What is a Computer Network?

A computer network is a collection of computing devices that are connected with each other for the purpose of information and resource sharing among a wide variety of users.

Each device in the network is called a node which is connected to other nodes through wired or wireless media.

Hardware Components

- **Servers** −Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds**: file servers, database servers, print servers etc.**
- **Clients** − Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers** − Peers are computers that provide as well as receive services from other peers in a workgroup network.
-

- **Transmission Media** − Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like **coaxial cable, fibre optic cables** etc; or maybe unguided media like **microwaves, infra-red waves** etc.
- **Connecting Devices** − Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

    a. Routers

    b. Bridges

    c. Hubs

    d. Repeaters

    e. Gateways

    f. Switches

Software Components

- **Networking Operating System** − Network Operating Systems is typically installed in the server and facilitate workstations in a network to share files, database, applications, printers etc.
- **Protocol Suite** − A protocol is a rule or guideline followed by each computer for data communication. Protocol suite is a set of related protocols that are laid down for computer networks. The two popular protocol suites are −
  - a. OSI Model (Open System Interconnections)
  - b. TCP / IP Model

# The features of a computer network are −

- **Sharing** − Computer networks enable sharing of files, software, hardware resources and computing capabilities.
- **Speed:** The communication speed among the components is fast enough to be comparable with a centralized system.
- **Scalability** − Sizes of computer networks dynamically increase with time. The networks have to be scalable so that they can evolve adequately for future deployments.
- **Integration** − All the components of the network work in a coordinated manner for a seamless user experience.
- **Security** − Networks allow security and access rights to the users for restricted sharing of resources and information.
- **Cost Effectiveness** − Networking reduces the deployment cost of hardware and software of a centralized system.
 - ○

Connecting Devices

a. Routers

A router is **a networking device that forwards data packets between computer networks**. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. ... A router is connected to two or more data lines from different IP networks.
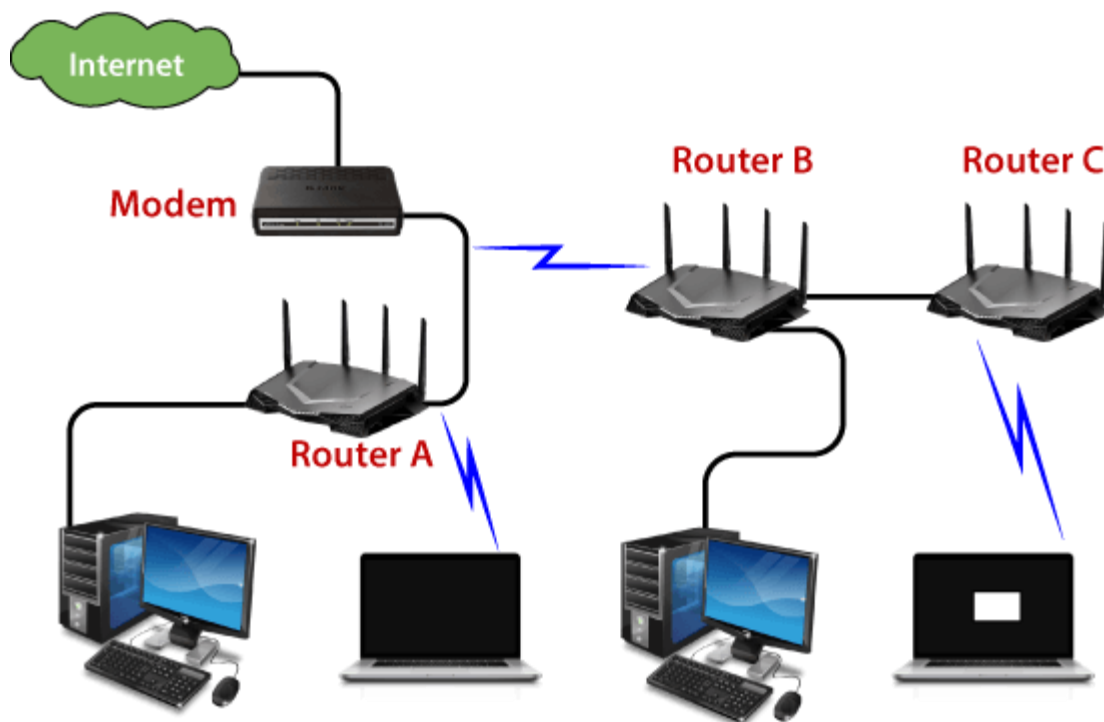
Modem is short for **"Modulator-Demodulator**." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize.

b. Bridges

A bridge is **a network device that connects multiple LANs (local area networks) together to form a larger LAN**. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network
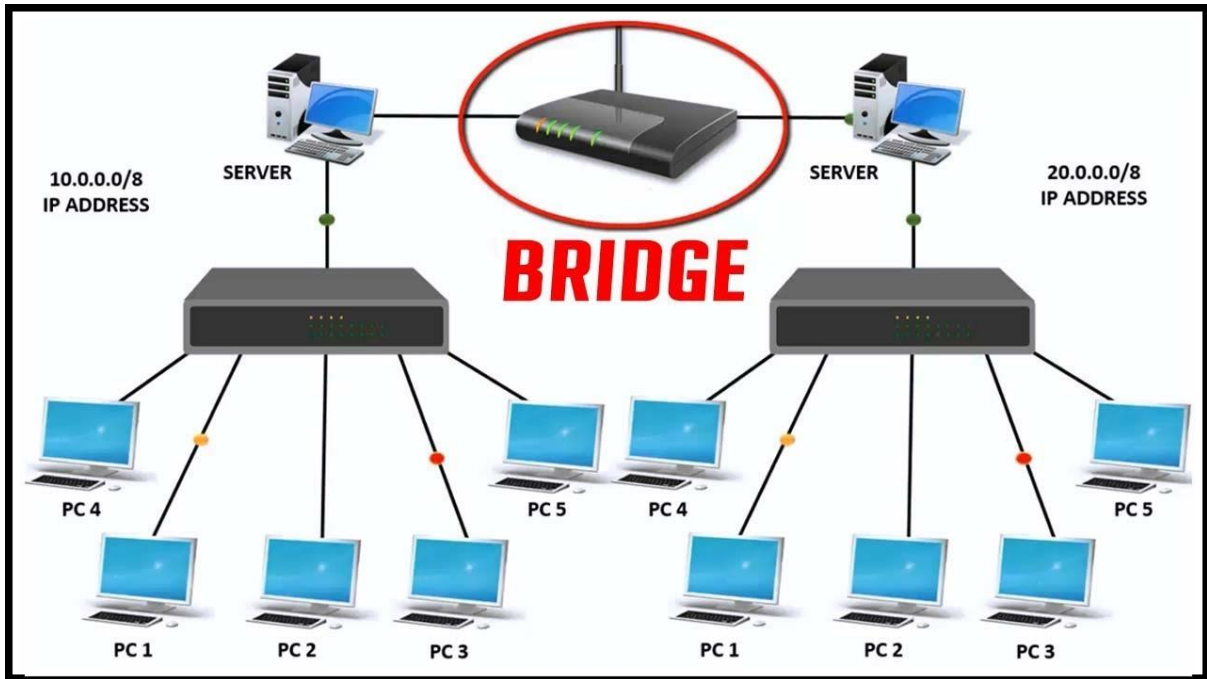
c. Hubs

A hub is **a physical layer networking device which is used to connect multiple devices in a network**. They are generally used to connect computers in a LAN. A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.


Broadcasting by a Hub
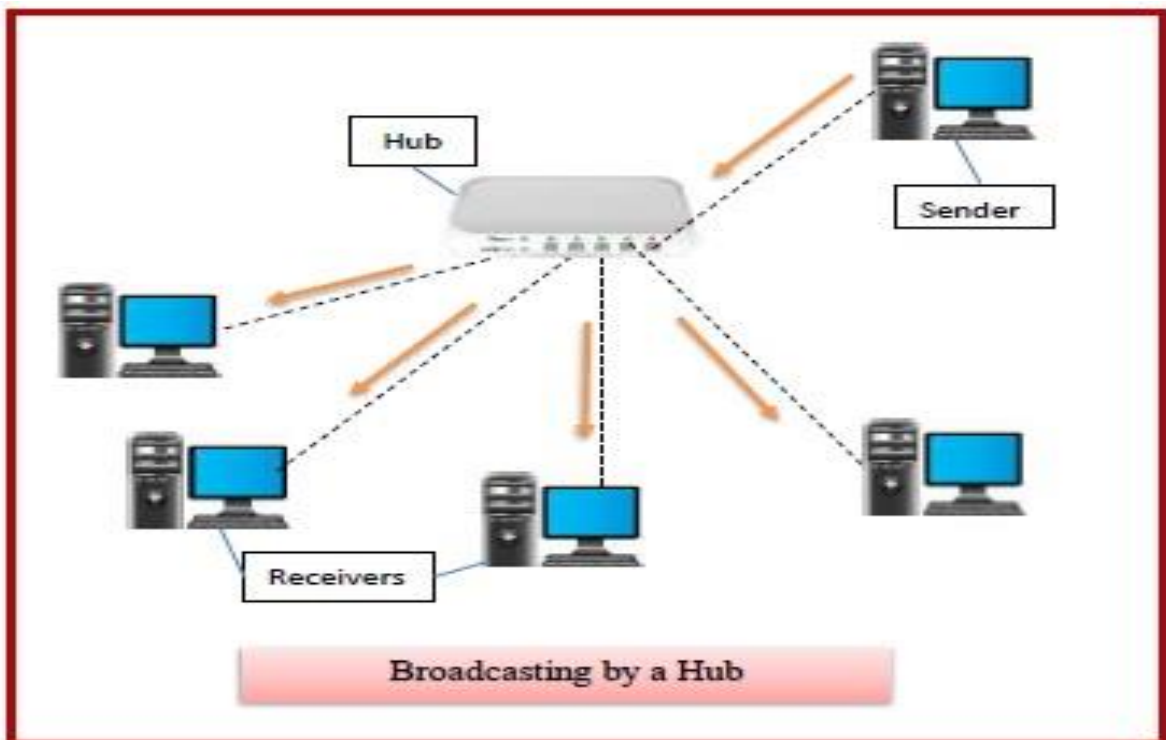
d. Repeaters

A repeater is **an electronic device in a communication channel that increases the power of a signal and retransmits it**, allowing it to travel further. Since it amplifies the signal, it requires a source of electric power. ... Use of the term has continued in telephony and data communications.
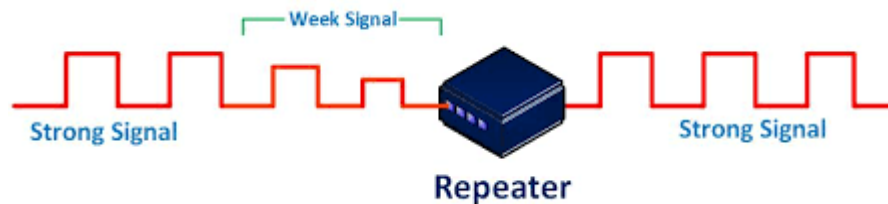
e. Gateways

A computer that sits between different networks or applications. The **gateway converts information, data or other communications from one protocol or format to another**. A router may perform some of the functions of a gateway. An Internet gateway can transfer communications between an enterprise network and the Internet.
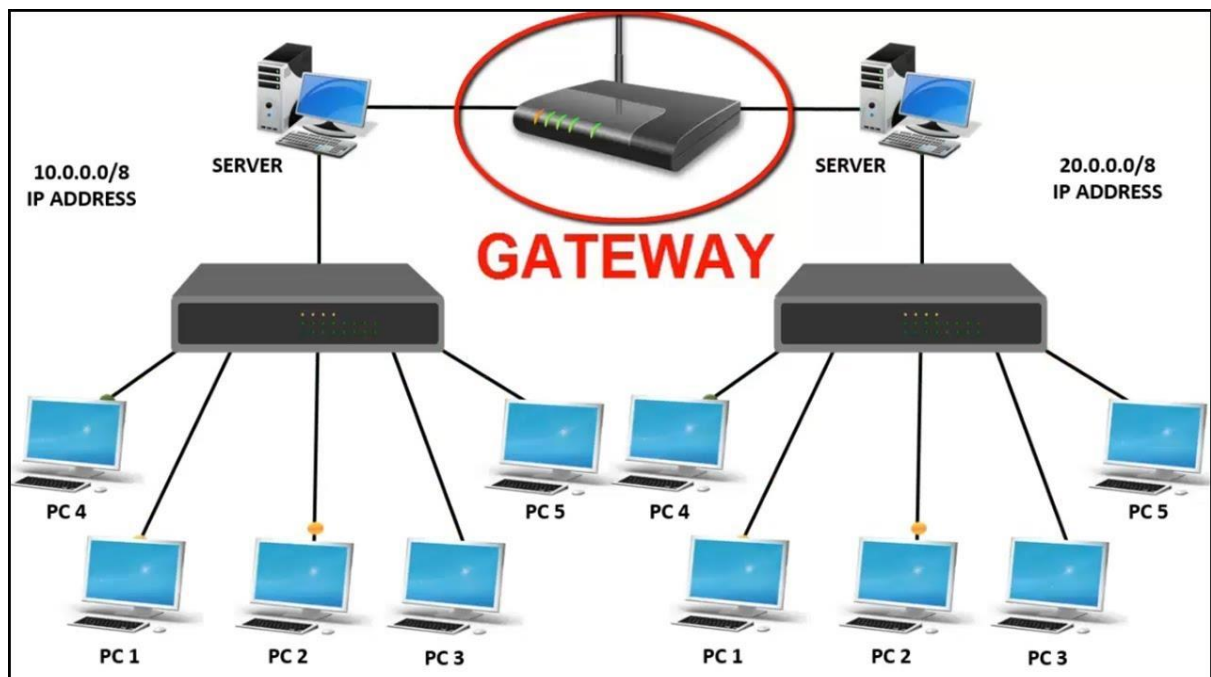
f. Switches

Switches are **key building blocks for any network**. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.
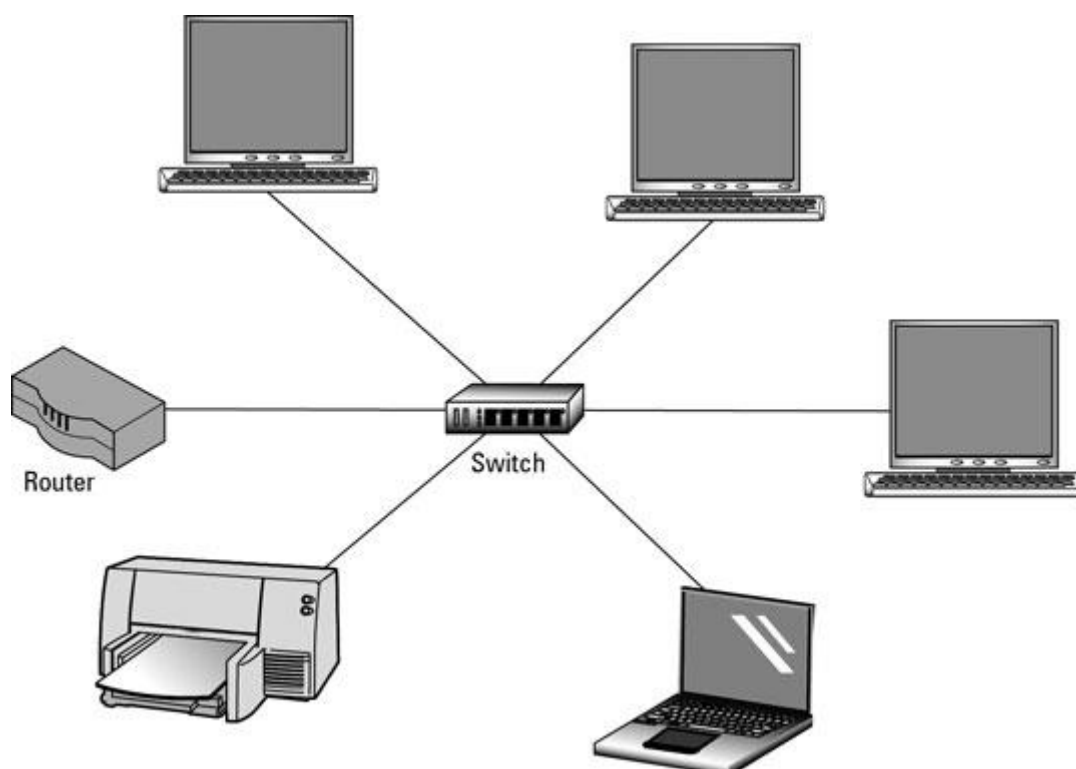
OSI Model

o   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.

o   OSI consists of seven layers, and each layer performs a particular network function.

o   OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

o   OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

o   Each layer is self-contained, so that task assigned to each layer can be performed independently.
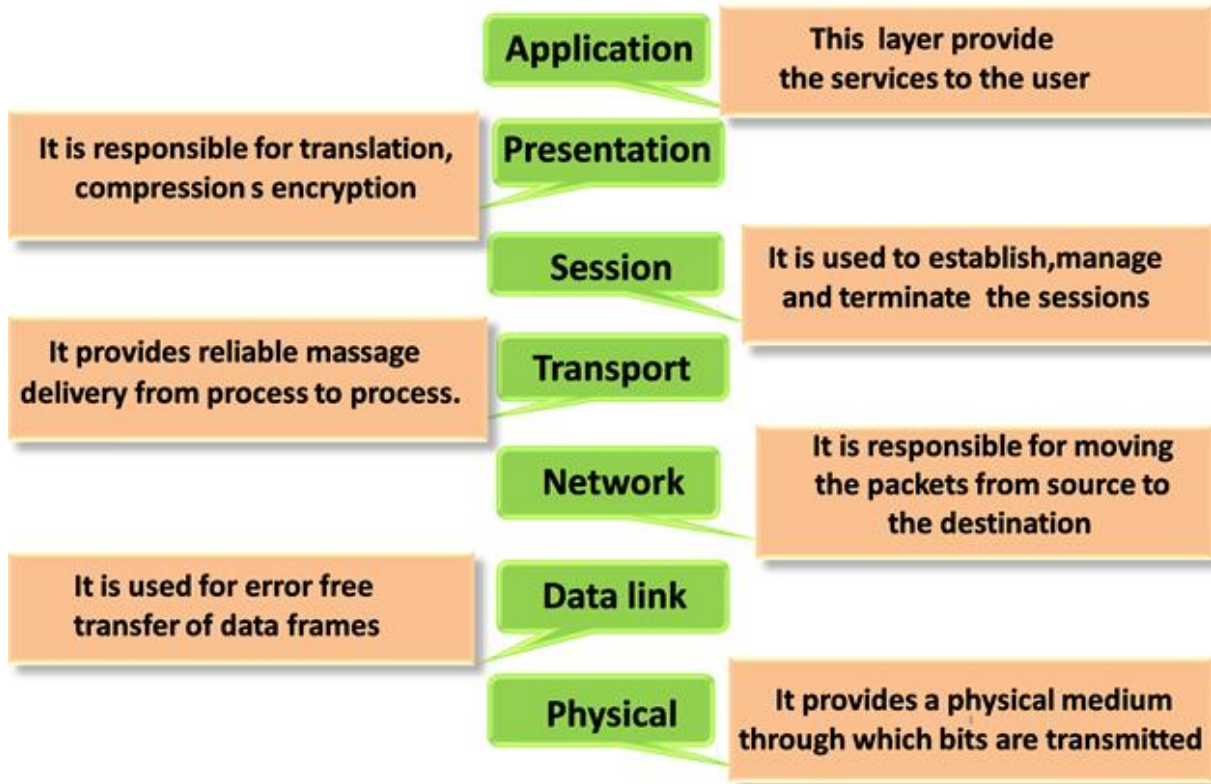
OSI Model:
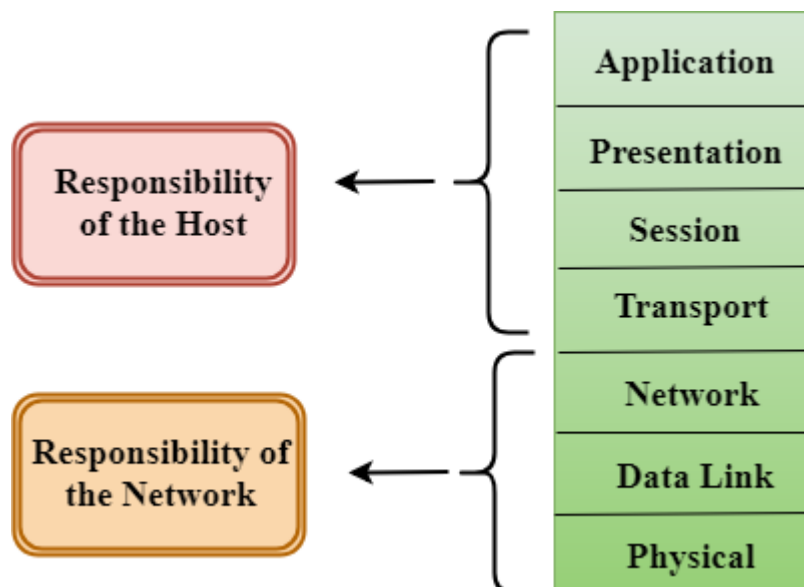
Characteristics of OSI Model

o The OSI model is divided into two layers: upper layers and lower layers.

o The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

o The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.
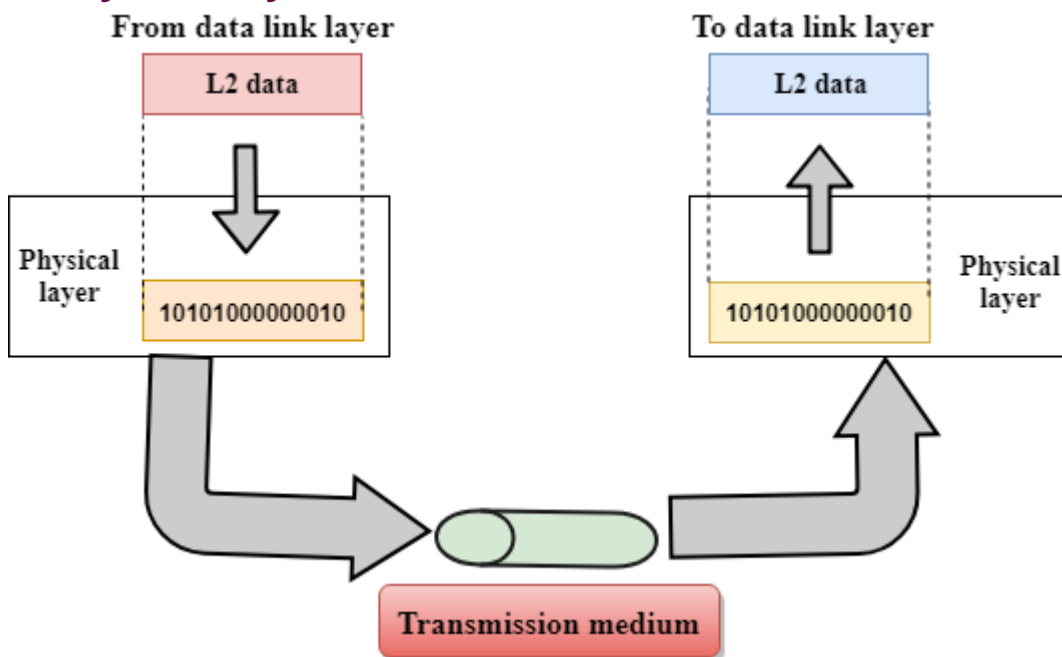
Functions of the OSI Layers

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

1.Physical layer

From data link layer   To data link layer

L2 data   L2 data

Physical layer   10101000000010   10101000000010   Physical layer

Transmission medium

o   The main functionality of the physical layer is to transmit the individual bits from one node to another node.

- It is the lowest layer of the OSI model.

- It establishes, maintains and deactivates the physical connection.

- It specifies the mechanical, electrical and procedural network interface specifications.

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.

2.Data-Link Layer
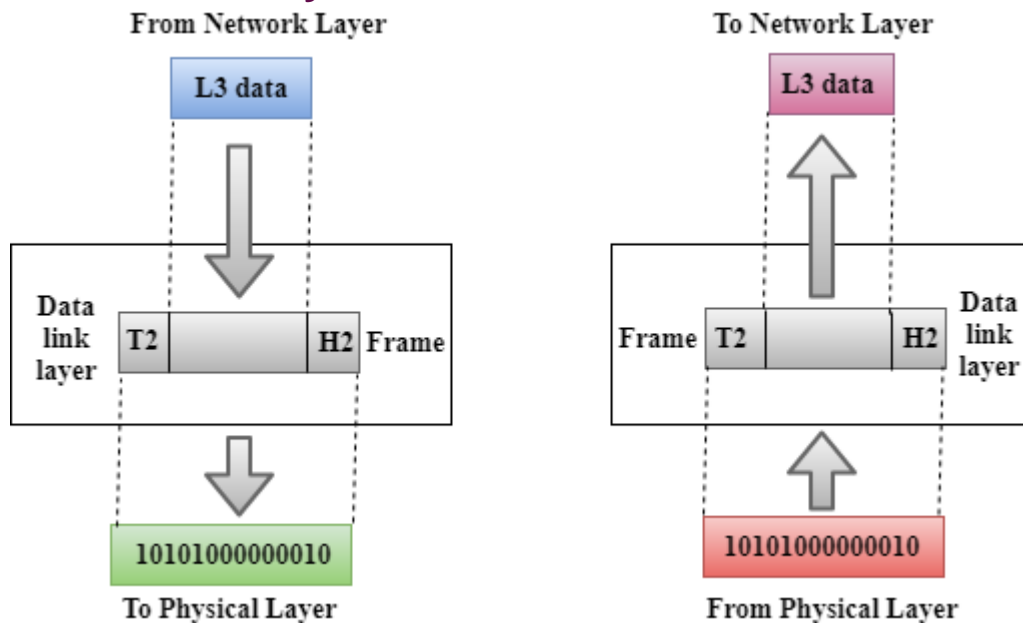
- This layer is responsible for the error-free transfer of data frames.

- It defines the format of the data on the network.

- It provides a reliable and efficient communication between two or more devices.

- It is mainly responsible for the unique identification of each device that resides on a local network.

- It contains two sub-layers:

    - **Logical Link Control Layer**

  - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.

- o It identifies the address of the network layer protocol from the header.
- o It also provides flow control.
  - o **Media Access Control Layer**
- o A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
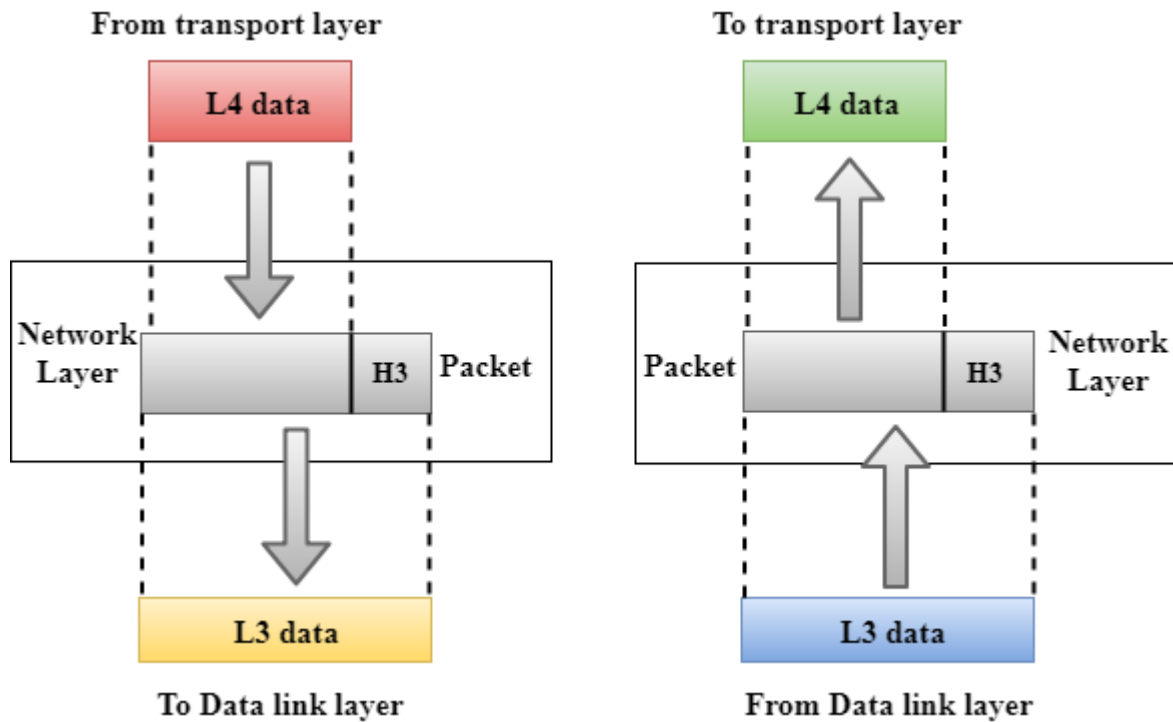- o It is used for transferring the packets over the network.

Functions of the Data-link layer

- o **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

Header	Packet	Trailer

- o **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- o **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- o **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- o **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3.Network Layer

From transport layer

L4 data

Network Layer

H3 | Packet

L3 data

To Data link layer

To transport layer

L4 data

Packet | H3

**Network Layer**

L3 data

From Data link layer

- o It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- o It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- o The Data link layer is responsible for routing and forwarding the packets.
- o Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- o The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

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

- o **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).

4. Transport Layer
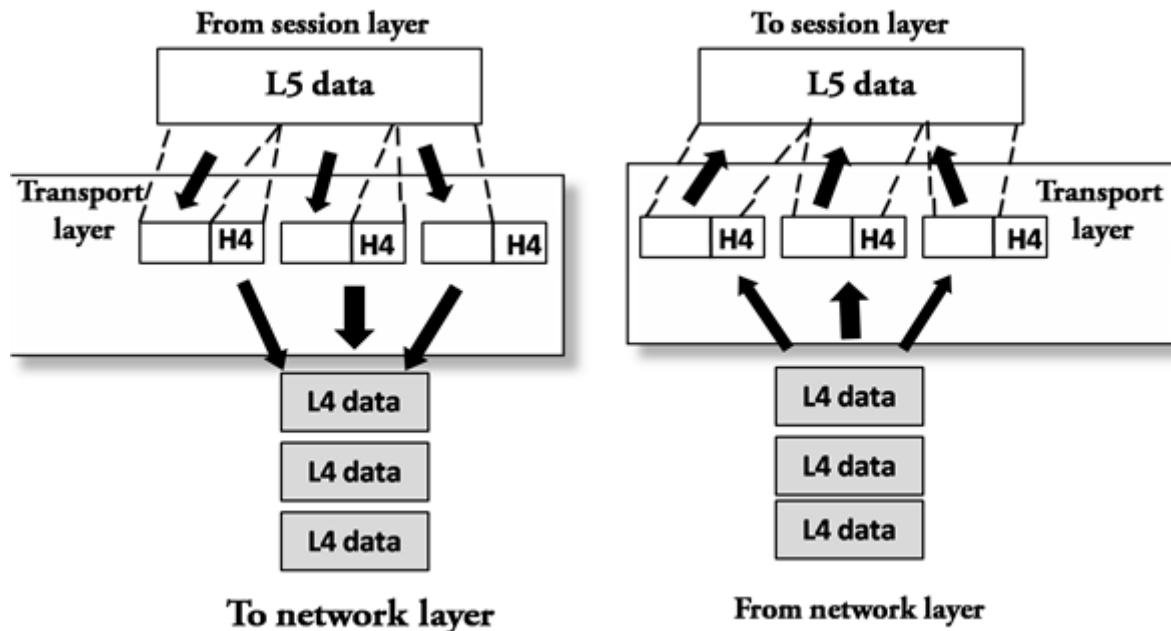
- o The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- o The main responsibility of the transport layer is to transfer the data completely.
- o It receives the data from the upper layer and converts them into smaller units known as segments.
- o This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- o **Transmission Control Protocol**
  - o It is a standard protocol that allows the systems to communicate over the internet.
  - o It establishes and maintains a connection between hosts.
  - o When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the

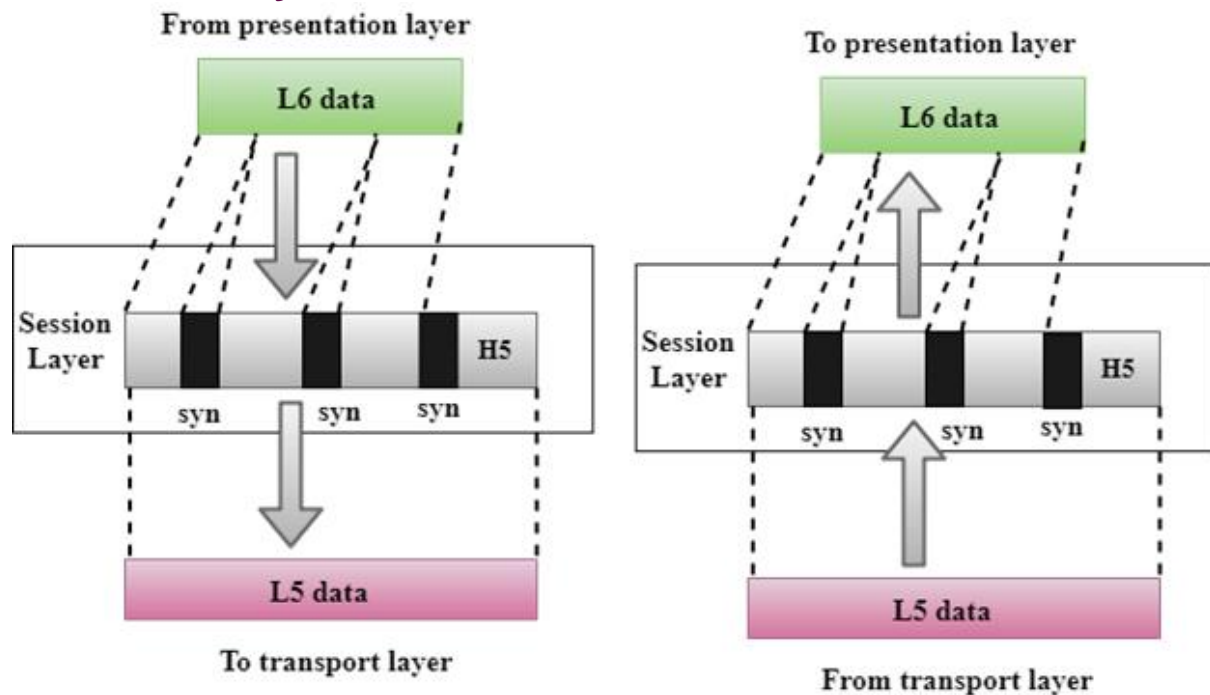destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- o **User Datagram Protocol**
    - o User Datagram Protocol is a transport layer protocol.
    - o It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- o **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- o **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- o **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- o **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- o **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5.Session Layer

From presentation layer

L6 data

Session Layer

syn   syn   syn

H5

To transport layer

To presentation layer

L6 data

Session Layer

syn   syn   syn
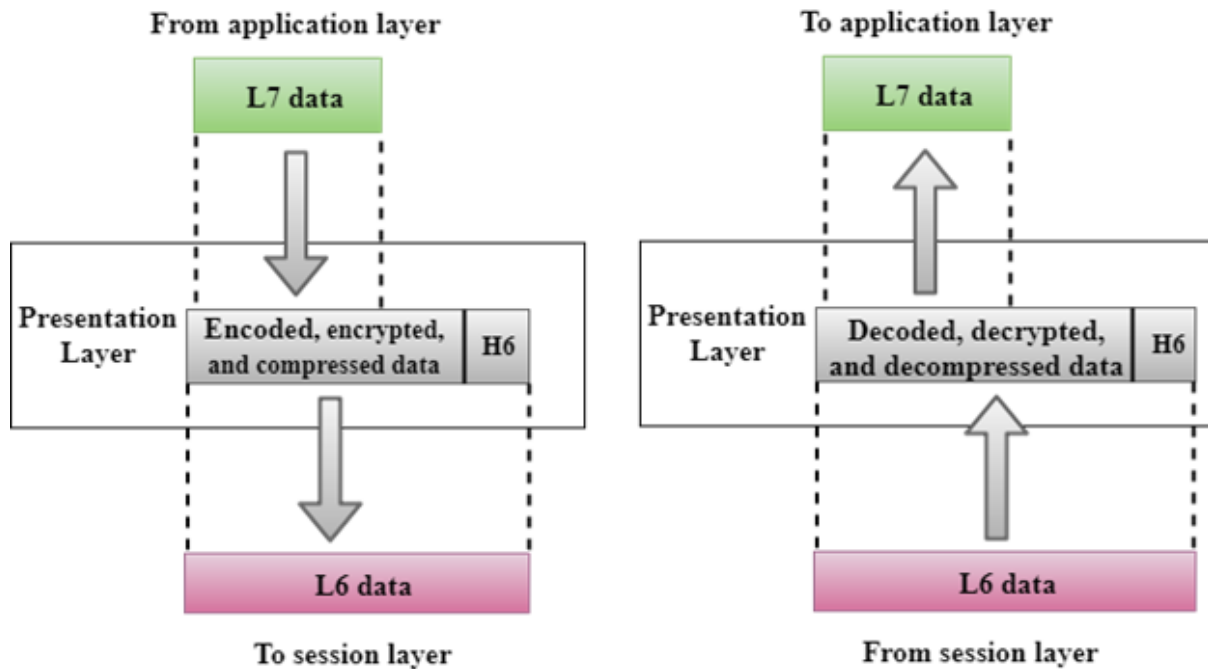
H5

From transport layer

- o It is a layer 3 in the OSI model.
- o The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- o **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

- o **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6.Presentation Layer

From application layer — L7 data → Presentation Layer → Encoded, encrypted, and compressed data | H6 → L6 data → **To session layer**

To application layer — L7 data ← Presentation Layer ← Decoded, decrypted, and decompressed data | H6 ← L6 data ← **From session layer**

- o A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- o It acts as a data translator for a network.
- o This layer is a part of the operating system that converts the data from one presentation format to another format.
- o The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- o **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- o **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- o **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.
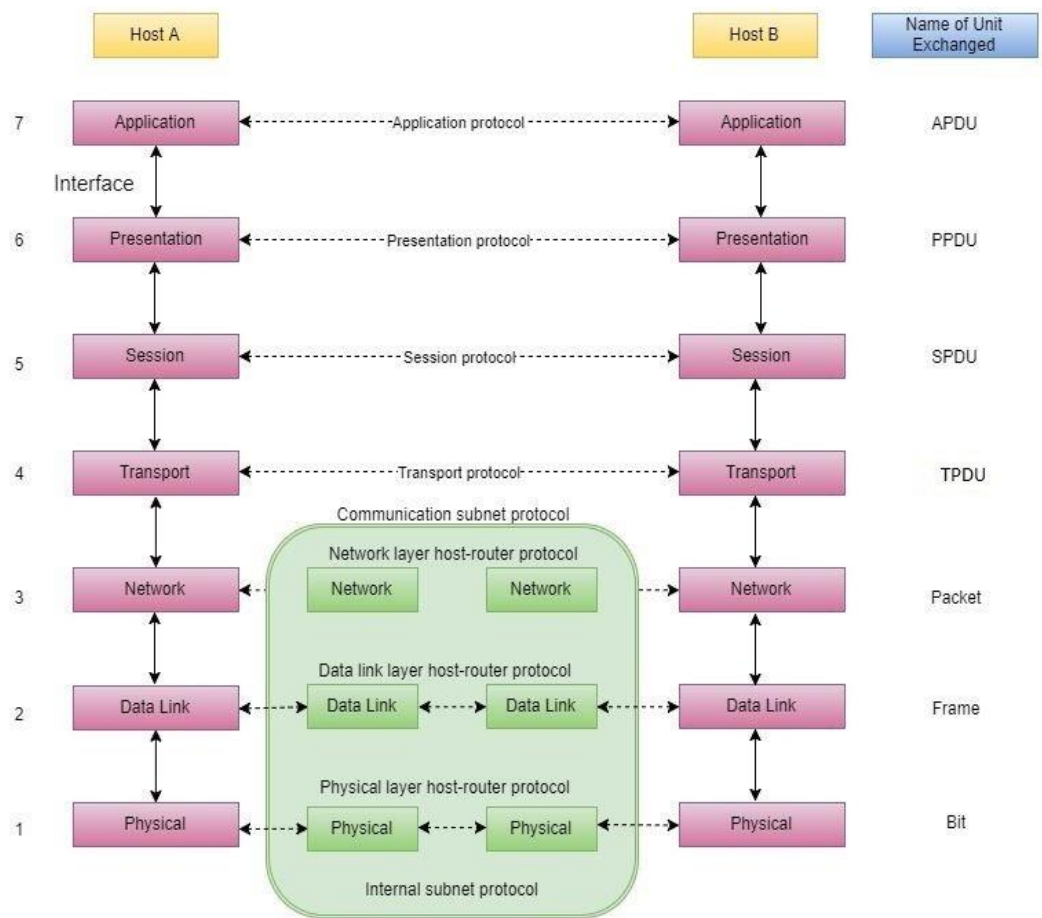
7.Application Layer
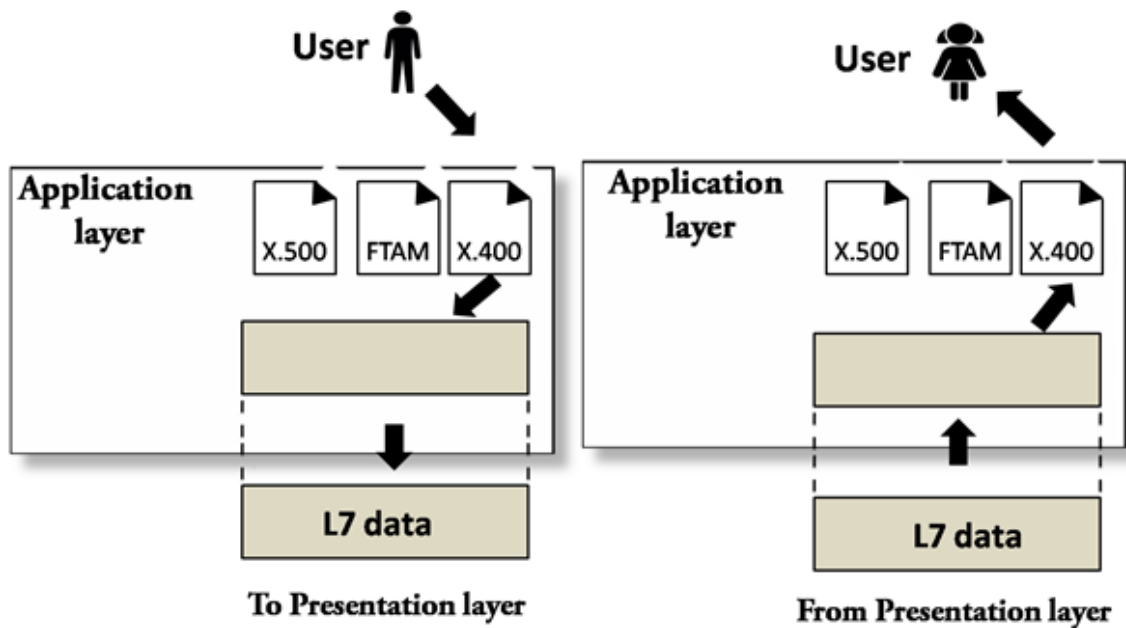
- o An application layer serves as a window for users and application processes to access network service.
- o It handles issues such as network transparency, resource allocation, etc.
- o An application layer is not an application, but it performs the application layer functions.
- o This layer provides the network services to the end-users.

Functions of Application layer:

- o **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- o **Mail services:** An application layer provides the facility for email forwarding and storage.
- o Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

|	Host A			Host B	Name of Unit Exchanged

7	Application	◄----- Application protocol ----►		Application	APDU
	Interface				
6	Presentation	◄----- Presentation protocol ----►		Presentation	PPDU
5	Session	◄----- Session protocol ----►		Session	SPDU
4	Transport	◄----- Transport protocol ----►		Transport	TPDU

Communication subnet protocol

Network layer host-router protocol

| 3 | Network | ◄-- | Network | Network | --► | Network | Packet |

Data link layer host-router protocol

| 2 | Data Link | ◄--► | Data Link | ◄--► | Data Link | ◄--► | Data Link | Frame |

Physical layer host-router protocol

| 1 | Physical | ◄--► | Physical | ◄--► | Physical | ◄--► | Physical | Bit |

Internal subnet protocol

The TCP/IP Reference Model

- TCP is Transmission Control Protocol.
- IP is Internet Protocol.
- Only 4 layers:

1	Application Layer
2	Transport Layer
3	Internet Layer
4	Link Layer (network)

TCP/IP Model Vs. OSI Model

OSI Reference Model	TCP/IP
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Internet Layer
Data Link Layer	Link Layer
Physical Layer	

Functions of TCP/IP layers:
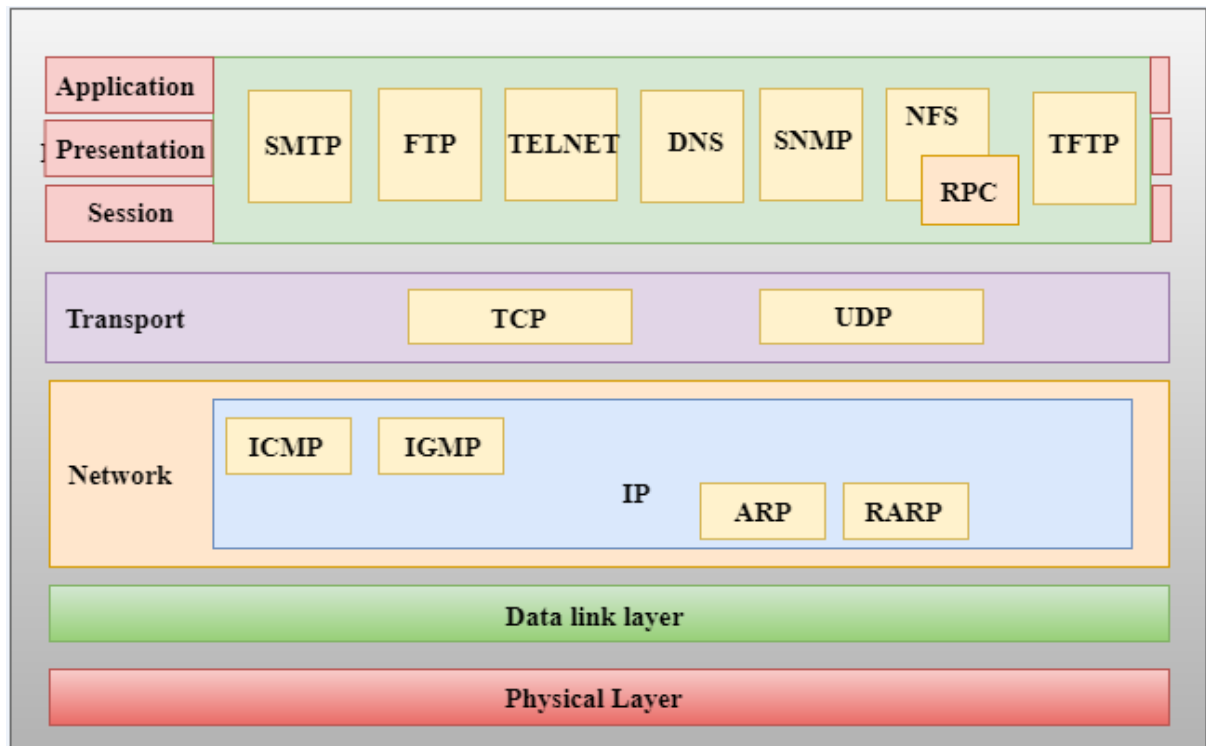
TCP/IP model

- o The TCP/IP model was developed prior to the OSI model.
- o The TCP/IP model is not exactly similar to the OSI model.
- o The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- o The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- o TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Network Access Layer

- o A network layer is the lowest layer of the TCP/IP model.
- o A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- o It defines how the data should be sent physically through the network.
- o This layer is mainly responsible for the transmission of the data between two devices on the same network.
- o The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- o The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- o An internet layer is the second layer of the TCP/IP model.
- o An internet layer is also known as the network layer.
- o The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- o **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- o **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- o **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- o **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into

smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

- o **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- o ARP stands for **Address Resolution Protocol**.
- o ARP is a network layer protocol which is used to find the physical address from the IP address.
- o **The two terms are mainly associated with the ARP Protocol:**
  - o **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - o **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

- o **ICMP** stands for Internet Control Message Protocol.
- o It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- o A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- o An ICMP protocol mainly uses two terms:
  - o **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.

- ICMP Reply: ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**
    Source port address: The source port address is the address of the application program that has created the message.
    Destination port address: The destination port address is the address of the application program that receives the message.
    Total length: It defines the total number of bytes of the user datagram in bytes.
    Checksum: The checksum is a 16-bit field used in error detection.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.

o   TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.

o   At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.

o   At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

o   An application layer is the topmost layer in the TCP/IP model.

o   It is responsible for handling high-level protocols, issues of representation.

o   This layer allows the user to interact with the application.

o   When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

o   There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

o   **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

o   **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.

o   **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.

o   **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names

instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

- o **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

- o **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Computer Network Types

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:
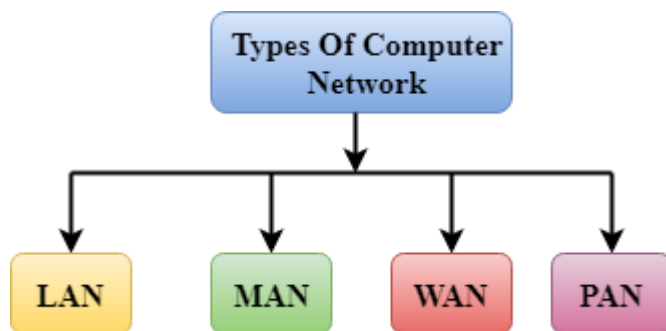
- o LAN(Local Area Network)
- o PAN(Personal Area Network)
- o MAN(Metropolitan Area Network)
- o WAN(Wide Area Network)

LAN(Local Area Network)

- o Local Area Network is a group of computers connected to each other in a small area such as building, office.

- o LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.

- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:
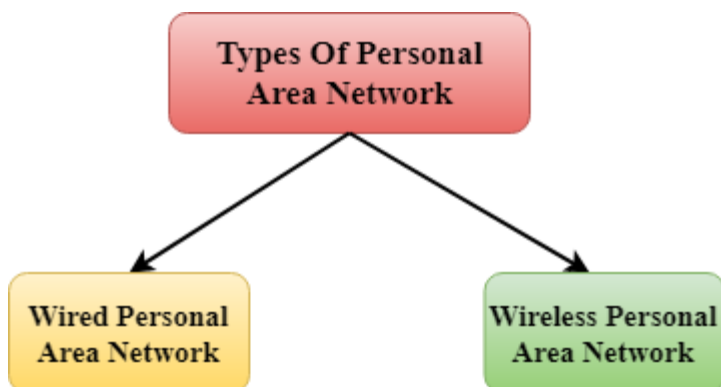
- o Wired Personal Area Network
- o Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

- o **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

- o **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.

- o **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- o A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.

- o Government agencies use MAN to connect to the citizens and private industries.

- o In MAN, various LANs are connected to each other through a telephone exchange line.

- o The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.

- o It has a higher range than Local Area Network(LAN).
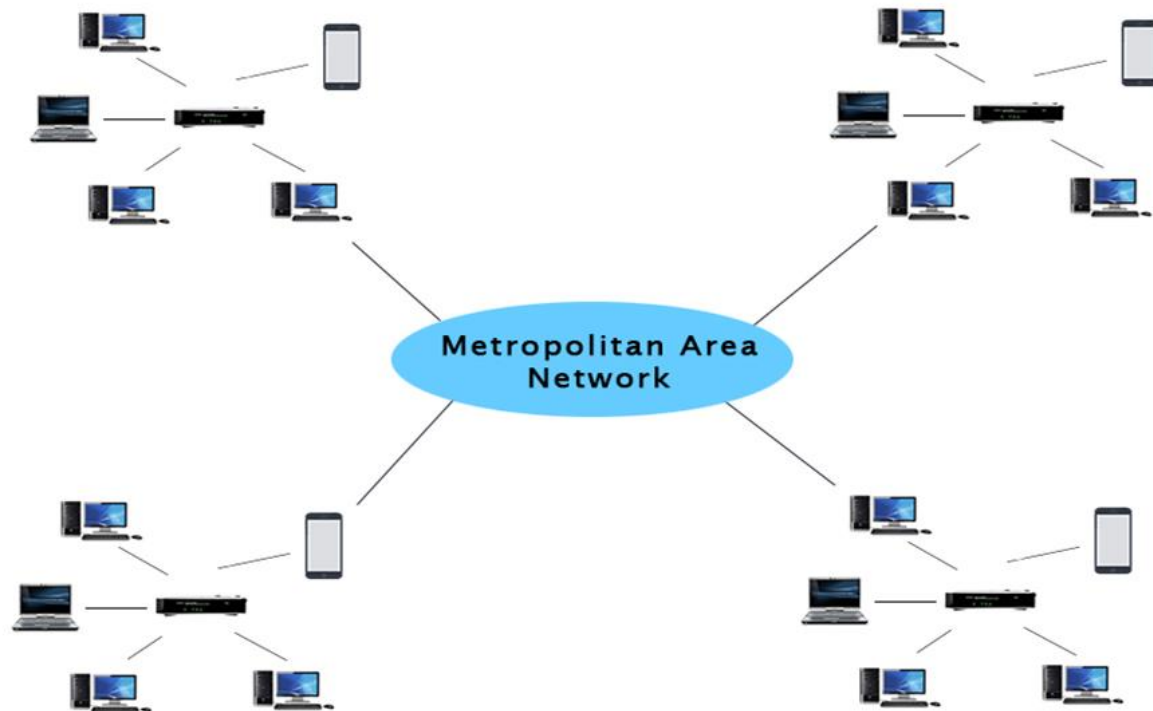
Uses Of Metropolitan Area Network:

- o MAN is used in communication between the banks in a city.
- o It can be used in an Airline Reservation.
- o It can be used in a college within a city.
- o It can also be used for communication in the military.

WAN(Wide Area Network)

- o A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- o A Wide Area Network is quite bigger network than the LAN.
- o A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- o The internet is one of the biggest WAN in the world.
- o A Wide Area Network is widely used in the field of Business, government, and education.
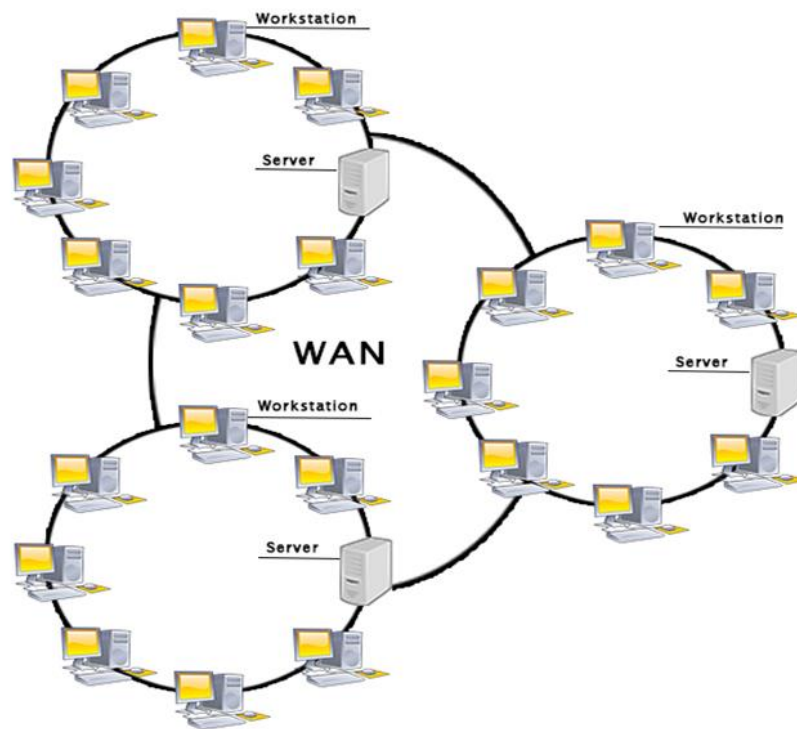
Examples Of Wide Area Network:

- o **Mobile Broadband:** A 4G network is widely used across a region or country.
- o **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- o **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- o **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- o **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- o **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- o **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.

- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- o **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.

- o **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.

- o **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.

- o **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.

- o **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

ARPANET

This may be considered as the breakthrough for many of current ideas, algorithms and Internet technologies. It started Paul Baran in 1960s funded by **Advanced Research Projects Agency** (*ARPA*), an organization of the united States Defense Department and, therefore, named as **Advanced Research Projects Agency Network** (**ARPANET**) predecessor of the modern Internet. It

was **world's first fully operational packet switching** computer **network** and the world's first successful computer network to implement the TCP/IP reference model that was used earlier by ARPANET, before being used in the Internet. The ARPANET is the first network that planed the seed of interent.

ARPANET was built to accommodate research equipment on packet switching technology and to allow resource sharing for the Department of Defense's contractors. The network interconnected research centers, some military bases and government locations. It soon became popular with researchers for collaboration through electronic mail and other services.

• It is basically a WAN. It was developed by the ARPA (Advanced Research Project Agency) in 1968 which is the research arm of 000.
• ARPANET was designed to service even a nuclear attack.
• Before ARPANET, the networks were basically the telephone networks which operated on the circuit switching principle.
• But this network was too vulnerable, because the loss of even one line or switch would terminate all the conversations.
• ARPANET used the concept of packet switching network consisting of subnet and host computers.
• The subnet was a datagram subnet and each subnet consists of minicomputers called IMPs (Interface Message Processors).
• Each node of the network used to have an IMP and a host connected by a short wire.
• The host could send messages of upto 8063 bits to its IMP which would break them into packets and forward them independently toward the destination.
• The subnet was the first electronic store-and-forward type packet switched network. So each packet was stored before it was forwarded.

Arpanet
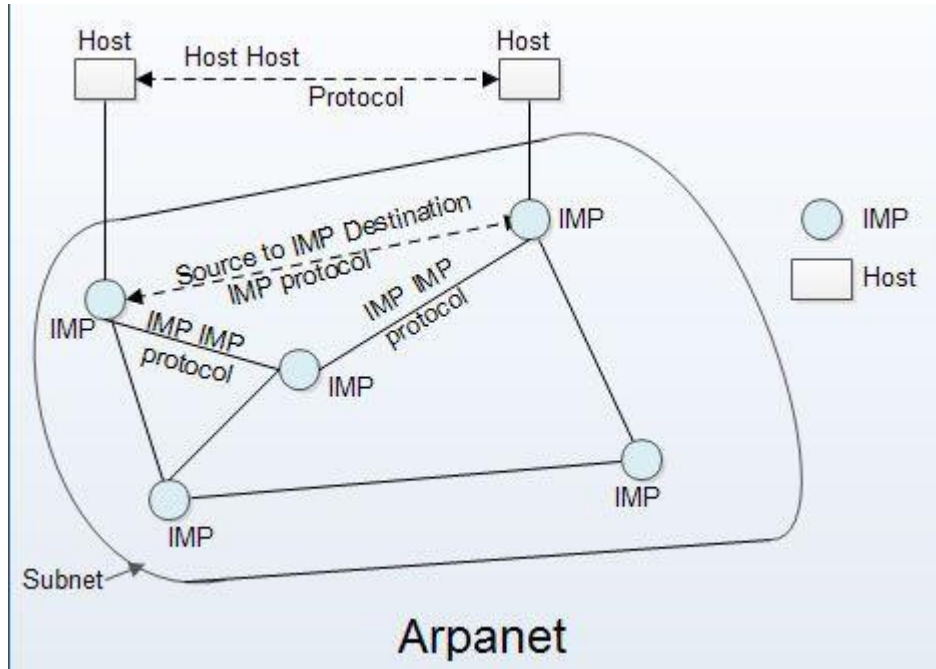
internet

Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web. It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide. It is set up by using cables such as optical fibers and other wireless and networking technologies. At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.

It is believed that the internet was developed by "Defense Advanced Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.

Why is the Internet Called a Network?

Internet is called a network as it creates a network by connecting computers and servers across the world using routers, switches and telephone lines, and other communication devices and channels. So, it can be considered a global network of physical cables such as copper telephone wires, fiber optic cables, tv cables, etc. Furthermore, even wireless connections like 3G, 4G, or Wi-Fi make use of these cables to access the Internet.

Internet is different from the World Wide Web as the World Wide Web is a network of computers and servers created by connecting them through the internet. So, the internet is the backbone of the web as it provides the technical infrastructure to establish the WWW and acts as a medium to transmit information from one computer to another computer. It uses web browsers to display the information on the client, which it fetches from web servers.

How does internet work?

Before understanding this let us understand some basics related to internet:

The internet works with the help of clients and servers. A device such as a laptop, which is connected to the internet is called a client, not a server as it is not directly connected to the internet. However, it is indirectly connected to the internet through an Internet Service Provider (ISP) and is identified by an IP address, which is a string of numbers. Just like you have an address for your home that uniquely identifies your home, an IP address acts as the shipping address of your device. The IP address is provided by your ISP, and you can see what IP address your ISP has given to your system.

A server is a large computer that stores websites. It also has an IP address. A place where a large number of servers are stored is called a data center. The server accepts requests send by the client through a browser over a network (internet) and responds accordingly.

To access the internet we need a domain name, which represents an IP address number, i.e., each IP address has been assigned a domain name. For example, youtube.com, facebook.com, paypal.com are used to represent the IP addresses. Domain names are created as it is difficult for a person to remember a long string of numbers. However, internet does not understand the domain name, it understands the IP address, so when you enter the domain name in the browser search bar, the internet has to get the IP addresses of this domain name from a huge phone book, which is known as DNS (Domain Name Server).

For example, if you have a person's name, you can find his phone number in a phone book by searching his name. The internet uses the DNS server in the same way to find the IP address of the domain name. DNS servers are managed by ISPs or similar organizations.

Now after understanding the basics, let us see how internet works?
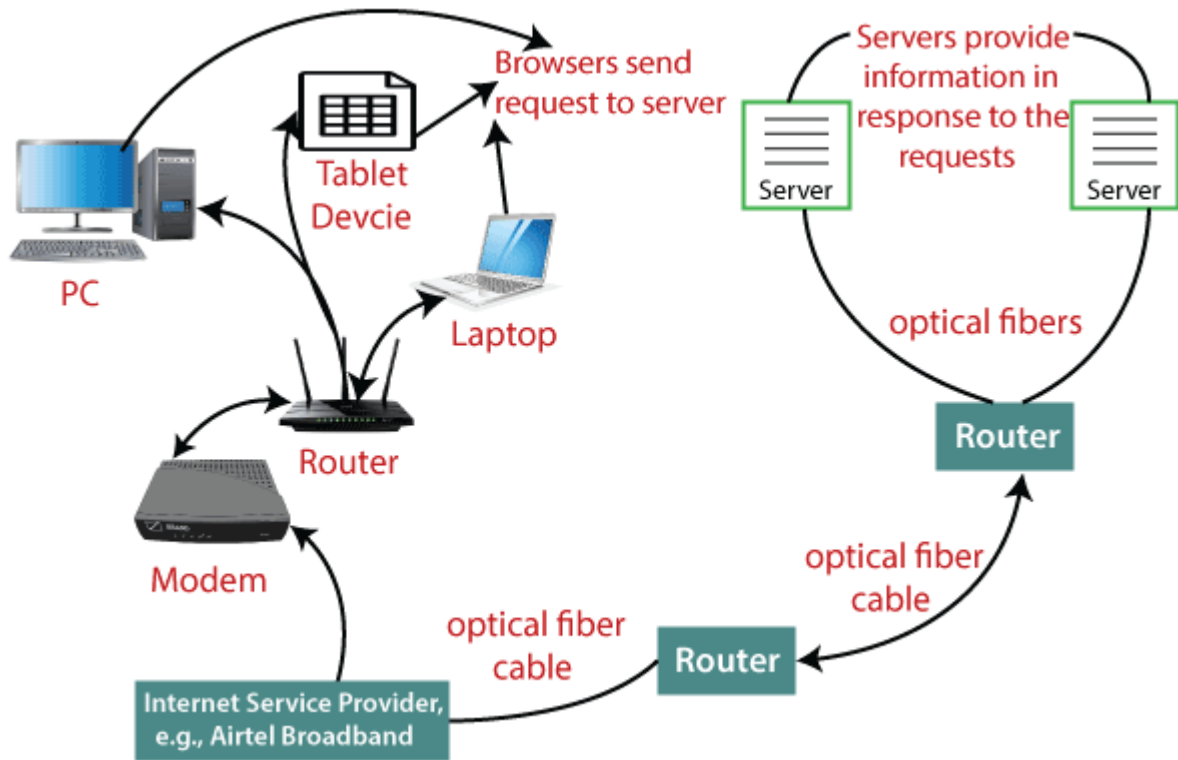
Advantages of the Internet:

- o **Instant Messaging:** You can send messages or communicate to anyone using internet, such as email, voice chat, video conferencing, etc.
- o **Get directions:** Using GPS technology, you can get directions to almost every place in a city, country, etc. You can find restaurants, malls, or any other service near your location.
- o **Online Shopping:** It allows you to shop online such as you can be clothes, shoes, book movie tickets, railway tickets, flight tickets, and more.
- o **Pay Bills:** You can pay your bills online, such as electricity bills, gas bills, college fees, etc.
- o **Online Banking:** It allows you to use internet banking in which you can check your balance, receive or transfer money, get a statement, request cheque-book, etc.
- o **Online Selling:** You can sell your products or services online. It helps you reach more customers and thus increases your sales and profit.
- o **Work from Home:** In case you need to work from home, you can do it using a system with internet access. Today, many companies allow their employees to work from home.
- o **Entertainment:** You can listen to online music, watch videos or movies, play online games.
- o **Cloud computing:** It enables you to connect your computers and internet-enabled devices to cloud services such as cloud storage, cloud computing, etc.
- o **Career building:** You can search for jobs online on different job portals and send you CV through email if required.

Physical layer

Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types Of Guided media:

Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.

Jacket   Twisted Pair   Bare Wire
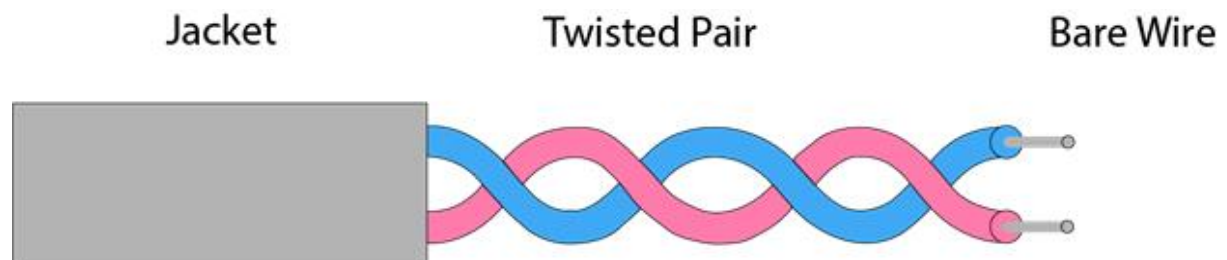
Types of Twisted pair:
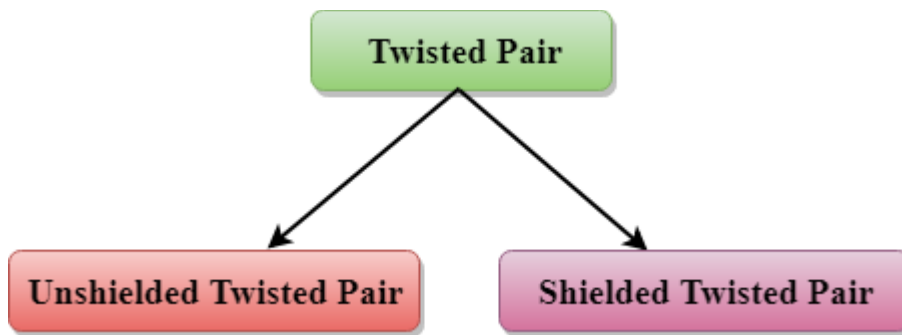
Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- o **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- o **Category 2:** It can support upto 4Mbps.
- o **Category 3:** It can support upto 16Mbps.
- o **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- o **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- o It is cheap.
- o Installation of the unshielded twisted pair is easy.
- o It can be used for high-speed LAN.

Disadvantage:

- o This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

- o   The cost of the shielded twisted pair cable is not very high and not very low.
- o   An installation of STP is easy.
- o   It has higher capacity as compared to unshielded twisted pair cable.
- o   It has a higher attenuation.
- o   It is shielded that provides the higher data transmission rate.

Disadvantages

- o   It is more expensive as compared to UTP and coaxial cable.
- o   It has a higher attenuation rate.

Coaxial Cable

- o   Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- o   The name of the cable is coaxial as it contains two conductors parallel to each other.
- o   It has a higher frequency as compared to Twisted pair cable.
- o   The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- o   The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).

Jacket   Shield   Insulator   Centre Conductor
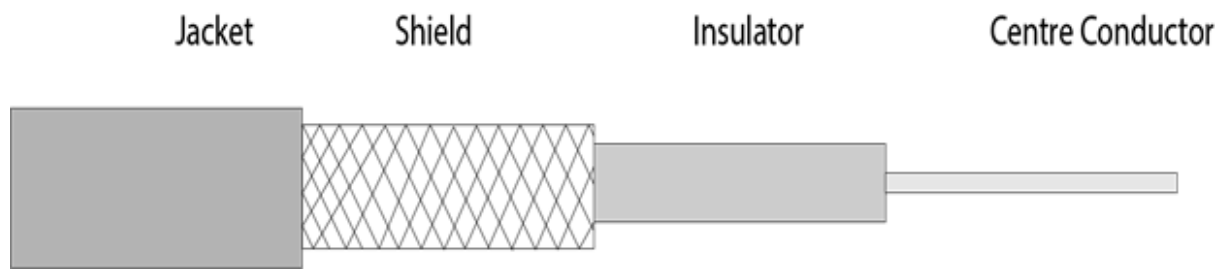
Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

o   The data can be transmitted at high speed.
o   It has better shielding as compared to twisted pair cable.
o   It provides higher bandwidth.

Disadvantages Of Coaxial cable:

o   It is more expensive as compared to twisted pair cable.
o   If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

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

Diagrammatic representation of fibre optic cable:
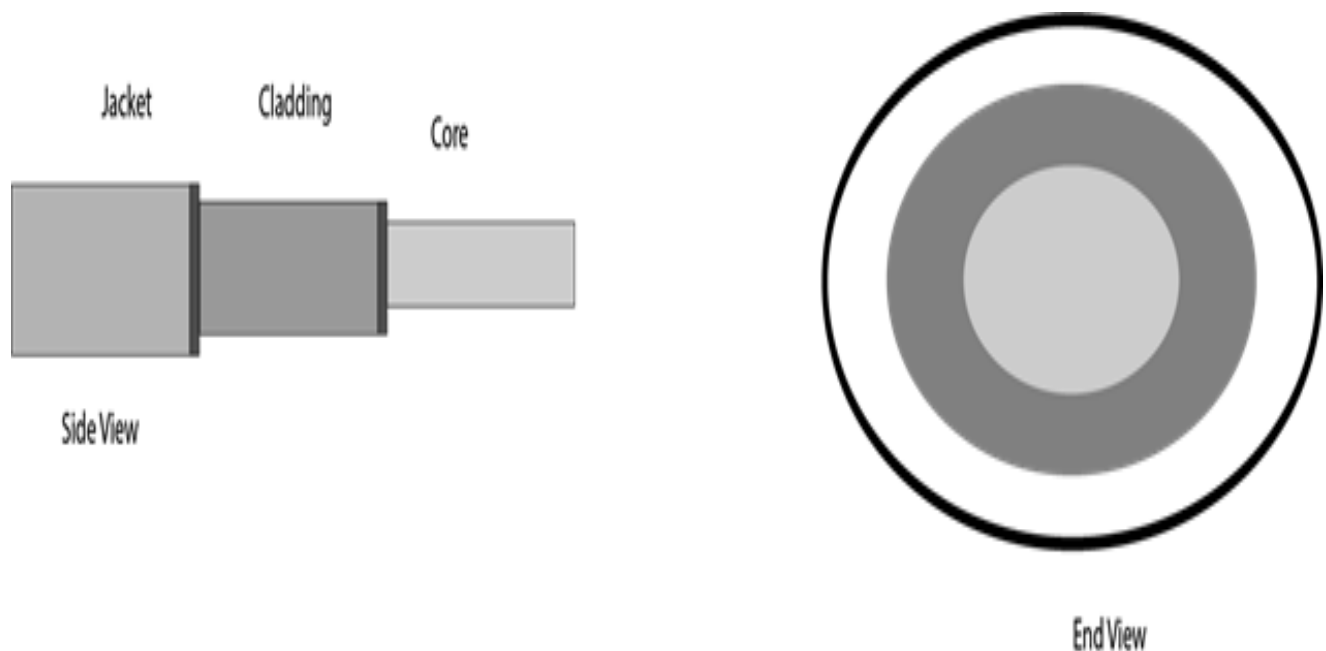
Basic elements of Fibre optic cable:

- o **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- o **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

UnGuided Transmission

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.
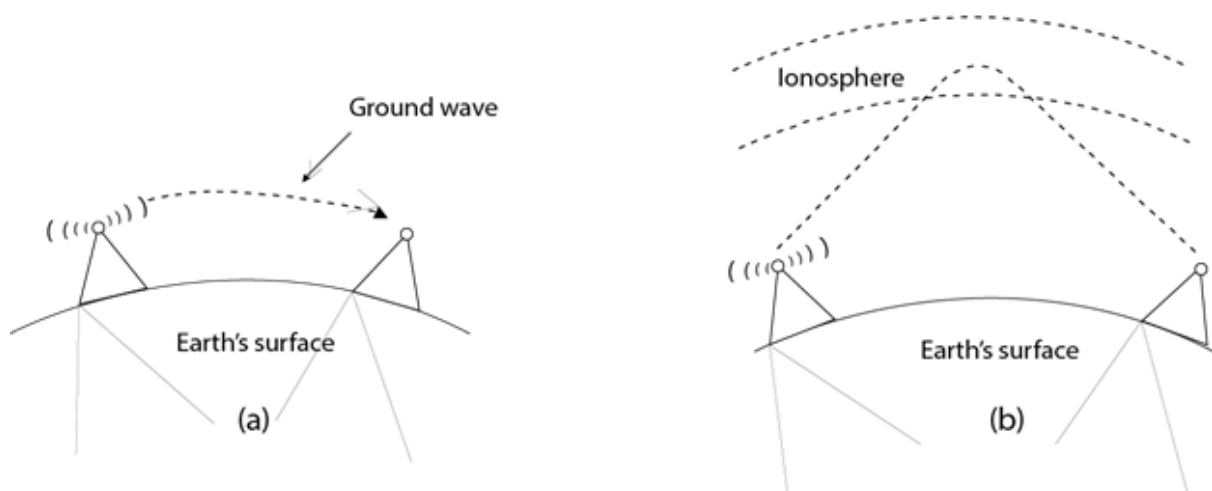
Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- o Radio transmission is mainly used for wide area networks and mobile cellular phones.
- o Radio waves cover a large area, and they can penetrate the walls.
- o Radio transmission provides a higher transmission rate.

Microwaves
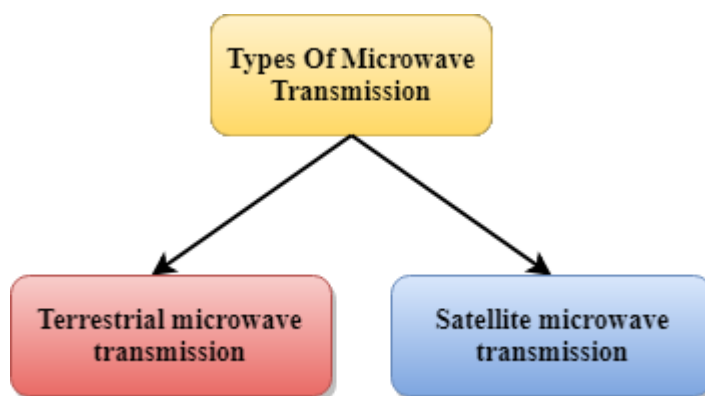
- o Terrestrial microwave
- o Satellite microwave communication.

Terrestrial Microwave Transmission

- o Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- o Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- o Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- o In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.

- o It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- o **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- o **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- o **Short distance:** It is inexpensive for short distance.
- o **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- o **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- o Microwave transmission is cheaper than using cables.
- o It is free from land acquisition as it does not require any land for the installation of cables.
- o Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- o Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- o **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- o **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- o **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- o **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- o A satellite is a physical object that revolves around the earth at a known height.

- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

How Does Satellite work?

The satellite accepts the signal that is transmitted from the earth station, and it amplifies the signal. The amplified signal is retransmitted to another earth station.

Advantages Of Satellite Microwave Communication:

- The coverage area of a satellite microwave is more than the terrestrial microwave.
- The transmission cost of the satellite is independent of the distance from the centre of the coverage area.
- Satellite communication is used in mobile and wireless communication applications.
- It is easy to install.
- It is used in a wide variety of applications such as weather forecasting, radio/TV signal broadcasting, mobile communication, etc.

Disadvantages Of Satellite Microwave Communication:

- Satellite designing and development requires more time and higher cost.
- The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.
- The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- o It supports high bandwidth, and hence the data rate will be very high.
- o Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- o An infrared communication provides better security with minimum interference.
- o Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.