What is Computer Network?

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

Computer Network uses distributed processing in which task is divided among several computers. Instead, a single computer handles an entire task, each separate computer handles a subset.

Following are the advantages of Distributed processing:

- **Security:** It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- **Faster problem solving:** Multiple computers can solve the problem faster than a single machine working alone.
- **Security through redundancy:** Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

Protocol

It is a set of rules that determine how data is transmitted between different devices in the same network.

Types of Protocols

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secure (HTTPS)
9. Telnet
10. Gopher

2.Port

What is a computer network port?

A port in computer networking is how a computer can use a single physical network connection to handle many incoming and outgoing requests by assigning a port number to each. The numbers go from 0 to 65535, which is a 16-bit number.

Some of these port numbers are specifically defined and always associated with a specific type of service -- for example, File Transfer Protocol (FTP) is always port number 21 and Hypertext Transfer Protocol web traffic is always port 80. These are called *well-known ports* and go from 0 to 1023.

VPN

Virtual Private Network (VPN) | An Introduction

Difficulty Level : Easy • Last Updated : 23 Sep, 2021

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

MAC

Introduction of MAC Address in Computer Network

Difficulty Level : Medium • Last Updated : 22 Mar, 2021

In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. Media Access Control Address is a physical address which works at Data Link Layer. In this article, we will discuss about addressing in DLL, which is MAC Address.

Media Access Control (MAC) Address –

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers –

1. Logical Link Control(LLC) Sublayer
2. Media Access Control(MAC) Sublayer

Command for Windows OS finding the MAC- ***ipconfig /all***

IP

What is IP?

← Prev Next →

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

The first version of IP (Internet Protocol) was IPv4. After IPv4, IPv6 came into the market, which has been increasingly used on the public internet since 2006.

Router

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Socket

A **socket** is one endpoint of a **two way** communication link between two programs running on the network.It is a sequence of ip address and port number which ensures the successful communication between sender and receiver.

Differences between Hub and Switch

Hub	Switch
They operate in the physical layer of the OSI model.	They operate in the data link layer of the OSI model.
It is a non-intelligent network device that sends message to all ports.	It is an intelligent network device that sends message to selected destination ports.
It primarily broadcasts messages.	It is supports unicast, multicast and broadcast.
Transmission mode is half duplex.	Transmission mode is full duplex.
Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.	Collisions do not occur since the communication is full duplex.
They are passive devices, they don't have any software associated with it.	They are active devices, equipped with network software.
They generally have fewer ports of 4/12.	The number of ports is higher – 24/48.

1. **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.

2. **Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol

3. **Gateway** – Gateways are also called protocol converters .A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

4. **Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer.

Topology

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

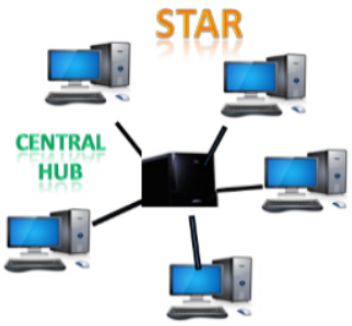
Bus Topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.

Star Topology



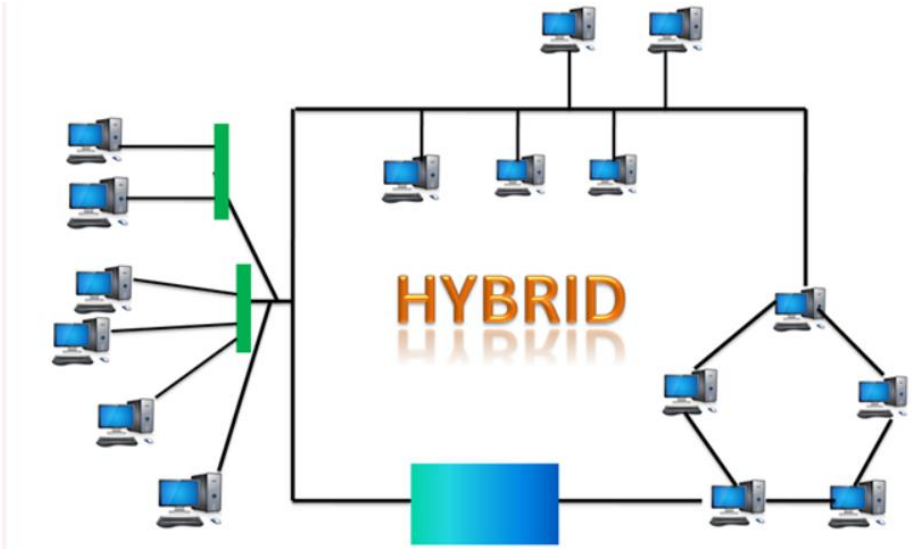
- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.

Tree topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.

Mesh topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Host

A host (or network host) is **a device that links with other hosts on a network.** It can either be a client or a server that sends and receives applications, services, or data. Hosts have their unique IP address on a TCP/IP network, consisting of the device's local number and the network number it belongs to.

DNS

DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

Address Resolution Protocol

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

A network interface card (NIC)

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer

Modem

Modem is a device that enables a computer to send or receive data over telephone or cable lines

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**.

The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

Depending on direction of data transmission, modem can be of these types −

- **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

RJ45 Connector

RJ45 is the acronym for **Registered Jack 45. RJ45 connector** is an 8-pin jack used by devices to physically connect to **Ethernet** based **local area networks (LANs)**

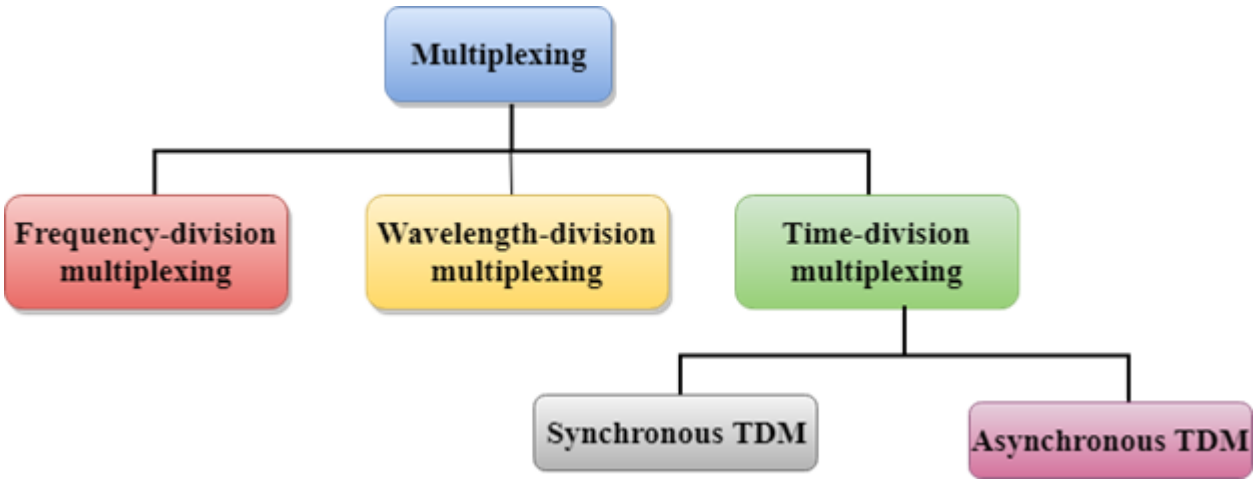
Wi-Fi Card

Wi-Fi is the acronym for **wireless fidelity. Wi-Fi technology** is used to achieve **wireless connection** to any network. **Wi-Fi card** is a **card** used to connect any device to the local network wirelessly.

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.



TCP	UDP
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	Header size is 8 bytes.
TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can’t be guaranteed in UDP.

Point of difference	Internet	Intranet	Extranet
Accessibility of network	Public	Private	Private
Availability	Global system.	Specific to an organization.	To share information with suppliers and vendors it makes the use of public network.
Coverage	All over the world.	Restricted area upto an organization.	Restricted area upto an organization and some of its stakeholders or so.
Accessibility of content	It is accessible to everyone connected.	It is accessible only to the members of organization.	Accessible only to the members of organization and external members with logins.
No. of computers connected	It is largest in number of connected devices.	The minimal number of devices are connected.	The connected devices are comparable with Intranet.
Owner	No one.	Single organization.	Single/ Multiple organization.
Purpose of the network	It's purpose is to share information throughout the world.	It's purpose is to share information throughout the organization.	It's purpose is to share information between members and external, members.
Security	It is dependent on the user of the device connected to network.	It is enforced via firewall.	It is enforced via firewall that separates internet and extranet.
Users	General public.	Employees of the organization.	Employees of the organization which are connected.

Basis	LAN	MAN	WAN
Full-Form	LAN stands for local area network.	MAN stands for metropolitan area network.	WAN stands for wide area network.
Geographic Span	Operates in small areas such as the same building or campus.	Operates in large areas such as a city.	Operates in larger areas such as country or continent.
Ownership	LAN's ownership is private.	MAN's ownership can be private or public.	While WAN also might not be owned by one organization.
Transmission Speed	The transmission speed of a LAN is high.	While the transmission speed of a MAN is average.	Whereas the transmission speed of a WAN is low.
Propagation delay	The propagation delay is short in a LAN.	There is a moderate propagation delay in a MAN.	Whereas, there is a long propagation delay in a WAN.
Congestion	There is less congestion in LAN.	While there is more congestion in MAN.	Whereas there is more congestion than MAN in WAN.

S.NO.	Flow control	Error control
1.	Flow control is meant only for the transmission of data from sender to receiver.	Error control is meant for the transmission of error free data from sender to receiver.
2.	For Flow control there are two approaches : Feedback-based Flow Control and Rate-based Flow Control.	To detect error in data, the approaches are : Checksum, Cyclic Redundancy Check and Parity Checking. To correct error in data, the approaches are : Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.
3.	It prevents the loss of data and avoid over running of receive buffers.	It is used to detect and correct the error occurred in the code.
4.	Example of Flow Control techniques are : Stop&Wait Protocol and Sliding Window Protocol.	Example of Error Control techniques are : Stop&Wait ARQ and Sliding Window ARQ.

What are the key elements of protocols?

The key elements of protocols are
a. Syntax
It refers to the structure or format of the data, that is the order in which they are presented.
b. Semantics
It refers to the meaning of each section of bits.
c. Timing
Timing refers to two characteristics: When data should be sent and how fast they can be sent.

What Does HOP Count Mean?

HOP counts refer to the number of devices, usually routers, that a piece of data travels through. Each time that a packet of data moves from one router (or device) to another — say from the router of your home network to the one just outside your county line — that is considered one HOP.

PING: Packet InterNet Groper

PING stands for Packet InterNet Groper in computer networking field. It is a computer network administration software utility used to test the network connectivity between two systems.

IPCONFIG stands for **Internet Protocol Configuration**. This is a command-line application which displays all the current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration, refreshes the DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name Server).

. IEEE stands for Institute of Electrical and Electronics Engineers.

What is **congestion**?

A state occurs in the network layer when the message traffic is so heavy that it slows down network response time.

- What happens when you type URL in your browser?

Steps are:

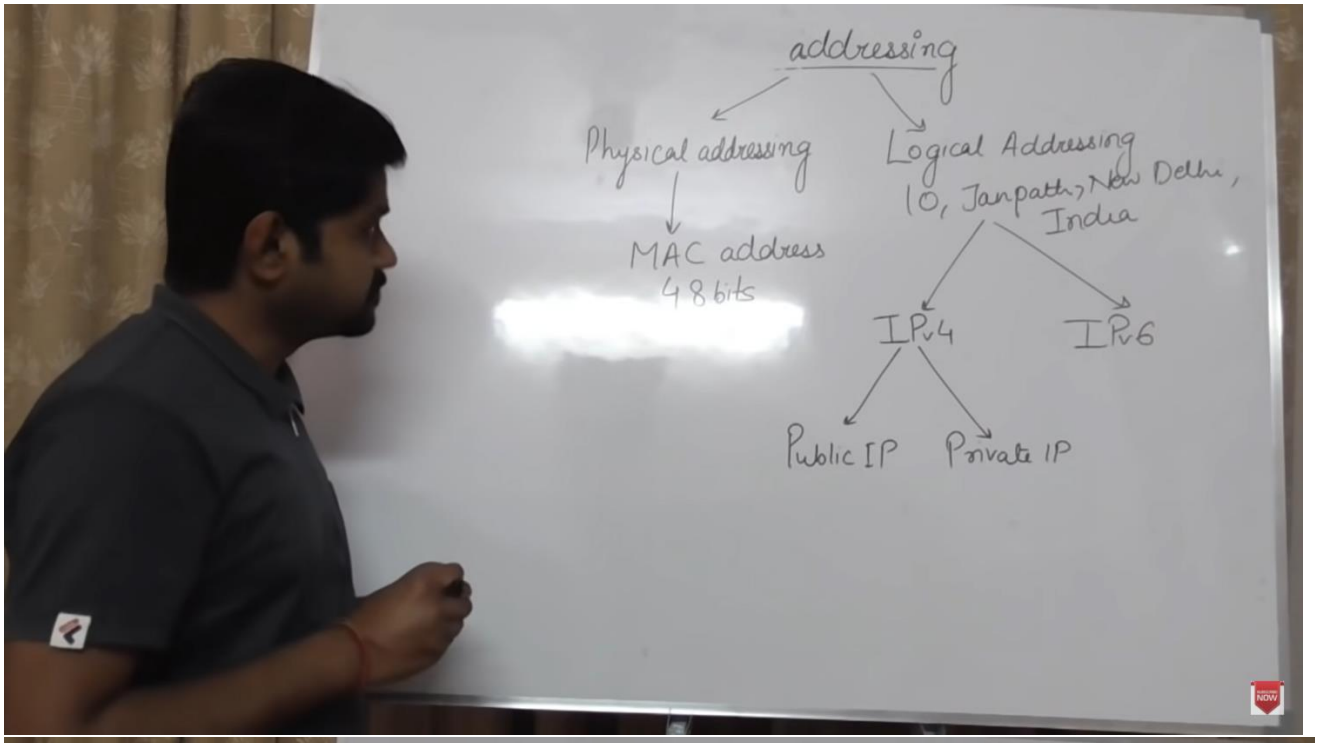
1. URL is typed in the browser.
2. If the requested object is in the browser cache and is fresh, move on to Step 8.
3. DNS lookup to find the IP address of the server.

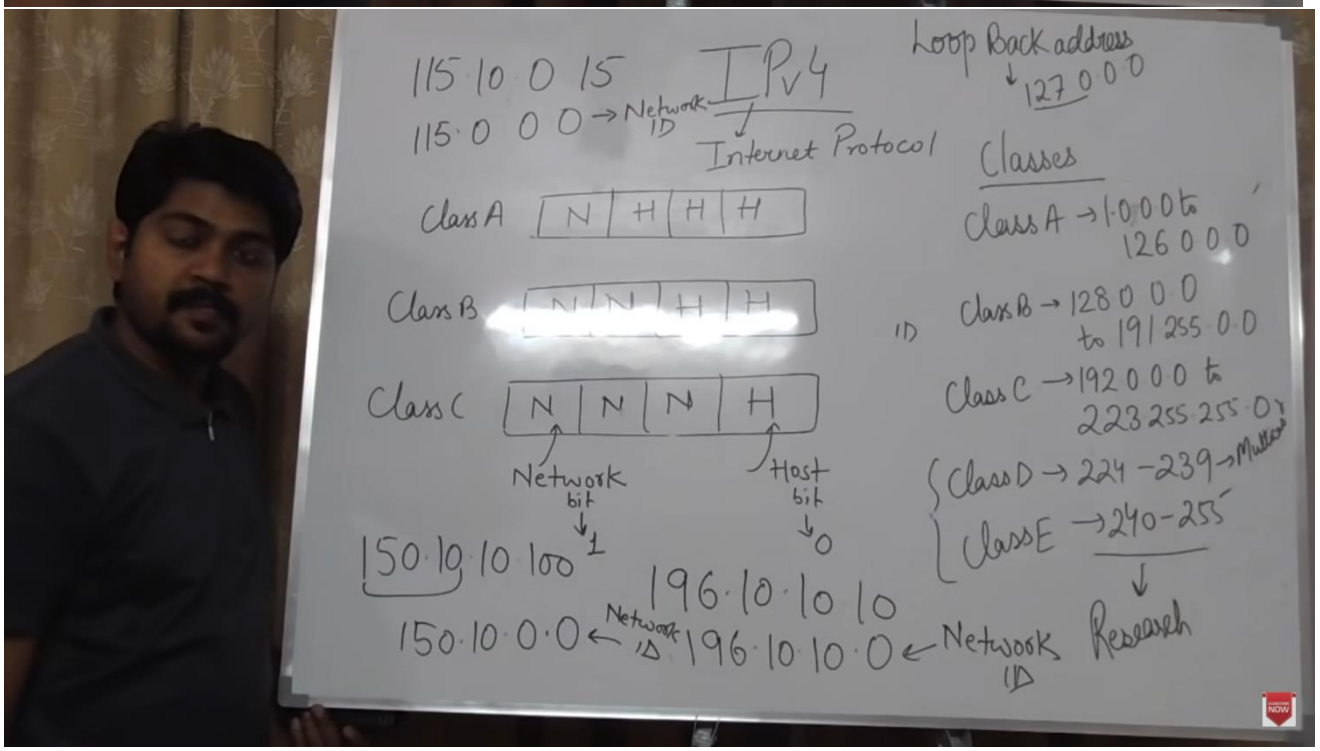
   Suppose we typed www.amazon.in, then this URL is converted into corresponding IP address of the host using DNS(Domain Name System). But, it is not so. Amazon has multiple servers in multiple locations to cater to the huge volume of requests they receive per second. Thus we should let Amazon decide which server is best suited to our needs.
4. Following is a summary of steps happening while DNS service is at work:

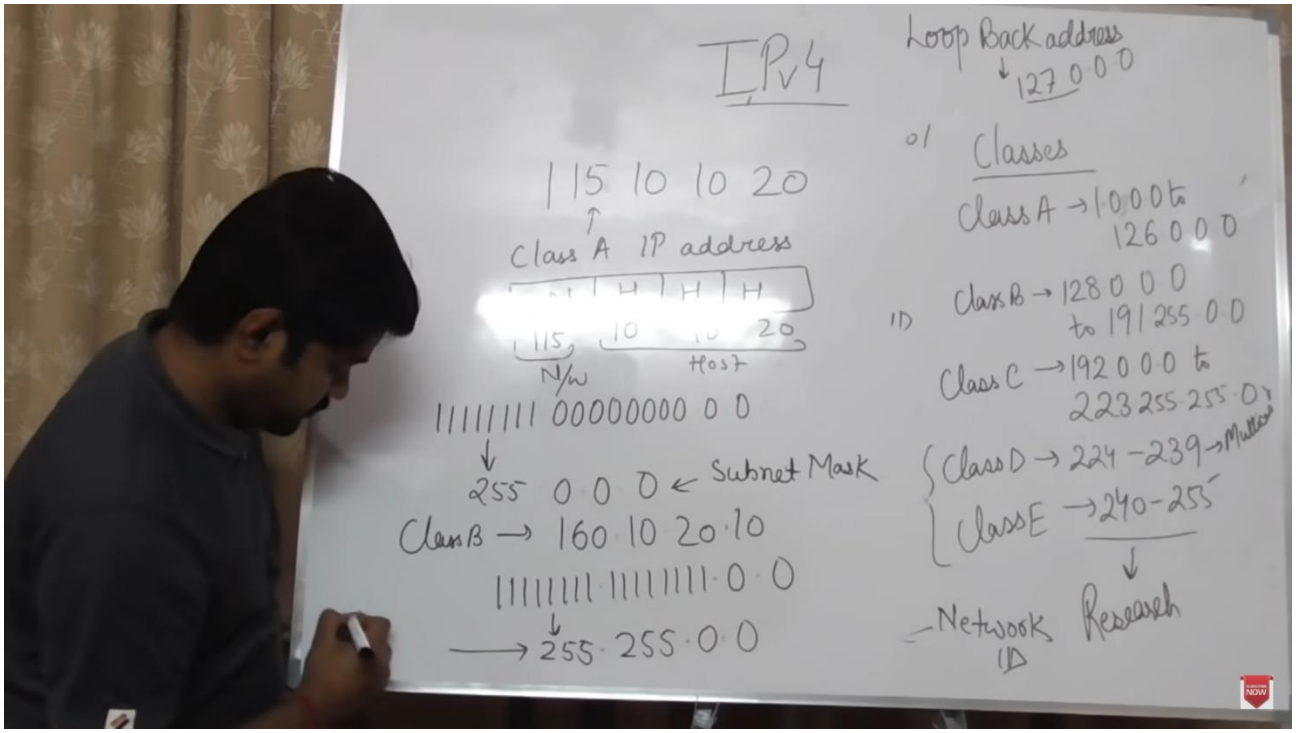
   - **Check browser cache**: browsers maintain a cache of DNS records for some fixed duration. So, this is the first place to resolve DNS queries.
   - **Check OS cache**: if the browser doesn't contain the record in its cache, it makes a system call to underlying Operating System to fetch the record as OS also maintains a cache of recent DNS queries.
   - **Router Cache**: if above steps fail to get a DNS record, the search continues to your router which has its own cache
   - **ISP cache**: if everything fails, the search moves on to your ISP. First, it tries in its cache, if not found - ISP's DNS recursive search comes into the picture. DNS lookup is again a complex process which finds the appropriate IP address from a list of many options available for websites like Google.

Differences between HTTP and HTTPS

- In HTTP, URL begins with “http://” whereas URL starts with “https://”
- HTTP uses port number 80 for communication and HTTPS uses 443
- HTTP is considered to be unsecure and HTTPS is secure
- HTTP Works at Application Layer and HTTPS works at Transport Layer
- In HTTP, Encryption is absent and Encryption is present in HTTPS as discussed above
- HTTP does not require any certificates and HTTPS needs SSL Certificates


addressing
Physical addressing
MAC address
48 bits
Logical Addressing
10, Janpath, New Delhi, India
IPv4
IPv6
Public IP
Private IP


115.10.0.15
115.0.0.0 → Network ID
IPv4
Internet Protocol
Loop Back address
127.0.0.0
Classes
Class A
N H H H
Class B
N N H H
Class C
N N N H
Network bit
Host bit
150.10.10.100
150.10.0.0 ← Network ID
196.10.10.10
196.10.10.0 ← Network ID
Class A → 1.0.0.0 to 126.0.0.0
Class B → 128.0.0.0 to 191.255.0.0
Class C → 192.0.0.0 to 223.255.255.0
Class D → 224-239 → Multicast
Class E → 240-255
Research



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Before starting it is better to get acquainted with a term called **Protocol Data Unit (PDU)**. The term PDU is used to refer to the packets in different layers of the OSI model. Thus PDU gives an abstract idea of the data packets. The PDU has a different meaning in different layers still we can use it as a common term.
To give a clear picture:-

1. The PDU of Transport Layer is called as a Segment.
2. The PDU of Network Layer is called as a Packet.
3. The PDU of the Data-Link Layer is called Frames.

1. **Segment:**
   The data from the application layer is broken into smaller parts as per the MSS of the network and the TCP header is added to the smaller parts. The size of the header can vary from 20B to 60B. But usually, the header is of size 20B(rest 40B are optional)

2. **Packets:**
   The segments received from the Transport layer are further processed to form the Packets.The IP packet has a header of varying sizes from 20B to 60B. But usually, it is 20B.

3. **Frames:**
   The Packets received from the Network Layer further processed to form the Frames.

Internet Control Message Protocol (ICMP)

Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide an error control. It is used for reporting errors and management queries.

TELNET

TELNET stands for **TE**rmina**L NET**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard **TCP/IP protocol** for virtual terminal service which is given by **ISO**. Computer which starts connection known as the **local computer**.

Bandwidth

The maximum amount of data transmitted over an internet connection in a given amount of time.

What's the difference?

Some internet terms are so similar that they're often confused with each other. We're here to help set the record straight.

Bandwidth vs speed

Bandwidth is how much information you receive every second, while speed is how fast that information is received or downloaded. Let's compare it to filling a bathtub. If the bathtub faucet has a wide opening, more water can flow at a faster rate than if the pipe was narrower. Think of the water as the bandwidth and the rate at which the water flows as the speed.

Bandwidth vs latency

Latency is sometimes referred to as delay or ping rate. It's the lag you experience while waiting for something to load. If bandwidth is the amount of information sent per second, latency is the amount of time it takes that information to get from its source to you.

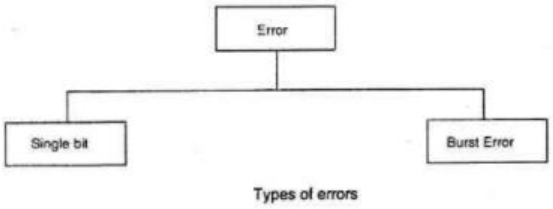
Bandwidth vs throughput

Throughput is how much information actually gets delivered in a certain amount of time. So if bandwidth is the max amount of data, throughput is how much of that data makes it to its destination – taking latency, network speed, packet loss and other factors into account.

Type of Errors

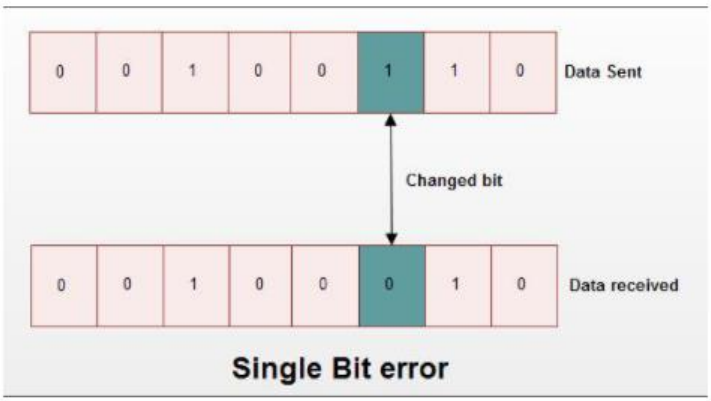
There are two main types of errors in transmissions:

1. Single bit error
2. Burst error



Types of errors

Single bit error: It means only one bit of data unit is changed from 1 to 0 or from 0 to 1 as shown in fig.



Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires. Single bit errors are the least likely type of error in serial transmission.

Burst Error: It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.

CIA triad in Cryptography

When talking about network security, the **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

Confidentiality :
Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information.

Integrity :
The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.

Availability :
This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network.

Difference between Unicast, Broadcast & Multicast

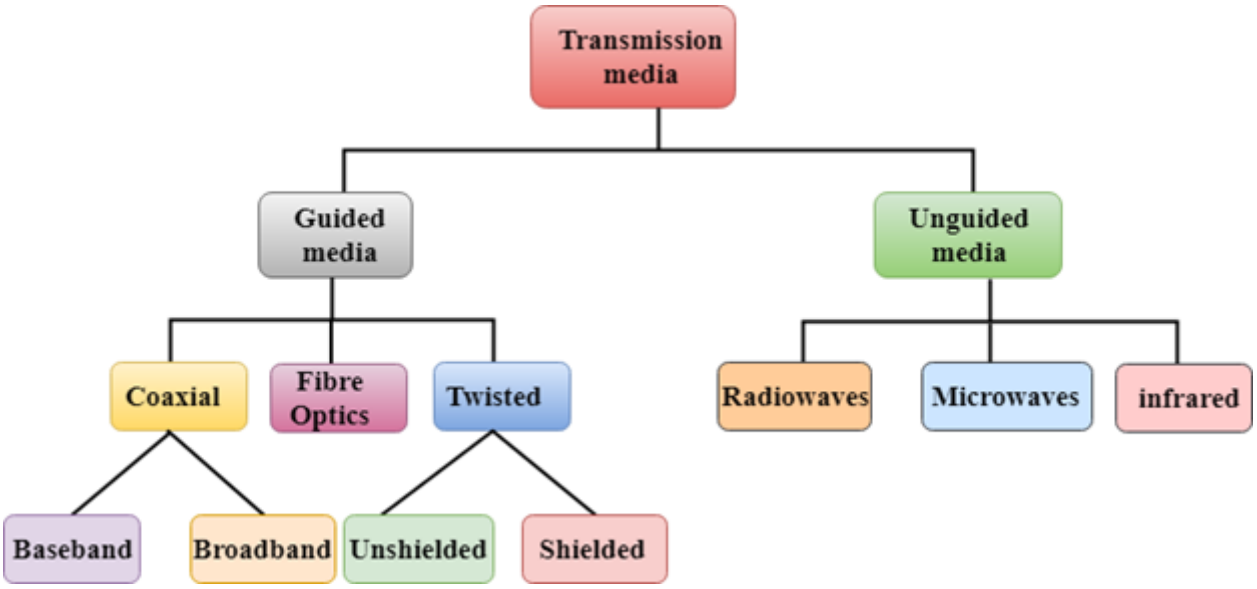
Data is transported over a network by three simple methods i.e. Unicast, Broadcast, and Multicast. So let's begin to summarize the difference between **these three:**

- **Unicast**: from one source to one destination i.e. One-to-One
- **Broadcast**: from one source to all possible destinations i.e. One-to-All
- **Multicast**: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many

Difference Between Unicast, Broadcast, and Multicast in Computer Network

Here is a list of the differences between Unicast, Broadcast, and Multicast in Computer Network.

Parameters	Unicast	Broadcast	Multicast
Basics	There is only one receiver and one sender.	There are multiple receivers and one sender.	There are multiple receivers and multiple senders.
Meaning and Definition	Unicast information transfer is helpful for transferring data from a single client to all the recipients over the same network.	Broadcast data transfer occurs when one sender transmits data to multiple recipients at any given time.	Multiple senders and recipients participate in the process of data transfer in Multicasting.
Mapping	It is a one-to-one type of data transfer.	It is a one-to-many type of data transfer.	It is a many-to-many type of data transfer.
Uses	It is very helpful when a single sender transmits data to a single recipient.	Broadcasting is mainly helpful for audio and video distribution by television networks.	These are helpful in the stock exchange, multimedia delivery, etc.

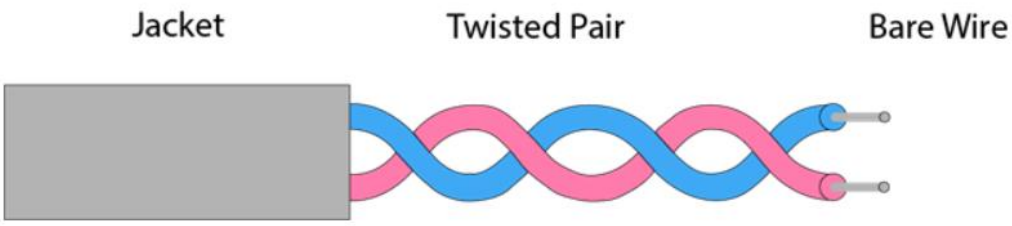


Twisted pair:

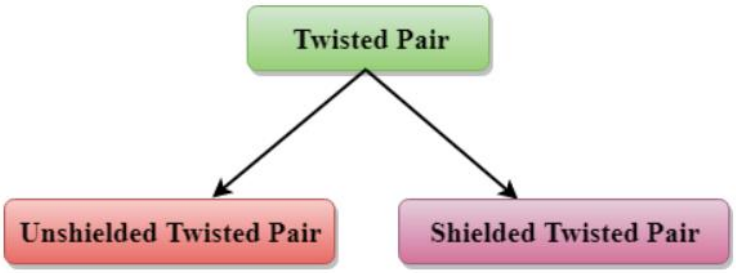
Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

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.

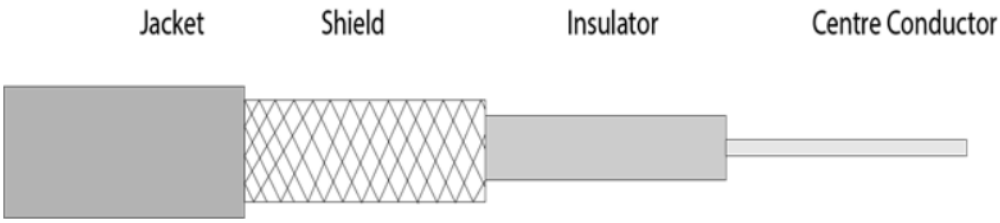


Types of Twisted pair:



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.

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.

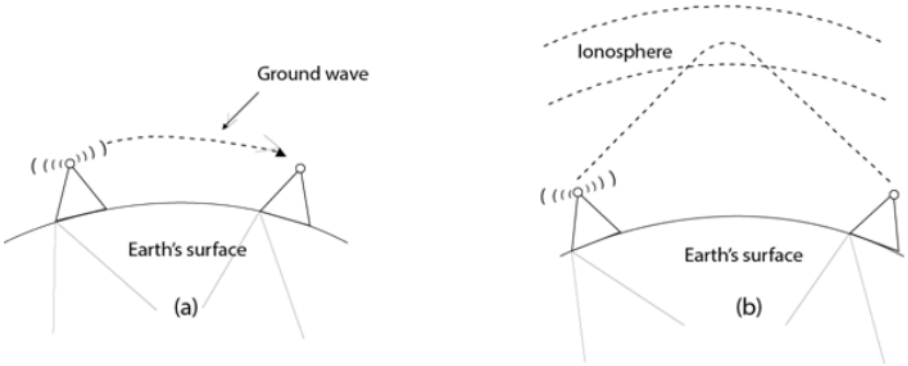
Diagrammatic representation of fibre optic cable:

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.

Radio waves

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



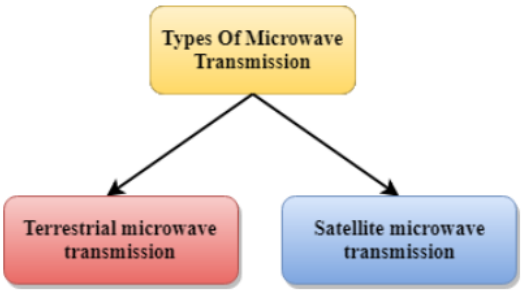
Applications Of Radio waves:

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

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:

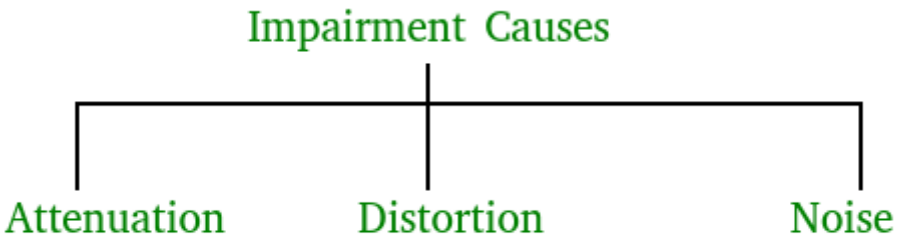
- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.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

Infrared

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

Characteristics Of Infrared:

- 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.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.



Attenuation – It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium.

Distortion – It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies

Noise – The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.