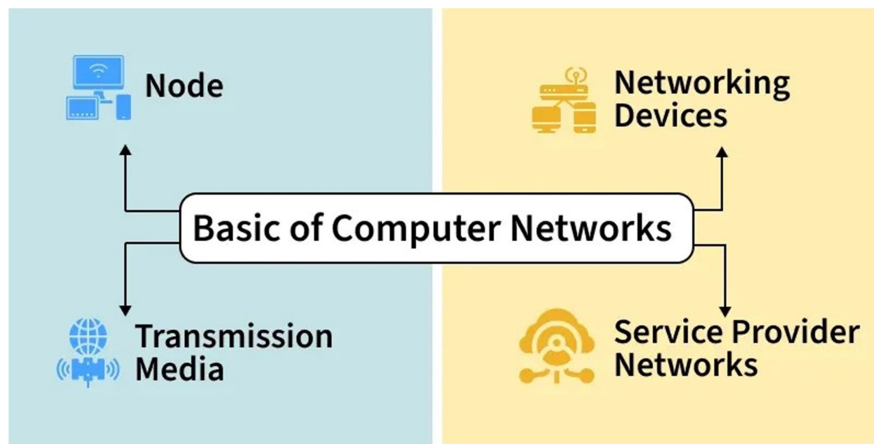


## Unit I- Network Basics

### Computer Network

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.

Computer networks enable the usage and sharing of any number of applications and services, including emails, video, audio and plenty of other types of data, over the internet. An example of a network is the [Internet](#), which connects millions of people all over the world.



- **Network:** A group of connected computers and devices that can communicate and share data.
- **Node:** Any device that can send, receive, or forward data in a network. This includes laptops, mobiles, printers, earbuds, servers, etc.
- **Networking Devices:** Devices that manage and support networking functions. This includes routers, switches, hubs, and access points.
- **Transmission Media:** The physical or wireless medium through which data travels between devices.
- **Wired media:** Ethernet cables, optical fibre.
- **Wireless media:** Wi-Fi, Bluetooth, infrared
- **Service Provider Networks:** Networks offered by external providers that allow users or organisations to lease network access and capabilities. This includes internet providers, mobile carriers, etc.

# Types

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

- LAN(Local Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

## LAN(Local Area Network)

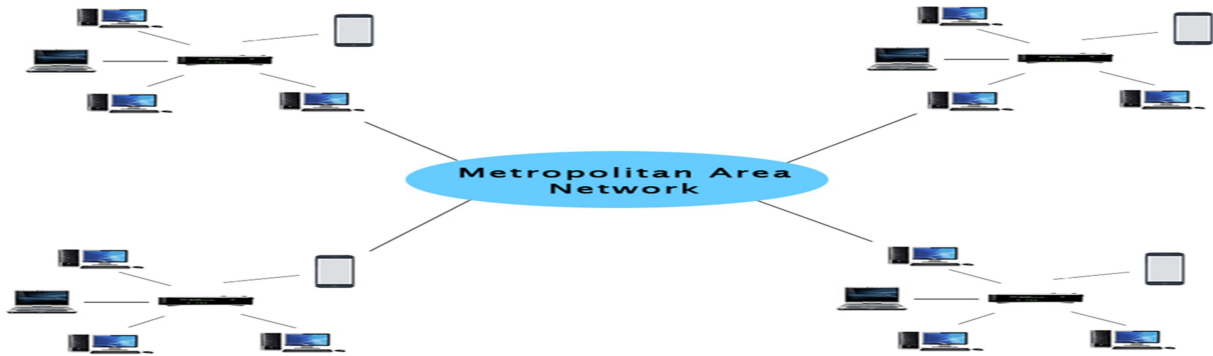
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware 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.

- It has a higher range than Local Area Network(LAN).



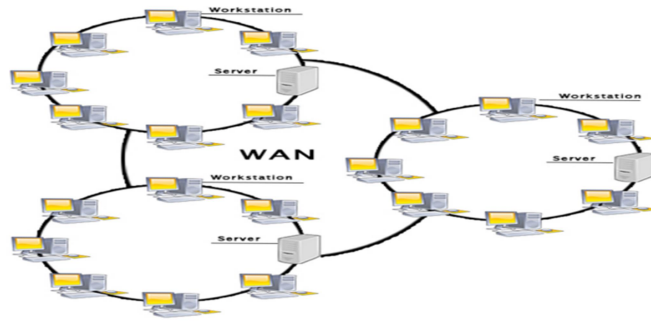
### **Uses Of Metropolitan Area Network:**

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

---

### **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.
- 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.
- **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:

- **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. **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **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.

### Disadvantages of Wide Area Network:

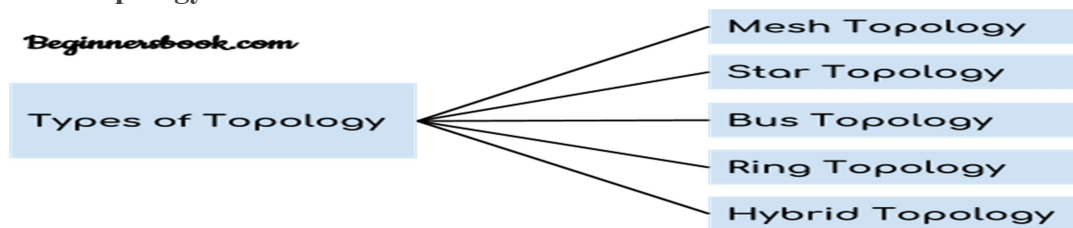
The following are the disadvantages of the Wide Area Network:

- **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.

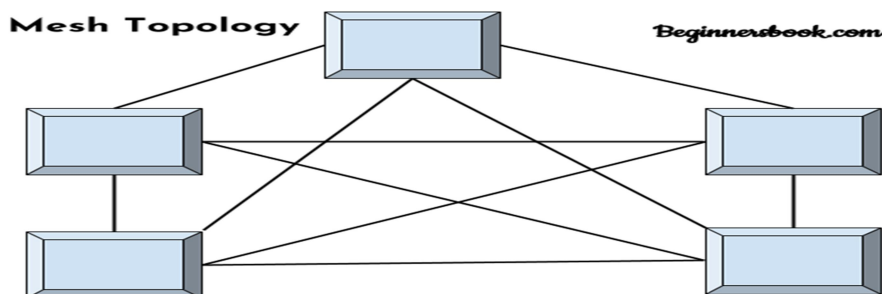
## Computer Network Topology

Geometric representation of how the computers are connected to each other is known as topology. There are five types of topology – Mesh, Star, Bus, Ring and Hybrid.

### Types of Topology



### Mesh Topology



In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Lets say we have n devices in the network then each device must be connected with (n-1) devices of the network.

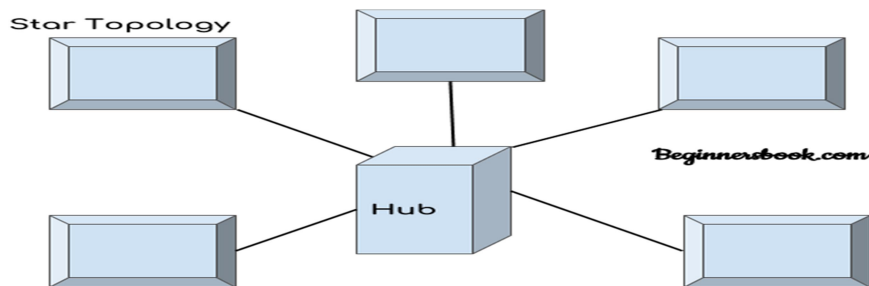
### Advantages of Mesh topology

1. No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
2. Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
3. Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
4. Fault detection is easy.

### Disadvantages of Mesh topology

1. Amount of wires required to connect each system is tedious and headache.
2. Since each device needs to be connected with other devices, number of I/O ports required must be huge.
3. Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

### Star Topology



In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

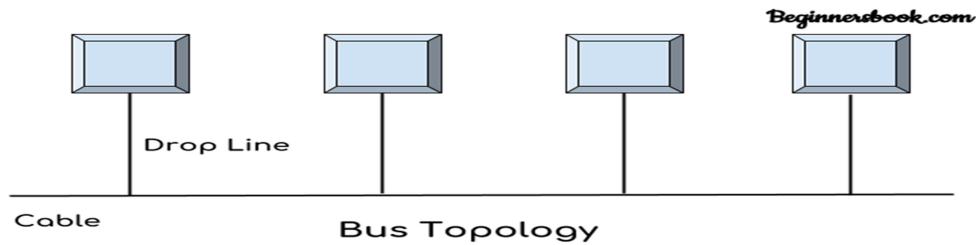
### Advantages of Star topology

1. Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
2. Easier to install
3. Less amount of cables required because each device needs to be connected with the hub only.
4. Robust, if one link fails, other links will work just fine.
5. Easy fault detection because the link can be easily identified.

## Disadvantages of Star topology

1. If hub goes down everything goes down, none of the devices can work without hub.
2. Hub requires more resources and regular maintenance because it is the central system of star topology.

## Bus Topology



In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

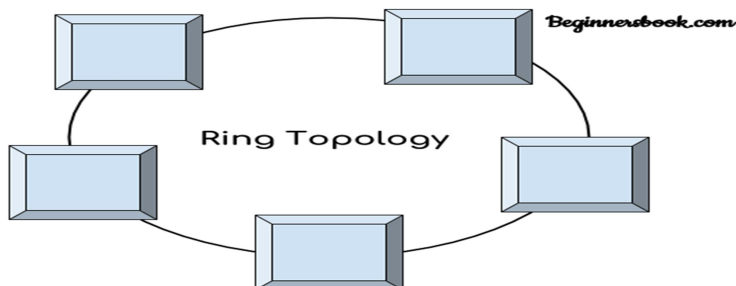
## Advantages of bus topology

1. Easy installation, each cable needs to be connected with backbone cable.
2. Less cables required than Mesh and star topology

## Disadvantages of bus topology

1. Difficultly in fault detection.
2. Not scalable as there is a limit of how many nodes you can connect with backbone cable

## Ring Topology



In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received

data is intended for other device then repeater forwards this data until the intended device receives it.

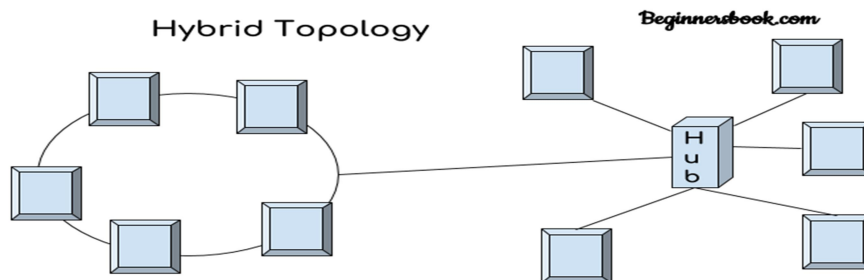
### Advantages of Ring Topology

1. Easy to install.
2. Managing is easier as to add or remove a device from the topology only two links are required to be changed.

### Disadvantages of Ring Topology

1. A link failure can fail the entire network as the signal will not travel forward due to failure.
2. Data traffic issues, since all the data is circulating in a ring.

### Hybrid topology



A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

### Advantages of Hybrid topology

1. We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
2. Scalable as we can further connect other computer networks with the existing networks with different topologies.

### Disadvantages of Hybrid topology

1. Fault detection is difficult.
2. Installation is difficult.
3. Design is complex so maintenance is high thus expensive.

## TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internet working, 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.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

### Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- 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.

### Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- 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:

- **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.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.

### **ARP Protocol**

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **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**

- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- 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.
- An ICMP protocol mainly uses two terms:
  - **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.

## 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.

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

---

## Application Layer

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

- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- 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:

- **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.
- **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.
- **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.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely.
- **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.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

**Synchronous data transmission** - is a data transfer method in which a continuous stream of data signals is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another. The data is sent in blocks (called frames or packets) spaced by fixed time intervals.

Synchronous transmission modes are used when large amounts of data must be transferred very quickly from one location to the other. The speed of the synchronous connection is attained by transferring data in large blocks instead of individual characters.



The following is a list of characteristics specific to synchronous communication:

- There are no gaps between characters being transmitted.
- Timing is supplied by modems or other devices at each end of the connection.

### **ASYNCHRONOUS TRANSMISSION**

In contrast, asynchronous transmission works in spurts and must insert a start bit before each data character and a stop bit at its termination to inform the receiver where it begins and ends.

The term *asynchronous* is used to describe the process where transmitted data is encoded with start and stop bits, specifying the beginning and end of each character.

An example of synchronous transmission is shown in the following figure.

**Figure 2. Asynchronous transmission**



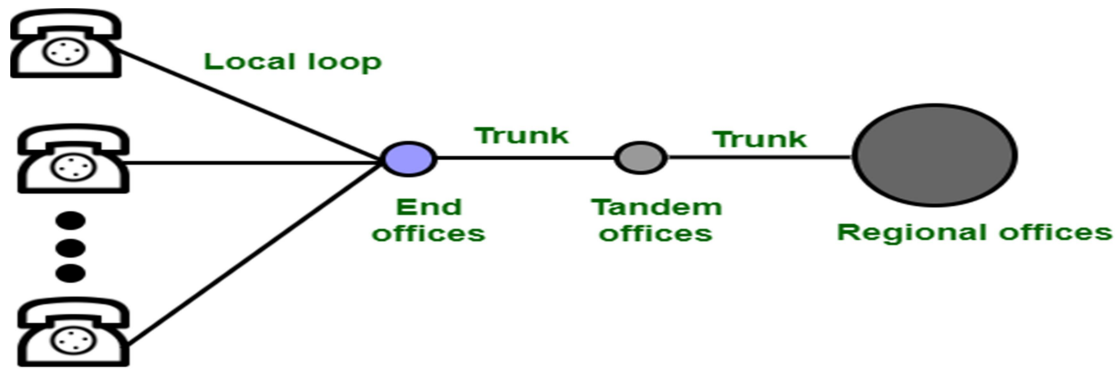
### **Introduction to Telephone Network**

Telephone Network is used to provide voice communication. Telephone Network uses Circuit Switching. Originally, the entire network was referred to as a plain old telephone system (POTS) which uses analog signals. With the advancement of technology, i.e. in the computer era, there comes a feature to carry data in addition to voice. Today's network is both analogous and digital.

**Major Components of Telephone Network:** There are three major components of the telephone network:

1. Local loops
2. Trunks
3. Switching Offices

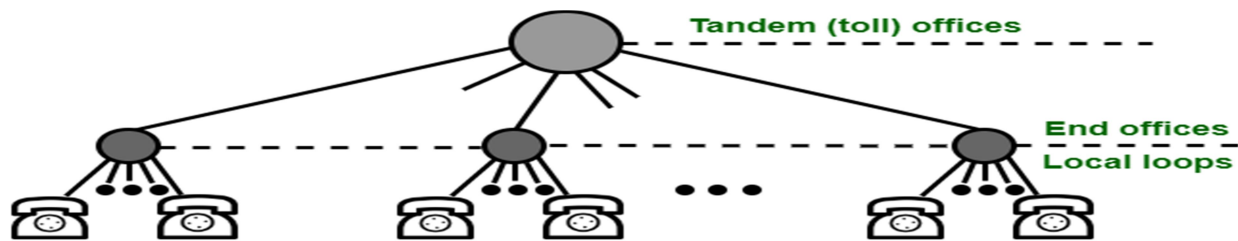
There are various levels of switching offices such as end offices, tandem offices, and regional offices. The entire telephone network is as shown in the following figure:



**Local Loops:** Local Loops are the twisted pair cables that are used to connect a subscriber telephone to the nearest end office or local central office. For voice purposes, its bandwidth is 4000 Hz. It is very interesting to examine the telephone number that is associated with each local loop. The office is defined by the first three digits and the local loop number is defined by the next four digits defines.

**Trunks:** It is a type of transmission medium used to handle the communication between offices. Through multiplexing, trunks can handle hundreds or thousands of connections. Mainly transmission is performed through optical fibers or satellite links.

**Switching Offices:** As there is a permanent physical link between any two subscribers. To avoid this, the telephone company uses switches that are located in switching offices. A switch is able to connect various loops or trunks and allows a connection between different subscribes.



Switching offices

#### Advantages of Telephone Network:

- It is a circuit-switched network.
- There is no transmission delay as any receiver can be selected.
- It is cheap in price because it is a widely spread network.

#### Disadvantages of Telephone Network:

- It requires a large time for connection.
- It has a low transmission speed.

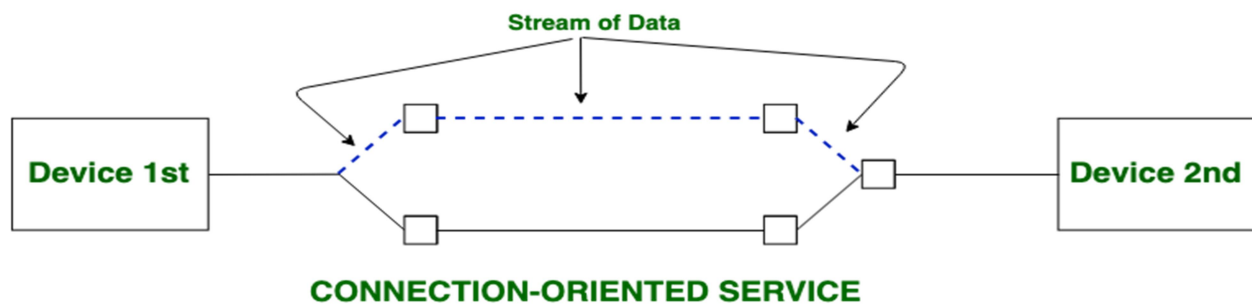
#### Applications of Telephone Network:

- It helps to connect people.
- It is used by business organizations to advertise their products.

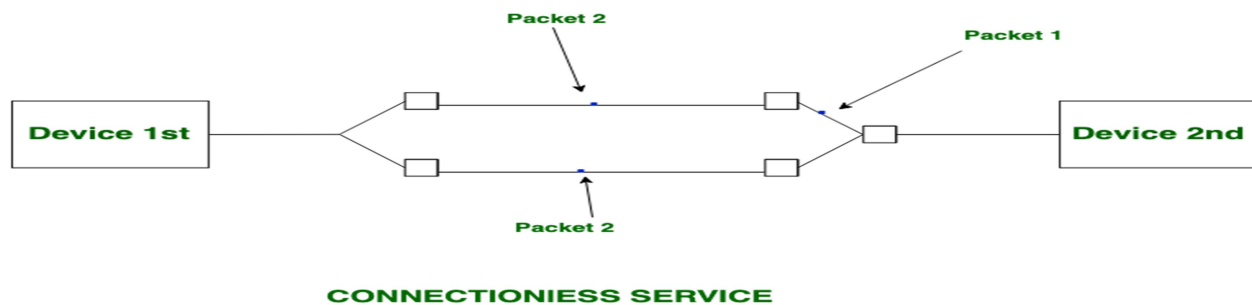
### Connection-oriented service

a connection-oriented service is used to establish an end-to-end connection between the sender and the receiver. Packets are forwarded to the receiver in the same sequence as they were sent by the sender in connection-oriented service.

is related to the telephone system. It includes connection establishment and connection termination. In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver.



**connectionless service-** is used to send data from one end to the other without establishing a connection. As a result, there is no need to establish a connection before delivering data from the transmitter to the receiver. It is not a dependable network service since it does not guarantee the passage of data packets to the recipient, and data packets can arrive at the receiver in any sequence. It does not include any connection establishment and connection termination. In this, Packets do not follow the same path to reach their destination.



### Connection-oriented vs Connectionless service:

Parameter	Connection-oriented	Connectionless
Related System	It is based on the telephone system in its architecture and development.	It is a postal system-based service.

Definition	It is used to establish an end-to-end connection between senders and receivers prior to transferring data across the same or a separate network.	It is used to transport data packets from senders to receivers without establishing a connection.
Virtual Path	It establishes a virtual connection between the sender and the recipient.	It does not establish a virtual link between the sender and the recipient.
Authentication	Before transferring data packets to the recipient, it requires authentication.	Before sending data packets, it does not require authentication.
Data Packets Path	All data packets are received in the same sequence as they were transmitted.	Same sequence of data packets is not guaranteed.
Bandwidth requirement	It takes more bandwidth to send data packets.	The data packets are sent using very low bandwidth.
Data Reliability	It is a more reliable connection service since it assures data packets travel from one end of a connection to the other.	It is not a reliable connection service since it does not ensure the passage of data packets from one end to the other in order to establish a connection.
Congestion	There is no congestion since it establishes an end-to-end link between sender and recipient during data transfer.	Congestion may occur as a result of not establishing an end-to-end connection between the source and receiver for data packet transmission.
Examples	A connection-oriented service is the Transmission Control Protocol (TCP).	Connectionless services include User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP).

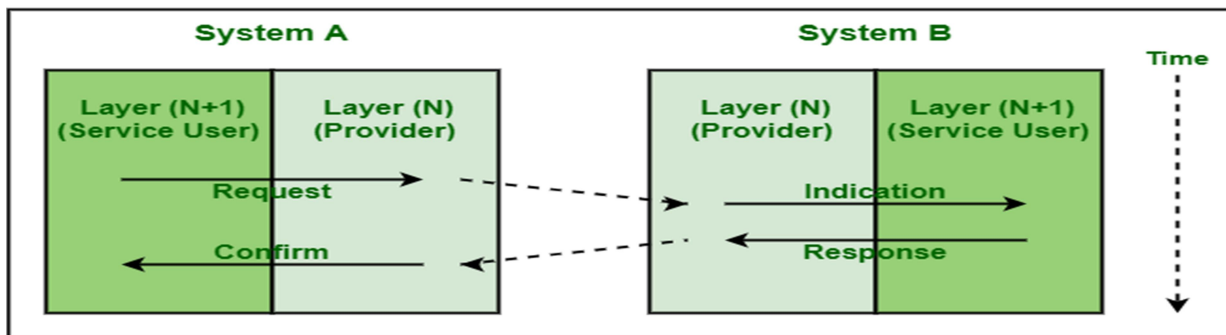
## Service primitives

**Service** generally includes set of various primitives. A primitive simply means Operations.

A Service is specified by set of primitives that are available and given to user or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by peer entity.

Primitive	Meaning
<b>Request</b>	It represent entity that wants or request service to perform some action or do some work (requesting for connection to remote computer).
<b>Indication</b>	It represent entity that is to be informed about event (receiver just have received request of connection).
<b>Response</b>	It represents entity that is responding to event (receiver is simply sending the permission or allowing to connect).
<b>Confirm</b>	It represent entity that acknowledges the response to earlier request that has

come back (sender just acknowledge the permission to get connected to the remote host).



### Primitives for Connection between Peer Protocol Entities

In the above diagram, these four primitives work as following :

- **Request** – This primitive is transferred or sent to Layer N by Layer (N+1) to just request for service.
- **Indication** – This primitive is returned by Layer N to Layer (N+1) to just advise of activation of service that is being requested or of action that is initiated by the service of Layer N.
- **Response** – This primitive is simply provided by Layer (N+1) in reply to indication primitive. It might acknowledge or complete action that is previously invoked by indication primitive.
- **Confirm** – This primitive is returned by the  $N^{\text{th}}$  layer to the requesting  $(N+1)^{\text{st}}$  layer to simply acknowledge or complete action that is previously invoked by request primitive.

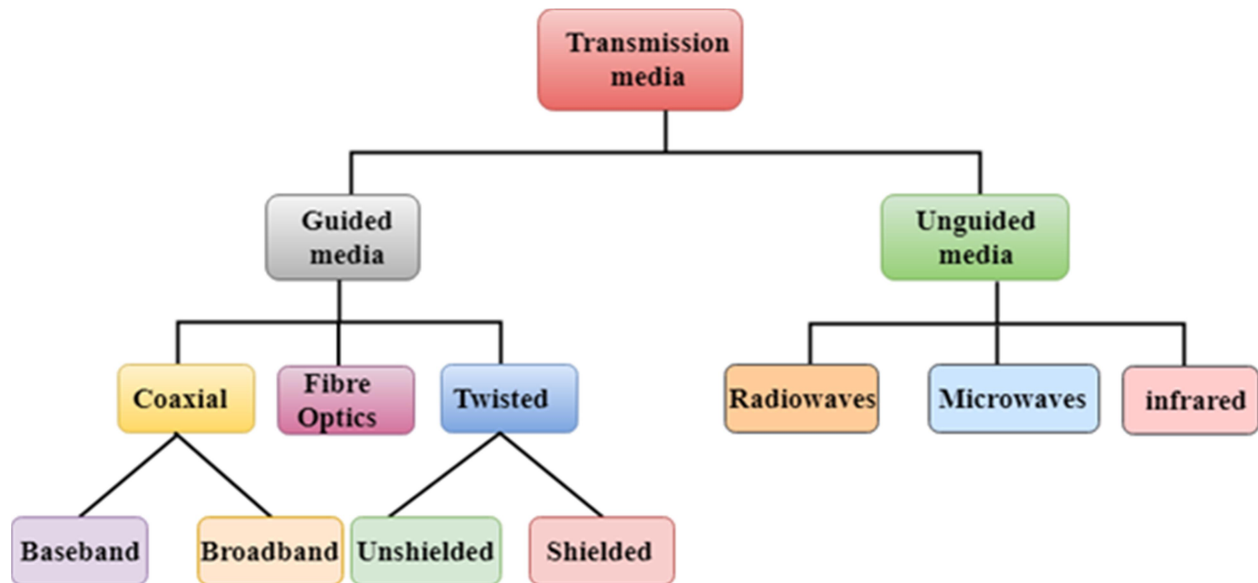
#### Parameters of Service Primitives :

Some of the Service Primitives need parameters. These are given below :

- **Connect. Request** – The initiating entity does this Connect.Request. It just specifies and determines machine that we want to get connected to, type of service that is being desired, and maximum size of packet or message that is used on connection.
- **Connect. Indication** – The receiver gets this Connect.Indication. It just specifies caller's identity service that we want to use like FTP and Telnet, etc., and maximum size of packets that are exchanged.
- **Connect. Response** – It just specifies whether or not it wants to accept or simply reject connection that is being requested.
- **Connect. Confirm** – It just finds out or determines what happened using the entity that is issuing the initial Connect. Request.

## Transmission media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another



## Guided Media

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

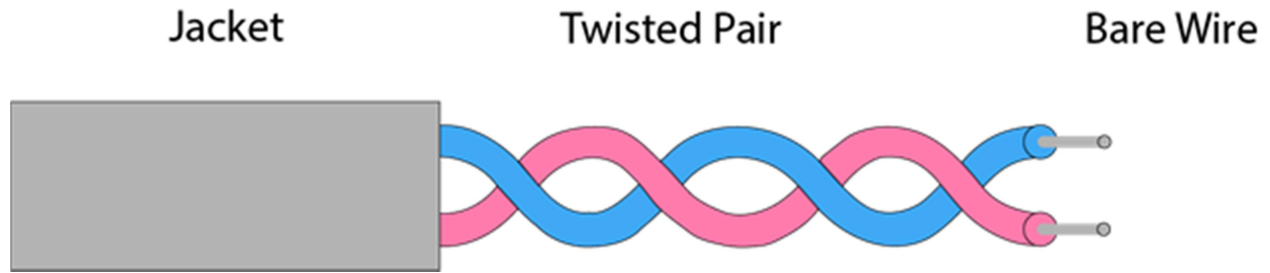
Types Of Guided media:

### Twisted pair:

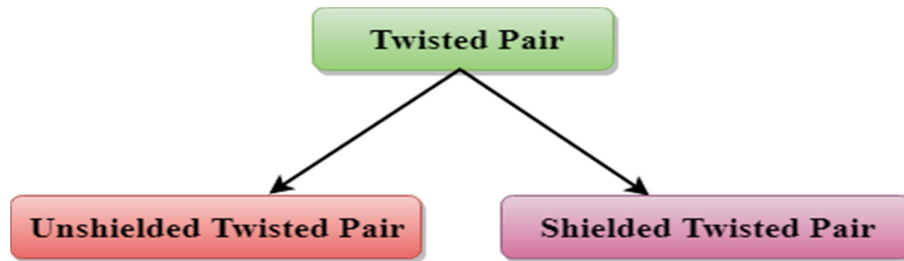
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

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.



### 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:

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

### Advantages Of Unshielded Twisted Pair:

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

### Disadvantage:

- 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:

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

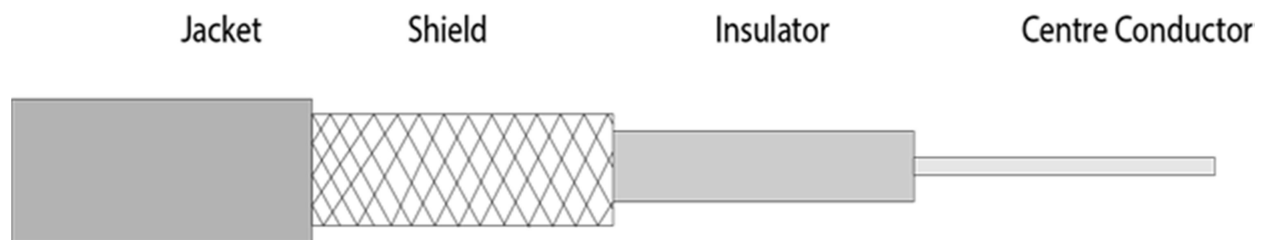
### Disadvantages

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

---

### Coaxial Cable

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



### 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:

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

## Disadvantages Of Coaxial cable:

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

---

## Fibre Optic

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

## Diagrammatic representation of fibre optic cable:



## Basic elements of Fibre optic cable:

- **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.
- **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.

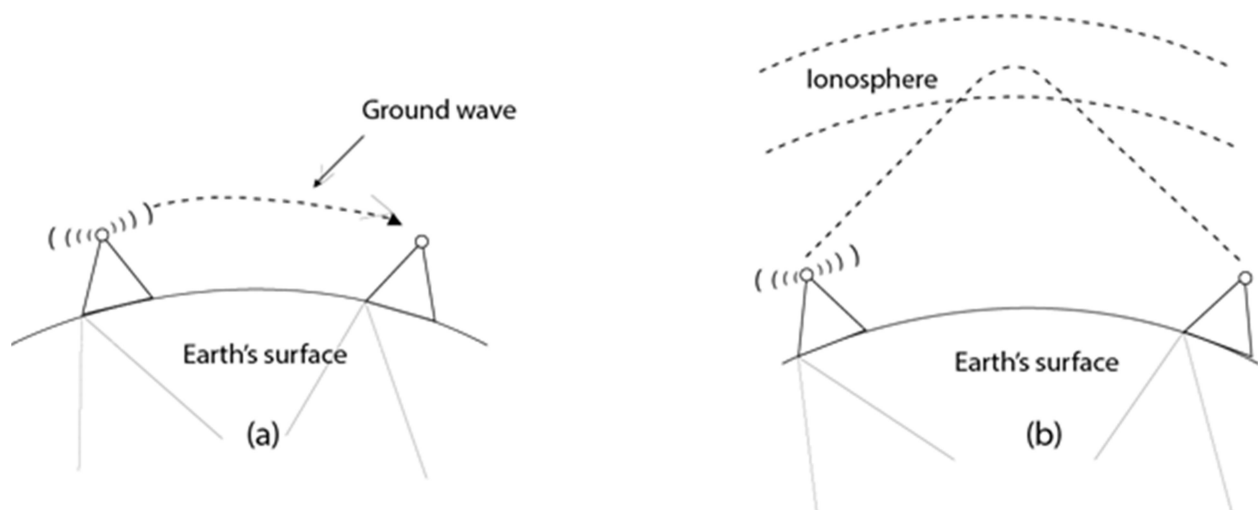
## UnGuided Transmission

- 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 Ghz.
- 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**.



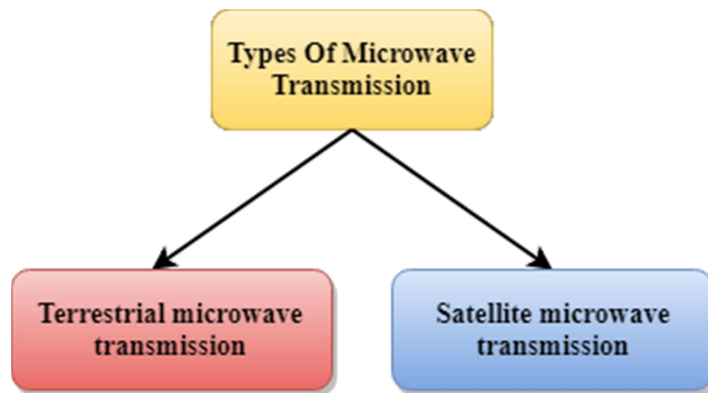
### Applications Of Radio waves:

- 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:

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

## Microwaves



Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

## Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- 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.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- 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:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.

- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

### **Advantages Of Microwave:**

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.

### **Disadvantages of Microwave transmission:**

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

### **Satellite Microwave Communication**

- 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.

### **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.

### **Infrared**

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared is 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:**

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