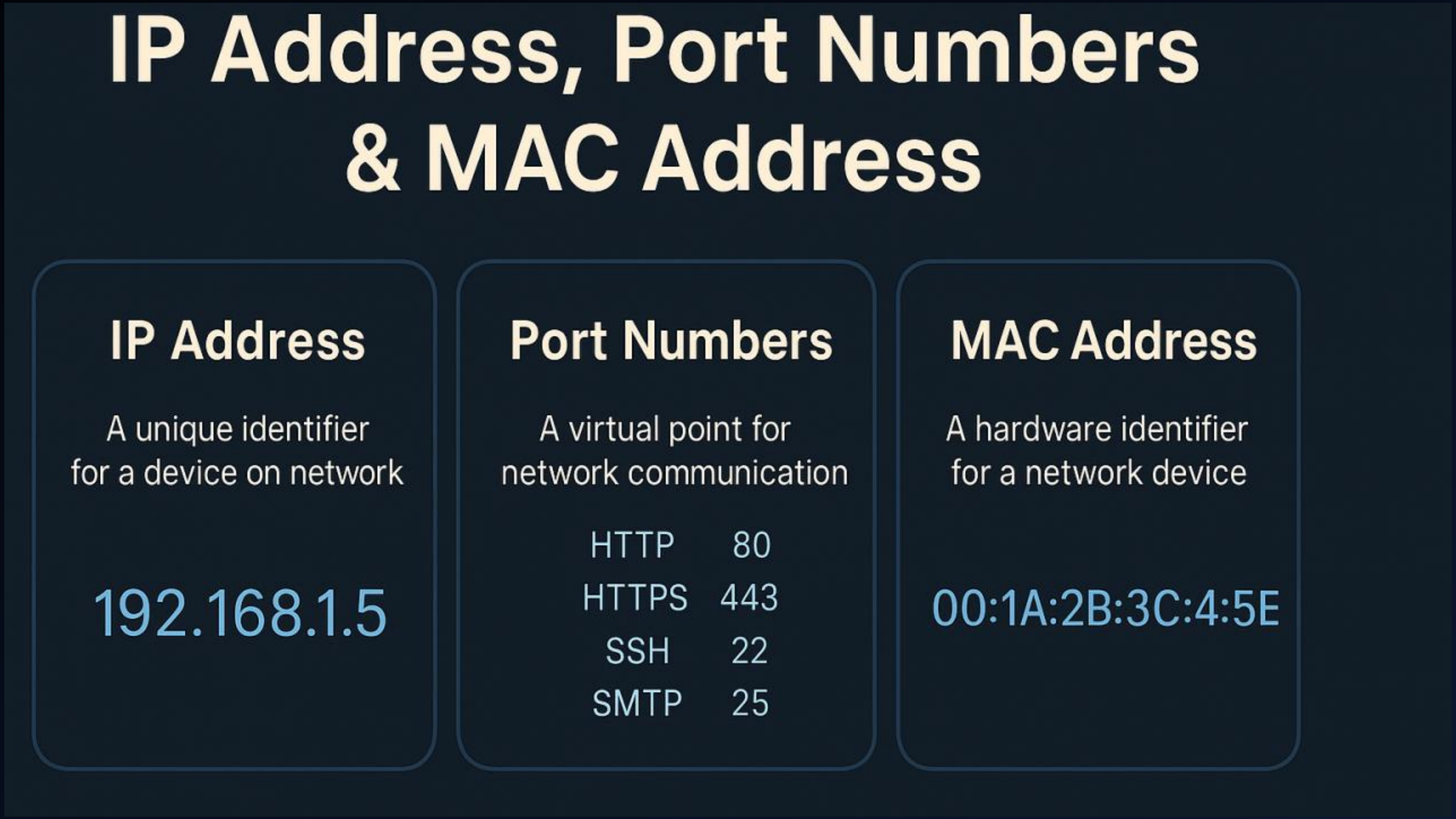


What We’ll Talk About

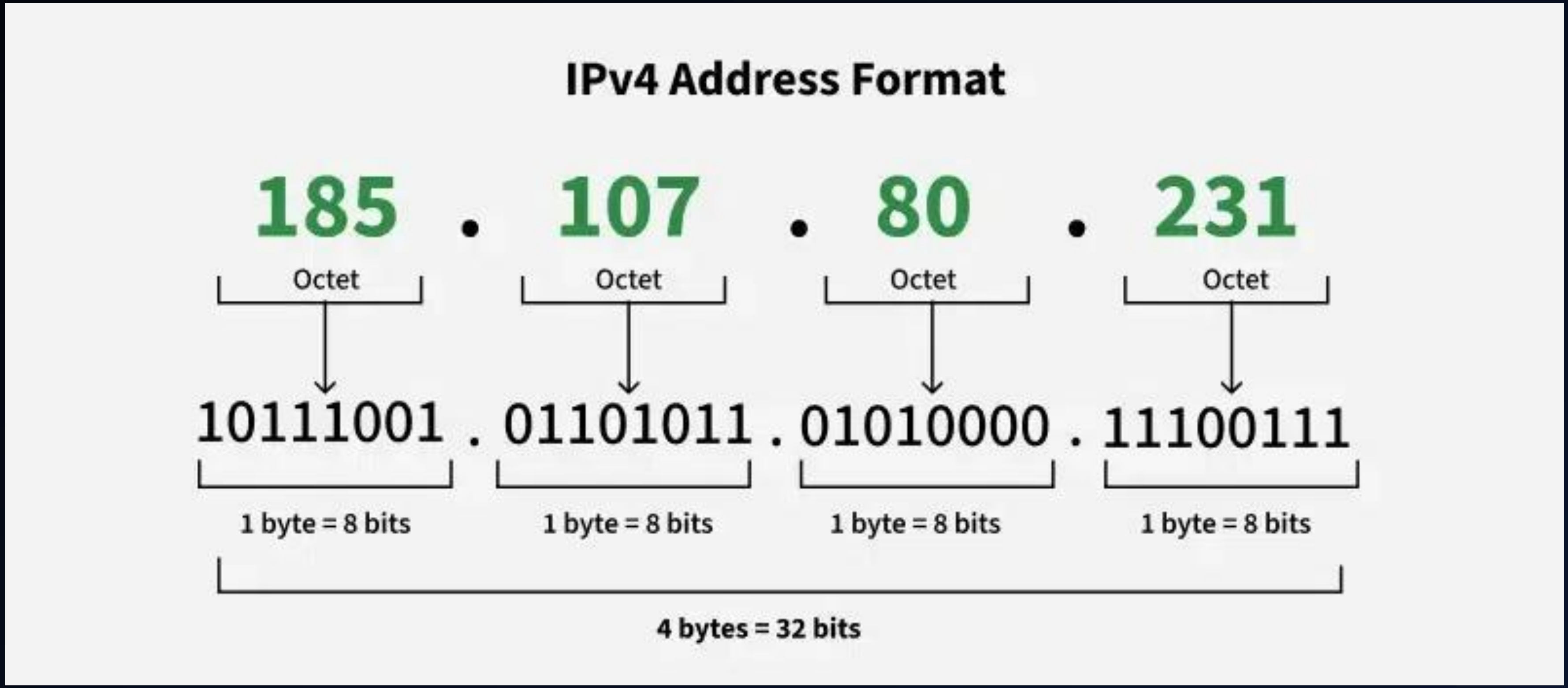
- IP Address
- Error Control
- Flow Control
- IPv4 Header
- Transport Layer
- Medium Access control
- Routing, Switching, IP Support Protocol
- Application Layer

IP Address

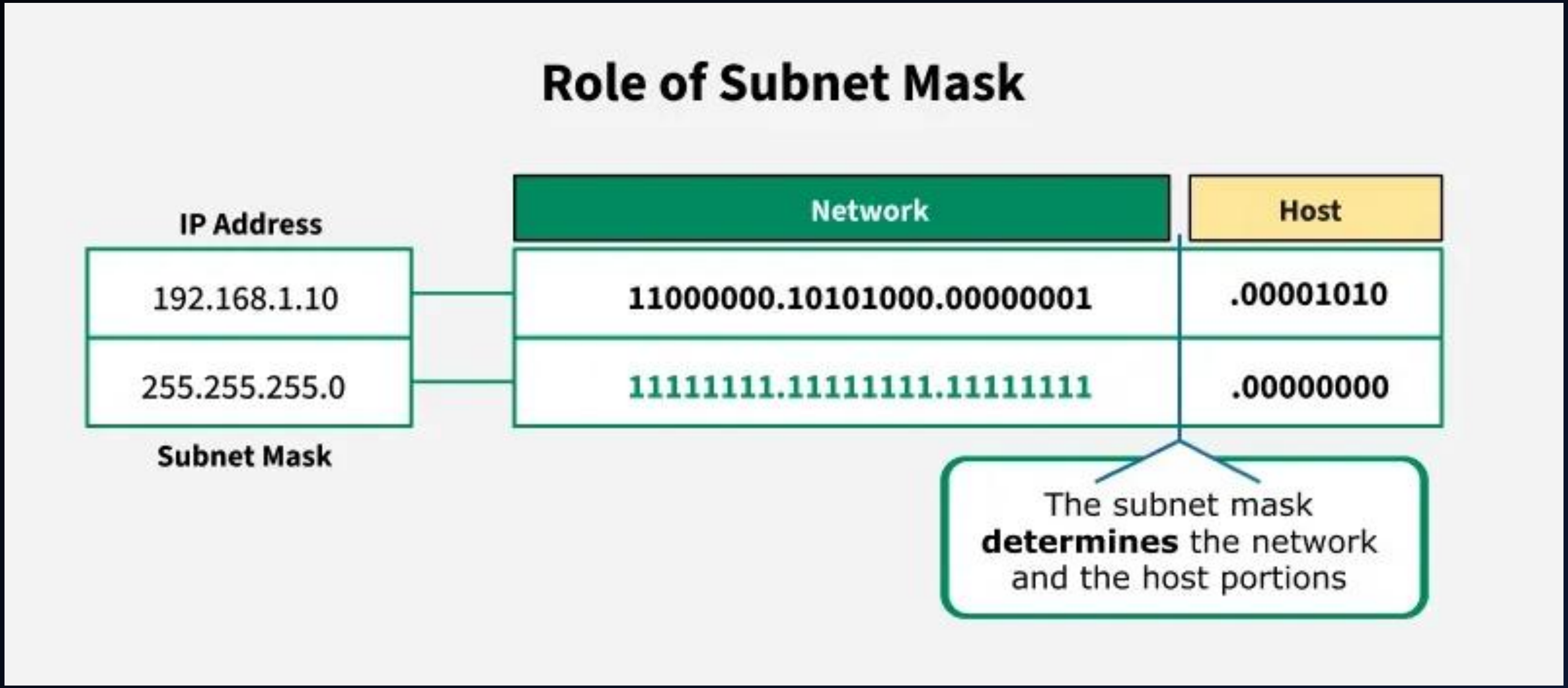
Does an Address Belong to a Device, Network, or Process?



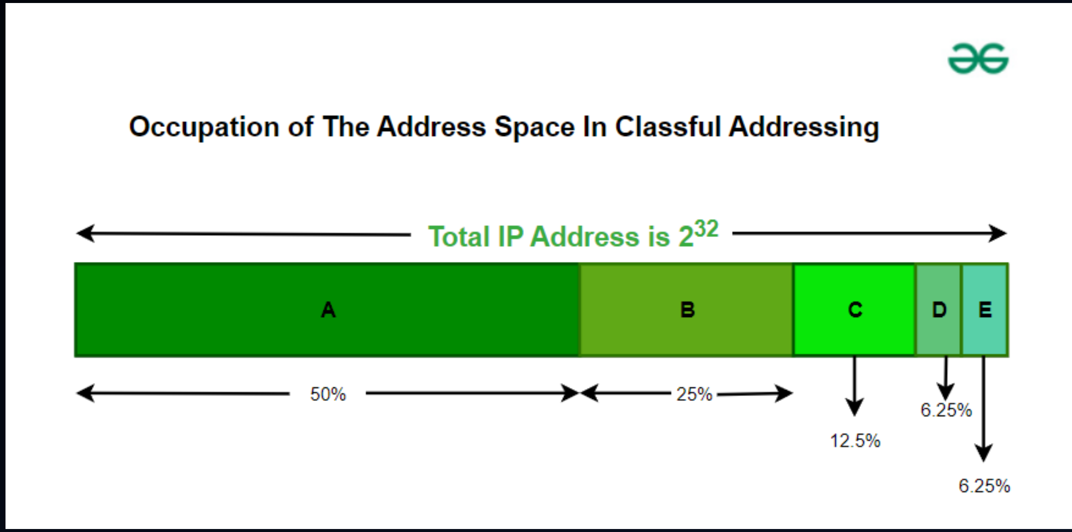
What’s an IPv4 Address?

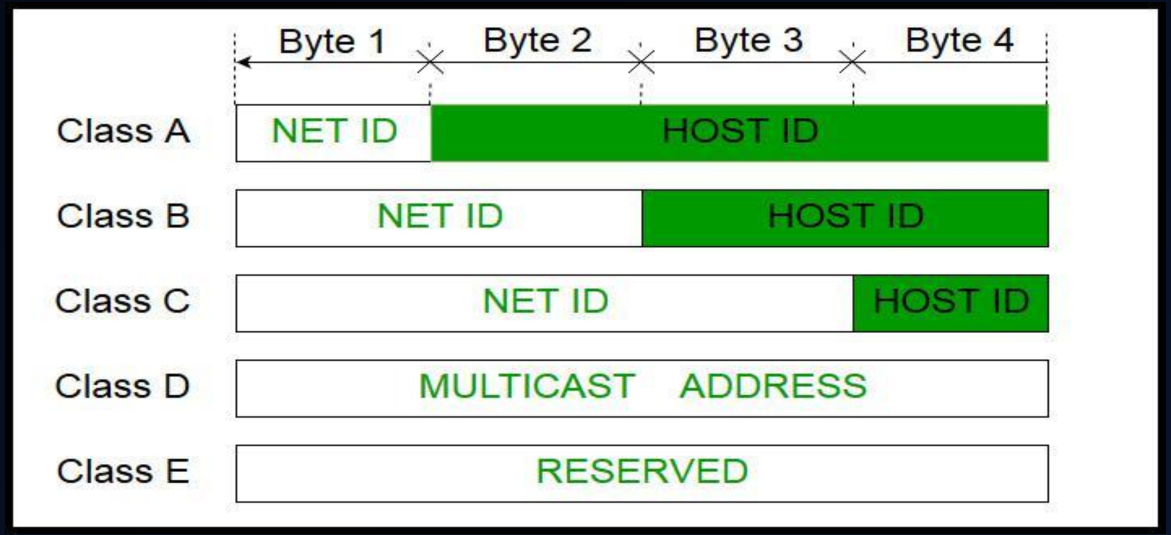


What's Subnet Mask?



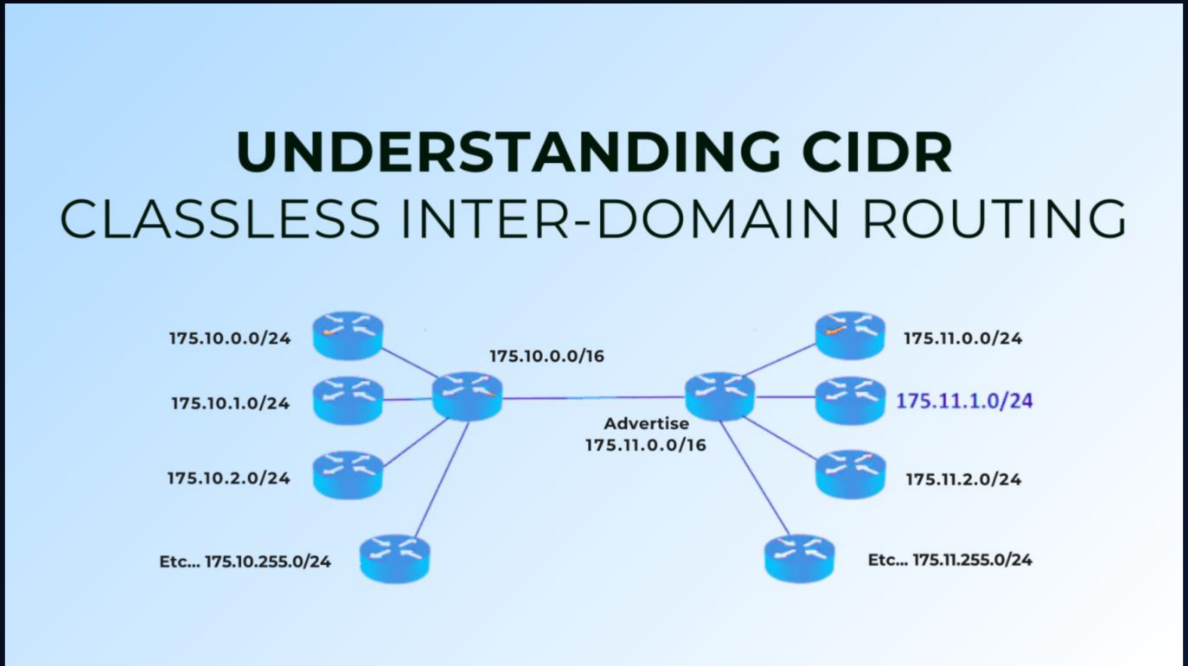
What's Classful Addressing?



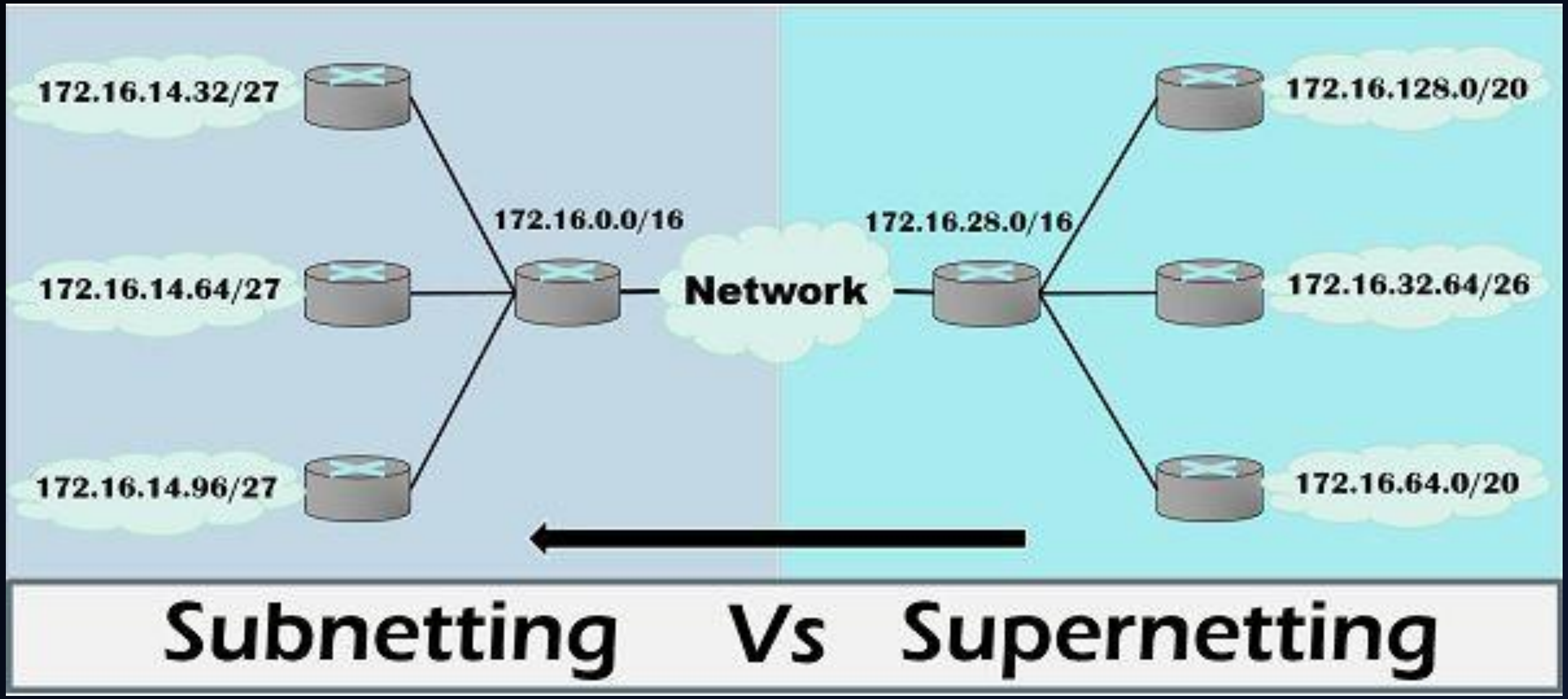


What's Classless Addressing?

- All IPs must be contiguous.
- Block size must be a power of 2 (2^n) simplifies network division.
- First IP of block divisible by block size least significant bits of host ID should be 0.

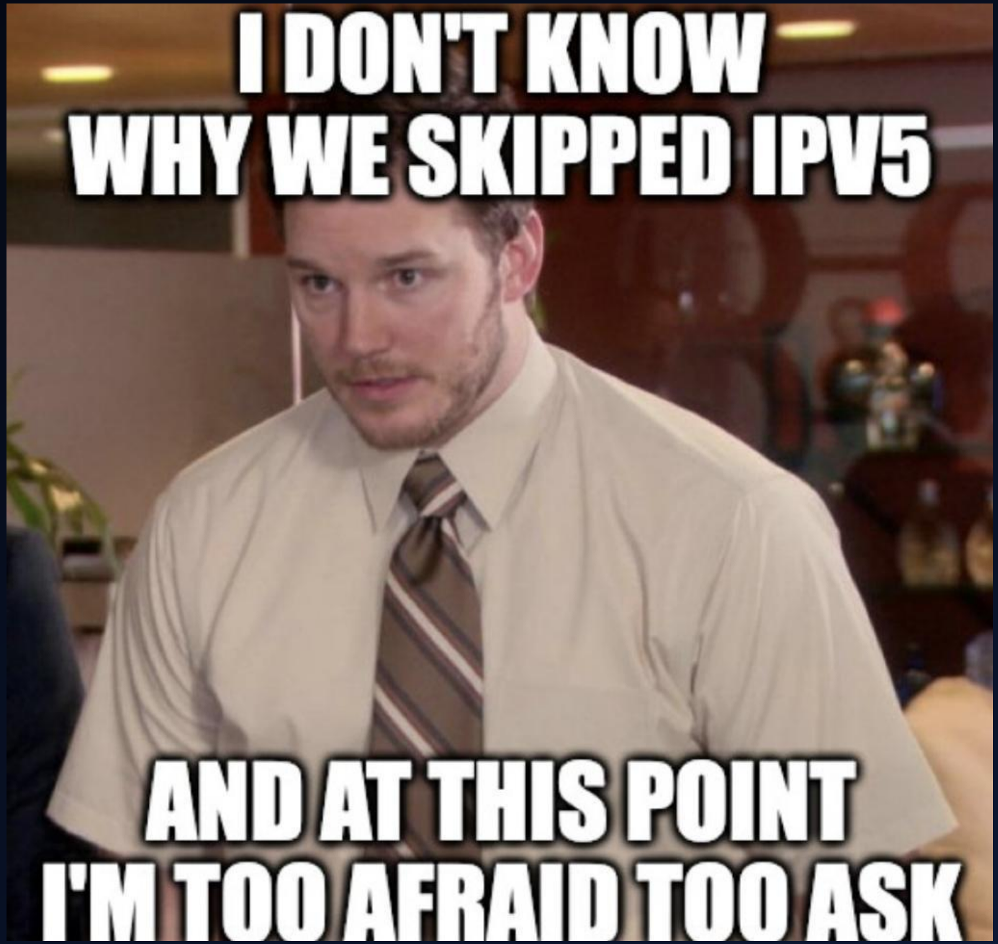


Subnetting vs Supernetting



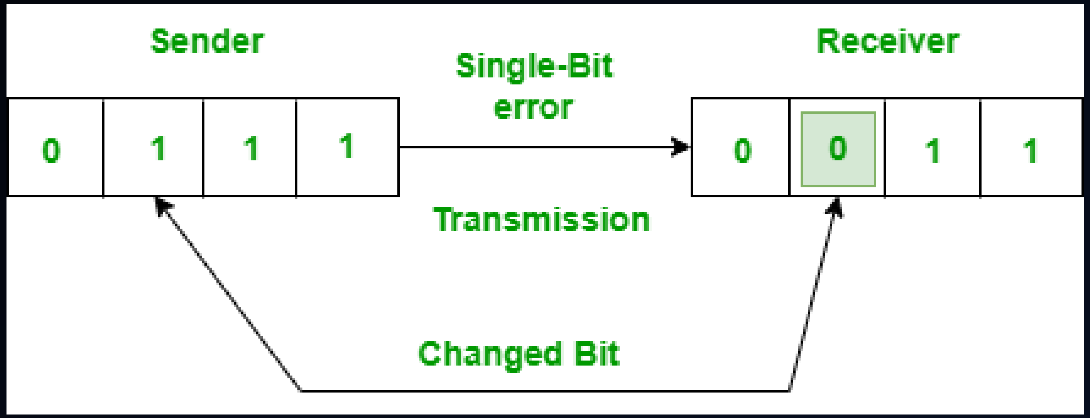
IPv6 Addressing

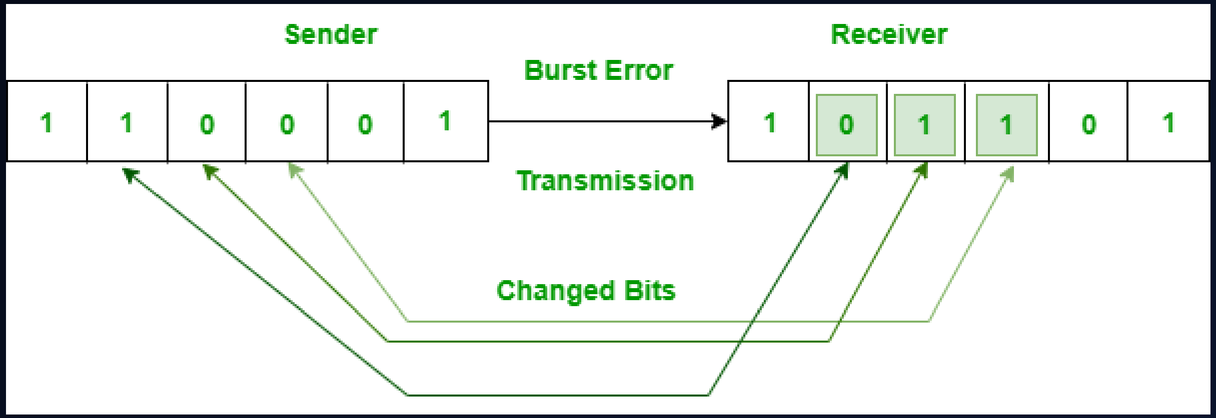
- Designed to replace IPv4 due to IPv4 address exhaustion.
- Uses 128-bit addresses → supports $\sim 3.4 \times 10^{38}$ unique addresses.
- It simplifies packet headers, making routing faster and more efficient.
- Security is built in with mandatory support for IPsec.
- It enables direct device connectivity with auto-configuration and better mobility support.



Error Control

What Errors Can Occur in a Network?



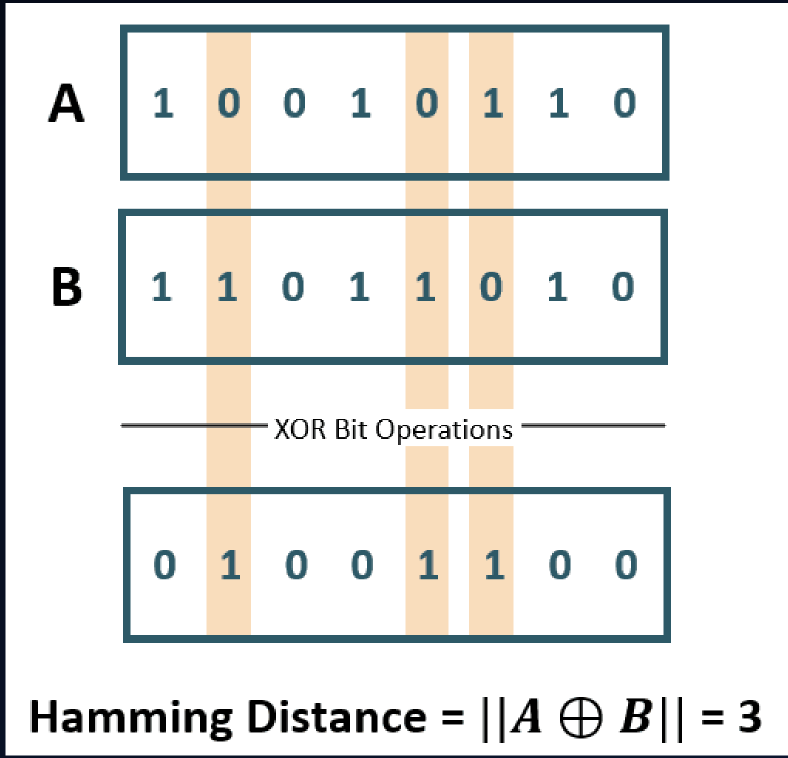


What’s Error Control

- Error Control
  - Error Detection
  - Error Correction

What's Hamming Distance

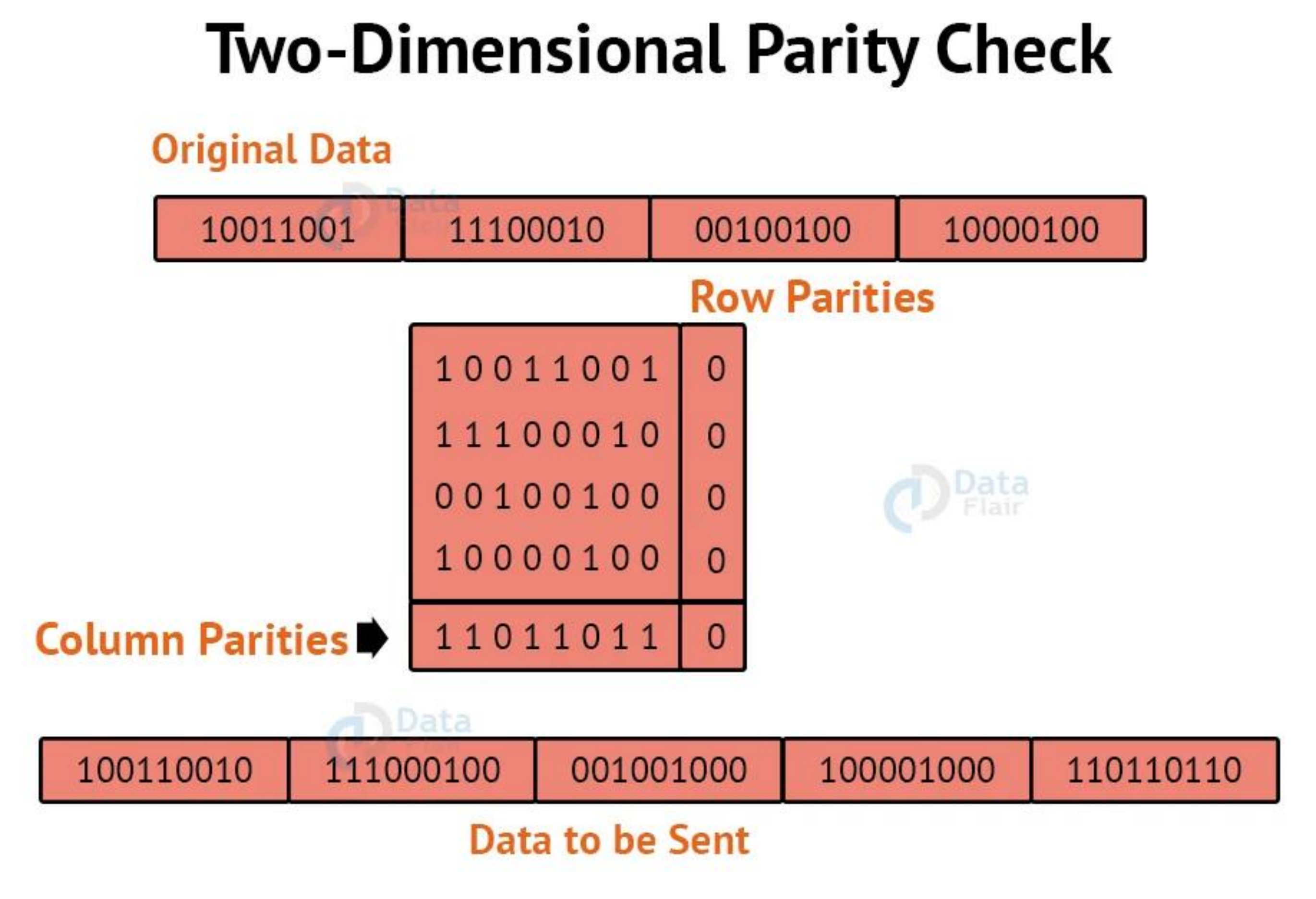
- **Minimum Hamming Distance rules:**
  - Detect up to **d errors**: Minimum distance ≥ d + 1
  - Correct up to **d errors**: Minimum distance ≥ 2d + 1



What are Error Control Methods

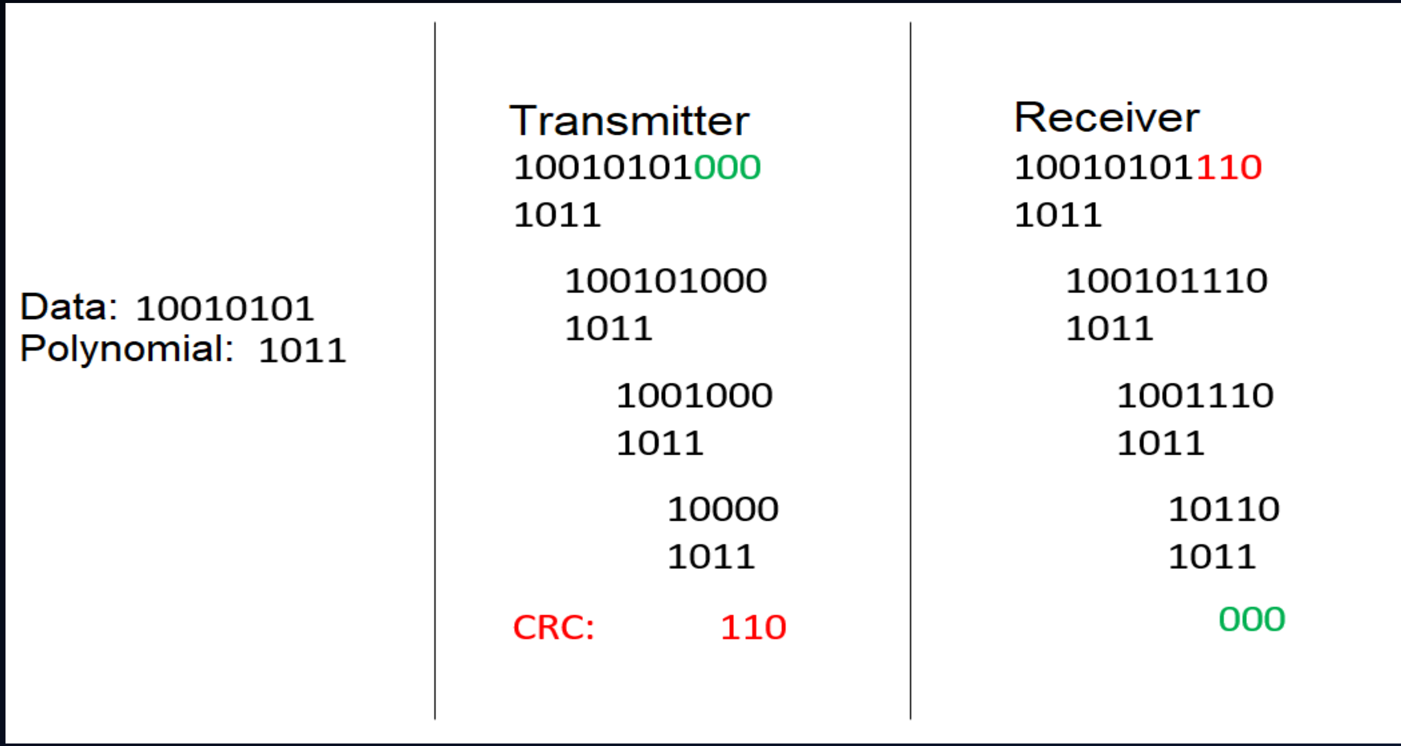
- For Detection:
  - Simple & 2D Parity
  - Cyclic Redundancy Code
  - Checksum
- For Correction
  - Hamming Code

Simple & 2D Parity

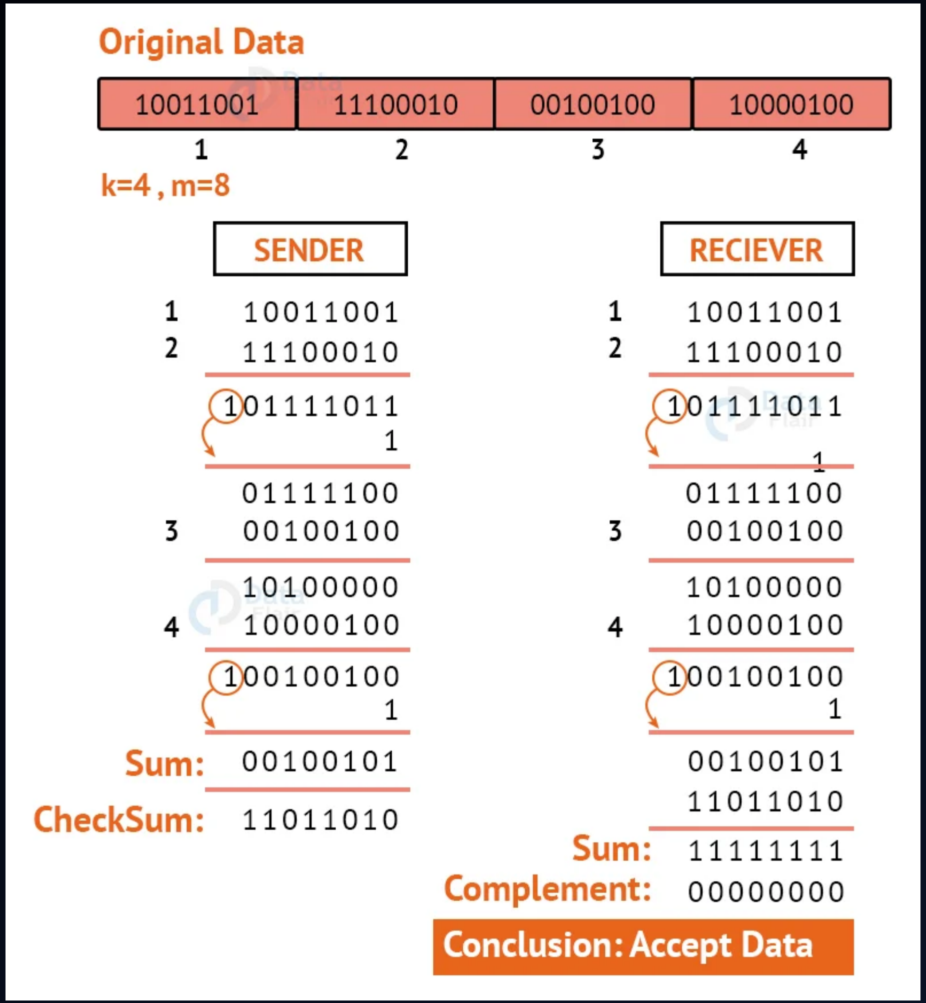


Cyclic Redundancy Code

- Good CRC Generator Polynomial
  - Must have more than one nonzero term.
  - Must not divide $x^n + 1$ for any n.
  - Must have a factor of $x + 1$.



Checksum



Checksum can fail if errors cancel each other out, this is why CRC is preferred for critical data.

Hamming Code

- Uses **parity bits** placed at positions that are powers of 2 (1, 2, 4, 8…).
- $m + r + 1 \leq 2^r$
  - m = number of data bits
  - r = number of parity bits

Position	0	1	2	3	4	5	6	7	8	9	10	11
R8	0	0	0	0	0	0	0	0	1	1	1	1
R4	0	0	0	0	1	1	1	1	0	0	0	0
R2	0	0	1	1	0	0	1	1	0	0	1	1
R1	0	1	0	1	0	1	0	1	0	1	0	1

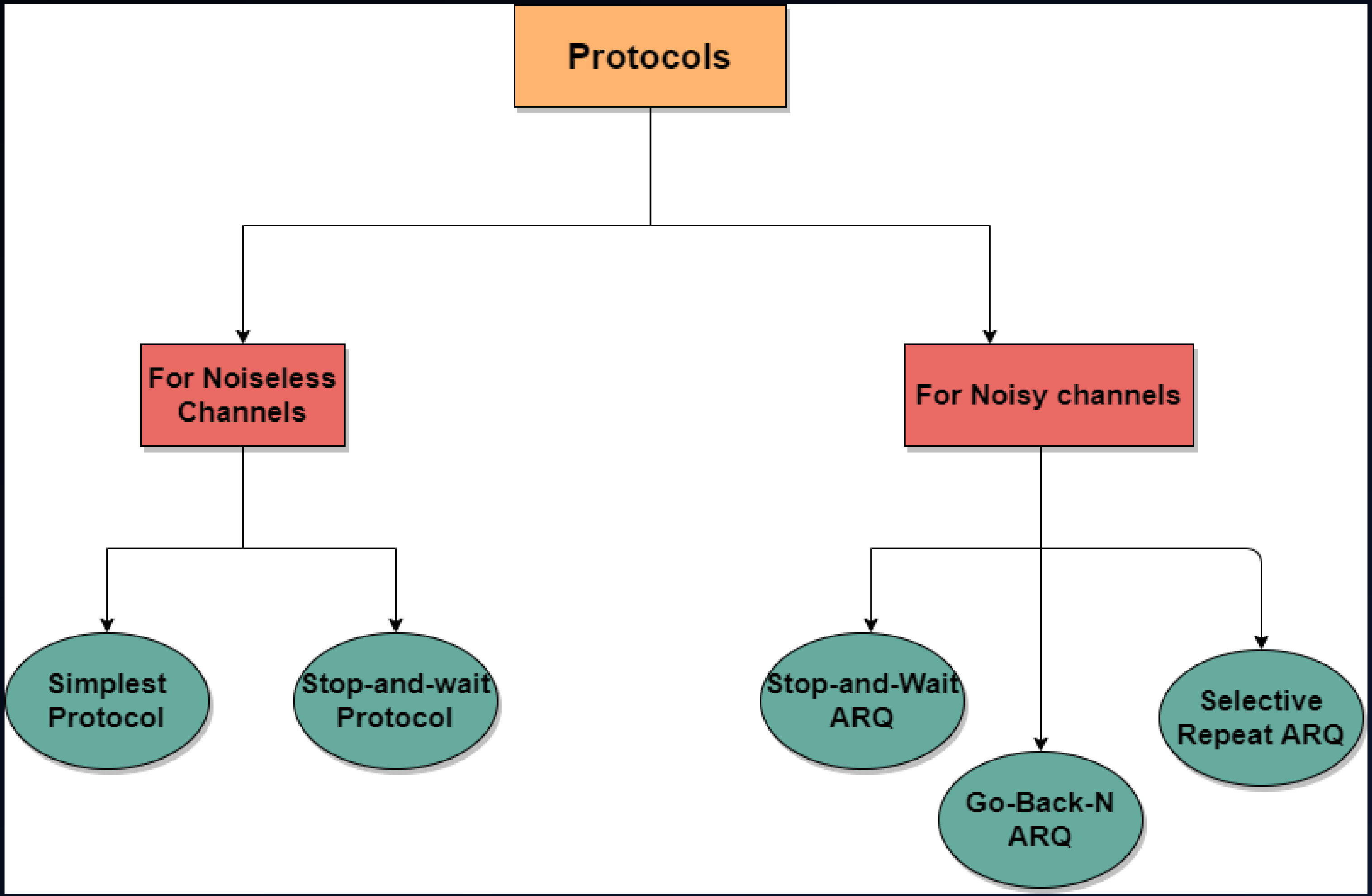
R1 - 1,3,5,7,9,11 R2 - 2,3,6,7,10,11 R4 - 4,5,6,7 R8 - 8,9,10,11

At a Glance

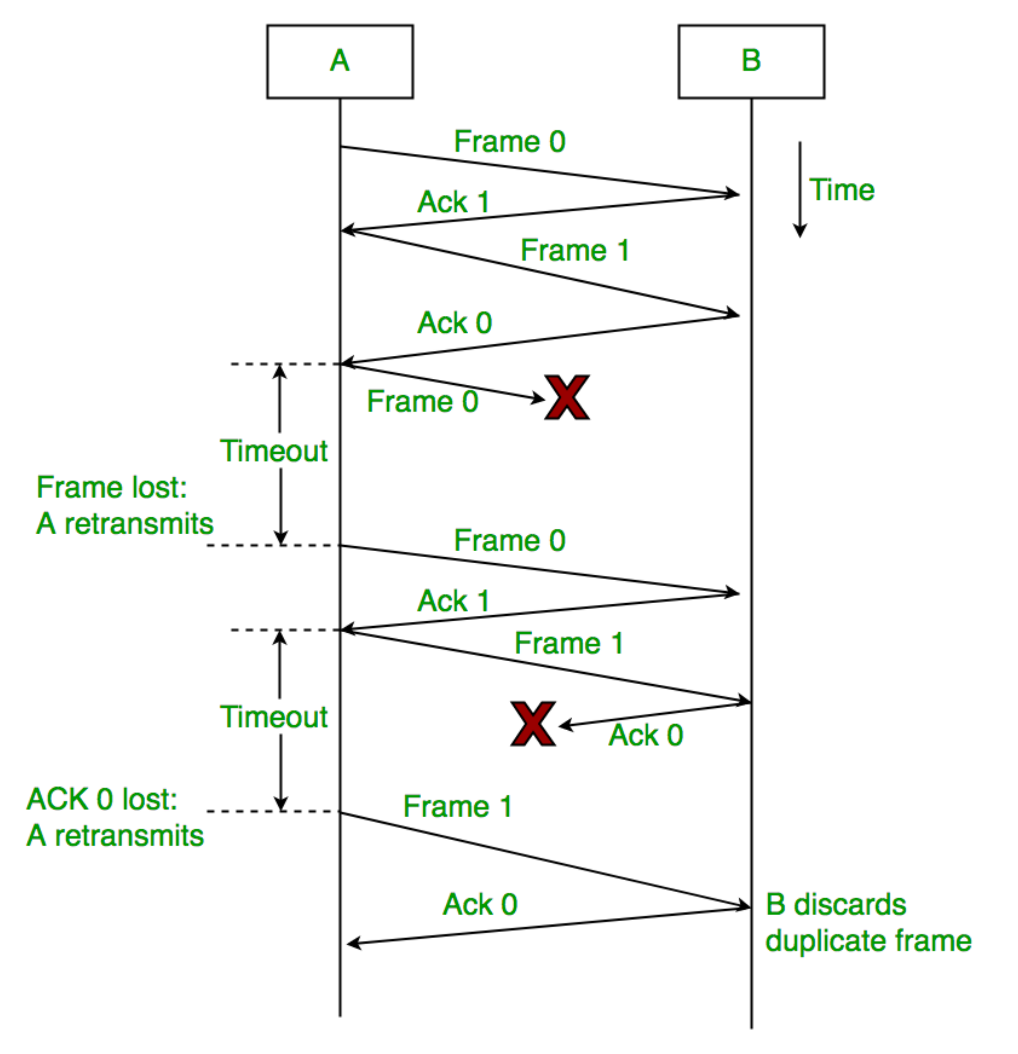
Method	Detects Errors	Corrects Errors	Notes / Comments
Parity Bit	1-bit (single-bit errors)	✕ None	Can detect **odd number of errors**, simple and fast
Checksum	Single-bit + some multiple-bit errors	✕ None	Simple sum of data words, less reliable than CRC
CRC	All single-bit, most multi-bit, burst errors ≤ CRC length	✕ None	Very reliable, used in network protocols
Hamming Code	All single-bit errors	1-bit	Can **detect and correct 1-bit errors**, uses parity bits

Flow Control

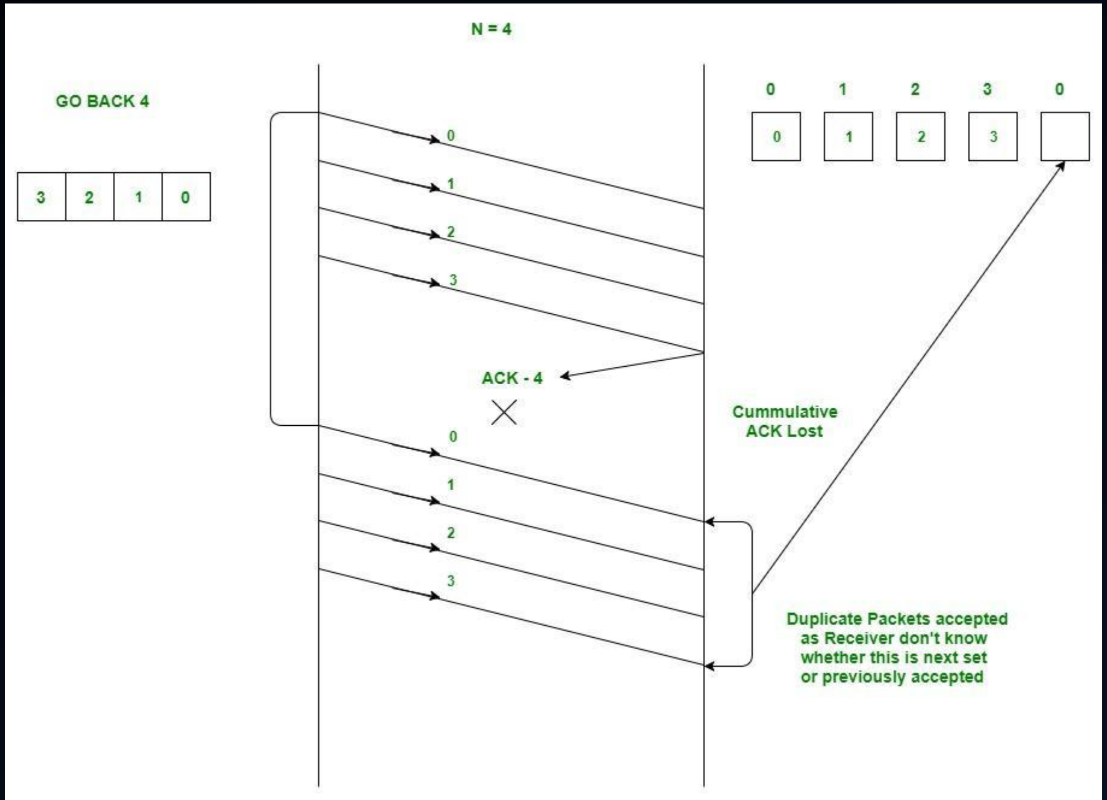
How Does a Network Control the Flow of Data?



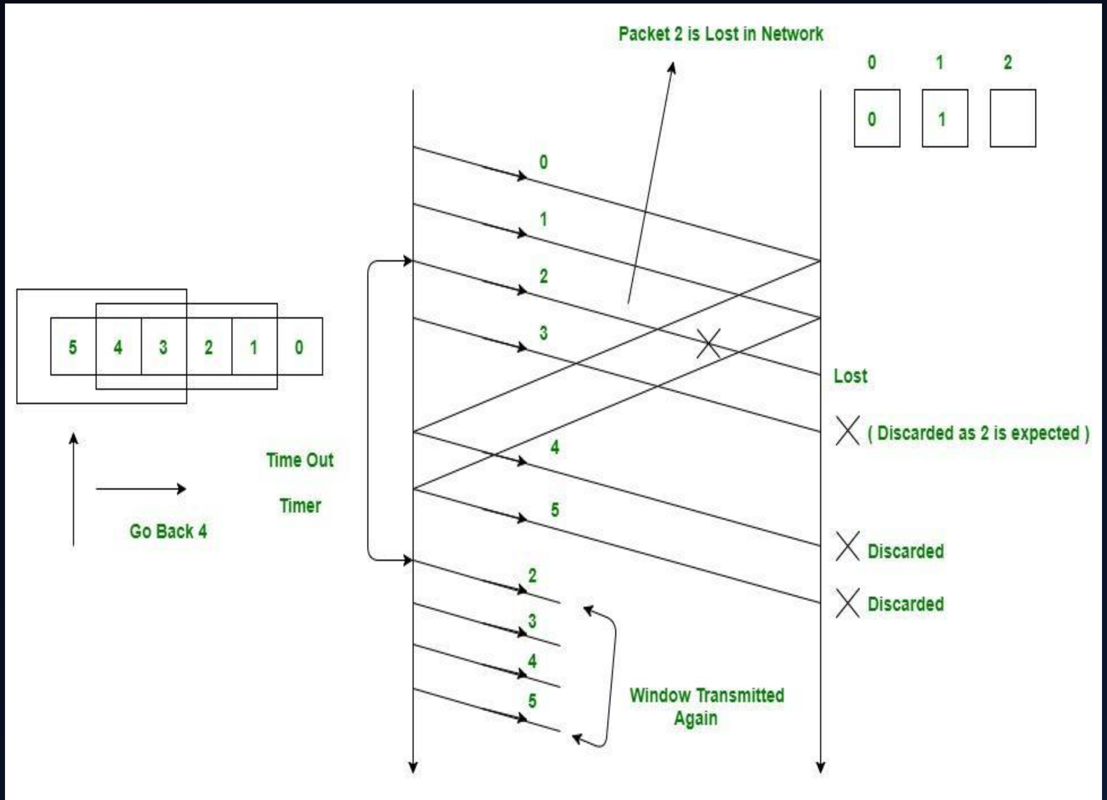
Stop-&-Wait ARQ



Go Back-N ARQ

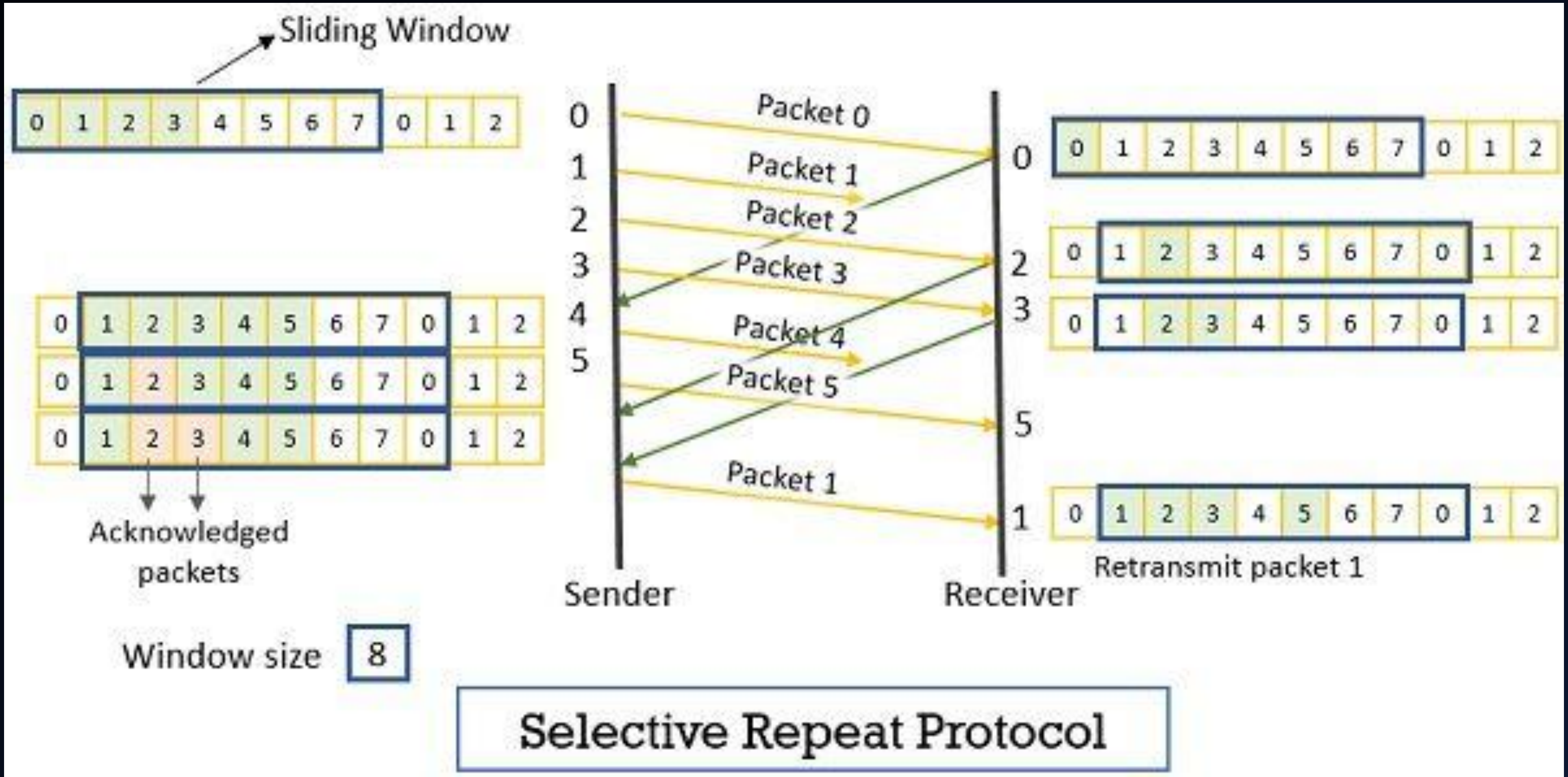


N = 4
GO BACK 4
3 2 1 0
0 1 2 3 0
0 1 2 3
0
1
2
3
ACK - 4
Cummulative
ACK Lost
0
1
2
3
Duplicate Packets accepted
as Receiver don't know
whether this is next set
or previously accepted



Packet 2 is Lost in Network
0 1 2
0 1
0
1
2
3
Lost
(Discarded as 2 is expected)
5 4 3 2 1 0
Time Out
Timer
Go Back 4
4
5
Discarded
Discarded
2
3
4
5
Window Transmitted
Again

Selective Repeat ARQ



Comparison of ARQ(Automatic Repeat reQuest) Protocols

Feature	Stop-and-Wait	Go-Back-N (GBN)	Selective Repeat (SR)
Sender Window Size	1	N	N
Receiver Window Size	1	1	N
Sequence Numbers	0,1	0 to N-1	0 to N-1
Acknowledgment	Individual	Cumulative	Individual
Retransmission	On timeout	On timeout of lost frame	Only lost frame
Efficiency	Low	Better than Stop-and-Wait	Highest
Buffer Requirement	Low	Moderate	High
Complexity	Simple	Moderate	Complex
Error Handling	Single frame	Multiple frames lost	Individual frames lost

Performance Analysis of ARQ Protocols

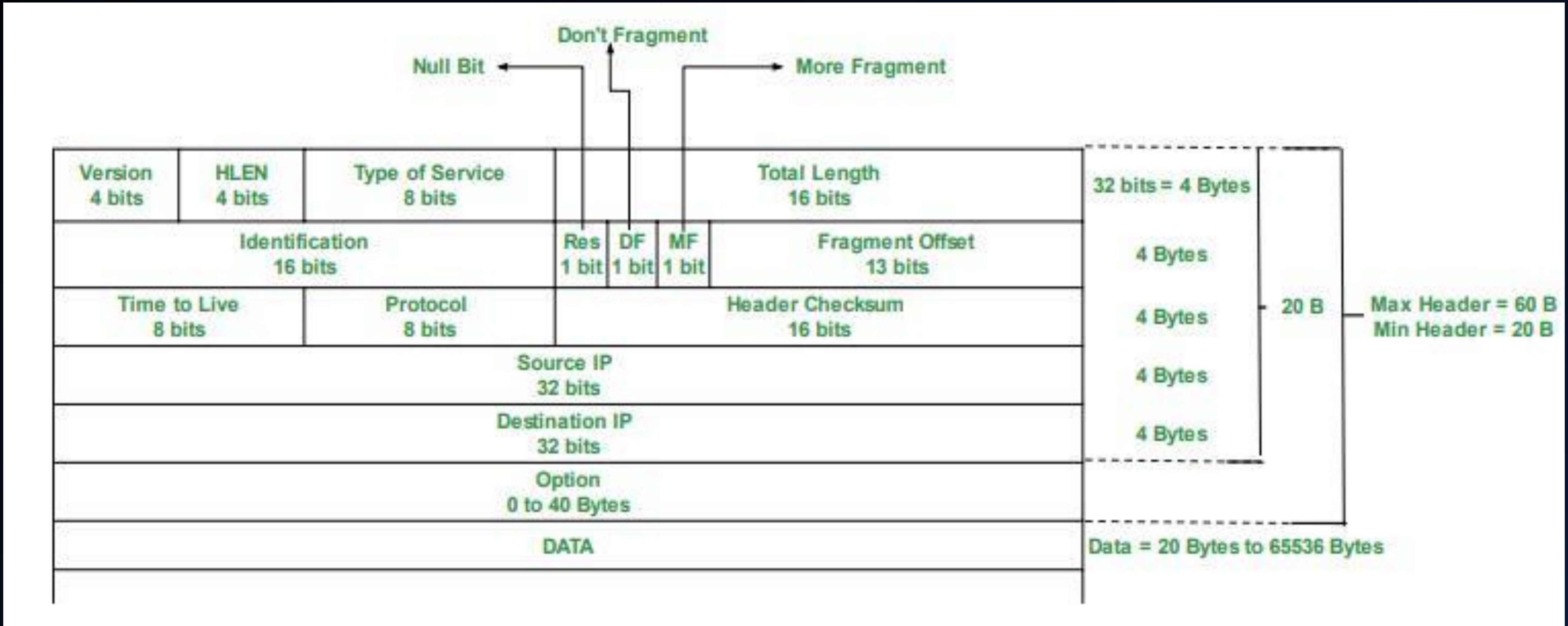
Parameter / Term	Meaning
$\boldsymbol{T_{d-f}}$	Transmission delay (time to send a frame)
$\boldsymbol{P_d}$	Propagation delay (time for signal to travel to receiver)
$\boldsymbol{Q_d}$	Queuing delay (time a frame waits in buffer)
PR_d	Processing delay (time to process a frame at sender/receiver)
$\boldsymbol{T_{d-ack}}$	Time to transmit acknowledgment
$\boldsymbol{RTT}$	Round Trip Time = $T_{d-f} + 2 * P_d + Q_d + \mathrm{PR_d} + \mathrm{T_{d-ack}}$

Protocol	Efficiency (η)
Stop-and-Wait	$\eta = \frac{T_d}{RTT}$
Go-Back-N (GBN)	$\eta \approx \frac{N * T_d}{RTT}$
Selective Repeat (SR)	$\eta \approx \frac{N * T_d}{RTT}$

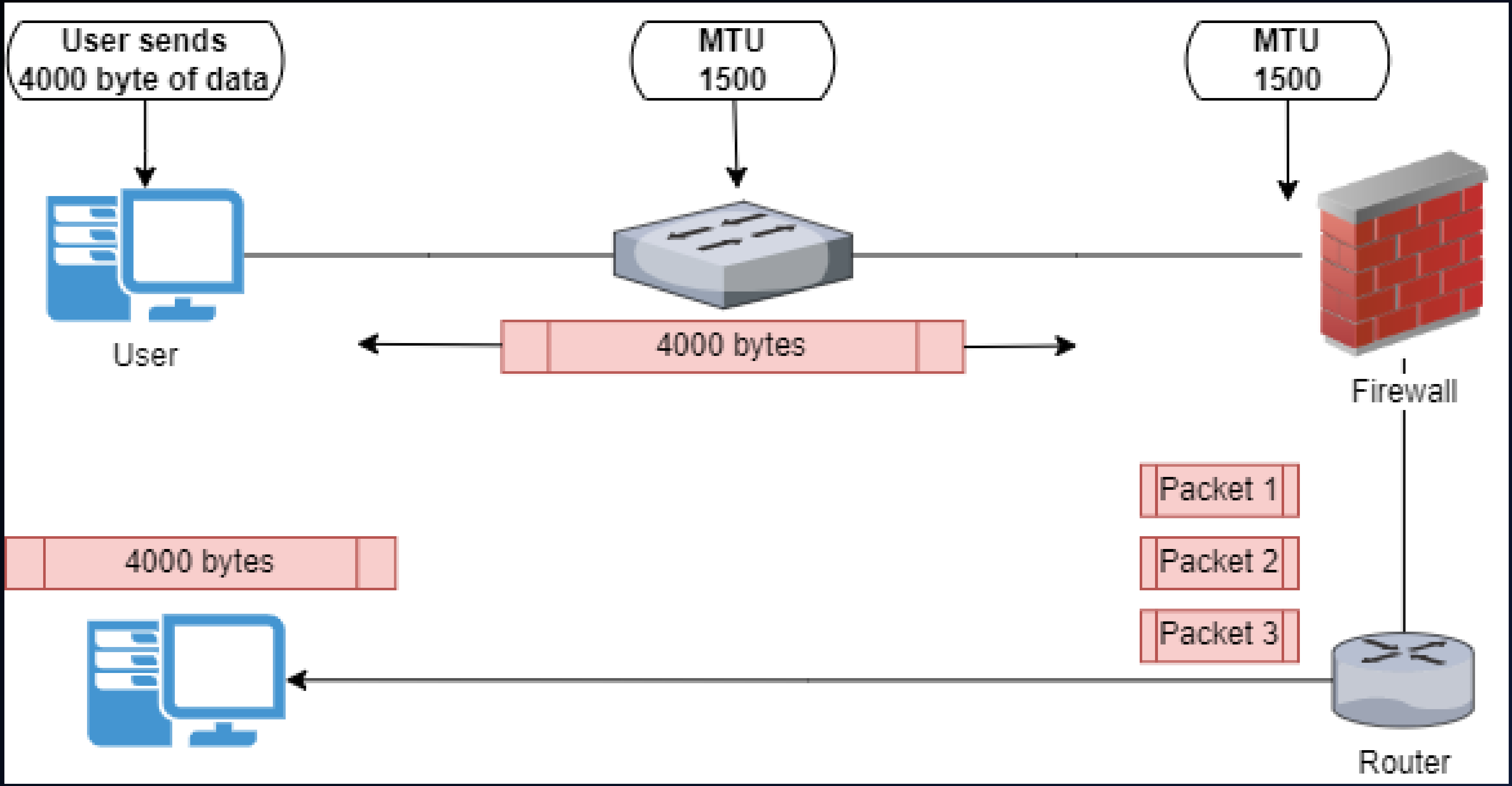
Throughput(τ) = Efficiency(η) * Bandwidth

IPv4 Header

Let’s Have a Look at the IPv4 Header



What's IPv4 Fragmentation



Facts About IPv4 Fields

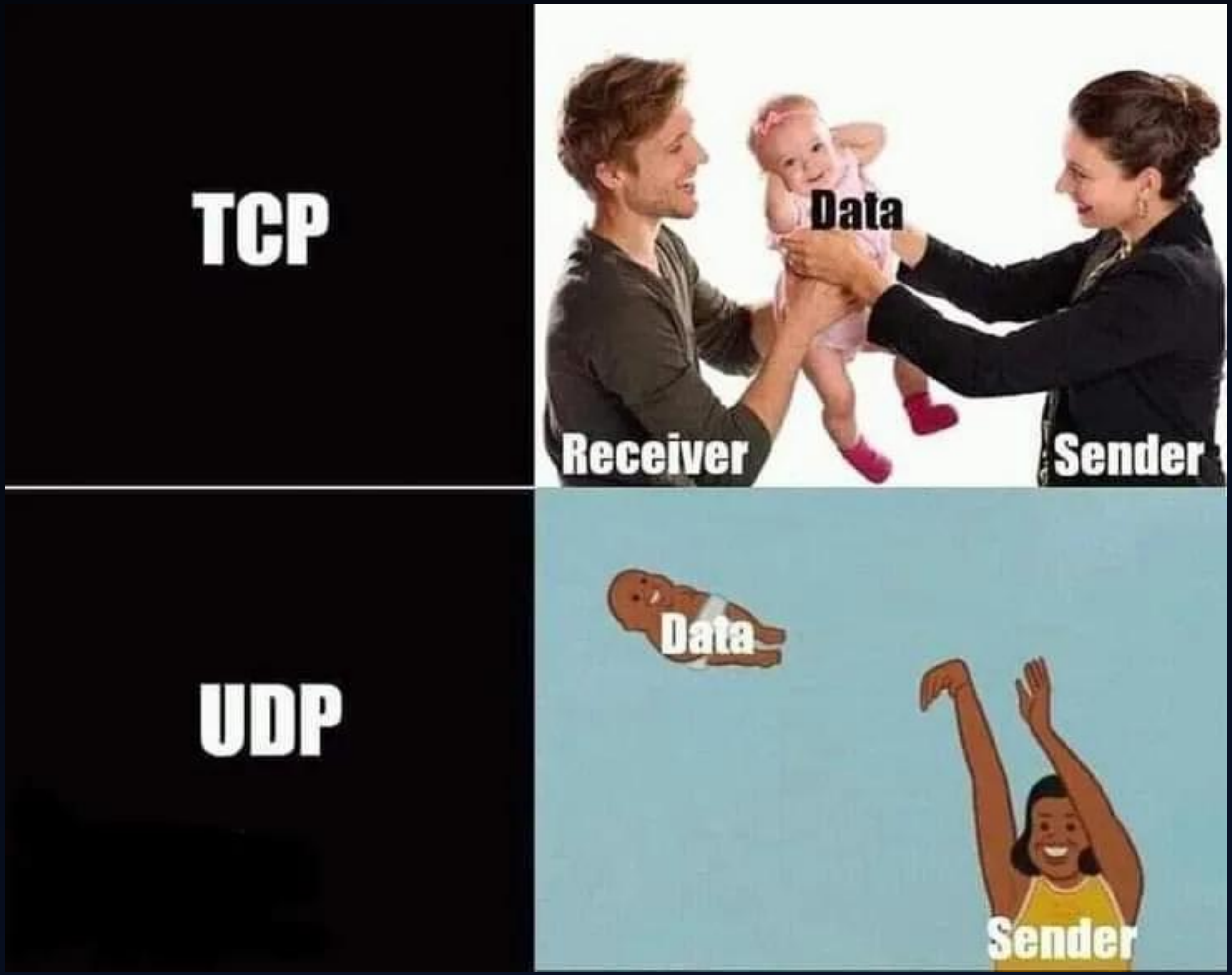
- HLEN is 4 bits, so maximum value it can store is 15. Header size ranges from 20 B to 60 B. This works because HLEN stores header length in units of 4 bytes. Actual header size = HLEN × 4 bytes
- Total Length (TLEN) is 16 bits. Maximum packet size = $2^{16} - 1 = 65{,}535$ bytes; Includes header + data
- Fragment Offset is 13 bits, but does not count bytes directly. Offset is measured in 8-byte units. Actual fragment position = Fragment Offset × 8 bytes. This is why fragment size must be a multiple of 8 bytes
  - Why scaling factor = 8? Saves bits in header, Allows large packet offsets using fewer bits

Facts About IPv4 Fields

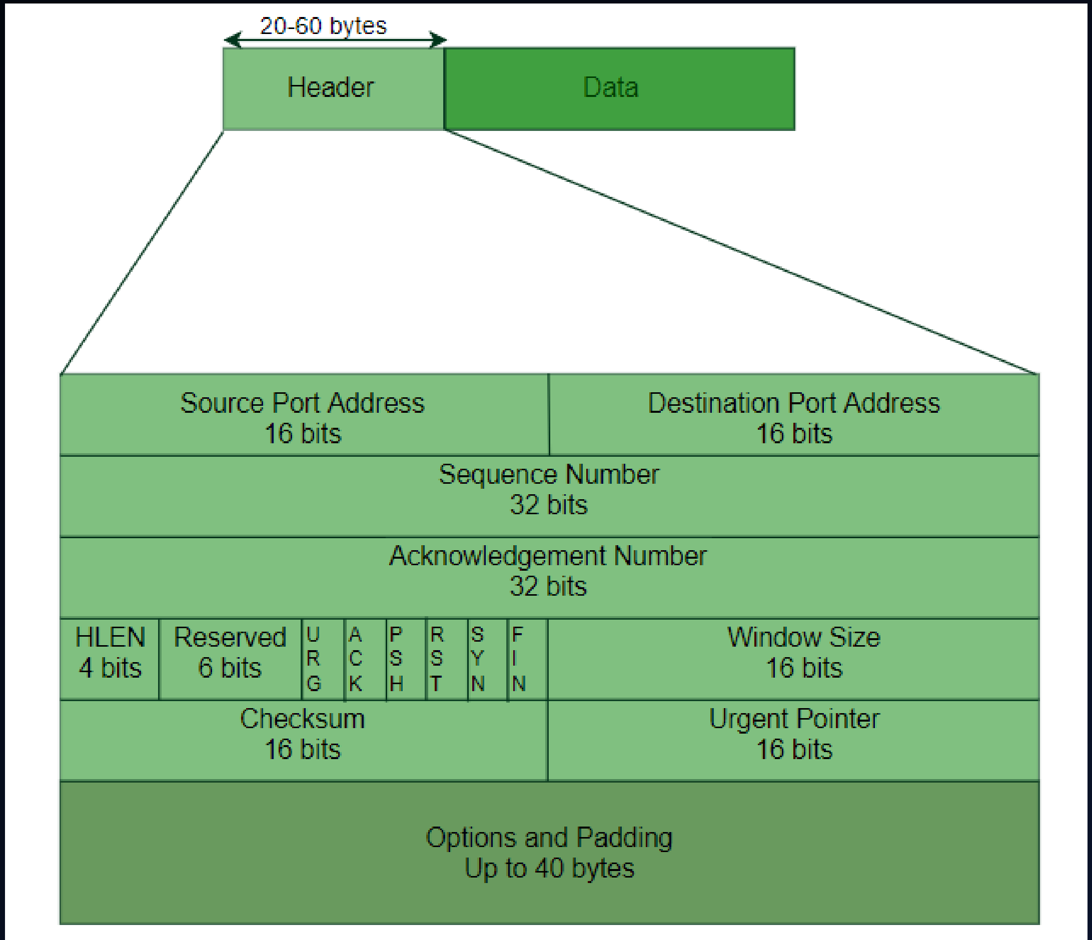
- TTL is 8 bits. Maximum value = 255. Decremented by 1 at each router. Prevents packets from looping forever
- Protocol field is 8 bits. Identifies the upper-layer protocol. Examples: TCP = 06, UDP = 17, ICMP = 01
- Type of Service (ToS) is 8 bits. Originally for delay, throughput, reliability, priority. Now split into DSCP (6 bits) + ECN (2 bits). "DSCP tells routers how important a packet is, ECN tells endpoints how congested the network is."
- Header Checksum covers header only. Recomputed at every hop because TTL changes.

Transport Layer

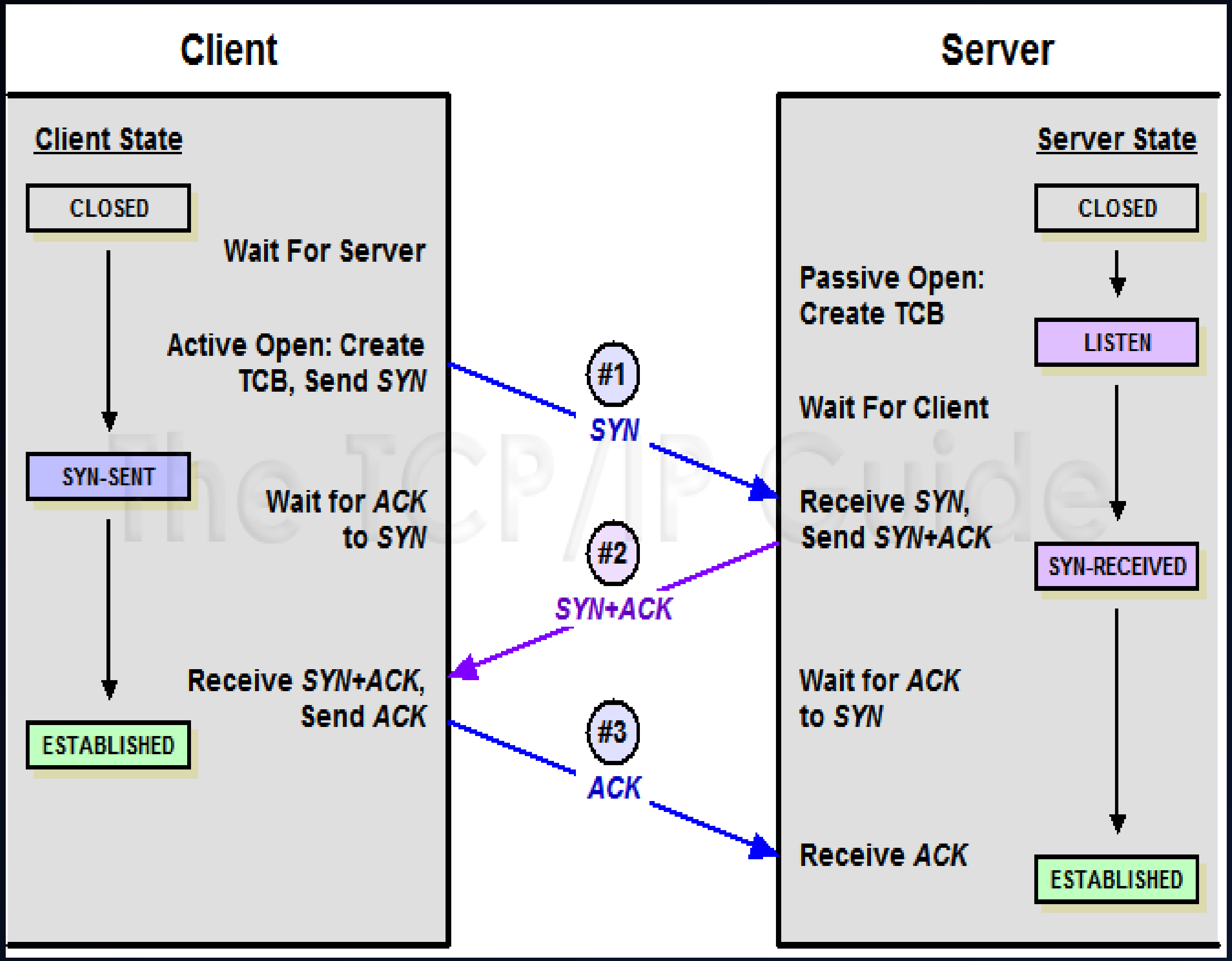
Let’s Move Towards the Transport Layer



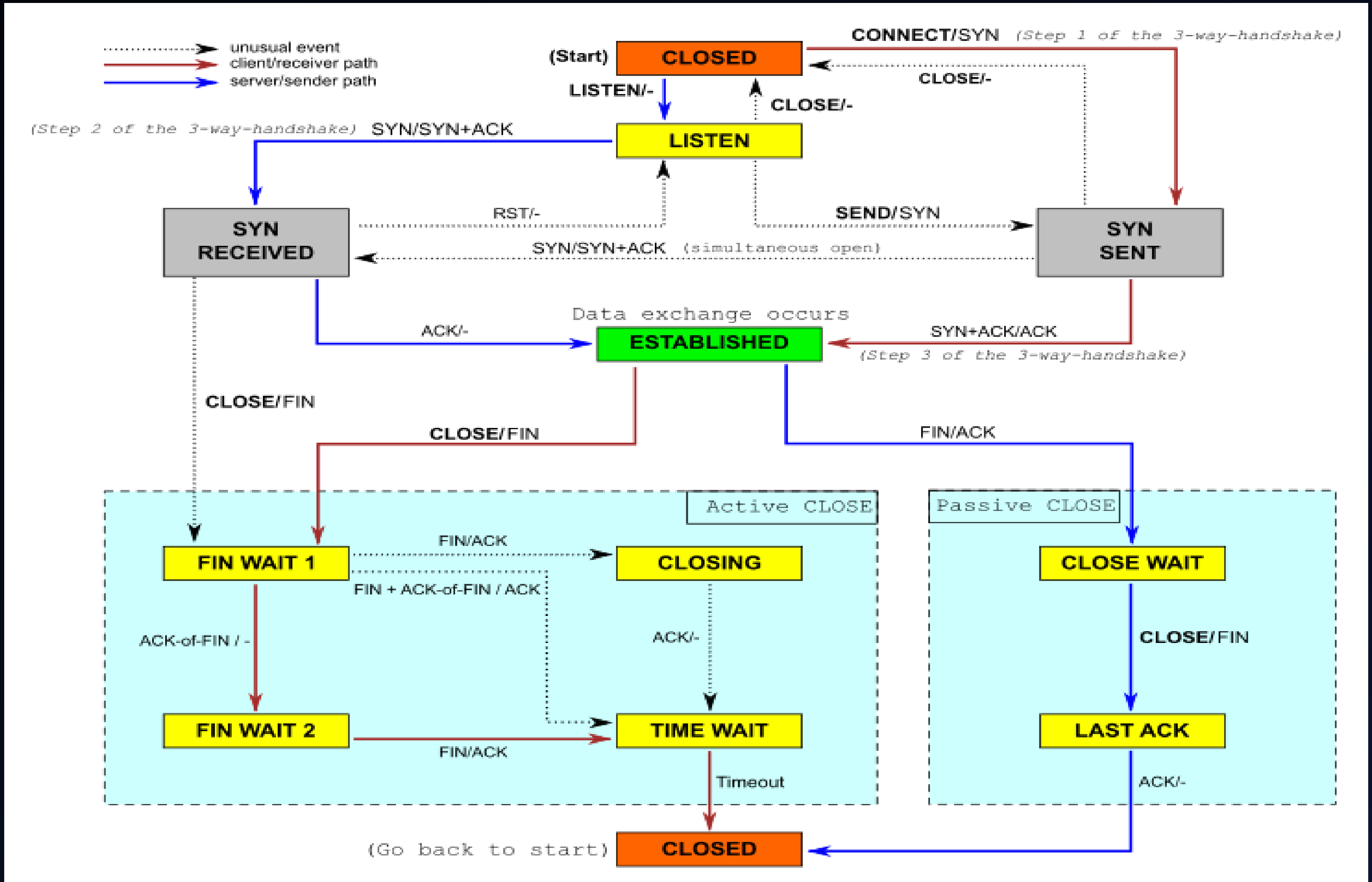
TCP Header


20-60 bytes
Header
Data
Source Port Address
16 bits
Destination Port Address
16 bits
Sequence Number
32 bits
Acknowledgement Number
32 bits
HLEN
4 bits
Reserved
6 bits
URG
ACK
PSH
RST
SYN
FIN
Window Size
16 bits
Checksum
16 bits
Urgent Pointer
16 bits
Options and Padding
Up to 40 bytes

TCP 3-Way Handshake



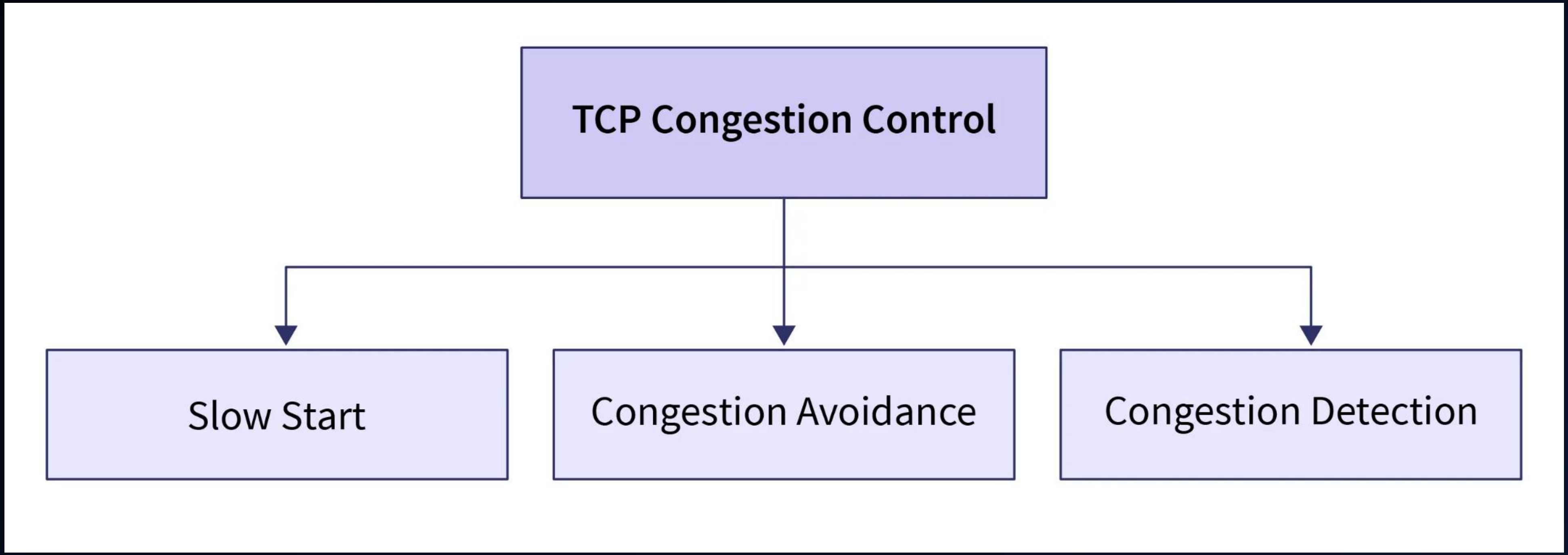
TCP State Transition



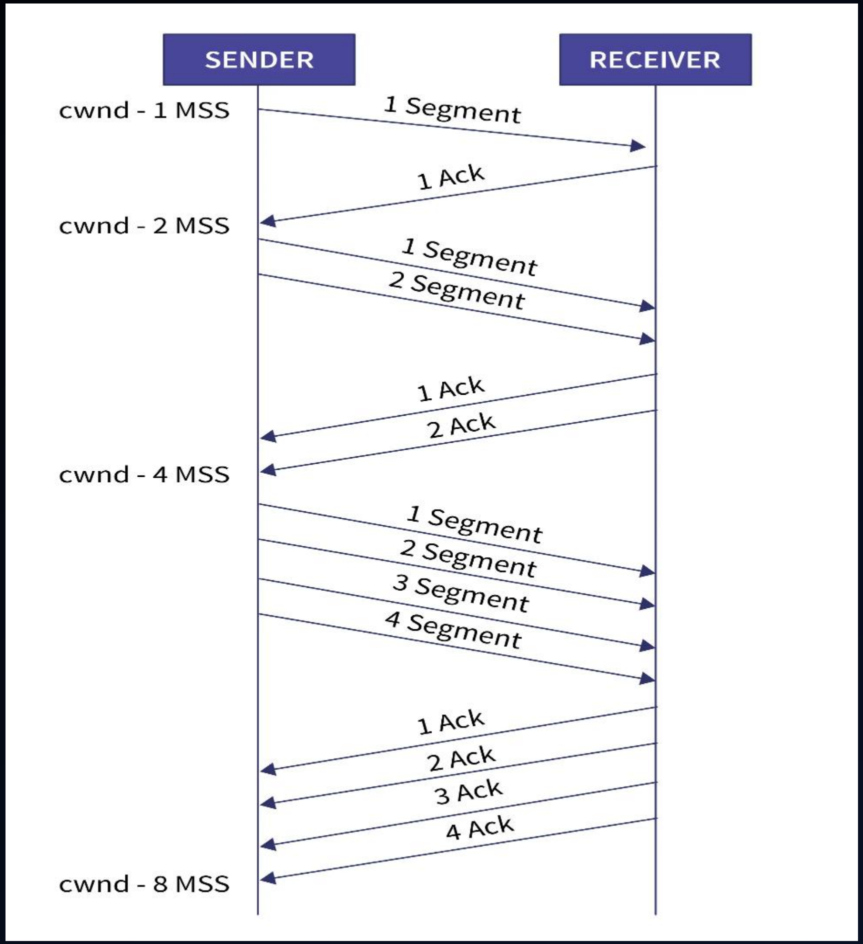
TCP Wrap Around Time

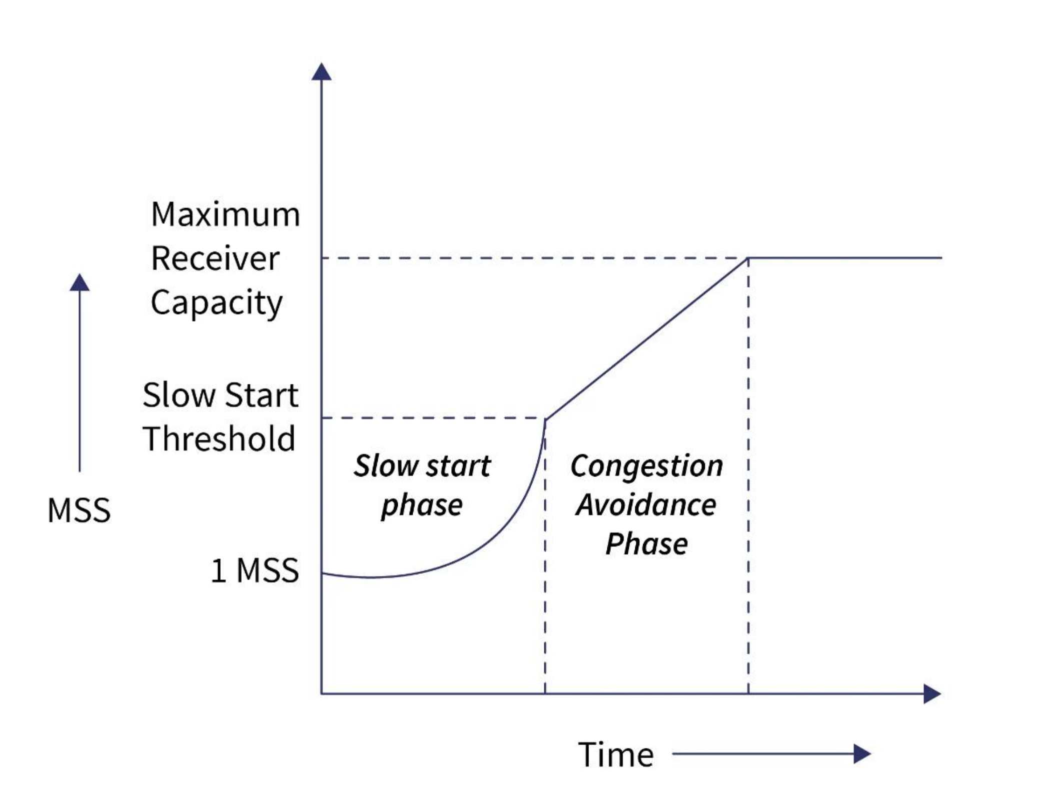
- Wrap Around time $= \dfrac{Total\ Sequence\ No(2^k)}{Bandwidth\ (B)}$
- Here we are assuming Sequence no field has k bits & Bandwidth is in Bytes/sec
- For lifetime of a packet $l\ sec$. minimum Sequence no required (in bits) = $l\ * B\ (\log_2 l * B)$

TCP Congestion Control

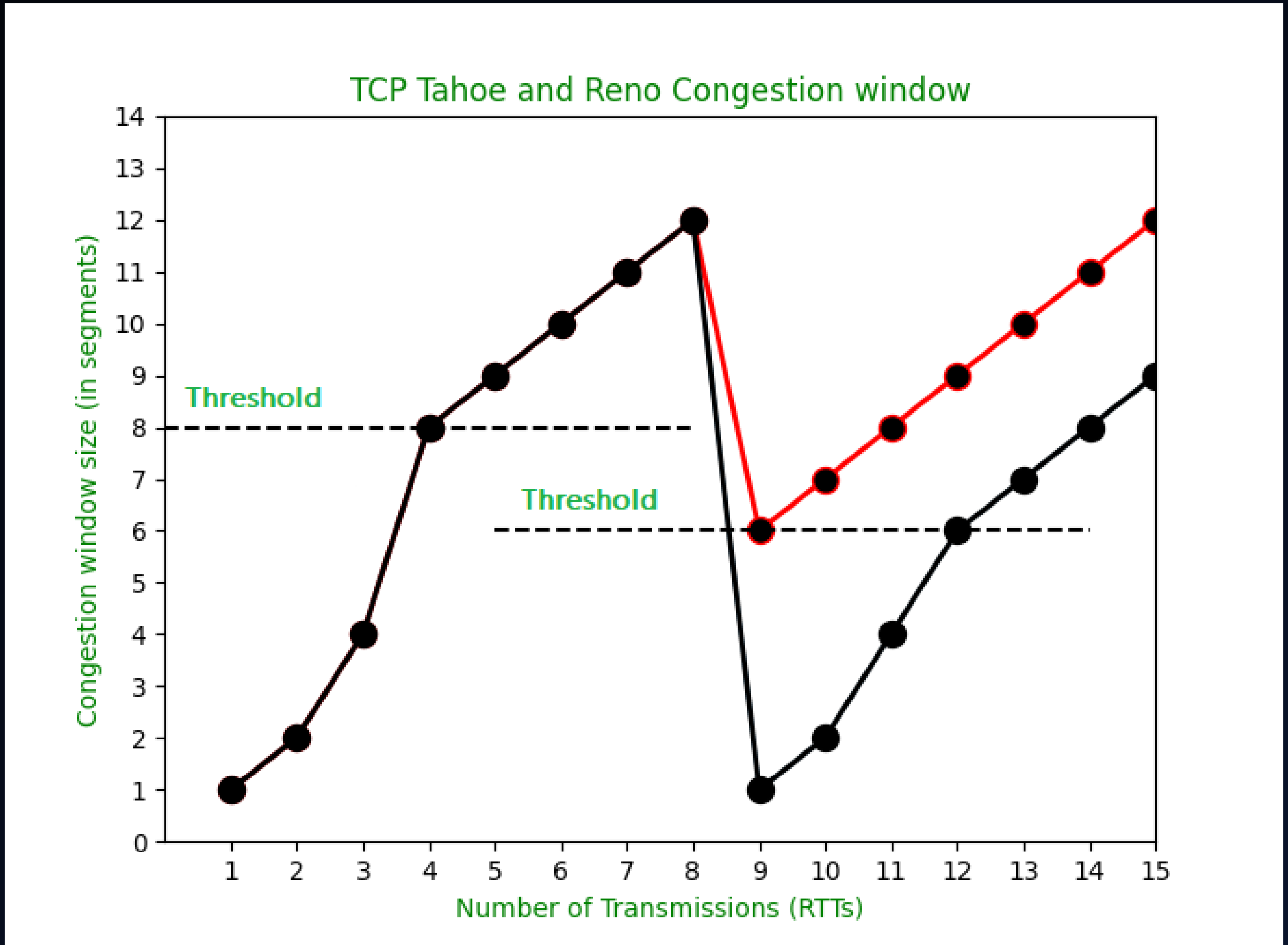


Congestion Control Phases

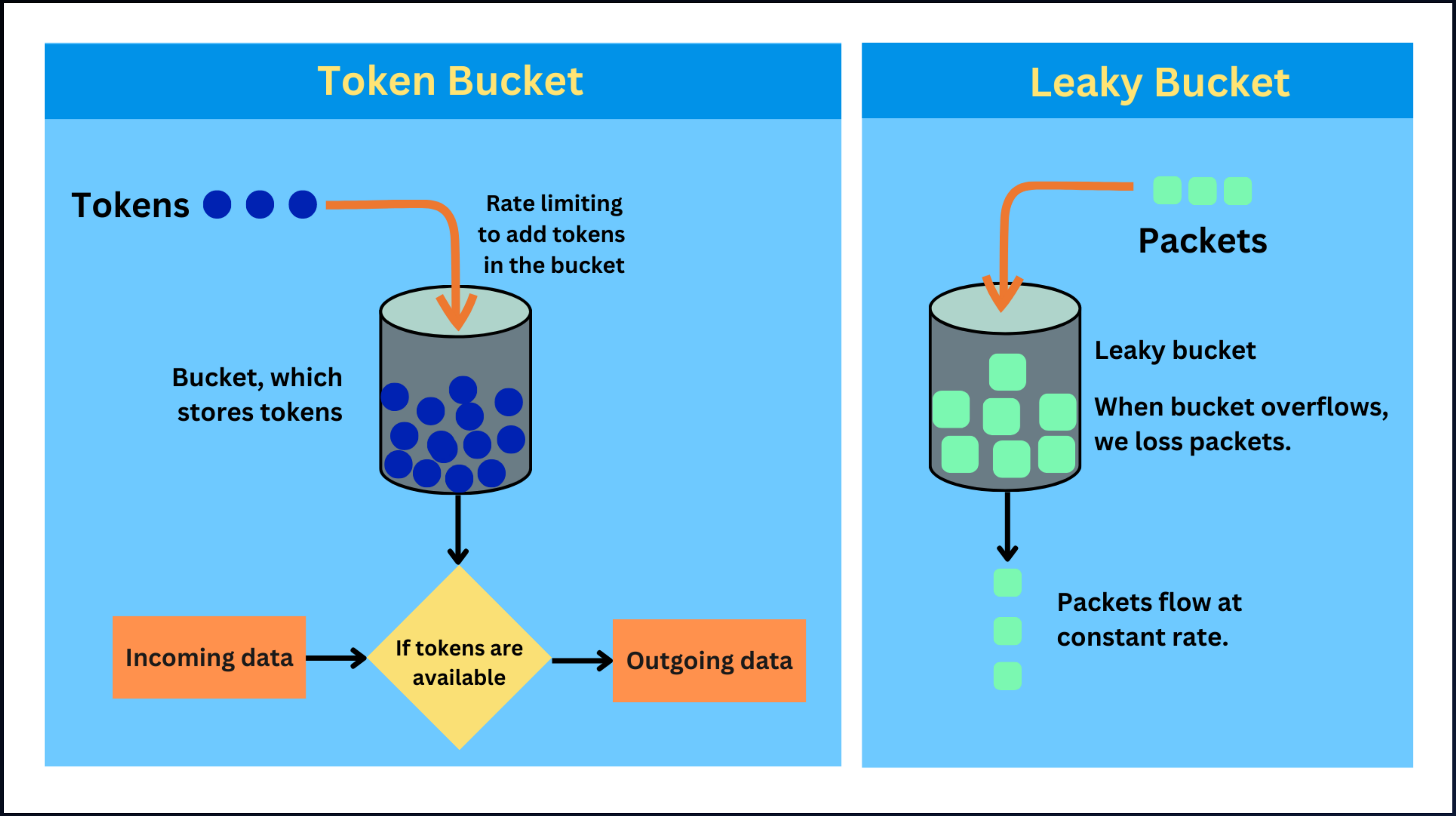




TCP Congestion Detection



Congestion Control Algorithms



Congestion Control Algorithms

LEAKY BUCKET

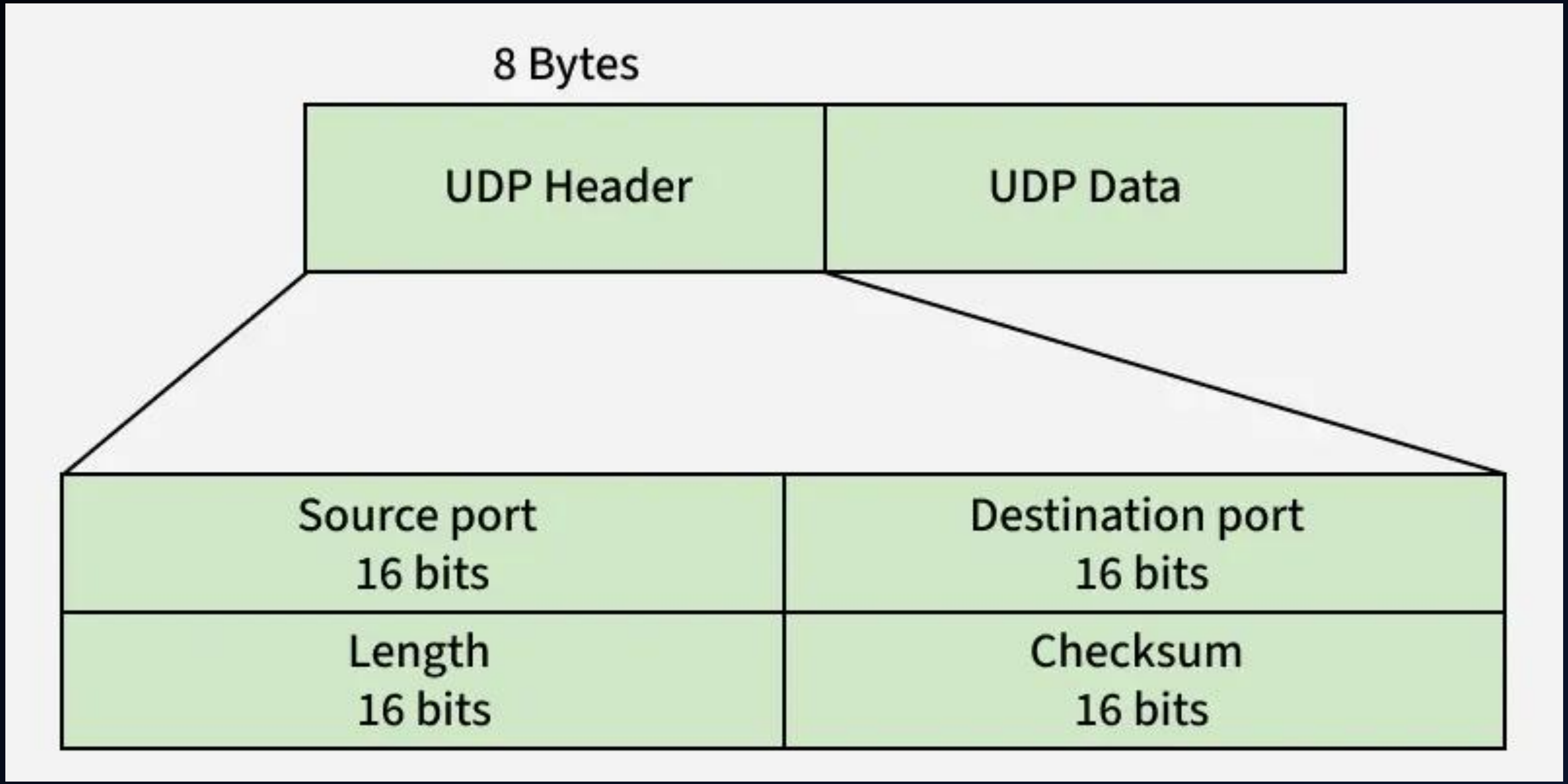
- Output rate (constant):
  $R_{out} = constant$
- Condition:
  - Input rate ≤ R_{out} → no packet loss
  - Input rate > R_{out} → packets dropped
- Queue constraint:
  $Queue\ size\ \leq\ Bucket\ capacity$

TOKEN BUCKET

- Let,
  - r = token generation rate (tokens/sec)
  - b = bucket capacity (tokens)
  - t = time interval (sec)
- Maximum data that can be sent in time t:

$$Data\ \leq\ b\ +\ r * t$$

UDP Header



8 Bytes
UDP Header
UDP Data
Source port
16 bits
Destination port
16 bits
Length
16 bits
Checksum
16 bits

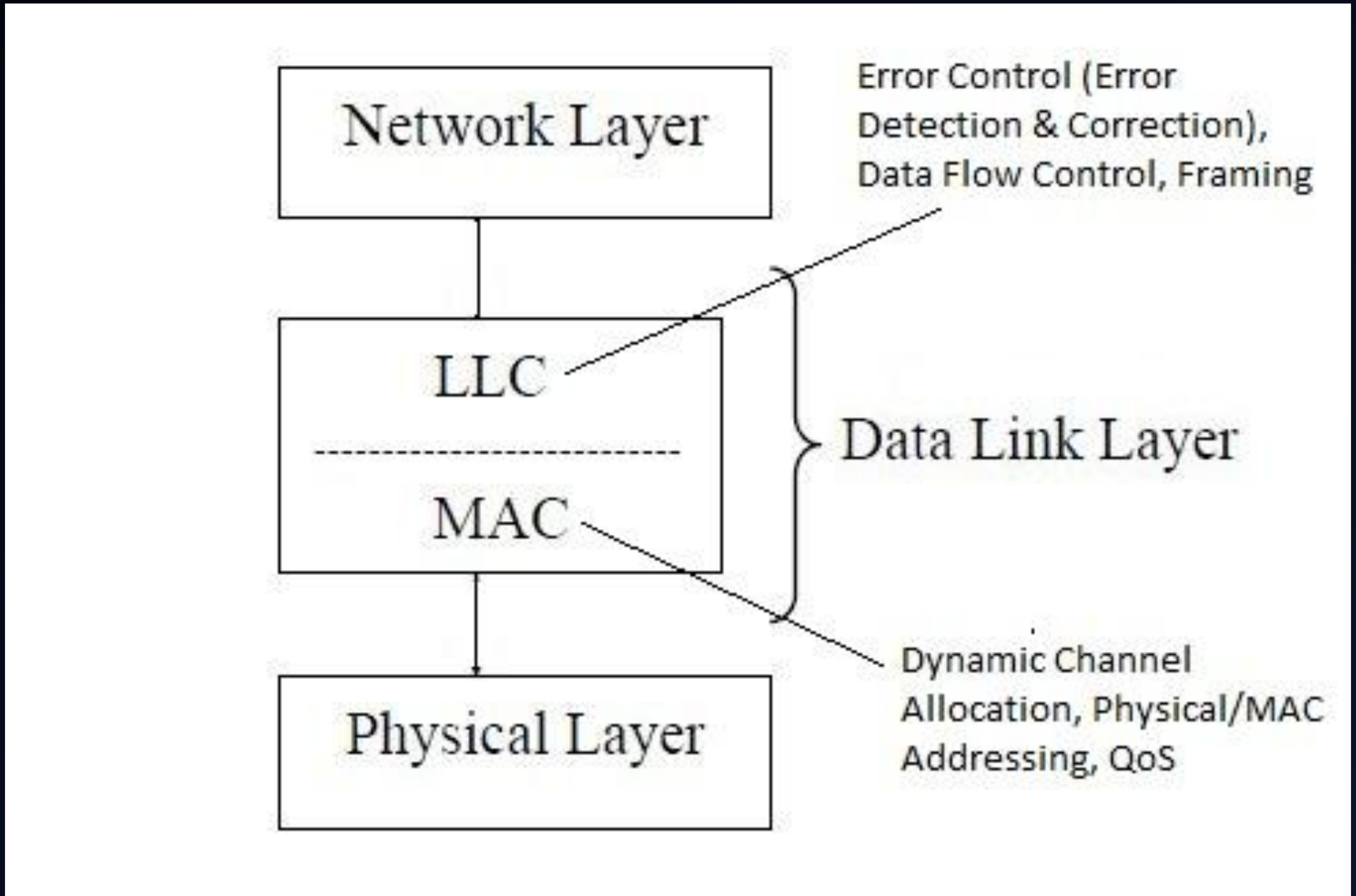
TCP vs UDP

TCP	UDP
Connected	Connectionless
State Memory	Stateless
Byte Stream	Packet/Datagram
Ordered Data Delivery	No Sequence Guarantee
Reliable	Lossy
Error Free	Error Packets Discarded
Handshake	No Handshake
Flow Control	No Flow Control
Relatively Slow	Relatively Fast
Point to Point	Supports Multicast
Security: SSL/TLS	Security: DTLS

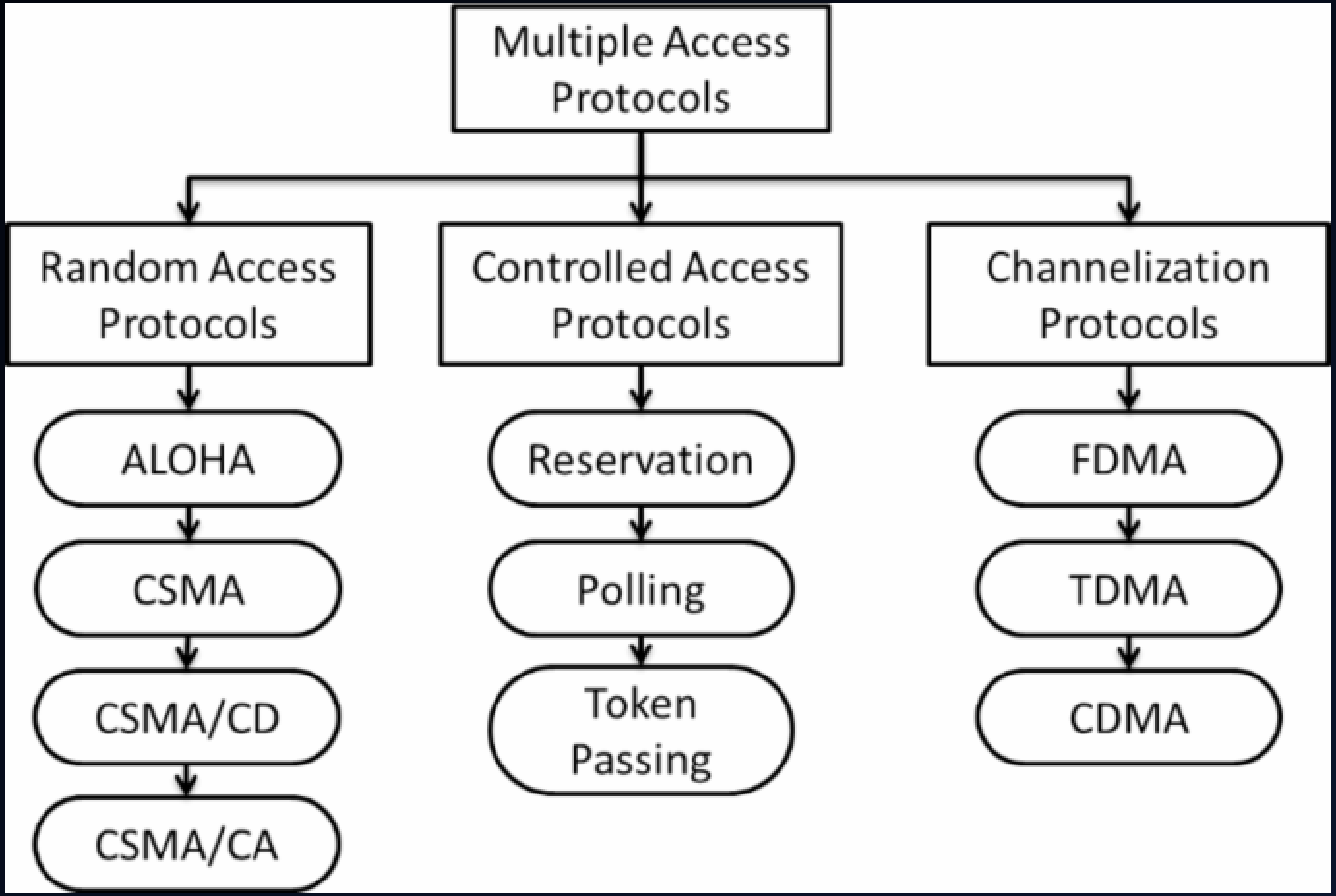
Medium Access Control

What’s Going On in the Medium Access Control Layer?

Where is the MAC Layer?



Multiple Access Protocols

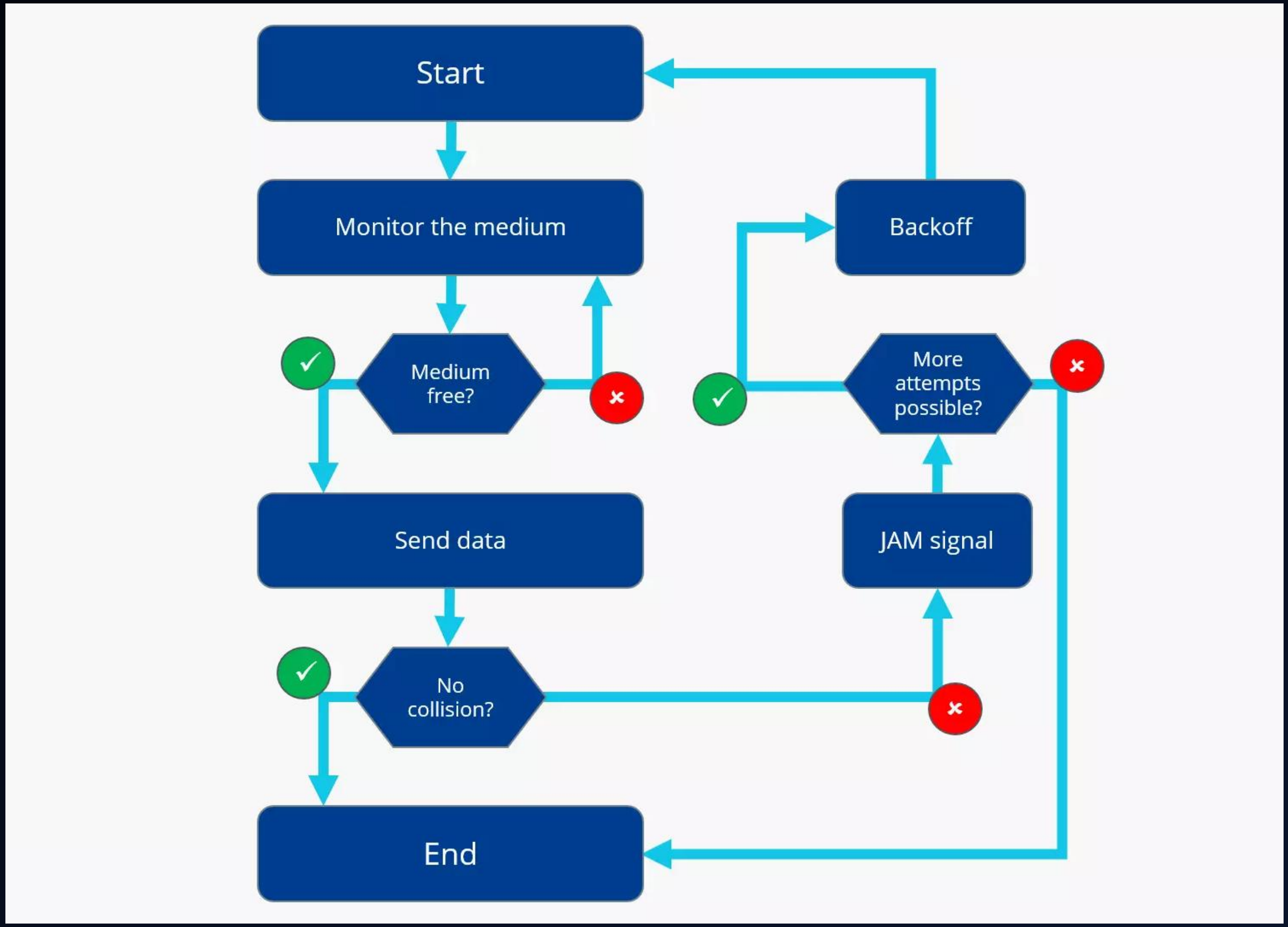


ALOHA

Differences between Pure ALOHA and slotted ALOHA

Pure ALOHA	Slotted ALOHA
Any Station can transmit data at any time.	Any station can transmit the data only at the beginning of any time slot.
Vulnerability time = 2 x Transmission time.	Vulnerability time = Transmission time.
The probability of successful transmission in Pure ALOHA is $G \times e^{-2G}$	The probability of successful transmission in Slotted ALOHA is $G \times e^{-G}$
The max probability of successful transmission in pure aloha occurs at G=½ and the value is $½ \times e^{-1}$ = 18.39%	The max probability of successful transmission in slotted aloha occurs at G=1, the value is $1 \times e^{-1}$ = 36.79%
Time is continuous and not synchronised.	Time is discrete and Synchronised.

Ethernet: CSMA/CD



CSMA/CD Binary Exponential Backoff

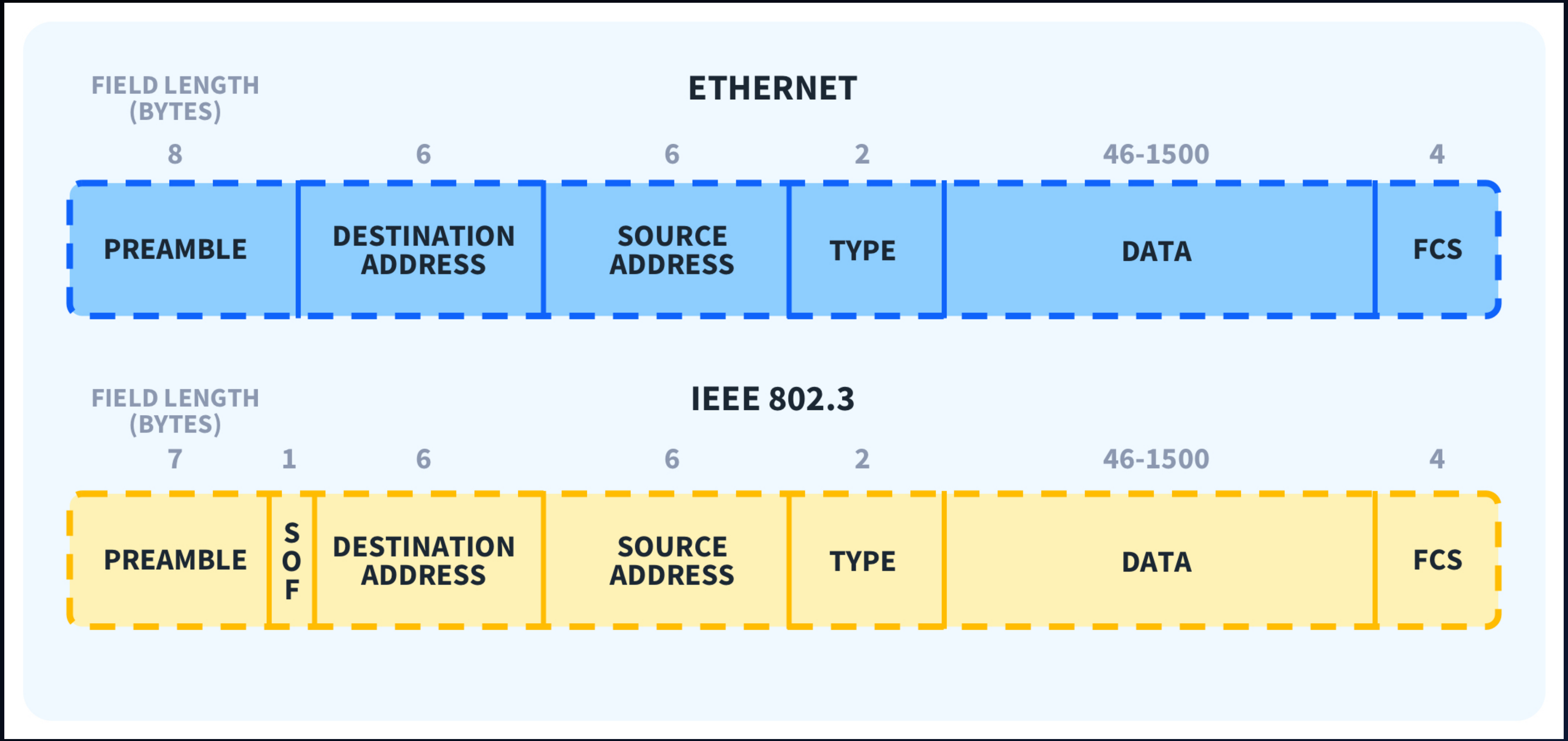
- After a collision, sender waits before retransmitting
- Collision detection condition:
- $T_d \geq 2P_d + T_{djam}$
  - Where T_d= frame transmission time, P_d= propagation delay, T_{djam}= jam signal transmission time

- Random backoff time:
  - Backoff = r × SlotTime, where r ∈ {0, 1, 2, … , 2^k− 1} (Let k = number of collisions (max 10 for backoff))
  - SlotTime: SlotTime = 2 × propagation delay
  - SlotTime = 51.2 µs (Ethernet)

- Probability of successful transmission: $P(success) = n * p * (1 - p)^{n-1}$
  - Where n = number of active nodes, p = probability that a node transmits

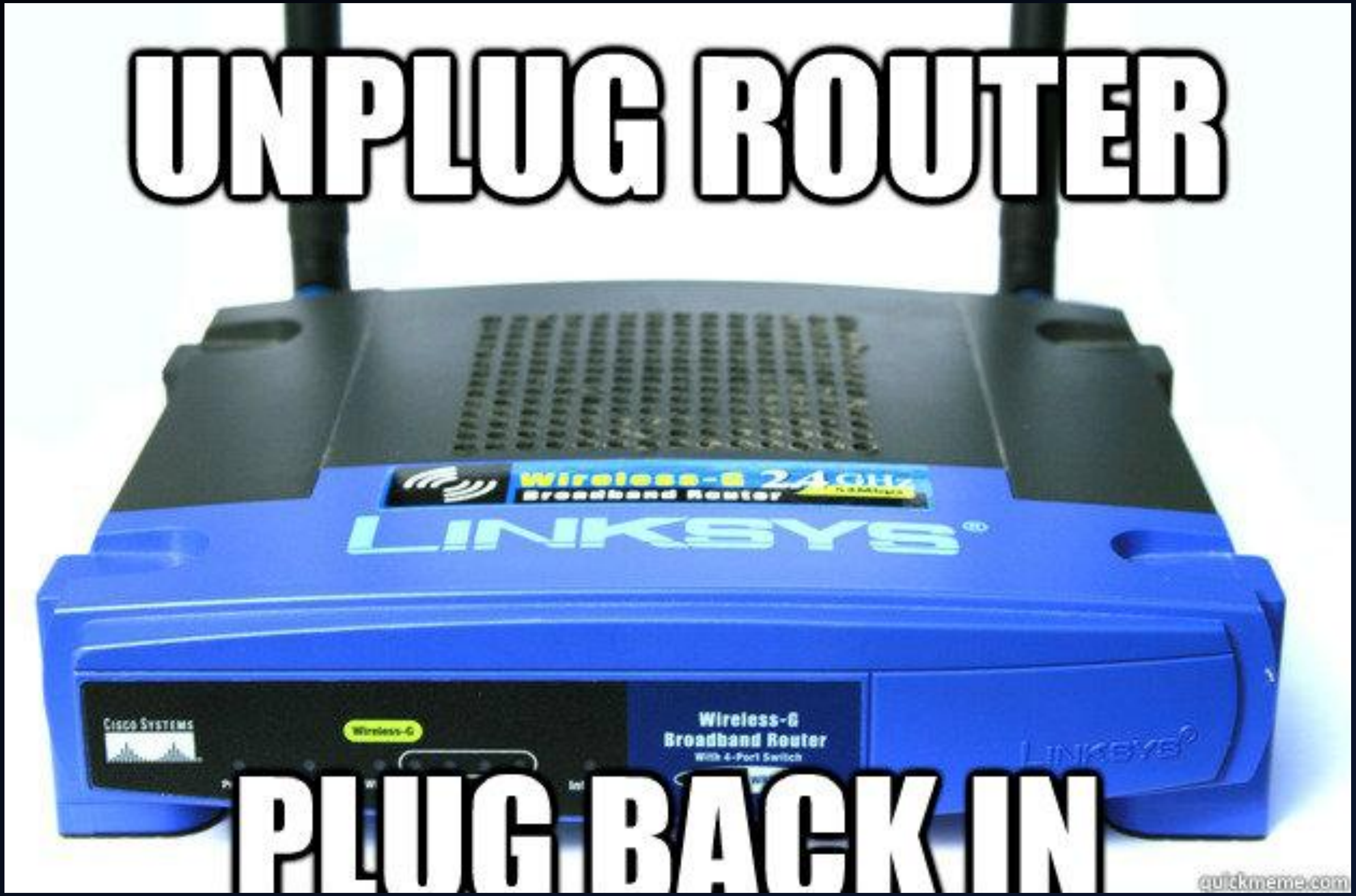
- After 16 collisions → transmission aborted

Ethernet Frame

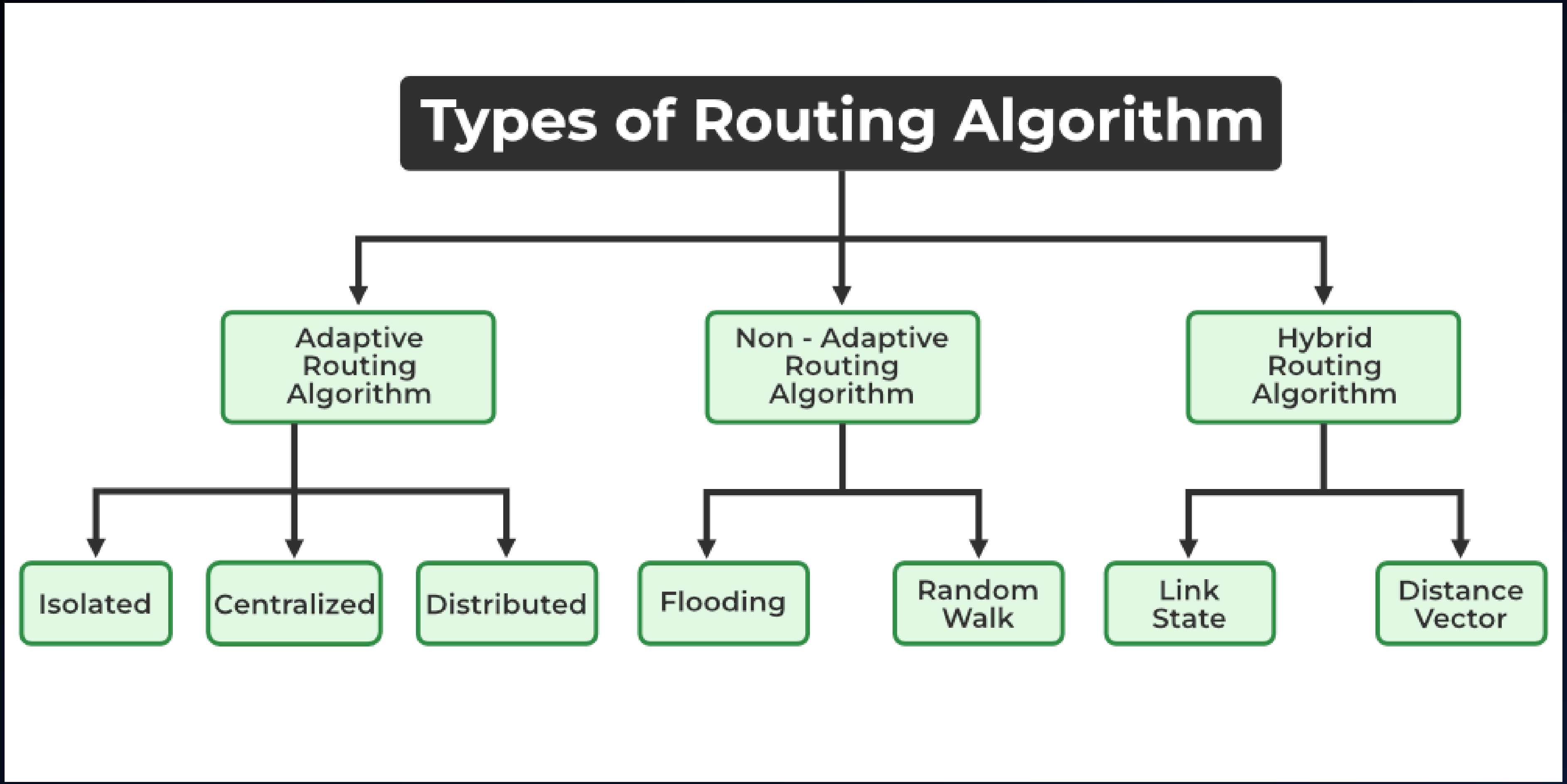


Routing, Switching, IP Support Protocol

How Does a Packet Get Routed in a Network?

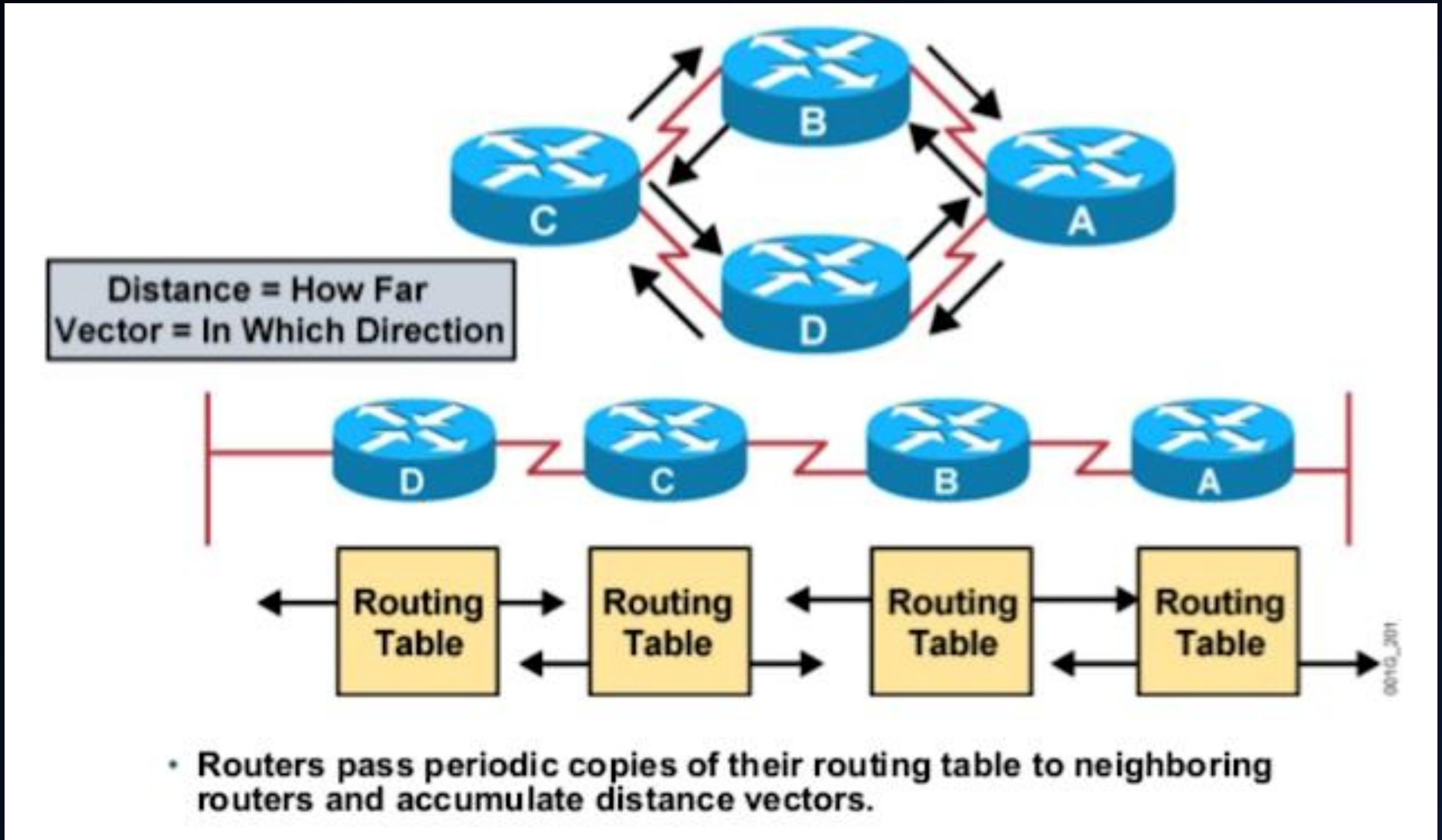


Routing Algorithms

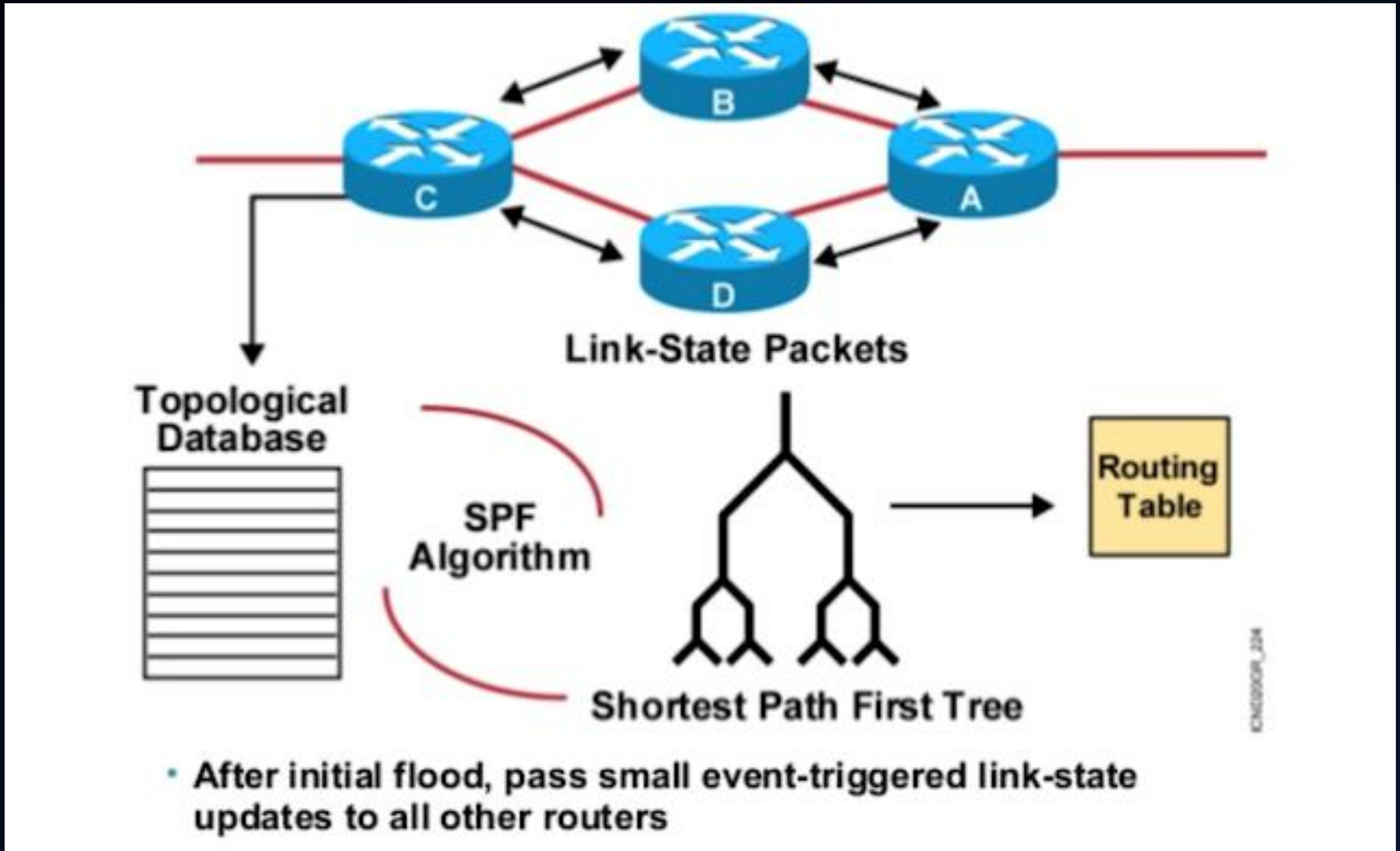


Flooding

Distance Vector Routing



Link State Routing

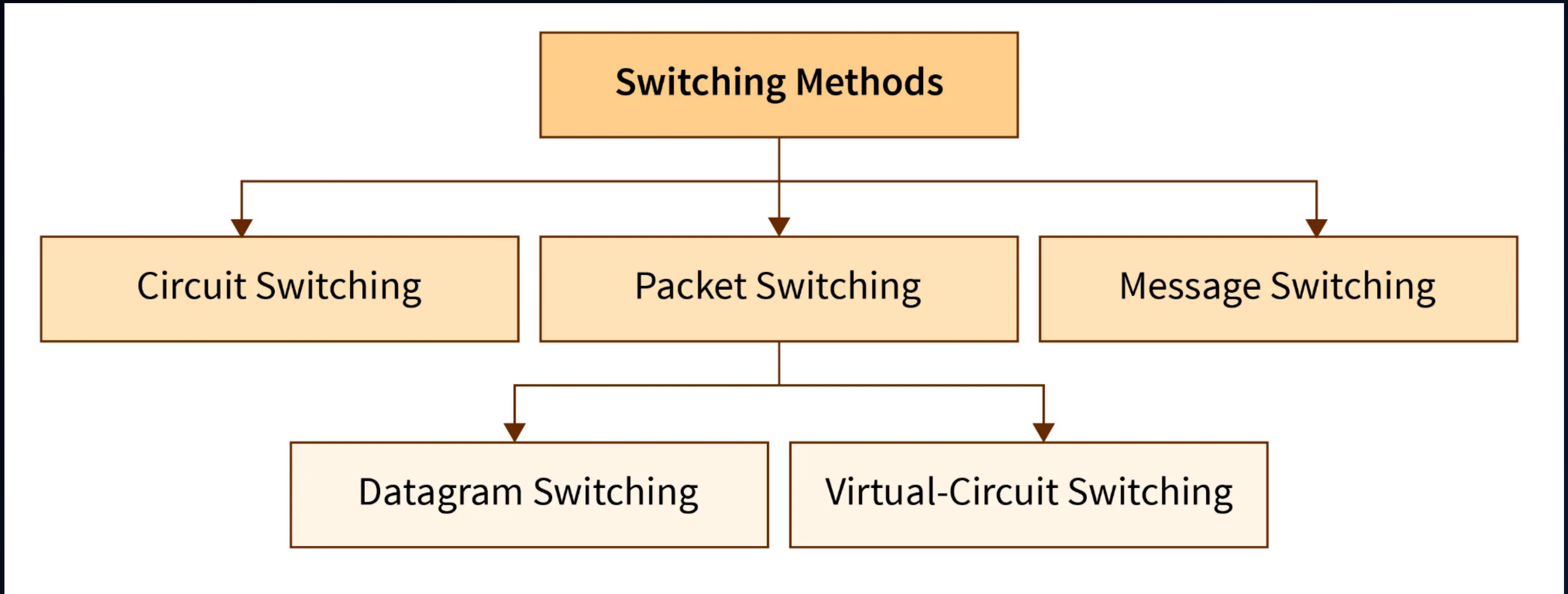


Distance Vector vs Link State Routing

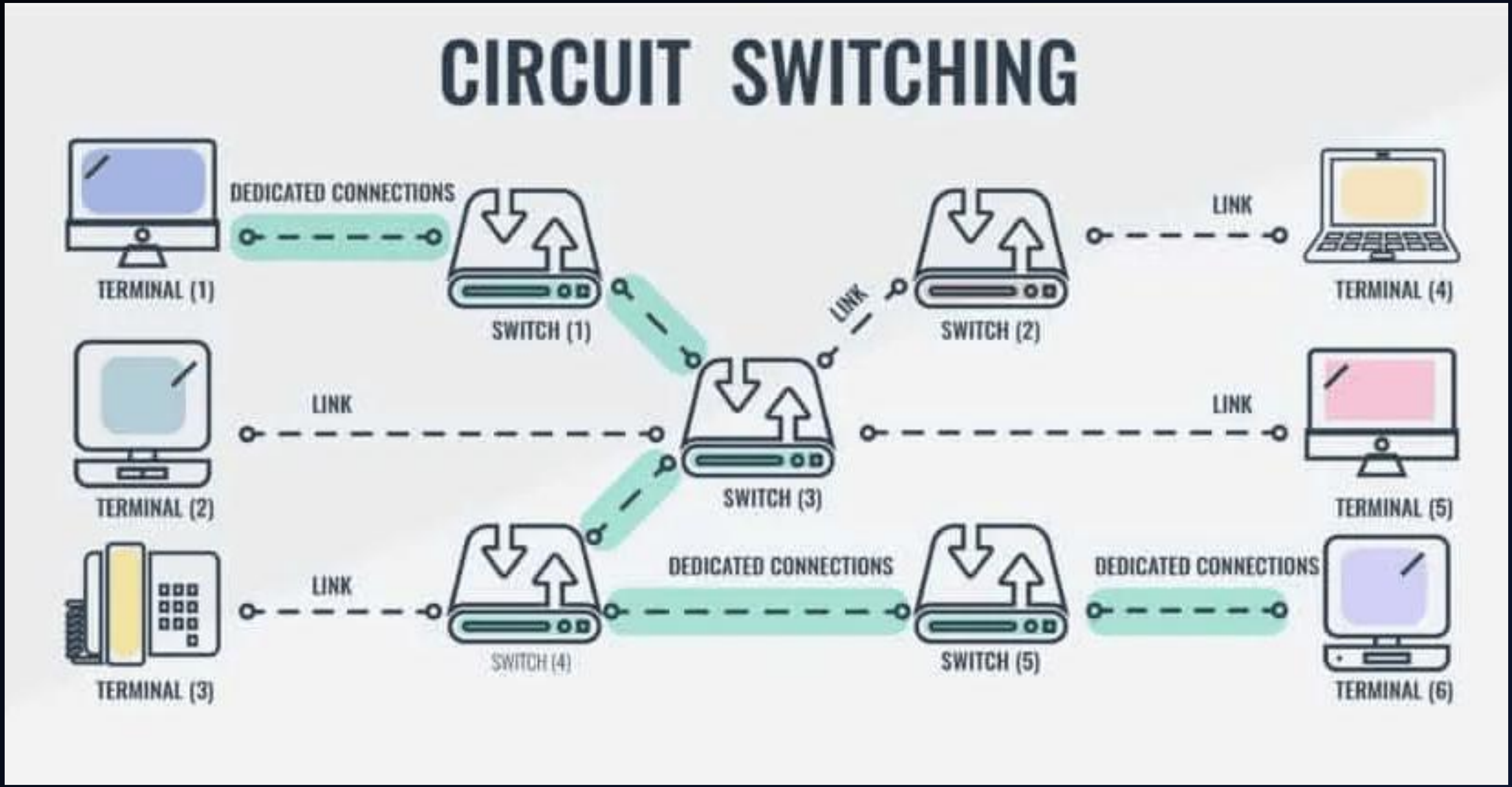
Features	Distance Vector	Link State
Convergence	Slow	Fast
Updates	Frequently	Event Triggered
Loops	Prone to routing Loops	Less Subjected to Routing Loops
Configuration	Easy	Difficult
Network Types	Broadcast for updates sent	Multicast for updates sent
Topology	doesn't know Network Topology	Knows entire Network Topology
Automatic Route Summarization	No	Yes
Path Calculation	Hop Count	Shortest Path -Metric
Scalability	Limited	Can be highly scalable
Protocols	RIP, IGRP	OSPF, IS-IS
Algorithm	Bredford Algorithm	Dijkstra-algorithm
Manual Route Summarization	Yes	Yes
Metric	Hop Count	Link Cost

Do Packets Really Hop Between Routers?

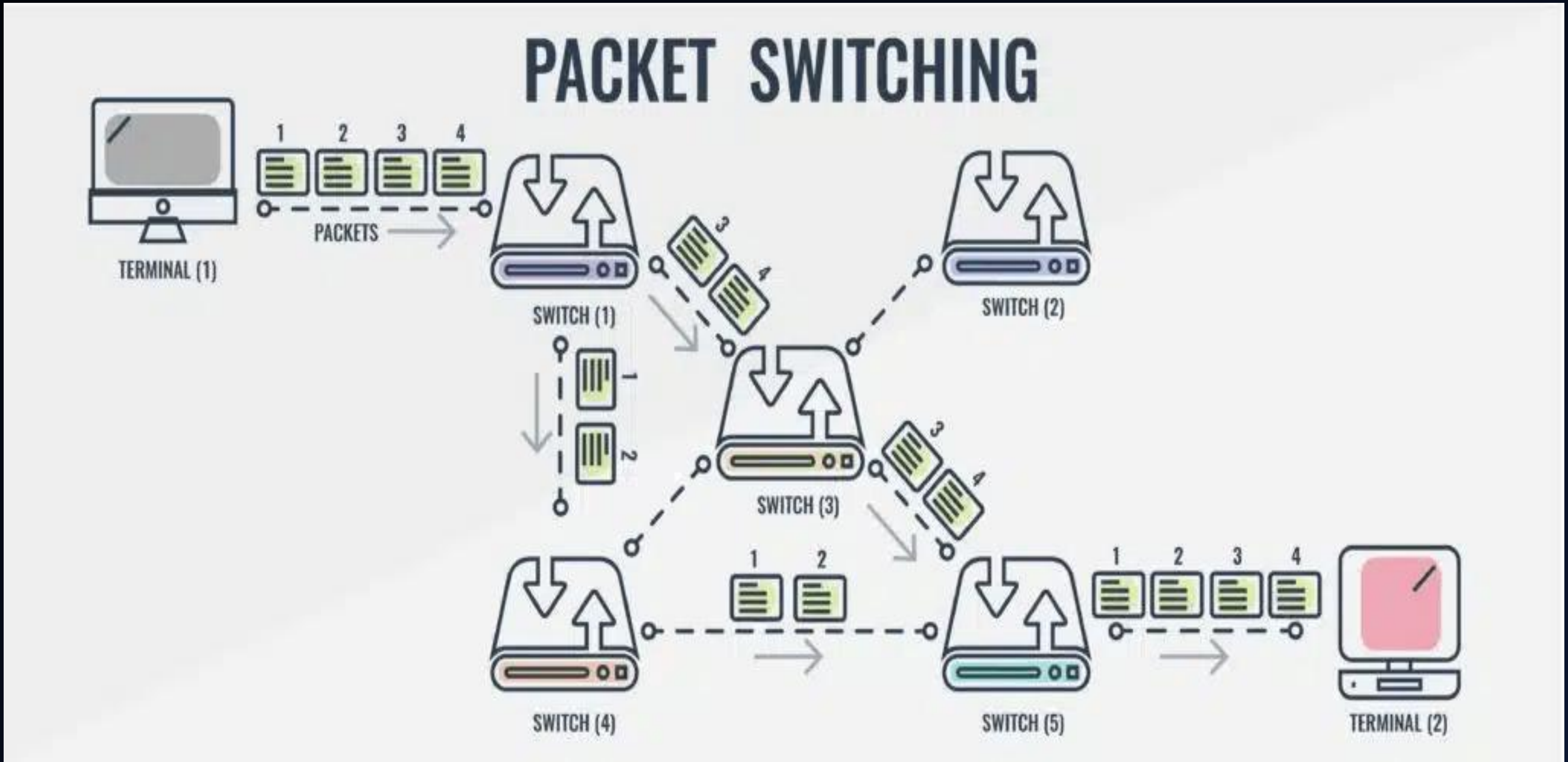
Switching Methods



Circuit Switching



Packet Switching



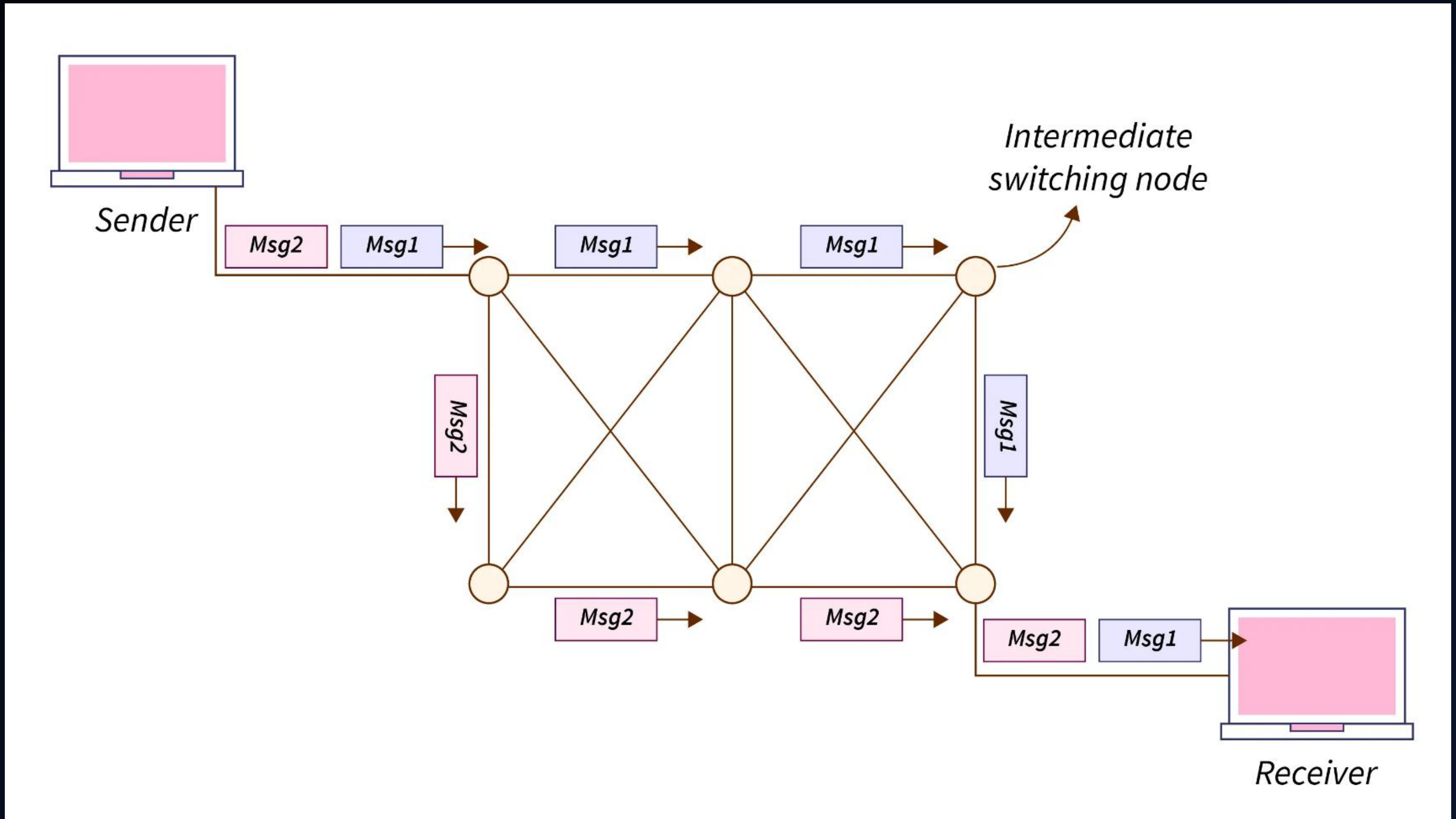
Circuit Switching vs Packet Switching

Circuit Switching	Packet Switching
Connection Oriented	Connection Less
Entire Message Have to follow same route during transmission	Entire Message can be divided and routed Independently
Implemented at Physical Layer	Implemented at Network Layer
Waste of bandwidth if Idle	No Waste of bandwidth if Idle
Initially designed for Voice Transmission	Initially designed for Data Transmission

Datagram vs Virtual-Circuit Packet Switching

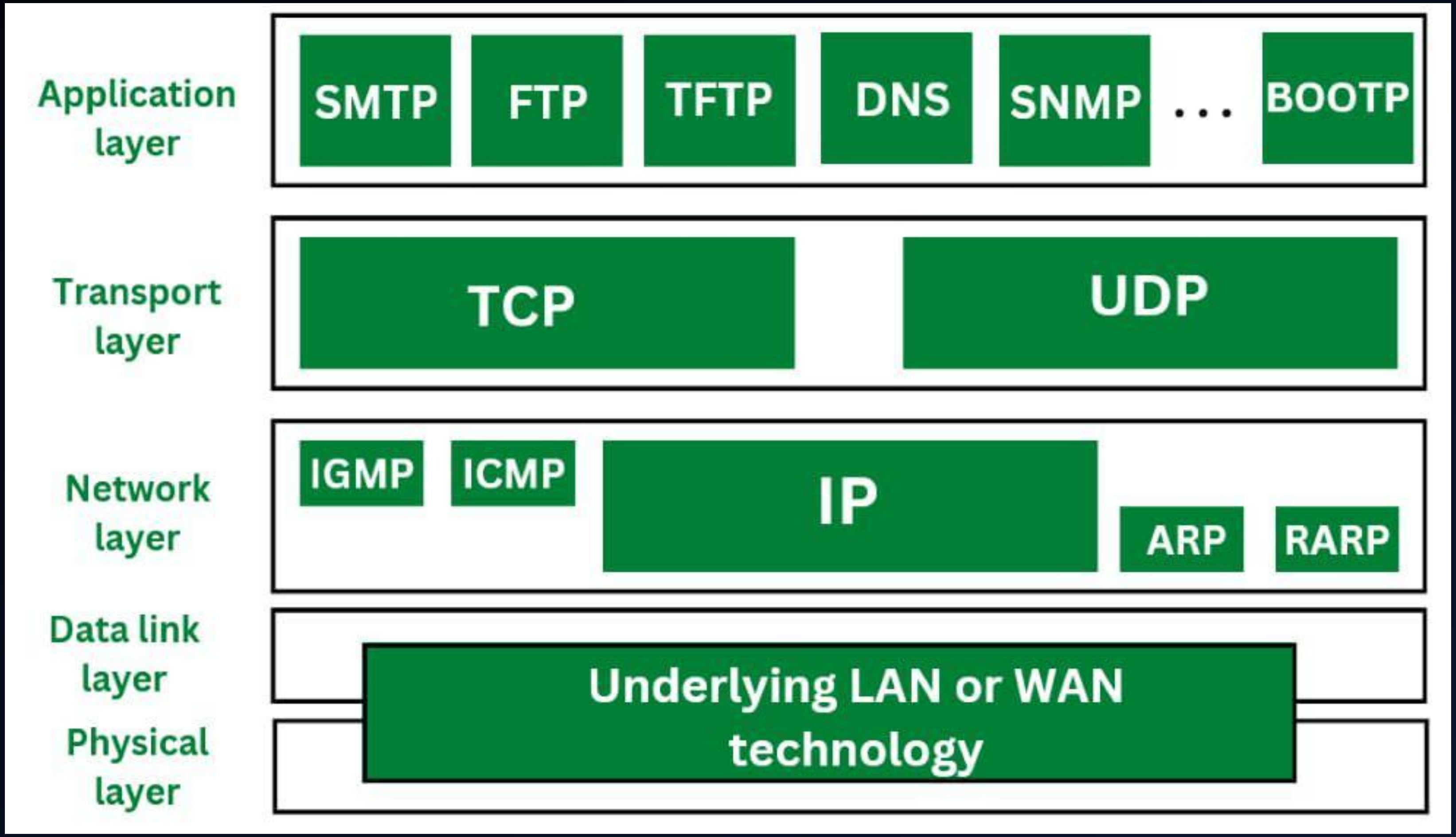
Datagram Packet Switching	Virtual-circuit Packet Switching
Two packets of the same user pair can travel along different routes.	All packets of the same virtual circuit travel along the same path
The packets can arrive out of sequence	Packet sequencing is guaranteed
Packets contain full Source, Destination addresses	Packets contain short VC Id. (VCI)
Each host occupies routine table entries	Each VC occupies routing table entries
Requires no connection setup	Requires VC setup. First packet has large delay
Also called Connection less	Also called connection oriented
Eg. Internet which uses IP Network protocol	Examples: X.25 and Frame Relay

Message Switching

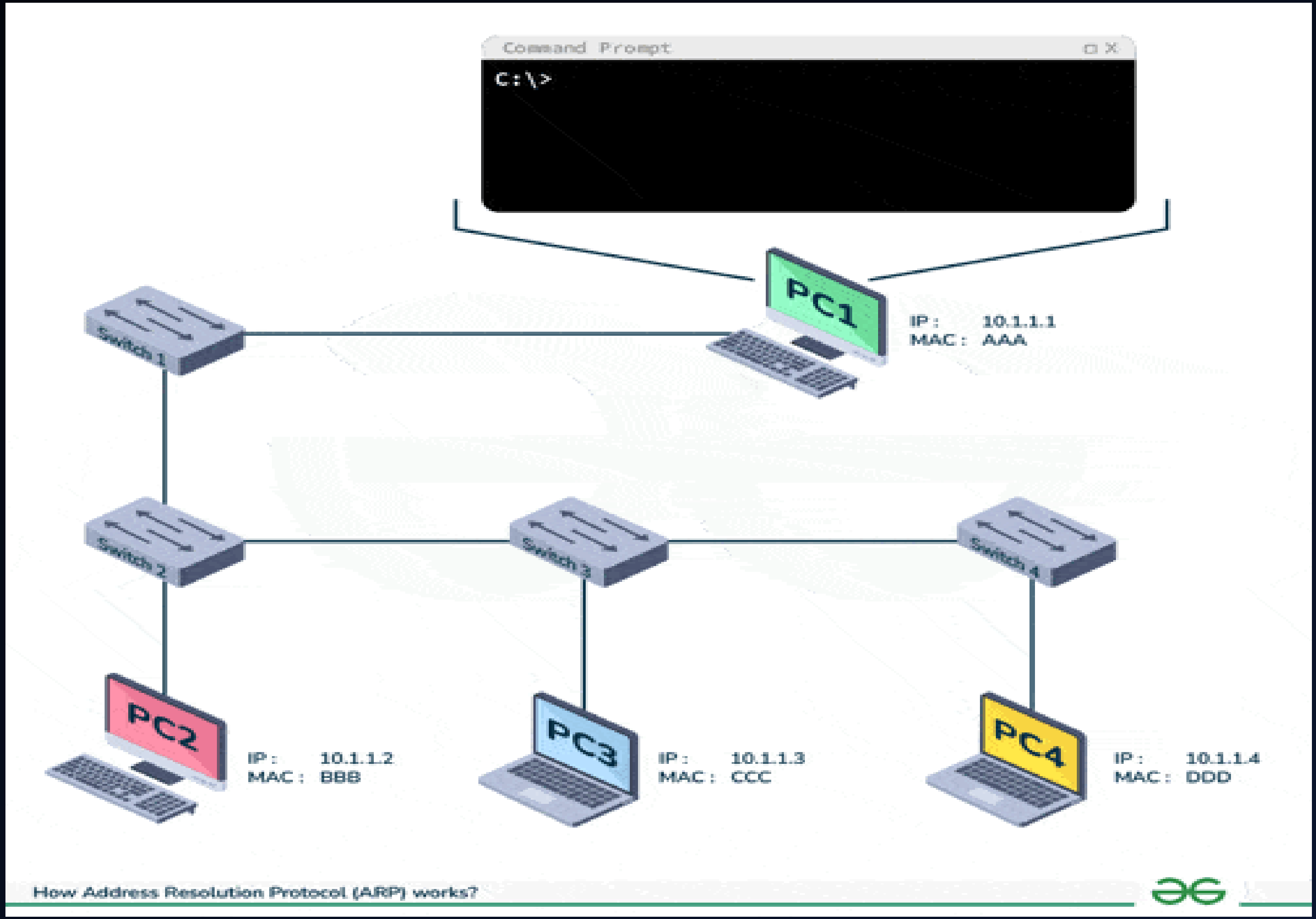


Does IP Need Supporting Protocols?

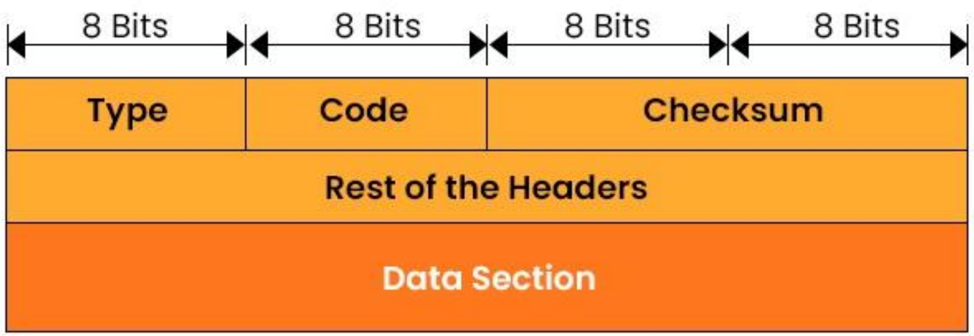
Network Layer Protocols



Address Resolution Protocol



Internet Control Message Protocol

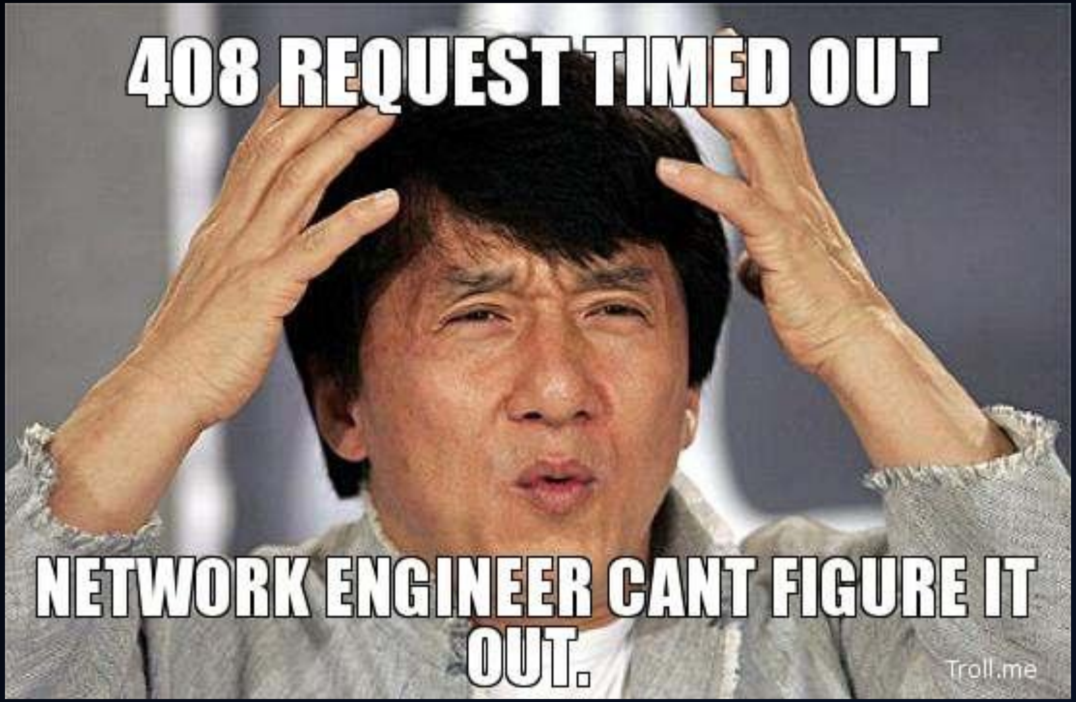


ICMP Message Format

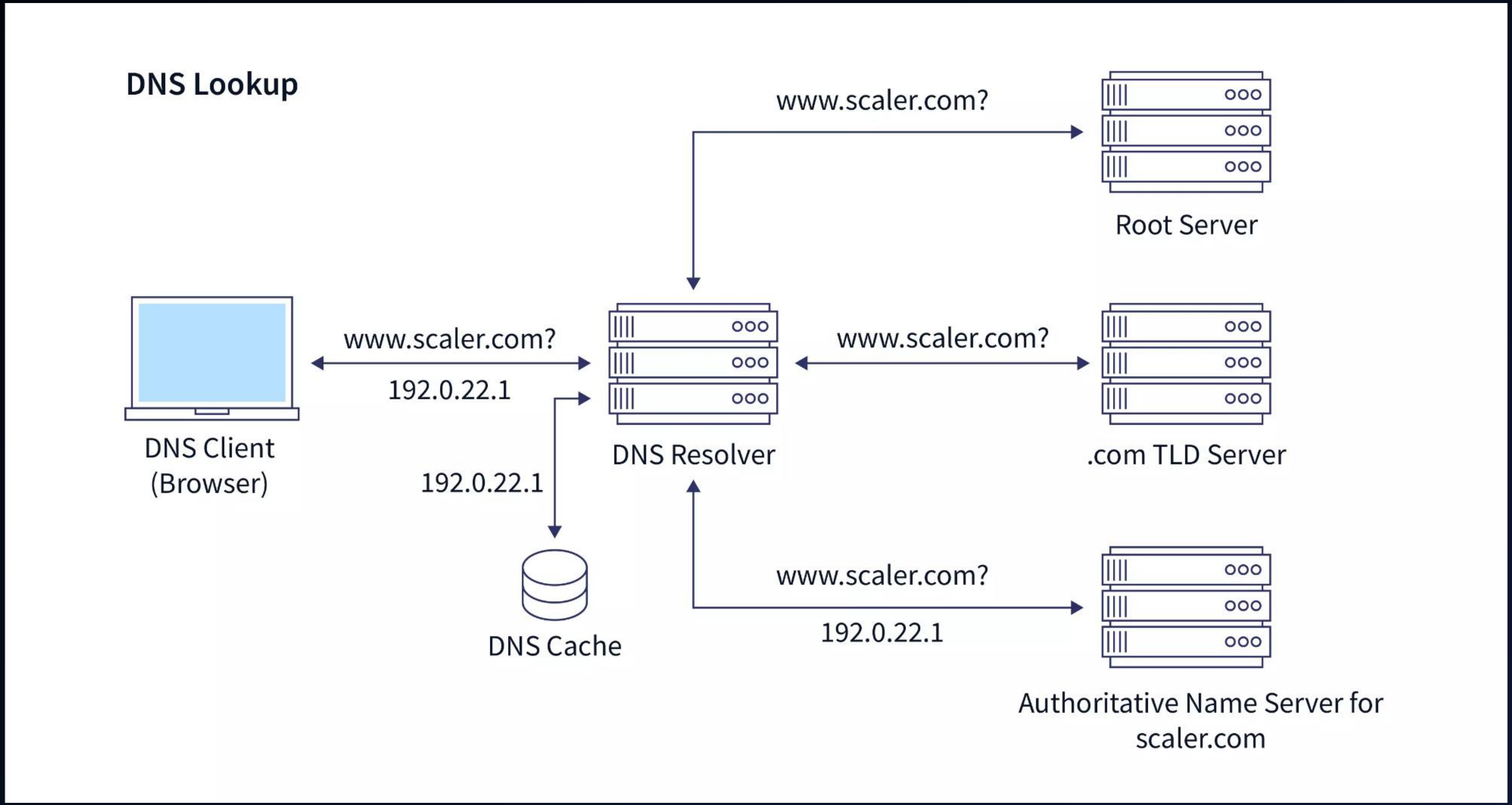
Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

Application Layer

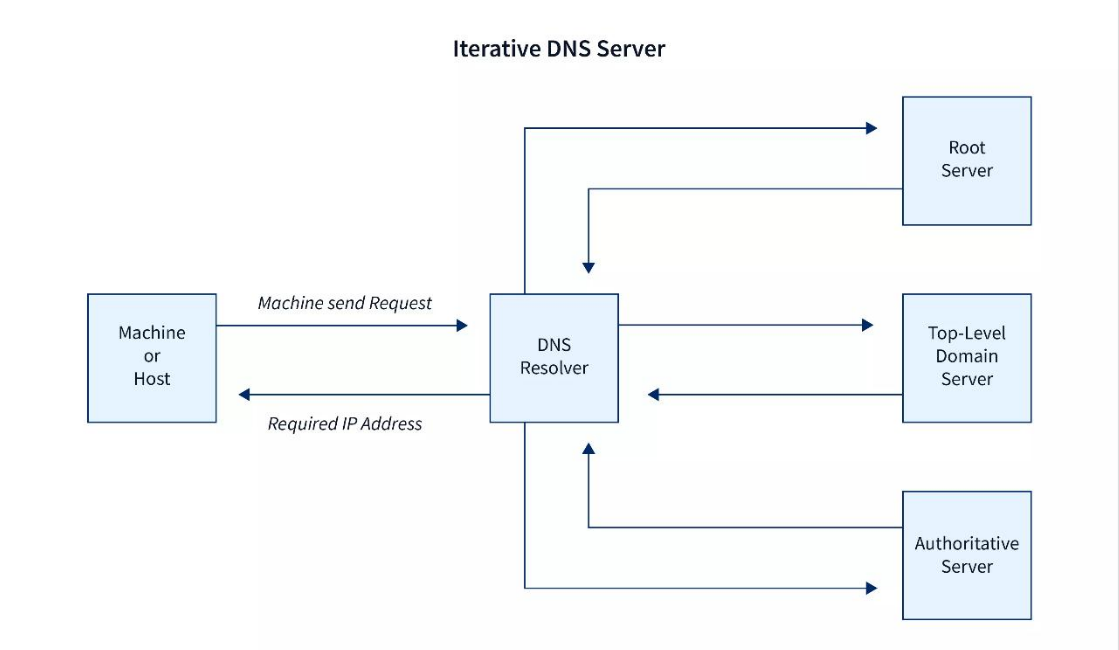
Why Is This Layer Called the Application Layer?

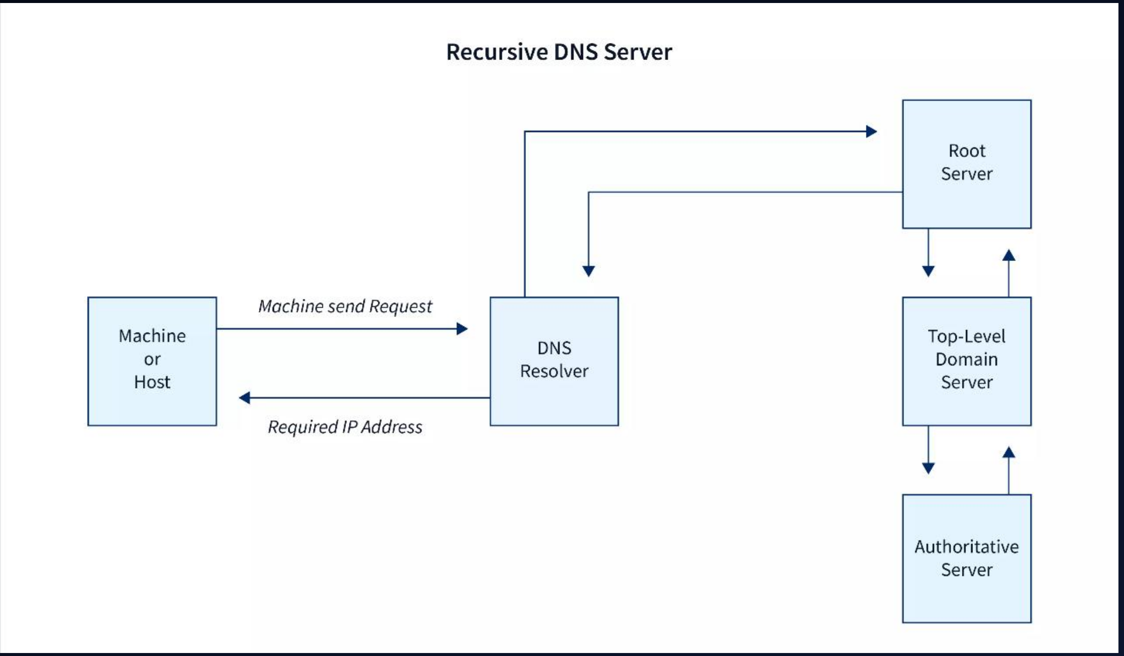


How DNS works?

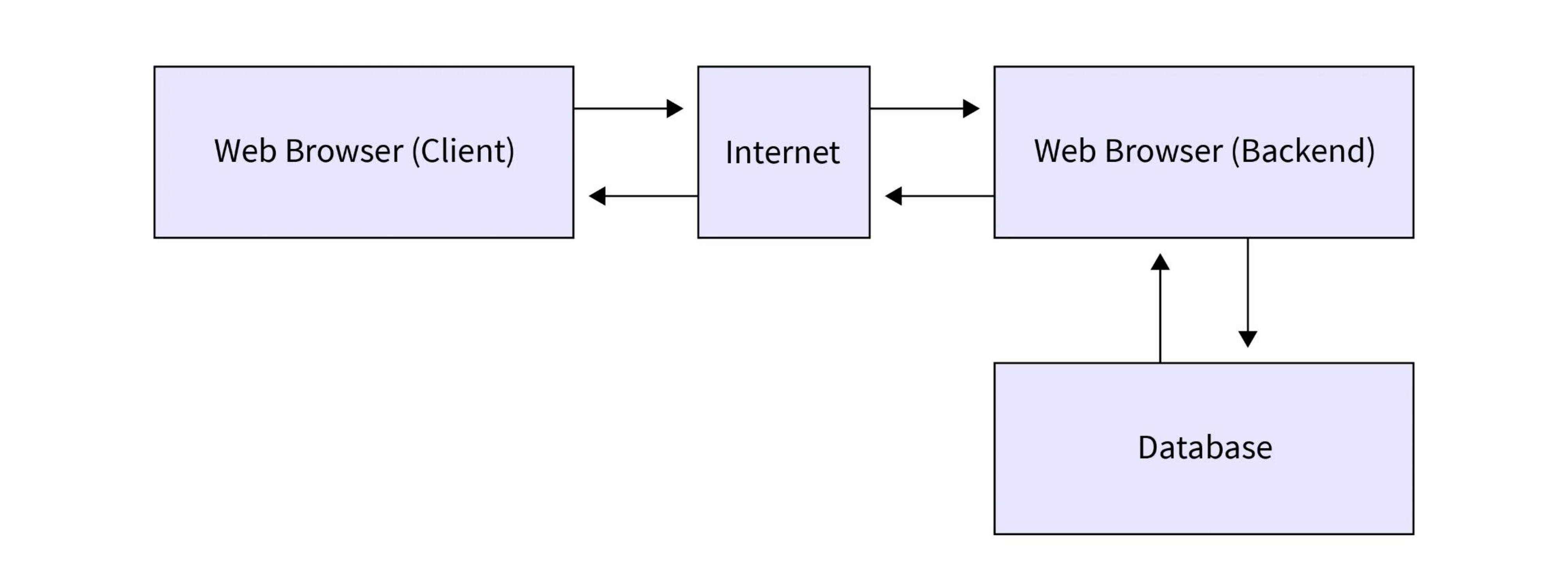


Types of DNS Lookup

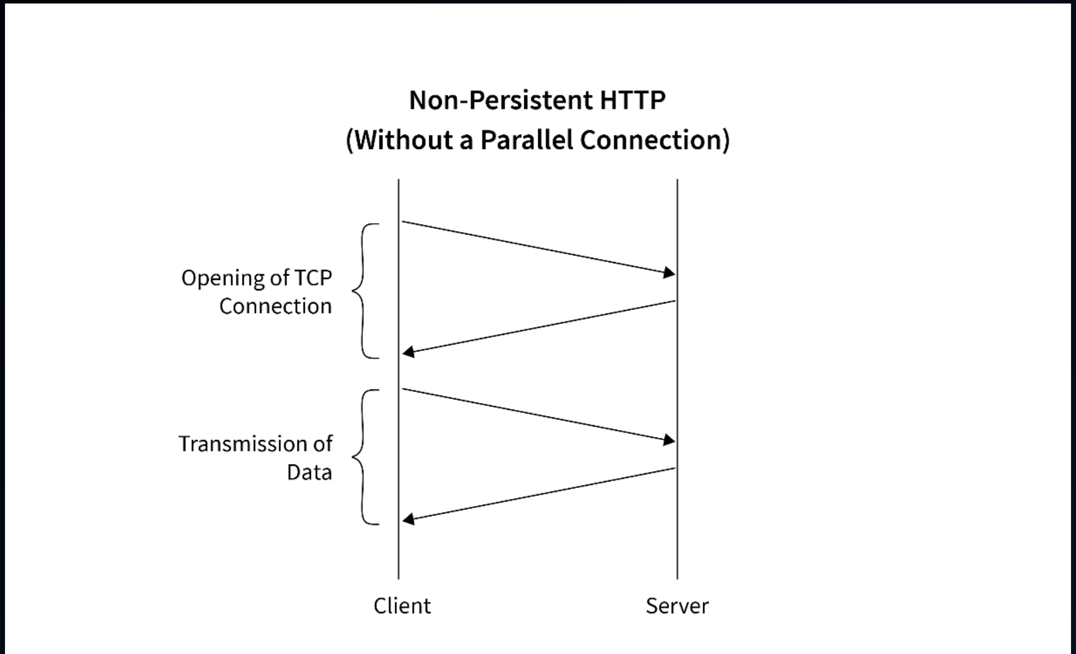


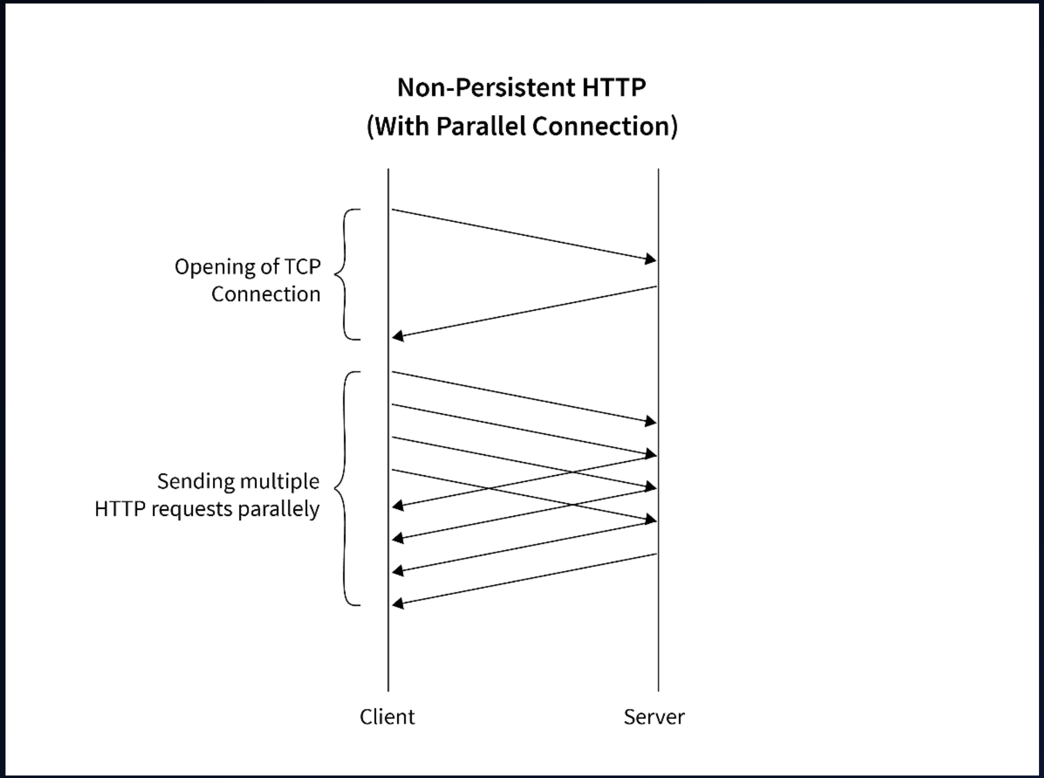


How HTTP works?

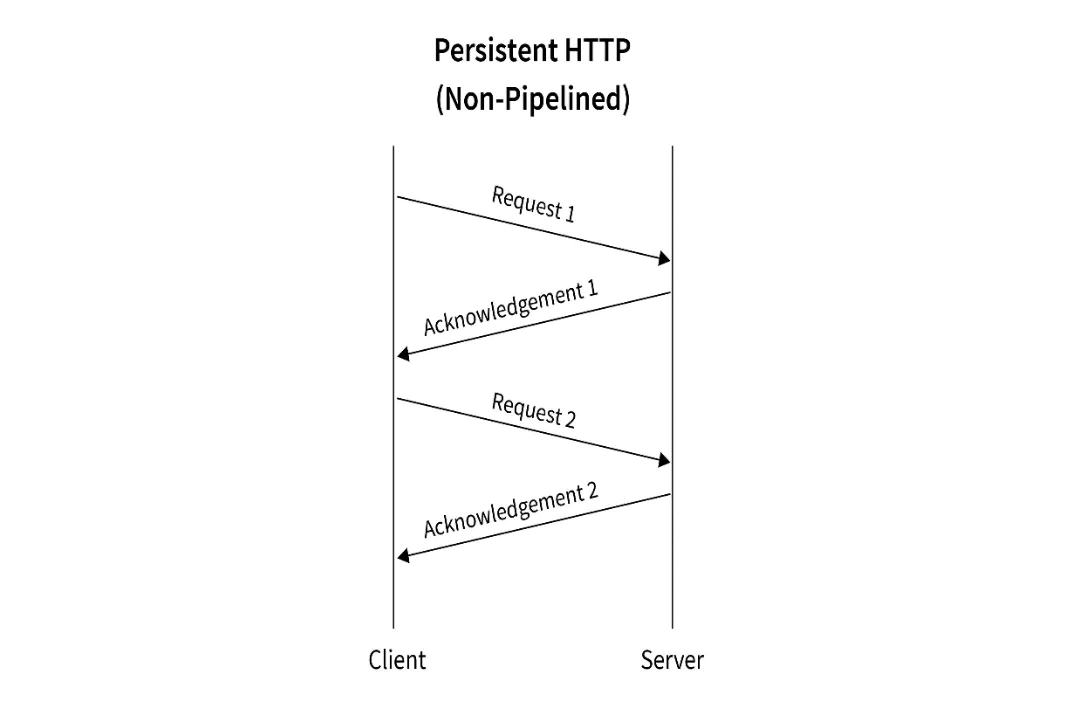


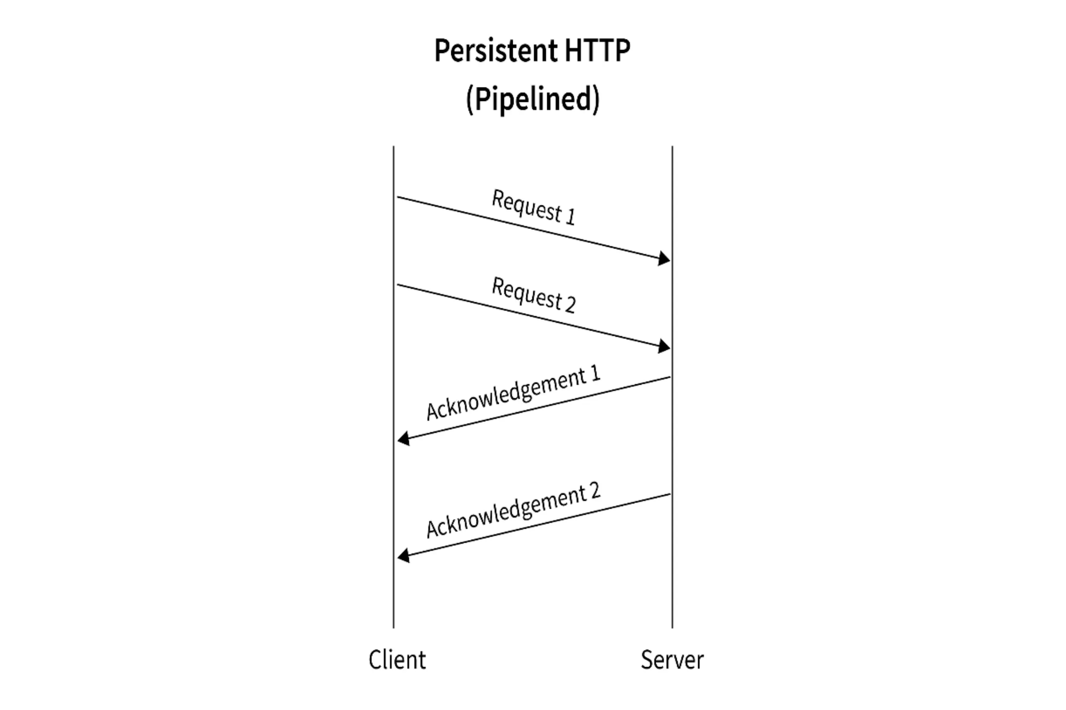
Non-Persistent HTTP



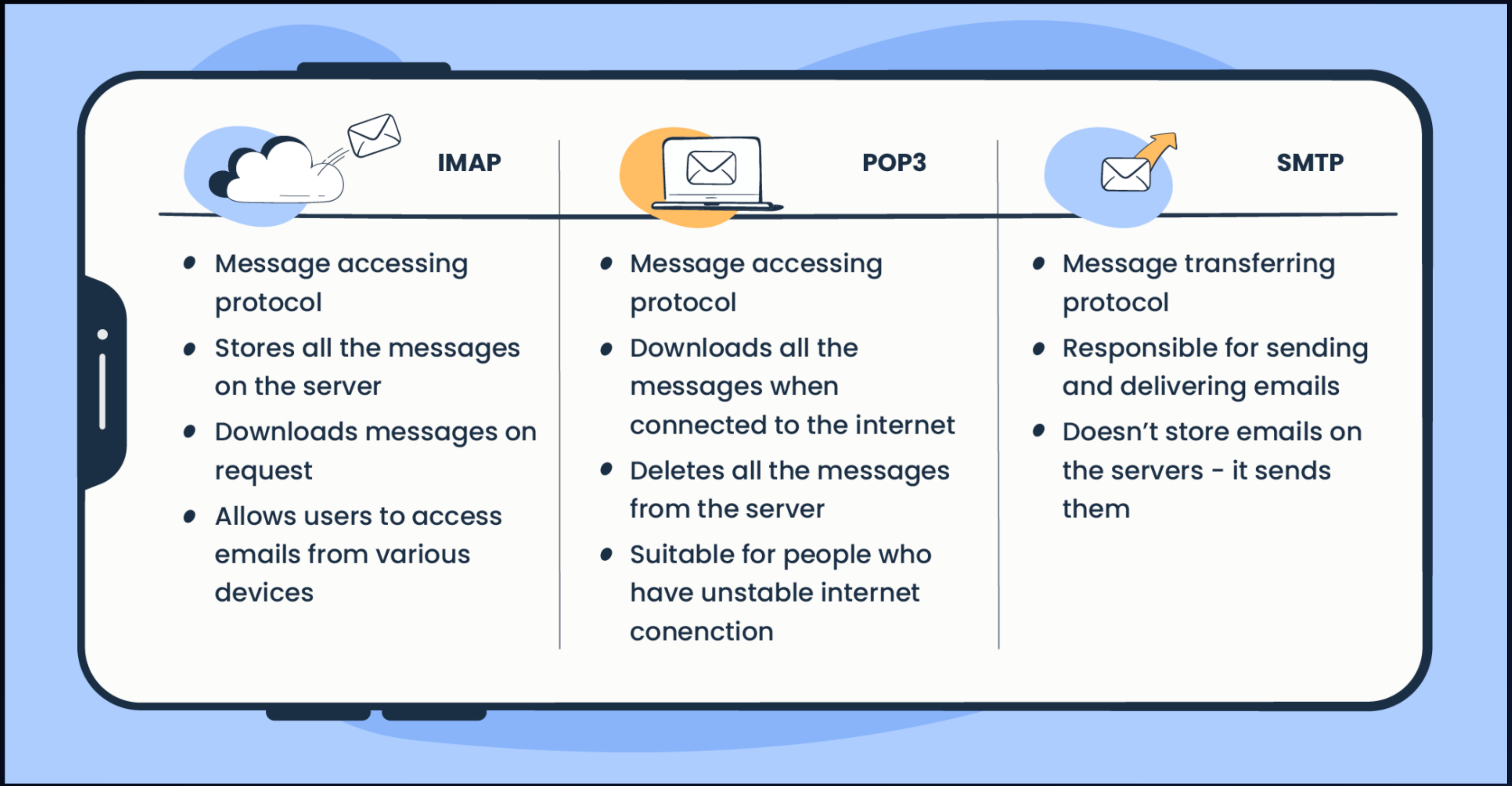


Persistent HTTP

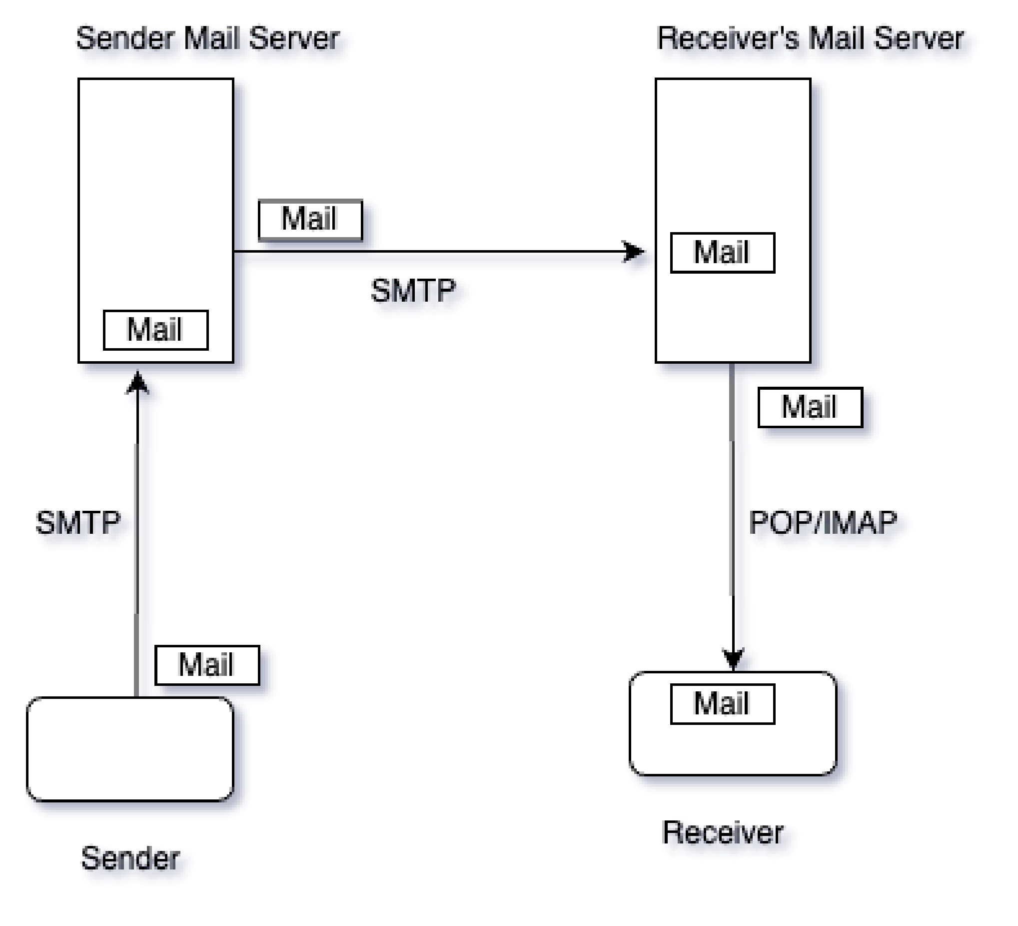




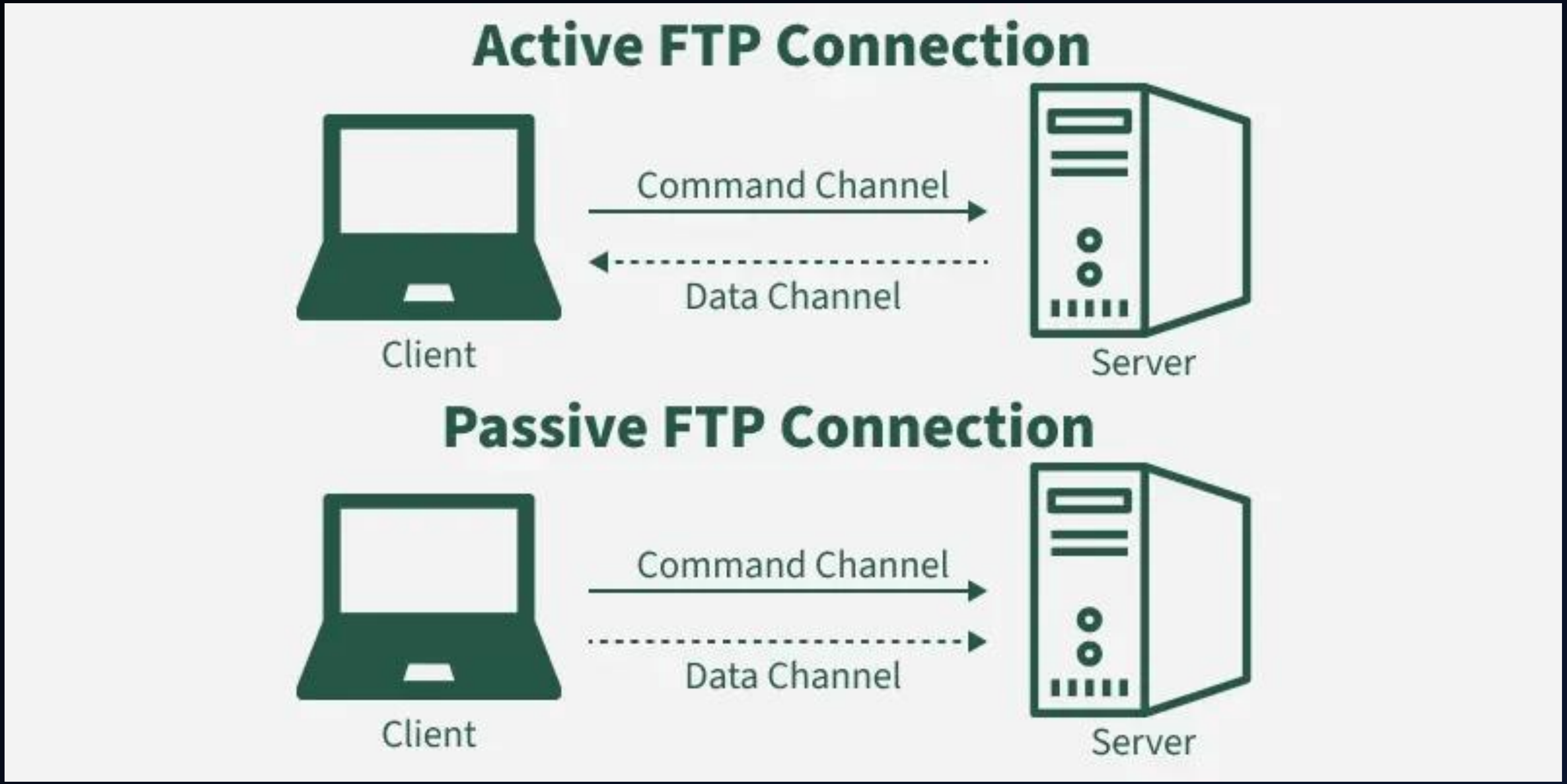
What Are SMTP, POP3, and IMAP?



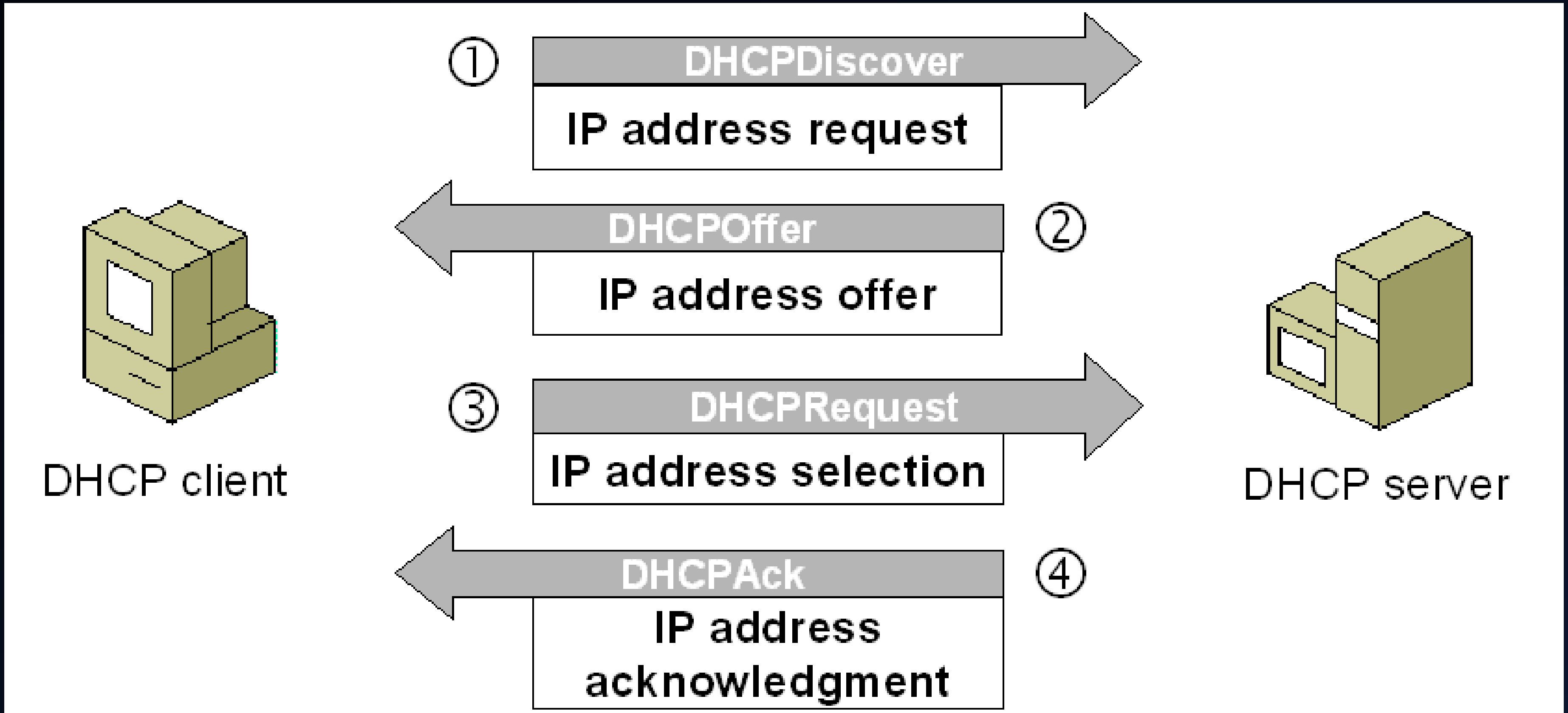
How Email Works: SMTP, POP3 & IMAP?



How FTP Works?



How DHCP Works



At a Glance

Protocol	Purpose	Port No(s)	TCP / UDP	Stateful?
DNS	Name → IP resolution	53	UDP / TCP	✗ No
HTTP	Web transfer	80	TCP	✗ No
SMTP	Send email	25 (Server → server) / 587 (client → server)	TCP	✓ Yes
POP3	Retrieve email	110	TCP	✓ Yes
IMAP	Access email	143	TCP	✓ Yes
FTP	File transfer	21 (Control)/ 20 (Data)	TCP	✓ Yes
DHCP	IP assignment	67 (Server) / 68 (Client)	UDP	✓ Yes

Some Interesting Facts

The first ARPANET message in 1969 was meant to be “LOGIN,” but the system crashed after “LO”—the Internet’s first word was an accident.

Designed during the Cold War, TCP/IP lets packets take multiple routes so the network survives even if parts are destroyed.

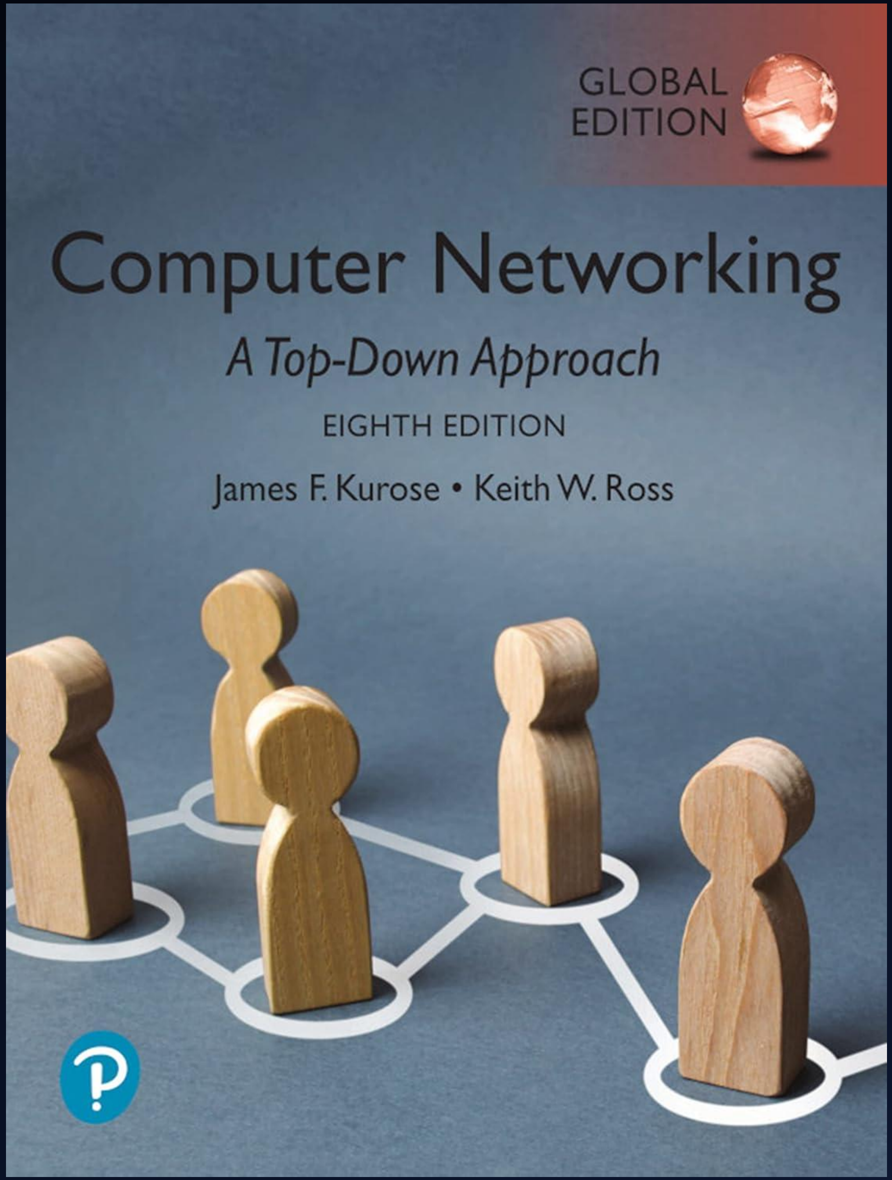
Some Interesting Facts

Ray Tomlinson used @ to separate user and machine names while testing ARPANET file transfers. That simple choice shaped email forever.

Early networks had too many collisions. Bob Metcalfe turned this flaw into a feature with CSMA/CD, letting Ethernet handle collisions instead of avoiding them.

WHERE TO GO NEXT?

- **Computer Networking: A Top-Down Approach**
  James Kurose, Keith Ross



“In theory, theory and practice are the same. In practice, they are not.”

— *Jan van de Snepscheut*