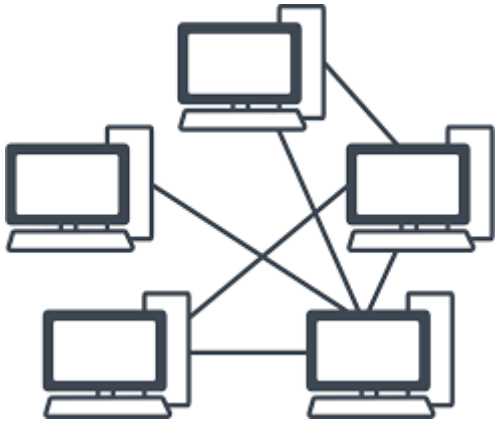
A computer network is a set of interconnected devices that communicate and share resources seamlessly.

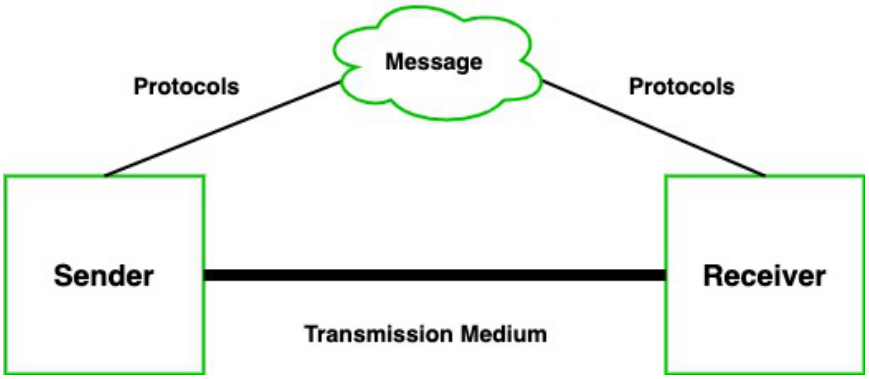
The primary purpose of a network is to enable communication and resource-sharing among its interconnected components. The aim of the computer network is the sharing of resources among various devices.



Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium / Communication Channels:** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Set of rules (Protocol):** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.



Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:

TCP(Transmission Control Protocol): It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer.

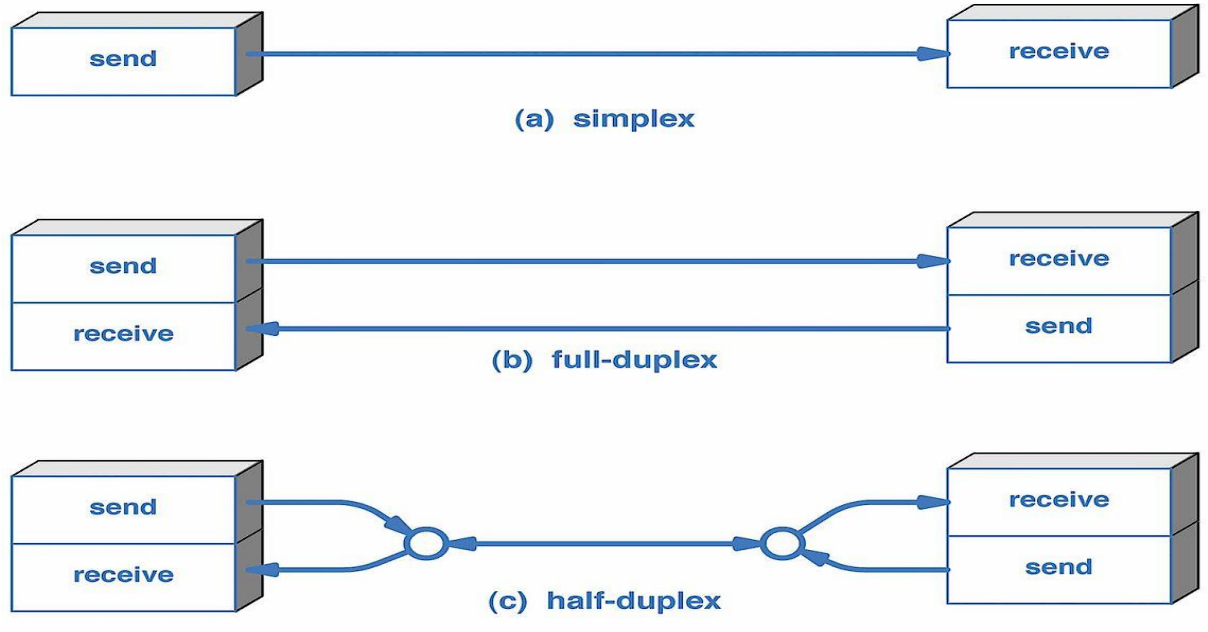
IP(Internet Protocol): computer determine which packet belongs to which device

Type of data communication

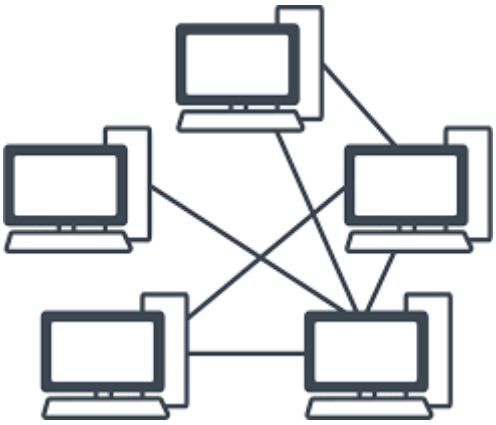
The data communication is divided into three types:

1. **Simplex Communication:** It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.

2. **Half Duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.
3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

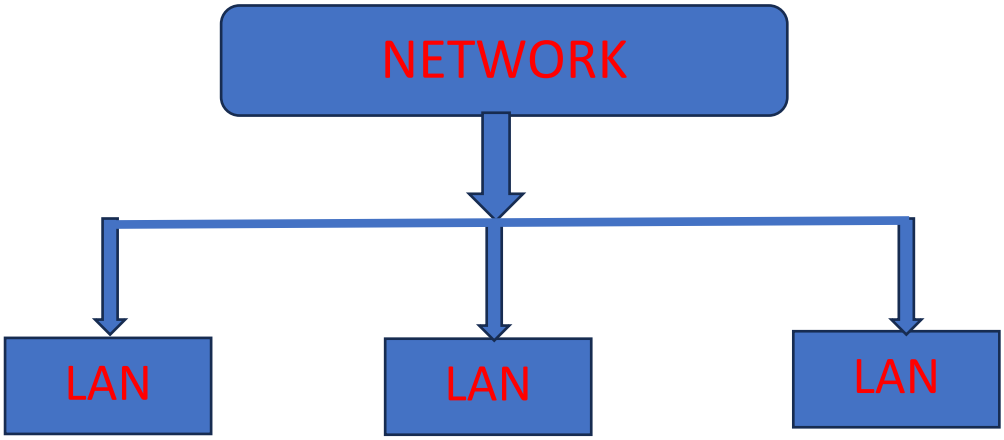


A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.



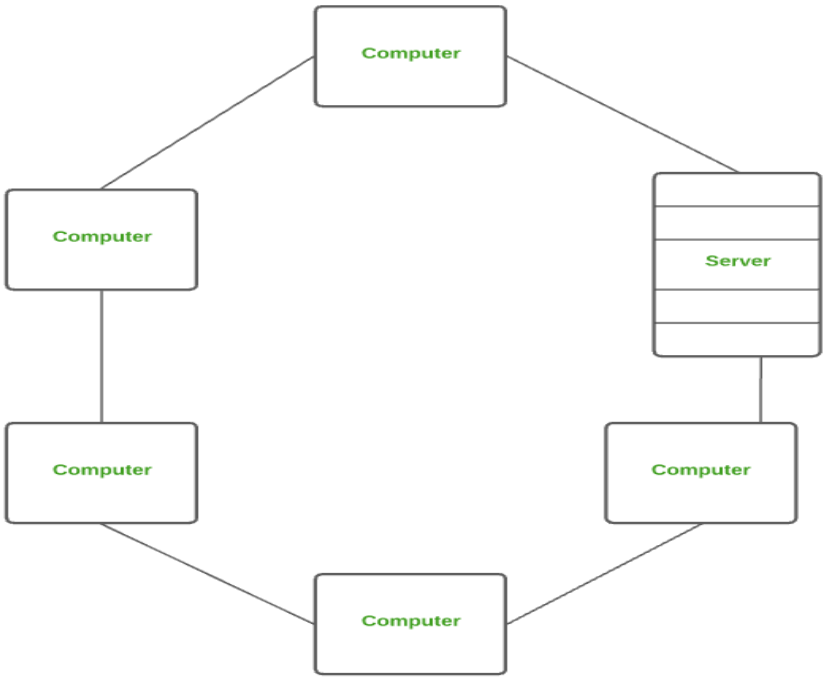
A computer network can be categorized by their size. **A** computer network **is mainly of** Three types**:**

1. Local Area Network(LAN)
2. Metropolitan Area Network(MAN)
3. Wide Area Network(WAN)



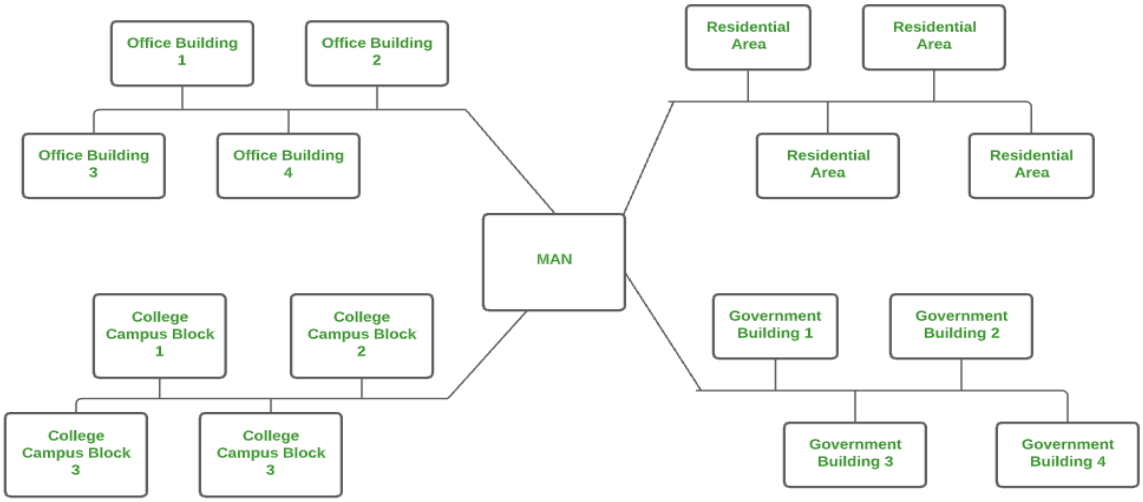
LAN(Local Area Network)

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



MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

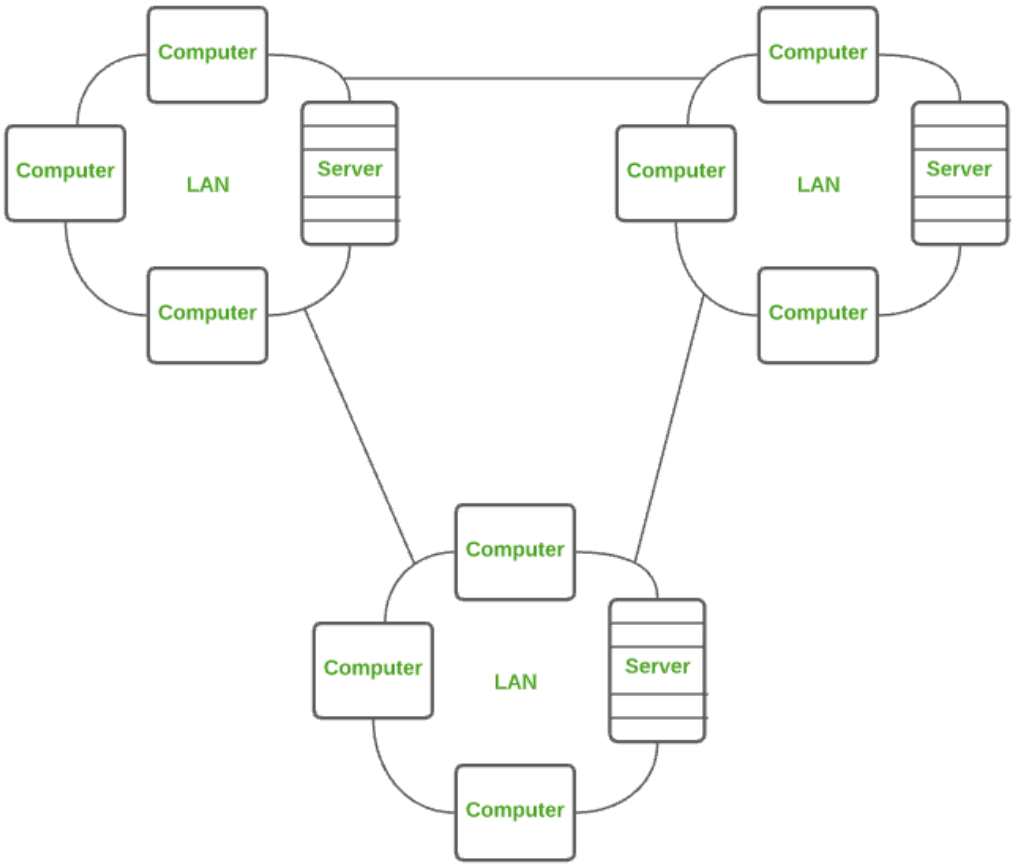


WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- 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.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.

Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **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.
- **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.



Parameters	LAN	MAN	WAN
Full Name	Local Area Network	Metropolitan Area Network	Wide Area Network
Technology	Ethernet & Wifi	FDDI, CDDi. ATM	Leased Line, Dial-Up
Range	Upto 2km	5-50 km	Above 50 km
Transmission Speed	Very High	Average	Low
Ownership	Private	Private or Public	Private or Public
Maintenance	Easy	Difficult	Very Difficult
Cost	Low	High	Very High

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.

Other Types of Computer Networks

1. Wireless Local Area Network (WLAN)
2. Storage Area Network (SAN)
3. System-Area Network (SAN)
4. Passive Optical Local Area Network (POLAN)
5. Enterprise Private Network (EPN)
6. Virtual Private Network (VPN)
7. Home Area Network (HAN)

History of Internet

The Internet was developed by Bob Kahn and Vint Cerf in the 1970s. They began the design of what we today know as the 'internet.' It was the result of another research experiment which was called ARPANET, which stands for Advanced Research Projects Agency Network and started in the year 1983.This was initially supposed to be a communications system for the Defense Team of the United States of America - a network that would also survive a nuclear attack. It eventually became a successful nationwide experimental packet network. But when was the first Internet started? It is believed that on 6 August 1991, when the World Wide Web opened to the public.

How Does the Internet Work?

Computers that we use every day are called clients because they are indirectly connected to the Internet through an internet service provider. When you open a webpage on your computer, you connect to the webpage, and then you can access it. Computers break the information into smaller pieces called packets, which are reassembled in their original order.

If we put the right address on a packet and send it to any computer which is connected as part of the internet, each computer would figure out which cable to send it down next so that it would get to its destination. With several computers on a network, it may create confusion even with unique addresses. This transfer of messages is handled by the Packet Routing Network, and hence a router is required to set up.

The Transfer Control Protocol is another system that makes sure no packet is lost or left behind because it might create a disrupted message at the receiving end.

The below are the steps for how the message is transferred.

1. First, Computer1 sends a message by IP address to Computer2
2. The message sent by Computer1 is broken into small pieces- packets.
3. These small pieces- packets are transferred concerning Transfer Protocol so that the quality is maintained.
4. Finally, these small pieces- packets reach Computer2 and are reassembled at their IP address.

The Internet works in a more complex manner than these above-given steps, but this might give a basic idea of how the internet works.

Father of the Internet: Tim Berners-Lee

Tim Berners-Lee was the man, who led the development of the World Wide Web, the defining of HTTP (HyperText Transfer Protocol), HTML (hypertext markup language) used to create web pages, and URLs (Universal Resource Locators). The development of WWW, HTTP, HTML and URLs took place between 1989 and 1991. Tim Berners-Lee was born in London and he graduated in Physics from Oxford University in 1976. Currently, Tim Berners-Lee is the Director of the World Wide Web Consortium, the group that sets technical standards for the web.

Tim Berners-Lee, Vinton Cerf is also named as an internet daddy other than Tim Berners-Lee. After being out for 10 years from high school, he began co-designing and co-developing the protocols and structure of what became the internet.

History of HTML

In 1945, Vannevar Bush first introduced the basics of hypertext. In 1990, Tim Berners-Lee invented the World Wide Web, HTML (hypertext markup language), HTTP (HyperText Transfer Protocol) and URLs (Universal Resource Locators. Along with his colleagues at CERN (an international scientific organization based in Geneva, Switzerland), Tim Berners-Lee was the primary author of HTML (hypertext markup language).

Evolution of the Internet

Although the Internet was developed much earlier, it only became popular in households in the 1990s. The emergence of the Internet can be tracked by how many businesses and homes started changing the way they worked and started connecting their laptops and other devices to the Internet. However, the concept of hypertext transfer protocol (HTTP) as we know it today, was created only during this time. This meant that people could access the same web pages on their devices now and share information.

There has been a dramatic growth in the number of internet users since its inception. As a result, the number of computer networks that are connected has grown exponentially too. It started with only connecting less than ten computers initially. Today, 440 million computers can be connected directly, making life easier for people across the globe. Sharing information and knowledge has become extremely easy for those that have access to the Internet. The country with the highest number of internet users is China, with 1.4 billion users, followed by India with 1.3 billion and the United States of America with a little over 0.3 billion users.

Standards and Administration:

Standards are necessary in networking to ensure interconnectivity and interoperability between various networking hardware and software components. Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.

Concept of Standard

Standards provide guidelines to product manufacturers and vendors to ensure national and international interconnectivity.

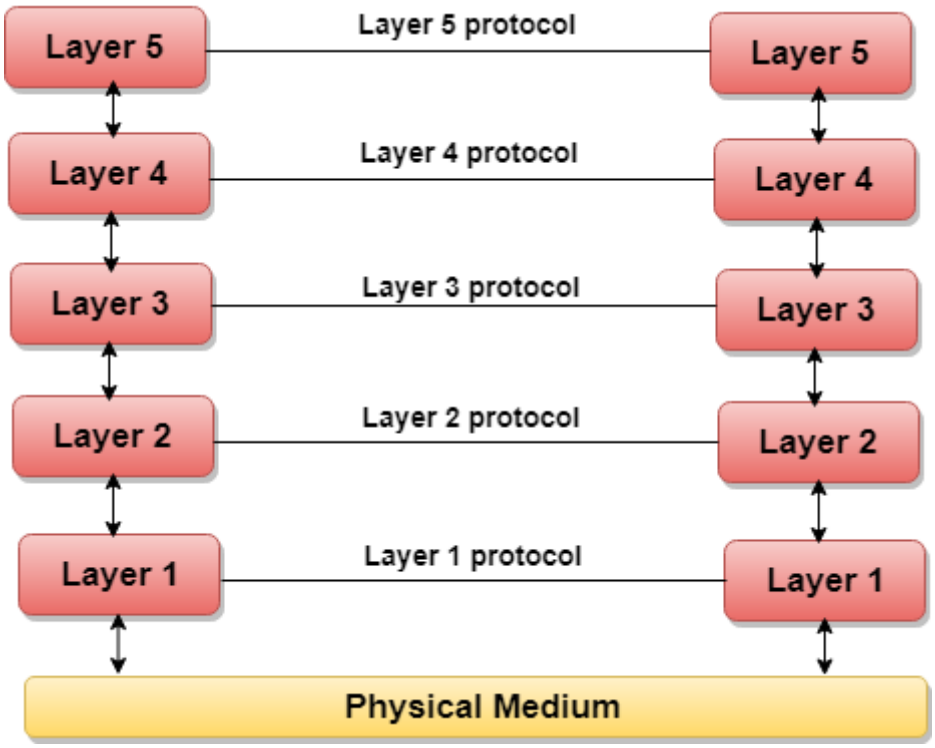
Data communications standards are classified into two categories:

1. De facto Standard o These are the standards that have been traditionally used and mean by fact or by convention
   These standards are not approved by any organized body but are adopted by widespread use.
2. De jure standard
   It means by law or by regulation.
   These standards are legislated and approved by an body that is officially recognized.
   Standard Organizations in field of Networking
   Standards are created by standards creation committees, forums, and government regulatory agencies.
   Examples of Standard Creation Committees :
   1. International Organization for Standardization(ISO)
   2. International Telecommunications Union – Telecommunications Standard (ITU-T)
   3. American National Standards Institute (ANSI)
   4. Institute of Electrical & Electronics Engineers (IEEE)
   5. Electronic Industries Associates (EIA) o
   Examples of Forums
   1. ATM Forum
   2. MPLS Forum
   3. Frame Relay Forum
   Examples of Regulatory Agencies:
   1. Federal Communications Committee (FCC)

Network Models

A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task.

Layered Architecture



- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.
- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a

higher layer and hiding the details from the layers of how the services are implemented.

- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.
- n case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Requirement of Layered architecture

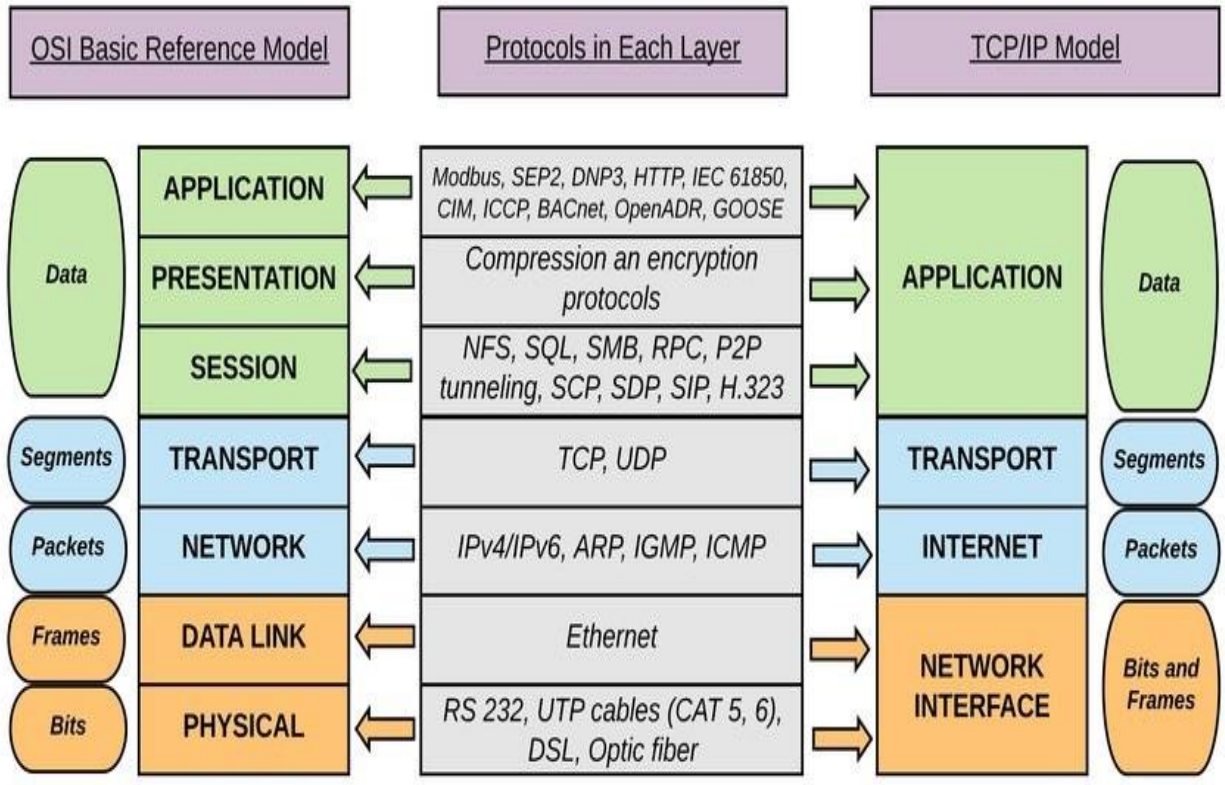
- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

OSI Model:

OSI stands for Open Systems Interconnection. It was developed by ISO – 'International Organization for Standardization', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. Each layer has a specific function and is responsible for specific aspects of communication.

The layers are:

- **Physical:** This layer deals with the physical components of the network, such as cables and network devices.
- **Data Link:** This layer manages the transfer of data between devices on the same network segment.
- **Network:** This layer routes data from one network to another.
- **Transport:** This layer ensures reliable delivery of data between endpoints.
- **Session:** This layer establishes and manages sessions between applications.
- **Presentation:** This layer formats and encrypts data for the application layer.
- **Application:** This layer provides the interface between the network and the end-user applications.



TCP/IP

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.

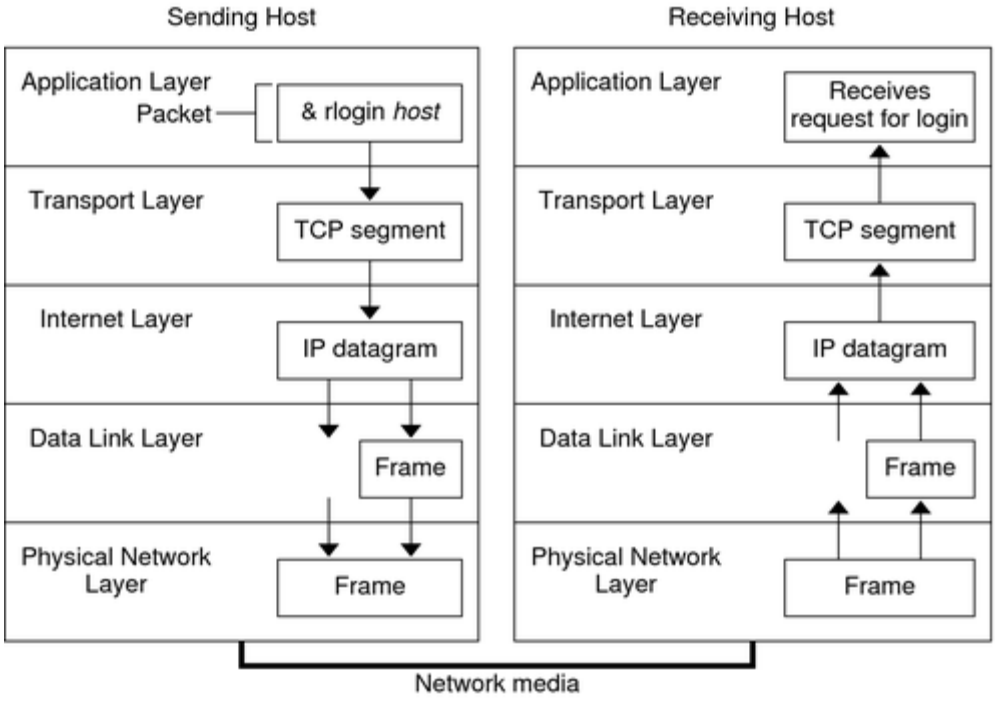
Work of TCP/IP

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

IP Protocol

The IP protocol and its associated routing protocols are possibly the most significant of the entire TCP/IP suite. IP is responsible for the following:

- **IP addressing** – The IP addressing conventions are part of the IP protocol. Designing an IPv4 Addressing Scheme introduces IPv4 addressing and IPv6 Addressing Overview introduces IPv6 addressing.
- **Host-to-host communications** – IP determines the path a packet must take, based on the receiving system's IP address.
- **Packet formatting** – IP assembles packets into units that are known as **datagrams**. Datagrams are fully described in Internet Layer: Where Packets Are Prepared for Delivery.
- **Fragmentation** – If a packet is too large for transmission over the network media, IP on the sending system breaks the packet into smaller fragments. IP on the receiving system then reconstructs the fragments into the original packet.



TCP Protocol

TCP enables applications to communicate with each other as though they were connected by a physical circuit. TCP sends data in a form that appears to be transmitted in a character-by-character fashion, rather than as discrete packets.

This transmission consists of the following:

- Starting point, which opens the connection
- Entire transmission in byte order
- Ending point, which closes the connection.

TCP attaches a header onto the transmitted data. This header contains many parameters that help processes on the sending system connect to peer processes on the receiving system.

TCP confirms that a packet has reached its destination by establishing an end-to-end connection between sending and receiving hosts. TCP is therefore considered a "reliable, connection-oriented" protocol.

Difference between the TCP and IP

The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP.

1. **Link Layer**- The Link Layer deals with transmitting data over physical connections.
2. **Internet Layer -** The Internet Layer routes data packets between networks.
3. **Transport Layer -** The Transport Layer ensures reliable transmission of data.
4. **Application Layer** - The Application Layer provides interfaces for various applications to communicate using the underlying transport protocols.

Advantages of TCP/IP Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is widely used for communication on the internet and other computer networks.

Some of the advantages of the TCP/IP model include the following:

- **Wide Adoption:** TCP/IP is the foundation of the internet and is widely used in a variety of networks and communication systems.
- **Simplicity:** The TCP/IP model is relatively simple compared to other network models, making it easier to understand and implement.
- **Scalability:** TCP/IP is designed to be scalable and can accommodate growth and changes in network size and complexity.
- **Interoperability:** TCP/IP is designed to be flexible and interoperable, allowing different networks and systems to communicate with each other.
- **Robustness:** TCP/IP is designed to be robust and reliable, ensuring the delivery of data even in the presence of network errors and failures.

- **Flexibility:** The TCP/IP model is flexible and allows for the integration of new technologies and applications into existing networks.

Disadvantages of TCP/IP Model

The TCP/IP model has several disadvantages:

- **Complexity:** The TCP/IP model has a complex structure with multiple layers, protocols, and standards, making it difficult for novice users to understand and implement.
- **Security:** Although it provides some security measures, it is still vulnerable to attacks such as hacking, malware, and denial-of-service (DoS) attacks.
- **Scalability:** As the number of internet-connected devices increases, the TCP/IP model may become less scalable and unable to accommodate the growing demands placed on it.
- **Performance:** The TCP/IP model's performance can be affected by network congestion, outdated protocols, and slow transmission speeds.
- **Flexibility:** The TCP/IP model is not very flexible, and changing or updating protocols can cause compatibility issues with existing systems.

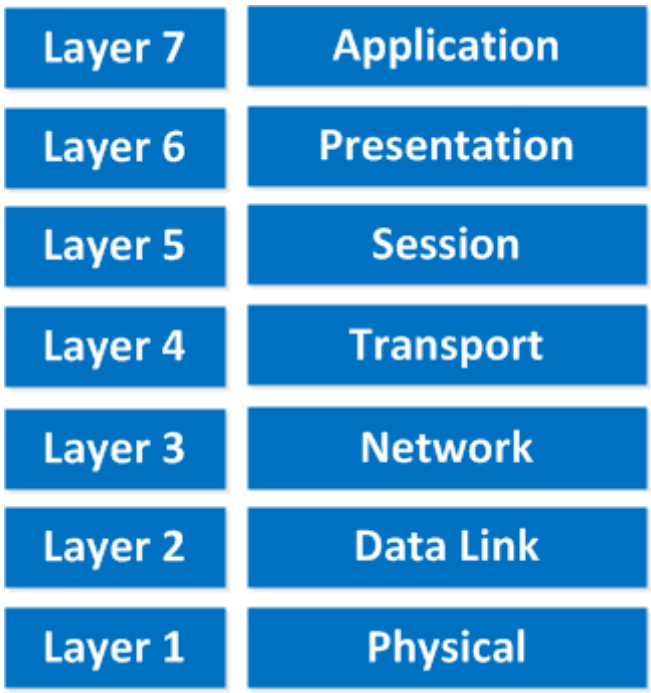
Difference between TCP/IP and OSI Model

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.
TCP/IP model network layer only provides	Connectionless and connection-oriented

TCP/IP	OSI
connectionless (IP) services. The transport layer (TCP) provides connections.	services are provided by the network layer in the OSI model.

OSI MODEL

OSI stands for Open Systems Interconnection. It was developed by ISO – 'International Organization for Standardization', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.



Physical layer-Layer 1

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.

- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

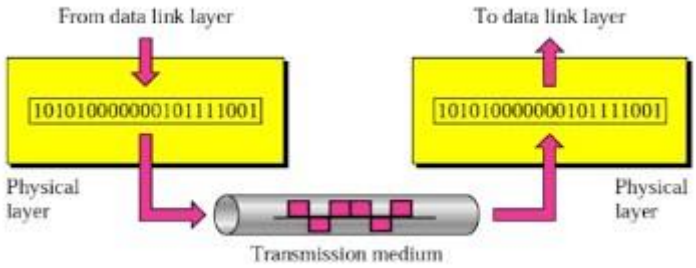
Data Link Layer (DLL) – Layer 2

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The Data Link Layer is divided into two sublayers:

Logical Link Control

Media Access Control



Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Network Layer – Layer 3

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

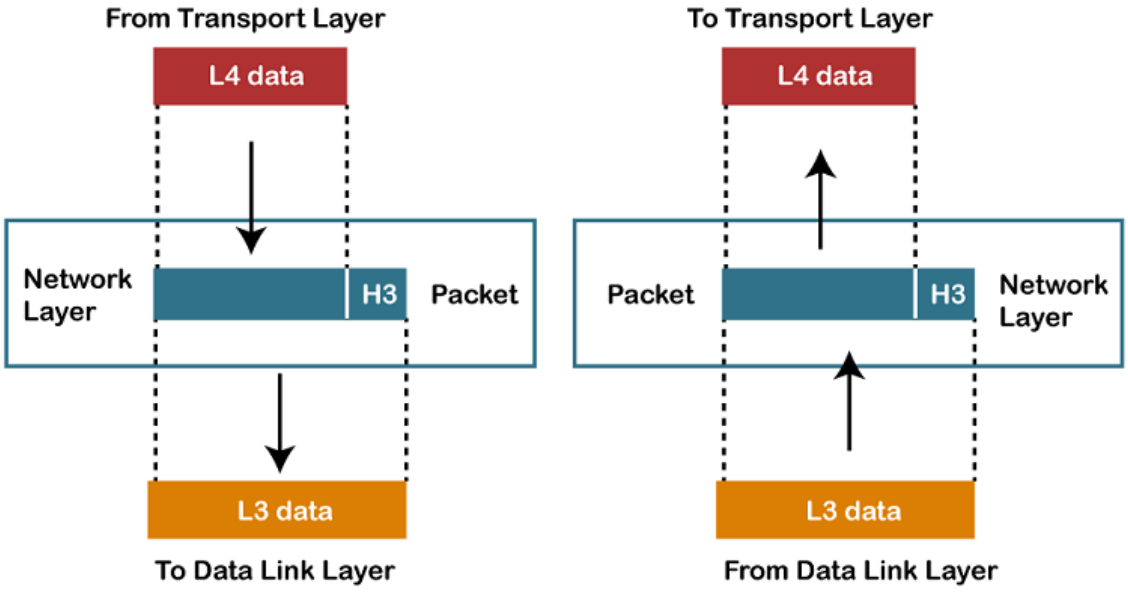
Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Transport Layer – Layer 4

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.



Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address.

Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

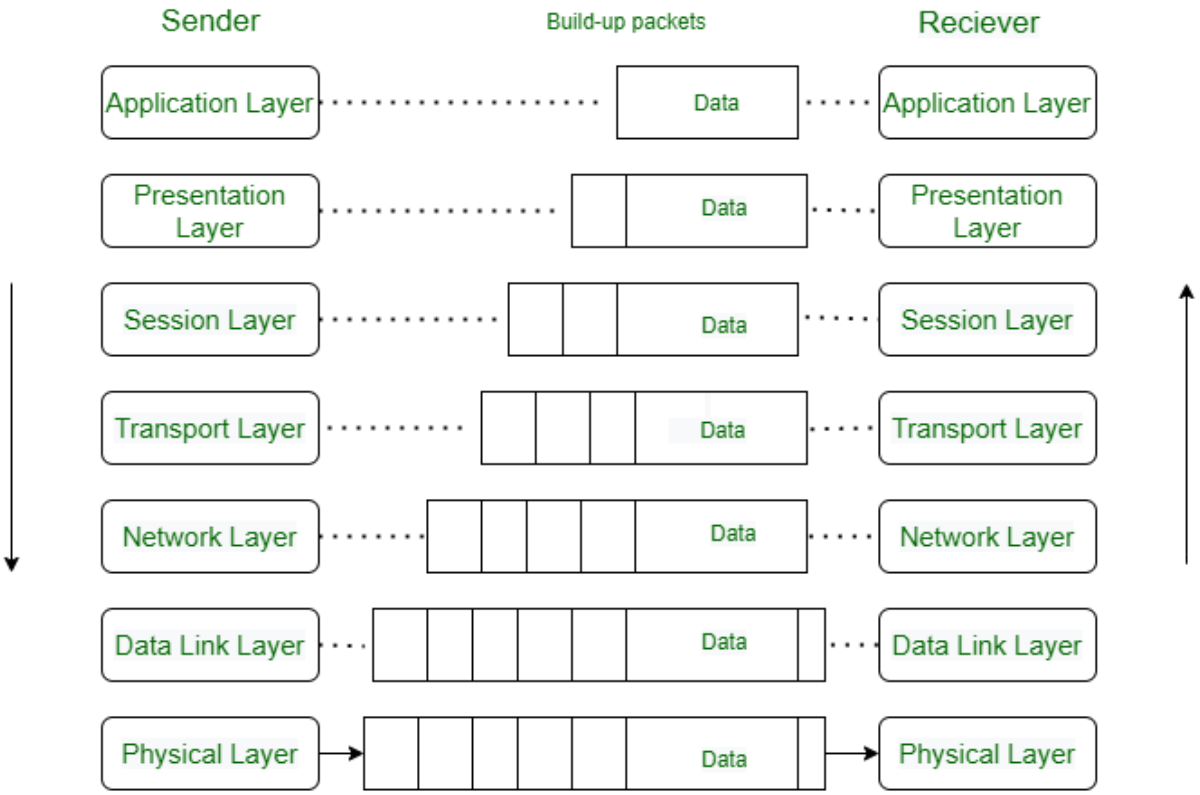
1. Connection-Oriented Service
2. Connectionless Service

1. Connection-Oriented Service: It is a three-phase process that includes

- Connection Establishment
- Data Transfer
- Termination/disconnection

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

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



Session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Functions of the Session Layer

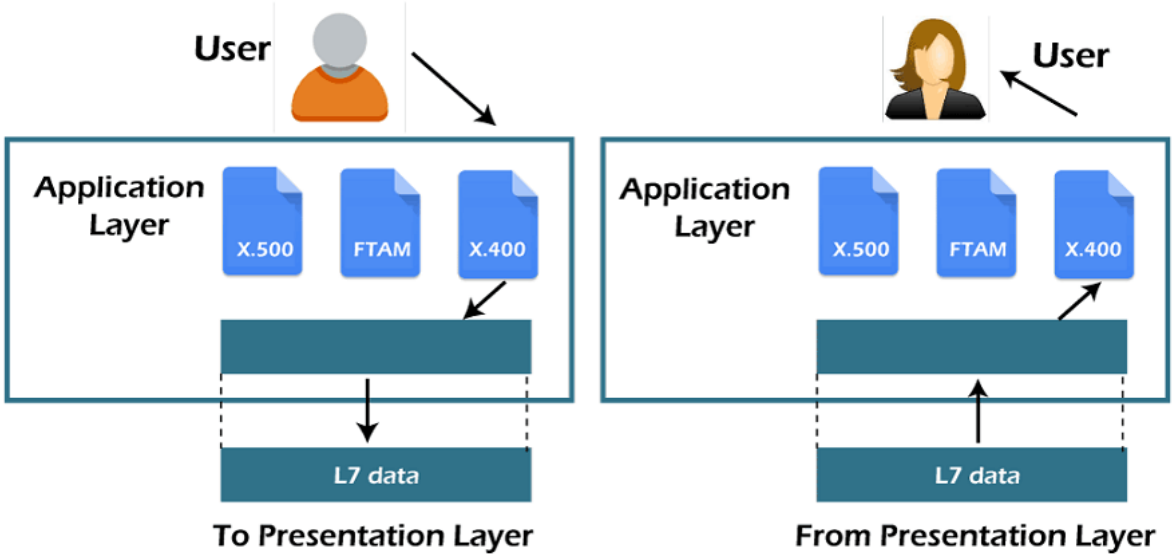
- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.

Synchronization: **This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the Presentation Layer – Layer 6**
The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.
- data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Application Layer – Layer 7
At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. The application Layer is also called Desktop Layer.



Functions of the Application Layer

The main functions of application layer are given below.

- Network Virtual Terminal: It allows a user to log on to a remote host.

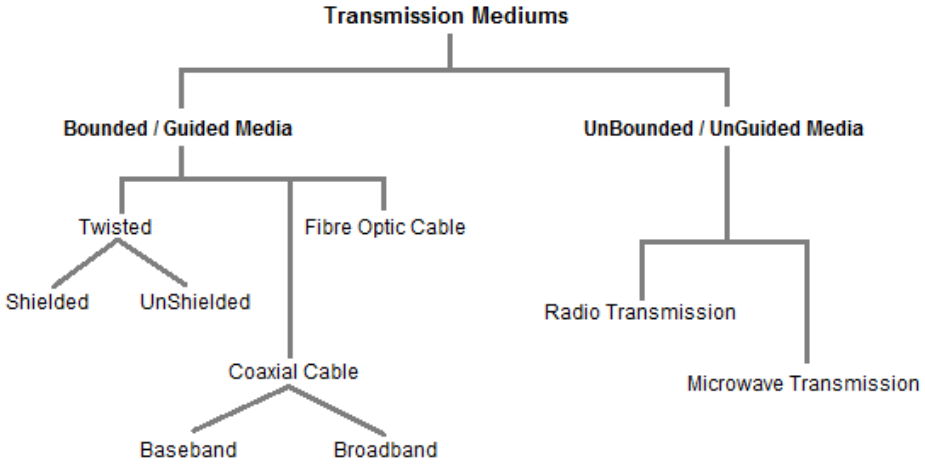
- FTAM- File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.
- Mail Services : Provide email service.
- Directory Services : This application provides distributed database sources and access for global information about various objects and services.

Transmission Mediums in Computer Networks

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to travel between one point to another(from source to receiver).

Electromagnetic energy (includes electrical and magnetic fields) includes power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.



Factors to be considered while choosing Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

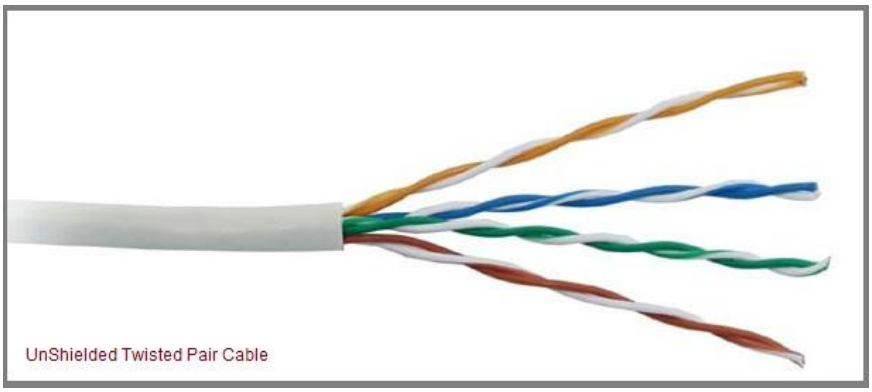
Twisted Pair is of two types :

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use**RJ-45** connector.



Advantages :

- Installation is easy
- Flexible

- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

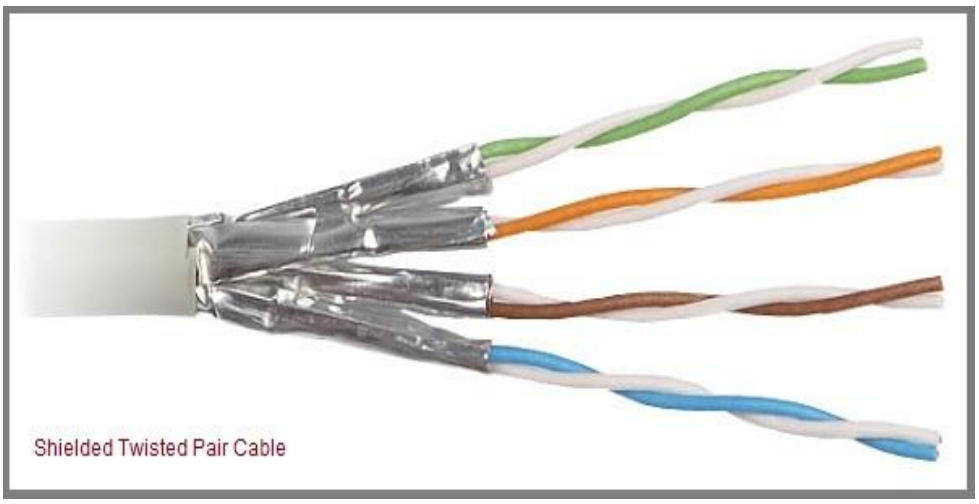
Disadvantages :

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.



Advantages :

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission

- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages :

- Difficult to manufacture
- Heavy

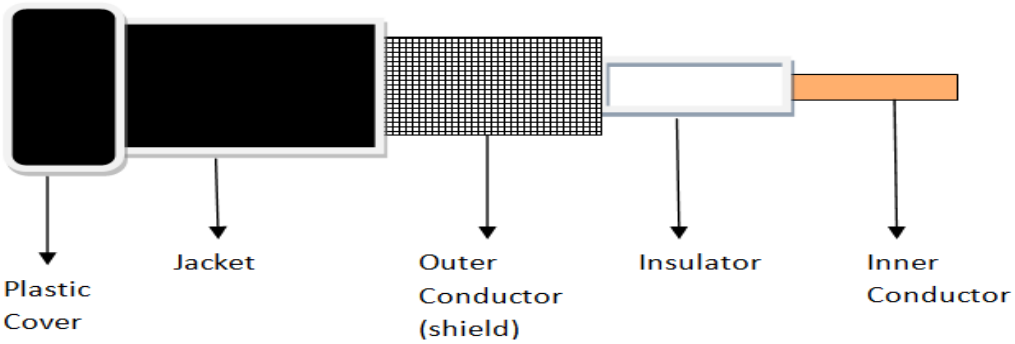
Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



There are two types of Coaxial cables :

BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages :

- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity
- Data transmission without distortion.
- The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages :

- Single cable failure can fail the entire network.
- Difficult to install and expensive when compared with twisted pair.
- If the shield is imperfect, it can lead to grounded loop.

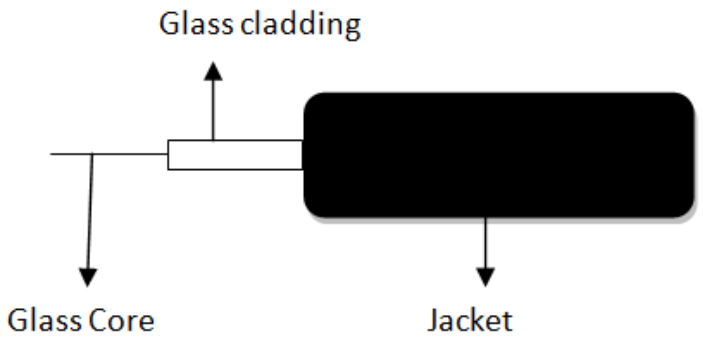
Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.

Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**



Advantages :

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages :

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

UnBounded/UnGuided Transmission Media

Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them. Types of unguided/ unbounded media are discussed below :

- Radio Transmission
- MicroWave Transmission

Radio Transmission

Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications.

Types of Propogation

Radio Transmission utilizes different types of propogation :

- **Troposphere :** The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet planes, wind is found here.
- **Ionosphere :** The layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

Microwave Transmission

It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

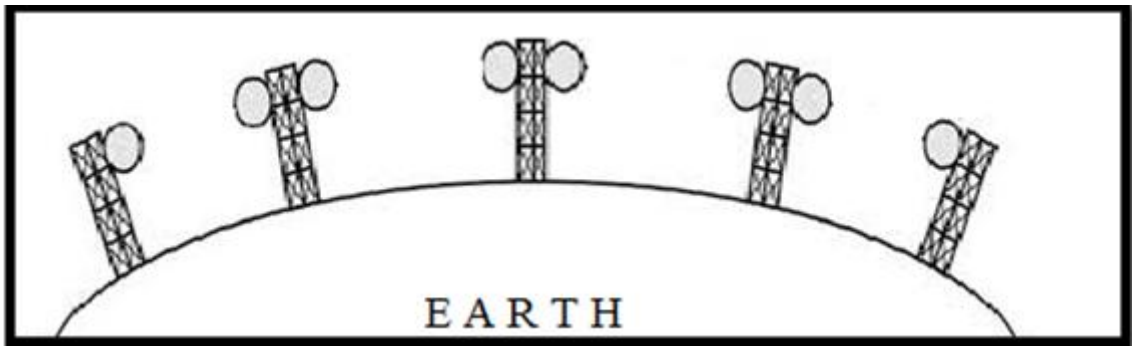
- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly

Terrestrial Microwave

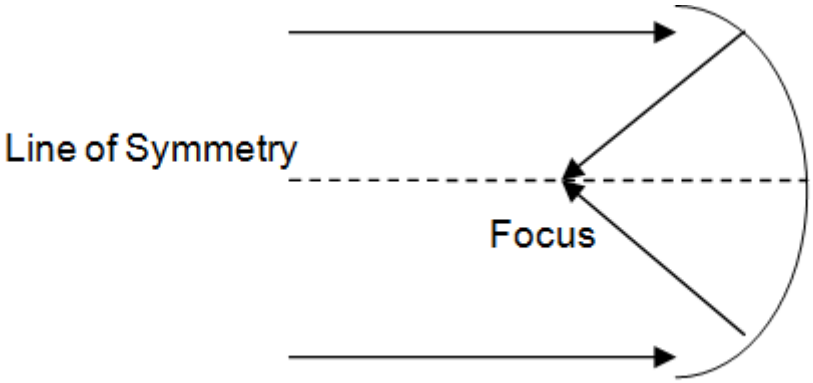
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world



There are two types of antennas used for terrestrial microwave communication :

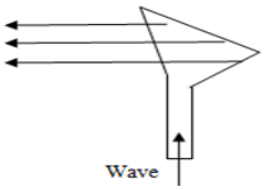
1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.



2. Horn Antenna

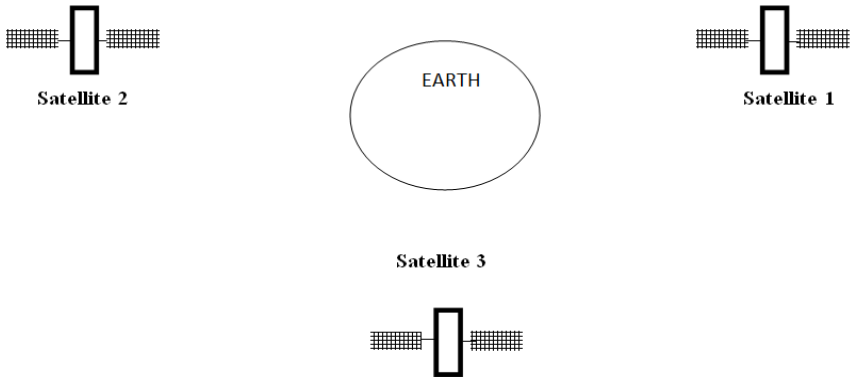
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.



Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 3600KM above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.



Features of Satellite Microwave :

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave :

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave :

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

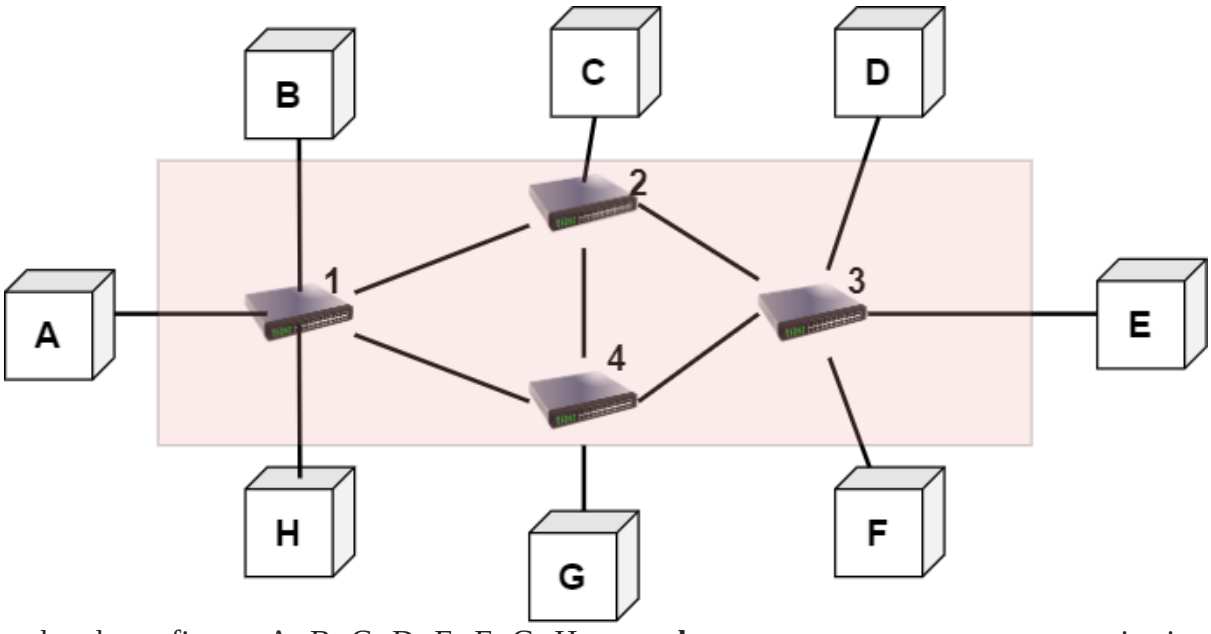
Switching

Switching is the process of transferring data packets from one device to another in a network, or from one network to another, using specific devices called **switches**. Switching takes place at the Data Link layer of the OSI Model. This means that after the generation of data packets in the Physical Layer, switching is the immediate next process in data communication.

Switched Networks

A switched network basically consists of a series of **interlinked nodes.** These interlinked nodes are known as **switches.**

- Thus in a switched network, connectivity is usually provided by making the **use of switches**.
- Switches are those devices that are capable of creating temporary connections between two or more devices that are linked to them.
- In this network, some switches are connected to the end system(like computer systems or telephones) while other switches are used for routing.
- The network device switch is mainly a layer-2 device of the OSI model.
- Packet forwarding is done by the switch on the basis of the MAC address.
- Thus the Switch mainly transfers the data only to the device that has been addressed (means having proper mac address). Because verification of destination address is done by the switch in order to route the packet appropriately.



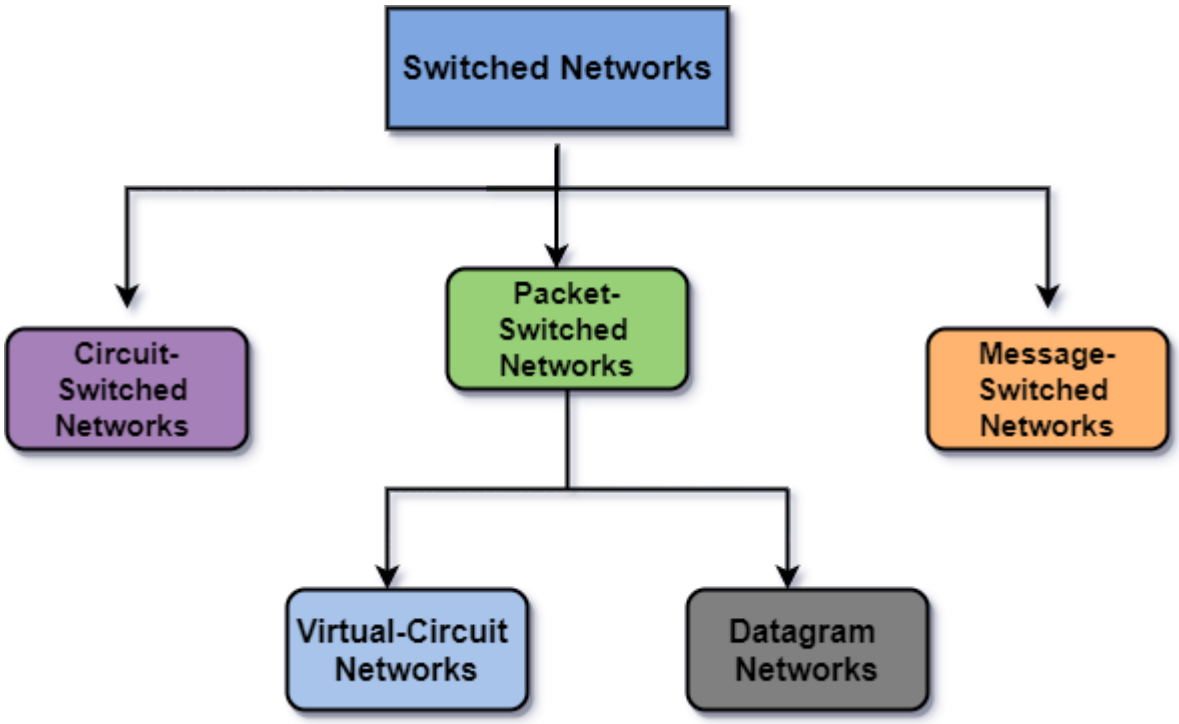
n the above figure; A, B, C, D, E, F, G, H are **end systems** or we can say communicating devices. And there are 4 switches labeled as 1,2,3,4. Also, you can see that each switch is connected to multiple links.

The concept of switching is needed for the effective utilization of the bandwidth. Also whenever two or more devices communicate with each other then there are many chances for

the occurrence of the collision of data packets in the network; switching is the best solution for this problem.

Methods of Switching

- Circuit Switching
- Packet Switching
- Message Switching



Circuit Switching:

In circuit switching network resources (bandwidth) are divided into pieces and bit delay is constant during a connection.

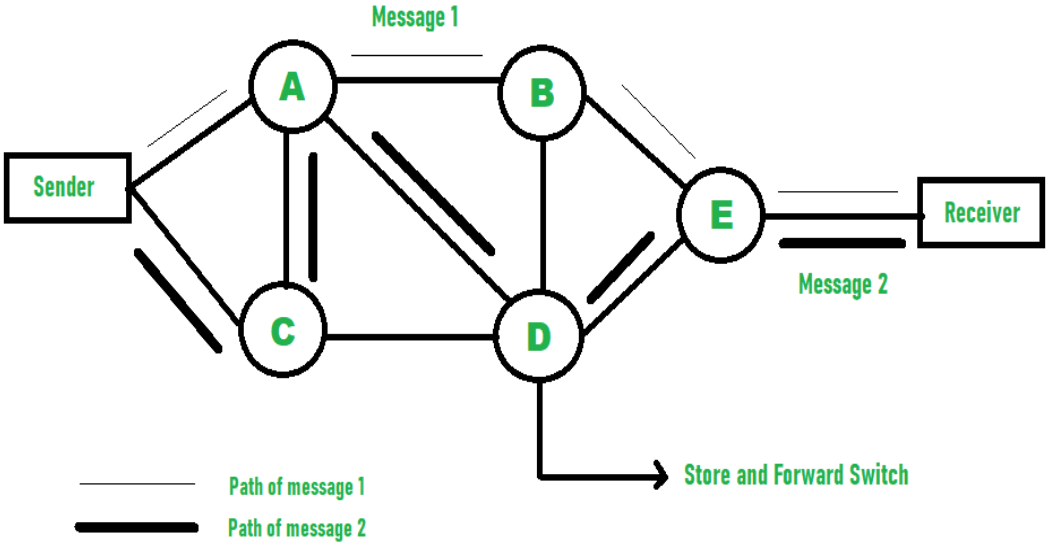
Telephone system network is one of the example of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.

- **Frequency Division Multiplexing :** *Divides into multiple bands*
  Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium.It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands,where each sub-band carry different signal. Practical use in radio spectrum & optical fibre to share multiple independent signals.

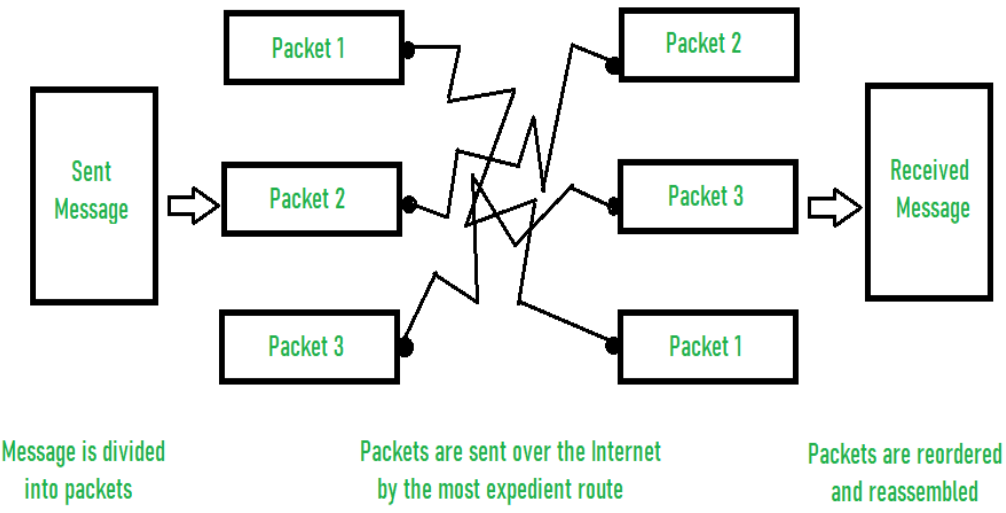
- **Time Division Multiplexing :** *Divides into frames*
  Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at

each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user.
Time division multiplexing (TDM) is also known as a digital circuit switched.

- MessageSwitching **:**
  In this technique, the entire message is transmitted without any break from one node to another. It firstly stores and then forwards information that requires more time. Due to this, the access time is increased. No direct link is present between the sender and the receiver.
- Example of message switching –



- **2.** Packet Switching **:**
  In packet switching, information is transferred in the form of data packets between the sender and the receiver. These packets are forwarded one by one from the sender to the receiver. Each packet is associated with a Header. Then, these packets then reassembled into the original message. This improves the performance as the time require to access the data packet is reduced. Due to this, the overall performance of the network is improved.
- Example of packet switching –



- **Difference between Message and Packet Switching :**

Message Switching	Packet Switching
A complete message is passed across a network.	Message is broken into smaller units known as Packets.
In this, computer language used is ASCII, baudot, morse.	In packet switching, binary type is used.
In message switching there is no limit on block size.	Packet switching places a tight upper limit on block size.
Message exist only in one location in the network.	Parts i.e. packets of the message exist in many places in the network.
Example: Hop-by-hop Telex forwarding and UUCP(UNIX-to-UNIX Copy Protocol)	Example: Frame Relay, IP, and X. 25
Physical links are allocated dynamically.	Virtual links are made simultaneously.
Access time is reduced due to increase in performance as packets are stored in disk.	Packets are stored in main memory.