Computer Networks Unit 1

UNIT I: Computer Network: Definitions, goals, components, Architecture, Classifications & Types. Layered Architecture: Protocol hierarchy, Design Issues, Interfaces and Services, Connection Oriented & Connectionless Services, Service primitives, Design issues & its functionality. ISOOSI Reference Model: Principle, Model, Descriptions of various layers and its comparison with TCP/IP. Principles of physical layer: Media, Bandwidth, Data rate and Modulations.

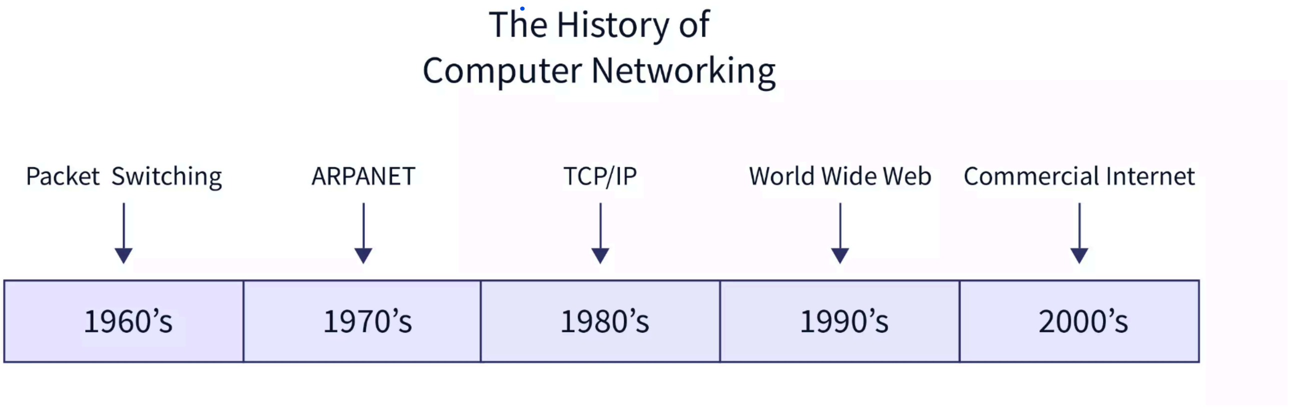
Computer Network:

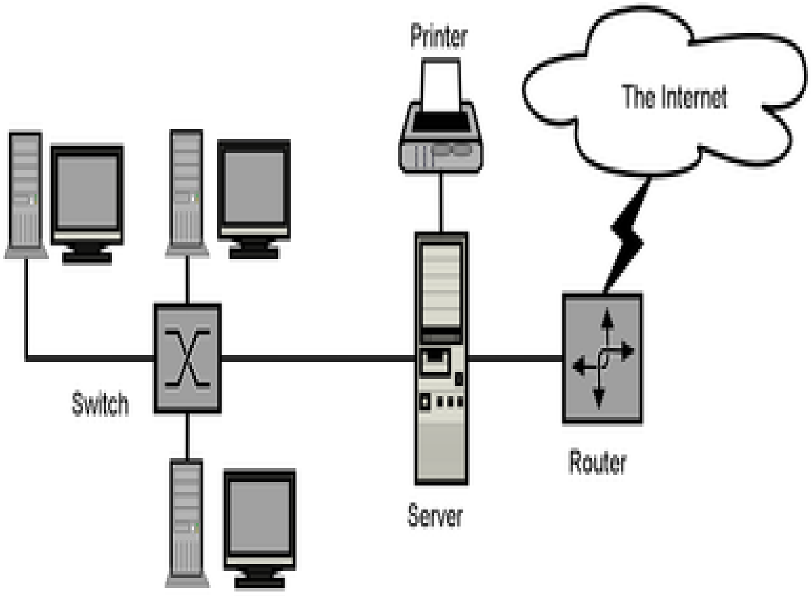
Definition- Imagine you have several computers, and you want them to talk to each other and share information.

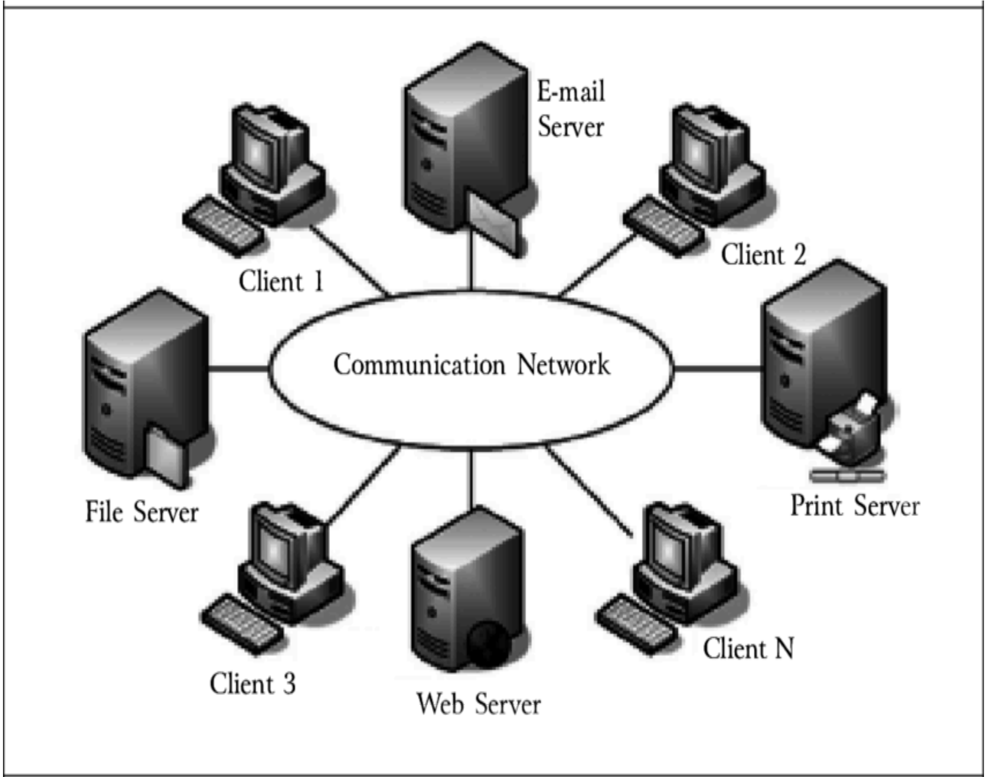
A computer network is like a digital neighborhood that connects these computers so they can communicate and share resources, such as files, printers, or an internet connection.

In simpler words, a computer network is a way for computers to connect and work together, allowing them to share and exchange information. It's like a digital community where devices can interact and collaborate.

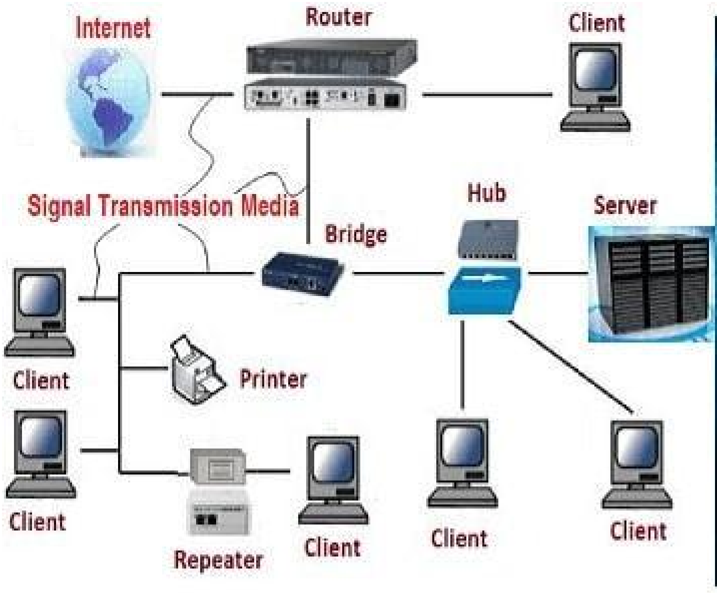
The first computer network was developed by the Advanced Research Projects Agency (ARPA). The ARPANET was developed in response to the Cold War.







Source: Saxena and Arora (2009)



Importance of computer network:

- Provides the best way of business communication.
- Streamline communication.
- Cost-effective resource sharing.
- Improving storage efficiency and volume.
- Cut costs on software.
- Cut costs on hardware.
- Utilizes Centralized Database.
- Increase in efficiency.
- Optimize convenience and flexibility.
- Allows File sharing.
- sharing of peripherals and internet access.
- Network gaming.
- Voice over IP (VoIP)
- Media Center Server.
- Centralized network administration, meaningless IT support.
- Flexibility.
- Allowing information sharing.
- Supporting distributed processing.
- User communication.
- Overcoming geographic separation.

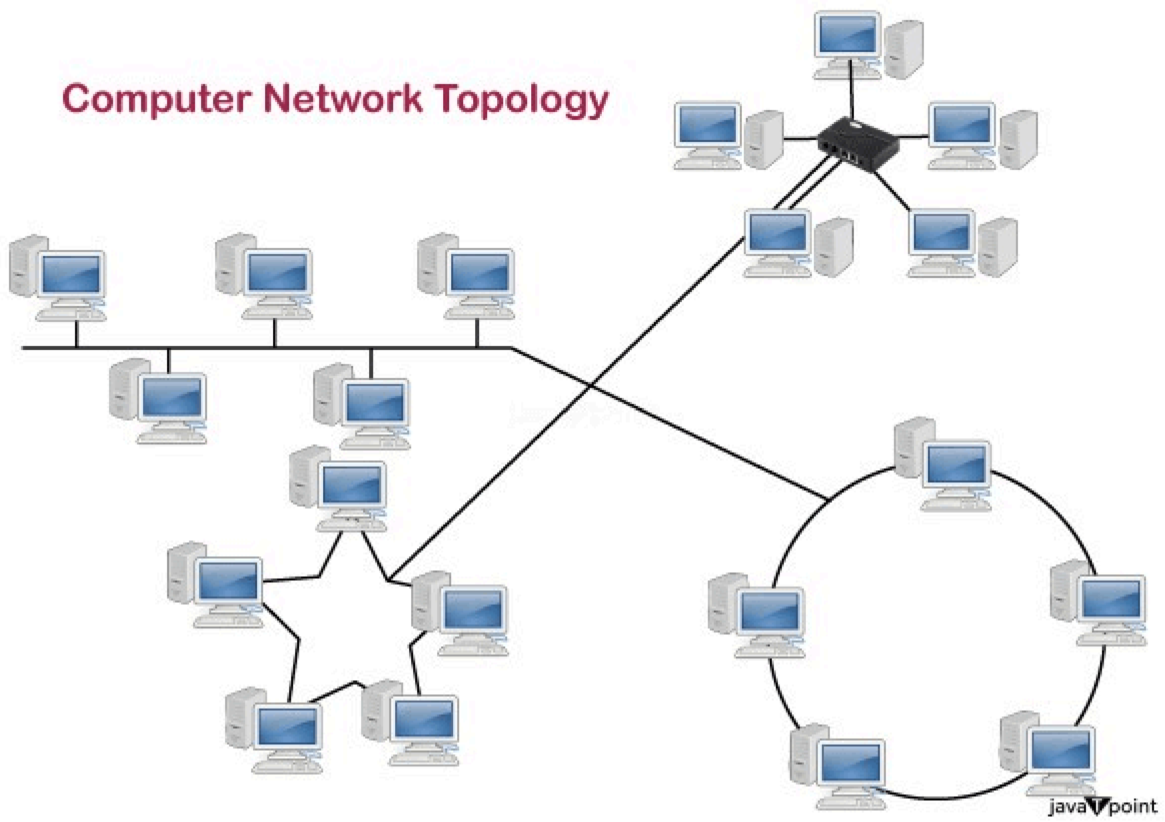
Key Elements:

Nodes: Nodes are the individual devices connected to the network. Examples include computers, servers, printers, and other devices.

Links: Links refer to the communication channels that connect nodes in a network. These can be wired, such as Ethernet cables, or wireless, like Wi-Fi connections.

Protocols: Protocols are a set of rules and conventions that govern how data is transmitted and received across a network. Examples include TCP/IP (Transmission Control Protocol/Internet Protocol), which is fundamental to the functioning of the Internet.

Topology: Topology refers to the physical or logical layout of a network. Common topologies include star, bus, ring, and mesh.



Goals of Computer Network:

The goals of a computer network can vary depending on the specific requirements and objectives of the organization or individuals implementing the network.

Resource Sharing: One of the primary goals of computer networks is to facilitate the sharing of resources such as files, printers, and applications among connected devices. This enables efficient use of resources and reduces redundancy.

Data Communication: Computer networks provide a means for seamless and efficient communication of data between devices. This includes the transmission of messages, files, and other forms of data.

Remote Access: Networks enable remote access to resources and services. Users can access data and applications from different locations, promoting flexibility and mobility.

Reliability and Availability: Networks are designed to provide reliable and available access to resources. Redundancy, fault tolerance, and other measures are implemented to ensure continuous operation even in the face of hardware failures or disruptions.

Cost Efficiency: Sharing resources through a network can lead to cost savings. For example, multiple users can share a single printer or a centralized server can store and manage data for an entire organization.

Scalability: Computer networks are designed to be scalable, allowing for the addition of new devices and resources as the organization or user's needs grow.

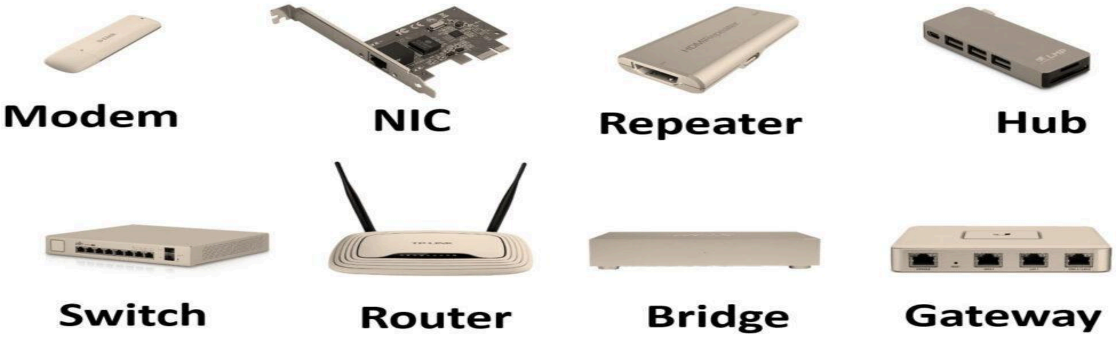
Data Security: Ensuring the security of data is a key goal of computer networks. Measures such as encryption, firewalls, and access controls are implemented to protect sensitive information from unauthorized access or malicious activities.

Components Of Computer Network-

A computer network consists of various components that work together to enable communication and resource sharing among connected devices. These components can be categorized into hardware and software components:

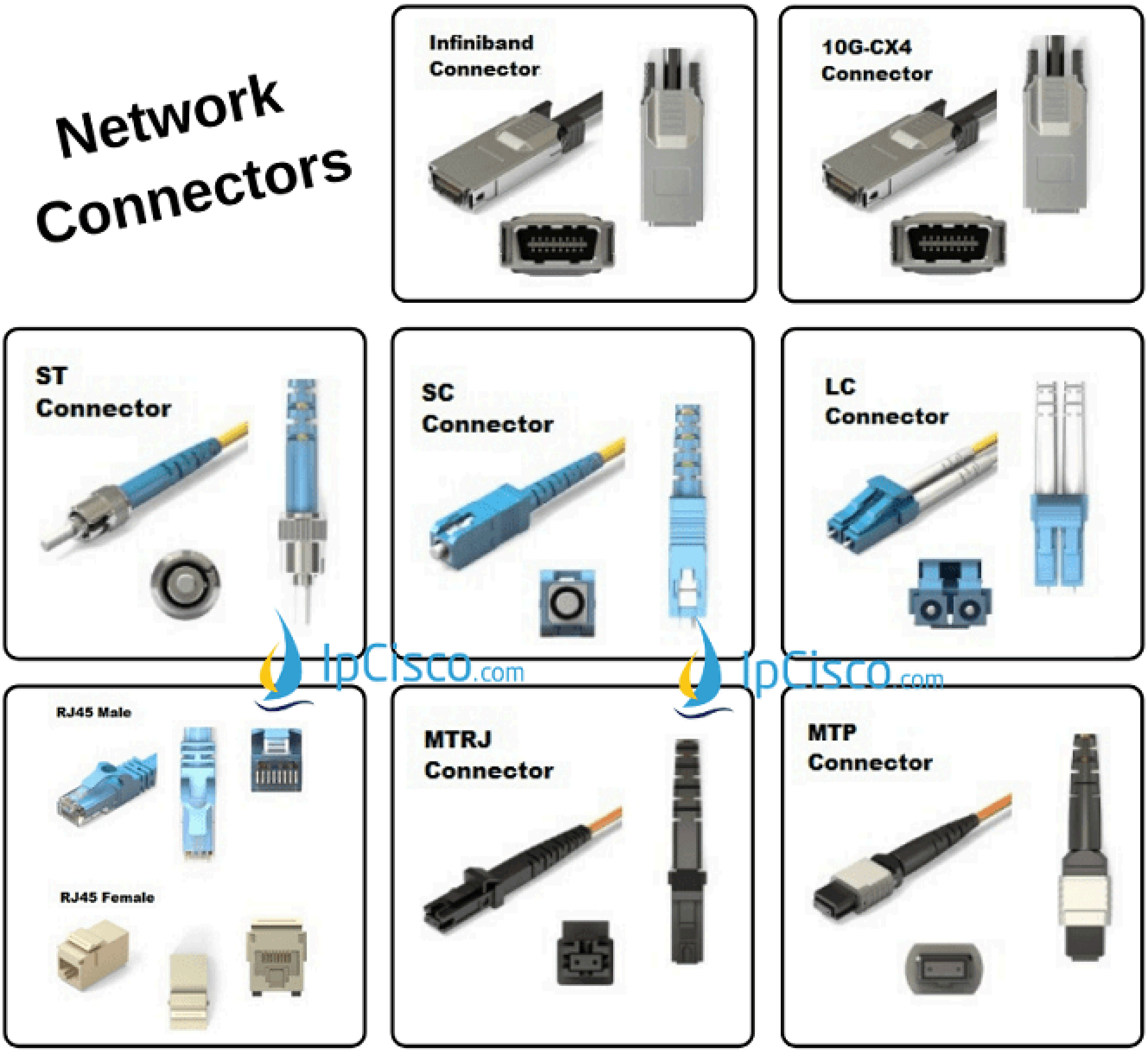
Hardware Components:

Devices/Nodes: These are the individual devices that are part of the network. Examples include computers, servers, routers, switches, printers, and other networked devices.

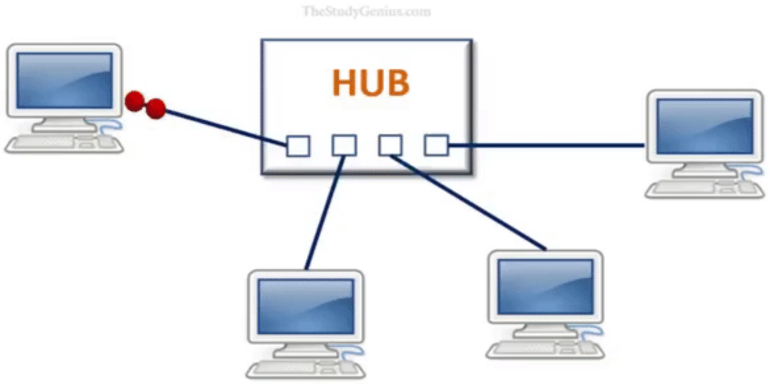


Types of Network Devices

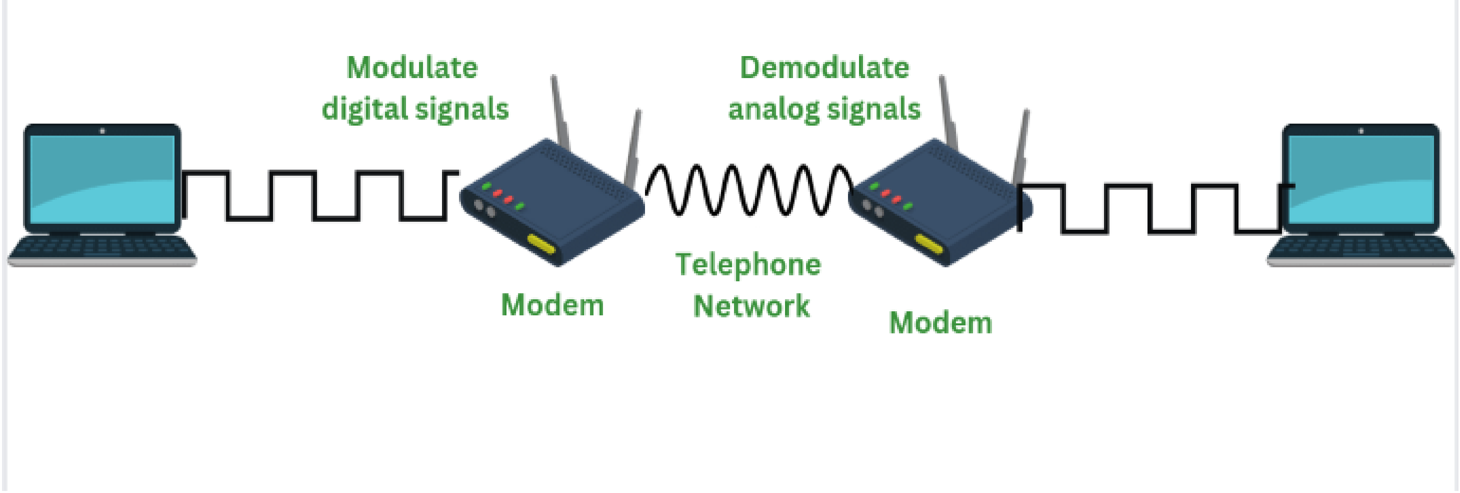
Network Cables and Connectors: Physical connections between devices are established using network cables, such as Ethernet cables. Connectors like RJ45 plugs are commonly used for wired connections.

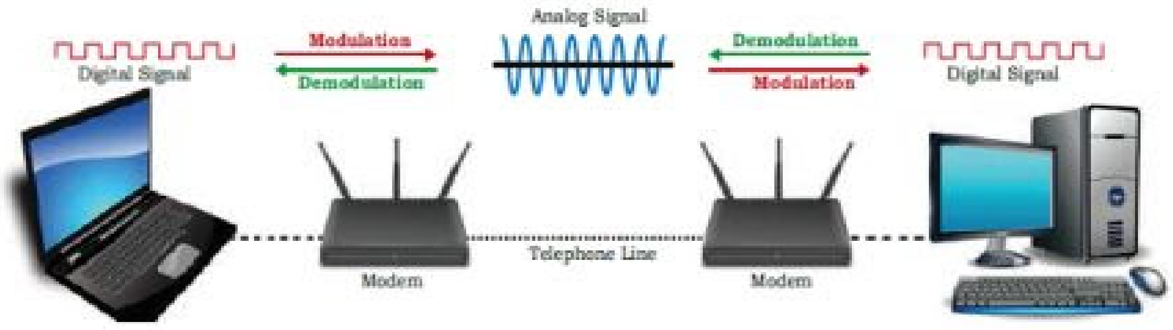


Hubs: While less common today, hubs were used to connect multiple devices in a network. Unlike switches, hubs do not intelligently manage data traffic.



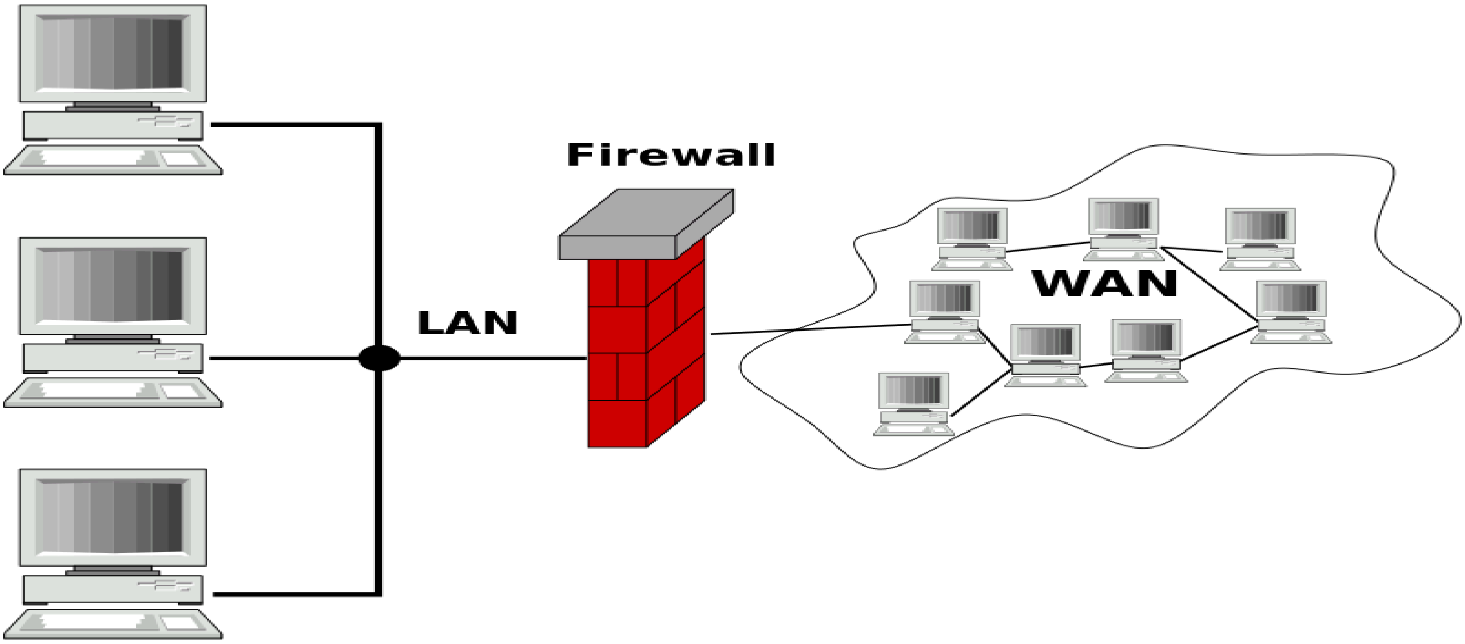
Modems: Modems (Modulator-Demodulator) are used to convert digital data from a computer into analog signals for transmission over telephone lines or other communication channels.

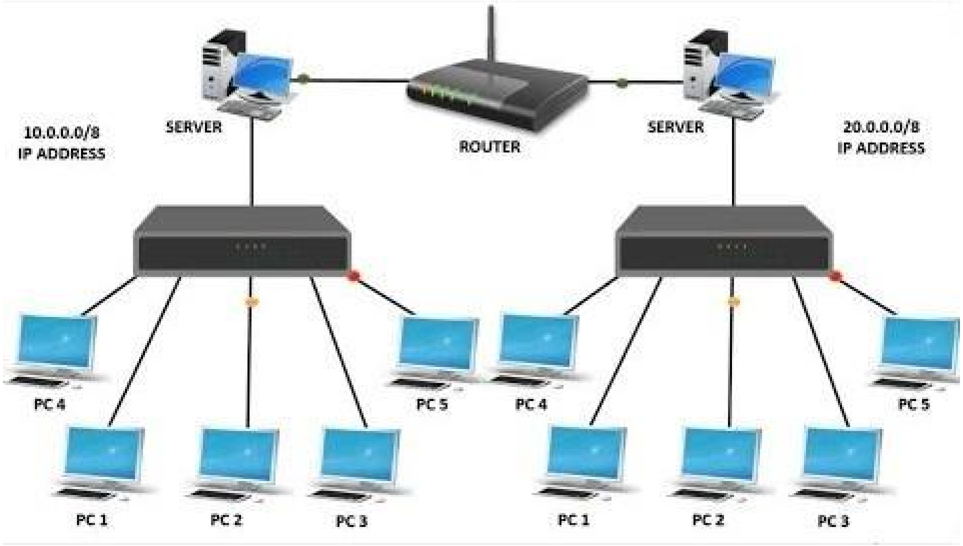




Modem Network

Firewalls: Firewalls can be both hardware and software components. They are designed to protect a network from unauthorized access and ensure the security of data.





Software Components:

Network Operating System (NOS): A network operating system is specialized software that provides network services, such as file sharing, printer sharing, and user authentication. Examples include Windows Server, Linux, and Novell NetWare.

Device Drivers: Device drivers enable the communication between the operating system and the network hardware (e.g., NIC drivers).

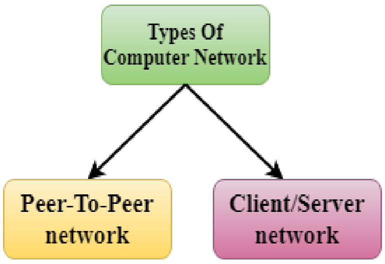
Protocol Suites: Protocols are sets of rules governing communication between devices in a network. Common protocol suites include TCP/IP (Transmission Control Protocol/Internet Protocol), which is foundational for the Internet.

Network Services: Various network services are provided by software components, including DNS (Domain Name System) for translating domain names to IP addresses, DHCP (Dynamic Host Configuration Protocol) for automatic IP address assignment, and more.

Computer Network Architecture

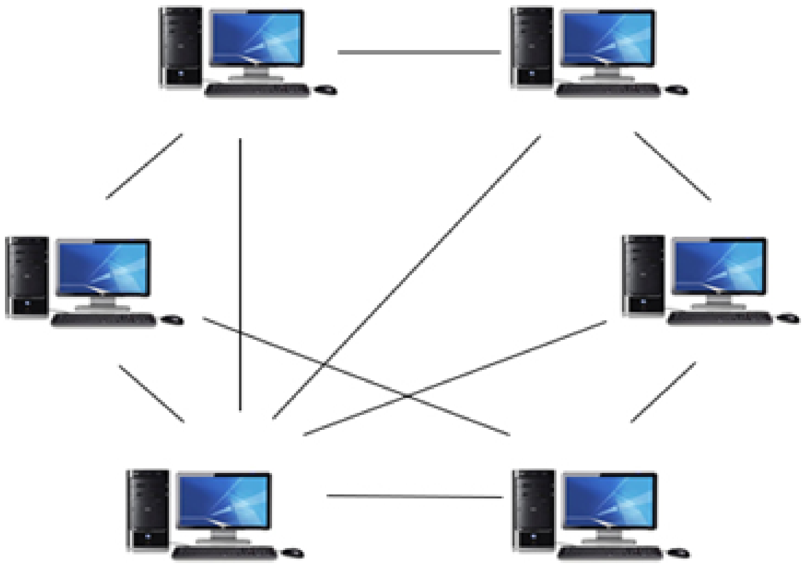
Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:



Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages of Peer-To-Peer Network:

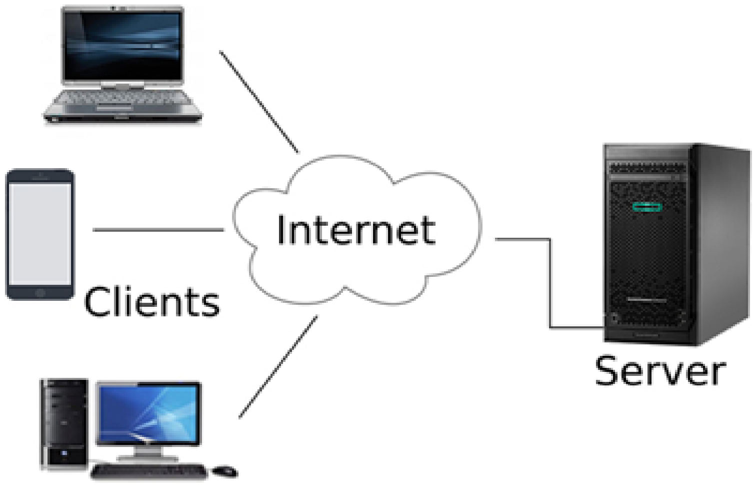
- It is less costly as it does not contain any dedicated server.
- If one computer stops working, other computers will not stop working.

Disadvantages of Peer-To-Peer Network:

- In the case of the Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a server while all other computers in the network are called clients.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to client 1 to initiate its communication with client 2.



Advantages of Client/Server network:

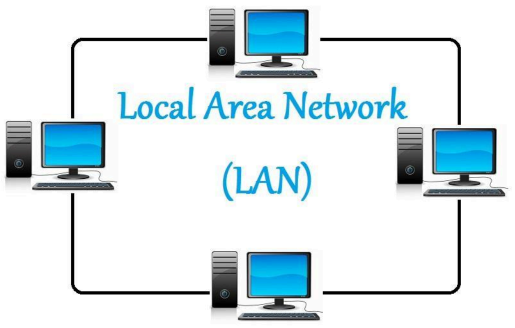
- A Client/Server network contains a centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.

Disadvantages of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.

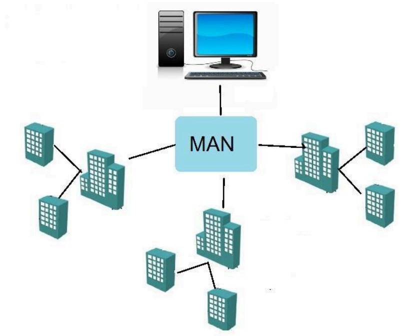
Types of Computer Network-

There are computer networks that help in building social relationships. These networks depend upon the speed at which the internet is provided. All these three networks, i.e., LAN, MAN, and WAN, are used for providing internet services to people.

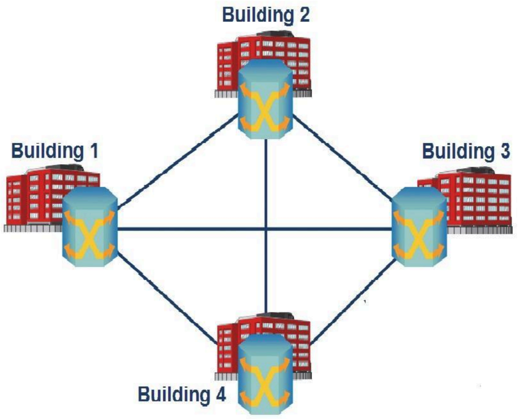


Local Area Network (LAN)

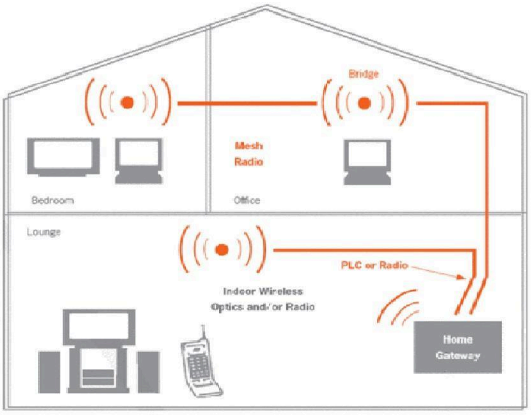
(WAN) Wide Area Network



Metropolitan Area Network



Campus Area Network(CAN)



Home Area Network(HAN)

Let us discuss about them in detail:

Basis	LAN	MAN	WAN
Full-Form	LAN stands for local area network.	MAN stands for metropolitan area network.	WAN stands for wide area network.
Geographic Span	Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as countries or continents.
Ownership	LAN's ownership is private.	MAN's ownership can be private or public.	While WAN also might not be owned by one organization.
Transmission Speed	The transmission speed of a LAN is high.	While the transmission speed of a MAN is average.	Whereas the transmission speed of a WAN is low.

Propagation delay	The propagation delay is short in a LAN.	There is a moderate propagation delay in a MAN.	Whereas, there is a long propagation delay in a WAN.
Congestion	There is less congestion in LAN.	While there is more congestion in MAN.	Whereas there is more congestion than MAN in WAN.
Design & Maintenance	LAN's design and maintenance are easy.	While MAN's design and maintenance are more difficult than LAN.	Whereas WAN's design and maintenance are also more difficult than LAN as well as MAN.
Fault tolerance	There is more fault tolerance in LAN.	While there is less fault tolerance.	In WAN, there is also less fault tolerance.

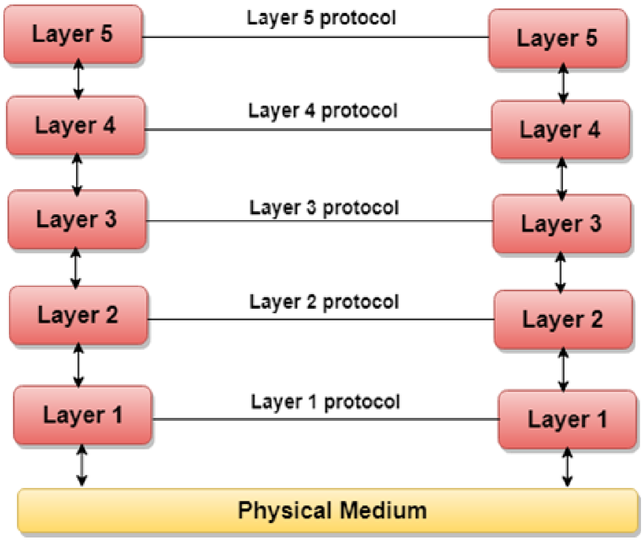
Layered Architecture-

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- The basic elements of layered architecture are services, protocols, and interfaces.

Service: It is a set of actions that a layer provides to the higher layer.

Protocol: It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern both the contents and order of the messages used.

Interface: It is a way through which the message is transferred from one layer to another layer.



- layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- A set of layers and protocols is known as network architecture.

Evolution of Layered Architecture

In computer networks, layered architecture is majorly used for communication. The two network models that makes use of layered architecture are:

- OSI Model
- TCP/IP Model

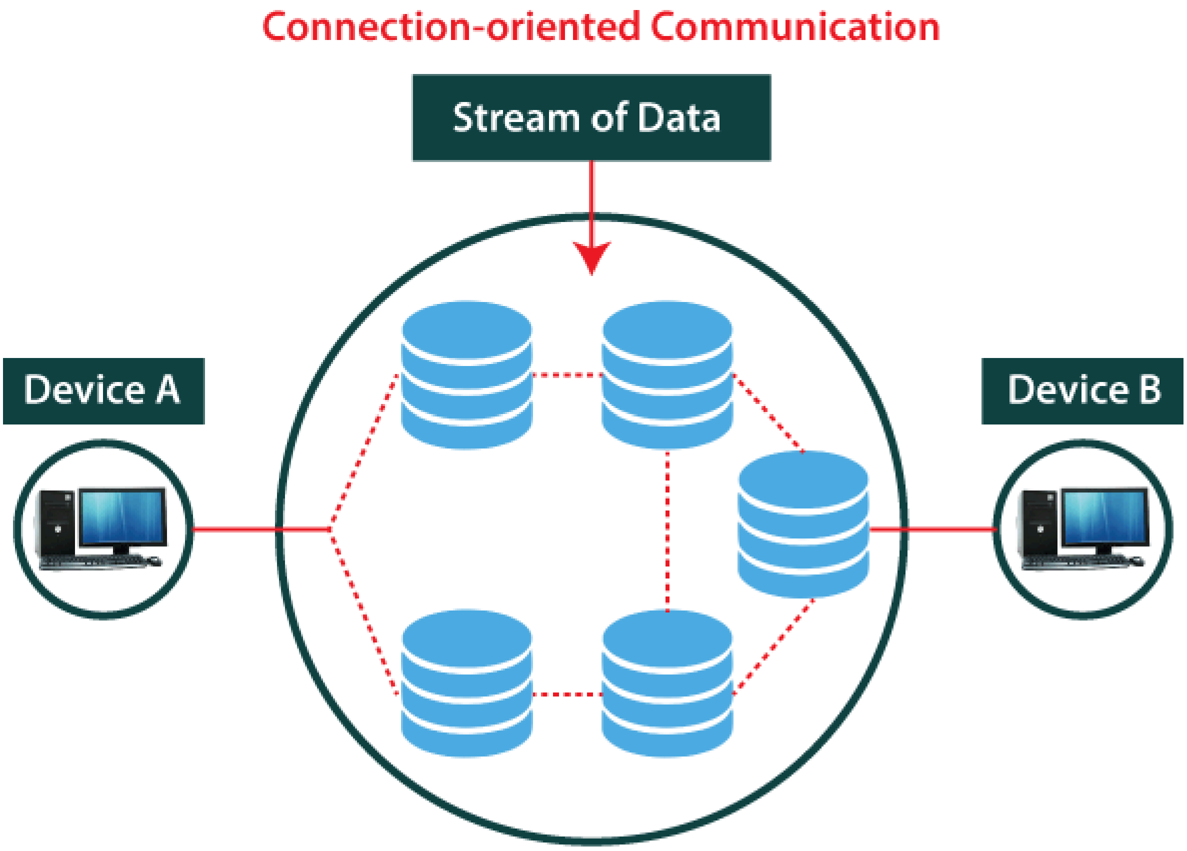
CONNECTION ORIENTED AND CONNECTIONLESS SERVICES

Connection Oriented Service:

It is a three-phase process which include-

- Connection Establishment
- Data Transfer
- Termination / disconnection

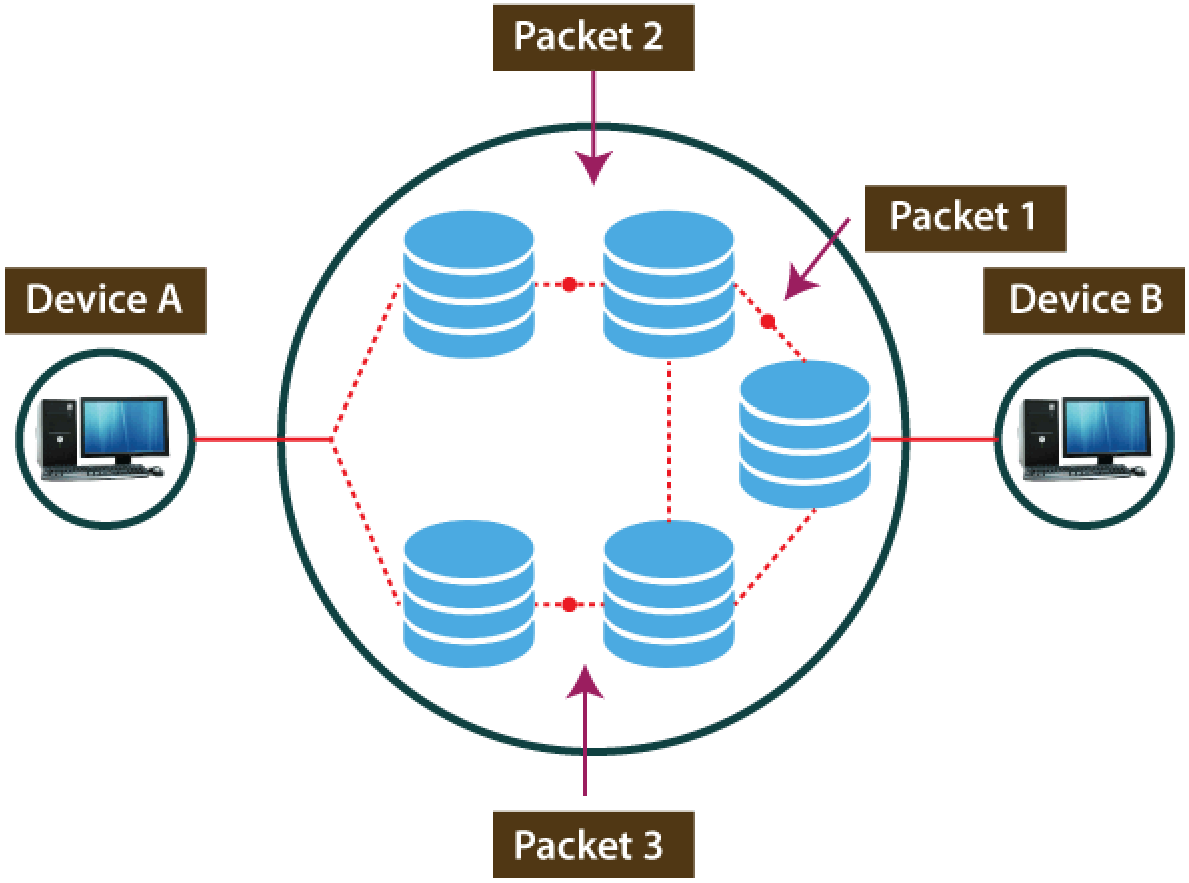
In this type of transmission, the receiving device sends an acknowledgement back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

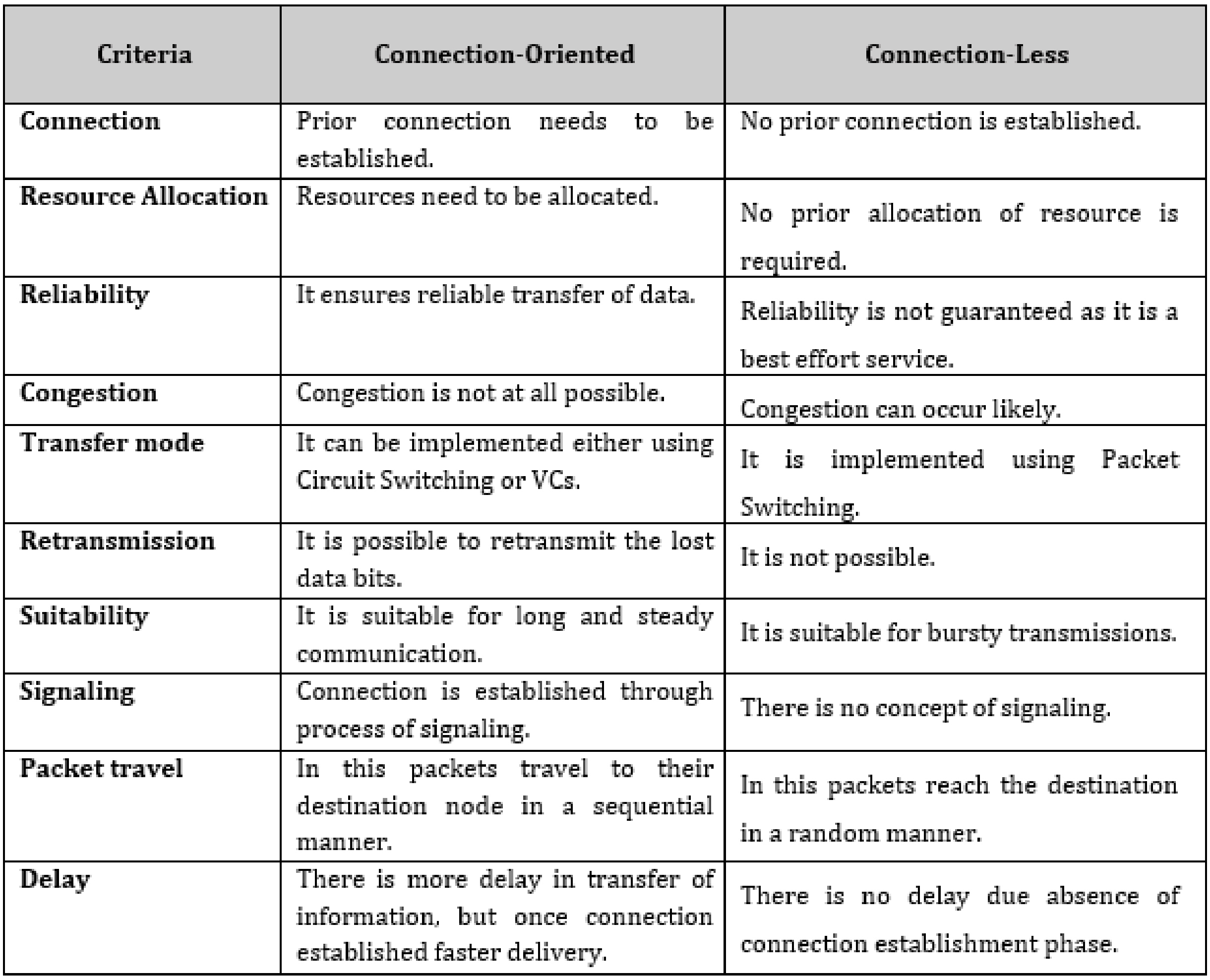


Connection less service:

It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Connectionless Communication





Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

SERVICE PRIMITIVES

- Service generally includes a set of various primitives. A **primitive simply means Operations.**
- A Service is specified by a set of primitives that are available and given to users or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by a peer entity. Each of the protocols that communicate in layered architecture also communicates in peer-to-peer manner with some of its remote protocol entities.
- Primitives are called calling functions between the layers that are used to manage communication among the adjacent protocol layers i.e., among the same communication node. The set of primitives that are available generally depends upon the nature of the service that is being provided.

Classification of Service Primitives:

Primitive	Meaning

Request	It represents an entity that wants or requests a service to perform some action or do some work (requesting for connection to a remote computer).
Indication	It represents an entity that is to be informed about an event (receiver just have received a request of connection).
Response	It represents an entity that is responding to an event (receiver is simply sending the permission or allowing it to connect).
Confirm	It represents an entity that acknowledges the response to an earlier request that has come back (sender just acknowledges the permission to get connected to the remote host).

Design issues-

Topology: Choose an appropriate network topology.

Size and Scale: Determine the network's size and scale.

Scalability: Design for future growth.

Performance: Address bandwidth and latency issues.

Reliability: Ensure continuous operation with redundancy.

Security: Implement measures to protect against threats.

Cost: Balance performance with budget constraints.

Management: Design for easy configuration and troubleshooting.

Interoperability: Ensure compatibility with different devices.

QoS: Address specific application requirements for quality of service.

Addressing and Naming: Develop strategies for IP addressing and domain naming.

Documentation: Maintain comprehensive documentation.

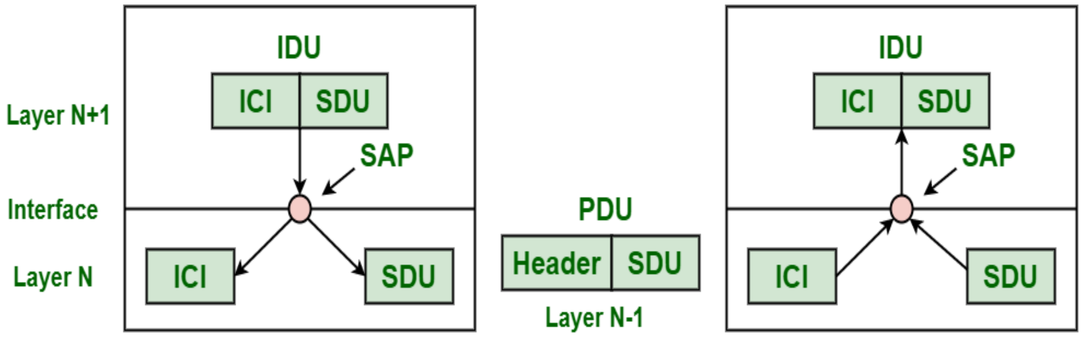
Environmental Considerations: Account for physical factors like temperature and power.

User Requirements: Align the design with end-user and application needs.

INTERFACES AND SERVICES

- Interfaces and Services is a process that generally provides and gives a common technique for each layer to communicate with each other. Standard terminology is basically required for layered networks to request and aim for the services are provided.

- Service is defined as a set of primitive operations. Services are provided by layer to each of layers above it.
- Below is diagram showing relations between layers at an interface. In the diagram, layers N+1, N, and N-1 are involved and engaged in the process of communication among each other.



Relationship Between Layers at an Interface

ISO-OSI REFERENCE MODEL

OSI stands for Open Systems Interconnection. It was developed by ISO – ‘International Organization of Standardization‘, in 1984. It is a 7 layer architecture with each layer having specific functionality to perform.

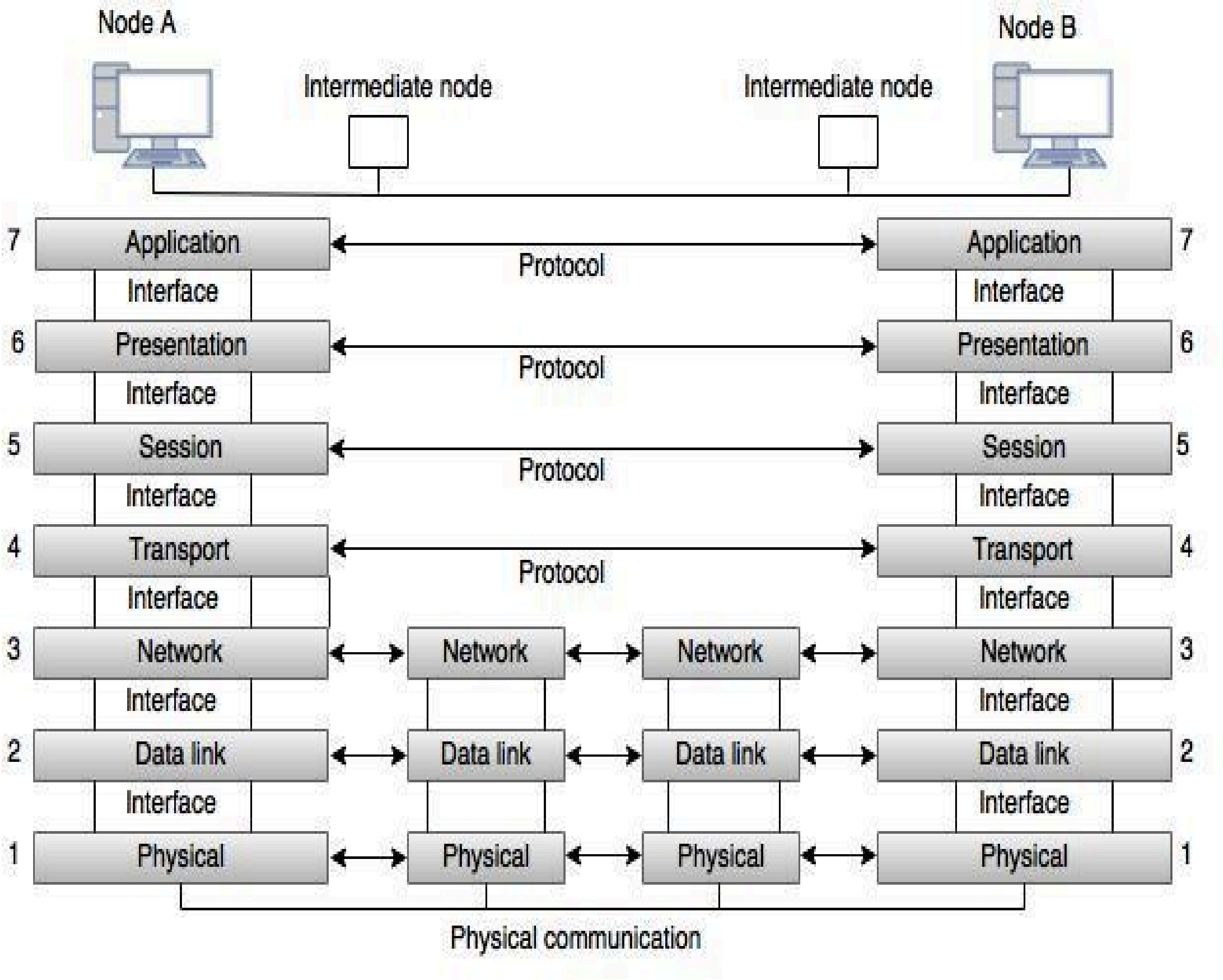
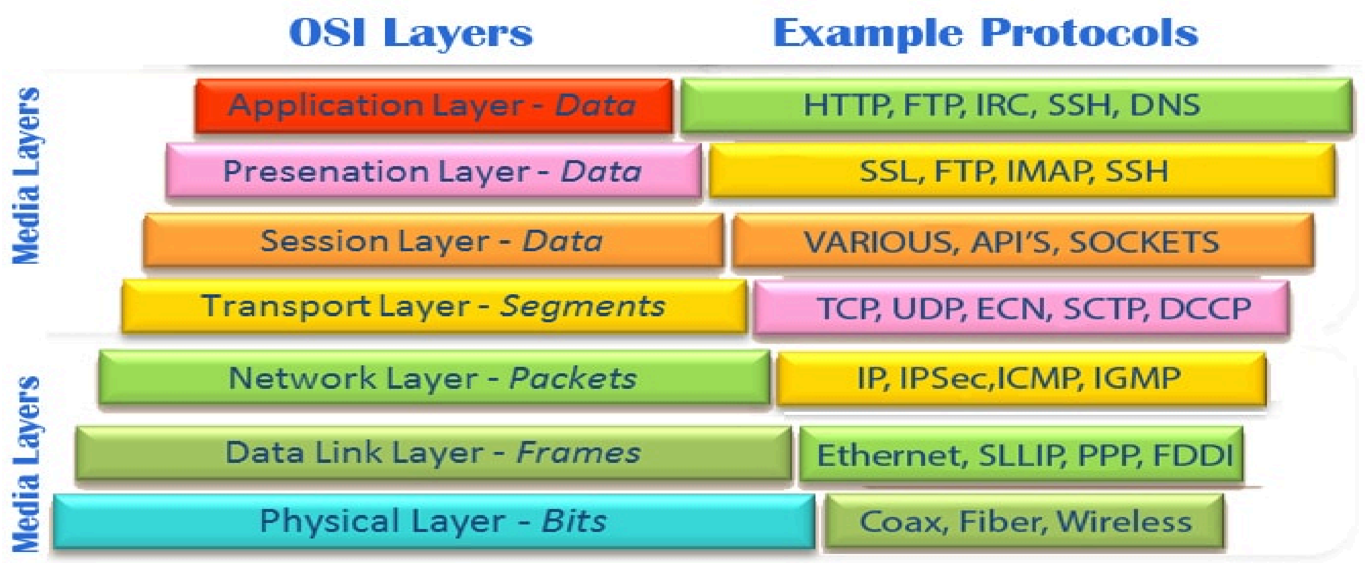
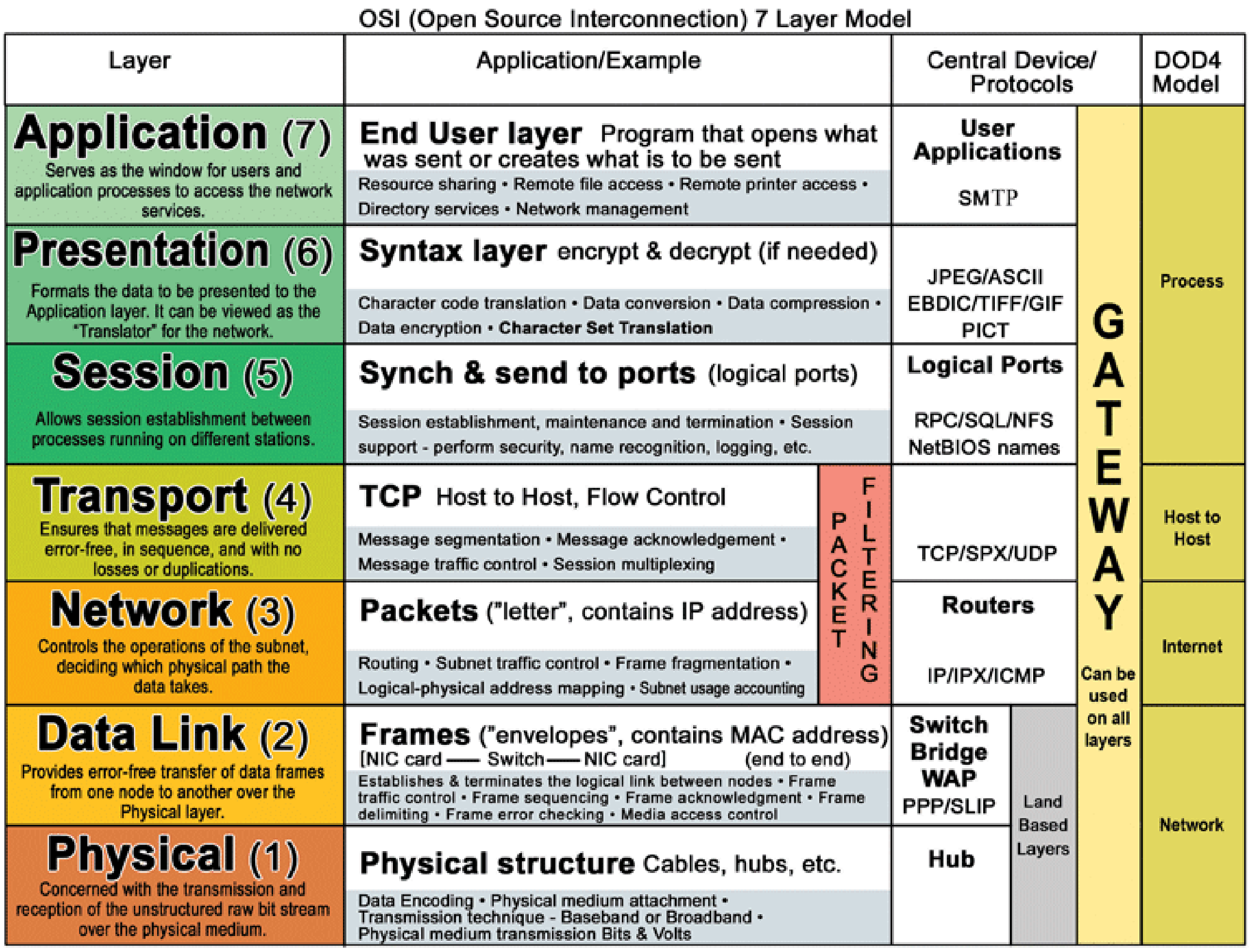


Fig: OSI Model

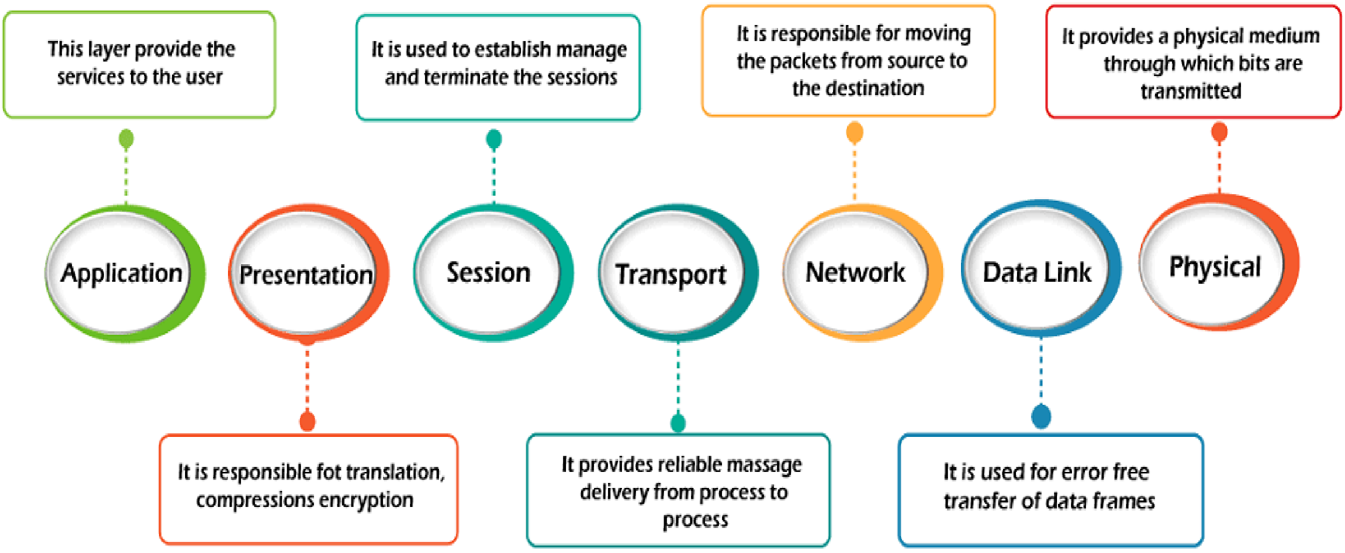


	OSI Layers	Example Protocols
Media Layers	Application Layer - *Data*	HTTP, FTP, IRC, SSH, DNS
	Presenation Layer - *Data*	SSL, FTP, IMAP, SSH
	Session Layer - *Data*	VARIOUS, API'S, SOCKETS
	Transport Layer - *Segments*	TCP, UDP, ECN, SCTP, DCCP
Media Layers	Network Layer - *Packets*	IP, IPSec,ICMP, IGMP
	Data Link Layer - *Frames*	Ethernet, SLLIP, PPP, FDDI
	Physical Layer - *Bits*	Coax, Fiber, Wireless



OSI (Open Source Interconnection) 7 Layer Model

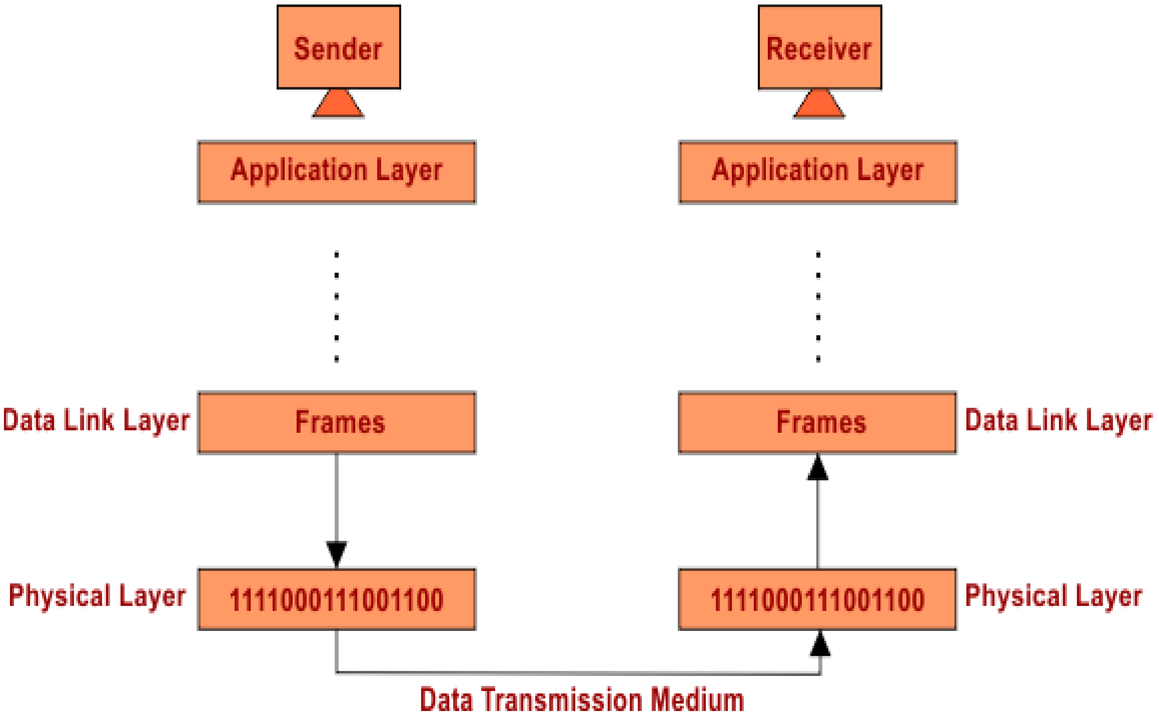
Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

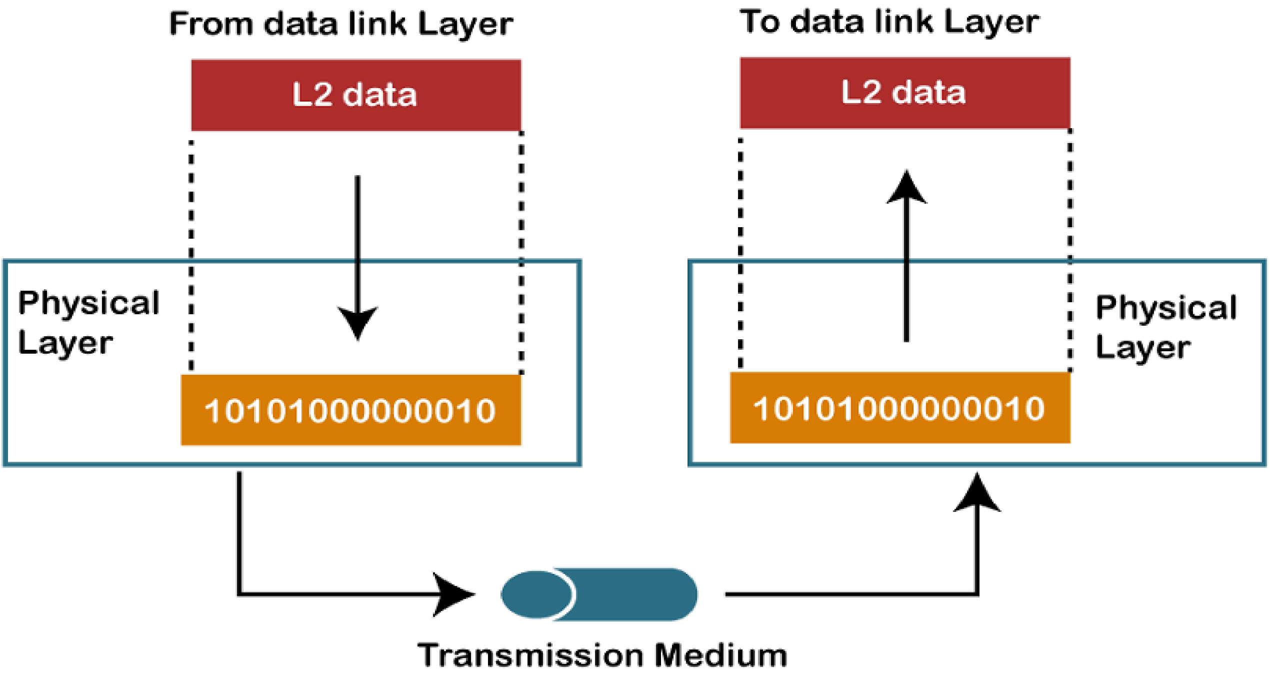


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames

Figure 1.1: OSI reference model

Layer 1: Physical layer





The physical layer has the following major functions:

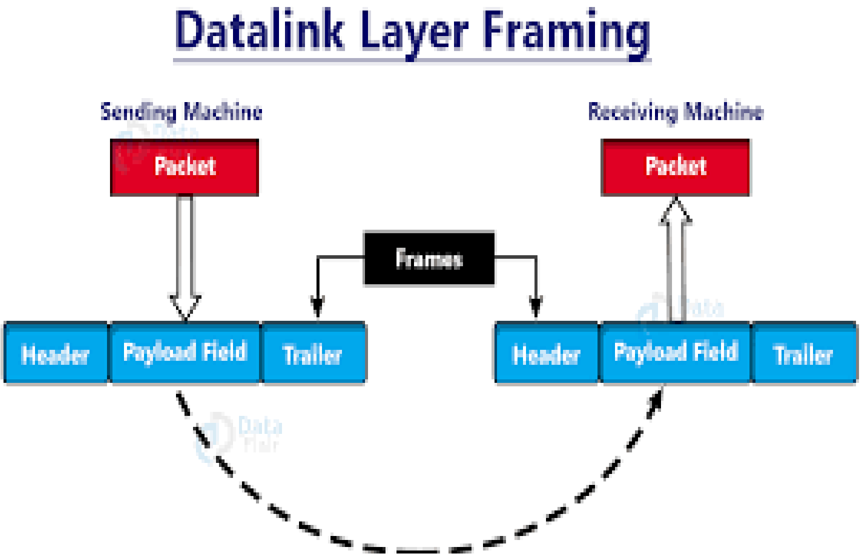
- It defines the electrical and physical specifications of the data connection.
- It defines the **relationship between a device and a physical transmission medium** (e.g., a copper or fiber optical cable).
- This includes the layout of pins, voltages, line impedance, cable specifications, signal timing, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.
- It defines the **protocol to establish and terminate a connection** between two directly connected nodes over a communications medium.

- It may define the protocol for **flow control.**
- It defines **transmission mode i.e. simplex, half duplex, full duplex.**
- It defines the **topology.**
- It defines a protocol for the provision of a (not necessarily reliable) connection between two directly connected nodes, and the modulation or conversion between the representation of digital data in user Equipment and the corresponding signals transmitted over the physical communications channel.

Cabling system components

- Adapters that connect media to physical interfaces
- Connector design and pin assignments
- Hub, repeater, and patch panel specifications
- Wireless system components
- Parallel SCSI (Small Computer System Interface)
- Network Interface Card (NIC)

Layer 2: Data link layer



The data link layer provides node-to-node data transfer - A reliable link between two directly connected nodes, by detecting and possibly correcting errors that may occur in the physical layer. The data link layer is divided into two sublayers:

Media Access Control (MAC) layer - Responsible for controlling **how devices in a network gain access to data** and permission to transmit it.

Logical Link Control (LLC) layer - Controls error checking and packet synchronization.

Basic Functions:

- **Allows a device to access the network** to send and receive messages
- **Offers a physical address** so a device’s data can be sent on the network
- **Works with a device’s networking software** when sending and receiving messages
- Provides error-detection capability

Common networking components that function at layer 2 include:

- Network interface cards
- Ethernet and Token Ring switches
- Bridges

Layer 3: Network layer

- The network layer provides the functional and procedural means of **transferring variable length data sequences (called datagrams) from one node to another connected to the same network.**
- It **translates logical network addresses into physical machine addresses.**
- Routing is also one of the main functions of the Network Layer, routing is the process of selecting paths in a network over which to send packets.
- Internet Control Message Protocol (ICMP) is network layer protocol and one of the main protocols of the Internet Protocol suite and is **used for error handling** and diagnostic purposes. Quality of Service (QOS) , although not the primary function of the network layer, is available in network layer protocols such as the Internet Protocol which allows certain traffic to be prioritized over others giving it preferential treatment.

Layer 4: Transport layer

The transport layer provides the functional and procedural means of transferring **variable- length data sequences from a source to a destination** host via one or more networks while maintaining the quality of service functions.

An example of a transport-layer protocol in the standard Internet stack is Transmission Control Protocol (TCP), usually built on top of the Internet Protocol (IP).

Some of the functions offered by the transport layer include:

- Application identification
- Client-side entity identification
- Confirmation that the entire message arrived intact
- Segmentation of data for network transport
- Control of data flow to prevent memory overruns
- Establishment and maintenance of both ends of virtual circuits
- Transmission-error detection
- Realignment of segmented data in the correct order on the receiving side
- Multiplexing or sharing of multiple sessions over a single physical link.

Layer 5: Session layer

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application.

It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network. Session layer functionality includes:

- □ Virtual connection between application entities
- □ Synchronization of data flow
- □ Creation of dialog units
- □ Connection parameter negotiations
- □ Partitioning of services into functional groups
- □ Acknowledgements of data received during a session
- □ Retransmission of data if it is not received by a device

Layer 6: Presentation layer

The presentation layer is responsible for how an application formats the data to be sent out onto the network. The presentation layer basically allows an application to read (or understand) the message.

Examples of presentation layer functionality include:

- □ Encryption and decryption of a message for security
- □ Compression and expansion of a message so that it travels efficiently
- □ Graphics formatting
- □ Content translation
- □ System-specific translation

Layer 7: Application layer

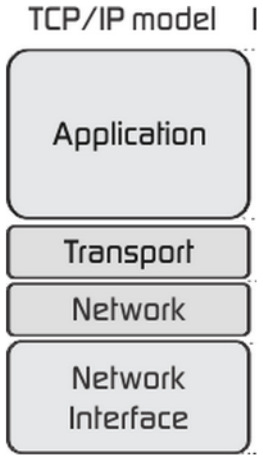
- The application layer provides an interface for the end user operating a device connected to a network.
- This layer is what the user sees, in terms of loading an application (such as Web browser or e-mail.

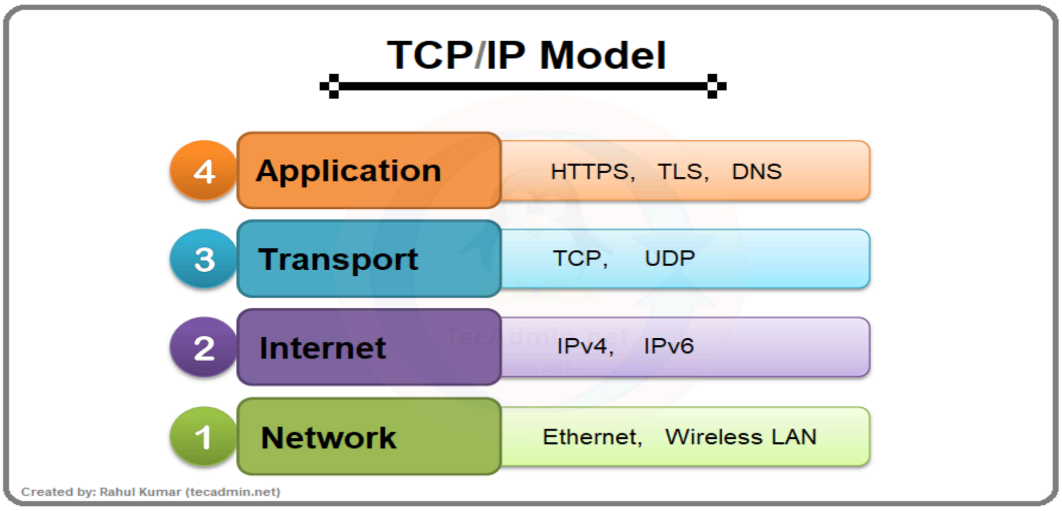
Examples of application layer functionality include:

□ Support for file transfers
□ Ability to print on a network
□ Electronic mail
□ Electronic messaging
□ Browsing the World Wide Web

TCP/IP MODEL

- The TCP/IP reference model is the network model used in the current Internet architecture. It is considered as the grandfather of the Internet, the ARPANET. The reference model was named after two of its main protocols, TCP (Transmission control Protocol) and IP (Internet Protocol).
- There are versions of this model with four layers and with five layers. The original four-layer version of the model is shown below.





Layer 4: Application Layer: The Application Layer in the TCP/IP model combines the functions of three layers from the OSI model: the Application, Presentation, and Session layers. This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- **HTTP and HTTPS:**HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions.
- **SSH:**SSH stands for Secure Shell. It is a terminal emulation software similar to Telnet. The reason SSH is preferred is because of its ability to **maintain the encrypted connection**. It sets up a secure session over a TCP/IP connection.
- **NTP:**NTP stands for Network Time Protocol. It is used to **synchronize the clocks** on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Layer 3: Host-To-Host (Transport) Layer: The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- **UDP:** The datagram delivery service is provided by UDP , the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

Layer 2: Internet or Internetworking Layer: This layer parallels the functions of OSI's Network layer. It defines the protocols which are **responsible for the logical transmission of data over the entire network**. The main protocols residing at this layer are as follows:

- **IP:**IP stands for Internet Protocol and it is responsible for **delivering packets from the source host to the destination** host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
- **ICMP:**ICMP stands for Internet Control Message Protocol. It is **encapsulated within IP datagrams** and is **responsible for providing hosts with information about network problems**.
- **ARP:**ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet. The Internet Layer is **responsible for routing packets of data from one device to another across a network**. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.

Example: Imagine that you are using a computer to send an email to a friend. When you click "send," the email is broken down into smaller packets of data, which are then sent to the Internet Layer for routing. The Internet Layer assigns an IP address to each packet and uses routing tables to determine the best route for the packet to take to reach its destination. The packet is then forwarded to the next hop on its route until it reaches its destination. When all of the packets have been delivered, your friend's computer can reassemble them into the original email message.

In this example, the Internet Layer plays a crucial role in delivering the email from your computer to your friend's computer. It uses IP addresses and routing tables to determine the best route for the packets to take, and it ensures that the packets are delivered to the correct destination. Without the Internet Layer, it would not be possible to send data across the Internet.

Layer 1: Network Access Layer: The Network Access Layer represents a collection of applications that require network communication. This layer is **responsible for generating data and initiating connection requests.** It operates on behalf of the sender to manage data transmission, while the Network Access layer on the receiver's end processes and manages incoming data.
The packet's network protocol type, in this case, TCP/IP, is identified by the network access layer. **Error prevention and "framing**" are also provided by this layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

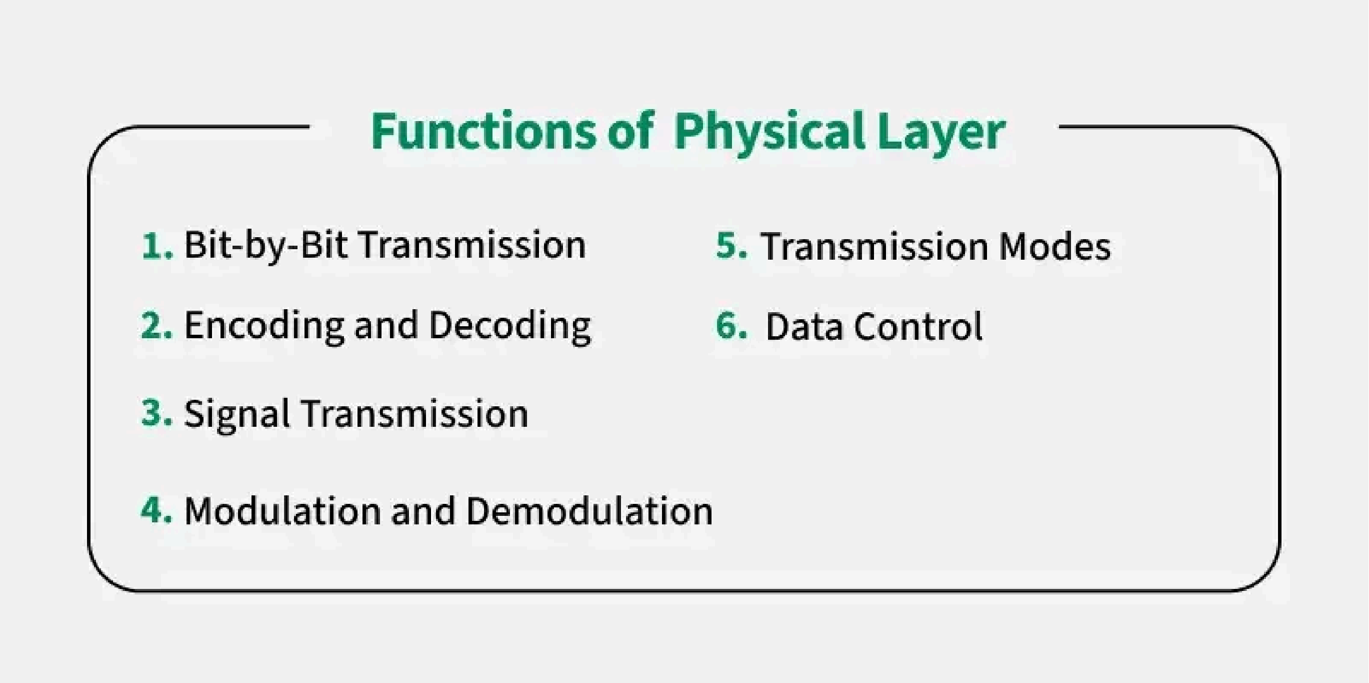
Principal of physical layer-

- The Physical Layer is the first layer of the OSI (Open Systems Interconnection) model and is primarily concerned with the physical transmission of data bits over a physical medium.
- It deals with the hardware aspects of transmitting raw binary data over a physical link or medium, without concern for the higher-layer protocols.
- The physical layer converts the data frame received from the data link layer into bits, i.e., in terms of ones and zeros. It maintains the data quality by implementing the required protocols on different network

modes and maintaining the bit rate through data transfer using a wired or wireless medium.

Functions Performed by Physical Layer

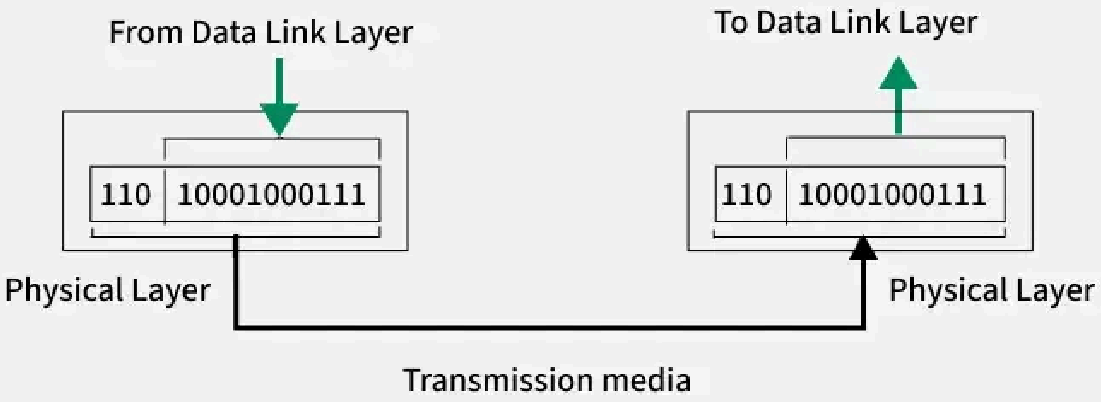
The **Physical Layer** is responsible for sending raw data as bits over a physical medium. It converts data into signals that can travel through wires, fiber optics, or wireless channels (**encoding**) and turns these signals back into data at the receiver (**decoding**). It ensures signals are transmitted correctly and uses techniques like **modulation** to prepare the data for transmission and **demodulation** to retrieve it at the other end. This layer also decides how data flows (one-way, two-way alternately, or simultaneously) through **transmission modes** and controls the speed and timing of data transmission to keep everything running smoothly.



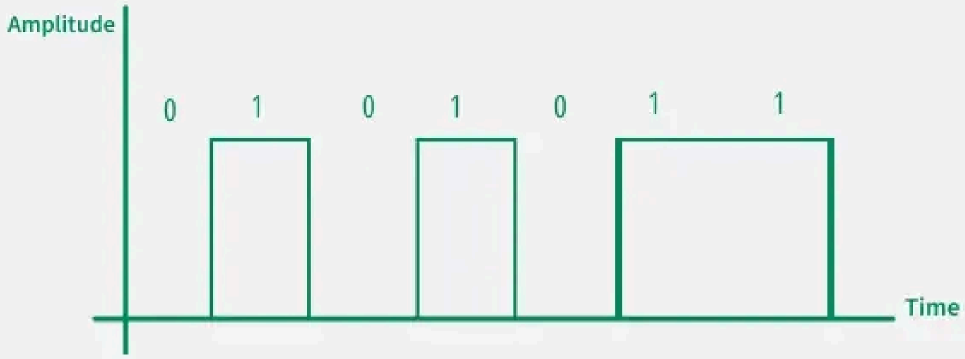
Functions of Physical Layer

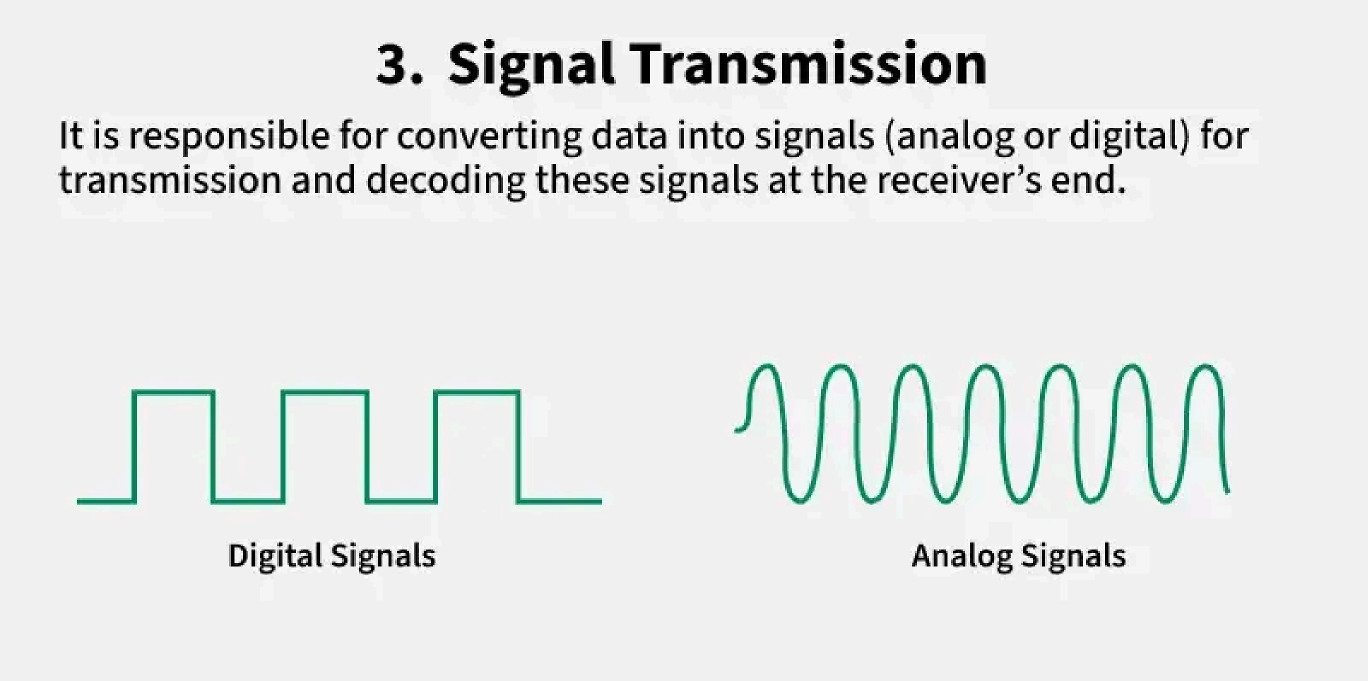
1. Bit-by-Bit Transmission
2. Encoding and Decoding
3. Signal Transmission
4. Modulation and Demodulation
5. Transmission Modes
6. Data Control

1. Bit-by-Bit Transmission



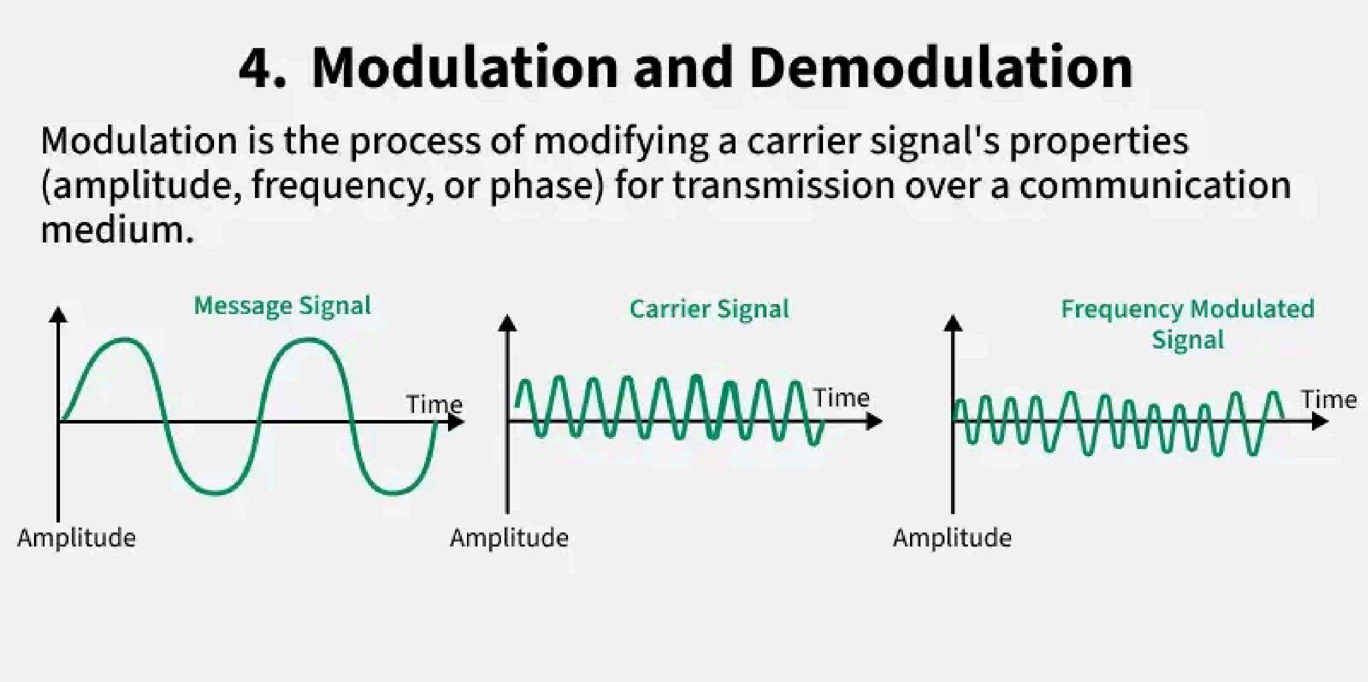
2. Encoding and Decoding





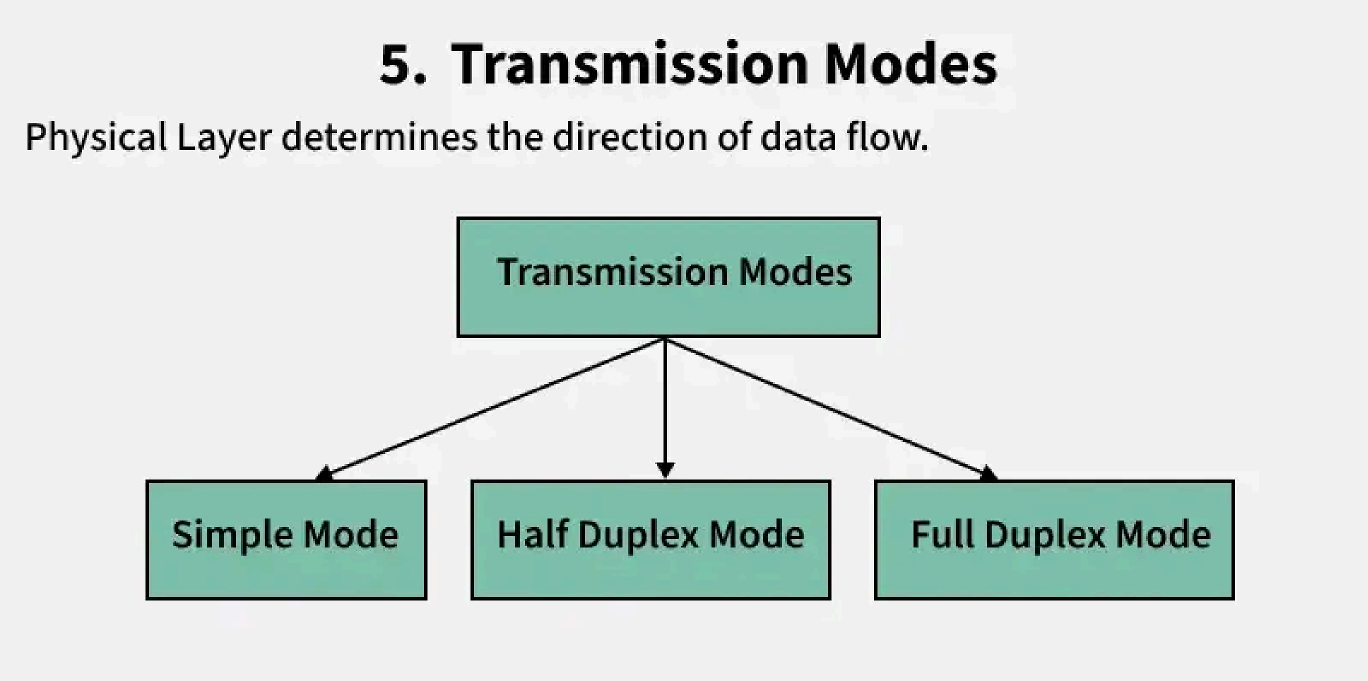
3. Signal Transmission

It is responsible for converting data into signals (analog or digital) for transmission and decoding these signals at the receiver's end.



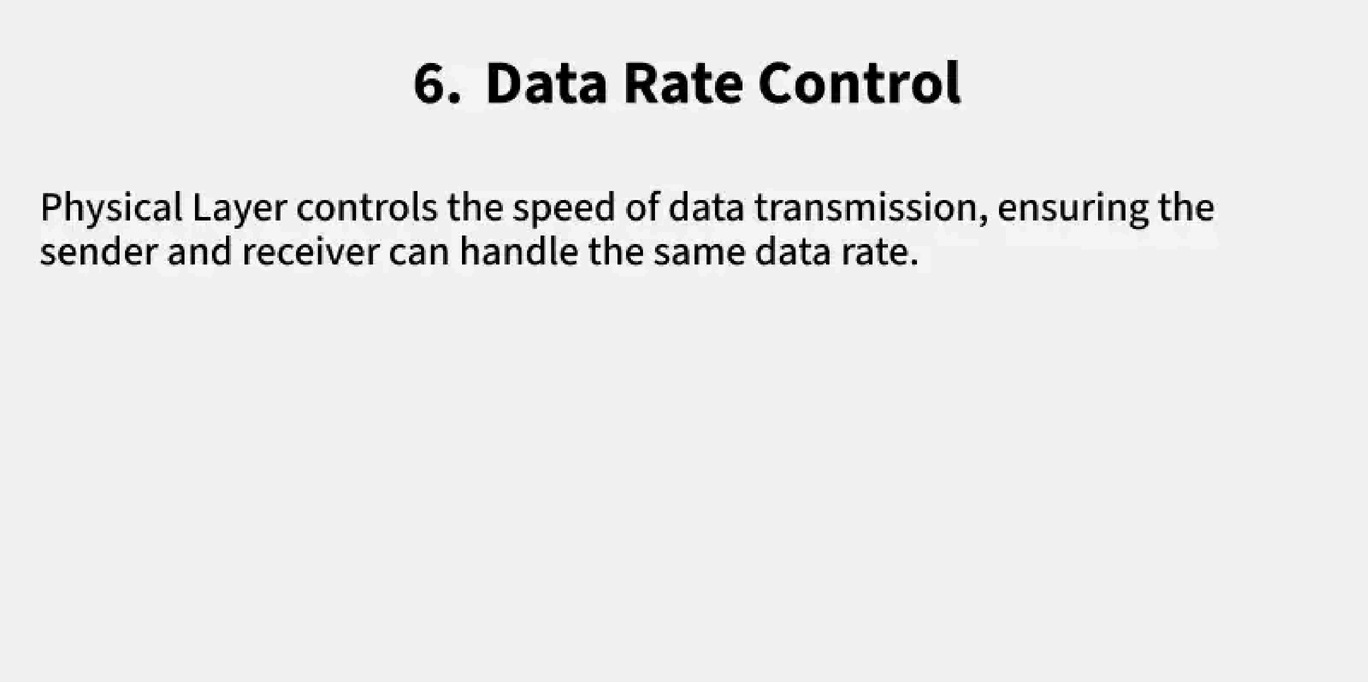
4. Modulation and Demodulation

Modulation is the process of modifying a carrier signal's properties (amplitude, frequency, or phase) for transmission over a communication medium.



5. Transmission Modes

Physical Layer determines the direction of data flow.

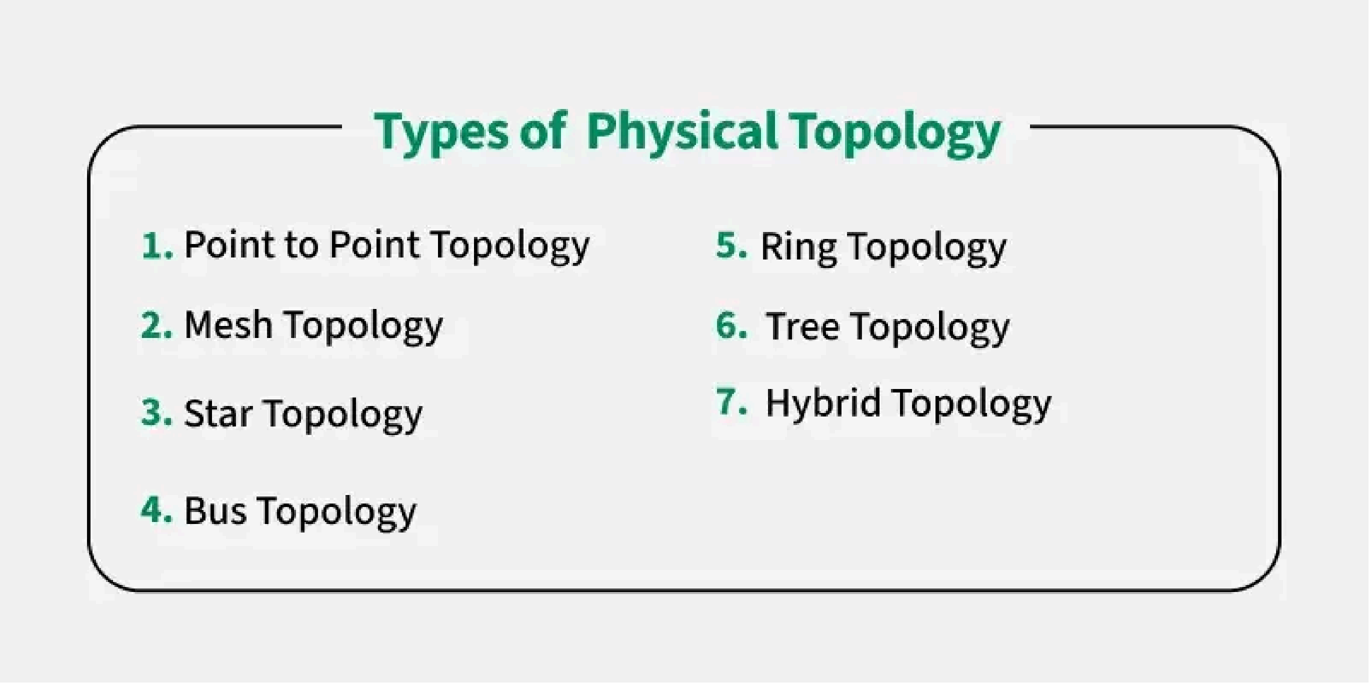


6. Data Rate Control

Physical Layer controls the speed of data transmission, ensuring the sender and receiver can handle the same data rate.

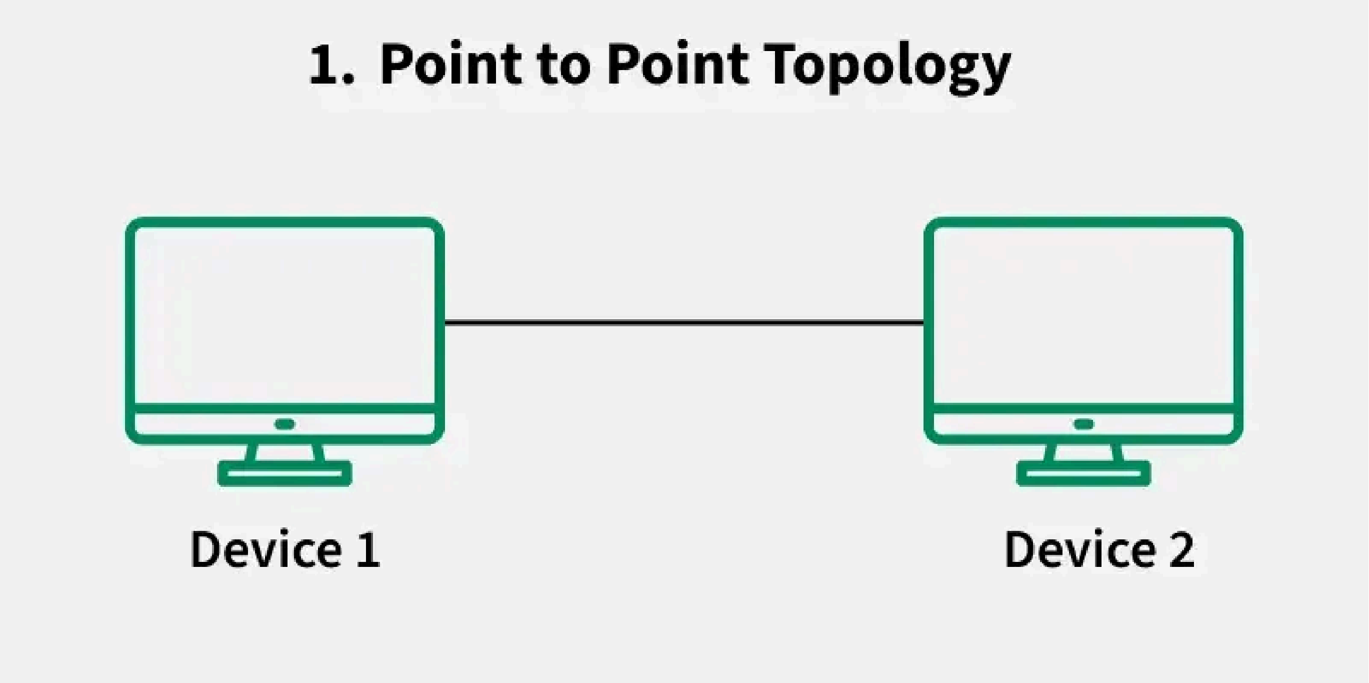
Physical Topologies

Physical topologies describe the physical arrangement of devices and cables in a network. Let’s take a look into different types of physical topologies :

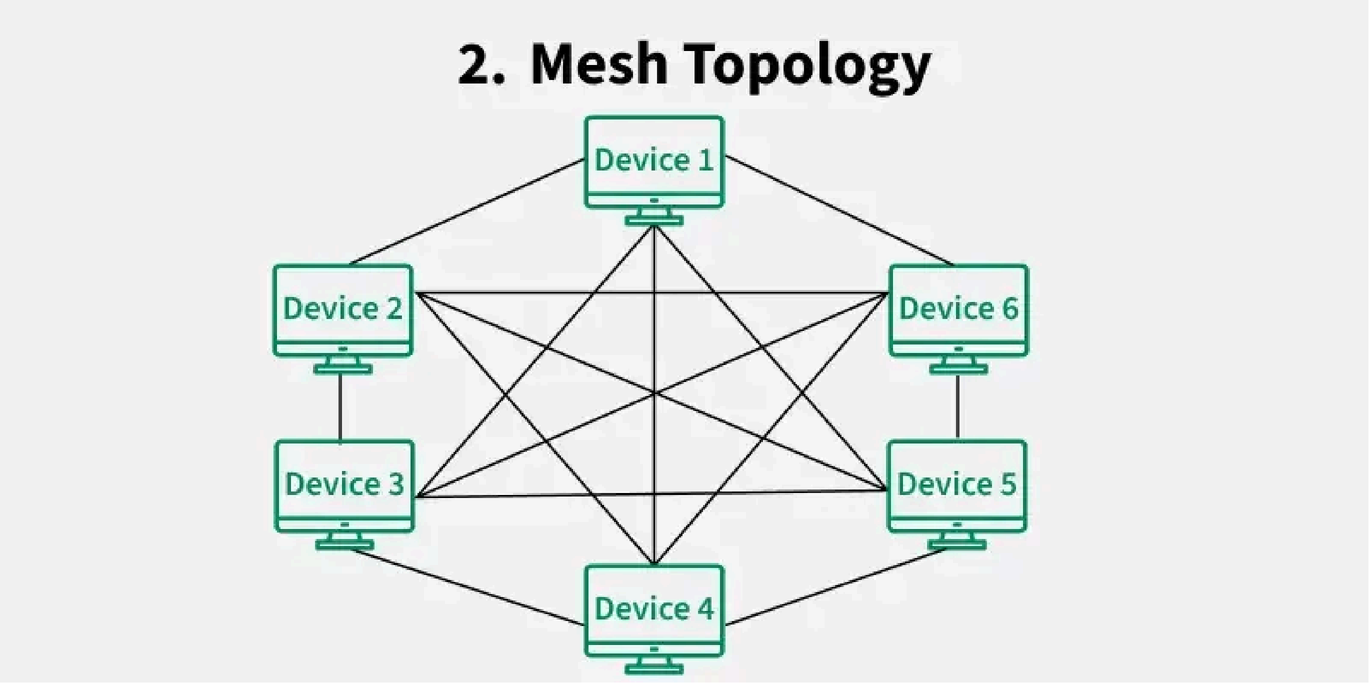


Types of Physical Topology

1. Point to Point Topology
2. Mesh Topology
3. Star Topology
4. Bus Topology
5. Ring Topology
6. Tree Topology
7. Hybrid Topology



Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the **protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.**

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is N C 2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

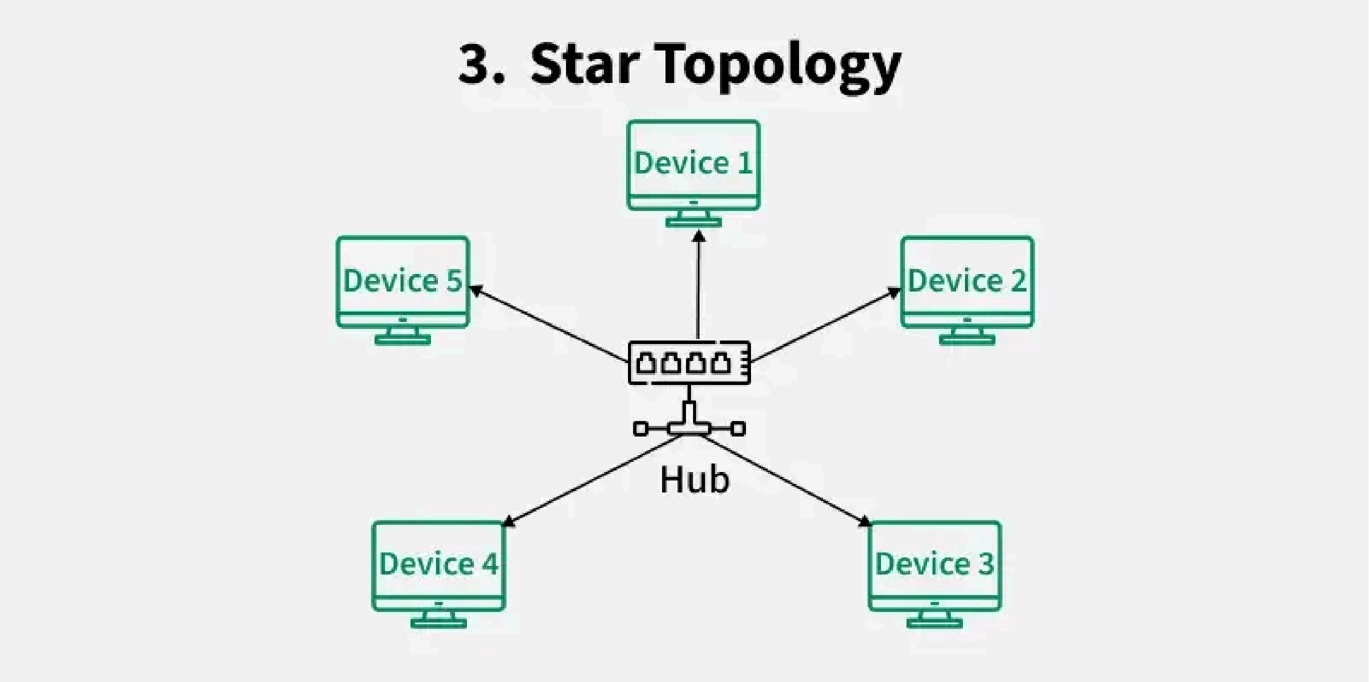
- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration are difficult.

- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A **common example of mesh topology is the internet backbone**, where various internet service providers are connected to each other via dedicated channels. This topology is **also used in military communication systems and aircraft navigation systems.**



In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. **Active hubs have repeaters in them**. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than

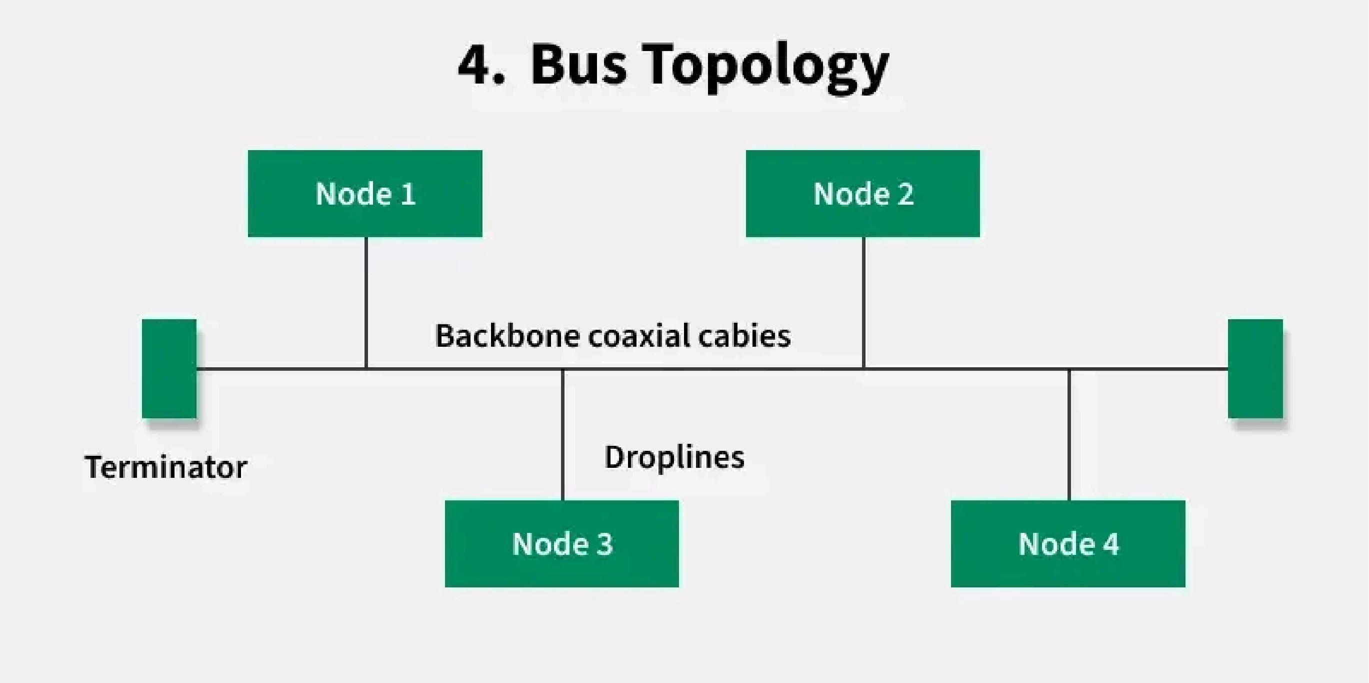
that.

- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a **local area network (LAN)** in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.



Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.

Advantages of Bus Topology

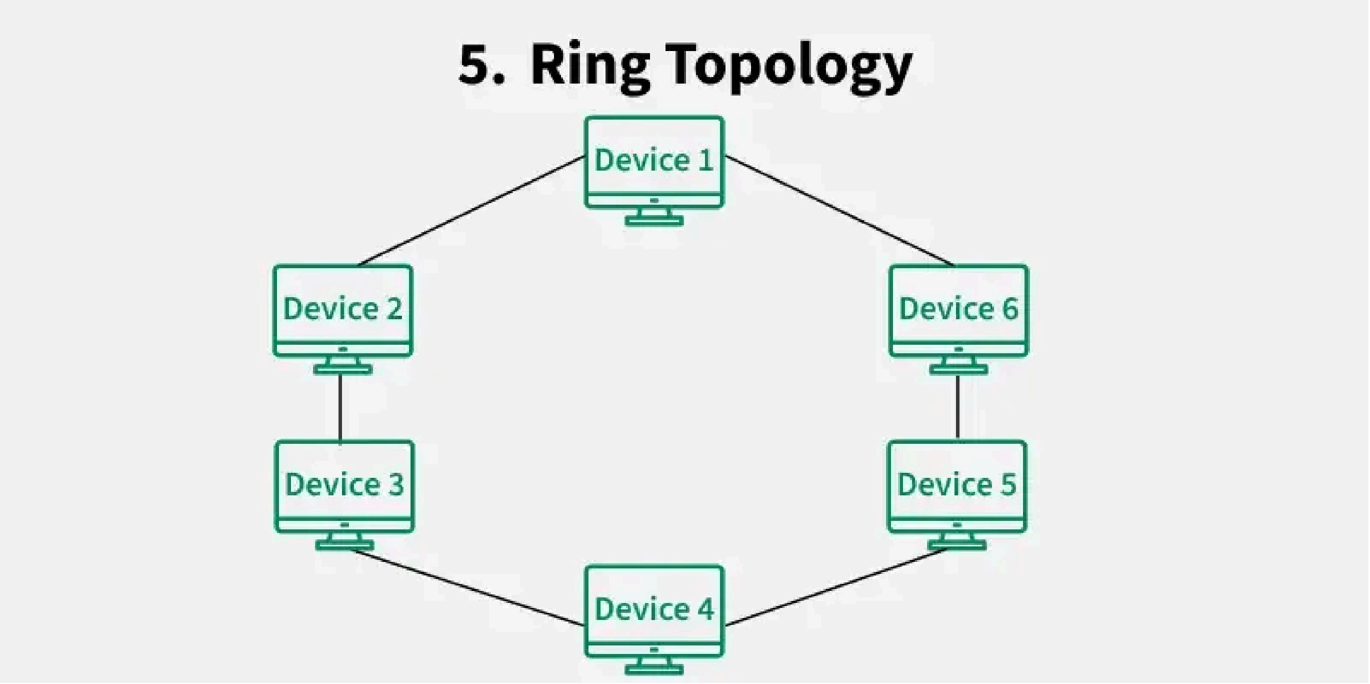
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.

- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Disadvantages of Bus Topology

- A bus topology is quite simple, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A **common example of bus topology is the Ethernet LAN**, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.



In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.
The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

- One station is known as a **monitor** station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

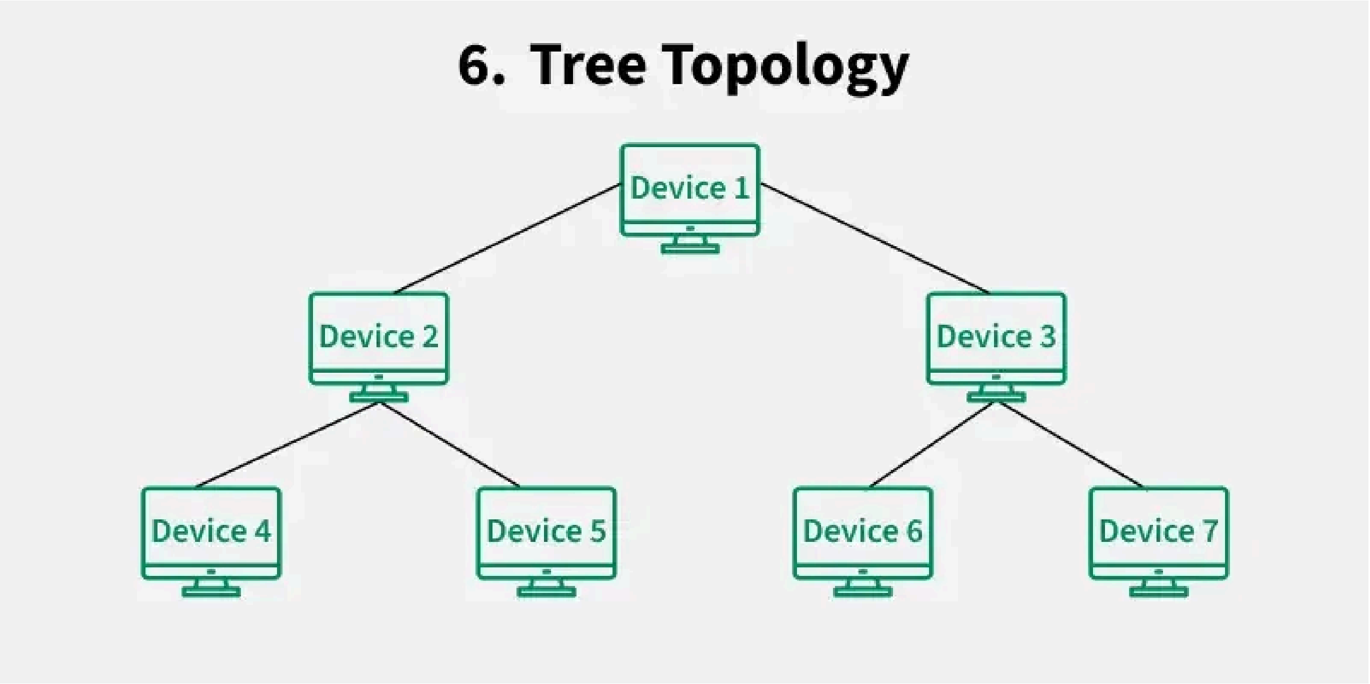
Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.

- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.



Tree topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like **DHCP** and **SAC (Standard Automatic Configuration)** are used.

In tree topology, the various secondary hubs are connected to the central hub which contains the repeater. This data flows from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

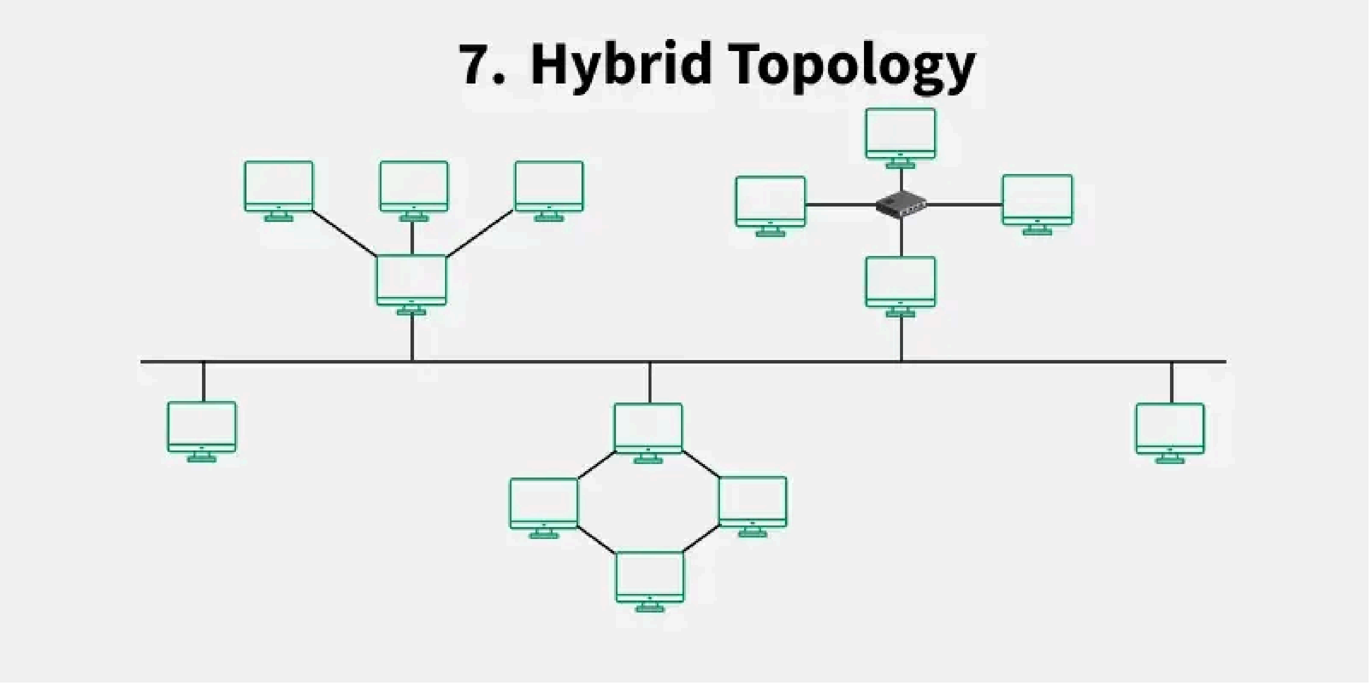
Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

Disadvantages of Tree Topology

- If the central hub fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a **tree topology is the hierarchy in a large organization**. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.



Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.

The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible** .
- The size of the network can be easily expanded by **adding new devices.**

Disadvantages of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**
- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices** .

A **common example of a hybrid topology is a university campus network**. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

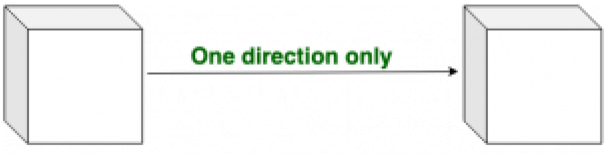
Line Configuration

- **Point-to-Point configuration:** In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.
- **Multi-Point configuration:** In a Multi-Point configuration, there is a line (link) through which multiple devices are connected.

Modes of Transmission Medium

Simplex mode: In this mode, out of two devices, only one device can transmit the data, and the other device can only receive the data.

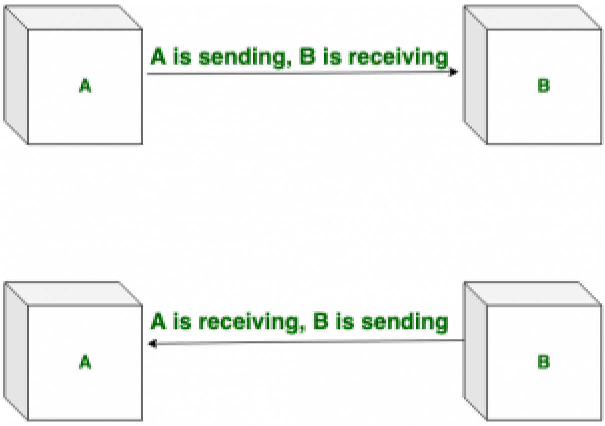
○ Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.



Simplex mode

Half Duplex mode: In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously.

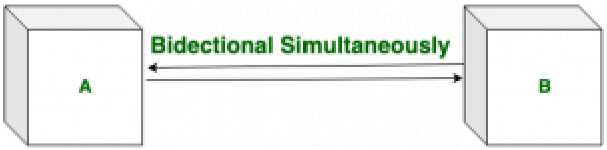
■ Examples- Walkie-Talkie, Railway Track, etc.



Half duplex mode

Full-Duplex mode: In this mode, both devices can send and receive the data simultaneously.

- ■ Examples- Telephone Systems, Chatting applications, etc.



○ Full duplex mode

Protocols in Physical Layer

Typically, a combination of hardware and software programming makes up the physical layer. It consists of several protocols that control data transmissions on a network. The following are some examples of Layer 1 protocols:

- **Ethernet (IEEE 802.3)** – Widely used for wired networks.
- **Wi-Fi (IEEE 802.11)** – For wireless communication.
- **Bluetooth (IEEE 802.15.1)** – Short-range wireless communication.
- **USB (Universal Serial Bus)** – For connecting devices over short distances.

Difference Between TCP/IP and OSI Model:

The TCP/IP or the Transmission Control Protocol/Internet Protocol is a communication protocol suite using which network devices can be connected to the Internet. On the other hand, the Open Systems Interconnection or OSI

Model is a conceptual framework, using which the functioning of a network can be described.

Difference between TCP/IP and OSI Model	
TCP/IP	**OSI Model**
The full form of TCP/IP is Transmission Control Protocol/ Internet Protocol.	The full form of OSI is Open Systems Interconnection.
It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network.	It is a structured model which deals with the functioning of a network.
In 1982, the TCP/IP model became the standard language of ARPANET.	In 1984, the OSI model was introduced by the International Organisation of Standardization (ISO).
It comprises of four layers: ● Network Interface ● Internet ● Transport ● Application	It comprises seven layers: ● Physical ● Data Link ● Network ● Transport ● Session ● Presentation ● Application
It follows a horizontal approach.	It follows a vertical approach.
The TCP/IP is the implementation of the OSI Model.	An OSI Model is a reference model, based on which a network is created.
It is protocol-dependent.	It is protocol-independent.

Rupanshi Patidar