Data Communications:
Data communications involve the transmission of digital data between two or more computers or devices. The data can be in the form of text, images, audio, or video.

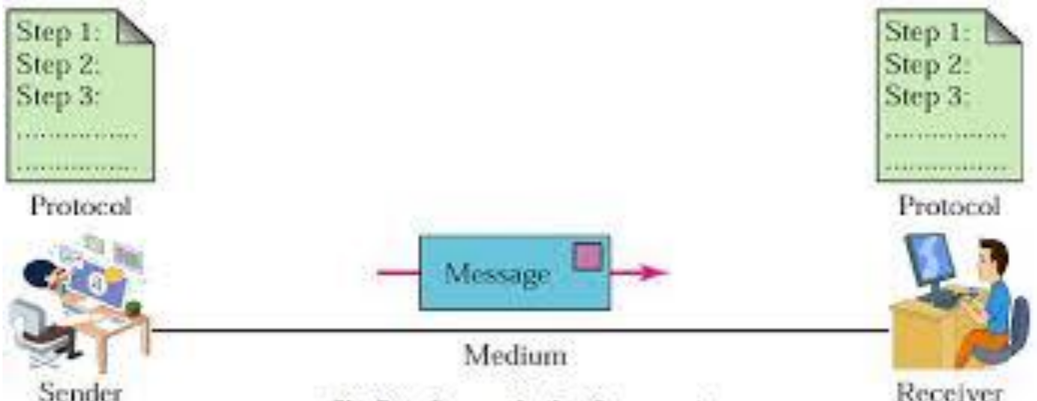
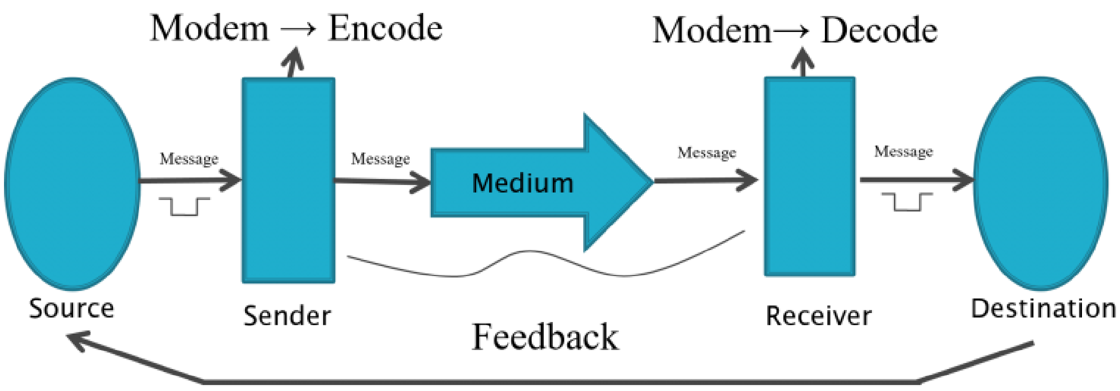


Fig: Data Communication Components

Characteristics of Data Communication:
The effectiveness of any data communications system depends upon the following four fundamental characteristics:
1. **Delivery**: The data should be delivered to the correct destination and correct user.
2. **Accuracy**: The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.
3**. Timeliness**: Audio and Video data has to be delivered in a timely manner without any delay; such a data delivery is called real time transmission of data.
4**. Jitter**: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmit

Components of Data Communication:
In data communication, there are several key components that work together to enable the exchange of information between devices. Here are the main components:



Data Communication System

1. **Message:** The information or data being transmitted, such as text, images, or audio.
2. **Sender**: The device or system that initiates the communication and sends the message. This can be a computer, phone, or other device.
3. **Receiver**: The device or system that receives the message. This can be another computer, phone, or device.
4. **Transmission Medium:** The physical path through which the message travels, such as a cable, wireless link, or fiber optic connection.

5. **Protocol:** A set of rules and standards that govern the communication process, ensuring that data is transmitted and received correctly. (e.g., TCP/IP).
6. **Hardware:** The physical devices involved in the communication process, such as modems, routers, and network interface cards (NICs).
7.**Software:** The programs and operating systems that manage the communication process, such as network operating systems and communication protocols.

These components work together to enable data communication, which involves the following steps:

- Encoding: Converting the message into a digital signal.
- Modulation: Modifying the digital signal to prepare it for transmission.
- Transmission: Sending the signal through the transmission medium.
- Reception: Receiving the signal at the destination device.
- Decoding: Converting the received signal back into its original form.

Efficiency of a data communication system:

Efficiency of a data communication system mainly depends on the following data transmission characteristics.

Data Transmission Speed
Data Transmission Mode (Direction of Data flow)
Data Transmission Method
Data Transmission Medium

Data Transmission Speed:

The amount of data (bit) that is transferred from one computer to another or from one device to another per second is called data transmission speed. That is, the data transfer rate of a communication system is called data transmission speed.

Bandwidth:

Data transmission speed is also called bandwidth. This bandwidth or data transmission speed is usually measured in units of Bit per Second (bps), Mbps, Gbps, etc. Binary digits 0 and 1 are called bits. It is expressed by b. 58 kbps means 58 kilobits of data is transferred from one device to another per second.

1 byte= 8 bit
1 kilobyte= 1024 Byte
1 Megabyte = 1024 Kilobyte
1 Gigabyte = 1024 Megabyte
1 Terabyte = 1024 Gigabyte

The higher the bandwidth of a system, the more data will be exchanged through the system.

Data transmission speed can be divided into three parts based on the speed of data transfer. E.g.

Narrow Band
Voice Band
Broad Band

Narrow band:

Data is transferred in a speed from 45 to 300bps. It is used in telegraph communication system.

Voice band:

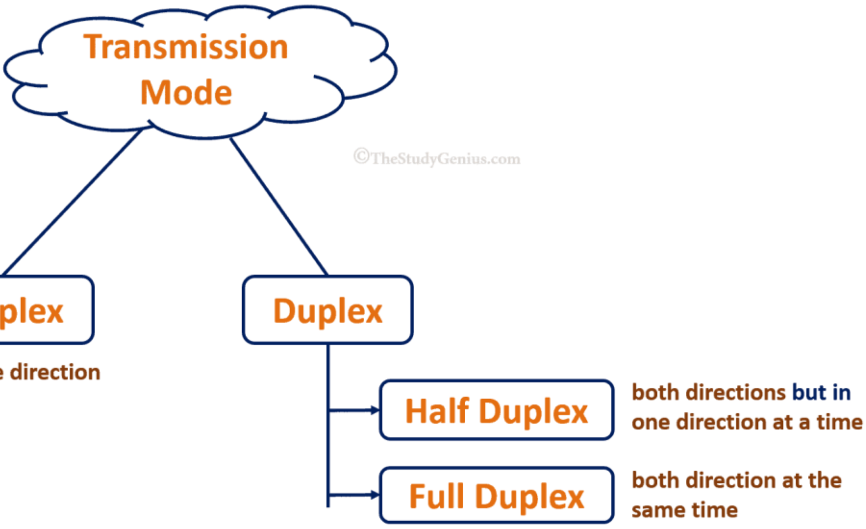
Data is transferred in a speed from 1200 to 9600bps. It is used in telephone system and also used in computer or peripheral devices.

Broad band:

Data is transferred in a speed from 1 Mbps to very high speed. It is used in data transmission through optical fiber cable, microwave etc.

Data Transmission Modes: (Direction of Data flow)

Data transmission modes determine the direction and timing of data flow between the sender and receiver.

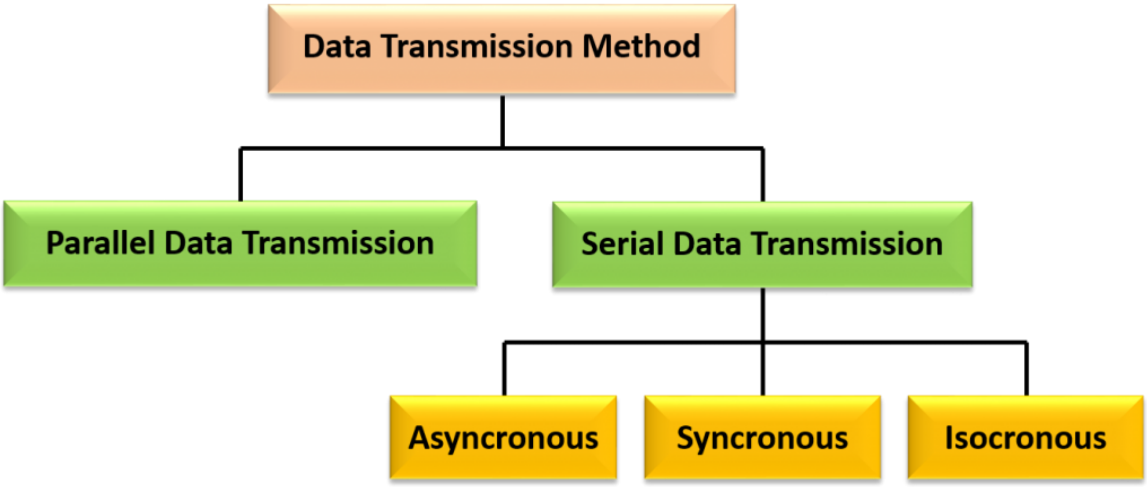


There are three primary modes of data transmission

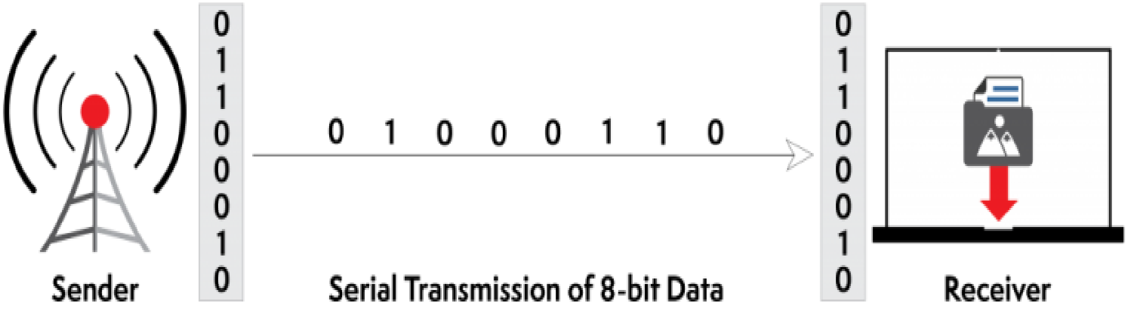
- **Simplex:** Data travels in one direction only. A device can only send the data but cannot receive it or it can receive the data but cannot send the data. (e.g., keyboard to computer).
- **Half-Duplex:** Data travels in both directions, but not simultaneously. (e.g., walkie-talkies).
- **Full-Duplex:** Data travels in both directions simultaneously (e.g., phone calls).

Data Transmission Method:

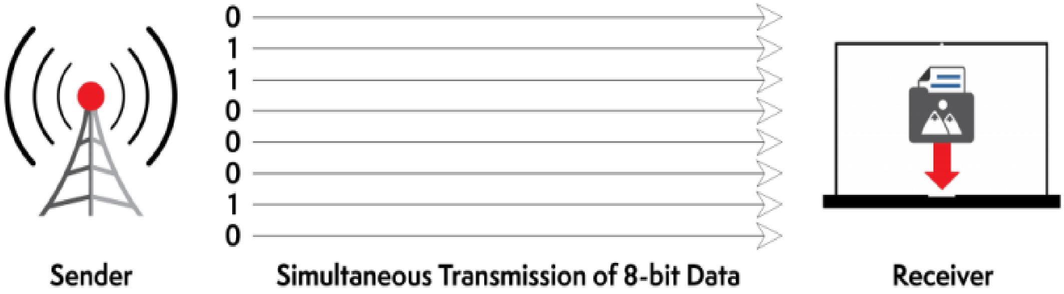
In data communication system the method used to establish link to different devices and bit synchronization with time for data transmission within is called data transmission method.



- **Serial Transmission:** In Serial data transmission, data bits are sent one after another over a single channel. Each bit has a clock pulse rate. Eight bits are transmitted at a time with a start and stop bit known as a parity bit, which is 0 and 1, respectively.



- **Parallel Transmission:** In Parallel data transmission, multiple data bits are sent at the same time over multiple channels. Each channel carries one bit at the same time.



For example- Parallel transmission is used to send data in video streaming. Because video streaming requires the transmission of large volumes of data. The data being sent is also time-sensitive as slow data streams result in poor viewer experience.

Isochronous transmission is similar to synchronous transmission but the time interval between blocks is almost zero.

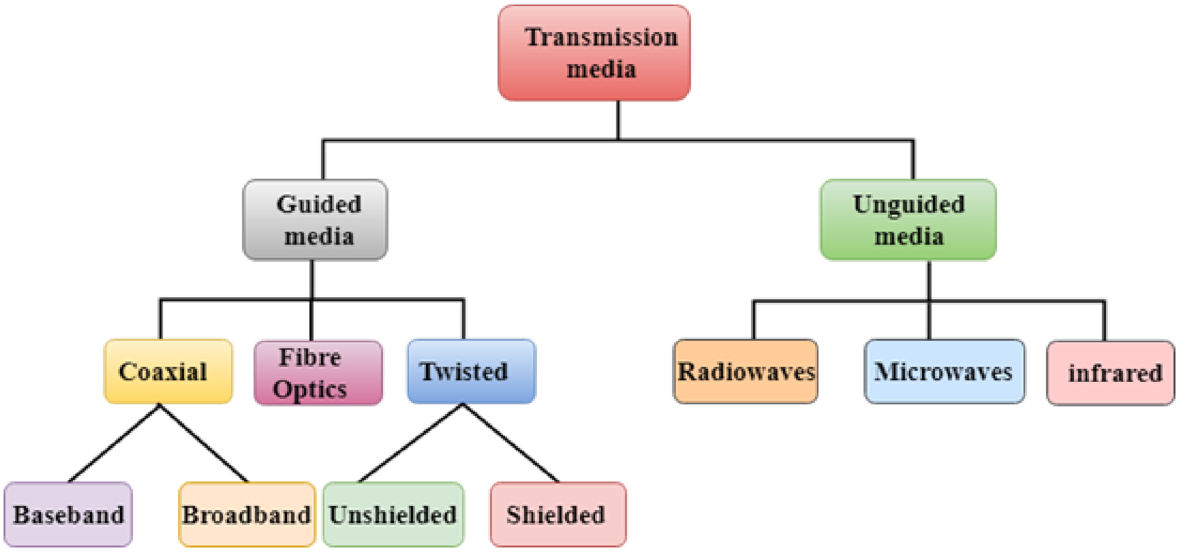
In this transmission synchronous and asynchronous data is collected from several devices within a time slot (125 micro-second) and then passed those collected data as time frame through a synchronous data link one after another.

Data Transmission Medium

Transmission media refers to the physical medium through which data is transmitted from one device to another within a network. This medium can be wired or wireless. The choice of medium depends on factors like distance, speed, and interference.

Guided or Wired Transmission Media

This type of media uses cables to transmit signals across the network. Wired media, often known as guided media, is a form of transmission medium. It has a finite range in the communication system and is also known as a Bounded transmission media

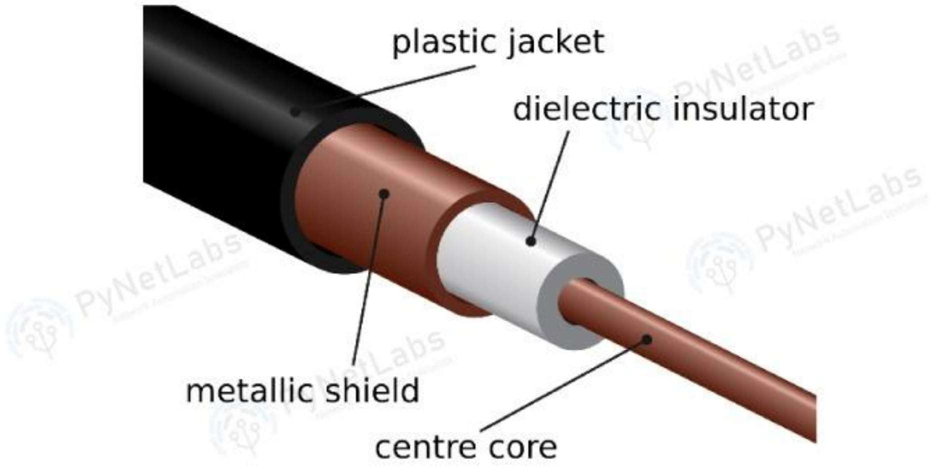


Coaxial:

The coaxial cables have a central copper conductor, surrounded by an insulating layer, a conducting shield, and the outermost plastic sheath. Thus, there are three insulation layers for the inner copper cable. There are two basic modes of data transmission in coaxial cables: baseband mode that has dedicated bandwidth, and broadband mode that has distributed cable bandwidth.

Cable TV and analog televisions mainly use coaxial cables. Coaxial cables have better resistance to cross talk than twisted pair cables. The coaxial cables are used for long distance communication. The most widely used types of coaxial cables are RG-59 and RG-6 (RG stands for 'radio guide'). RG-59 has lesser shielding and is suitable for short cable lengths and cable TV connections.

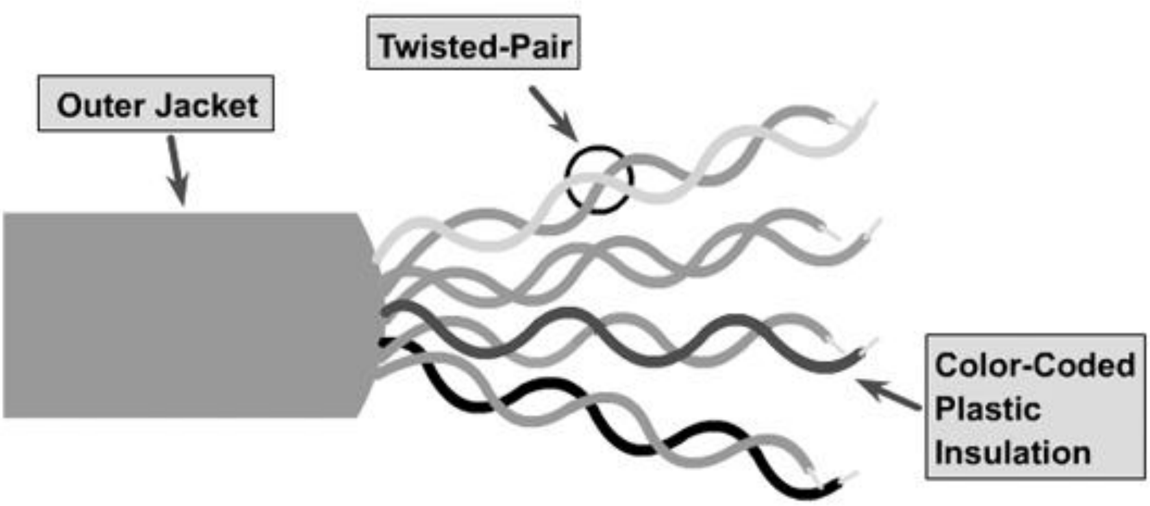
RG-6 has better insulation than RG-59 and is used for satellite TV and digital signal transmissions for better strength and longer distances.



Twisted Pair Cable:

A Twisted Pair Cable is defined as a type of network cabling that consists of pairs of wires twisted together. The wires are insulated conductors generally made of copper and twisted together. This cable has eight insulated wires. These are paired in groups of 2 and are twisted together based on a color code. The twisting is done to decrease interference caused by the adjacent wires. One conductor is used to carry the signal, and the other one is used only as a ground reference. This twisting helps reduce electromagnetic interference (EMI), making the cable less susceptible to external disturbances. The twisted pair is further divided into two parts, i.e., shielded and unshielded.

A **twisted pair cable is used for** connecting computers, switches, routers, printers, IP cameras, and PoE devices in a LAN.

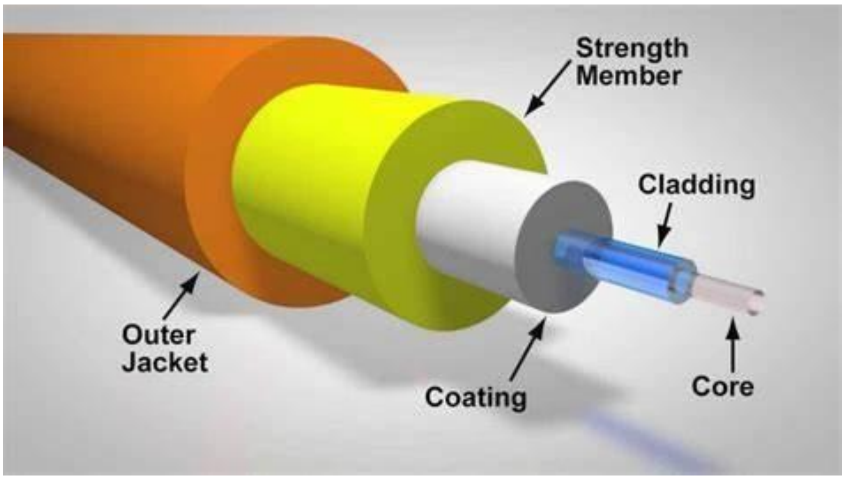


Unshielded Twisted Pair Cable (UTP): These consist of two insulated copper wires that are coiled around one another. These types of transmission media block interference without depending on any physical shield. The unshielded twisted pair are very affordable and are simple to set up. These provide a high-speed link.

Shielded Twisted Pair (STP): This twisted cable consisted of a foil shield to block external interference. The insulation within these types of twisted cables allows a greater data transmission rate. These are used in fast-data-rate Ethernet and in data and voice channels of telephone lines.

Optical Fiber Cable:

Fibre optic cable is a cable that uses electrical signals for communication. Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light. The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring. Fibre optics provide faster data transmission than copper wires.

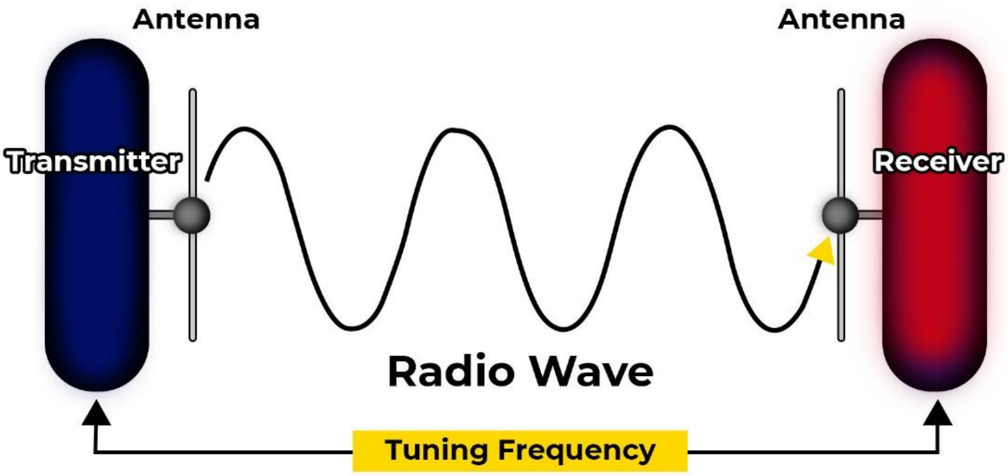


Unguided or Wireless Transmission Media

Unguided media, also termed as unbound transmission medium, is a method of transmitting data without the need for cables. Physical geography has no bearing on these media. Unguided media are also known as wireless communication. It is a wireless transmission media channel that does not need a physical medium to connect to network nodes or servers.

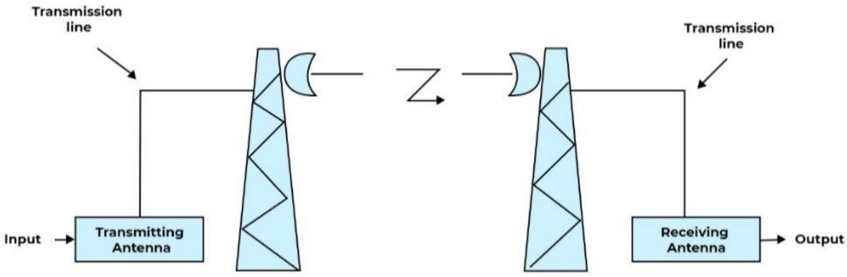
Radio Waves:

Radio waves are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission. An antenna is a crucial component of radio wave transmission, which is responsible for converting electrical energy into radio waves.



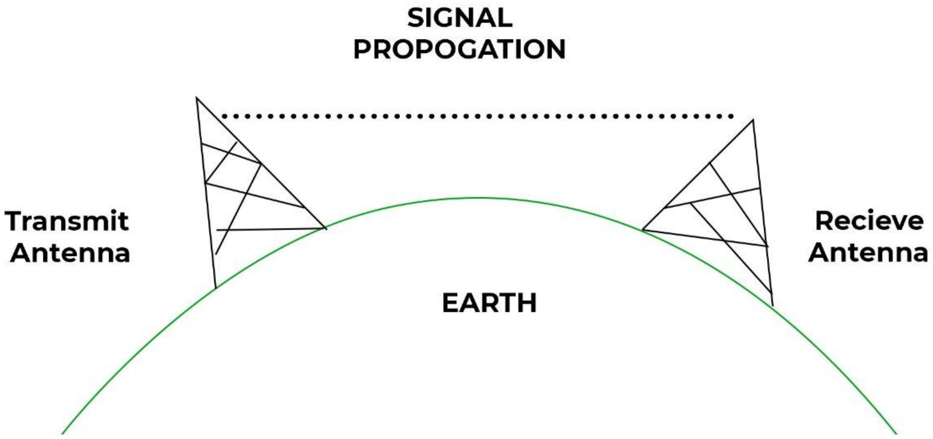
Microwave Transmission:

Microwave transmission is a method of transmitting data through high-frequency electromagnetic waves over long distances. The antenna plays a crucial role in microwave transmission, as it converts electrical signals into microwave energy and transmits them through the air.

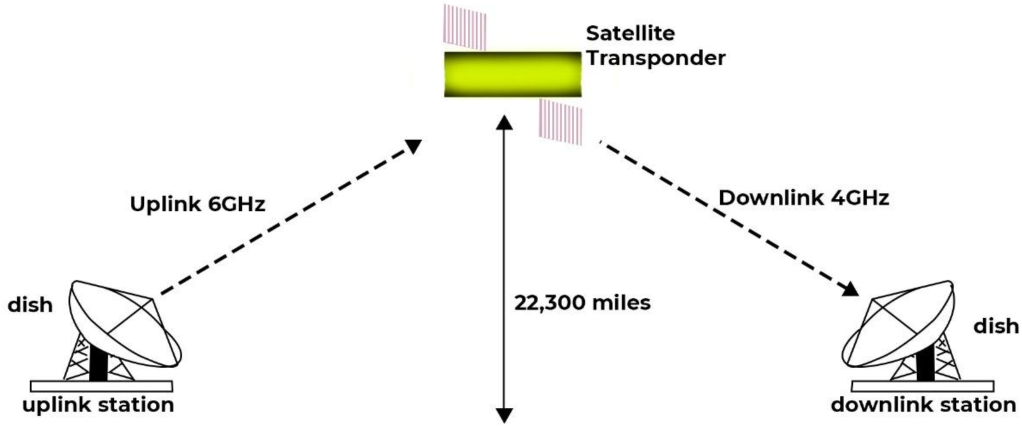


Types of Microwave Transmission

Terrestrial Microwaves: These microwaves are used for communication purposes, especially between two points on the Earth's surface. One such example is the communication between two towers or buildings.

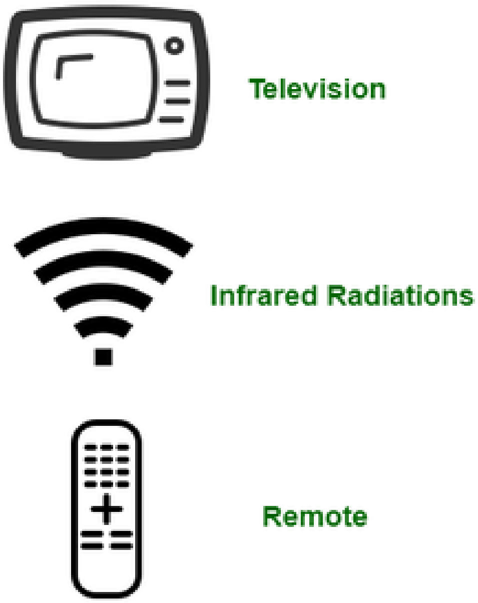


Satellite Microwaves: These microwaves are used for communication between the Earth and a satellite in orbit. It is crucial for global communication and broadcasting**.**



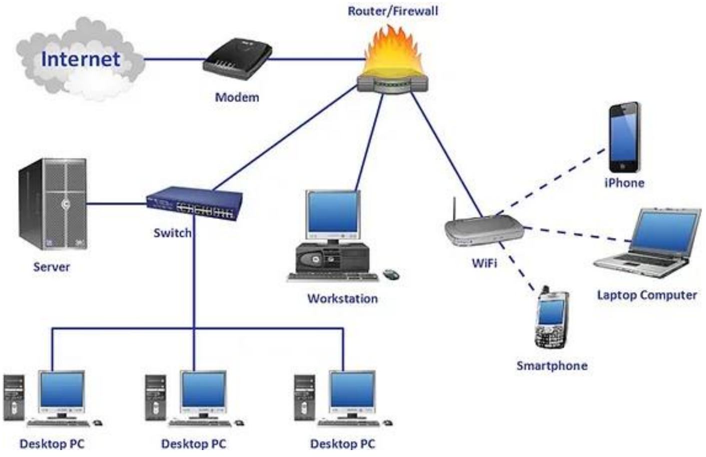
Infrared:

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



Networks

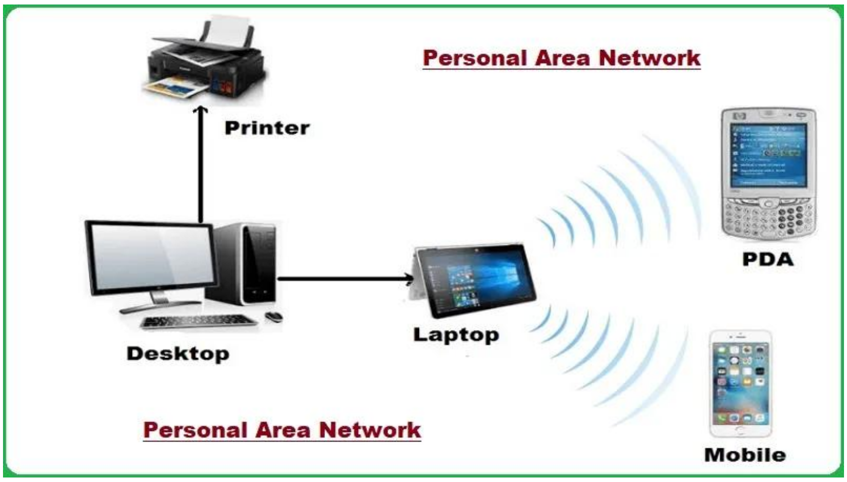
A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.



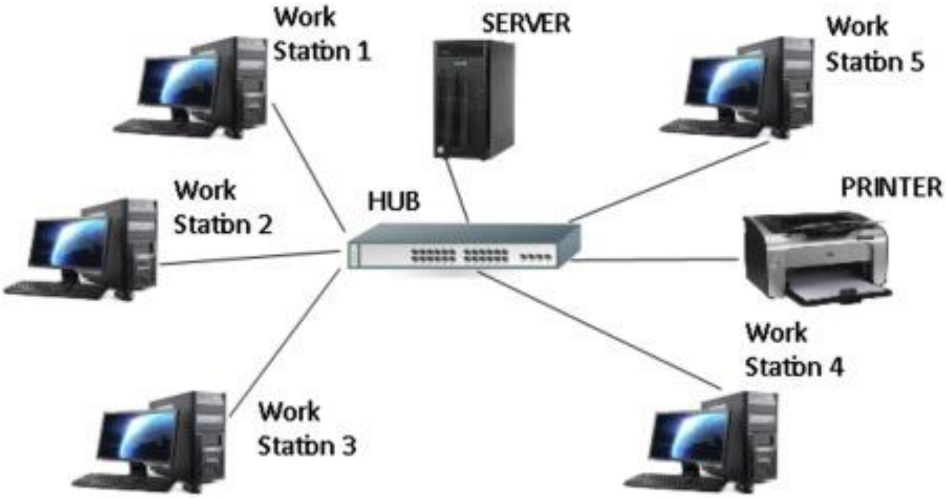
Types of Networks

Computer networks can be classified based on several criteria, such as the transmission medium, the network size, the topology, and organizational intent. Based on a geographical scale, the different types of networks are:

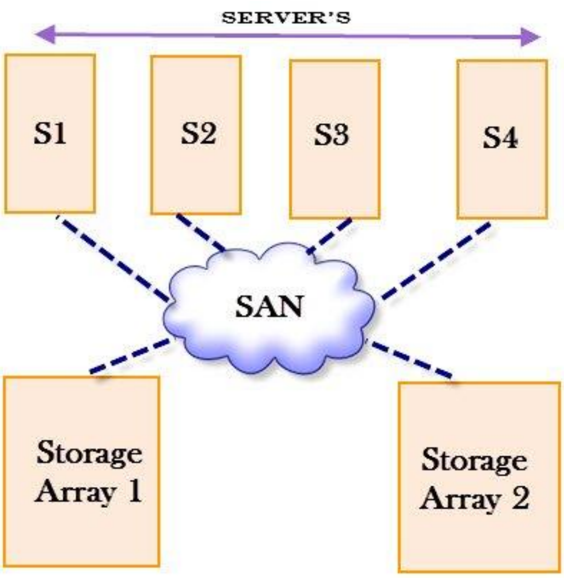
Personal area network (PAN): PAN refers to a network used by just one person to connect multiple devices, such as laptops to scanners, etc.



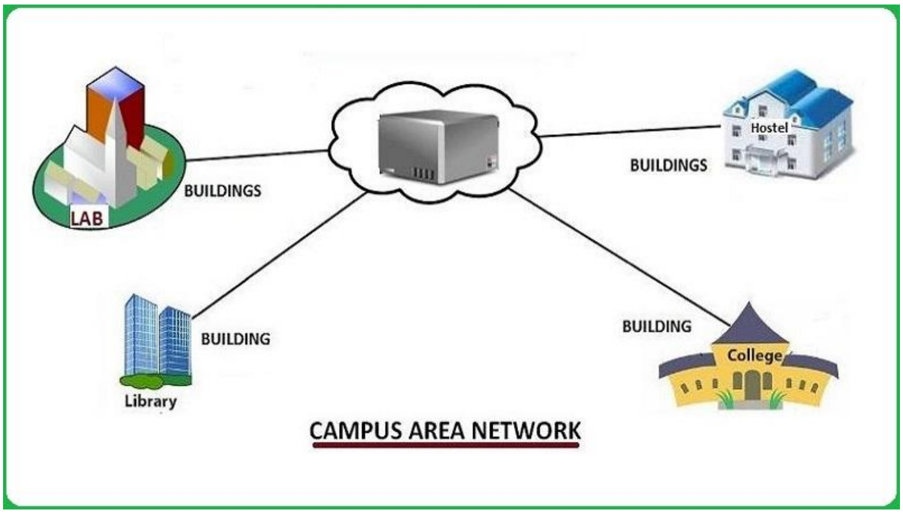
Local area network (LAN): The local area network connects devices within a limited geographical area, such as schools, hospitals, or office buildings. Once they connect, users have access to the same resources. For example, you might use a LAN when you connect your laptop to the internet at your home and print a document from a printer on the same network.



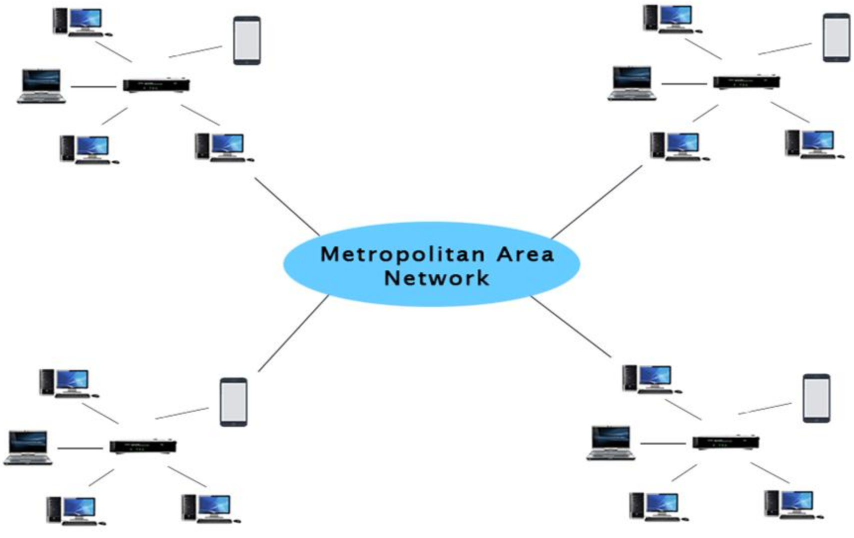
Storage area network (SAN): SAN is a dedicated network that facilitates block-level data storage. This is used in storage devices such as disk arrays and tape libraries.



Campus Area Network Definition: A campus area network (CAN) is a computer network that consists of multiple interconnected local area networks (LAN) in order to cover a limited geographic area, such as a military base, school campus, university campus, etc.



Metropolitan area network (MAN): MAN is a large computer network that spans across a city.
Wide area network (WAN): Wide area networks cover larger areas such as large cities, states, and even countries.



Virtual private network (VPN): VPN is an overlay private network stretched on top of a public network.

Cloud network: Technically, a cloud network is a WAN whose infrastructure is delivered via cloud services.

Based on organizational intent, networks can be classified as:

Intranet: Intranet is a set of networks that is maintained and controlled by a single entity. It is generally the most secure type of network, with access to authorized users alone. An intranet usually exists behind the router in a local area network. An intranet is a private network accessible only to an organization's staff. It’s used to share company information and resources among employees securely.
Extranet: An extranet is similar to the intranet but with connections to particular external networks. It is generally used to share resources with partners, customers, or remote employees.
Internet: The internet (or the internetwork) is a collection of multiple networks connected by routers and layered by networking software. This is a global system that connects governments, researchers, corporates, the public, and individual computer networks.

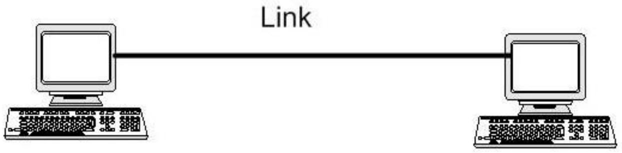
Types of Connections in Data communication:

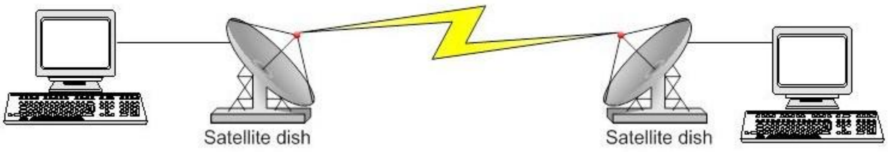
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another

There are two possible types of connections: point-to-point and multipoint.

Point-to-Point connection

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. It offers a dedicated and secure connection between two locations, ensuring high-speed and reliable data transmission. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

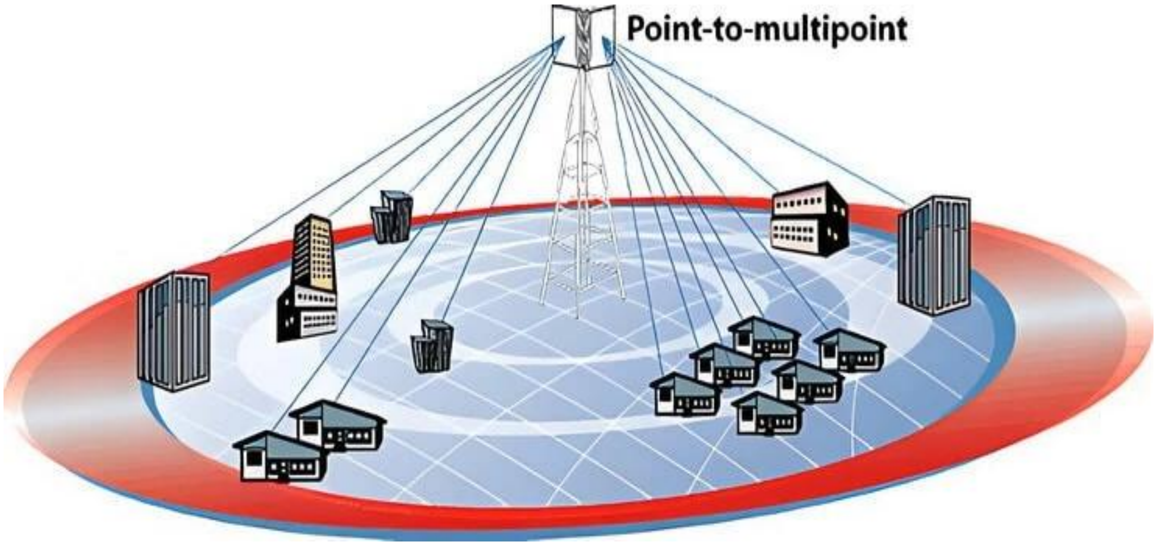




An example of a point-to-point connection is a telephone call between two individuals

Multi-point communication:

A multi-point communication refers to a communication link established between a single sender and multiple receivers. In this type of communication, the sender broadcasts the data, and multiple receivers can receive the data simultaneously. Multi-point communication is commonly used for broadcasting, multicast, or video conferencing purposes.



An example of a multipoint connection is a video conference call. Multiple participants can join the call from different locations, and all of them can see and hear each other.

Network Topology:

Network topology refers to the arrangement of elements in a communication network such as links, nodes, and so on. The term network topology refers to the arrangement of various types of telecommunication networks, such as command and control radio networks, industrial field buses, and computer networks. Local area networks, a common computer network installation, contain examples of network topologies.

Network topologies are classified into two types: physical and logical. While logical topology emphasizes the pattern of data transfer between network nodes, physical topology emphasizes the physical layout of the connected devices and nodes

Network topology impacts network performance, security and scalability, making it a crucial concept in network design and management.

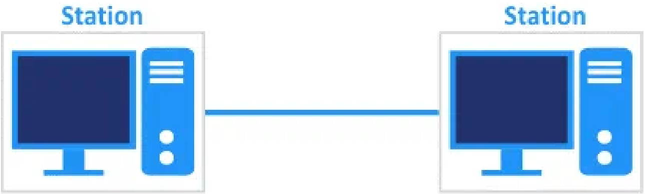
Types of network topologies:

- Point-to-point topology
- Bus topology
- Ring topology
- Star topology
- Tree topology
- Mesh topology
- Hybrid topology

Point-to-point topology:

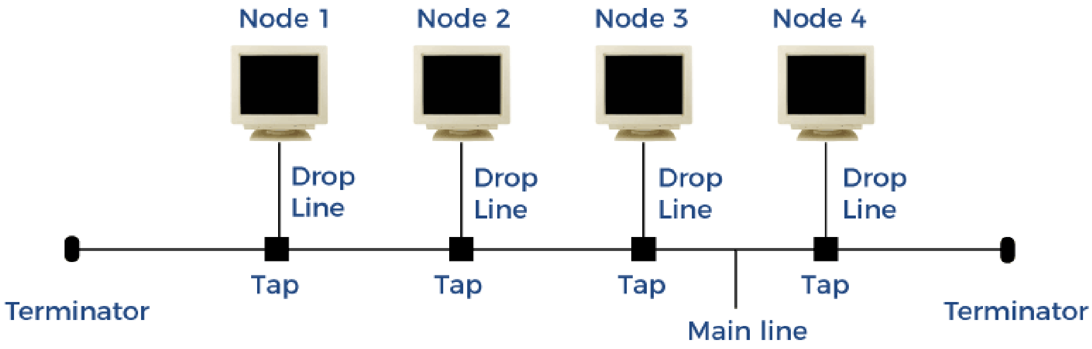
Point-to-point topology is the simplest network configuration, connecting two nodes directly through a dedicated communication link. This setup resembles a direct line between two endpoints, allowing for efficient and fast data transfer.

Point to Point Topology



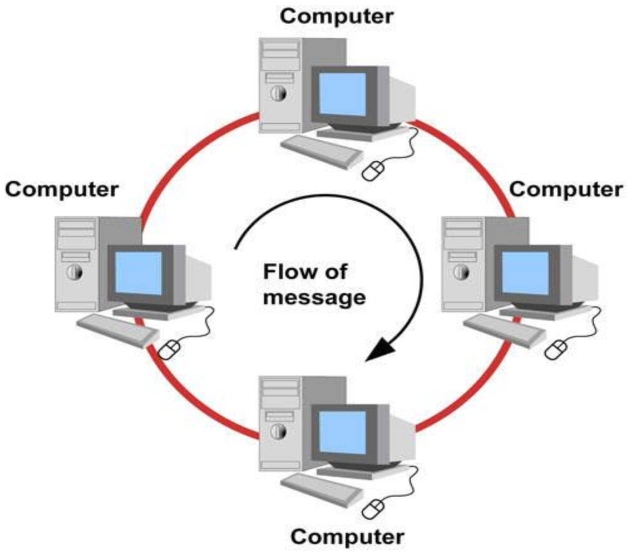
Think of a telephone call between two people. In a point-to-point topology, like that call, two connected devices communicate directly without interference, sharing the entire bandwidth for high performance and low latency

Bus network topology -- Also known as backbone network topology, the simplest type of topology is called a bus topology, in which **network communication** takes place over a single bus or channel. There are numerous taps and drop lines connected to the bus. Drop Lines are cables that connect the bus to the computer, and taps are connectors. In other words, each node is connected to a single transmission line. Data travels in both directions along the cable.

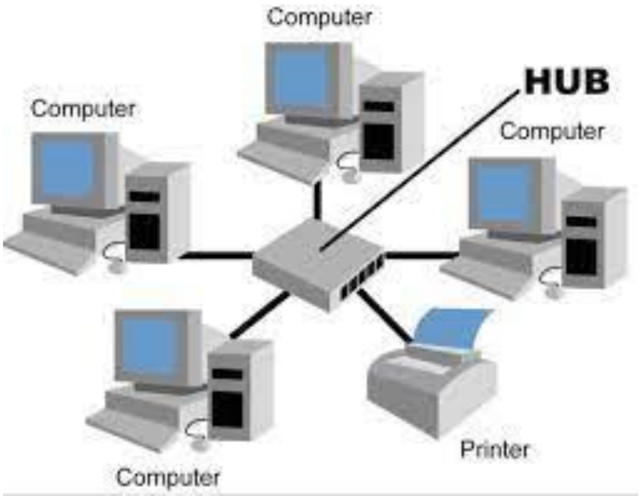


Bus Topology

Ring Topology: When two computers are connected to form a ring, the topology is known as a ring topology. The message passing is circular and unidirectional. A fixed amount of time is allotted for each computer to access the network for transmission in this deterministic network topology. Each node is a part of a closed loop.

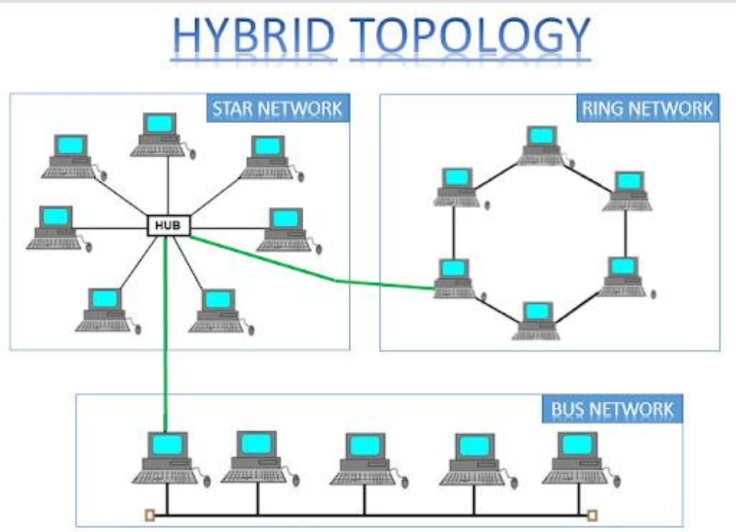


Star Topology: In star topology connects each node to a central hub. The hub or switch acts as a bridge between the nodes. Any node making a service request or offering a service must first get in touch with the hub. The other connected devices function as clients in a star topology, while the hub and switch serve as a server.

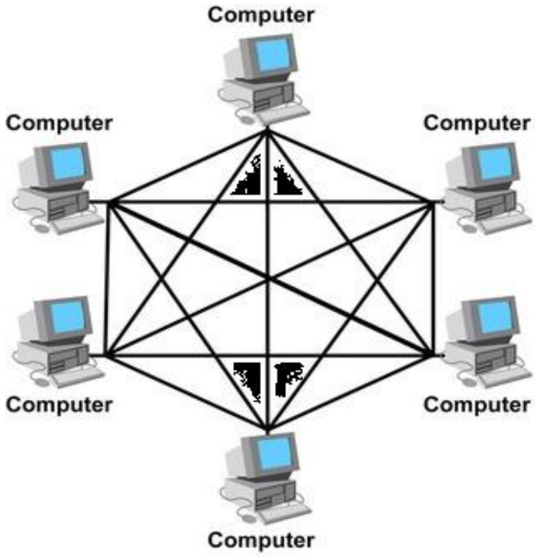


In star topology, each device (many institutes, airports, hospitals, and banks) in the network completely depends on the central hub, i.e. if the hub fails, the whole network fails.

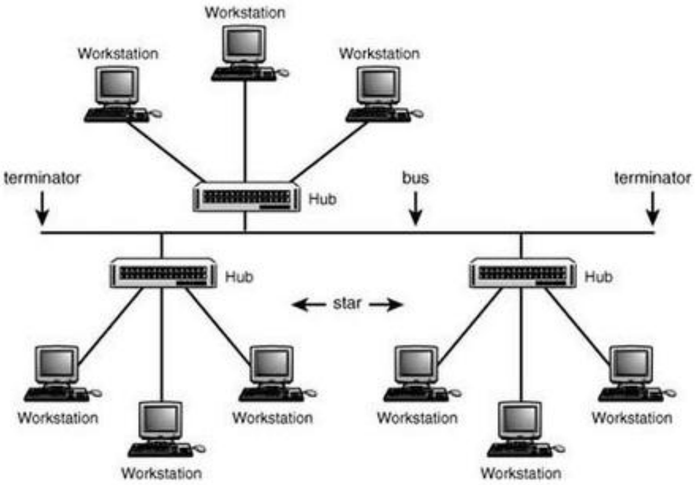
Hybrid Topology: A hybrid topology is a computer topology made up of two or more topologies. All topologies in this topology are interconnected based on their needs to form a hybrid. It can support a large number of nodes



Mesh Topology: Mesh technology is a network configuration in which computers are linked to one another by numerous redundant connections. There are numerous methods for transferring from one computer to another. It lacks a switch, hub, or any other central computer that acts as a communication hub.



Tree Topology: A “tree topology" is one in which all nodes are either directly or indirectly connected to the main bus cable. Bus and Star topologies are combined to create tree topology. With a tree topology, the network is split up into manageable segments that can be easily maintained.



Protocols in Data Communication:

Protocols are crucial in defining how data is transmitted and received over networks. Here are some key ones:

- TCP/IP (Transmission Control Protocol/Internet Protocol): This is the backbone of the internet. It ensures reliable data transmission between devices
- HTTP/HTTPS (HyperText Transfer Protocol/Secure): Used for transmitting web pages over the internet. HTTPS adds a layer of security via SSL/TLS.
- FTP (File Transfer Protocol): Used for transferring files between a client and a server.
- SMTP (Simple Mail Transfer Protocol): Used for sending emails.
- IMAP/POP3 (Internet Message Access Protocol/Post Office Protocol): Used for retrieving emails from a server.
- SNMP (Simple Network Management Protocol): Used for managing and monitoring network devices.

Standards in Data Communication:

Standards ensure that different devices and systems can communicate effectively. Here are some key standards:

- IEEE 802.3 (Ethernet): A set of standards for wired networking.
- IEEE 802.11 (Wi-Fi): Standards for wireless networking.
- ITU-T (International Telecommunication Union - Telecommunication): Provides international standards for telecommunications.
- ISO/IEC 27001: Standards for information security management.
- USB (Universal Serial Bus): Standards for wired connections between devices.

OSI :

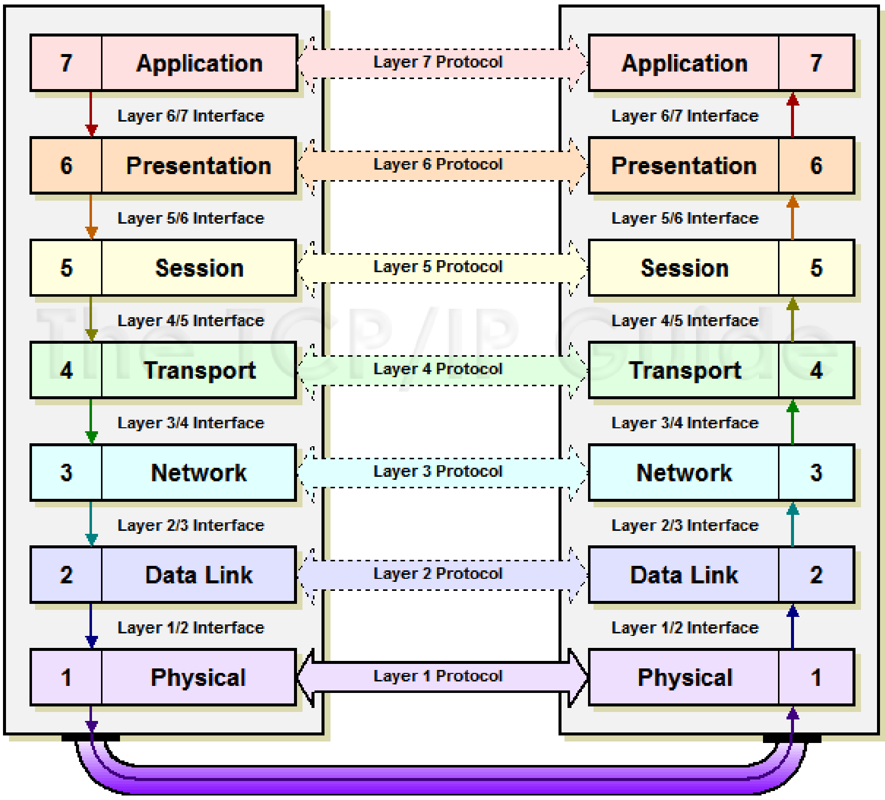
OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

OSI model was developed by the International Organization for Standardization (ISO). OSI consists of seven layers, and each layer performs a particular network function. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

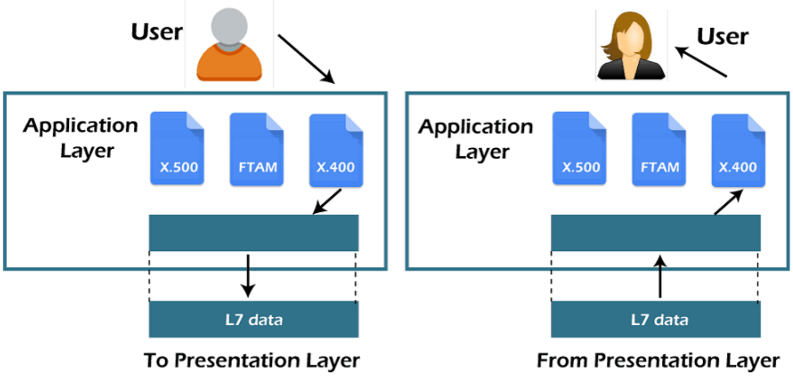
1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Application Layer:

An application layer is not an application, but it performs the application layer functions. This layer provides the network services to the end-users. The application layer includes protocols designed for end-users. For example, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP).

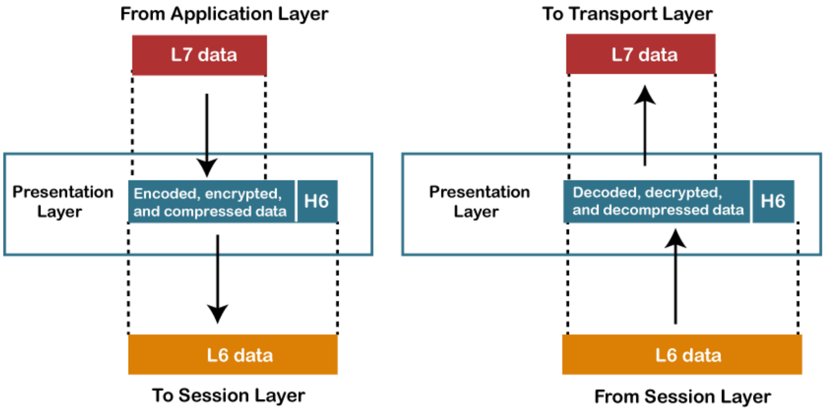
HTTP : It is the main way web browsers and servers communicate to share information on the internet.
FTP: transfer of computer files from a server to a client on a computer network.
SMTP: It is a communication protocol used for sending and receiving email messages over the Internet



Presentation Layer:

The Presentation layer is also known as the syntax layer. The presentation layer is primarily responsible for translating data from network data to the formats expected by an application.
The presentation layer deals with:

- Data conversion
- Character code translation
- Data compression
- Encryption and decryption

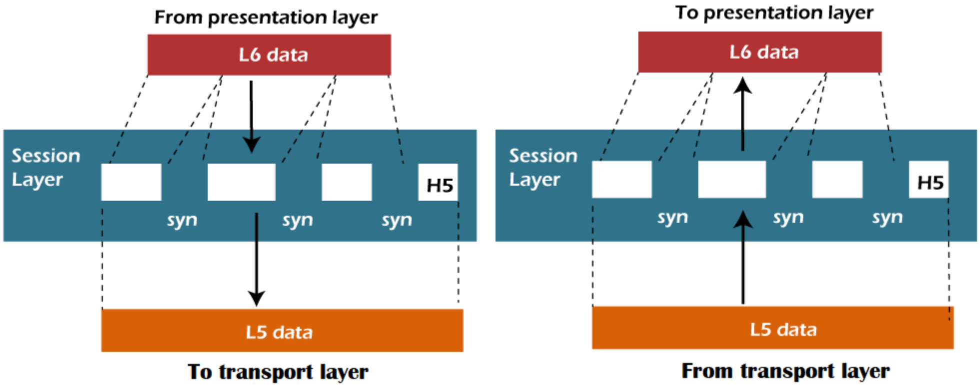


To send text across a network, the characters of the alphabet convert via a character coding system, such as the American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC) that is then encrypted and compressed and sent over the network. On the receiving end, the process reverses. Different kinds of data get translated into different format codes. Ensures that data is in a usable format. SSL/TLS, JPEG, ASCII.
SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a network.
JPEG (Joint Photographic Experts Group) - JPEG is a widely used image format that employs lossy compression techniques to reduce file size while maintaining a reasonable image quality

ASCII (American Standard Code for Information Interchange) - ASCII is a character encoding standard used to represent text in computers, telecommunications equipment, and other devices

Session Layer:

Its primary function is to manage and control the dialogues (sessions) between computers.



Functions of Session Layer:

Session Establishment, Maintenance, and Termination:

Establishment: Sets up a connection between two devices. This involves authentication and authorization to ensure that communication occurs between valid users

Maintenance: Maintains the session for the duration of the communication, keeping it active and handling any interruptions.

Termination: Properly closes the session once the communication is complete, ensuring that all resources are freed.

Synchronization:

Checkpoints: Places checkpoints in the data stream, so in case of a failure, data can be retransmitted from the last checkpoint rather than from the beginning.

Recovery: Provides mechanisms for resuming communication after a disruption.

Dialog Control:

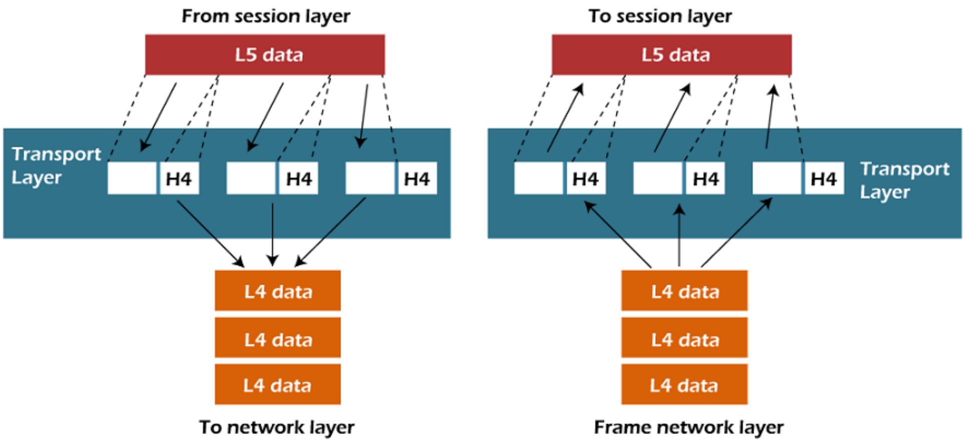
Manages the dialog between two devices, ensuring that data can flow in an organized manner. It can operate in full-duplex (simultaneous two-way communication) or half-duplex (alternating two-way communication).

Session Management:

Coordinates multiple communication streams, ensuring that data from different sessions doesn't get mixed up.

Transport Layer:

The transport layer transmits end-to-end data between two devices interacting on the network, making sure that data isn't lost, misconfigured or corrupted. Common transport layer protocols include the Transmission Control Protocol (TCP) for connection-oriented data transmission and the User Datagram Protocol (UDP) for connectionless data transmission.

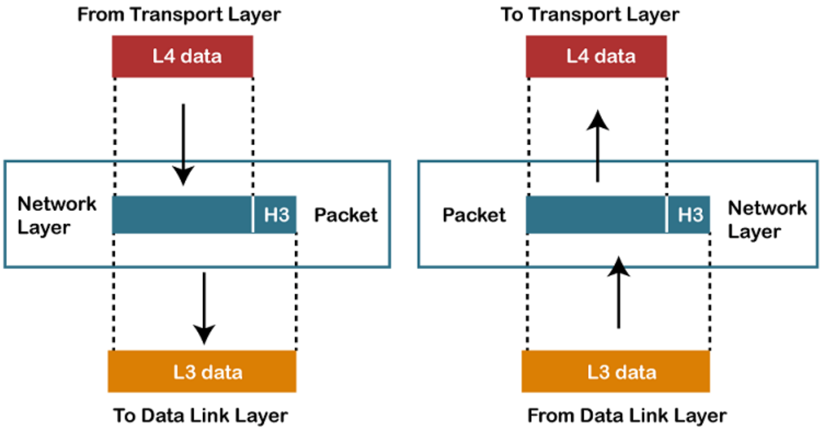


Some of the essential functions in this layer include:

- Error control, flow control, and congestion control are ways to keep track of data packets, check for errors and duplication, and then to resend if there is an error or failure.
- Service-point addressing ensures that data is delivered to the correct protocol, identified by a port number.
- Packet segmentation and reassembly are processes for dividing data and sending it sequentially, then rechecking it at its destination for integrity and accuracy.

Network Layer:

The network layer handles data addressing, routing and forwarding processes for devices interacting across different networks. If the devices are on the same network, they don't need the network layer to interact. Network protocols such as Internet (IPv4) Protocol version 4 and Internet Protocol version 6 (IPv6).



Functions of Network Layer:

Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

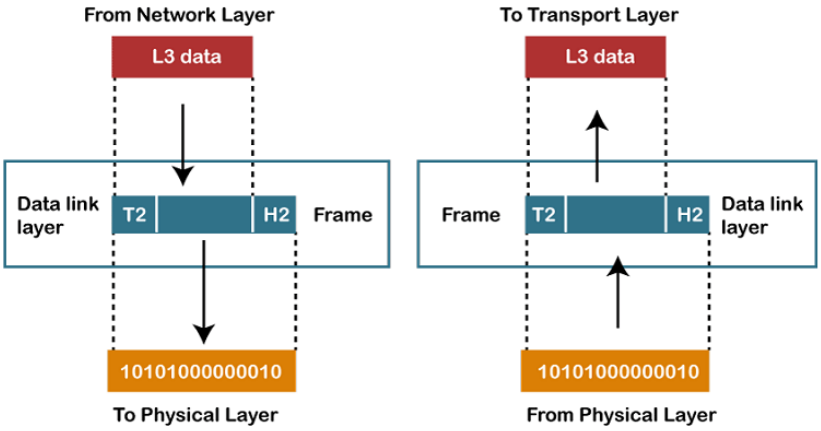
Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

Data Link Layer:

The data link layer breaks data to be transmitted into frames for transmission at the physical layer. It also manages connections between two different nodes, including setting up the connection, identifying and correcting any bit errors that occur at the physical layer, and terminating the connection once the session is complete.

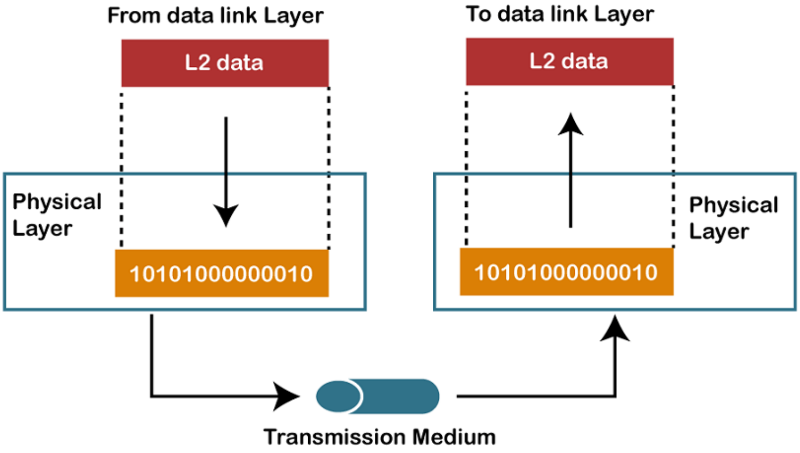


The OSI data link layer has two sublayers:

- The Logical Link Control (LLC) sublayer manages flow and error controls to ensure accurate data transmission between the network devices.
- The Media Access Control (MAC) sublayer manages access and permissions for transmitting data between devices. The function of this sublayer is to manage which device controls a channel, moment to moment.

Physical layer:

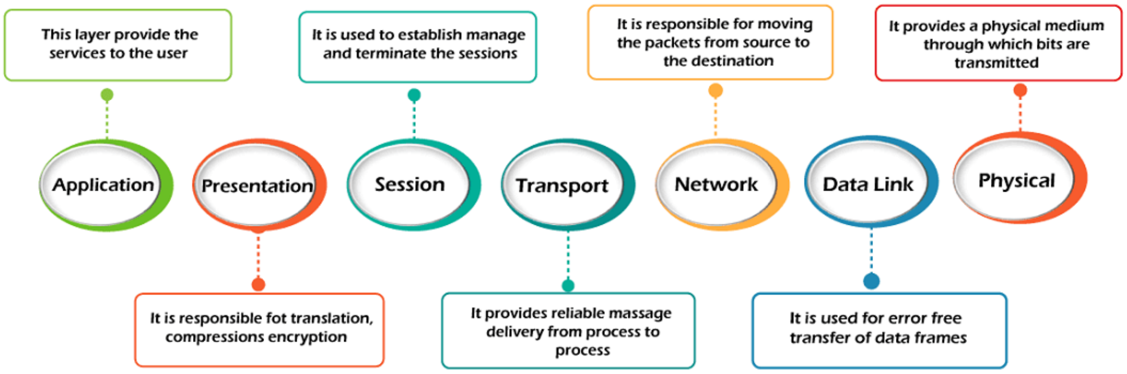
The first OSI model layer describes the physical connections between devices in a network. Electrical, optic, or electromagnetic signal data moves from device to device through the physical infrastructure defined by this layer.



Functions of a Physical layer:

Line Configuration: It defines the way how two or more devices can be connected physically.
Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
Topology: It defines the way how network devices are arranged.
Signals: It determines the type of the signal used for transmitting the information.

Summary of OSI


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

TCP/IP

The Transmission Control Protocol (TCP) is a communication protocol responsible for ensuring that data is transferred reliably and in order between the two devices. IP is the network layer protocol responsible for routing network traffic. The TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers. The model is often referred to as the TCP/IP stack.

The TCP/IP model is divided into four different layers:

Application layer
Transport layer
Internet layer
Network Access layer

Functions of TCP/IP Layers

The Application Layer: The application layer is closest to the end user. And this is the layer that users interact with directly, including protocols such as HTTP, FTP, and SSH. This layer is responsible for providing applications with access to the network.

The Transport Layer: The transport layer ensures that data is delivered reliably and efficiently from one point to another. This layer handles data transmission between hosts, including protocols like TCP and UDP.

The Internet Layer: The network layer is responsible for routing data through the web. This layer delivers data packets from one host to another, including the IP protocol.

The Link Layer: The link layer provides reliable data links between the two nodes — for example, protocols like ethernet and Wi-Fi.

Protocols Used :

There are four main protocols used in TCP/IP: the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), the Internet Protocol (IP), and the Internet Control Message Protocol (ICMP).

- TCP ensures that data is delivered reliably and in order.
- UDP is used for applications where data doesn't need to be delivered reliably or needs to be delivered quickly without the overhead of TCP.
- IP is the protocol that routes data from one computer to another.
- ICMP is used for error-checking and for managing traffic congestion.

All four of these protocols are essential for the proper functioning of the internet. They work together to ensure that data is delivered quickly, reliably, and in the appropriate order.

There are some other protocols also notable, and there are,

- Address Resolution Protocol (ARP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Domain Name System (DNS)

Advantages of TCP/IP:

- Scalability: The TCP/IP model is highly scalable and can accommodate small and large networks.
- Reliability: The model is robust and reliable, making it suitable for mission-critical applications.
- Flexibility: It is very flexible, allowing for interoperability between different types of networks.
- Security: The various protocols in the model provide robust security measures.
- Cost-effectiveness: TCP/IP is relatively inexpensive to implement and maintain.

Disadvantages of TCP/IP:

- Complexity: The model is quite complex and requires a certain degree of expertise to configure and maintain.
- Vulnerability: Because of its complexity, it is vulnerable to attack.
- Performance: Performance can be degraded due to network congestion and latency.

Switching :

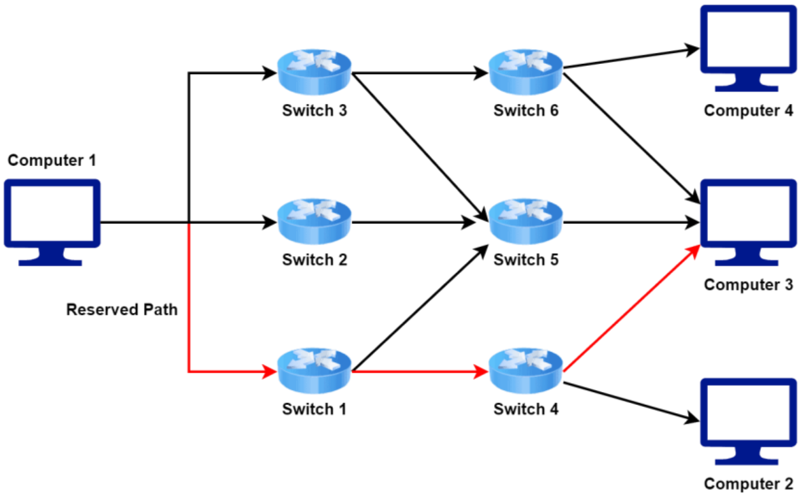
Switching allows multiple devices to share the same communication channel simultaneously. As a result, it improves the efficiency of the network.

There’re three main switching techniques used in computer networks:

- circuit switching
- packet switching
- message switching

Circuit Switching

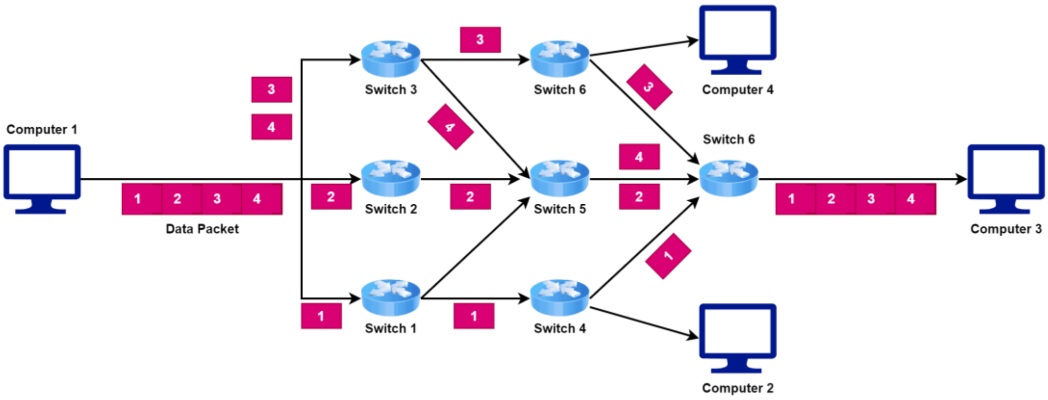
When two devices want to communicate in a circuit-switched network, they establish a connection by setting up a dedicated path between them. This path is reserved exclusively for the duration of the communication. Hence, no other devices can use it during that specific time.



Once we establish the connection, we can transfer data between devices over the dedicated path. This path typically comprises a series of interconnected switches or nodes that route the data to its destination. We mainly use circuit switching in traditional telephone networks

Packet Switching

We divide data into small packets and transmit them over the network independently. Each packet contains the data and destination address information required to route the packet to its destination.

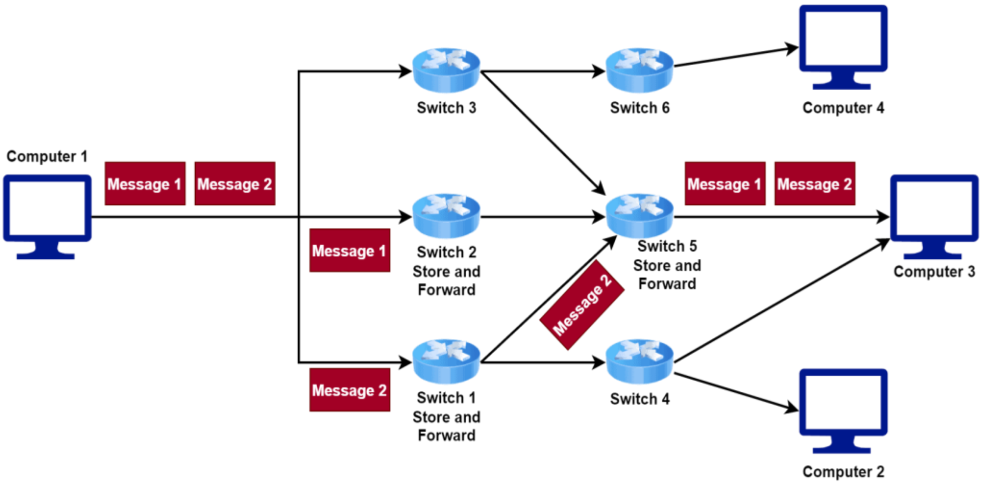


In packet switching, each packet travels separately through the network and can take different paths to reach its destination. This approach allows for more efficient use of network resources because we can transmit multiple packets simultaneously over the same network.

Packet switching is a robust and reliable method of data transmission. If one packet is lost or delayed, it doesn’t affect the transmission of other packets, as we route packets independently through the network. The Internet is an example of a packet-switched network.

Message Switching

In message switching, we divide a message into fixed-length blocks or frames. we transmit each frame independently through the network. Additionally, each intermediate node stores the frames until the entire message is received. Finally, the nodes forward the entire message to its destination. Unlike packet switching, message switching is a store-and-forward method of data transmission. It means that each intermediate node stores the entire message until it can be forwarded to the next node. This can result in longer transmission times compared to packet switching. We can only transmit each message when an intermediate node receives all the parts of the message.



Datagram Networks