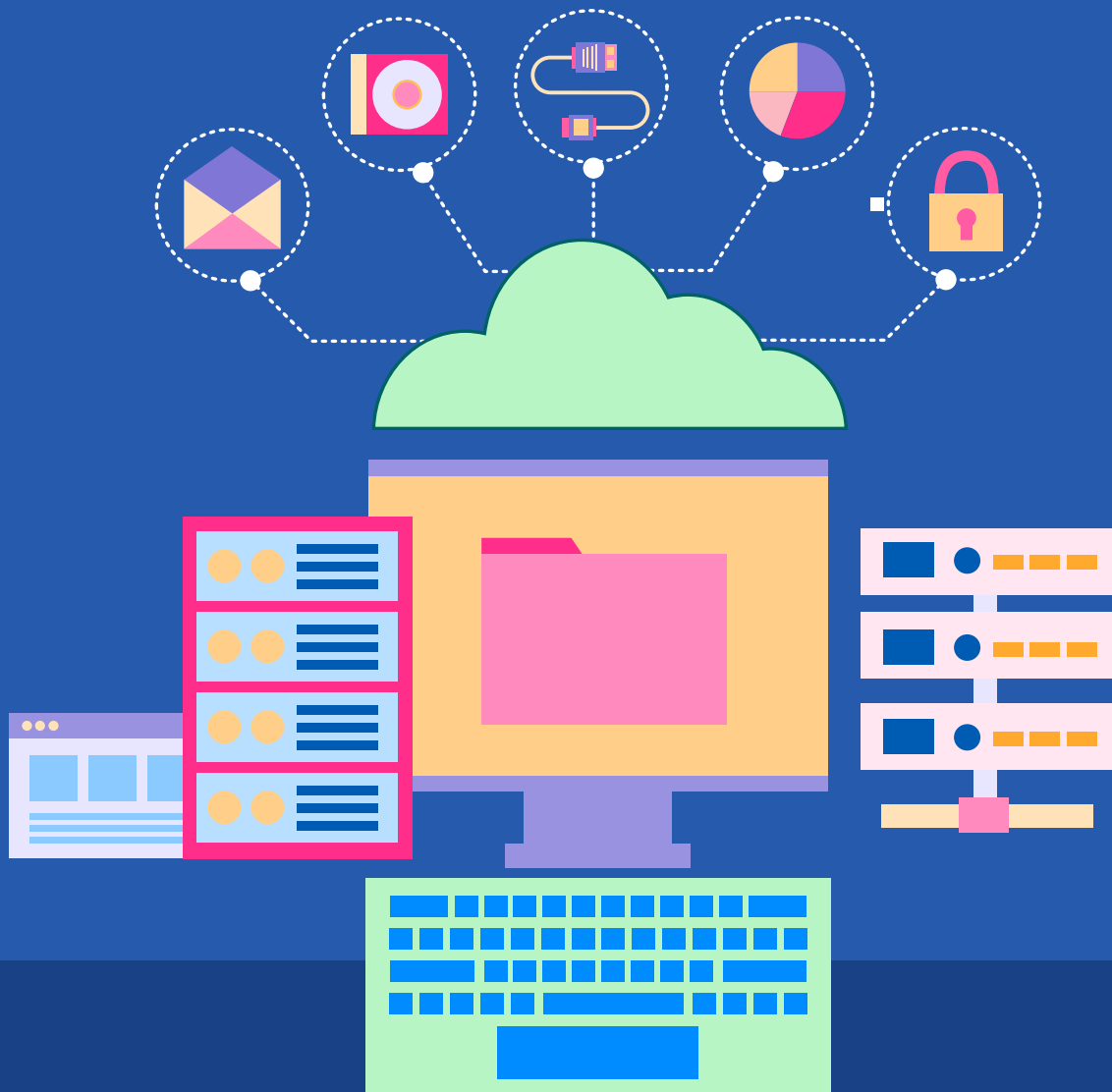


Computer Networks



India's best tech learning company

Learn industry-relevant skills with top tech veterans



126% Avg. CTC Hike

Top 1% Industry Instructors

900+ Placement Partners

Programs We Offer

Software Development
Course



Data Science &
Machine Learning



The Scaler Recipe to Transform Your Career

A structured & flexible
program, that cares for you

Be Mentored 1:1 by
Experienced Professionals

Become part of a thriving
community for life

Discover & connect with Alumni



Sudhanshu Gera
Software Engineer III

Pre Scaler
Wipro Limited

Post Scaler
Walmart*

↗ 200% Hike



Ankit Pangasa
Senior Software Engineer

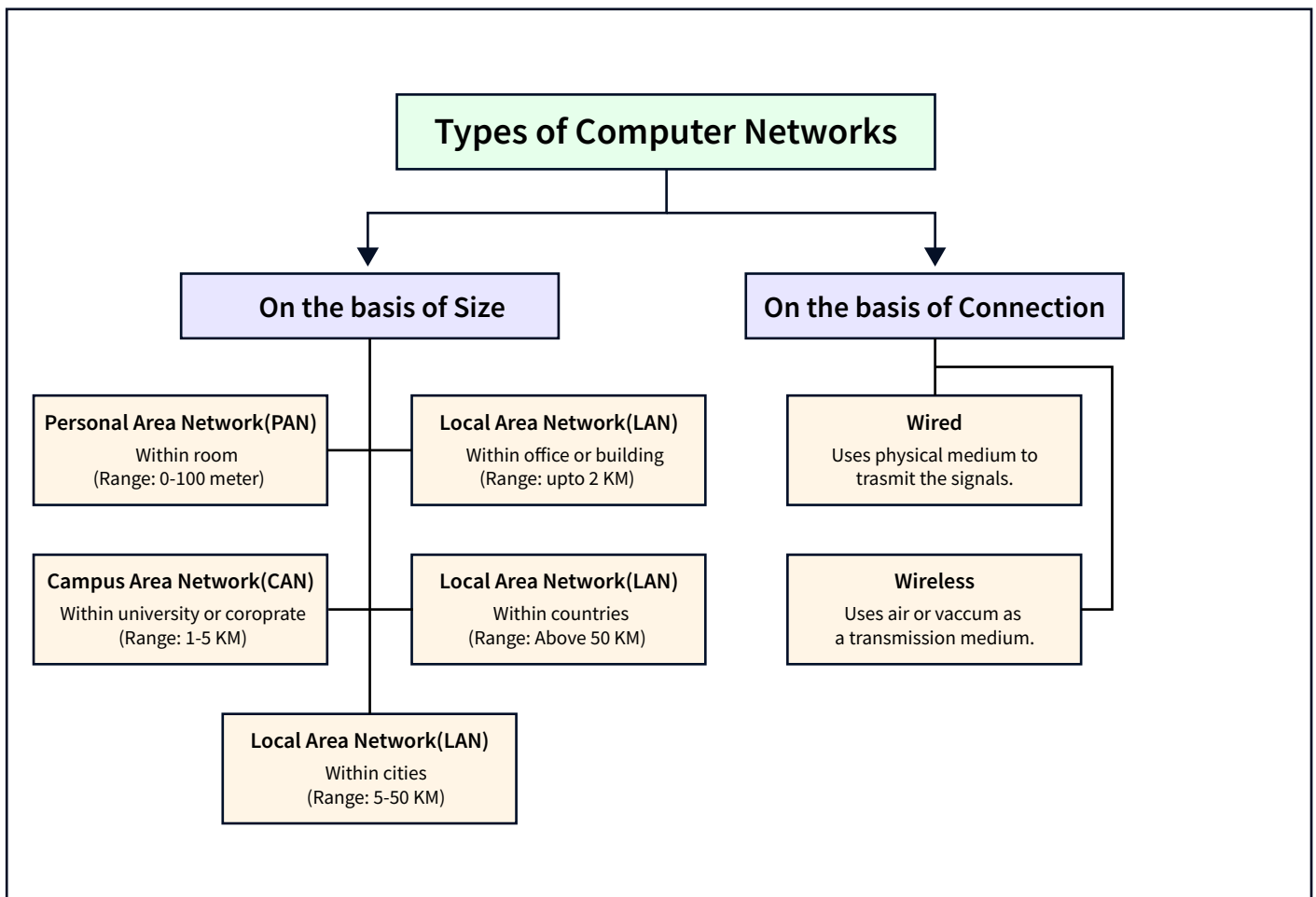
Pre Scaler
Adobe

Post Scaler
Google

↗ 200% Hike

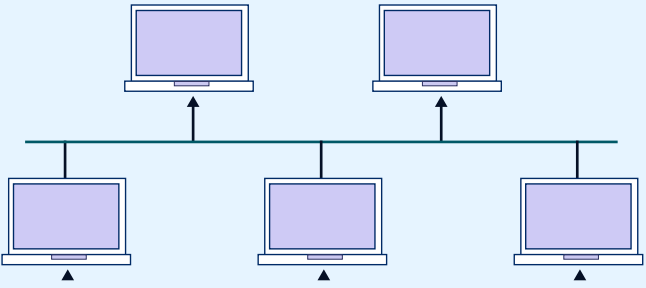
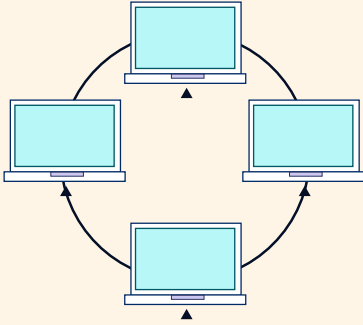
Connect with Alumni

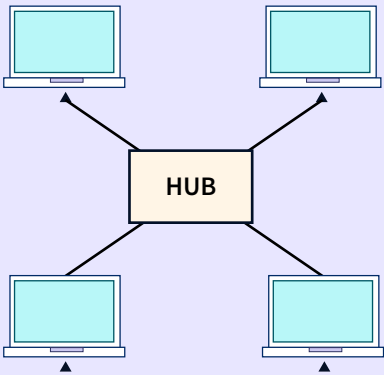
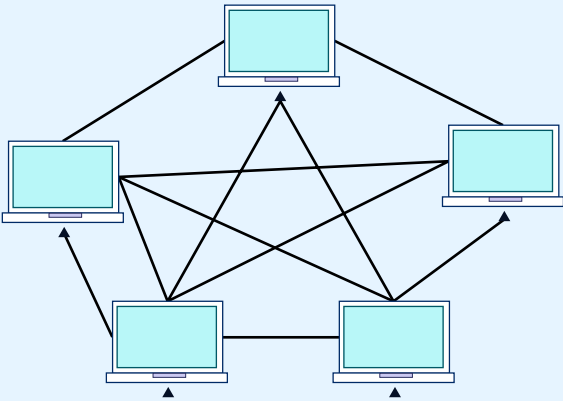
A computer network is a system of interconnected devices that enables communication and data sharing between them, facilitating resource sharing.



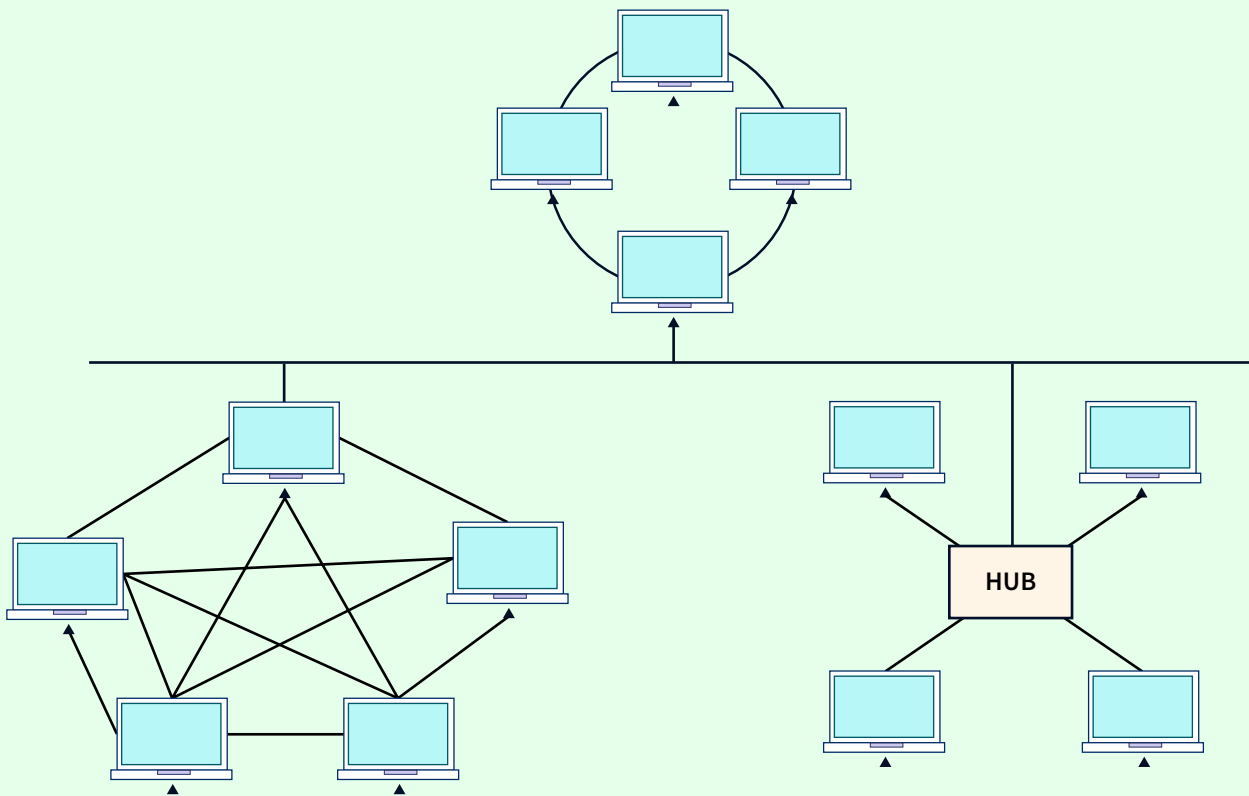
02

Network Topologies

Bus Topology	Ring Topology
	
<ul style="list-style-type: none"> Nodes connected to the single central cable. Simple and inexpensive. Limited scalability and reliability. 	<ul style="list-style-type: none"> Nodes connected in a circular fashion. Data travels in one direction. Difficult troubleshooting. Consistent performance.

Star Topology	Mesh Topology
	
<ul style="list-style-type: none"> Nodes connected central hub. Easy to manage and reliable. Dependency on central hub. 	<ul style="list-style-type: none"> Every node connects to every other node. Highly reliable but expensive. Provides redundancy. Complex to set up and manage.

Hybrid Topology



- Combination of two or more different types of topologies.
- Offers advantages of multiple topologies.
- Provides flexibility and scalability.

03

Network Components and Devices

Devices

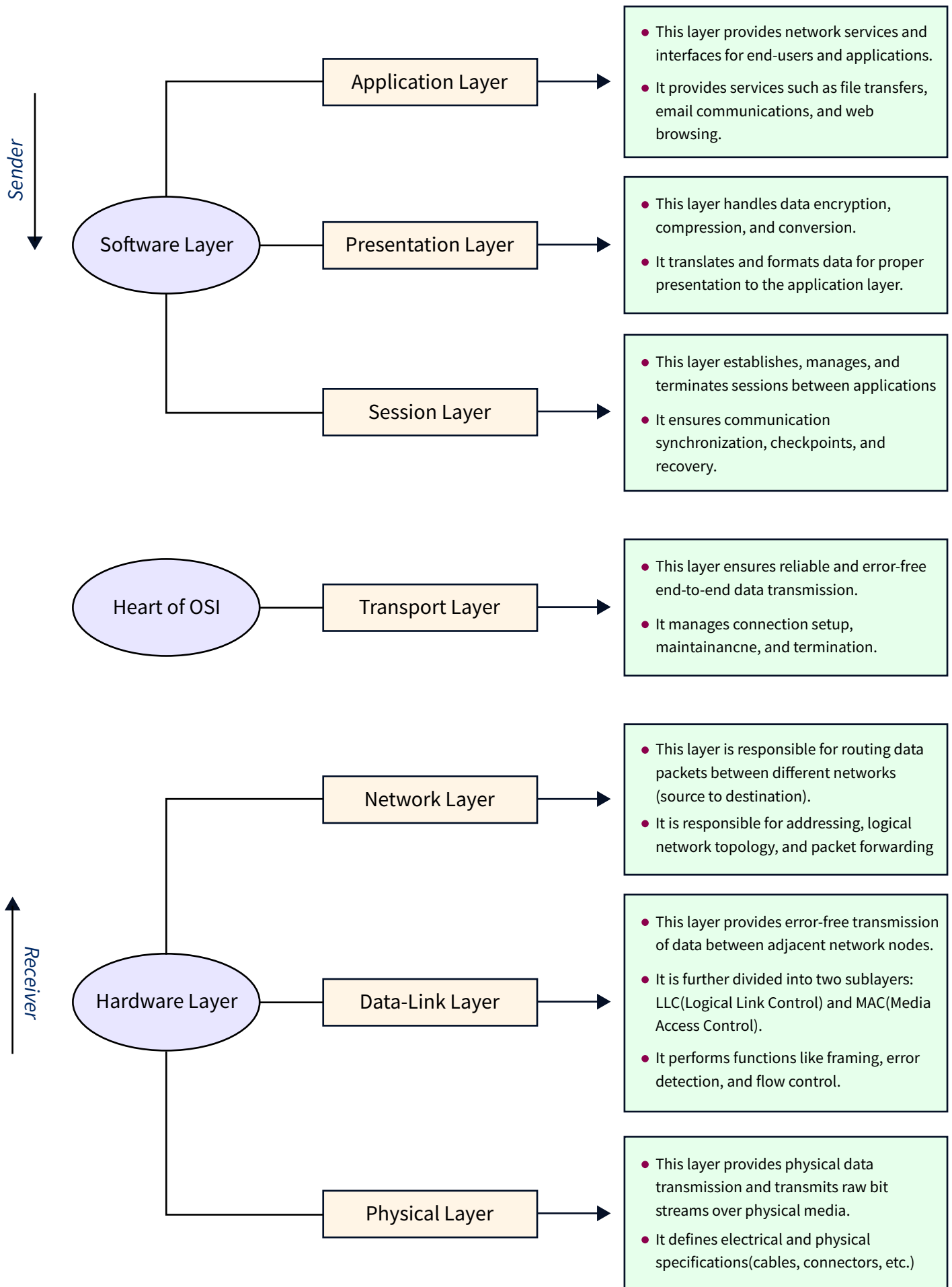
Device Name	Function
Repeaters	Two port device used to re-generate the signal strength.
Hubs	It is a multiport repeater.
Bridges	It is a Two port device used to connect multiple LANs. It also filters the incoming signals.
Switches	It is a multiport bridge and a layer two device.
Routers	It is a layer three device and used to connect two networks.
Gateway	It is used to connect and facilitate communication between different types of networks by translating protocols.
Modem	It modulate and demodulate analog signals, enabling digital devices to transmit and receive data over analog communication channels such as telephone lines or cable
Firewall	It monitor and control incoming and outgoing network traffic, acting as a barrier between a trusted internal network and untrusted external networks.
NICs	A Network Interface Card (NIC) is a hardware component that enables a computer to connect to a network and communicate with other devices.

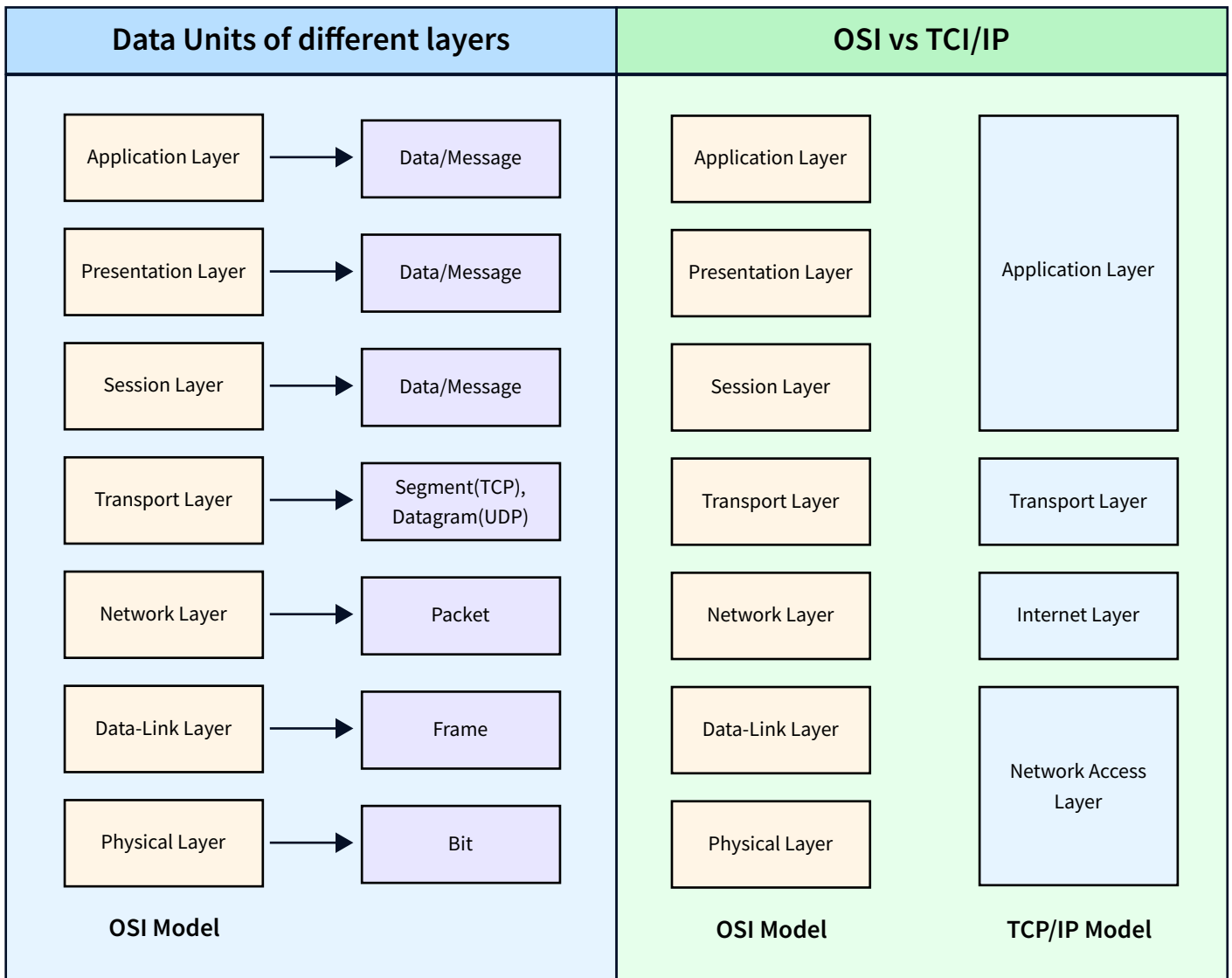
Media

Wired	Wireless
<ul style="list-style-type: none">● Ethernet Cables (Twisted Pair):<ul style="list-style-type: none">– Cat5e: Common for basic networking.– Cat6/Cat6a: Higher bandwidth and faster data transfer.– Cat7/Cat8: Enhanced shielding for even higher speeds.● Coaxial Cables:<p>Used for cable television (RG-6) and some broadband connections. Provides high bandwidth but less than fiber optics.</p>● Fiber Optic Cables:<p>Fiber optic cable is a high-speed, transparent, and flexible medium for transmitting data using pulses of light, providing faster and more reliable communication compared to traditional copper cables.</p>	<p>Wireless media refers to the transmission of data over a network without the use of physical cables, utilizing radio waves or infrared signals for communication.</p>

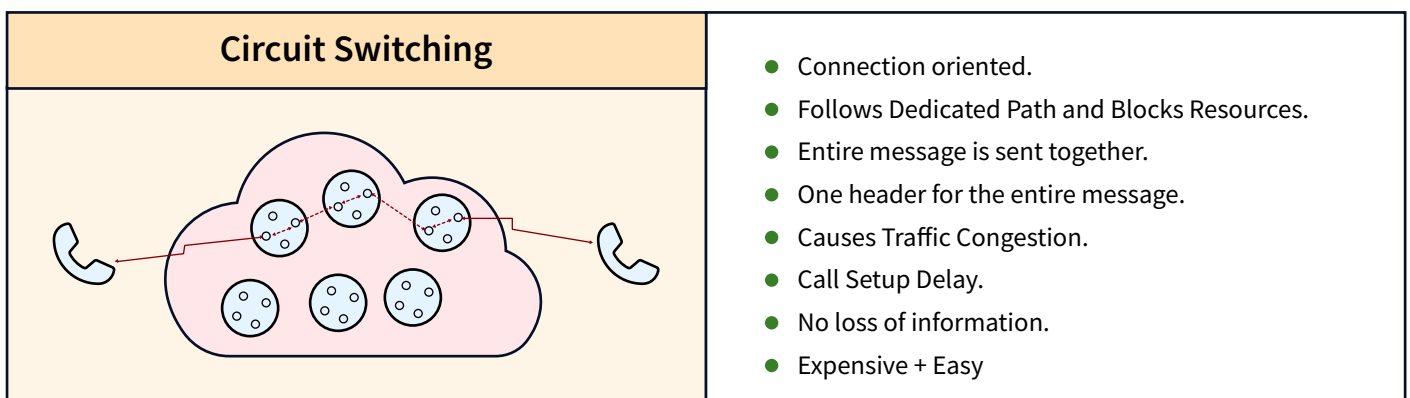
04 OSI Model

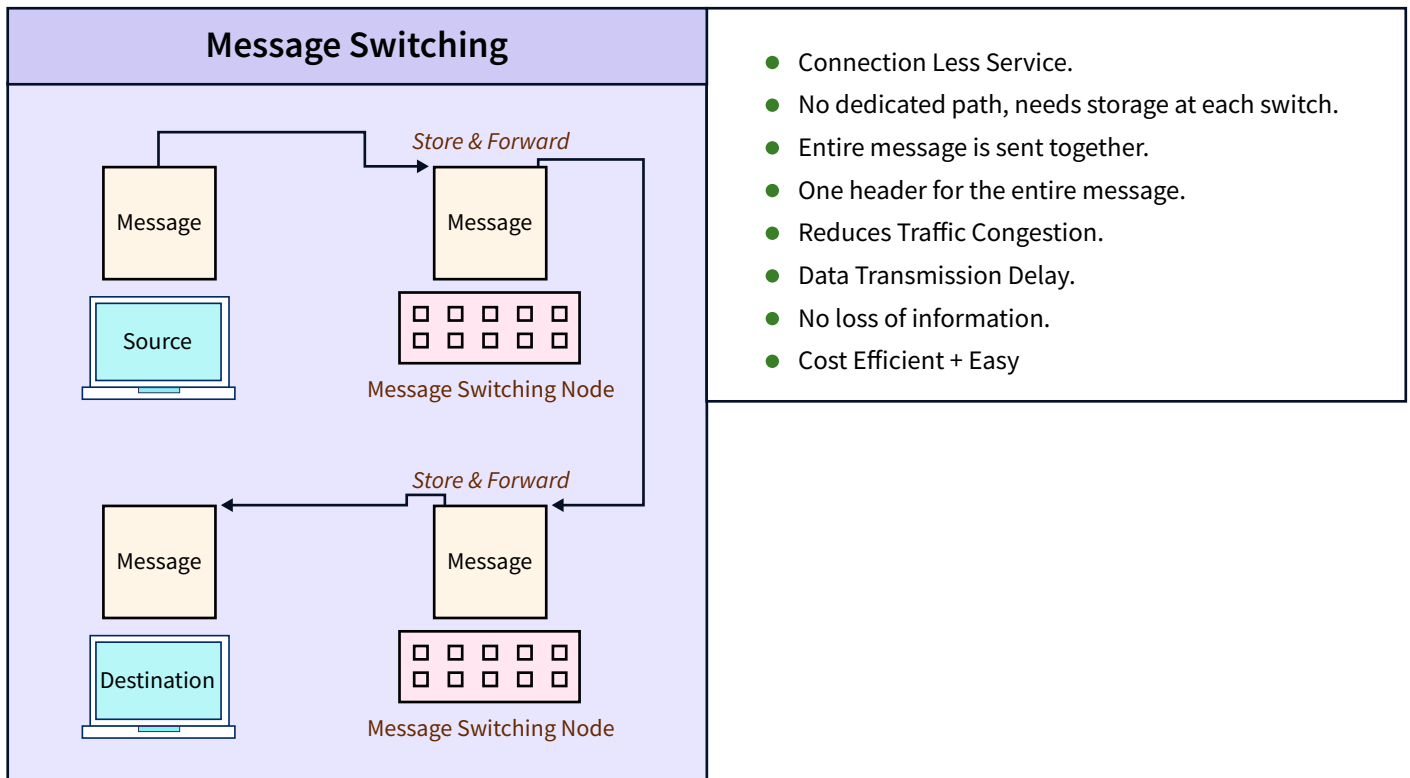
The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven abstraction layers.





05 Switching techniques



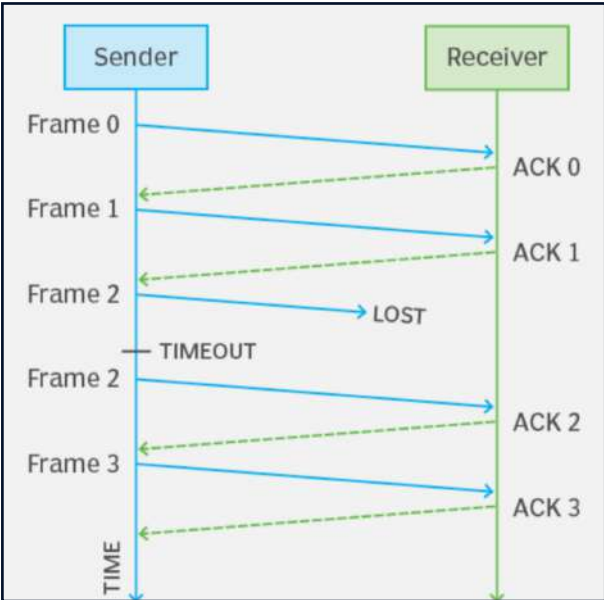
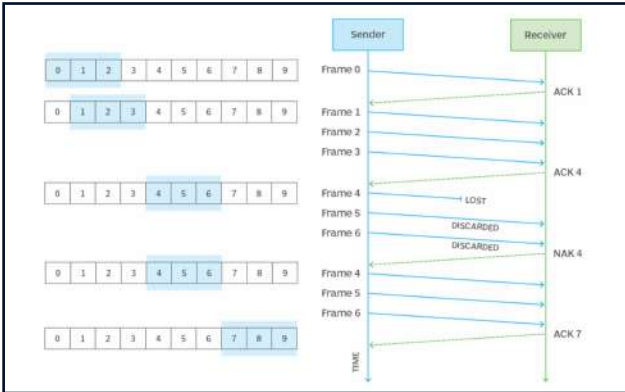


Packet Switching

Virtual Circuit	Datagram Service
<ul style="list-style-type: none"> ● Connection Oriented. ● Follows Dedicated Path and Blocks Resources. ● Message is broken down into packets. ● Only first packet has Global Header. ● Can Cause Traffic Congestion. ● Call Setup & Data Transmission Delay. ● No loss of information. ● Expensive + Complex 	<ul style="list-style-type: none"> ● Connection Less Service. ● No dedicated path, needs storage at each switch. ● Message is broken down into packets. ● Global Header in all packets. ● Reduces Traffic Congestion. ● Data Transmission Delay. ● Packets can get lost. ● Cost Efficient + Easy.

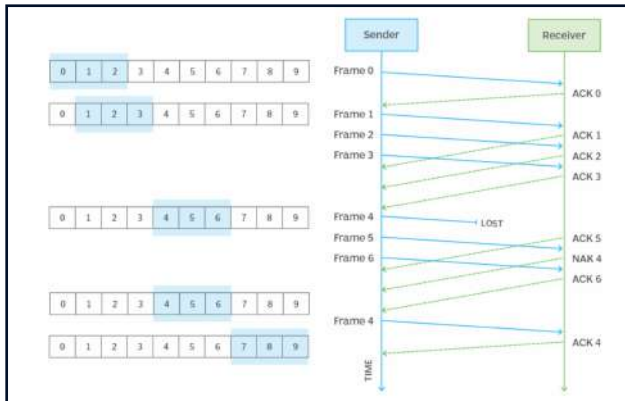
Flow Control Protocol

Flow control protocols are mechanisms used to regulate the flow of data between sender and receiver to ensure efficient and reliable communication.

Stop and wait	Go-Back-N
<p>Stop and Wait ARQ is a flow control protocol that ensures reliable data transmission. The sender sends one data frame at a time and waits for an acknowledgment from the receiver before sending the next frame.</p>	<p>Go-Back-N ARQ is a flow control protocol that allows the sender to transmit a number of frames without waiting for individual acknowledgments. If an acknowledgment is not received, the sender resends all the frames from the last acknowledged one.</p>
 <p>The diagram illustrates the Stop and Wait protocol. A vertical timeline on the left represents the Sender, and a vertical timeline on the right represents the Receiver. <ul style="list-style-type: none"> Frame 0 is sent from Sender to Receiver. ACK 0 is received at the Sender. Frame 1 is sent from Sender to Receiver. ACK 1 is received at the Sender. Frame 2 is sent from Sender to Receiver. The frame is marked as 'LOST'. A 'TIMEOUT' period is indicated on the Sender's timeline. Frame 2 is re-sent from Sender to Receiver. ACK 2 is received at the Sender. Frame 3 is sent from Sender to Receiver. ACK 3 is received at the Sender. A vertical arrow labeled 'TIME' points downwards on the Sender's timeline.</p>	 <p>The diagram illustrates the Go-Back-N protocol. A vertical timeline on the left represents the Sender, and a vertical timeline on the right represents the Receiver. <ul style="list-style-type: none"> Frames 0, 1, 2, and 3 are sent from Sender to Receiver. ACK 1 is received at the Sender. Frame 4 is sent from Sender to Receiver. ACK 4 is received at the Sender. Frame 5 is sent from Sender to Receiver. Frame 5 is marked as 'LOST'. Frame 6 is sent from Sender to Receiver. Frame 6 is marked as 'DISCARDED'. Frame 4 is re-sent from Sender to Receiver. Frame 4 is marked as 'DISCARDED'. Frame 5 is re-sent from Sender to Receiver. Frame 5 is marked as 'DISCARDED'. Frame 6 is re-sent from Sender to Receiver. Frame 6 is marked as 'DISCARDED'. Frame 7 is sent from Sender to Receiver. ACK 7 is received at the Sender. A vertical arrow labeled 'TIME' points downwards on the Sender's timeline. Above the timeline, four windows of size N=4 are shown, representing the sender's buffer state at different points in time.</p>

Selective Repeat

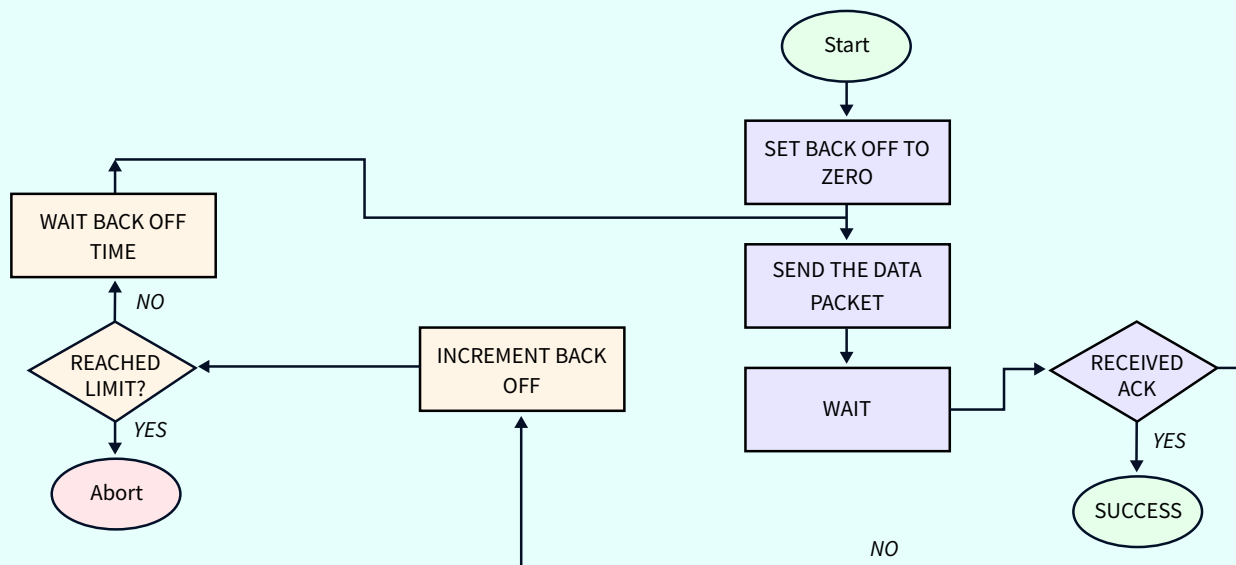
Selective-Repeat ARQ is a flow control protocol that allows the sender to transmit a number of frames without waiting for individual acknowledgments. If an acknowledgment is not received, only the specific frame(s) that were not acknowledged are resent.



Multiple Access Protocols

Multiple Access Protocols are used to allow multiple devices to share a common communication channel.

Aloha



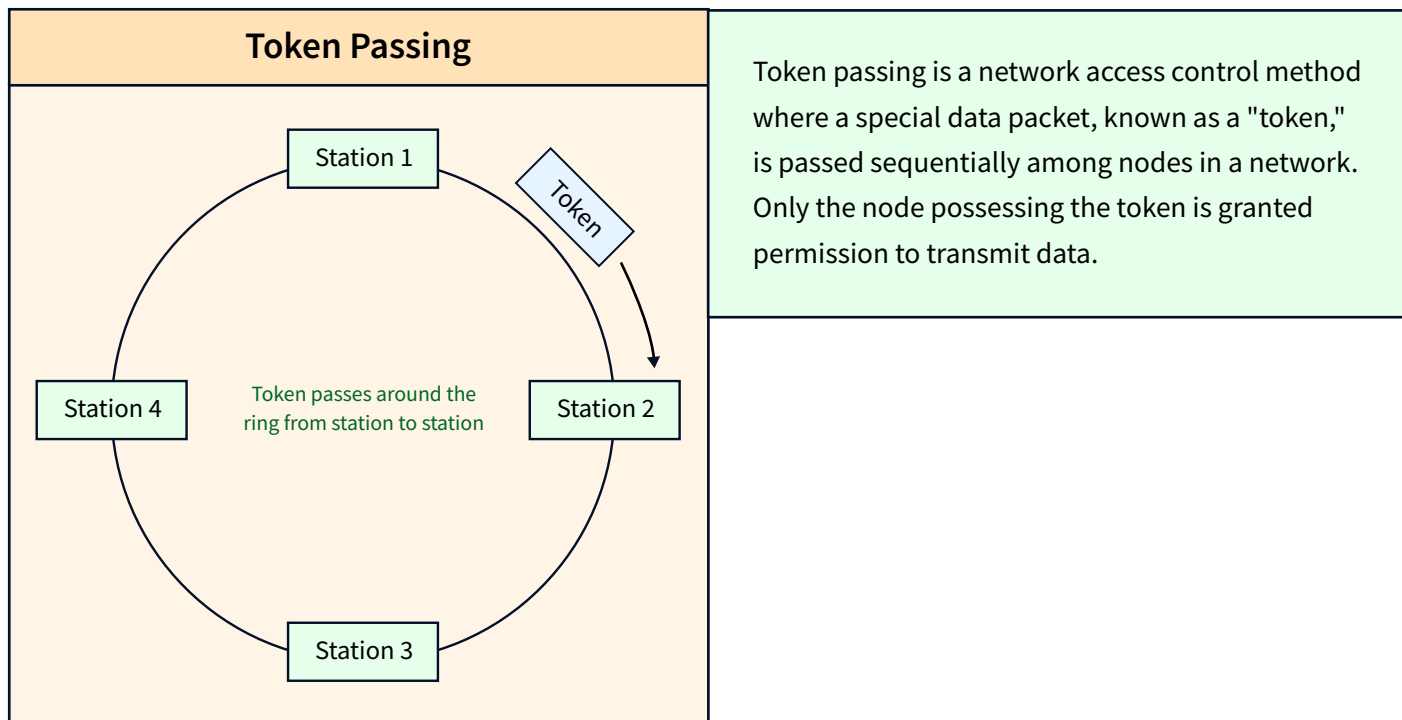
Aloha is a random access protocol used in wireless networks. Devices can transmit data at any time, but collisions can occur if multiple devices transmit simultaneously. It has variants like pure Aloha and slotted Aloha.	Pure ALOHA allows stations to transmit data at any time, with collisions resolved after detection, while Slotted ALOHA introduces synchronized time slots for more efficient collision management.
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

CSMA (Career Sense Multiple Access)	CSMA/CD (Career Sense Multiple Access/Collision Detection)
Carrier Sense Multiple Access (CSMA) is a multiple access protocol that allows devices to sense the network before transmitting. Transmissions are deferred if the channel is busy.	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is used in Ethernet networks. It adds collision detection to CSMA, and if a collision occurs during transmission, devices stop transmitting and wait for a random time before retrying.

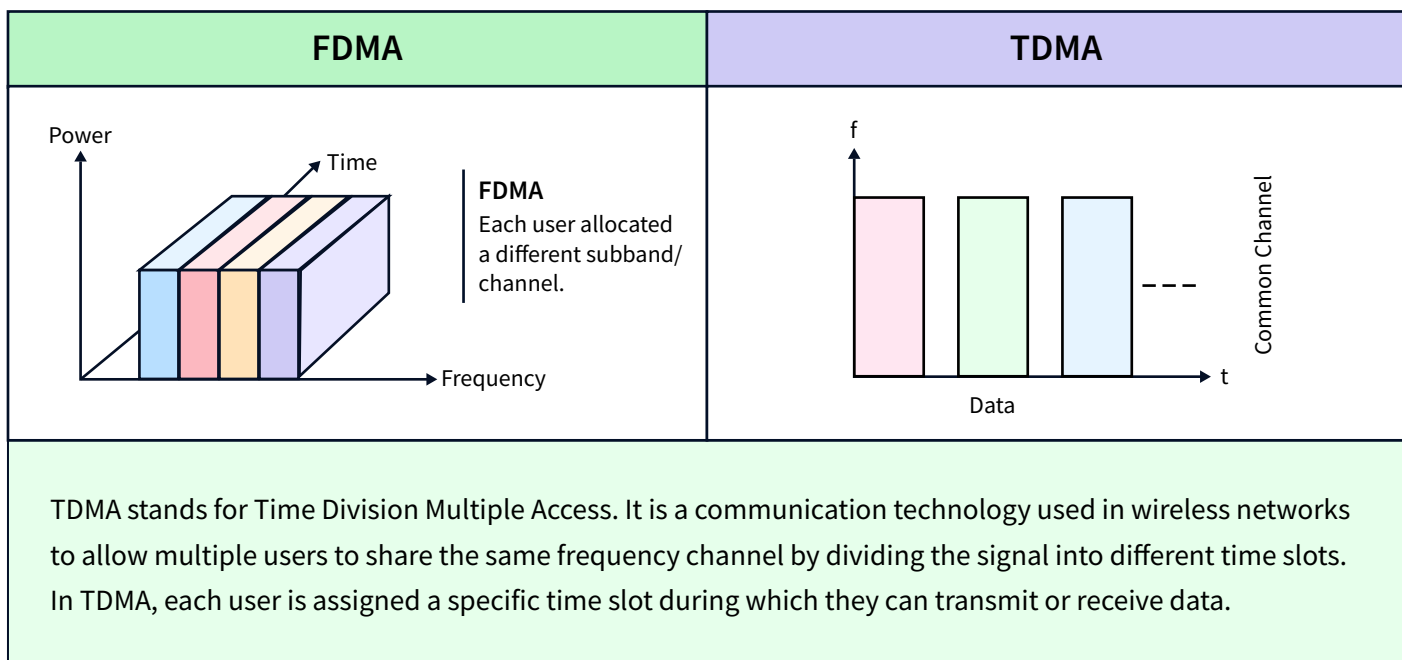
CSMA/CA (Career Sense Multiple Access/Collision Avoidance)
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used in wireless networks. It adds collision avoidance mechanisms to CSMA, such as Request to Send (RTS) and Clear to Send (CTS) messages.

Control Access Protocol

Polling
Polling is a communication protocol where a central device (e.g., a server) systematically queries or polls other devices (e.g., clients) to check for their status or to request information. This protocol is used to manage and control the flow of data in a network by actively seeking updates from connected devices.



Channelization Protocol



Routing Algorithm

Routing Protocols are used by routers to determine the best path for data packets to reach their destination.

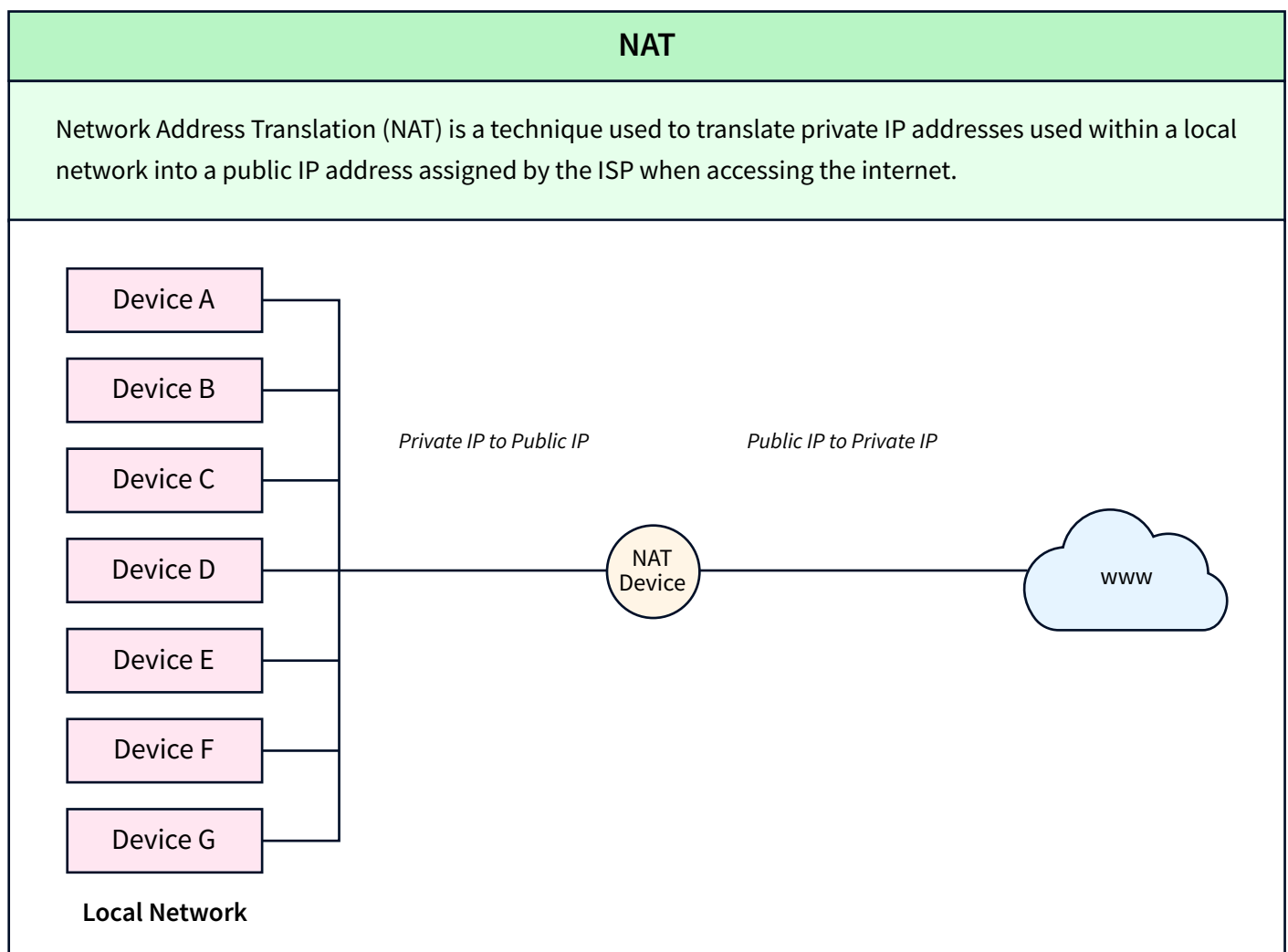
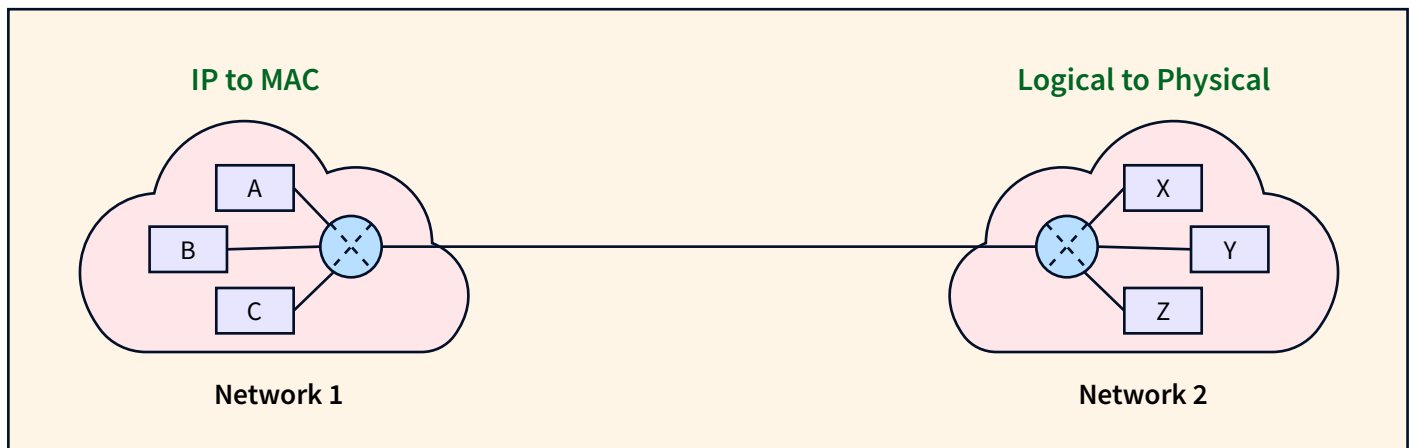
	Distance Vector (RIP)	Link state (OSPF)	Path Vector (BGP)
Interior/Exterior	Interior	Interior	Exterior
Default Metric	Hop Count	Cost (100 MBPS/BW)	Multiple Attributes
Convergence	Slow	Fast	Average
Updates	Full table	Only changes	Only changes
Algorithm	Bellman-Ford	Dijkstra	Best Path

TCP vs UDP

Transmission Control Protocol	User Datagram Protocol
Connection oriented.	Connection less
Reliable	Less Reliable
Error control is mandatory	Error control is optional
Slow transmission	Fast transmission
More Overhead	Less Overhead

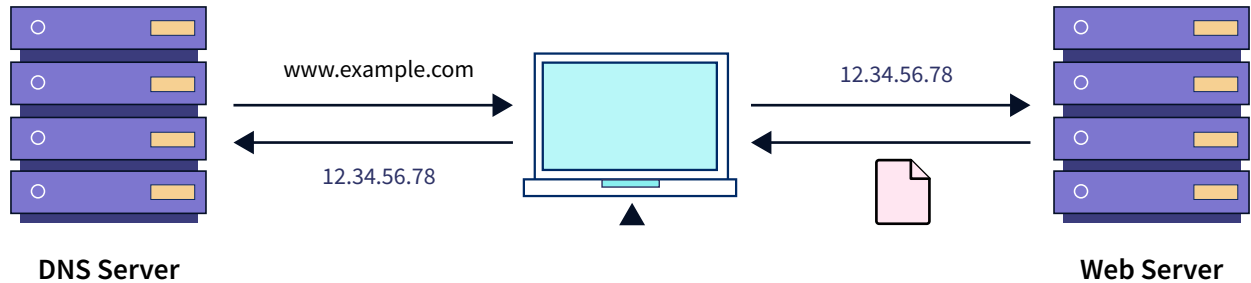
ARP

Address Resolution Protocol (ARP) maps an IP address to the corresponding MAC address on a local network. It is used to discover and associate IP and MAC addresses of devices within a LAN.



DNS

Domain Name System (DNS) translates human-readable domain names into IP addresses. It allows users to access websites using domain names instead of remembering the IP addresses.



HTTP/HTTPS	FTP	DHCP	POP3
Hypertext Transfer Protocol (HTTP) is a protocol used for transmitting web pages and resources over the internet. HTTPS is a secure version that uses encryption to protect data transmission.	File Transfer Protocol (FTP) is a protocol used for transferring files between a client and a server on a network. It provides functions for file upload, download, and management.	Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and network configuration details to devices in a network, eliminating the need for manual configuration.	Post Office Protocol (POP3) is an email protocol used for retrieving emails from a mail server. It allows users to access and download their emails to their devices.

IMAP

IMAP, or Internet Message Access Protocol, is a standard email protocol used to retrieve messages from a mail server. Unlike the older POP (Post Office Protocol), which primarily downloads emails to a local device and removes them from the server, IMAP allows users to view and manipulate their emails directly on the mail server.

07

IP Addressing and Subnetting

IP addressing is the assignment of unique numerical labels (IP addresses) to devices on a computer network, enabling them to communicate and identify each other within the Internet Protocol (IP) suite.

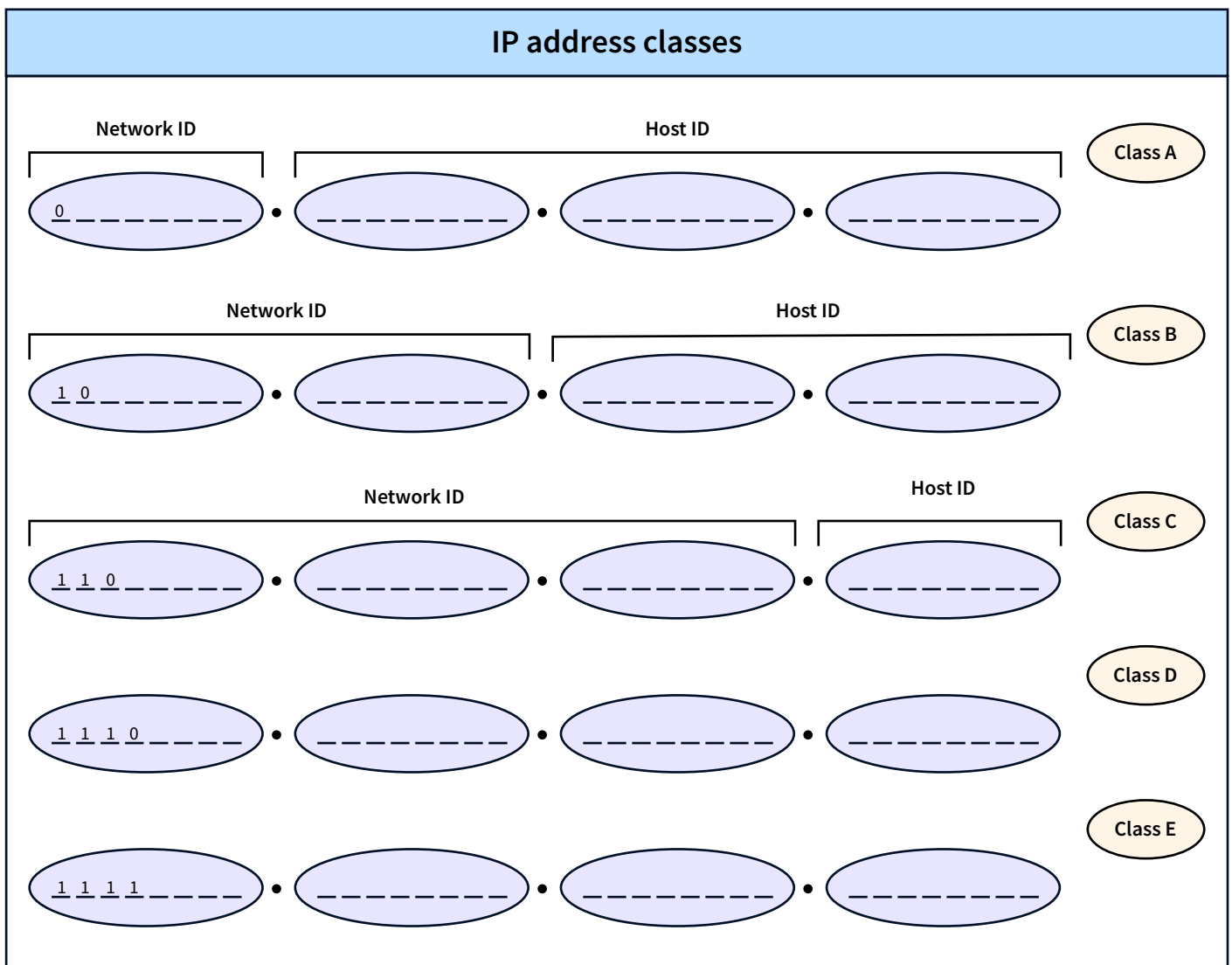
IP vs MAC

Feature	IP Address	MAC Address
Layer	Network Layer (Layer 3)	Data Link Layer (Layer 2)
Purpose	Identifies devices on a network globally	Identifies devices on a local network
Assignment	Can be dynamic (DHCP) or static	Hard-coded into the network interface by the manufacturer
Scope	Unique within a network, routable on the internet	Unique within a local network
Changes	Can change due to network reconfiguration	Generally remains constant for the device's lifetime
Examples	IPv4: 192.168.1.1, IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334	00:1A:2B:3C:4D:5E (hexadecimal)

IPv4 Header				
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

IPv6 Header				
Version	Traffic Class		Flow Label	
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

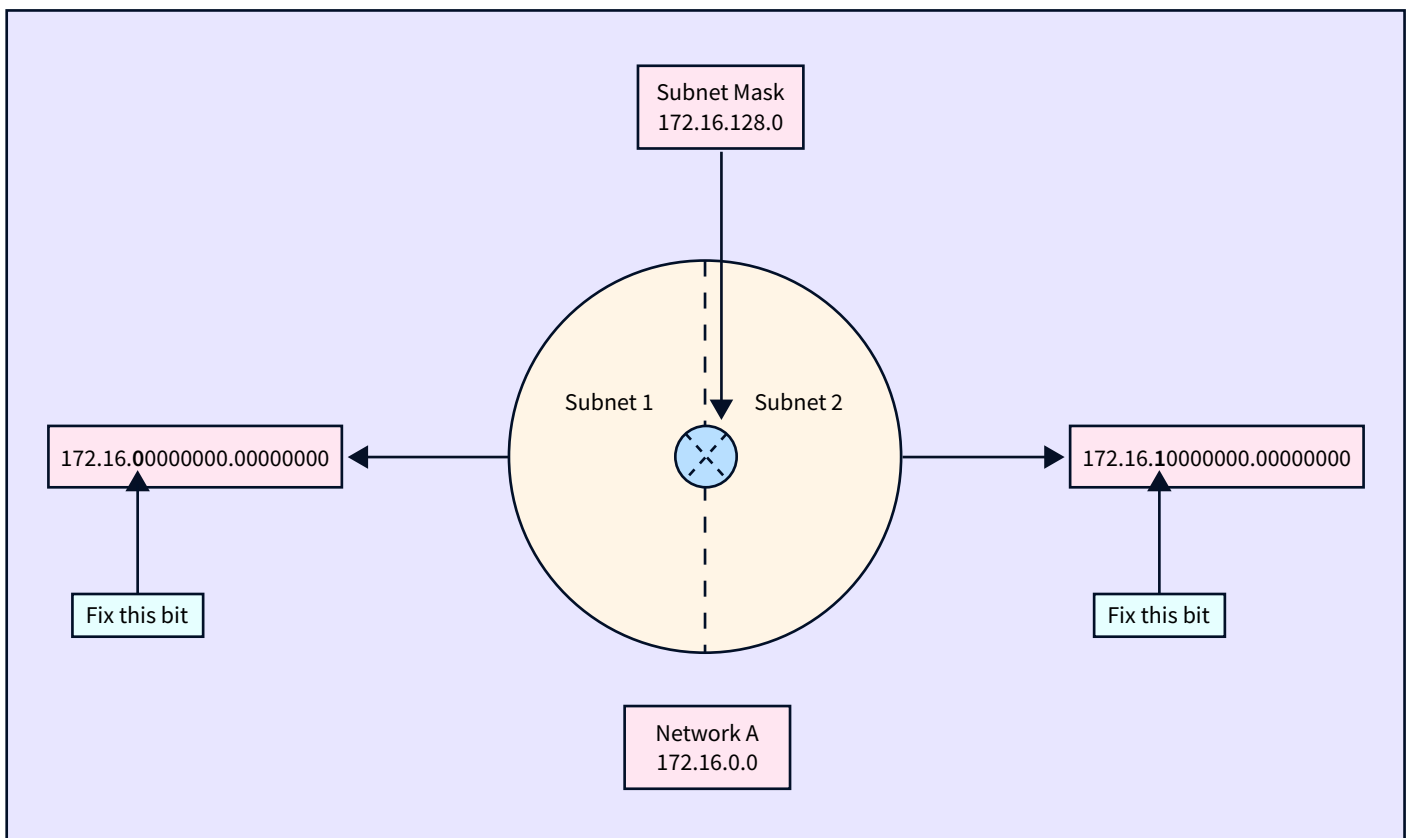
Version - 4 bits IHL - 4 bits Type of Service - 8 bits Total Length - 16 bits Identification - 16 bits Flags - 3 bits Fragment Offset - 13 bits TTL - 8 bits Protocol - 8 bits Header Checksum - 16 bits Source Address - 32 bits Destination Address - 32 bits Options - variable Padding - variable	Version - 4 bits Traffic Class - 8 bits Flow Label - 20 bits Payload Length - 16 bits Next Header - 8 bits Hop Limit - 8 bits Source address - 128 bits Destination address - 128 bits
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Public IP	Private IP
<p>A Public IP (Internet Protocol) address is a unique address assigned to a device connected to a network that is accessible from the internet. It allows the device to communicate with other devices and services on the internet and is used for identifying and routing data packets to the correct destination.</p>	<p>A private IP address is an address reserved for use within a private network and is not routable on the public internet. Private IP addresses are commonly used in local networks, such as homes or businesses, and are typically assigned to devices like computers, printers, or routers within that network.</p>

Subnetting

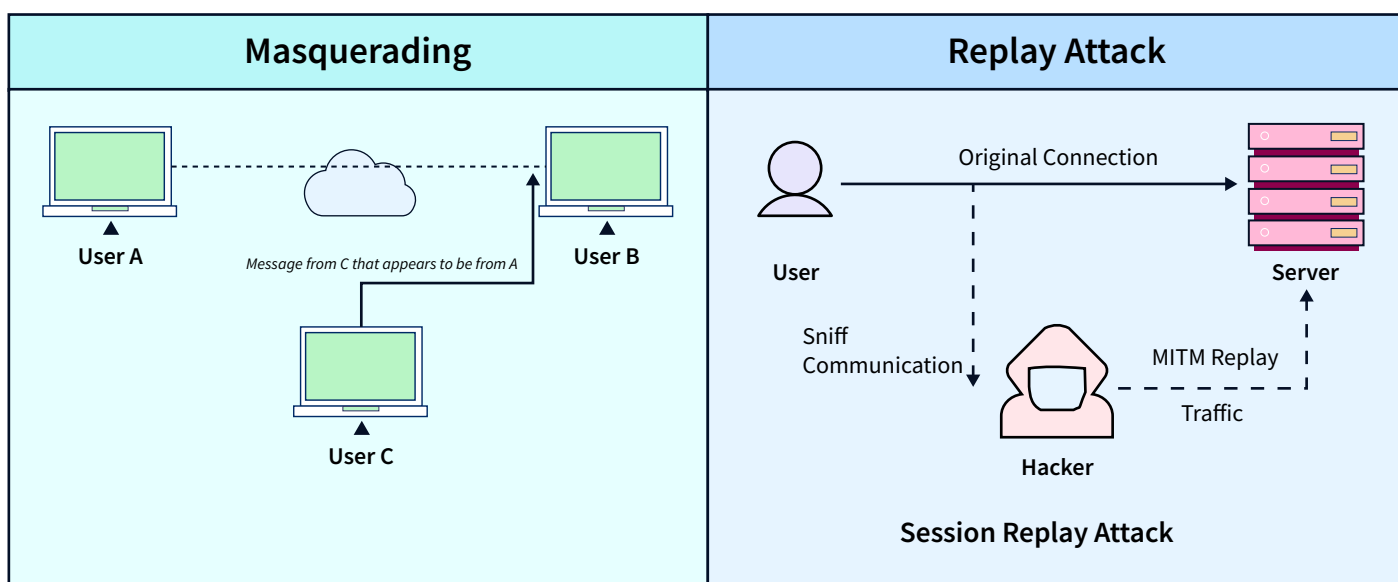
Subnetting refers to the practice of dividing a larger network into smaller, more manageable sub-networks or subnets. Subnetting is commonly done to improve network performance, enhance security, and efficiently allocate IP addresses.

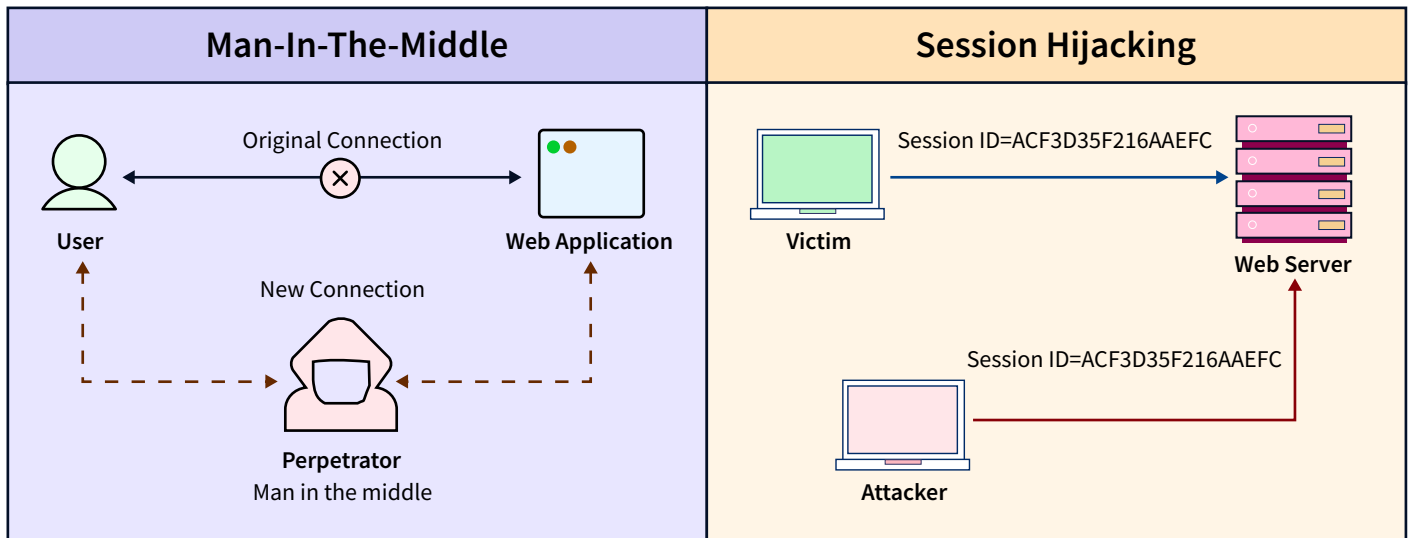


A subnet mask is a 32-bit numerical value that divides an IP (Internet Protocol) address into network and host portions. It is used in conjunction with IP addresses to create subnets within a larger network. The subnet mask contains a series of contiguous 1-bits followed by contiguous 0-bits, with the 1-bits indicating the network portion and the 0-bits representing the host portion of the address. Subnet masks are essential for subnetting and help in organizing and managing IP addresses within a network.

08 Network Security

Common network security threats





IDS	VPN	SSL/TLS
Intrusion Detection Systems are security tools designed to monitor and analyze network or system activities for signs of unauthorized access, misuse, or security policy violations. They generate alerts or take predefined actions when suspicious activities are detected.	Virtual Private Networks are secure, encrypted connections established over the internet, enabling users to access a private network from a remote location securely. VPNs protect data during transmission and provide a secure communication channel over the public internet.	SSL and TLS are cryptographic protocols that ensure secure communication over a computer network, such as the internet. They establish a secure connection by encrypting data during transmission between a client and a server.

09 Points to remember

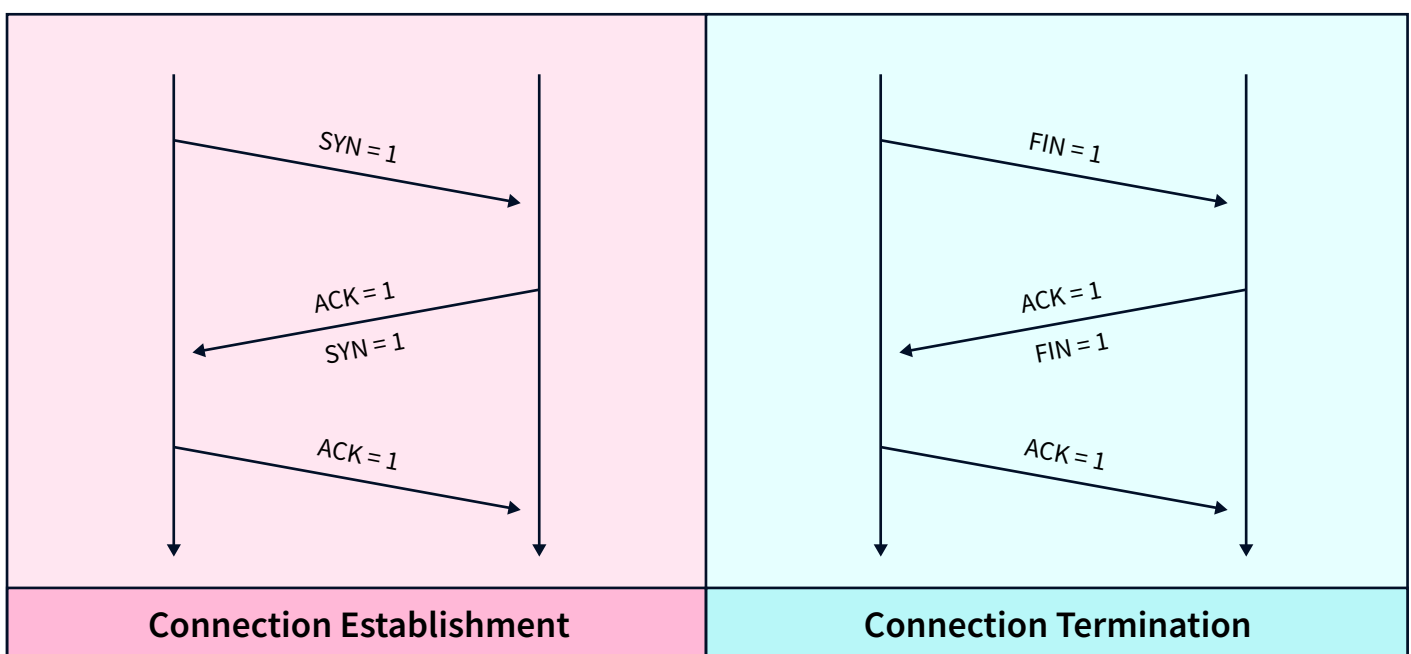
Remember the helpful acronym "Please Do Not Throw Sausage Pizza Away" to remember the layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Important Ports in Transport layer

Category	Range
Well Known Ports	0 to 1023
Registered Ports	1024 to 49151
Private Ports	49152 to 65535

Ports No.	Protocol	Protocol
20	TCP	FTP data
21	TCP	FTP Control
22	TCP	SSH
25	TCP	SMTP
53	UDP, TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
443	TCP	SSL

3-way handshake protocol






Miscellaneous

- The OSI Model is not commonly used for practical network design and it is widely taught and serves as an educational tool to understand network communication principles and concepts.
- Devices like routers operate at the Network Layer, switches and bridges at the Data Link Layer, and hubs, repeaters and modems at the physical Layer.
- The bottom layers (1-4) deal with the physical and logical aspects of data transmission, while the upper layers (5-7) focus on the application and user interface.
- Wi-Fi: A widely used wireless technology that allows devices to connect to a local area network (LAN) or the internet without the need for physical cables. Wi-Fi is commonly used in homes, businesses, and public spaces.
- Cellular Networks: Mobile communication networks that provide wireless connectivity over a wide area. Technologies like 4G LTE and 5G enable mobile devices to connect to the internet and communicate with each other.

SCALER TOPICS



Unlock your potential in software development with
FREE COURSES from **SCALER TOPICS**!

Register now and take the first step towards your future Success!



PRATEEK NARANG

C++ for Beginners

 5.9k enrolled  **Free**



TARUN LUTHRA

Java for Beginners

 6.8k enrolled  **Free**

That's not it. Explore 20+ Courses by clicking below

[Explore Other Courses](#)

Practice **CHALLENGES**
and become 1% better everyday



CIFAR-10 Image Classification Using PyTorch
Article

 No. Of Questions : 3

[Go to Challenge >](#)



How to Build a Snake Game in JavaScript?
Article

 No. Of Questions : 3

[Go to Challenge >](#)

[Explore Other Challenges](#)