Unit-1 Data Communication: Introduction

Contents

1.1 Data Communication

In Data Communications, data generally are defined as information that is stored in digital form. Data communications is the process of transferring digital information between two or more points. Information is defined as the knowledge or intelligence.

For data communications to occur, the communicating devices must be part of communication system made up of a combination of hardware (physical equipment) and software (programs).

The five components of data communication system are

1) **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2) **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3) **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation telephone handset, television, and so on.
4) **Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5) **Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data - The word ‘data’ refers that representation of information in an understandable form by the two parties who are creating and using it. The Webster dictionary defined data as “information in digital form that can be transmitted or processed”. The data may be in any form such as text, symbols, images, videos, signals and so on.

Communication - Communication is a referred as exchanging information from one entity to another entity in a meaningful way. The entities may be referred as human being, machines, animals, birds, etc. The communication could be done between the two entities / parties. The meaningful way refers that

the meaning of the communication must be understandable between the two entities. The figure 1.1 shows the model for communication between two people.

Data communications can be summarized as the transmission, reception, and processing of digital information. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

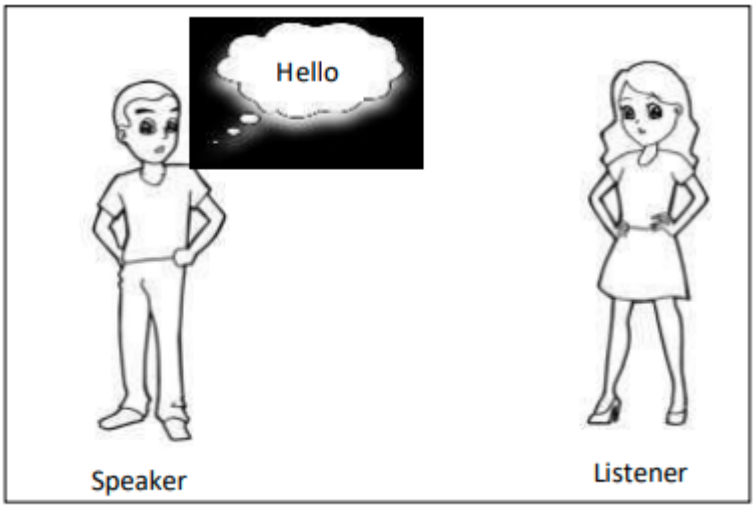


Figure 1.1 Communication between two persons

1.1.2 Characteristics

1) **Resource Sharing:** It means that all computers within network share resource. The goal is to make all programs, data and devices available to anyone on the network without considering the physical location of the resource and user.
2) **High Reliability:** Networks provide high reliability by having alternative source of supply. All files can be replicated on two or more machines so if one of them is unavailable then other copies could be used.
3) **Saving Money:** Network consists of two or more computers. Mostly in networking, one computer works as server and other as client means only server requires connection with resource and all other clients can easily access it.
4) **Scalability:** Network is able to increase system performance as the work grows, just by adding more processor.
5) **Time Saving:** For e.g., E-mail services require less time compared to postal services.
6) Improve Performance: We can improve the performance of network by adding network hardware and software.

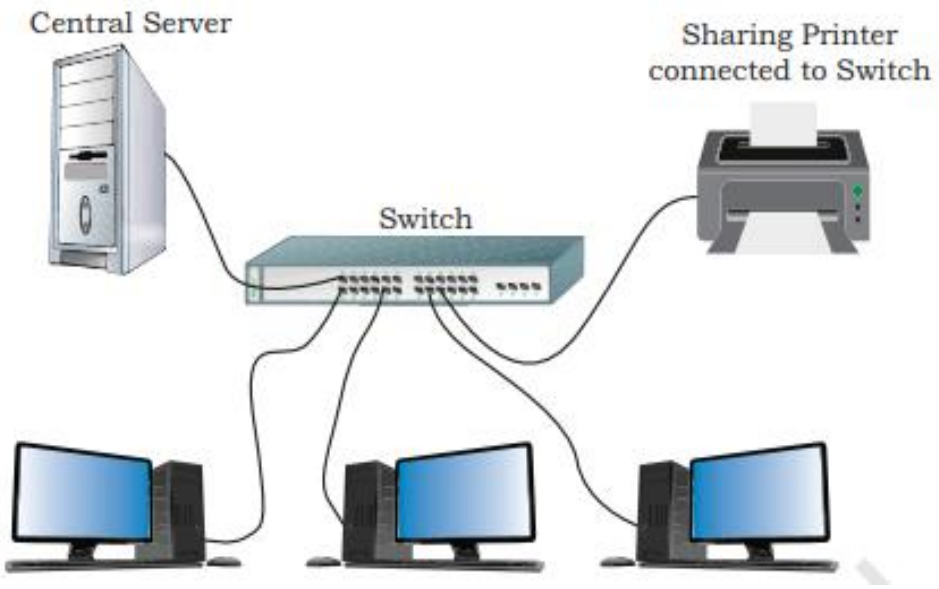


Figure 1.2 A simple network of computing devices

1.2. Computer Network

1.2.1 Pros and Cons of Computer Network

Advantages of Computer Network

1) **Efficient management of resources:** A network offers the user to share their resources. For example a user can share a single high quality printer rather than putting a number of low qualities and less expensive printer at individual desktops.
2) **Faster data sharing:** Transferring files across a network is almost and always faster than other non-network means of data transfer. For e.g., network resources such as scanners, Fax machines, Printers etc can be shared over a network.
3) **Centralized Software Management:** A well-managed centralized data storage system allows multiple users to access data from different locations. This helps in keeping the data up-to-date and ensures that unauthorized person do not attempt tempering or changing the important data.
4) **High reliability:** Network provides high reliability by having alternative sources of supply. All files could be replicated on two or more machines so if one of them is unavailable then other copies could be used.
5) **Security:** Files, programs and resources can be protected and access can be restricted by using user rights. Specific files can be restricted from being copied thereby protect copyright materials.
6) **Efficient communication:** E-mail, online conferencing, project monitoring can lead to better communication between workgroups and help to improve productivity.

Disadvantages of Computer Network

1) **It lacks independence:** People will rely more on computer work, instead of applying own effort for their tasks. Apart from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.
2) **It lacks robustness:** If a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.
3) **It allows for more presence of computer viruses and malware:** There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.

4) **It poses security difficulties:** Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.
5) **It requires an expensive set-up:** The initial set up cost is high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. It would also need network interface cards (NICs) for Workstations in case they are not built in.
6) **Its light policing usage promotes negative acts:** It has been observed that providing users with internet connectivity has caused various distractions like online gaming. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters.

1.2.2 Applications of Computer Network

1) **Marketing and Sales:** Marketing persons use them to collect, exchange and analyses data related to customer.
2) **Financial Services:** Credit history searches, foreign exchanges, investment services and electronic fund transfer etc.
3) **Electronic Messaging:** E-mail services are possible using networks.
4) **Manufacturing:** Computer Networks are used in the manufacturing process. CAD-computer assisted design and CAM-computer assisted manufacturing, these two applications use networks to provide services.
5) **Directory Services:** It allows list of files to be stored in particular location and search operation for the file.
6) **Information Services:** World Wide Web offers the information services.
7) **Cellular Telephone:** Today cellular networks make it possible to maintain wireless phone connection over large distance.
8) **Teleconferencing:** It allows conferences to occur without the participant being in same place. It includes text, audio and video conferencing.
9) **Electronic Data Interchange:** It allows business information to be transferred without using paper.
10) **Cable Television:** Cable television is also used for the computer network concepts.

1.3 Standard Organizations for Data Communication

1) ISO – International Standards Organization

ISO is the world's largest developer and publisher of international standards founded in1946.Forexample, ANSI (American National Standards Institute) is a member of ISO.ISO standards are published as ISO serial-no e.g., ISO 8632.

2) CCITT – Consultative Committee for International Telephony and Telegraphy. This committee was devoted to the research and establishment of standards for telecommunications. CCITT has defined many important standards for data communication. CCITT standards are published as L.serial-no e.g., l.440.

3) ANSI – American National Standards Institute

ANSI is a private non-profit organization that creates standards for computer industry. ANSI C is a version of C language approved by the ANSI committee. The organization also co-ordinates US standards with international standards so that American products can be used worldwide.

4) IEEE – Institute of Electrical and Electronics Engineers

IEEE is an international non-profit, professional organization for the advancement of technology related to electricity. IEEE was formed when AIEE merged with IRE. IEEE standards are published as

IEEE serial-no e.g., IEEE 908.

5) ITU – International Telecommunications Union

ITU is the oldest international organization, established to standardize and regulate international radio and telecommunication. Its main tasks include standardization, allocation of the radio spectrum and organizing interconnection arrangements between different countries to allow international phone calls.

6) ISOC – Internet Society

ISOC is an international educational organization that provides direction in internet related standards and policy. ISOC provides financial support structure and promote activities for development of internet.

7) IETF – Internet Engineering Task Force

IETF develops and promotes internet standards, dealing in particular with standards of the TCP/IP protocol suite. The IETF is organized into large number of working groups and informal discussion groups, each dealing with a specific topic.

8) EIA – Electronic Industries Association

EIA is a trade organization for electronics manufacturers. It developed standards to ensure the equipment of different manufacturers was compatible. EIA standards are published as EIA-serial-no (EIA-232).

1.4 Types of Area Networks

Network is classified according to their geographical size. Network refers to three primary categories.

1) LAN (Local Area Network)

2) MAN (Metropolitan Area Network)

3) WAN (Wide Area Network)

<table>
<tr><th>Inter processor distance</th><th>Processor located in same</th><th>Example</th></tr>
<tr><td>0.1 m</td><td>Circuit board</td><td>Data flow machine</td></tr>
<tr><td>1 m</td><td>System</td><td>Multicomputer</td></tr>
<tr><td>10m</td><td>Room</td><td rowspan="3">Local Area Network</td></tr>
<tr><td>100m</td><td>Building</td></tr>
<tr><td>1km</td><td>Campus</td></tr>
<tr><td>10km</td><td>City</td><td>Metropolitan Area Network</td></tr>
<tr><td>100km</td><td>Country</td><td rowspan="2">Wide Area Network</td></tr>
<tr><td>1000km</td><td>Continent</td></tr>
<tr><td>10,000km</td><td>Planet</td><td>The Internet</td></tr>
</table>

Table 1.3 Classification of computer network according to their geography

LAN (Local Area Network)

LAN is a group of network computers and network communication devices interconnected within the geographically limited area like office building, computer lab or campus. LAN tends to use only one type of transmission medium i.e., cabling.

Characteristics of LAN

1) It allows- users to share storage devices like printer, application data and other network resources.
2) It transfers data at high speed (more than 1 mbps).
3) It exists in limited geographical area (Up to few kilometres).
4) Multiple accesses (many can use it at the same time).
5) It is having a lower error rate.
6) Its technology is generally less expensive.

Advantages of LAN

1) LAN provides a cost-effective multi-user computer environment.
2) LAN can fit any site requirement.
3) Any number of users can be accommodated.
4) Allows sharing of mass central storage and printers.
5) It is flexible and growth oriented.
6) It provides data integrity.

Fig 1.3 LAN

MAN (Metropolitan Area Network)

A MAN covers a much larger area and might cover an entire city. It may be a single network such as cable television network or it may be a means of connecting a number of LANs together into a larger network. So that resources may be shared LAN to LAN as well as device to device. For example, a company can use a MAN to connect the LANs in all of its offices through a city.

Characteristics of MAN

1) A special category or standard has been adopted for MAN and this standard is now implemented and it's called DQDB (Distributed Queue Dual Bus).
2) Using this standard, a MAN extends up to 30-40 km, or 20-25 miles.

Advantages of MAN

1) A MAN can cover a wider area than a LAN.
2) Information can be disseminated more widely, rapidly and significantly.

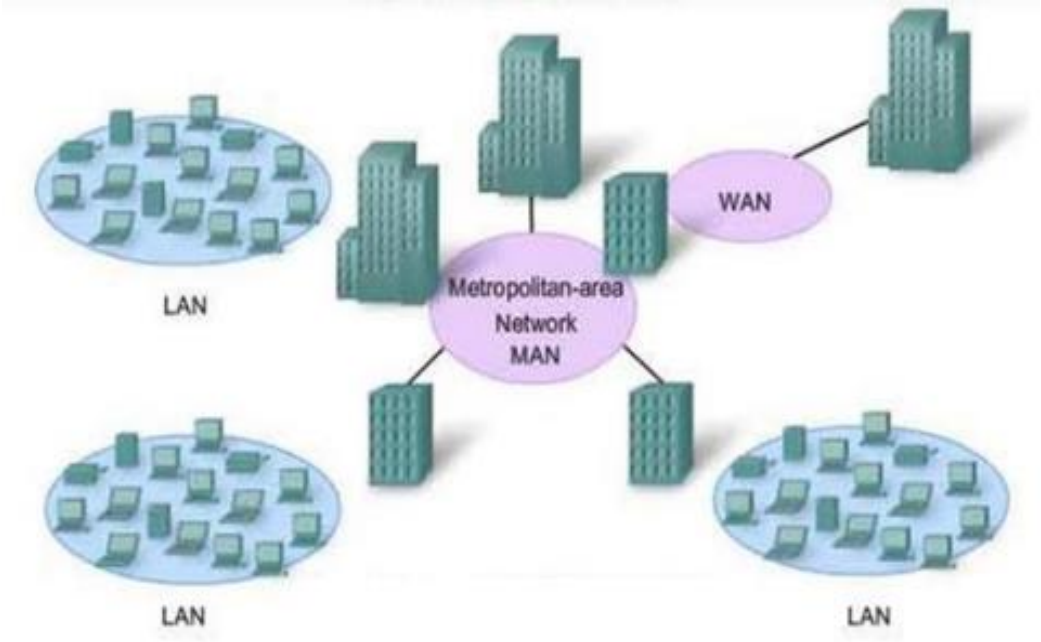


Fig 1.4 MAN

WAN (Wide Area Network)

When a network is spread over wide areas such as cities, states, countries or continent it is called a WAN Communication on a wan takes place via telephone lines, satellite or microwave transmission rather than physical cable. Most WANs are combinations of LANs and other types of communication.

Types of WAN

Public Network - Public network are those networks, which are installed and run by the telecommunication authorities and are available to any organization or individuals who subscribes.

Private Network - The basic technology used in all forms or private WAN is to use private or more usually leased circuit to link the location to be served by the network.

Characteristics of WAN

1) They exist in unlimited geographical area.
2) They are more susceptible to error due to the distance the data can travel.
3) They interconnect multiple LAN.
4) They are more sophisticated and complex than LAN.
5) Their technology is expensive.

Advantages of WAN

1) Setting up a WAN allows you to share sensitive data with all your sites without having to send the information over the Internet.
2) WAN ensures maximum availability and reliability.
3) A WAN eliminates the need to buy email or file servers for each office.

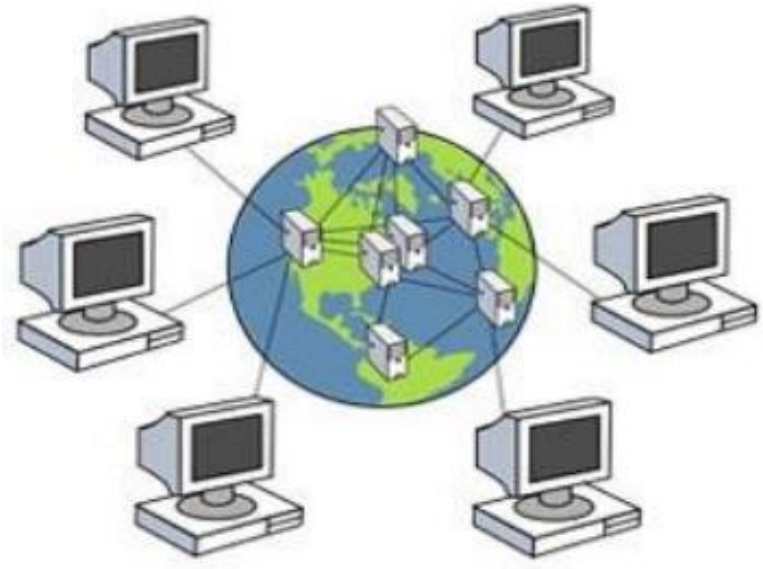


Fig 1.5 WAN

1.5 Line Configuration and its Classification

Line configuration defines the attachment of communication devices to a link. A link is a physical communication pathway that transfers data from one device to another device. For communication to occur, two devices must be connected in some way to the same link at the same time.

There are two possible line configurations: Point to Point and Multi Point. Point to Point has three types:

1) Unicast 2) Multicast 3) Broadcast

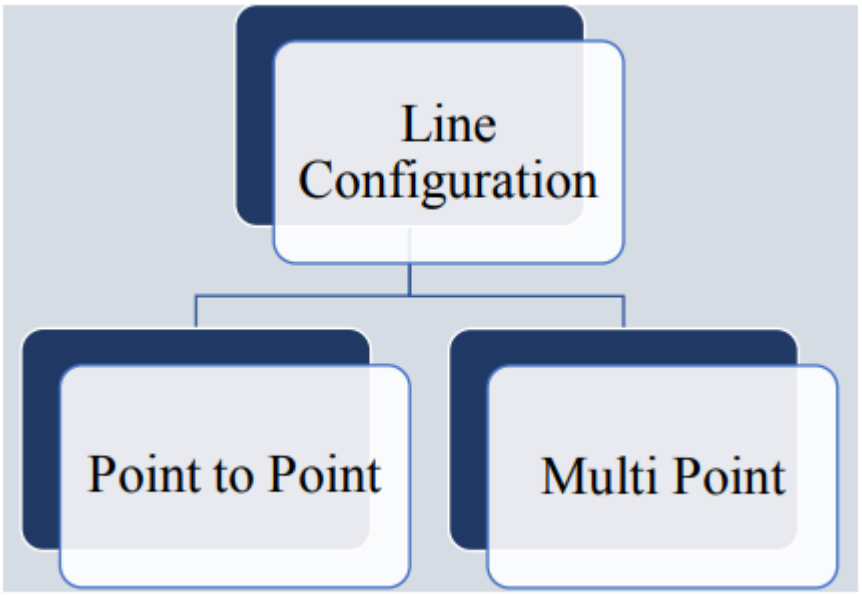
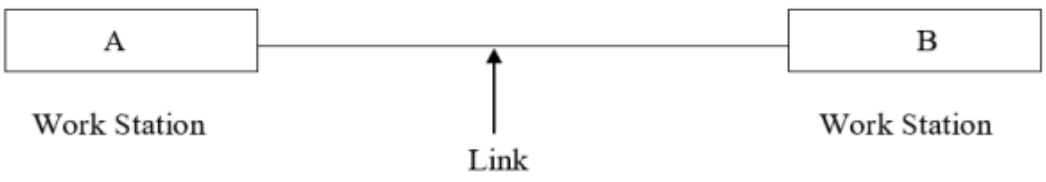


Fig 1.6 Line Configuration

Point to Point



Two and only two devices are connected by a dedicated link. Dedicated link means that link carries traffic between connected devices only and no other devices can use it. In this configuration, entire capacity of the channel is reserved for transmission between two devices.

E.g., Line configuration between the remote control and television.

There are 3 types of Point to Point networks: Unicast, Multicast and Broadcast.

1. Unicast

Information is sent from only one sender to only one receiver. One-to-one connection between client and server. E.g., HTTP, SMTP, TELNET.

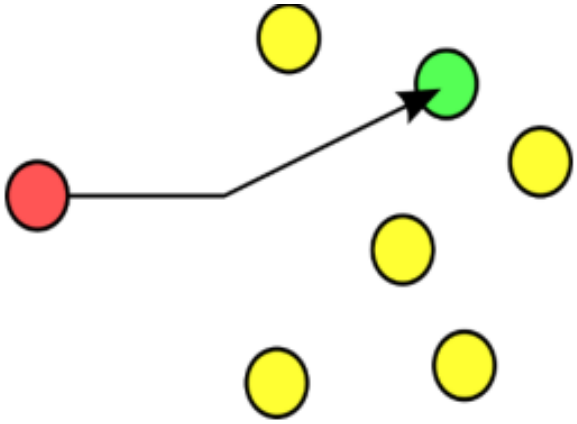


Fig 1.7 Unicast

2. Multicast

One or more senders send information to set of receivers. It saves bandwidth since same information can be received at same time. E.g., one computer transmits video channel to a specific group of computers.

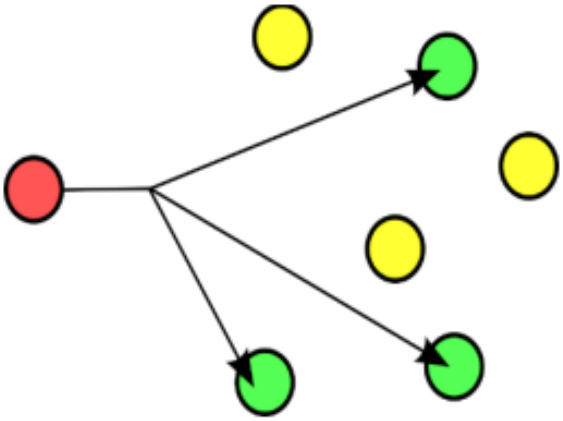


Fig 1.8 Multicast

3. Broadcast

Information is sent from one computer but received by all the computers connected to the network. A computer transmits a packet of type ‘broadcast’ which in turn is received by all the other computers. For e.g., a computer booting up and requesting for an IP address.

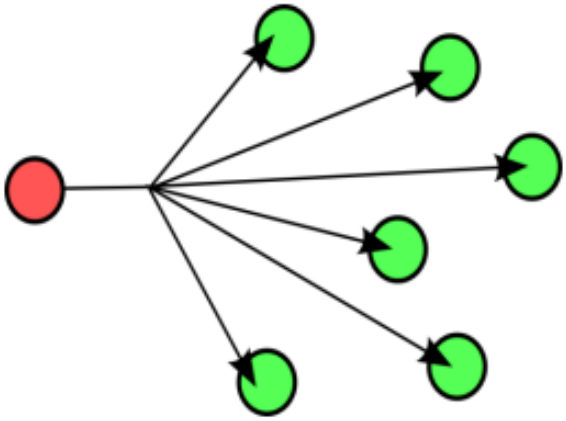


Fig 1.9 Broadcast

Multipoint

A multipoint line configuration is one in which more than two specific devices share a single link. In this configuration, the capacity of the channel is shared either spatially or temporarily.

1) Spatially Shared Line Configuration: Several devices using the link simultaneously (at same time) is called spatially shared line configuration.
2) Time Shared Line Configuration: Some fixed time slots given to the users to communicate is called time-shared line configuration.

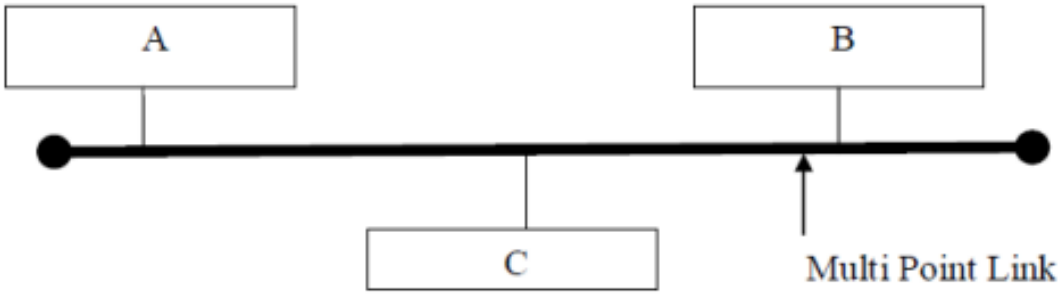


Fig 1.10 Multipoint

1.6 Types of Network Topologies

Topology

Topology refers to the way in which interconnection path between many users or nodes are arranged. Topology describes the actual physical layout of the network transmission media which includes the location of the computers and how the cable runs between them.

The various types of Topologies are bus, star, ring, mesh and tree topology.

BUS Topology

It is also known as linear bus topology. It consists of several computers attached via drop lines to a long common cable that acts as a backbone to link all the devices in the network. In bus topology, data on the network is send to all the computers on the network. However, only the computer that has the address matching the address in the signal accepts the data. The other computers reject the data.

Only one computer at a time can send message. A computer must wait until the bus is free before it can transmit. The failure of one computer does not affect the performance of the network. Bus topology is a passive topology in which the computers on the bus only listen to the data being sent and are not responsible for moving the data.

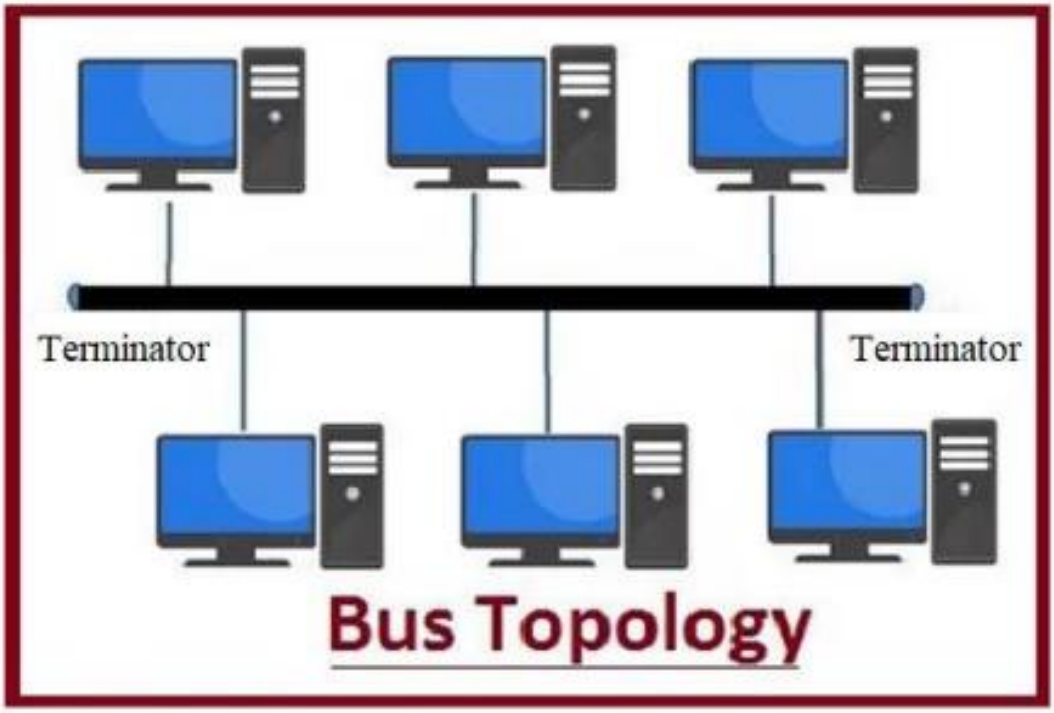


Fig 1.11 BUS TOPOLOGY

Advantages of BUS Topology

1) It is very simple.
2) Reliable in very small network.
3) Easy to use
4) Easy to understand.
5) It is easy to extend the bus topology.
6) It is less expensive than other cabling methods.
7) Bus requires the least amount of cable to connect the computers together.

Disadvantages of BUS Topology

1) Bus topology cannot work efficiently under heavy network traffic.
2) Too many extensions on a bus can weaken the electric signal.
3) Troubleshooting a bus can prove to be quite difficult.
4) Entire network shuts down if there is a break in the main cable.
5) Terminators are required at both ends of the backbone cable to avoid ringing problem.

Star Topology

In star topology each device has dedicated point to point link only to a central controller usually called HUB. The devices are not directly linked to each other. A star topology does not allow direct traffic between devices. The controller acts as an exchange, if any device wants to send a data to another, it sends the data to the controller, which then relay the data to the other connected devices.

If the central controller fails, the entire network is disabled. However, if one computer or the cable that connects it to the HUB fails, the rest of the network continues to function normally. Each computer is connected to central HUB, this topology requires more cable.

Fig 1.12 STAR TOPOLOGY

Advantages of STAR Topology

1) It is easy to modify and add new computers to a star topology network without disturbing the rest of the network.
2) There is a central point, controller or HUB in star network; it is easier to diagnose network problems.
3) Single computer failure does not bring down the whole network.

Disadvantages of STAR Topology

1) If the central HUB fails, the entire network fails to operate.
2) More cable is required compared to BUS topology.
3) More expensive than linear bus topology.

Ring Topology

In ring topology computers are connected on single circle of cable shown in fig. There are no terminating ends. A signal is passed along the ring in one direction from device to device until it reaches the destination. Each device in ring is connected to a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. Failure of one computer in ring affects the entire network.

The network uses token passing method for transferring data. A short message called a token is passed around the ring until a computer needs to send data to another computer. The receiving computer returns a message to the originator indicating that message has been received. The sending computer then creates another token and places it on the network. This allows another station or device to capture the token and begin transmitting.

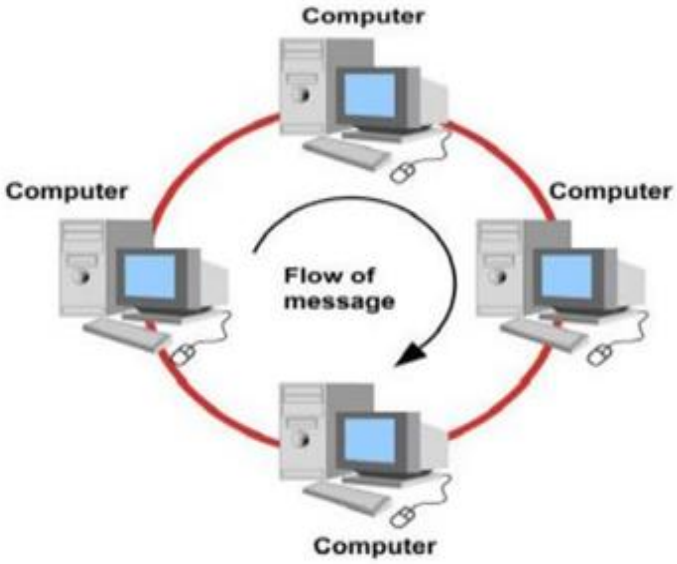


Fig 1.13 RING TOPOLOGY

Advantages of RING Topology

1) The network efficiency can approach 100% under condition of heavy load.
2) The network allows equal access to all computers.

Disadvantages of RING Topology

1) Failure of one computer in ring can affect the whole network.
2) Adding and removing the computer disturbs the network.
3) It is difficult to troubleshoot.

Mesh Topology

In a mesh topology every device has a dedicated point-to-point link to every other device shown in fig. The term dedicated means that the link carries traffic only between the two devices it connects. A fully connected mesh network therefore has n(n-1)/2 physical channels to link n devices. To accommodate that many links, every device on the network must have n-1 input/output ports.

There are two types of mesh topology namely Full mesh and partial mesh topology. In Full mesh topology, every node has a circuit connected to every other node in the network. So, it is more expensive. Partial mesh topology is less expensive comparatively.

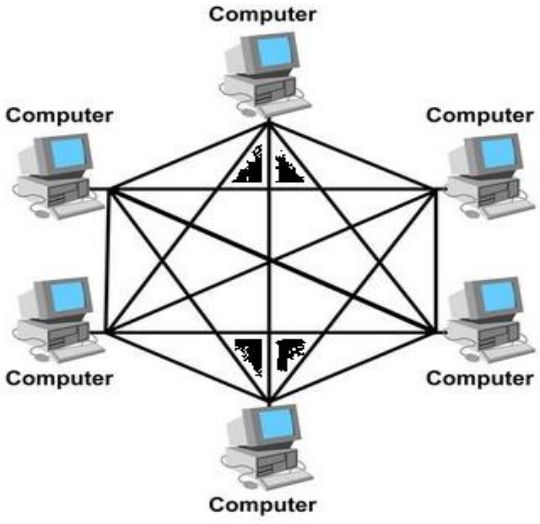


Fig 1.14 MESH TOPOLOGY

Advantages of MESH Topology

1) The use of dedicated link guarantees that each connection can carry its own data load thus eliminating the traffic problem that can occur when links must be shared by multiple devices.
2) It is robust, means if one links becomes unusable it does not incapacitate the entire system.
3) It provides privacy or security means while every message travels along a dedicated line, only the intended recipients see and prevent other users from gaining access to message.
4) Point to point link makes fault identification easy.

Disadvantages of MESH Topology

1) More cables and more numbers of I/O ports are required.
2) Hardware required to connect each link can be expensive.
3) Installation and reconfiguration are difficult because every device must be connected to every other device.
4) It is usually implemented in limited fashion.

Tree Topology

A tree topology is variation of star; nodes in a tree are linked to central hub that control traffic to the network shown in fig. Every device does not plug directly into the central hub. The majority of devices connect to secondary hub that in turn is connected to the central hub. The majority of devices connect to secondary hub that in turn is connected to the central hub.

The central hub in the tree is an active hub. The active hub contains a repeater, which is a hardware device that regenerates the received bit patterns before sending them out. The secondary hub may be active or passive. A passive hub provides simple physical connection between the attached devices.

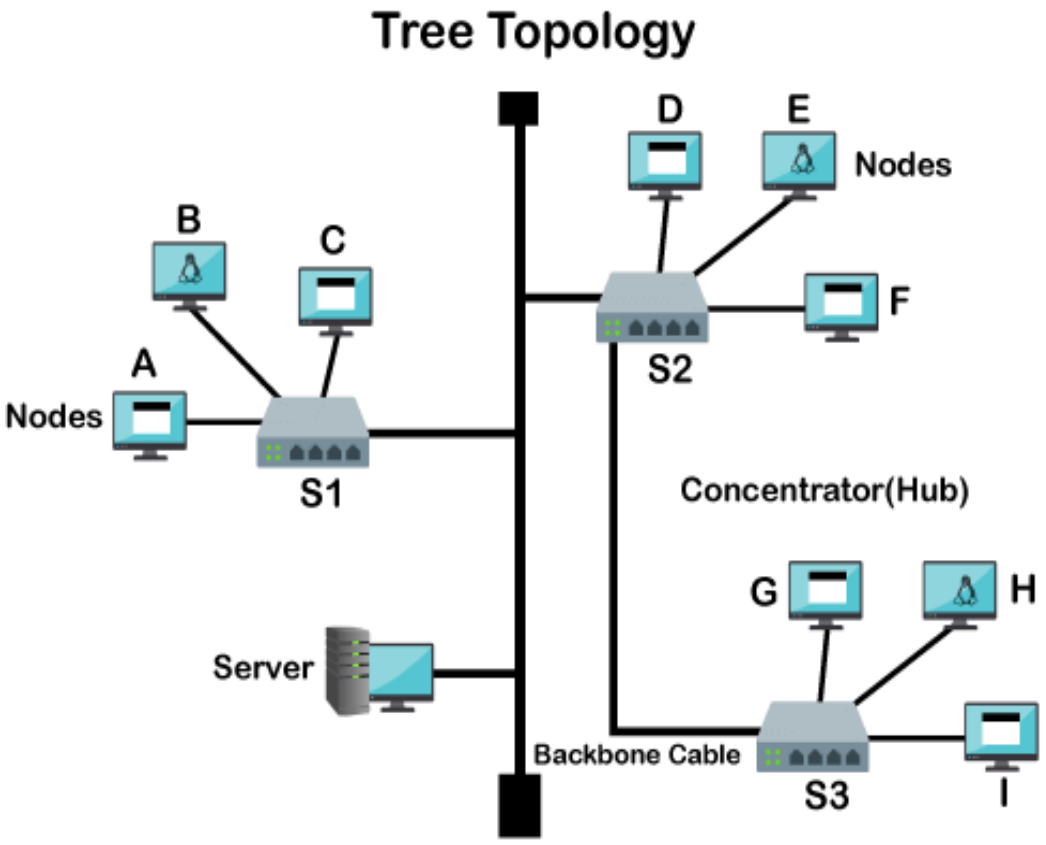


Fig 1.15 TREE TOPOLOGY

Advantages of TREE Topology

1) More devices to be attached to a single central hub.
2) It increases the distance a signal can travel between devices.
3) It allows the network to isolate and prioritize the communication from different computers
   e.g., cable TV.

Disadvantages of TREE Topology

1) Overall length of each segment is limited by the type of cabling used.
2) If the backbone line breaks, the entire segment goes down.
3) More difficult to configure and wire than other topologies.

1.7 Data Flow Modes

Transmission mode means transferring of data between two devices. It is also known as communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

There are three types of transmission mode:

1) Simplex Mode

2) Half-Duplex Mode

3) Full-Duplex Mode

Simplex Mode

In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

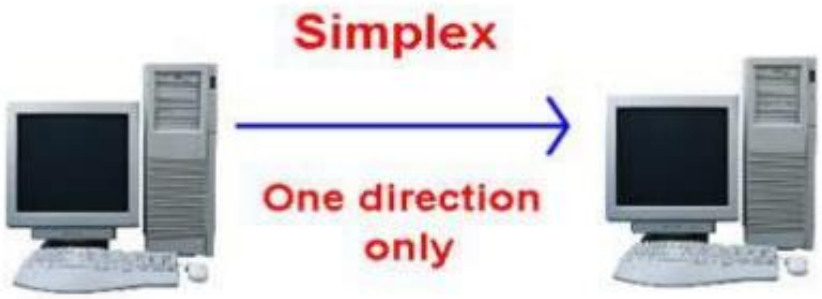


Fig 1.17 Simplex

Half-Duplex Mode

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

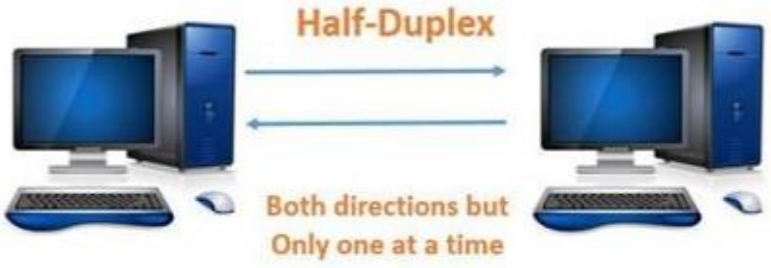


Fig 1.18 Half Duplex

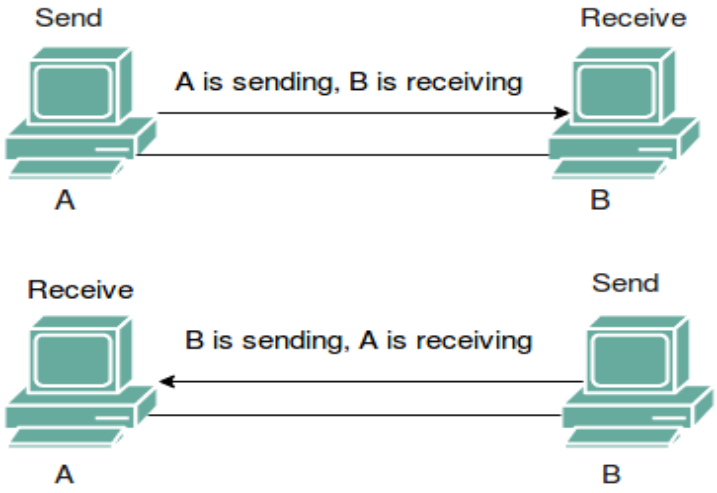


Fig 1.19 Half Duplex Example

Full-Duplex Mode

In full-duplex mode, both stations can transmit and receive simultaneously. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and other for receiving. Or the capacity is divided between signals travelling in both directions.

Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel however must be divided between the two directions. Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

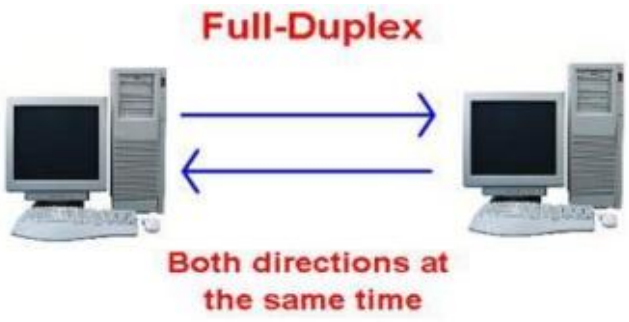


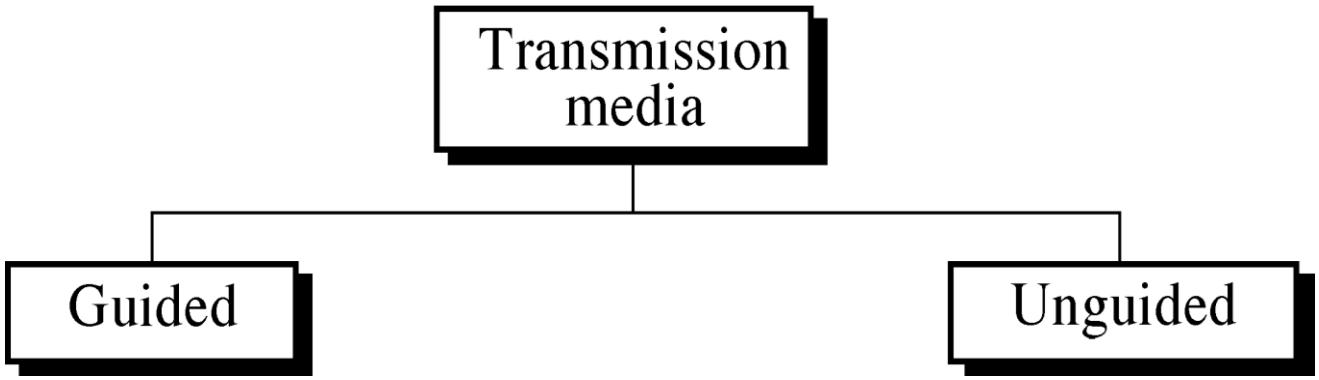
Fig 1.20 Full Duplex

Unit-2 Transmission Media

2.1 Transmission Media: Introduction

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium is the air in a classroom when a professor delivers lectures to students.

Computers and other telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy, which is propagated through Transmission Media.



Guided Media

Guided transmission media uses a “cabling” system that guides the data signals along a specific path. Guided media is also known as “Bounded Media”. Guided media are those that provide medium of data transmission from one device to another. It includes twisted pair cable, coaxial cable and fiber optic cable.

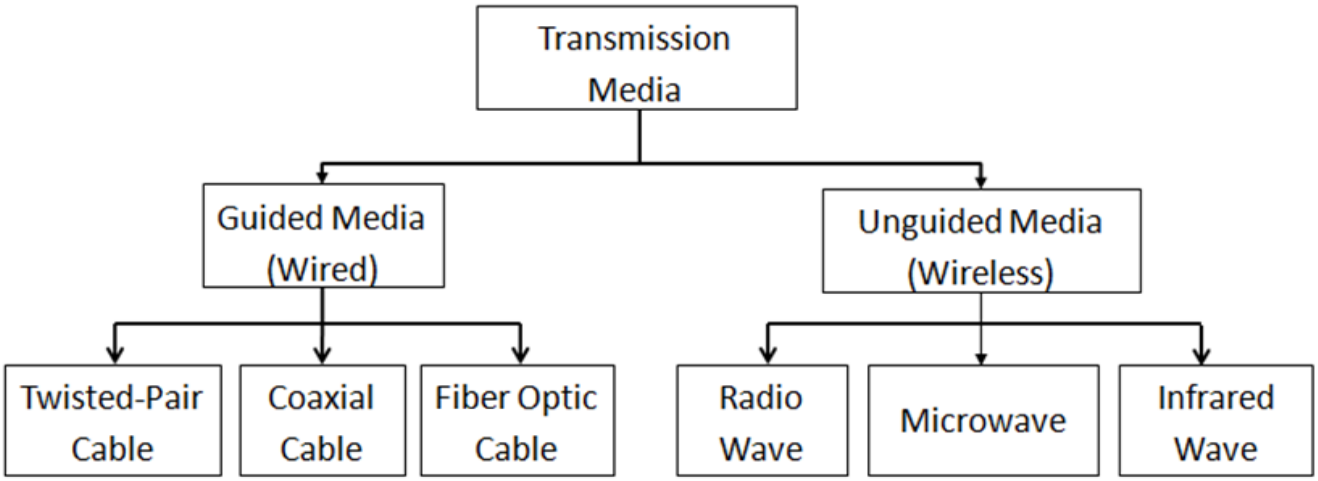
Unguided Media

Unguided media transports electromagnetic waves without using a physical conductor. Signals are normally broadcast through air and thus are available to anyone who has a device capable of receiving them. Unguided media is also known as “Unbounded Media”. This type of communication is often referred to as wireless communication.

2.1.1 Definition

Guided transmission media uses a “Cabling” system that guides the data signals along a specific path. Guided media is also known as “Bounded Media”.

2.1.2 Classification

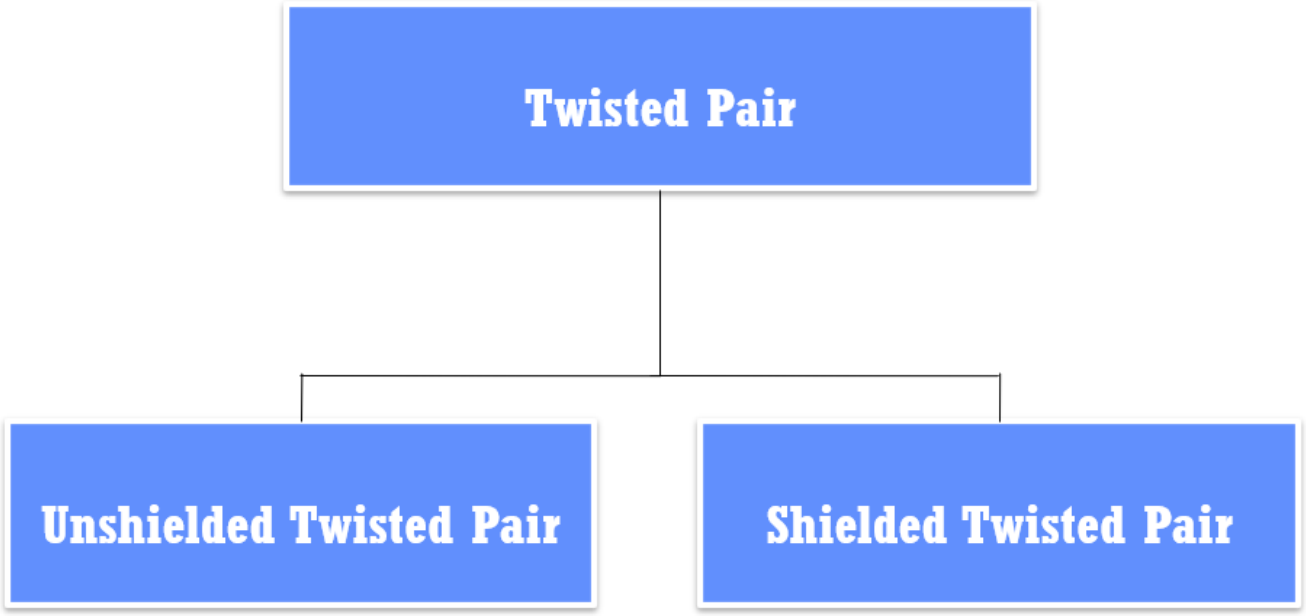


2.2 Guided Media

Guided media are those that provide medium from one device to another. It includes twisted pair Cable, coaxial cable and fiber optic cable.

2.2.1 Twisted Pair Cable

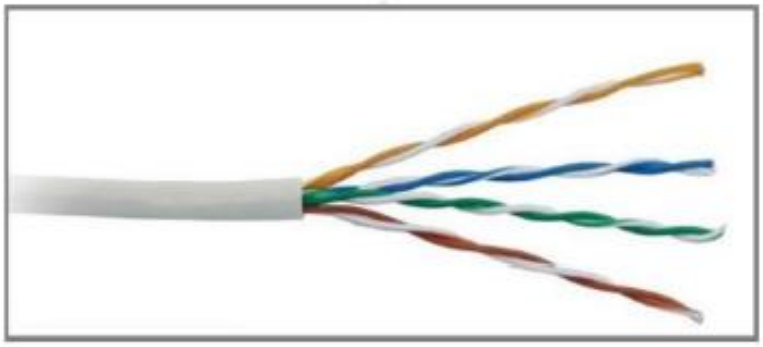
Twisted pair cable comes in two forms unshielded twisted pair cable and shielded twisted pair cable.



Unshielded Twisted Pair Cable (UTP)

It is the most common type of telecommunication medium in use today. It is used mostly in telephone system; its frequency range is suitable for transmitting both data and voice. Frequency range suitable for UTP is 100Hz to 5MHz.

As shown in fig. twisted pair consists of two conductors each with its own coloured plastic insulation. One potential problem of UTP is that its wire can be affected by EMI (Electromagnetic interference) from devices. This can create a noise over wires, which can damage the signal.

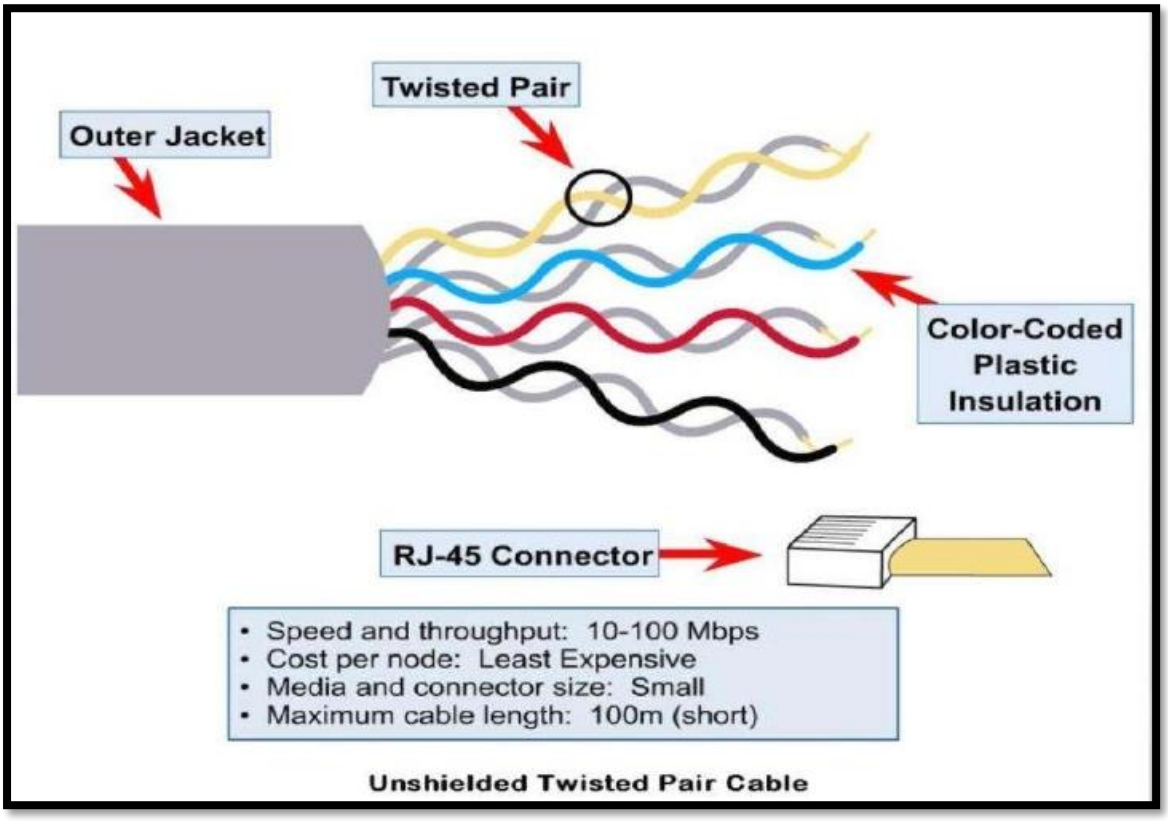


Advantages of UTP

1) Low cost
2) Easy to use
3) Flexible
4) Easy to install

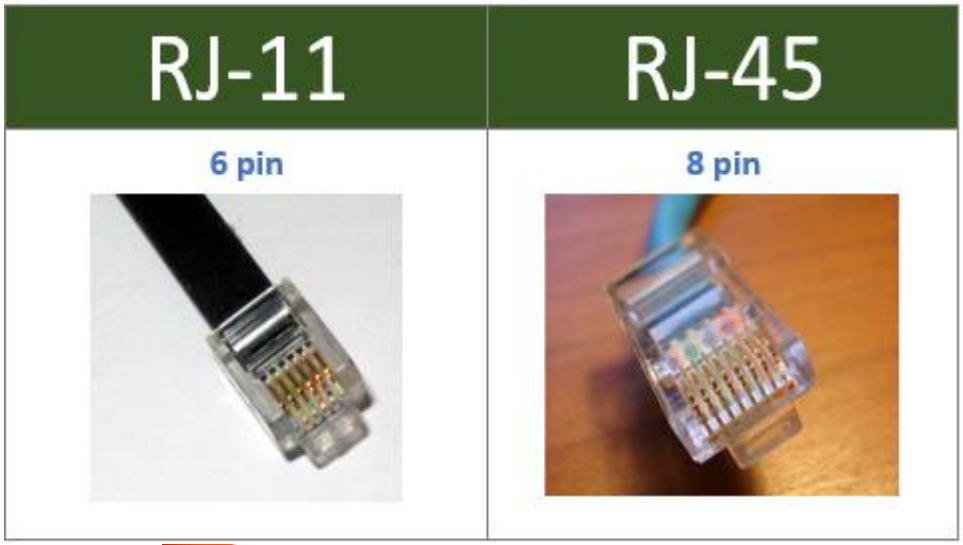
Dis-advantages of UTP

1) Limited to only 100 mts.
2) Most affected by interference.
3) Easy to tap into.



UTP Connectors

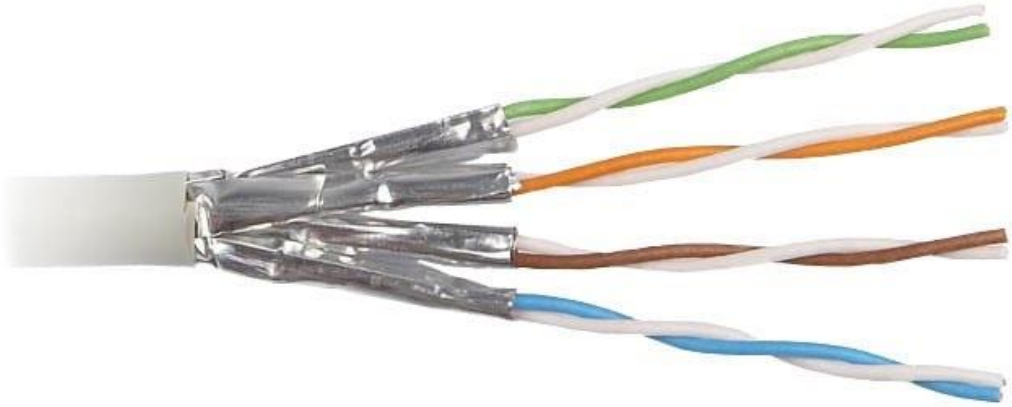
UTP is most commonly connected to network devices via a type of snap-in plug like that which is used with telephone jacks. Each wire in a cable is attached to one conductor (or pin) in the connector. The most frequently used is an RJ45 (Registered Jack). Connector with eight conductors, one for each wire of four twisted pair as shown in fig.



Shielded Twisted Pair Cable (STP)

STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors, which are a higher quality and more protective jacket than UTP has. This gives STP excellent insulation to protect the transmitted data from outside interference.

STP is less susceptible to electrical interference and supports higher rates over longer distance than UTP. Materials and Manufacturing requirements make STP more expensive than UTP, but less susceptible to noise. STP has the same quality consideration and uses the same connectors as UTP, but the shield must be connected to ground.

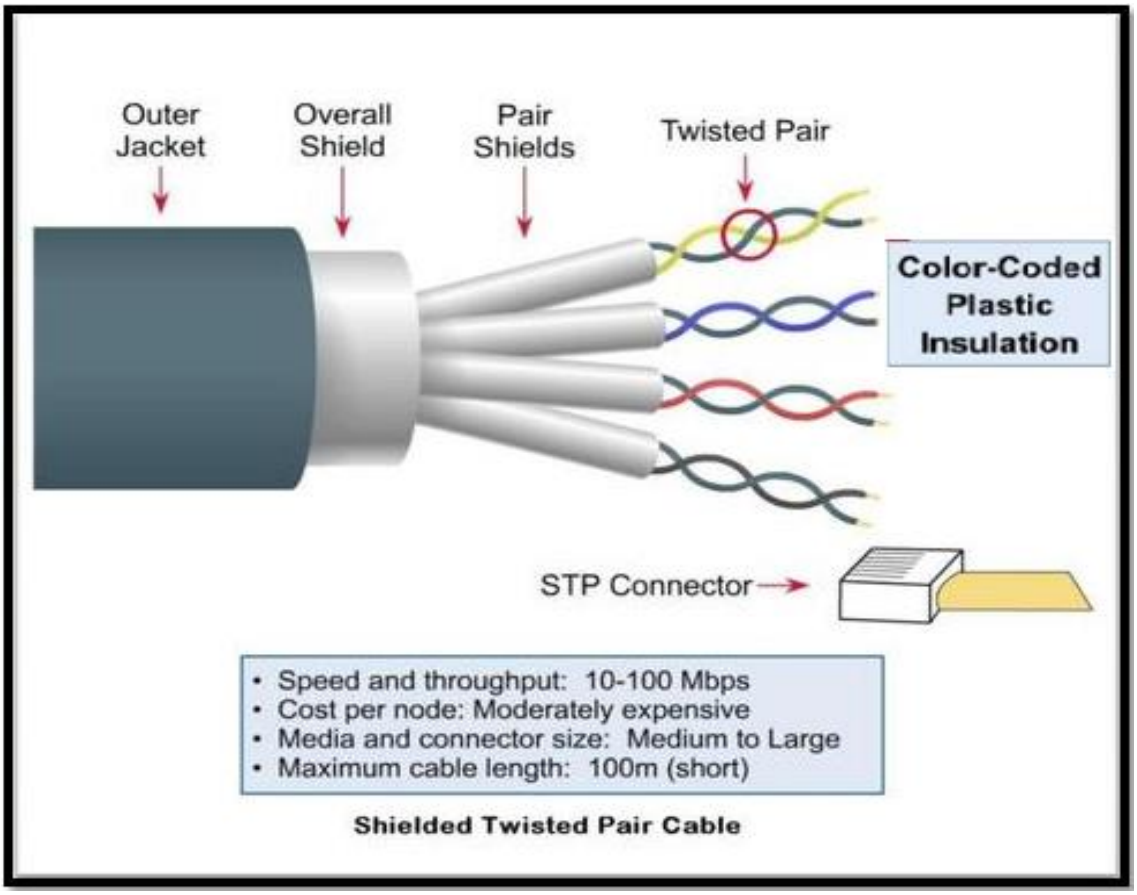


Advantages of STP

1) Less affected by interference.
2) Difficult to tap into.

Dis-advantages of STP

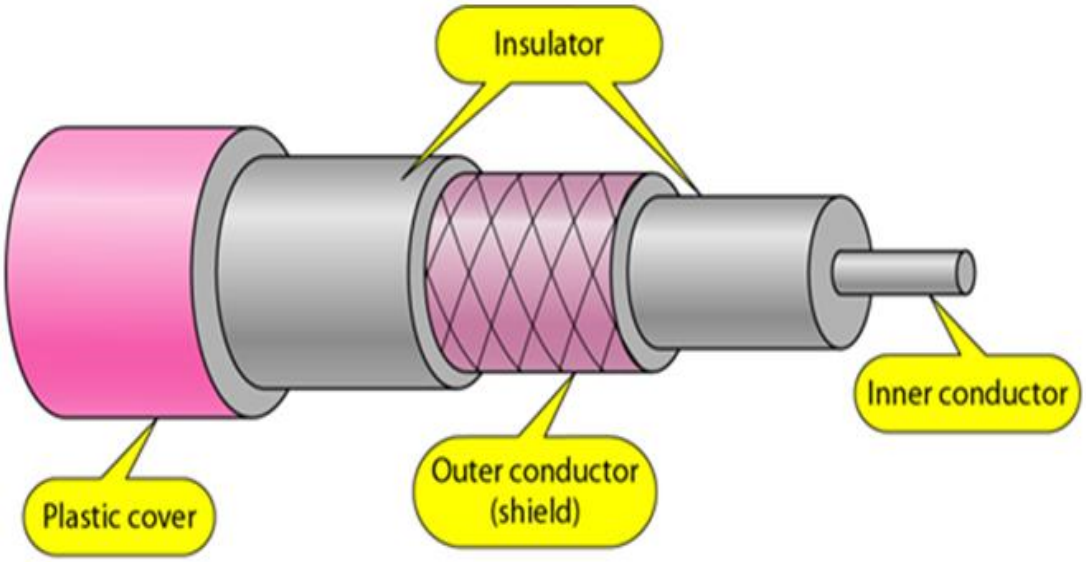
1) High cost
2) Difficult to use
3) It is not Flexible
4) Difficult to install



2.2.2 Coaxial Cable

Co-axial cable has better shielding than twisted pairs, so it can span longer distances at higher speed. coaxial cable carries signals of higher frequency range than twisted pair cable. Frequency range suitable for coaxial cable is 100 KHz to 500MHz.

Coaxial cable has central core conductor of solid or standard wire (usually copper) enclosed in an insulating sheath, which is in turn encased in an outer conductor of metal foil, braid or combination of two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath and whole cable is protected by plastic cover.



There are two types of coaxial cable:
1) Thin (Thinnet)
2) Thick (Thicknet)

Thinnet Coaxial Cable

It is a flexible coaxial cable about 0.25 inches thick. This type of coaxial cable is flexible and easy to work with; it can be used in almost any type of network installation almost in BUS topology.

Thinnet coaxial cable can carry a signal up to approximately 185 meters (about 607ft) before the signal starts to suffer from attenuation. Thinnet is included in a group that referred to as the RG-58 (radio grade) family and has 50-ohm impedance. Commonly used for digital transmission.

Thicknet Coaxial Cable

Thicknet is relatively rigid coaxial cable about 0.5 inches in diameter. Thick net can carry signal for 500 meters [about 1640 ft] Therefore, because of thicknet's ability to support data transfer over linger distance it is sometimes used as backbone to connect several smaller thinnet based networks.

A device called a transceiver connects the thinnet coaxial to the larger thicknet coaxial cable. RG-8, RG-9 and RG-11 used for thicknet coaxial cable. 75-ohm commonly used for analog transmission.

Advantages of Coaxial Cable

1) Coaxial cable is the most widely used in n/w cable.
2) Coaxial cable is relatively inexpensive, light, flexible and easy to work with.
3) It can be easily installed.
4) Coaxial cable is good choice for longer distance and for reliably supporting higher data rates.

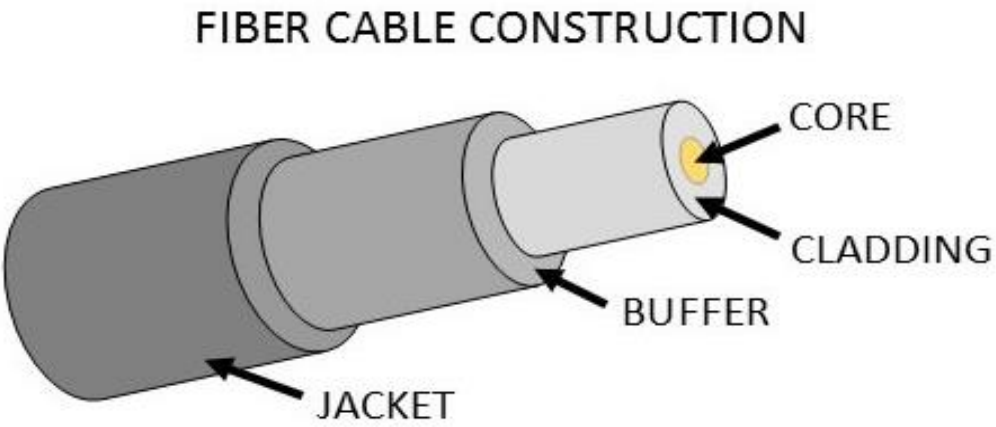
Dis-Advantages of Coaxial Cable are

1) Coaxial cable is harder to work with.
2) It does not allow running cable from every office to a central location.

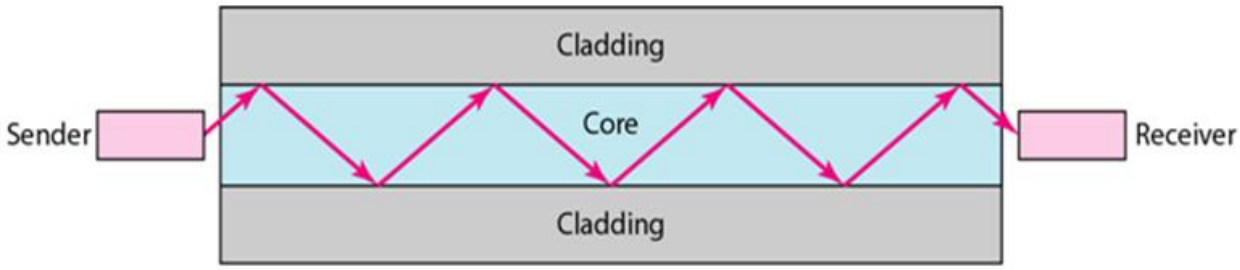
2.2.3 Fiber Optic cable

Fiber optic cable is similar to coax expect without braided mesh conductor as shown in fig. above. Following figure shows the composition of typical fibre optic cable. At the centre is the glass

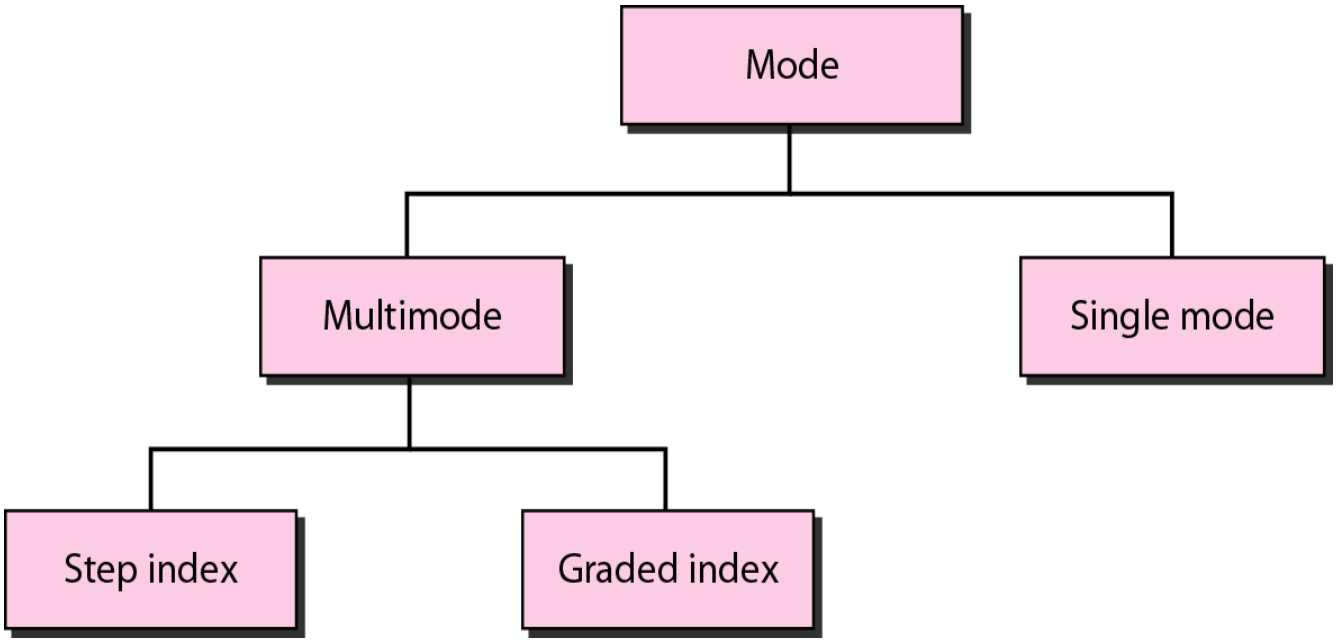
core through which light propagates. In multimode fibres, the core is 50 microns in diameter, about the thickness of human hair. In the single mode fibre, the core is 8 to 10 microns.



A core is surrounded by glass cladding with lower refractive index than the core, to keep all the light in the core. Next comes, a thin plastic jacket to protect the cladding. As shown in fig. fibers are typically grouped together in bundles protected by an outer sheath. Two types of light sources can be used for signaling, (LED and diodes) LED and semiconductors lasers.



Propagation Modes have two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.



Multimode

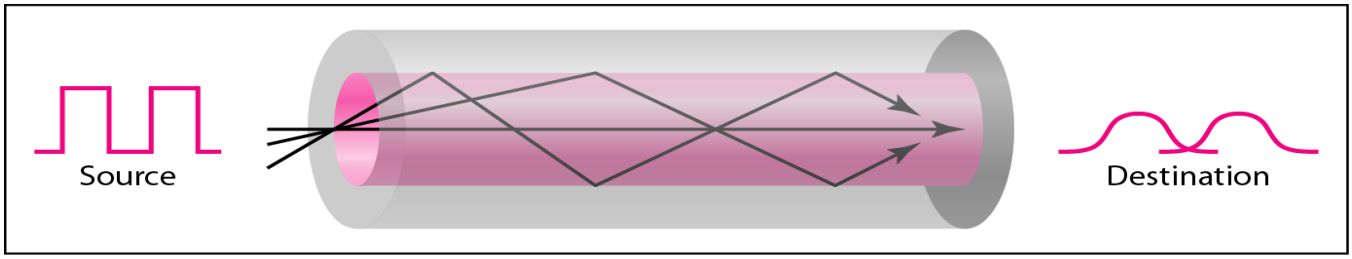
Multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core. The density of the core remains constant from the centre to the edges.

A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion.

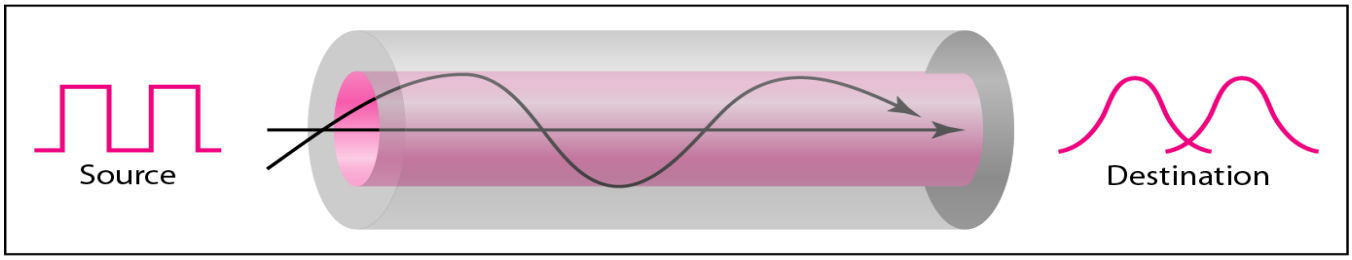
Single-Mode

It uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction).

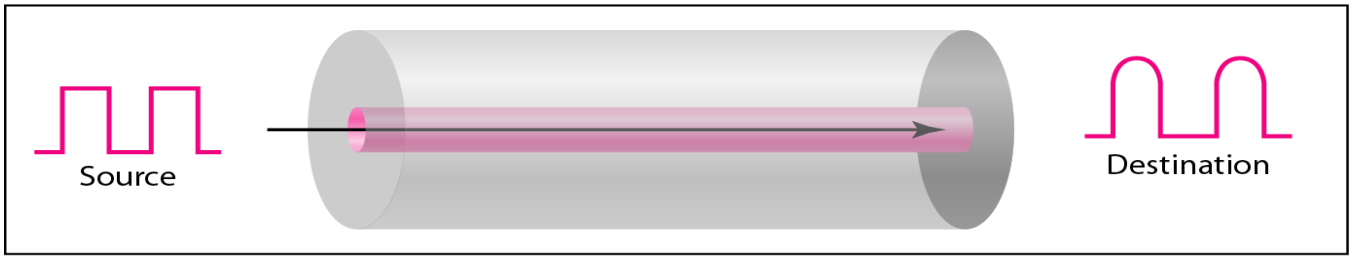
The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

Advantages of Fiber Optic Cable

The major advantage offered by fiber optic cable over twisted pair and coaxial cable.

1) **Less weight:** Fiber is much lighter than copper. If we take twisted pair for the distance of two km then its weight is 8000 kg. But two fibers have more capacity and weight is only 100 kg.
2) **Noise Resistance:** Fiber optic transmission uses light rather than electricity, so noise is not a factor.
3) **Less Signal attenuation:** A signal can run for miles without requiring regeneration.
4) **Higher Bandwidth:** It supports higher bandwidth and hence has higher data rates than either twisted pair or coaxial cable.
5) **Excellent Security:** it provides excellent security because they do not leak light and they are quite difficult to tap.

Disadvantages of Fiber Optic Cable

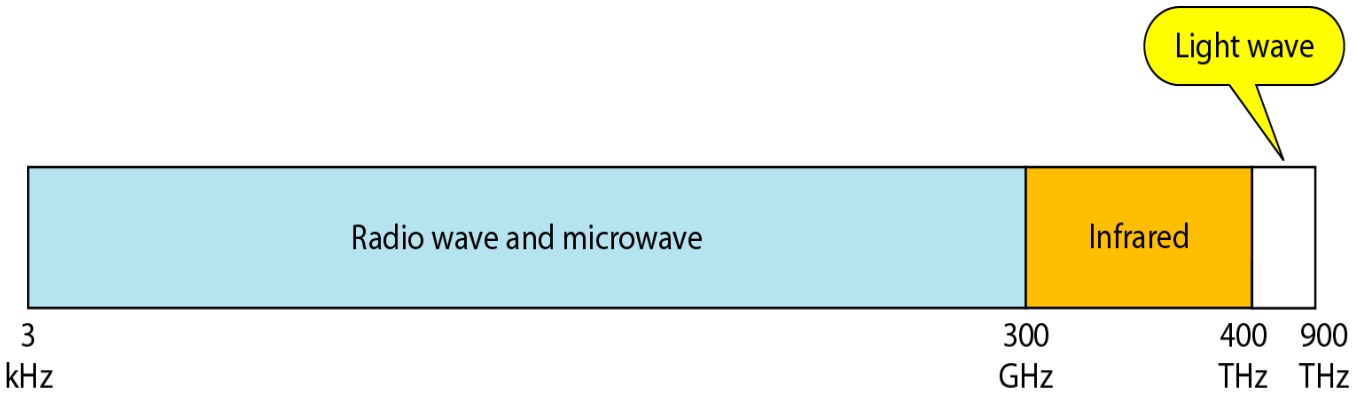
1) **Cost:** Fiber optic cable is expensive.

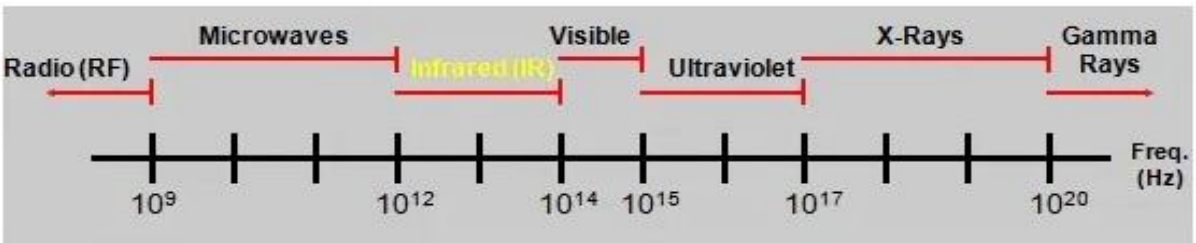
2) **Installation/Maintenance:** Suitably skilled and qualified person is required for maintaining and installing fiber optic cable.
3) **Unidirectional (one direction):** Propagation of light is unidirectional. If we need bi-directional communication then two fibers are needed.

2.3 Unguided Media

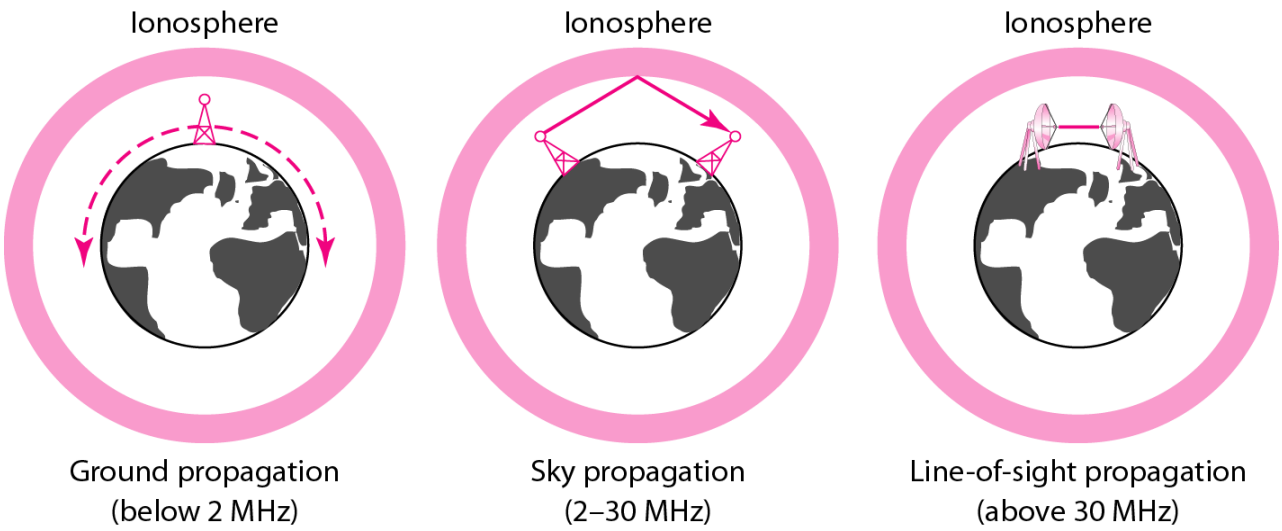
Unguided media transport electromagnetic waves without using a physical conductor. Signals are normally broadcast through air and thus are available to anyone who has a device capable of receiving them. This type of communication is often referred to as wireless communication. The characteristics of this media make them good alternative in situations where it is difficult or impossible to use cables.

Unguided media broadly classified into following categories:
1) Radio wave
2) Microwaves
3) Infrared



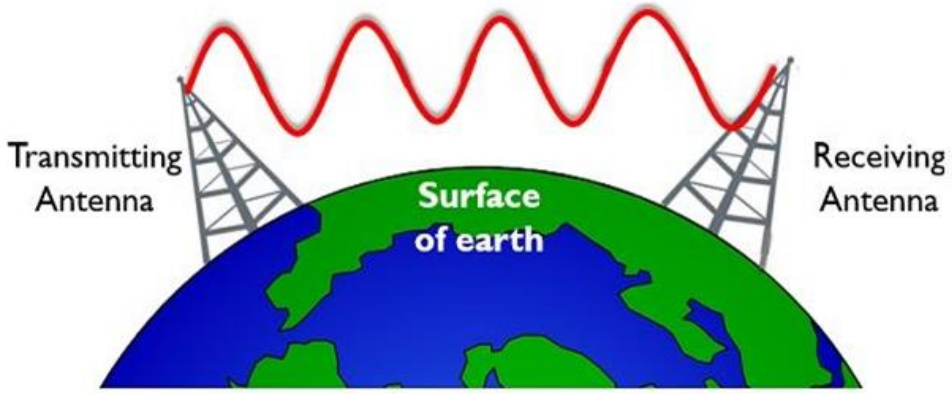


Unguided signals can travel from source to destination in several ways. There is ground propagation, sky propagation, and line-of sight propagation.



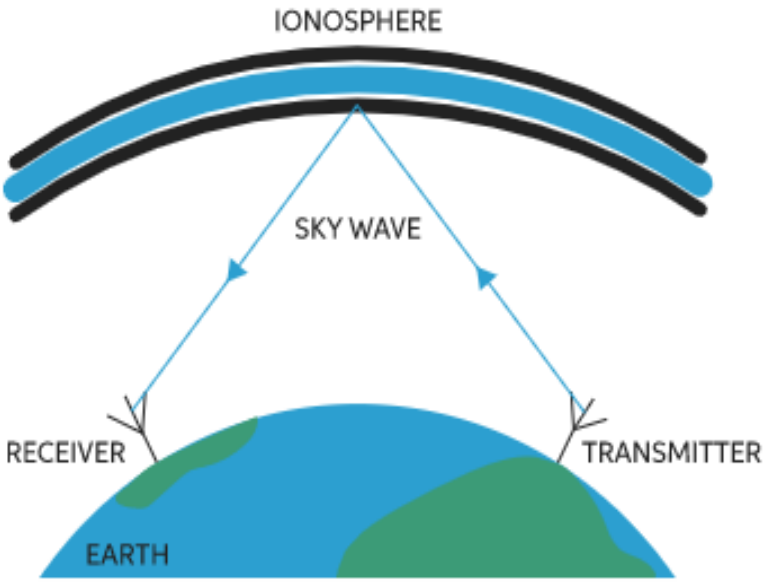
Ground Propagation

In this propagation, radio waves travel through lowest portion of atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of planet. Distance depends on the amount of power, the greater the distance.



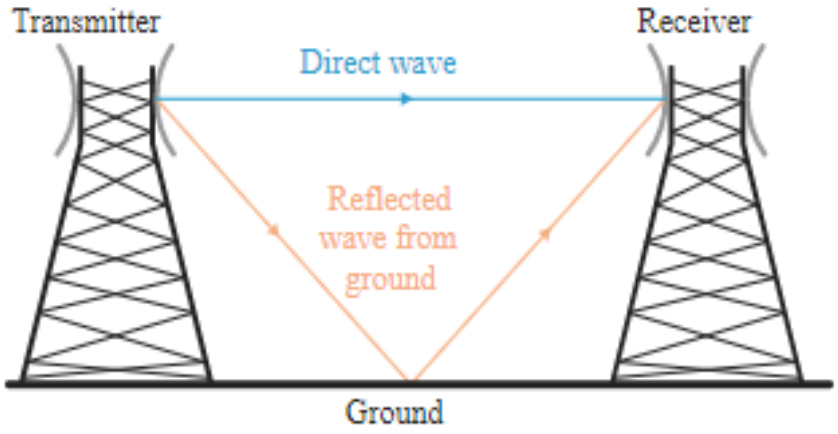
Sky Propagation

In this propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower power output.



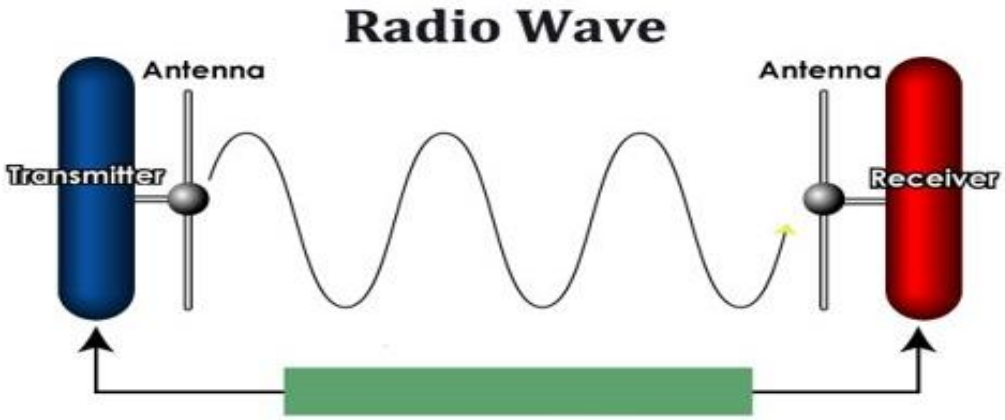
Line of Sight Propagation

In this propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by curvature of earth. Line-of-sight propagation is tricky because radio transmission cannot be completely focused.



2.3.1 Radio Waves

Radio waves are electromagnetic waves occurring on radio frequency portion of the electromagnetic spectrum. A common use is to transport information through the atmosphere or outer space without wires. Radio waves are distinguished from other kinds of electromagnetic waves by their wavelength, a relatively long wavelength in an electromagnetic spectrum.



Although there is no clear-cut differentiation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves. Waves ranging in between 1 and 300 GHz are called microwaves. However, the behavior of the waves, rather than frequencies, is a better criterion for classification. Radio waves are easy to generate, can travel a long distance, and penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.

Radio waves are also Omni directional, meaning that they travel in all directions from the source, so that the transmitter and receiver do not have to be carefully aligned physically. Radio waves propagate in the sky mode.

Advantages of Radio Waves

1) Radio waves, particularly those waves that propagate in the sky mode, can travel long distances, for example AM radio.
2) Radio waves, particularly those of low and medium frequencies, can propagate walls, so they are widely used for communication, both indoors and outdoors.
3) Radio waves are also Omni directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna can send waves that can be received by any receiving antenna.

Disadvantages of Radio Waves

1) Radio waves are also Omni directional, meaning that they travel in all directions from the source. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using same frequency or band.
2) Radio waves can penetrate the walls. So, we cannot isolate a communication to just inside or outside a building.
3) The radio wave band is relatively narrow, just under 1 GHz, compared to the microwave band. When this band is divided into sub bands, the sidebands are also narrow, leading to low a data rate for digital communications.

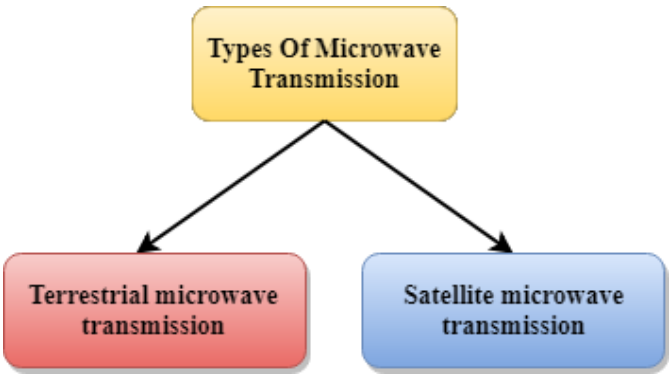
Application of Radio Waves

The Omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.

1) AM and FM radio.
2) Television broadcasts.
3) Cordless phones.
4) Paging.
5) GPS receivers.
6) Police radio.
7) Wireless clocks etc.

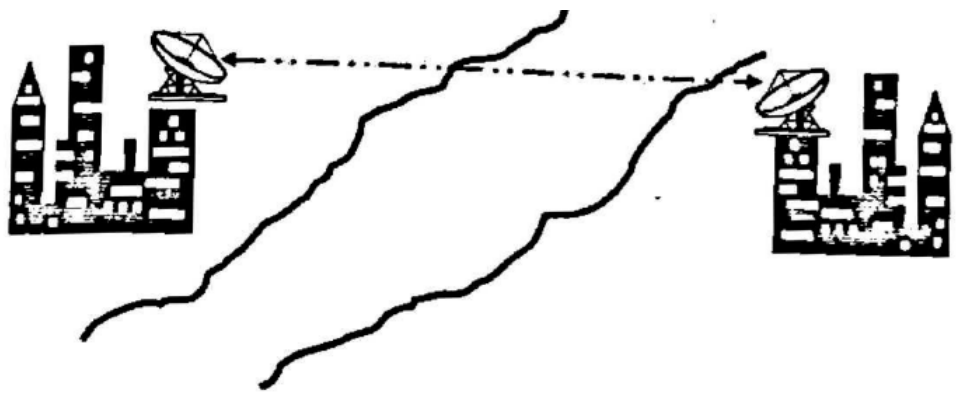
2.3.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Micro waves are unidirectional. When an antenna transmits micro waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned without interfering with another pair of aligned antennas. Microwave's uses line of sight propagation.



Terrestrial Microwave

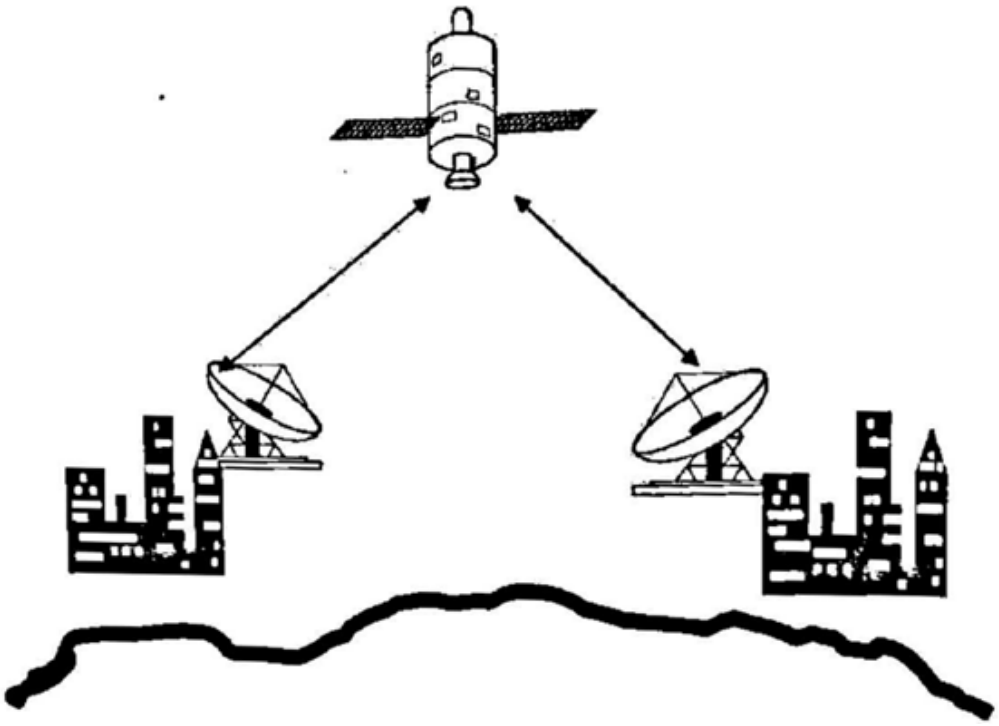
Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another. Microwaves are unidirectional as the sending and receiving antenna is to be aligned. It works on the line-of-sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.



Terrestrial Microwave

Satellite Microwave

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. 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.



Satellite Microwave

Advantages of Microwaves

1) Micro waves are unidirectional, and sending and receiving antennas need to be aligned, so they are not interfering with another pair of aligned antenna.
2) The micro wave's band is relatively wider, compared to the radio wave band. When this band is divided into sub bands, the sidebands are also wider, leading to higher data rate for digital communications.
3) Micro waves are relatively inexpensive and simple to install.

Disadvantages of Microwaves

1) The micro waves travel in a straight line, if the towers are too far apart, the earth will get in the way. Consequently, repeaters are often needed for long distance communication periodically.
2) Very high frequency micro waves cannot able to penetrated walls. Its disadvantage if receivers are inside the buildings.

Application of Microwaves

1) Cellular phones
2) Satellite networks
3) Wireless LANs

2.3.3 Infrared Waves

Electromagnetic waves having frequencies from 300 GHz to 400 THz are called Infrared waves. Infrared waves are widely used for short-range communication. The remote controls used on televisions, VCRs, and stereos all use infrared communication. Infrared waves are line of sight propagation.

Advantages of Infrared Waves

1) Infrared waves are relatively directional, cheap, and easy to build.
2) Infrared waves having high frequency, so they are not able to penetrate the walls. So, Infrared system in one room will not interfere with a similar system in adjacent room.
3) Infrared waves are useful for short range communication.
4) It is more secure against taping.
5) It is useful to communicate wireless keyboard and mouse with the PC by using Infrared port.

Disadvantages of Infrared Waves

1) Infrared waves are useless for long range communication.
2) They do not pass-through solid objects.
3) We cannot use infrared waves outside buildings because the sun's ray contains infrared that can interfere with the communication.

Application of Infrared Waves

1) The remote controls used on televisions, VCRs, and stereos are based on Infrared.
2) Short-ranged wireless communication e.g., wireless keyboard and mouse in PC by using Infrared port.
3) Used in military, such as: target acquisition, surveillance, homing and tracking.
4) Used in thermal efficiency analysis, remote temperature sensing, spectroscopy, and weather forecasting.

Unit-3 Network Devices

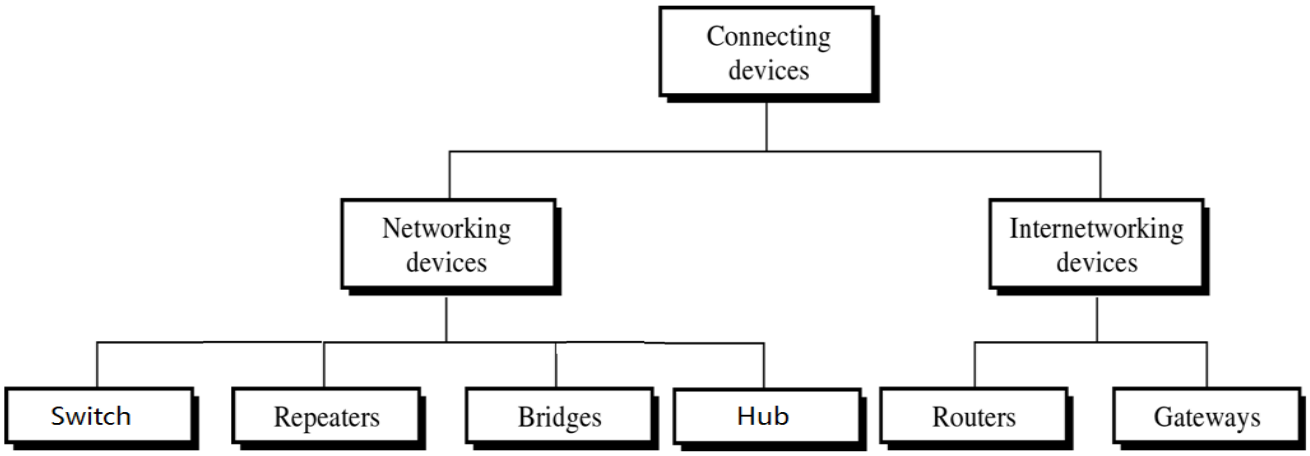
3.1 Network Devices

Computer networks usually require a great deal of equipment to function properly. LANs and WANs typically include network interface cards, repeaters, hubs, bridges, routers and switches. The network device is one kind of device used to connect devices or computers together to transfer resources or files like fax machines or printers.

3.1.1 Definition

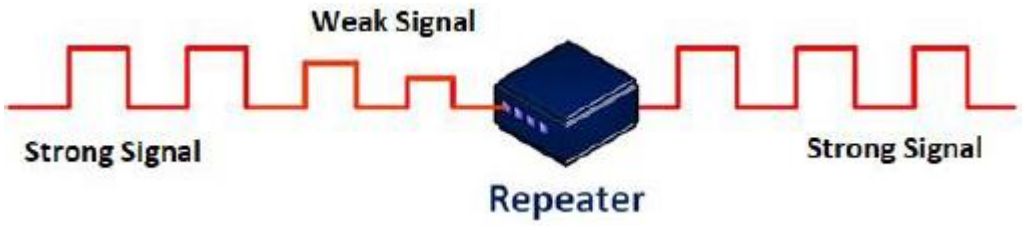
Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. Devices which are used to form a network are called Networking devices.

3.1.2 Types

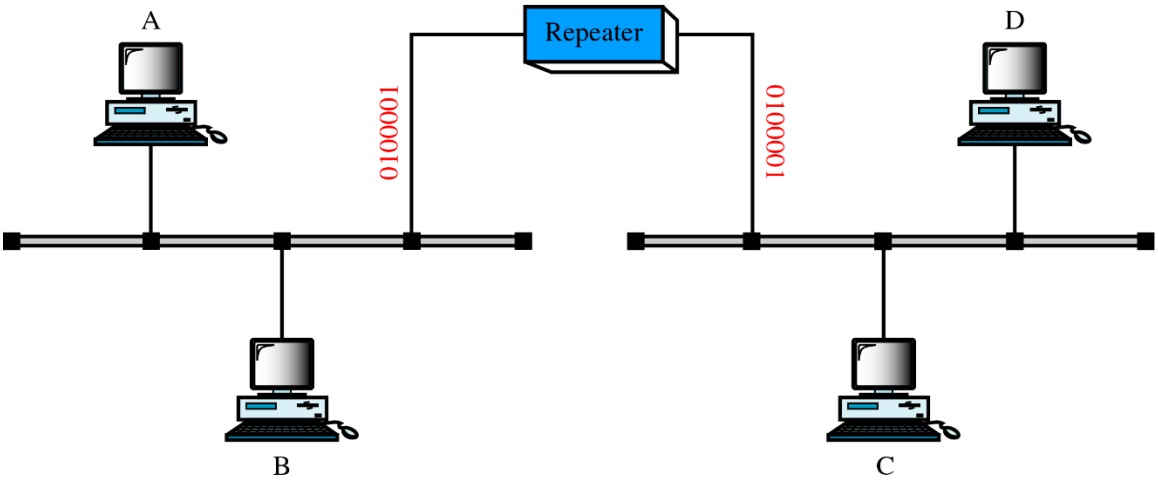


Repeater

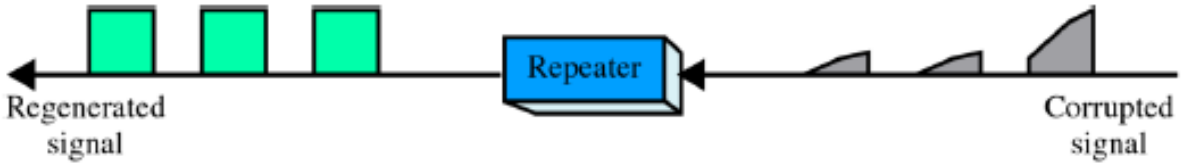
Repeater is an electronic device, which operates, only in physical layer of the OSI model. Signal that carries information within a network can travel a fixed distance before noise can affect integrity of the data.



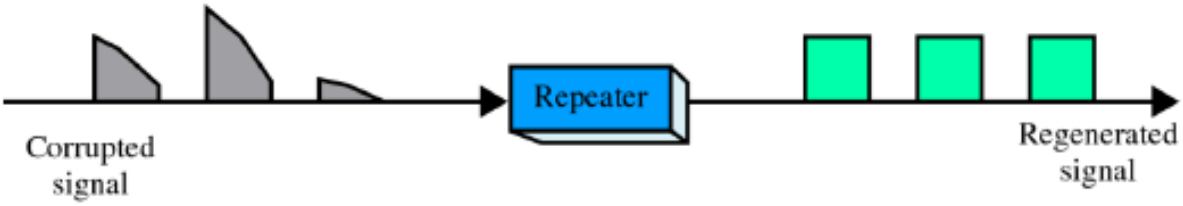
A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss.



Repeater installed on a link receives the signal before it becomes too weak or corrupted, regenerates the original bit pattern & puts the new refreshed copy back onto the link. A repeater allows us to extend only the physical length of a network. A repeater does not change the functionality of the network.



(a) Right-to-left transmission.



(b) Left-to-right transmission.

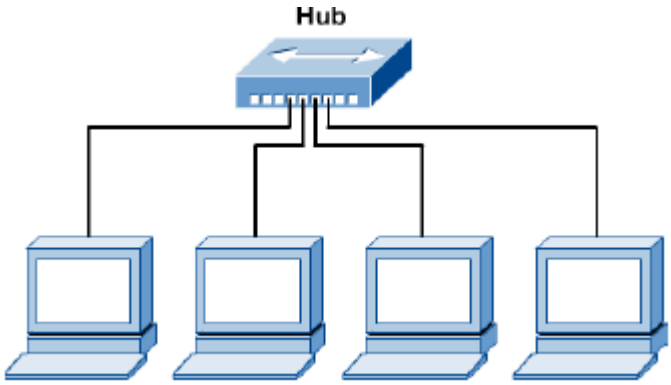
Repeater is not an Amplifier

An amplifier cannot differentiate between the intended signal and noise signal, means it amplifiers equally everything fed into it. A repeater does not amplify the signal, it regenerates it. When it receives a noise signal or corrupted signal, it creates a copy bit for bit at the original strength. The location of a repeater on a link is important. A repeater must be placed so that a signal reaches it before any noise changes the meaning of any of the bits.

Hub

A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at a port, it is copied to the other ports so that all segments of the LAN can see all packets.

Hub is used to create connections between stations in a physical star topology. Hub is a central network device that connects network nodes. It is also referred as concentrators. It enables central network management. It can have multiple inputs & outputs all active at one time. It permits large number of computers to be connected on a single or multiple LANs. It enables high speed communication and also provides connection for several different media types (coaxial, fiber optic, twisted pair).



Types of Hub

1) Active Hub
2) Passive Hub
3) Intelligent Hub

Active Hub

Most hubs are active in that they regenerate and retransmit the signals the same way a repeater does. In fact, because hubs usually have eight to twelve ports for computers to connect to, they are often called multiport repeaters. Active hubs need electrical power to run. It contains a repeater which is h/w device that regenerates the received bits before sending to the link.

Passive Hub

It provides physical connection between the attached devices. Passive hubs act as connection points and do not amplify or regenerate the signal; the signal passes through the hub. Passive hubs do not require electricity to run.

Intelligent Hub

Intelligent hubs are enhanced active hubs. It will accommodate several different types of cables. A hub-based network can be expanded by connecting more than one hub. It also has functions which can add intelligence to a hub like hub management.

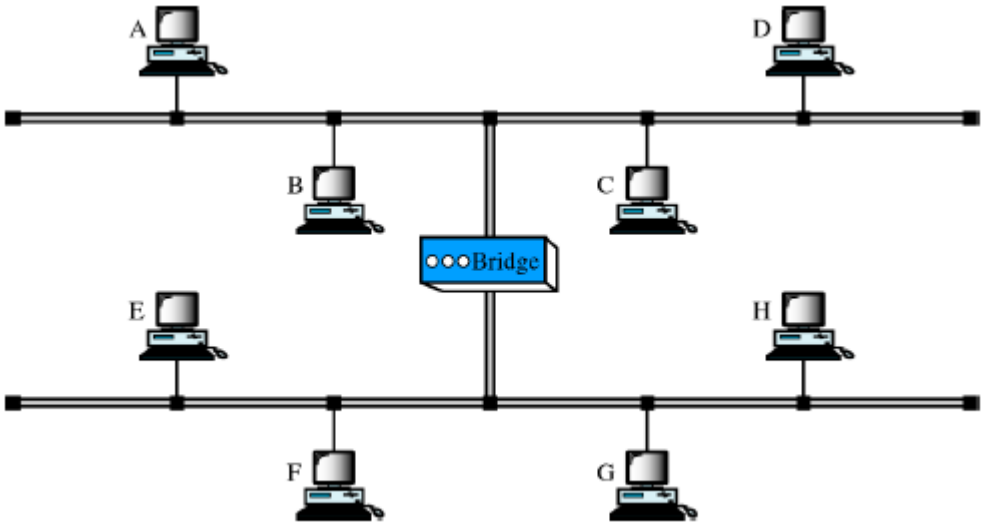
Limitation of Hub

1) It does not have mechanisms such as collision detection and retransmission of packets.
2) It cannot connect different network architectures.
3) It broadcasts message to all computers and there is no privacy.

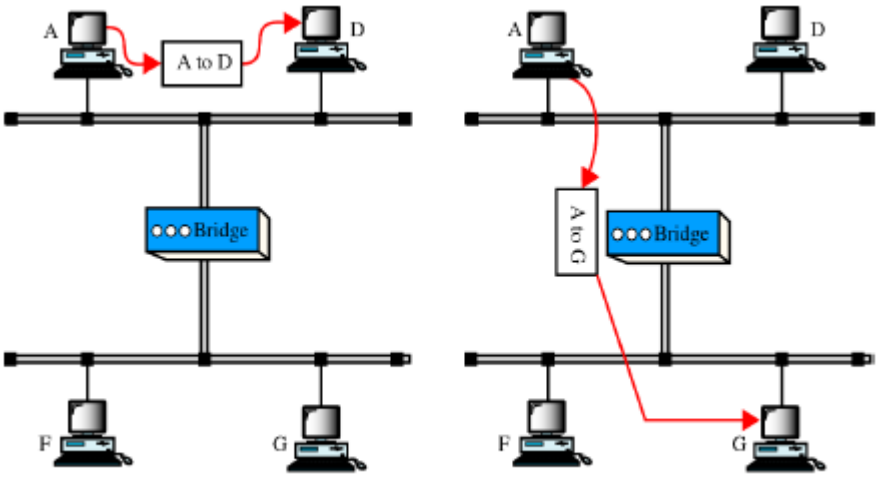
Bridge

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.

Bridges operate in both the physical and data link layer of the OSI model as shown in figure. A bridge connects two or more LANs. Bridges can divide a large network into smaller segments. Bridges contain logic (software) that allows them to keep the traffic for each segment separate, in this way they filter traffic. Bridges transmit frames only to the separate segment. Like this way bridges filter the traffic (handle traffic). Bridges can also provide security through this partitioning of traffic (Means preventing unauthorized access).



Bridges operates at the data link layer, so giving it access to the physical addresses of all stations connected to it. When a frame enters a bridge, it regenerates the signal and it checks the address of the destination and forwards the new copy only to the segment to which address belongs. As a bridge found frame, it reads the address contained in the frame & compares that address with a table of all stations on both segments. When the bridge finds correct match, it find to which segment the station belongs and send the frame only to that segment.



Bridge must have a look up table that contains the physical addresses of every station connected to it. The table also indicates to which segment each station belongs. From figure if packet from A passed to the device D through the bridge. In this case, both devices are on the same segment (upper segment). So packet is blocked from crossing into the lower segment. Because no need to pass on lower segment. Suppose packet generated by device A is send to device G. At this time bridge allows the packet to cross and send packet to the lower segment. So finally it is received by station G.

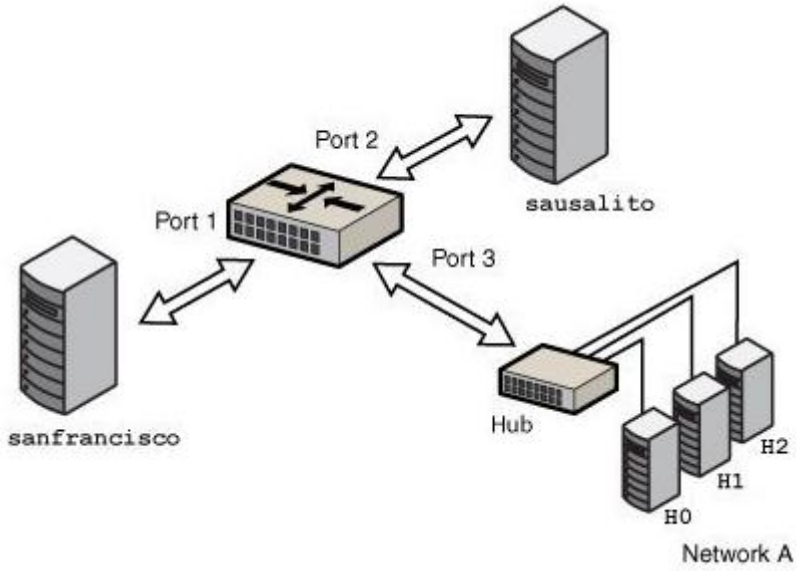
Types of Bridges

1) Simple Bridge
2) Multiport Bridge
3) Transparent Bridge

Simple Bridge

A simple bridge is the most primitive and least expensive types of bridge. A simple bridge links two segments. It contains a table that lists the physical addresses of all stations connected with the bridge. In this bridge, physical addresses must be entered manually that makes them primitive. Before a simple bridge can be used, an operator enters the addresses of every station. In this bridge, updating of the devices is time consuming process. Whenever a new station is added, the table must be modified means new entry

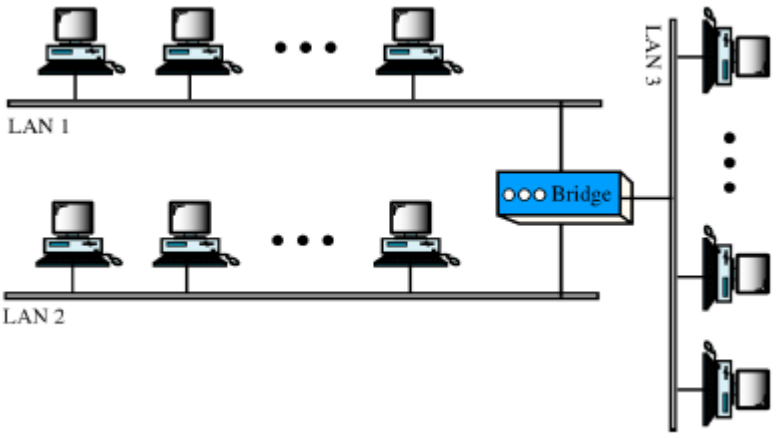
for new device. If station is removed then also address must be deleted from the table. So, installation and maintenance of simple bridges are time consuming.



Multiport Bridge

Multiport bridge can be used to connect more than two LANs. In this bridge three tables are created, each one holding the physical address of stations reachable through the corresponding port. Transparent Bridge. Transport Bridge builds its table of physical station addresses on its own as it performs its bridge functions. Table is automatically built by frame movements in the network. When transparent bridge is first installed, its table is empty. When it receives packet it looks at source & destination address. Destination address is used for forwarding decision to the particular segments. Source address is used for adding entries to the table and for updating table. As it reads source address it notes which side the packet came from and the segment to which it belongs.

It checks destination address to decide where to send packet. If it is not inside table, it sends the packet to all of the station on both segments except sender (source) station. When the first packet is transmitted by each station, the bridge makes entries inside the table with corresponding segment. So, at last table completed with all station addresses and segment. Next packet send by each station refers the table entry.

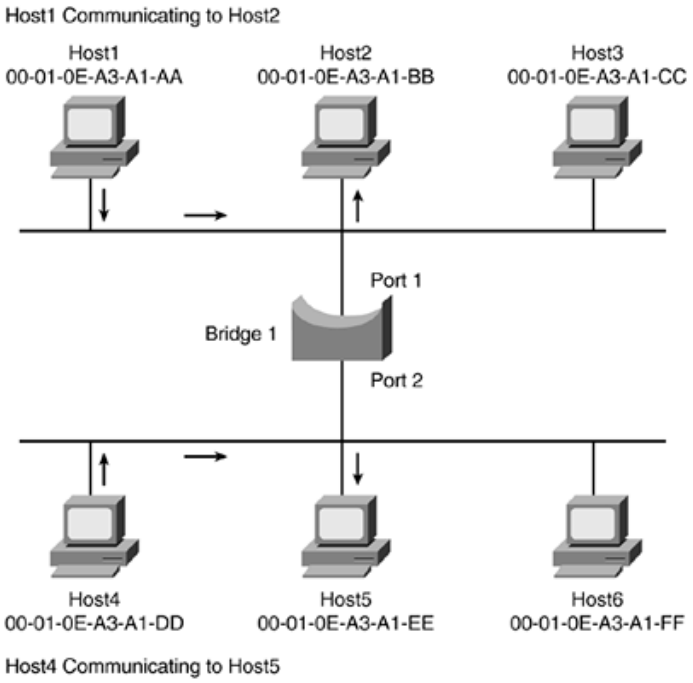


Transparent Bridge

A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary.

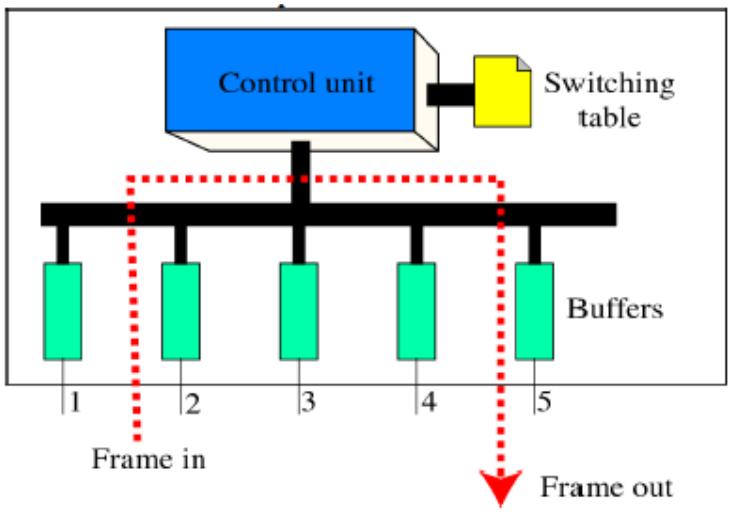
According to the IEEE 802.1 d specification, a system equipped with transparent bridges must meet three criteria:

1) Frames must be forwarded from one station to another.
2) The forwarding table is automatically made by learning frame movements in the network.
3) Loops in the system must be prevented.



Switch

A network switch is a computer networking device which connects devices together on a computer network by using packet switching to receive, process and forward data to the destination device.
Switches provide bridging functionality with greater efficiency. It acts as multiport bridge to connect devices or segments in a LAN. Switch has a buffer for each link to which it is connected. Switch operates in Data Link Layer of the OSI model. When it receives a frame, it stores the frame in buffer of receiving link & checks address to find outgoing link. If the outgoing link is free the switch sends the frame to that particular link.



Two different Strategies of switch

1) Store and Forward switch.
2) Cut-through switch.

Store and Forward Switch
This switch stores the frame in the input buffer until the whole packet has arrived.
Cut-through Switch
It forwards the frame to the output buffer as soon as the destination address is received.

Two Types of Switch

1) 2-Layer switch

2) 3-Layer switch

2-Layer Switch

Layer 2 switches works at data link layer. It does not provide routing facilities. It is cheap compare to layer 3 switches. It is less efficient. It does not work like a router.

A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity.

However, a two-layer switch can be more sophisticated. It can have a buffer to hold the frames for processing.

3-Layer Switch

Layer 3 switches works at data-link layer as well as network layer. It provides routing facilities. It is costly compare to layer 2 switches. It is more efficient.

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding.

	Layer 2 switches	**Layer 3 switches**
1	Layer 2 switches works at data link layer.	Layer 3 switches works at data link layer as well as network layer.
2	It does not provide routing facilities.	It provides routing facilities.
3	It is cheap compare to layer 3 switches.	It is costly compare to layer 2 switches.
4	It is less efficient.	It is more efficient.
5	It does not work like a router.	It works like a router.

Router

Routers operate in the physical, data link and network layers of the OSI model as shown in figure. It is most active in network layer. Routers are able to access network layer address (logical address) of the device. It contains software that enables them to determine which of several paths between those addresses is best for data transmission. A packet sent from a station on one network to a device on a nearby network goes first to the router which switches packet to the destination network. Router consults with a routing table when packet is ready to be forwarded. Simplest function of routers is to receive packets from one connected network and pass them to second connected network.

Types of Routers

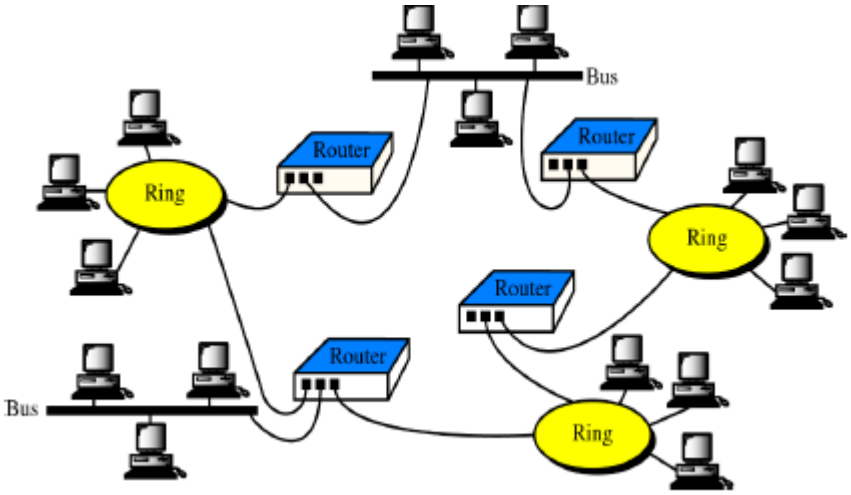
Static Router

Routing table's information's are entered manually. Means this administrator enters the route for each destination into the table. It cannot update automatically when there is change (shutdown of routers or breaking of link or some fault in connection) in the internet. It is more secure. It always uses the same route.

Dynamic Router

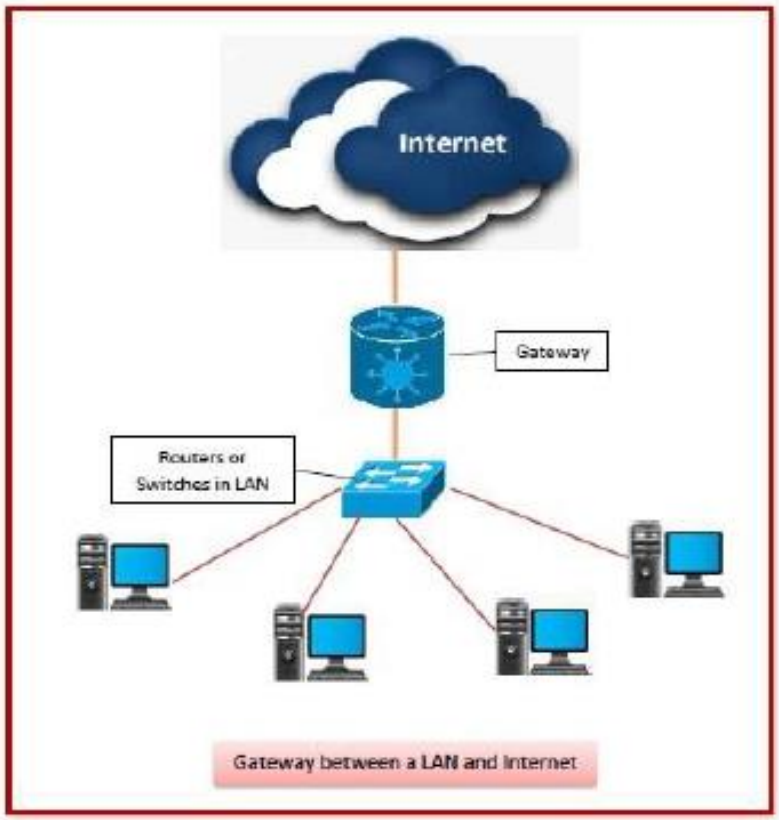
Routing table is created automatically. Table is updated using one of the dynamic routing protocols whenever there is change (shutdown of routers or breaking of link or some fault in connection) in the internet.

	switch	**router**
1	It operates at data link layer	It operates at network layer
2	It connects different computers within a network	It connects two or more different networks
3	A switch works on the basis of MAC address	A router works on the principle of IP address
4	Switch are comparatively less intelligent than router	Router are comparatively more intelligent than switch
5	A switch does not use any algorithms	A router uses routing algorithm to calculate best path for routing data packets



Gateways

Gateways operate in all seven layers of OSI model as shown in figure. Gateway is also called as protocol converter. Gateway is used to connect two different network systems. A Router is used to transfer, accept and relay packets only across networks using similar protocols. A gateway can accept a packet formatted for one protocol and converts into a packet formatted for another protocol before forwarding it. Gateway must adjust data rate, size and format. It converts the protocol from one network to another.



Unit-4 Layered Models

4.1 Network Model Based on Layered Architecture

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. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

The main aim of the layered architecture is to divide the design into small parts. 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.

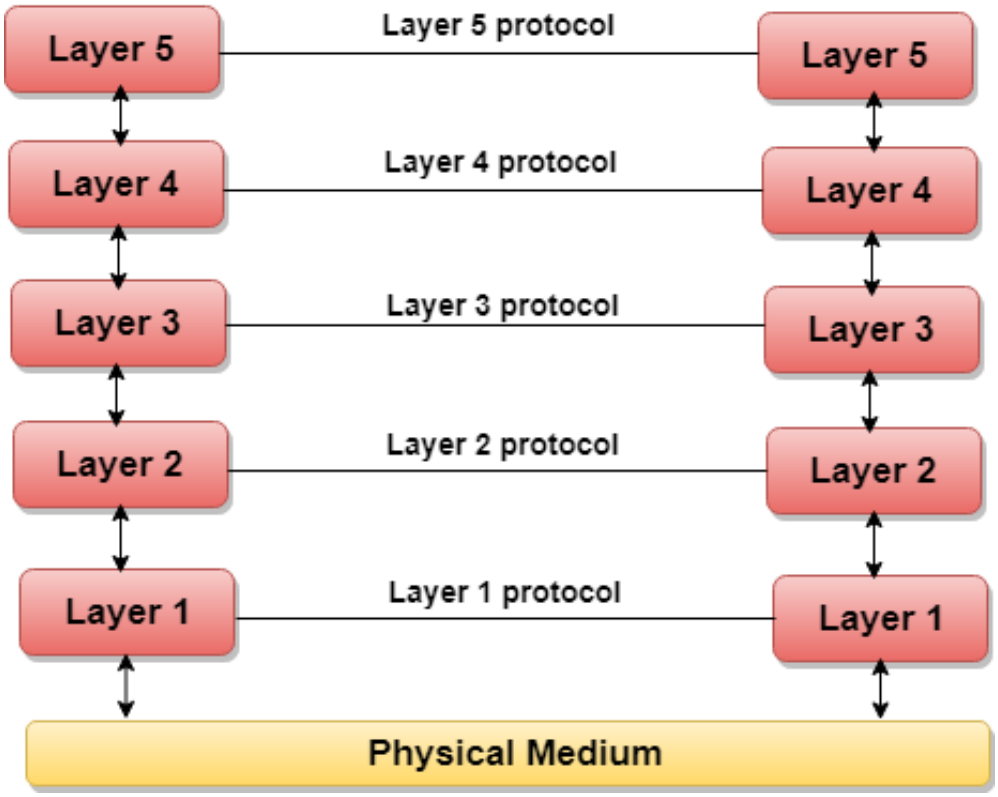
Interface: It is a way through which the message is transferred from one layer to another layer.

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.

In 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.

Let's take an example of the five-layered architecture.



Need 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 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.

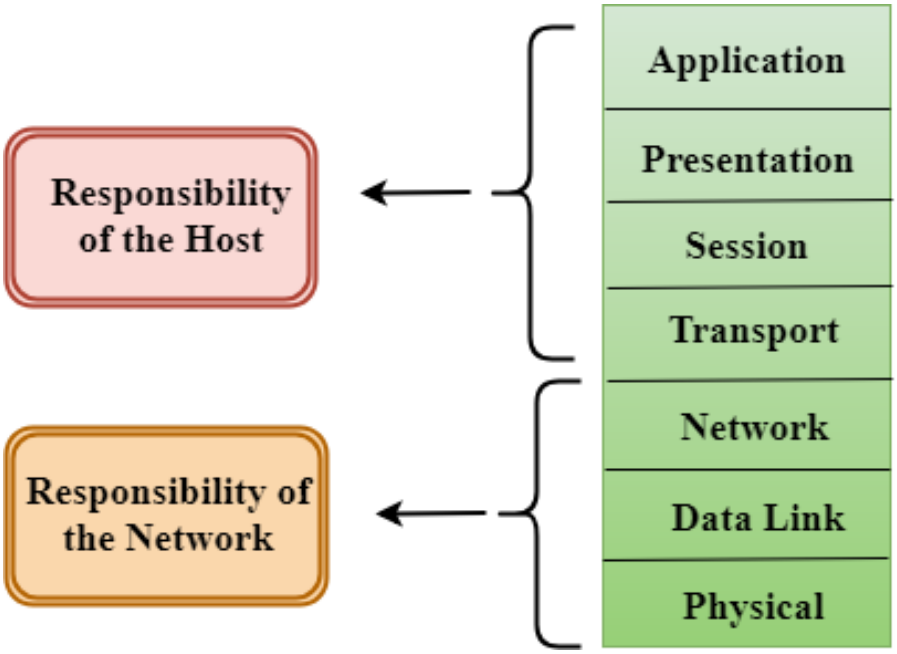
Easy to test
Each layer of the layered architecture can be analyzed and tested individually.

4.2 OSI Model

OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer. OSI consists of seven layers, and each layer performs a particular network function.

OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task. Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model



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

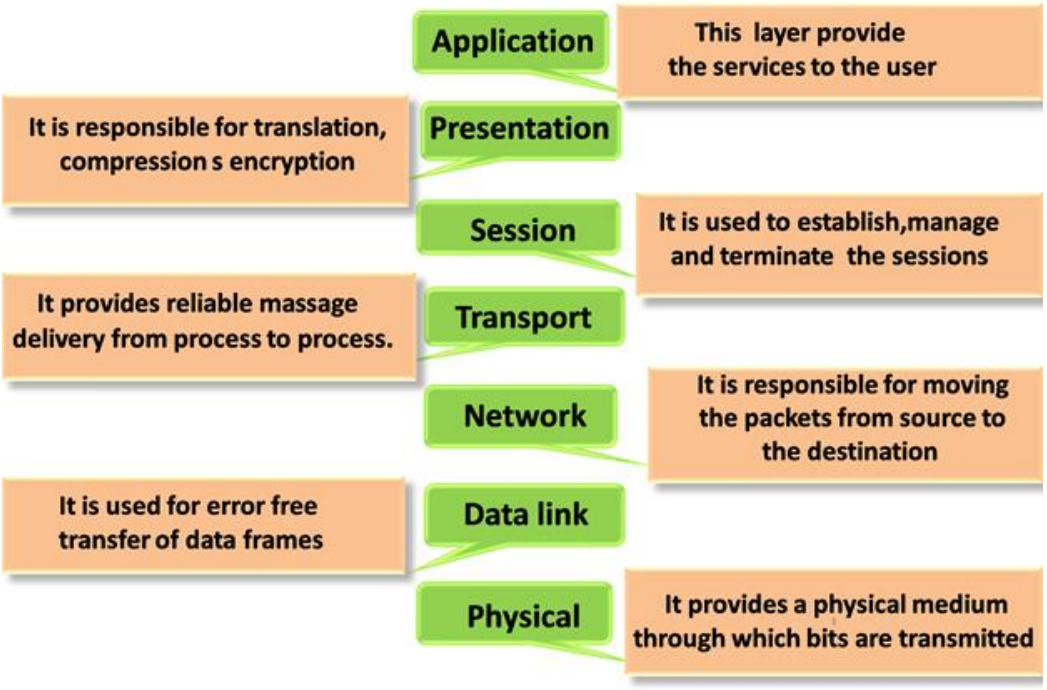
The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing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

The purpose of each layer in the OSI reference model is to provide service to the next layer above it by hiding the upper layer from the complications of the layer below it. Layer 1, 2 and 3 that is physical, data link and network layers are the Network Support Layer. Layer 5, 6 and 7 which is session, presentation and application layers is the User Support Layer. Transport layer links the network support layers and user support layers. OSI Model serves the purpose of providing general design guidelines for data communication systems. It is a learning tool that can be used to understand how modern computer systems communicate.

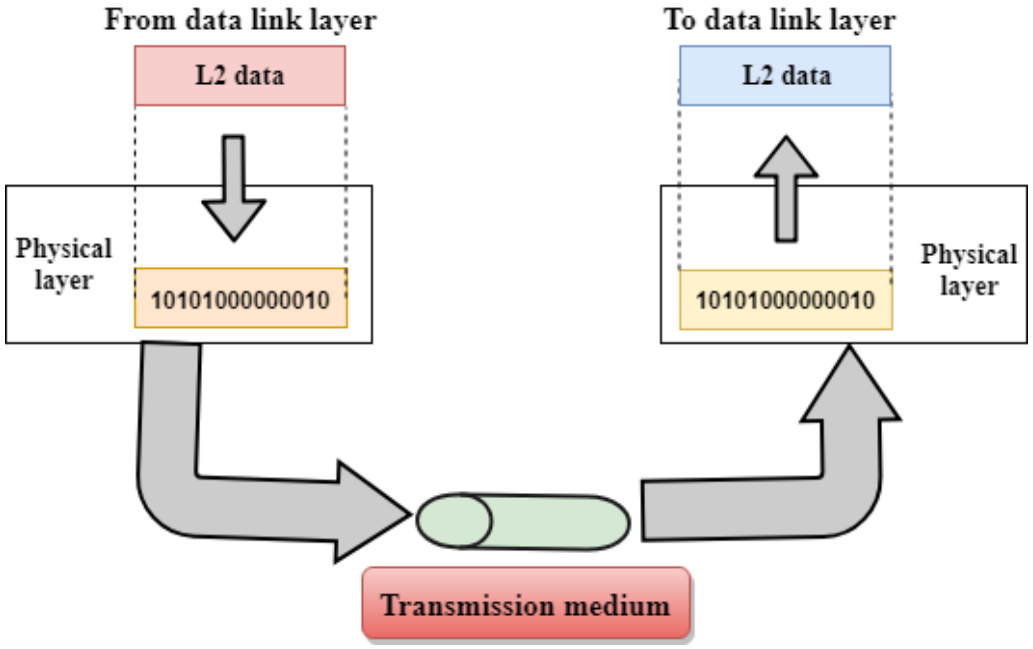
Functions of the OSI Layers

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

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



Physical layer



The physical layer is the bottom layer of OSI model. It is concerned with transmitting raw bits over a physical medium. It defines the physical structure of network (physical topology). The main functionality of the physical layer is to transmit the individual bits from one node to another node. It is the lowest layer of the OSI model. It establishes, maintains and deactivates the physical connection. It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer

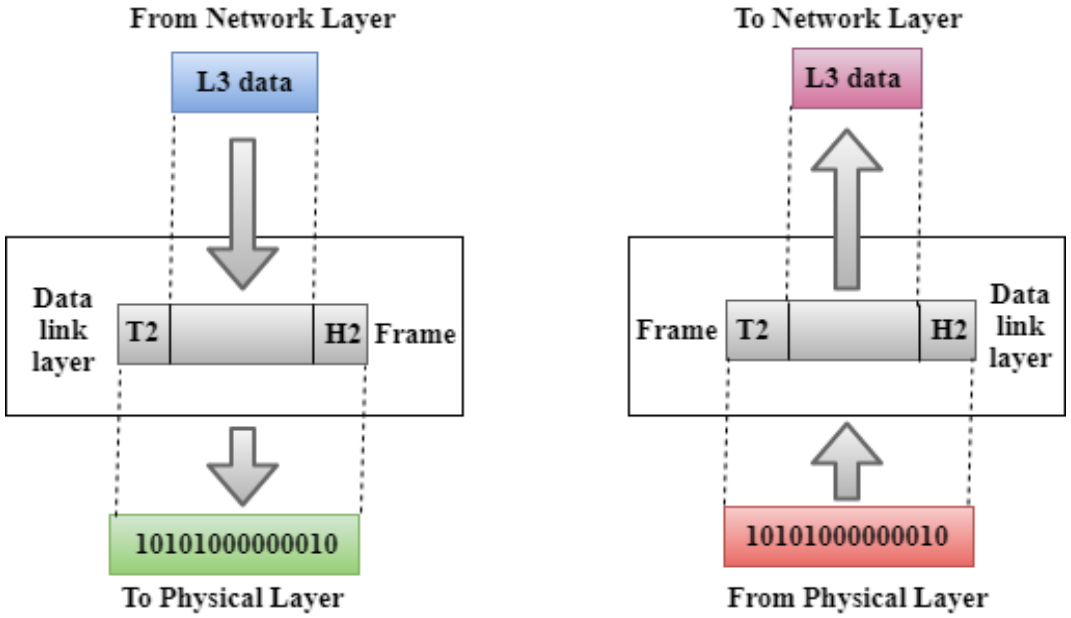
Line Configuration
It defines the way how two or more devices can be connected physically.

Data Transmission
It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

Topology
It defines the way how network devices are arranged.

Signals
It determines the type of the signal used for transmitting the information.

Data-Link Layer



A Data Link layer specifies raw data in which bits are grouped into frames and specific frame format. This layer is responsible for the error-free transfer of data frames. It defines the format of the data on the network. It provides a reliable and efficient communication between two or more devices. It is mainly responsible for the unique identification of each device that resides on a local network.

It contains two sub-layers:

Logical Link Control Layer

1) It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
2) It also provides flow control.

Media Access Control Layer

1) A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
2) It determines hardware addresses and responsible for transferring the packets over the network.

Functions of the Data-link layer

Framing
The data link layer translates the physical layer's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address. It transmits the frames sequentially and process the acknowledgement frames sent back by the receiver.

Physical Addressing

The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header. This header defines the physical address of the sender as well as the receiver.

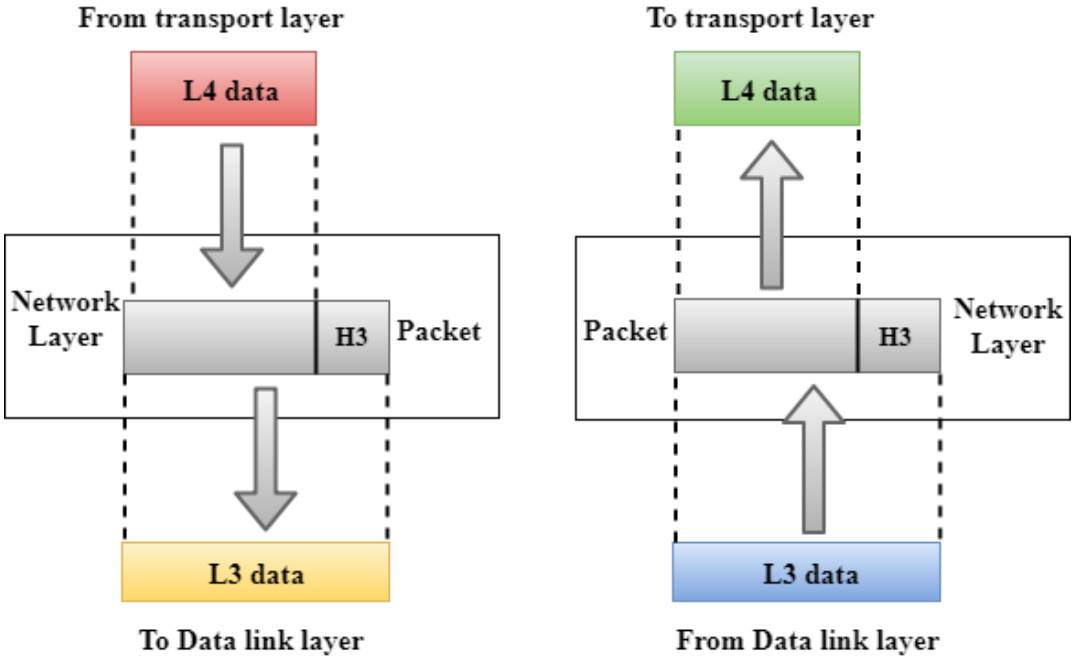
Flow Control

Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

Error Control

It is a mechanism to prevent duplication of frames in case a frame is destroyed due to noise or other reasons. Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.

Network Layer



It manages device addressing, tracks the location of devices on the network. It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors. The Network layer is responsible for routing and forwarding the packets. Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork. The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IPv4 and IPv6.

Functions of Network Layer

Internetworking

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

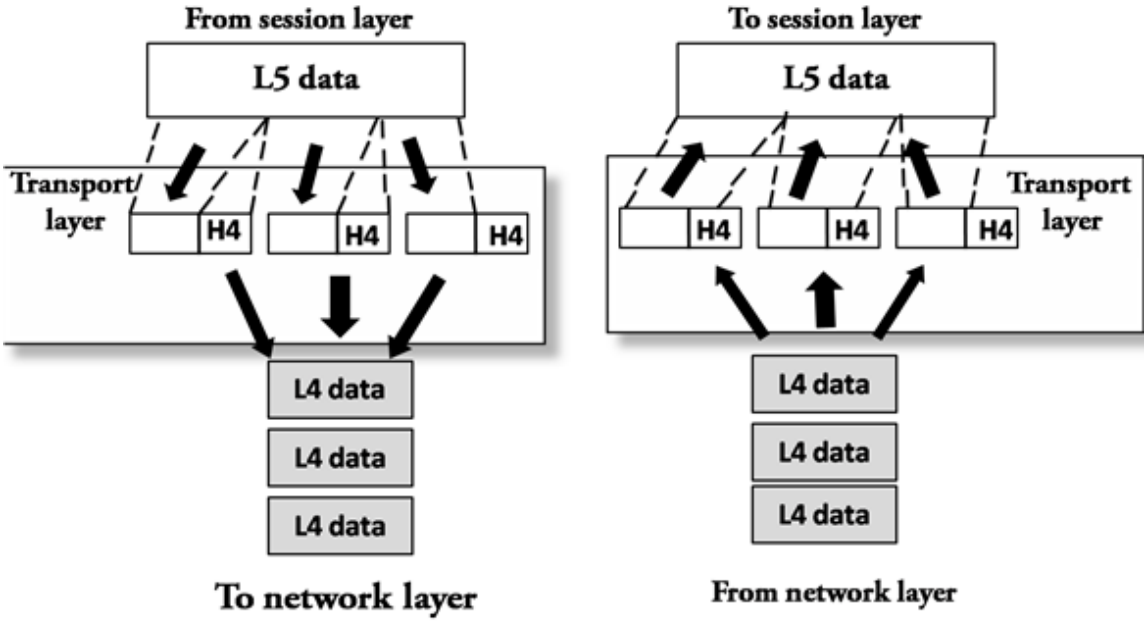
Logical Addressing

A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet. It is used to distinguish the source and destination system used when packet passes the network boundary.

Routing

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

Transport Layer



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

Functions of Transport Layer

Segmentation and reassembly

When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers. It identifies and replaces the lost packets during transmission.

Connection control

Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

Flow control

The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link. It controls the data flow between sender and receiver. It ensures that the transmitting device does not send more data than the receiving device can handle.

Error control

The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error. It corrects faulty transmission. It acknowledges successful transmission.

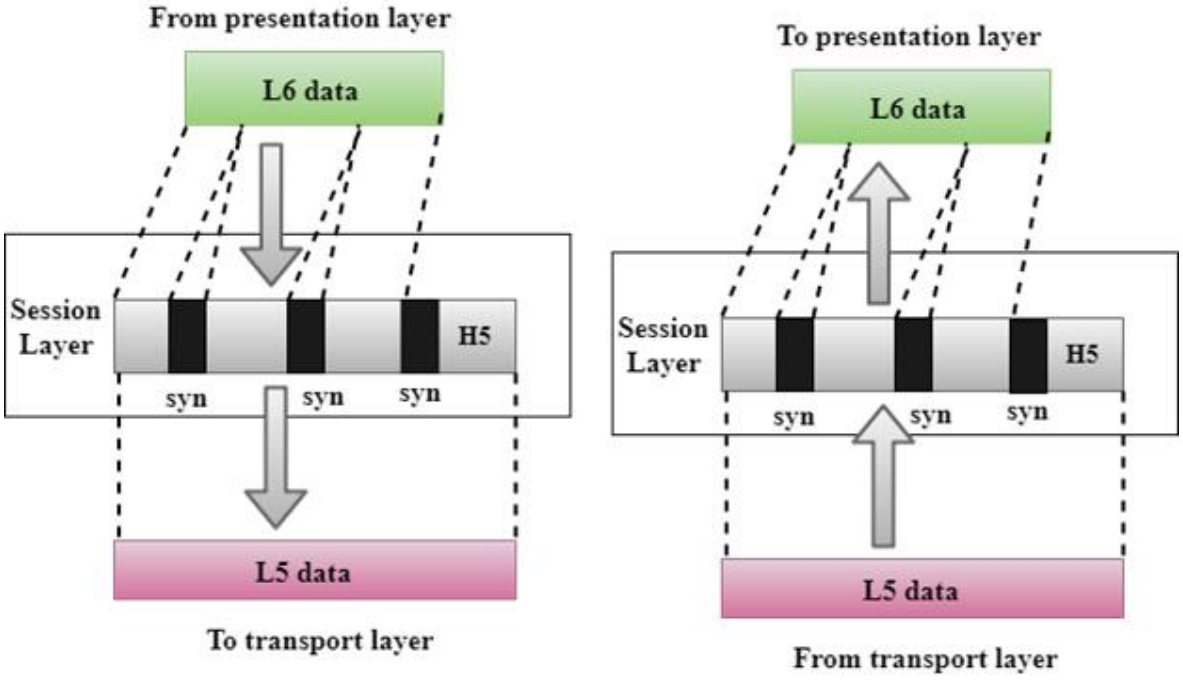
Session Layer

The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices. It is responsible for synchronizing data exchange between computers, structuring communication sessions and other issues directly related to conversations between network computers.

Functions of Session layer

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

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



Presentation Layer

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

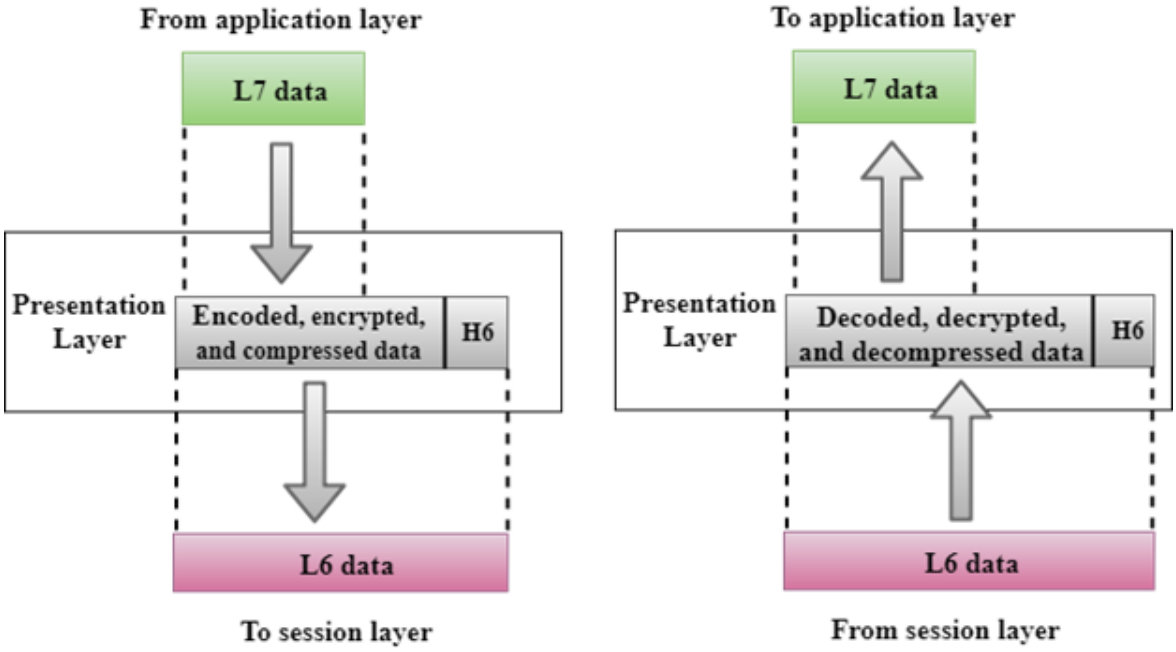
Functions of Presentation layer

Translation
The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

Encryption
Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

Compression

Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.



Application Layer

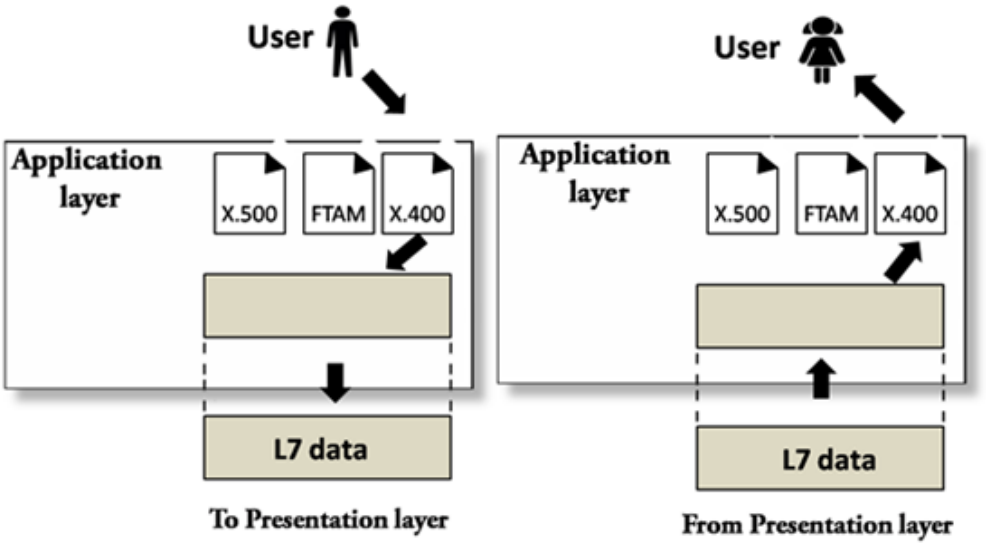
An application layer serves as a window for users and application processes to access network service. It handles issues such as network transparency, resource allocation, etc. An application layer is not an application, but it performs the application layer functions. This layer provides the network services to the end-users.

Functions of Application layer

File transfer, access, and management (FTAM)
An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

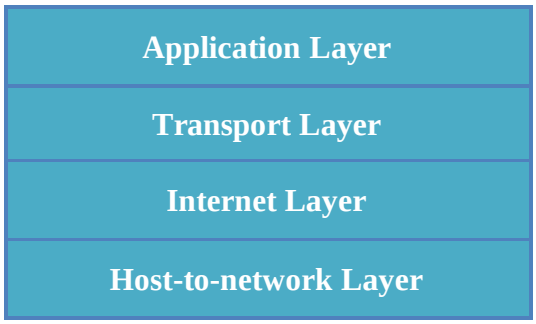
Mail services
An application layer provides the facility for email forwarding and storage.

Directory services
An application provides the distributed database sources and is used to provide that global information about various objects.



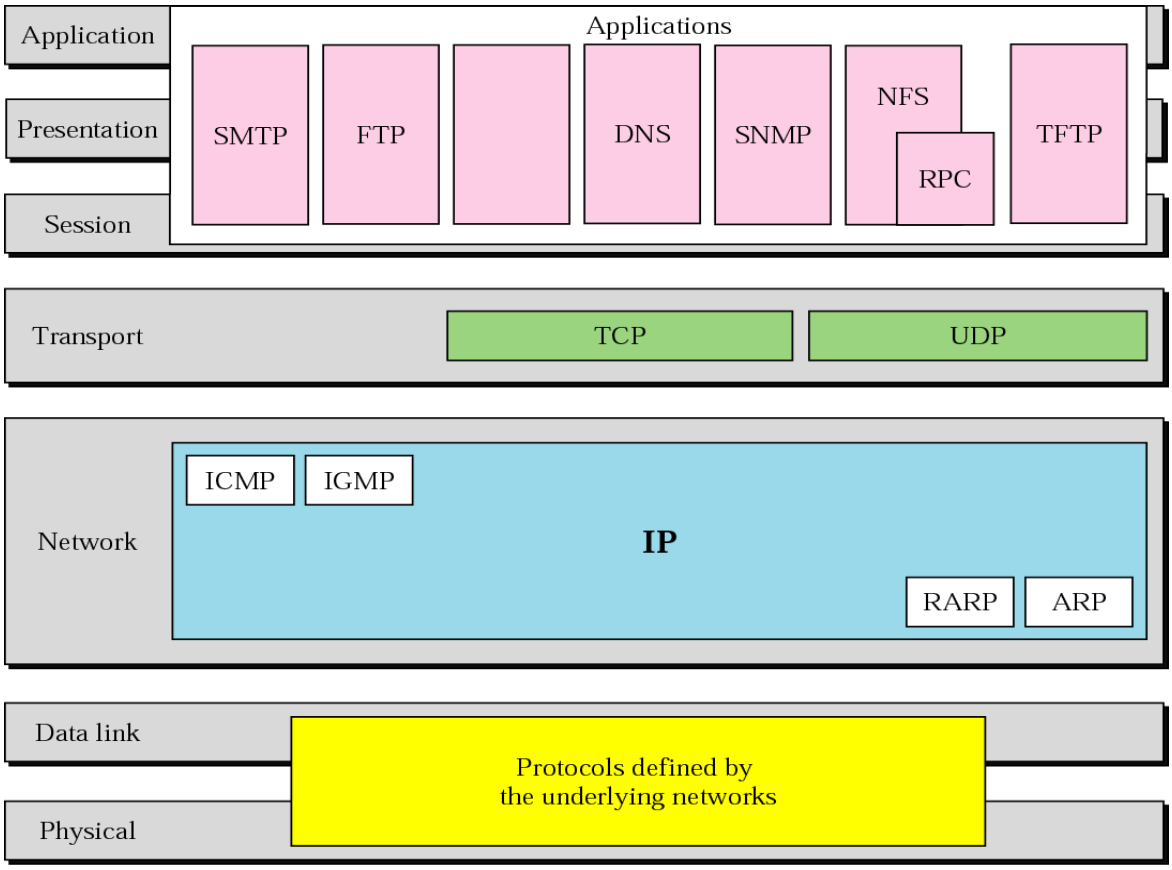
4.3 TCP/IP model

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 four layers: the application layer, transport layer, internet layer, host-to-network layer.



The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer. TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality. Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers



Host-to-Network Layer

A Host-to-Network layer is the lowest layer of the TCP/IP model. A Host-to-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. The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

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.

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 mainly associated with the ARP Protocol are:
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.

RARP Protocol

RARP stands for Reverse Address Resolution Protocol). RARP is used to find the IP address of the node when its physical address is known.

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.

IGMP (Internet Group Message Protocol): IGMP has been designed to help a multicast router to identify the hosts in a LAN that are members of a multicast group.

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 Transmission control protocol and User Datagram protocol.

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.

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 does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

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. But people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

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.

TFTP

TFTP stands for Trivial Transfer Protocol. TFTP protocol simply copies the file here they do not need to solve the problems provided in FTP. Here there are only two operations:

1) Reading - It means copying a file from the server site to the client site.
2) Writing - It means copying a file from the client site to the server site.

4.4 Connection-Oriented and Connectionless Service

Data communication is a telecommunication network to send and receive data between two or more computers over the same or different network. There are two ways to establish a connection before sending data from one device to another, that are **Connection-Oriented** and **Connectionless Service**. Connection-oriented service involves the creation and termination of the connection for sending the data between two or more devices. In contrast, connectionless service does not require establishing any connection and termination process for transferring the data over a network.

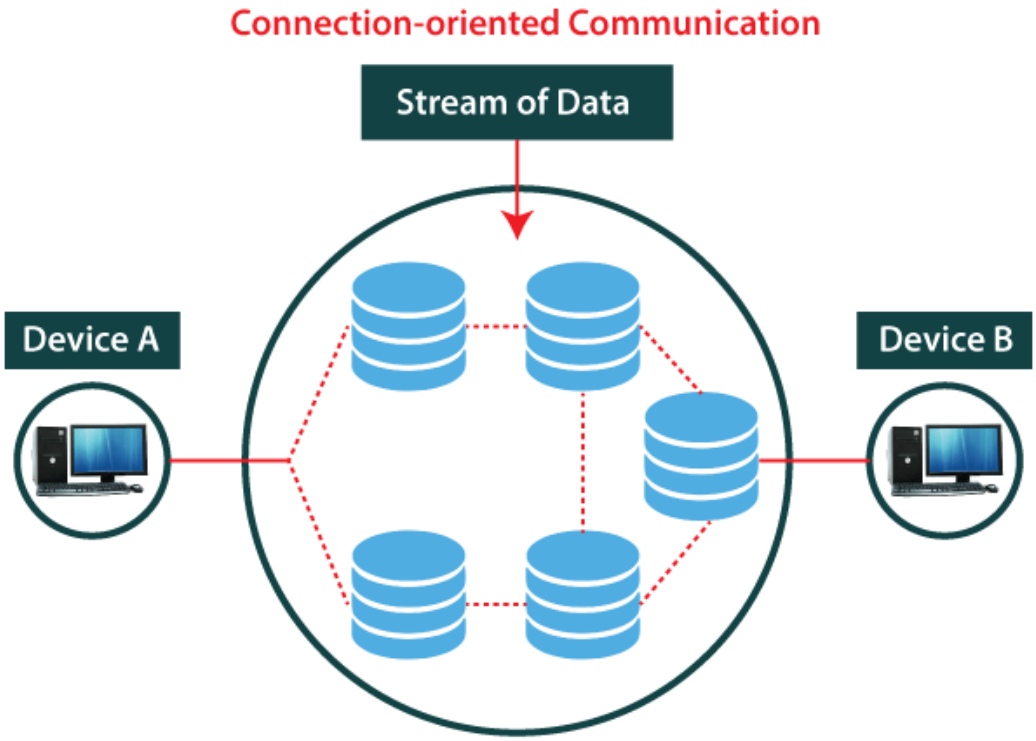
Connection-Oriented Service

A connection-oriented service is a network service that was designed and developed after the telephone system. A connection-oriented service is used to create an end-to-end connection between the sender and the receiver before transmitting the data over the same or different networks. In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them. It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.

Suppose, a sender wants to send data to the receiver. Then, first, the sender sends a request packet to a receiver in the form of an SYN packet. After that, the receiver responds to the sender's request with an (SYN-ACK) signal/packets. That represents the confirmation is received by the receiver to start the communication between the sender and the receiver. Now a sender can send the message or data to the receiver.

Similarly, a receiver can respond or send the data to the sender in the form of packets. After successfully exchanging or transmitting data, a sender can terminate the connection by sending a signal to the receiver. In this way, we can say that it is a reliable network service.

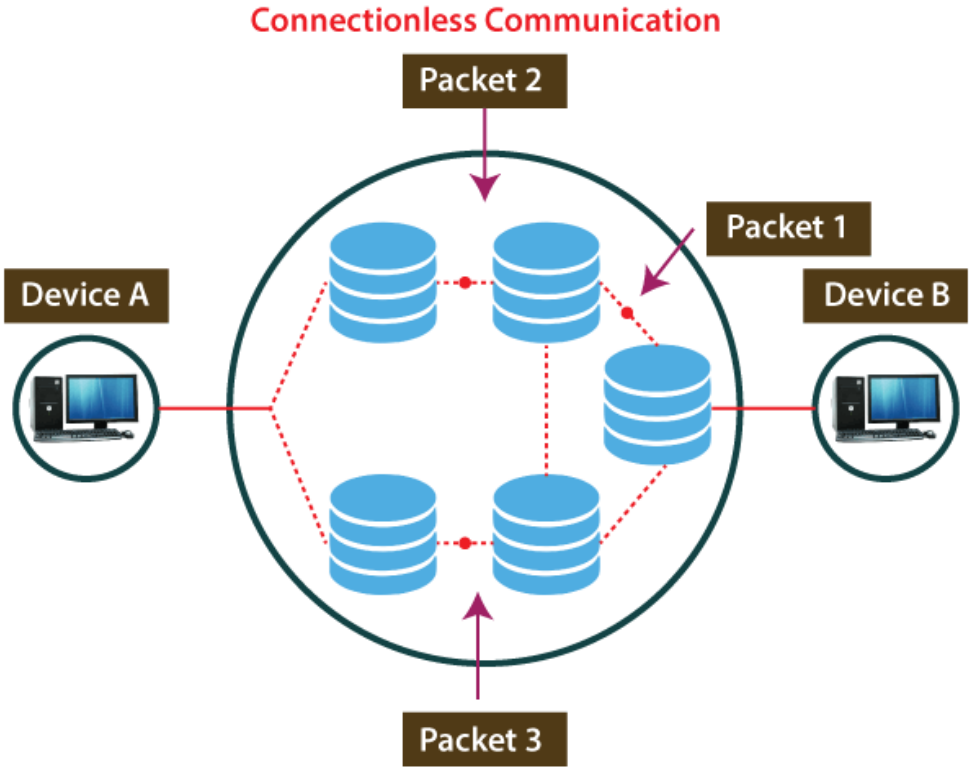
TCP (Transmission Control Protocol) is a connection-oriented protocol that allows communication between two or more computer devices by establishing connections in the same or different networks. It is the most important protocol that uses **internet protocol** to transfer the data from one end to another. Hence, it is sometimes referred to as TCP/IP. It ensures that the connection is established and maintained until the data packet is transferring between the sender and receiver is complete.



Connectionless Service

A connection is similar to a postal system, in which each letter takes along different route paths from the source to the destination address. Connectionless service is used in the network system to transfer data from one end to another end without creating any connection. So it does not require establishing a connection before sending the data from the sender to the receiver. It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver. Therefore, we can say that the data packet does not follow a defined path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.

For example, a sender can directly send any data to the receiver without establishing any connection because it is a connectionless service. Data sent by the sender will be in the packet or data streams containing the receiver's address. In connectionless service, the data can be travelled and received in any order. However, it does not guarantee to transfer of the packets to the right destination.

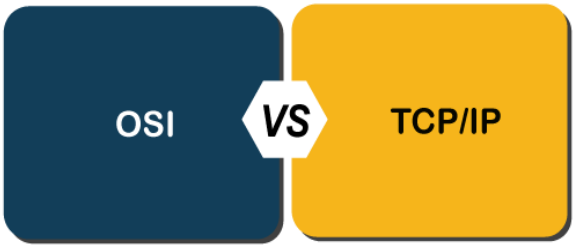


The UDP (User Datagram Protocol) is a connectionless protocol that allows communication between two or more devices without establishing any connection. In this protocol, a sender sends the data packets to the receiver that holds the destination address. A UDP does not ensure to deliver the data packets to the correct destination, and it does not generate any acknowledgment about the sender's data. Similarly, it does not acknowledge the receiver about the data. Hence, it is an unreliable protocol.

4.5 Connection-Oriented vs Connectionless Service

	Connection Oriented Services	Connectionless Services
1	Connection must be established prior to data transmission.	Data is sent without any prior establishment of connection.
2	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
3	Data transmission speed is low.	Data transmission speed is high.
4	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
5	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
6	It provides acknowledgement.	It doesn’t provide acknowledgement.
7	TCP is example of connection-oriented services.	UDP is the example of connectionless services.

Differences between the OSI and TCP/IP model



Let's see the differences between the OSI and TCP/IP model in a tabular form:

	OSI Model	TCP/IP Model
1	It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
2	OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
3	It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
4	This model is based on a vertical approach.	This model is based on a horizontal approach.
5	In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
6	In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.
7	Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
	It consists of 7 layers.	It consists of 4 layers.
	OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
	The usage of this model is very low.	This model is highly used.

Unit-5 IP Protocol and Network Applications

5.1 IP Protocol
5.2 Addressing Schemes
5.3 Subnet and Masking
5.4 DNS
5.5 Email Protocols
5.6 FTP
5.7 HTTP

5.1 IP Protocol

The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol does not provide a reliable communication facility. There are no acknowledgments, it is either end-to-end or hop-by-hop.

Definition

The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits from a source to a destination over an interconnected system of networks.

IP Address

An address that identifies the connection of host to its network is called IP address. An IP address is 32-bit address. It is unique address. Unique here means two devices on Internet can never have same address at same time.

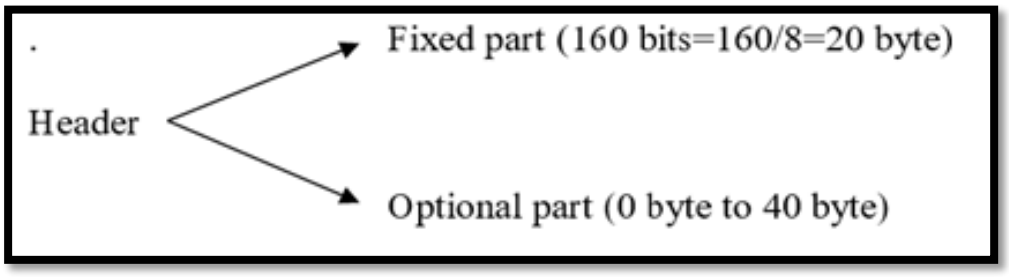
IP Datagram

Datagram is a variable length packet consisting of two parts

1) Header
2) Data IP datagram

Header (20-60 bytes)	Data
Total 20-65,536 bytes	

Header is 20 to 60 bytes in length and contains information required to routing and delivery of datagram. IPV4 header format shown in fig.



Types of IP Address Notation

Two notations that shows the IP address

1) Binary notation
2) Dotted Decimal notation

Binary Notation

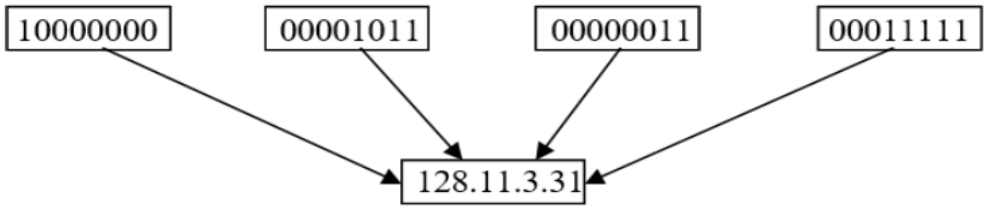
IP address is 32-bit address. To make address readable, one or more spaces is usually inserted between each 8 bits.

10000000	00001011	00000011	00011111
8 bits	8 bits	8 bits	8 bits total= 32bits
1 byte	1 byte	1 byte	1 byte total = 4 byte

EXAMPLE OF AN IP ADDRESS IN BINARY NOTATION

Dotted – Decimal Notation

To make 32-bit address shorts and easier to read Internet address are written in decimal from with decimal points separated by dot. So, it is called dotted decimal Notation.

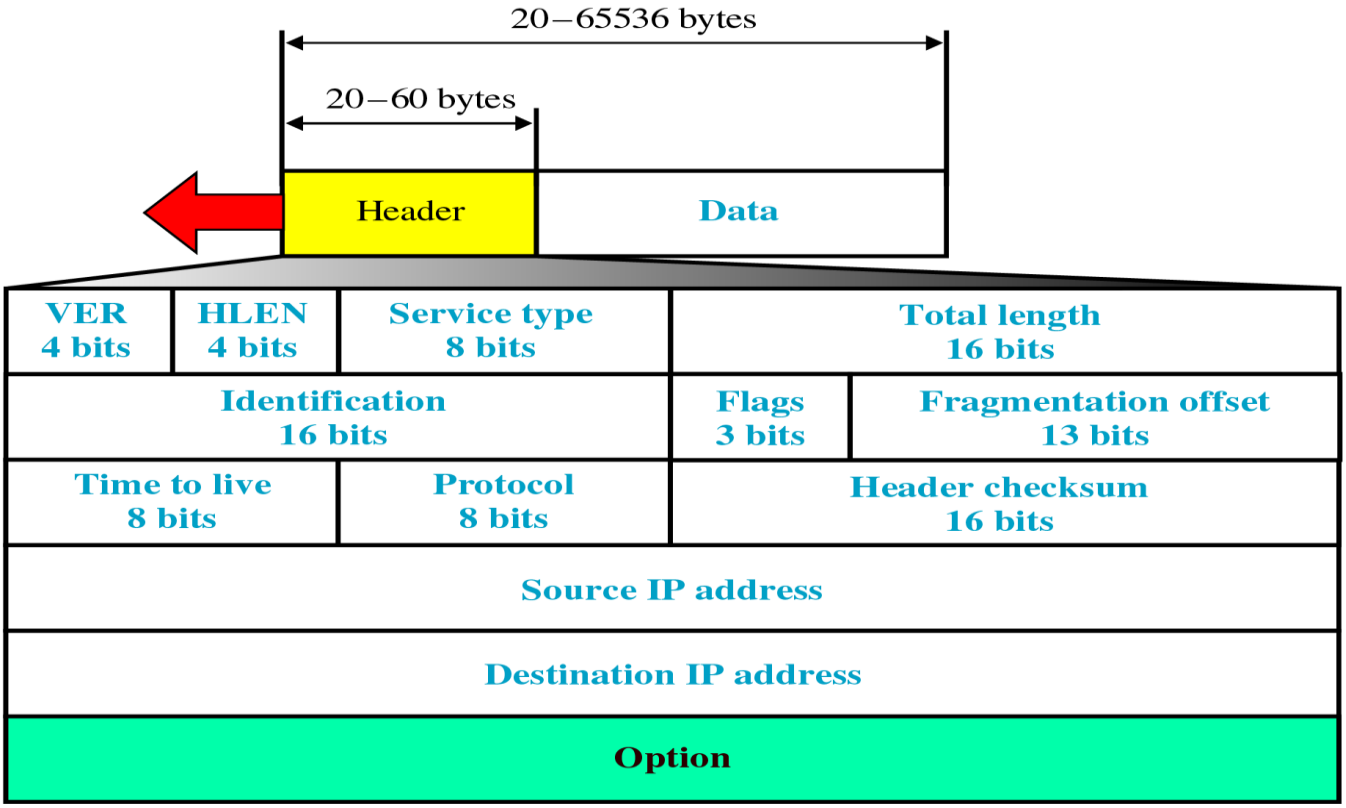


EXAMPLE OF AN IP ADDRESS IN DOTTED DECIMAL NOTATION

IPv4

IPv4 stands for Internetwork Protocol Version 4. The Address Space is 32 bits. The length of header is 20-60 bytes. The number of Header fields is 12. Checksum field is used to measure error in the header. There are 4 bytes allocated for each address in the header. Internet protocol Security with respect to network security is optional.

IPv4 Header Format



VER: Version

This field defines the version of IP. Currently version is 4: IPv4 with a binary value 0100. IPv6: IP version 6, with binary value 0110.

HLEN: Header Length

This field defines the length of header in IP diagram. Length is in multiples of 4 bytes. This is 4-bit information means number between 0 and 15 (0000-1111), which is multiply by 4 bytes.

Service Type

This field defines how the datagram should be handled. It contains bits that specify the type of services the sender wants, such as reliability, delay and level of throughput.

Total length

This field defines total length of IP datagram. Header length + Data length = Total length. This is 16-bit field. From this 20-60 bytes are the header and the rest of it is data from upper layer.

Identification

Identification field is used in fragmentation. A datagram when passing through different network may be divided into fragments to match the network frame size. So, each fragment is identified with sequence number in this field. All the fragments have same identification number. This identification number helps the destination in rearrangement process of datagram.

Fragmentation Offset

The fragmentation offset is a pointer that shows position of fragment in the original datagram.

Time to live

This field is used to control the maximum numbers of hops (routers) visited by the datagram. This prevents the datagram from going back and forth forever between routers.

Protocol

This field defines the higher-level protocol that uses the services of the IP layer. Higher layer protocols such as TCP, UDP, ICMP, IGMP etc.

Header Checksum

This is 16-bit field used to check the header part, not the rest of packet.

Source IP address

This field specifies 4 bytes (32 bit) Internet address of the source. This field must remain unchanged during the time datagram travels from one network to another.

Destinations IP addresses

This field defines IP address of destination. This is also 4 byte Internet address. This field must remain unchanged during the time the datagram travels from one network to another.

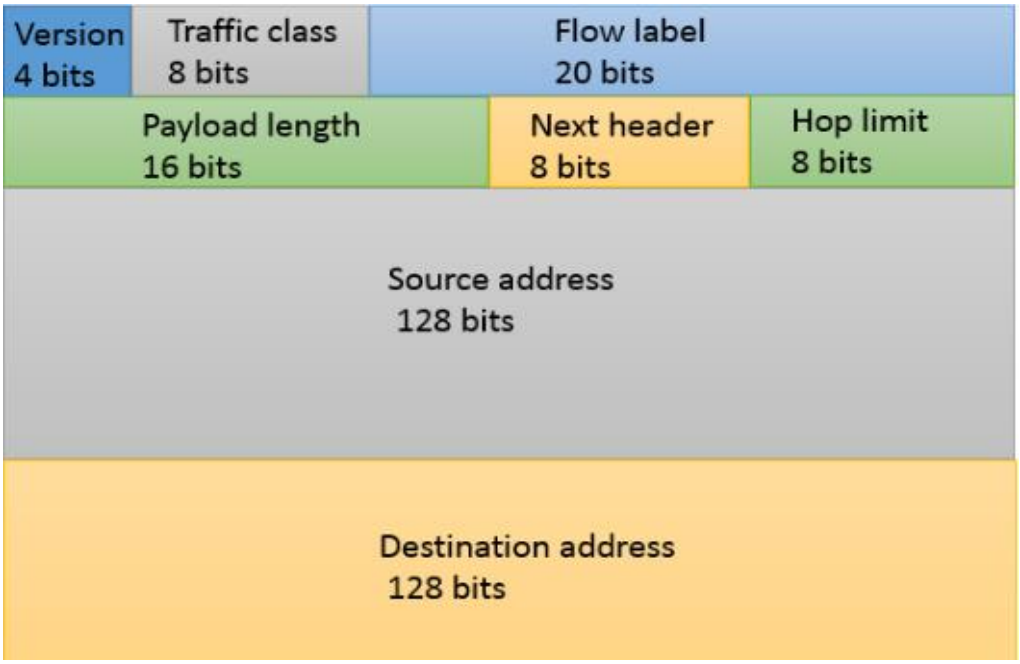
Options

Optional part means it is not required for every datagram. They are used for network testing, debugging, control routing, timing, management etc. Options field gives more functionality to the IP datagram.

IPv6

IPv6 stands for Internetwork Protocol Version 6. In IPv6, format and length of IP addresses were changed along with the packet format. IPv6 provide 128 bits addressing. IPv6 has some advantages over IPv4. Checksum field is eliminated from the header. Internet protocol Security with respect to network security is mandatory.

IPv6 Header Format



VER (Version)
The four-bit field defines the version number of IP.

TRAFFIC CLASS
The four-bit field to set the priority of the packet with respect to traffic congestion.

FLOW LABEL
The flow label is the field that is designed to provide special handling for a particular flow of data.

PAYLOAD LENGTH
The two-byte payload length field defines the total length of the IP datagram excluding the base header.

NEXT HEADER
The next header is an eight-bit field defining the header the follow the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header for an Upper layer protocol like UDP or TCP. Each extension header also contains this field.

HOP LIMIT
The eight-bit hop limit field serves the same purpose as the TTL field in IPv4.

SOURCE ADDRESS
The source address field is a 16-byte internet address that identifies the original source of the datagram.

DESTINATION ADDRESS
The Destination address field is 16-byte address that identifies the final destination of the datagram. However, if the source routing is used, this field contains the address of the next router.

Features of IPv6

1) **Large Address Space**
   IPv6 address is 128-bits long. It provides very large address space compare to IPv4.
2) **Better Header Format**
   IPv6 uses a new header format in which option are separated from header and inserted (when required) between header and data.

Header	Options	Data

3) **New Options**
   IPv6 has new options to allow for additional functionalities.
4) **Allowing Extension**
   IPv6 is designed to allow the extension of the protocol if required by new technologies.
5) **Support for Resource Allocation**
   In IPv6, the type of service field has been removed, but flow label has been added to enable the source to request special handling of packet. This is used to support traffic such as real-time audio and video.
6) **Support for more Security**
   IPv6 provides more security compare to IPv4. The encryption and authentication options in IPv6 provide confidentiality to the packet.

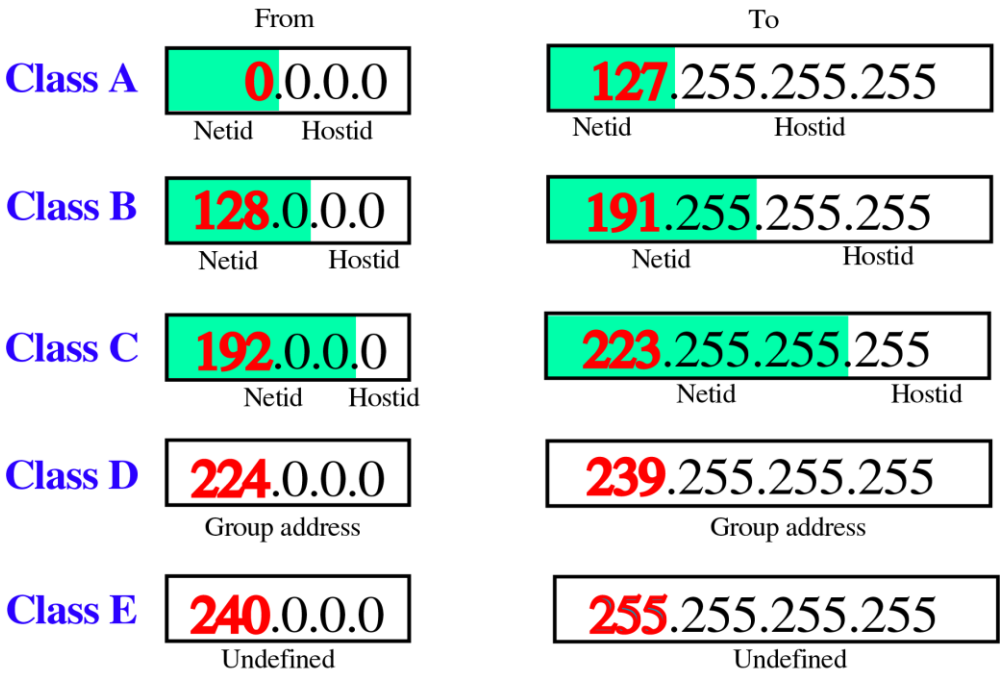
Addressing Schemes

Classful Addressing

The address space is divided into five classes: Class A, Class B, Class C, Class D and Class E. Addresses in classes A, B and C are used for unicast communication i.e. one source to one destination. Addresses in class D are used for multicast communication i.e. one source to many destination. Addresses in class E are reserved for future use. IP addresses in class A, B and C is divided into net id and host id.

Net id - Network Identification Number

Host id - Host Address



Finding the class in Binary Notation

If we want to find out the class of any IP address by using binary notation then we have to consider the first byte and the method is like below in the fig. If any IP address starting with binary 0 then it belongs to class A. If it starts with binary 10 then it belongs to class B. If it starts with binary 110 then it belongs to class C. If it starts with binary 1110 then it belongs to class D. If it starts with binary 1111 then it belongs to class E.

Finding the class in Dotted-Decimal Notation

If we want to find out the class of any IP address by using dotted decimal notation then we have to consider the first byte and the method is like above in the fig. If an IP address starts with decimal in between 0 to 127 it belongs to class A, if it starts is between 128 to 191 it belongs to class B. if it starts between 192 to 223 it belongs to class C, if it starts between 224 to 239 it belongs to class D, , if it starts between 240 to 255 it belongs to class E.

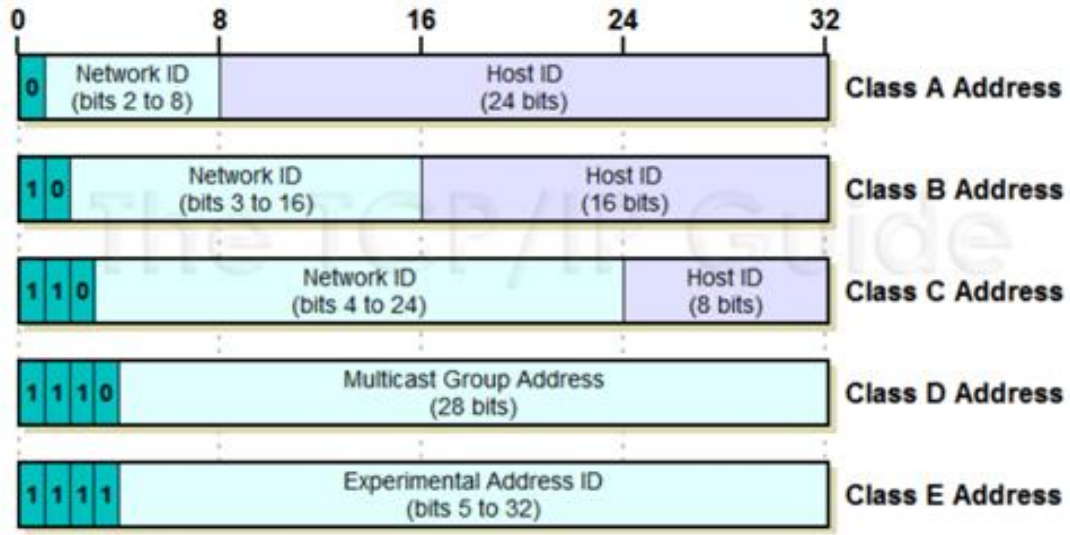
Network Address

The network address is an address that defines the network itself, it cannot be assigned to host.

Net id	Host id
Specific	All 0's

Properties of Network Address

1) All host id bytes are 0's.
2) The network address defines the network to the rest of Internet. Router can route a packet based on network address.
3) The network address is first address on the block.
4) Given the network address, we can find the class of address.



	Range for first byte
Class A	0 - 127
Class B	128 - 191
Class C	192 - 223
Class D	224 - 239
Class E	240 - 255

Classless Addressing

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity.

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:

1) The addresses in a block must be contiguous, one after another.
2) The number of addresses in a block must be a power of 2 (1, 2, 4, 8,...).
3) The first address must be evenly divisible by the number of addresses.

Subnet and Masking

Subnet

Dividing a larger network into smaller sub-networks is called subnetting. IP address is 32-bits long. In the addressing, one portion of the address indicates a network (net id), and the other portion indicates the host (or device) on network (host id).

IP addressing are designed with two-level of hierarchy. To reach a host on Internet, we must first reach to network using first portion of address (net id). Then we must reach the host it self-using the second portion (host id).

[Network Net id host id]

Sometimes these two levels of hierarchy is not suitable to the organization, so at that point network needs to be divided into several smaller networks.

The further division of a network into smaller networks called sub networks. For example, University has many departments. The university has one network address, but its departments have several sub networks addresses. Each sub network is identified by its sub network address. When we divide a network into several subnets, we have three level of hierarchy.

[Network Sub Network Host]

For Example:

Without Sub Netting

Two level Hierarchy

141.14.2.21 Class B address

141.14 • **2.21**
Net Id Host Id

With Sub Netting

Three level Hierarchy

141.14 • **2** • **21**
Net Id Sub-Net Id Host Id

Masking

Masking is a process that extracts the address of the network from an IP address. When a router receives a packet with destination address, it needs to route the packet. The routing is based on network address and sub network address. The router outside the organization (Network) routes the packet based on the network address. The router inside the organization routes the packet based on sub network address. A network administrator knows the network address and sub network addresses but router does not. Router uses masking process.

Router uses masking process. Masking is a process that extracts the address of network from an IP address. Masking can be done whether we have sub-netting or not. If we have not sub-netted the network, masking extracts the network address from an IP address. If we have sub-netted, masking extracts the sub-network address from an IP address.

For Example

IP address - 141.14.2.21

Mask - 255.255.0.0

Network Address - 141.14.0.0

Class	Default Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0
D	N/A
E	N/A

DNS

To identify an entity, the internet uses an IP address, which uniquely identifies the connection of a computer to the internet. But user prefers to use names instead of numeric addresses. Because of remember numeric addresses are difficult compare to names. Therefore, we need a system that can map a name to an address or an address to name. The naming scheme used in internet is called the DNS (Domain Name System). In DNS names must be unique because the addresses are unique.

Domain names are case insensitive. Each domain is partitioned into sub domains and these are further partitioned and so on. Once an organization has been assigned domain, the suffix is received for the organization. Means no other organization will be assigned the same name and suffix. Means unique domain suffix is assigned to each organization. To map a name into an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter. The resolver sends a UDP packet to local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to caller processor.

DNS names are defined in an inverted tree structure with the root at top. Each node in the tree has a label, which is a string with maximum of 63 characters.

Domain Name

Each node in a tree has a domain name. A full domain name is a sequence of labels separated by dots. Full path names must not exceed 255 characters. Domain names are always read from the bottom to top. Last label is the label of the root. The root label is a null string (Empty String). Means a full domain name always ends in a null label.

Name Server

Information contained in the domain name system must be stored. It is very inefficient and not reliable to have just one computer store such large information. Because, any failure on that computer makes data inaccessible. To solve above problem, we have to distribute the information among many computers called DNS servers. One way to do this is to divide the whole space into many domains based on first level.

DNS allows domains to be divided future into smaller domains. Each server can be responsible for a domain. We have a hierarchy of servers. DNS name space is divided into zones. (Non-overlapping area) Each zone contains some part of a tree and also contain name server. The server makes a database called a zone file and keeps all the information for every node under that domain. Root server is a server whose zone consists of a whole tree. It has authority to other servers, keeping references to those servers.

DNS in the Internet

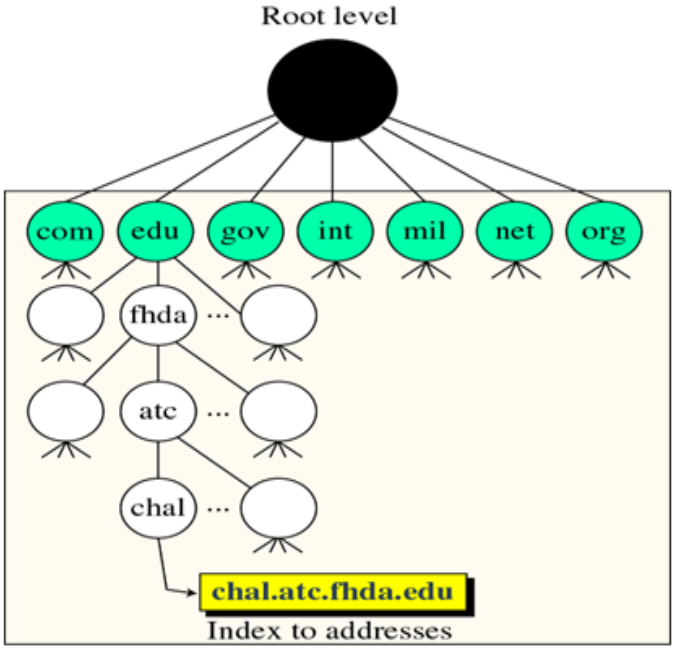
In the internet, domain name space is divided into three different sections-

1) Generic domain.
2) Country domain.
3) Inverse domain.

Generic Domain

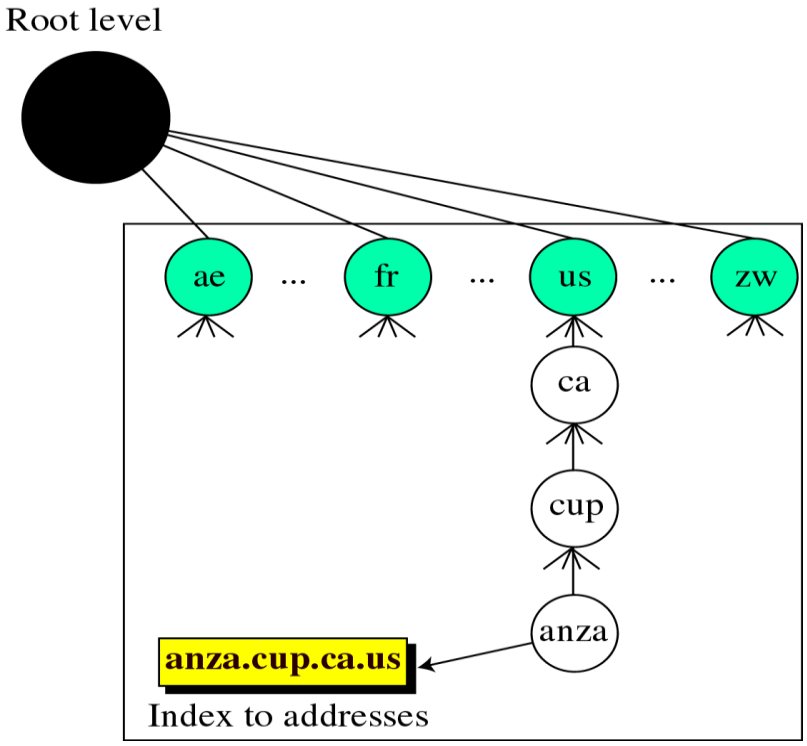
Generic domain defines registered hosts according to their generic behaviour. Each node in a tree defines a domain. In first level, generic domain uses three-character codes.

1) Com – Commercial organization
2) Edu – Educational Institutions
3) Mil – Military Groups
4) Org – Non-profit organization
5) Int – International organization
6) Gov – Government institutions
7) Net – Network Organizations



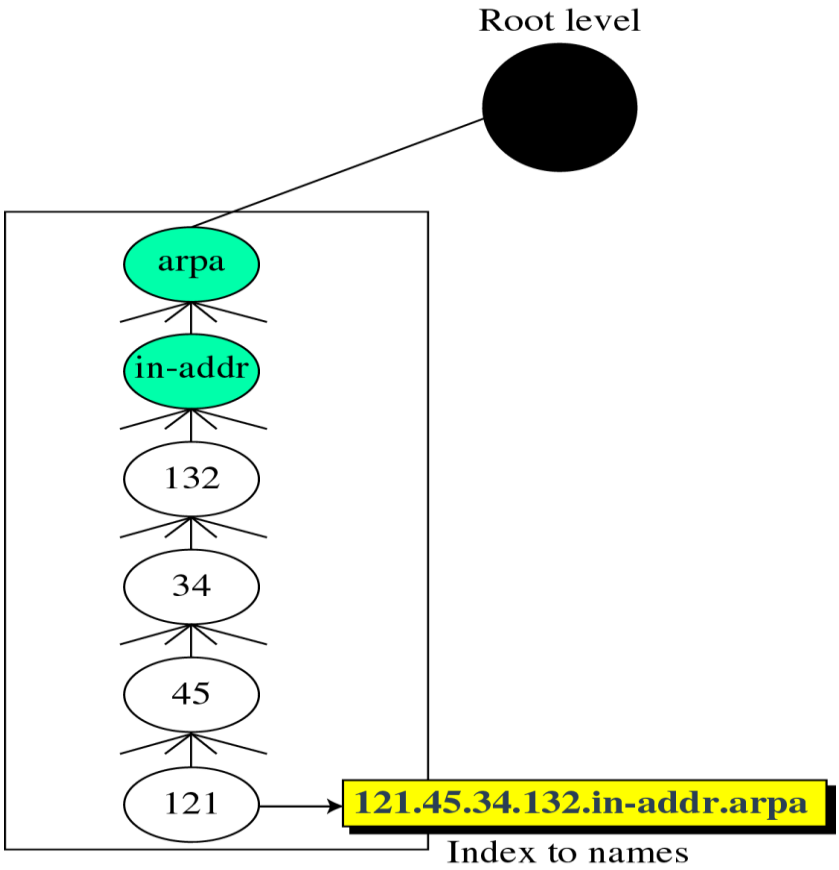
Country Domain

It uses a two-character country abbreviation in place of three-character abbreviation at first level.



Inverse Domain

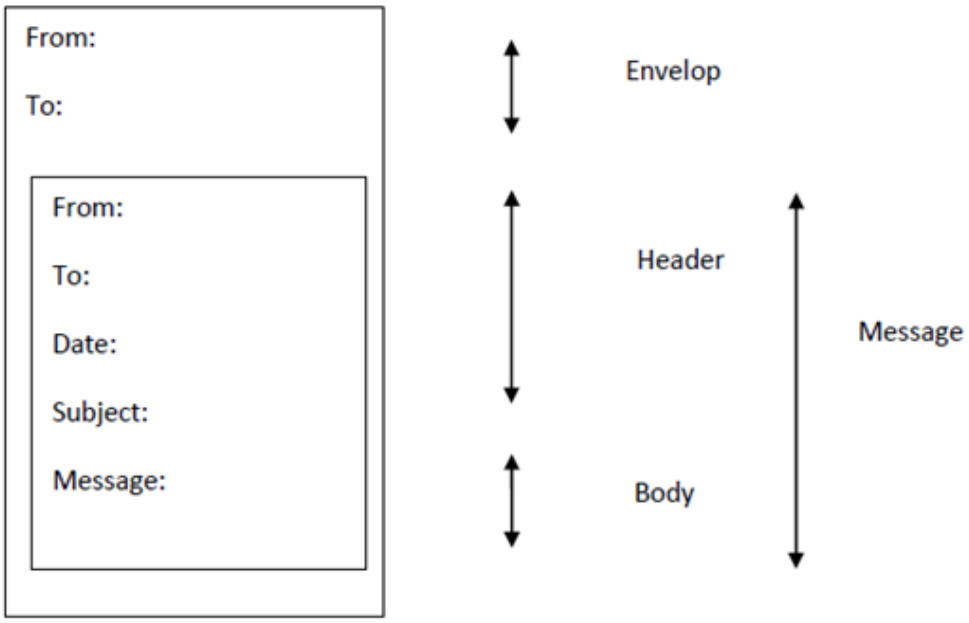
It is used to map an address to a name. When a server has received a request from a client to do a task. Whereas server has a file that contains a list of authorized clients, server lists only the IP address of the client.



Email Protocols

Electronic mail, often abbreviated to e-mail, or simply mail, is a store-and-forward method of writing, sending, receiving and saving messages over electronic communication systems. The term "e-mail" applies to the internet e-mail systems based on simple mail transfer protocol (SMTP), to network systems based on other protocols and to various mainframe, minicomputer, or intranet systems allowing users within one organization to send messages to each other in support of workgroup collaboration.

E-mail is most popular network services. It is system for sending message to other computer uses based on email address. Sending message that include text, audio, video or graphics. Sending single message to one or more recipients. SMTP is standard protocol use for electronic mail in the internet.



Sending Mail: Format of email

To send mail, the user creates mail that looks very similar to postal mail. It has two parts.

1) Envelope.
2) Message.

Envelope

It contains the sender address, the receiver address and other information.

Message

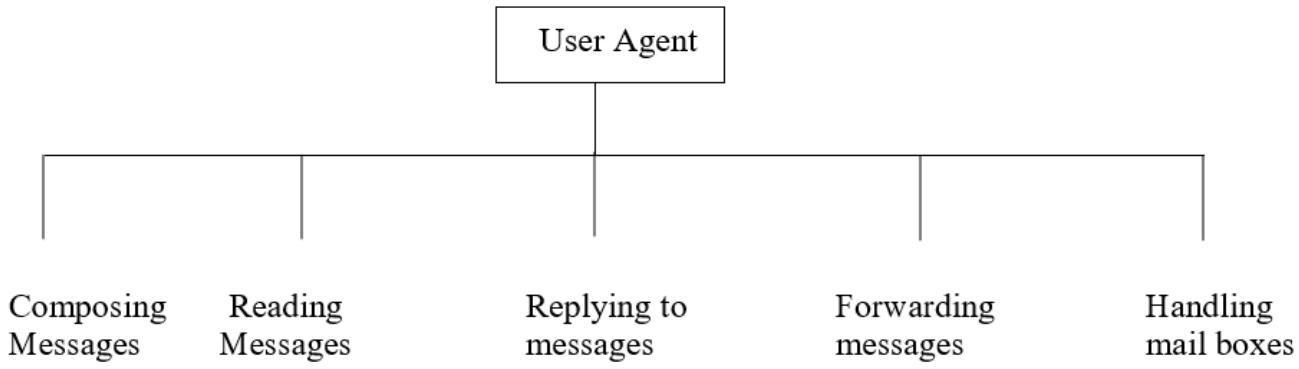
It contains the header and body. Header of the message contains the address of the sender, receiver and subject of message, data, etc. Body of the message contains the actual information to be read by recipient**.**

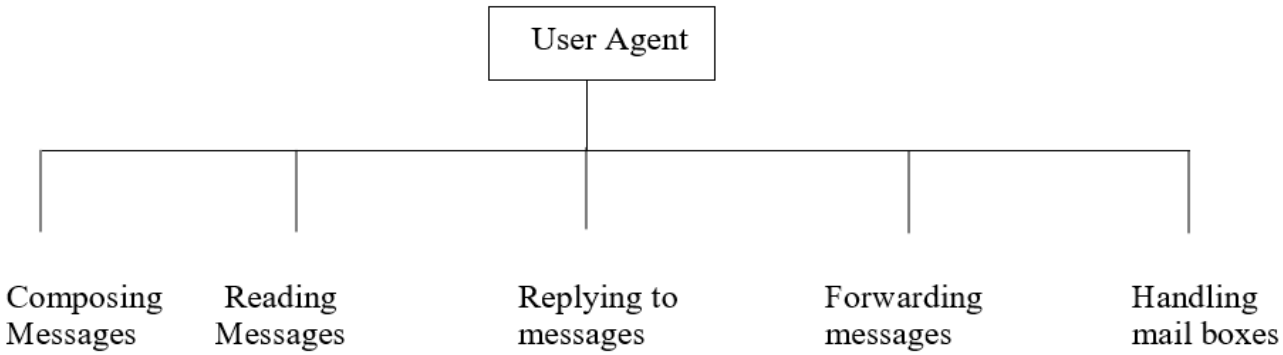
Receiving Mail

The email system periodically checks the mail-boxes. If a user has mail, it informs the user with notice. If the user is ready to read the mail, a list is displayed on the screen which contains brief summary of email.

User Agents

The user agent prepares the message, creates the envelope and puts the message in envelope. Mail transfer agent transfers the mail across the internet.





Composing Messages

User Agent provides a template (or form) on the screen to be filled in by user. A user can use their favourite text editor or word processor to create the message and impart it or cut and paste into the user agent.

Reading Messages

When a user login, first User Agent checks the mail in the incoming mailbox. User Agent show a one-line summary of each received mail which contain the following details Number field of the message, the size of the message, the sender's name, the subject field, flag field, which shows if the mail is new, already read but not replied, read and replied and so on.

Replying Messages

After reading messages, a user can use the user agent to reply to the message. The reply message contains the original message and the new message.

Forwarding Messages

Forwarding means to send the message to the third party. A user agent allows the receiver to forward the message, with or without extra comments to a third party.

Handling Mailboxes

User agent creates two mailboxes

1) Inbox
2) Outbox

Each box is a file with special format that can be handled by user agent. The inbox keeps the entire received emails unit they are deleted by the user. The Outbox keeps all the sent emails until the user deletes them.

SMTP

Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the internet use SMTP to send messages from one server to another. The messages can then be retrieved with an e-mail client using either POP (Post Office Protocol) or IMAP (Internet Message Access Protocol).

SMTP client and SMTP server has two components

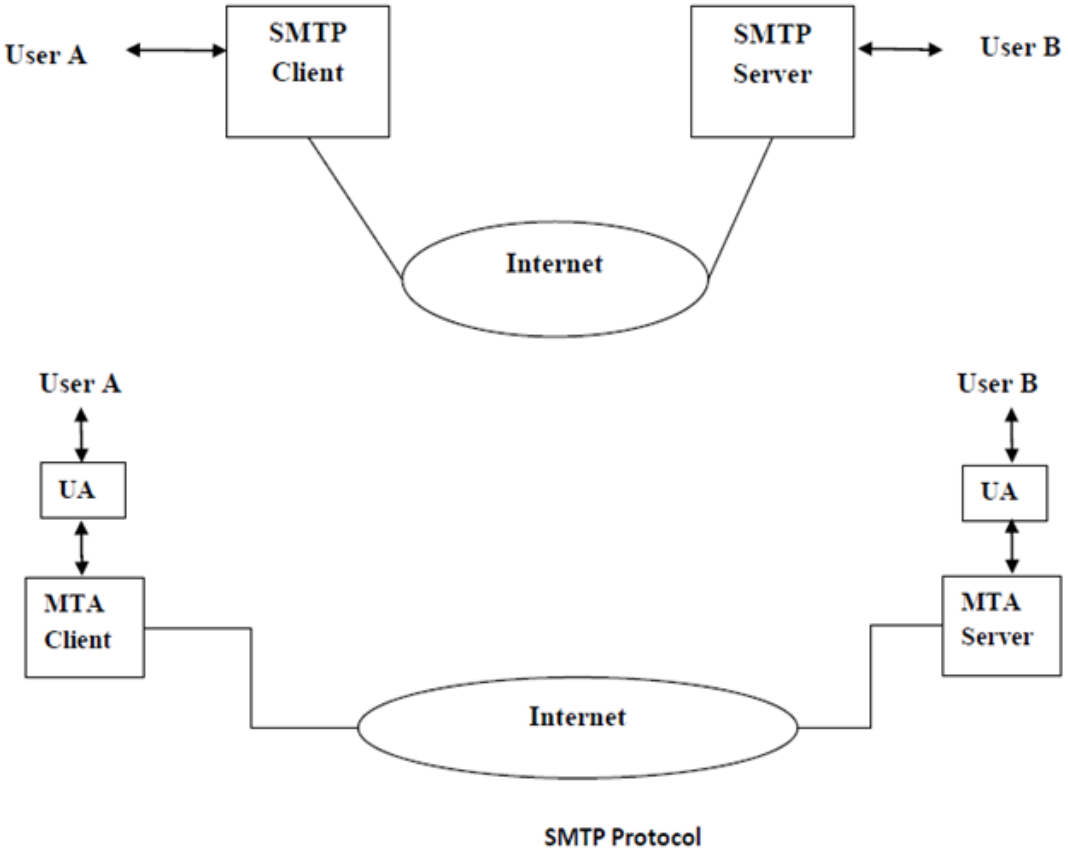
1) UA – User Agent
2) MTA – Mail Transfer Agent

User Agent

The UA prepares the message, creates the envelope and puts the message in envelope.

Mail Transfer Agent

MTA transfers the mail across the internet.



POP3

Post Office Protocol, a protocol used to retrieve e-mail server. Most e-mail applications sometimes called an e-mail client use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol). Local e-mail clients uses the Post Office Protocol version 3 (POP3), an application-layer internet standard protocol, to retrieve e-mail from remote server over TCP/IP connection.

POP3 stands for Post Office Protocol. POP3 is an extremely simple mail access protocol. The user agent of the client opens a TCP connection to the mail server of the server. After TCP connection is established, POP3 progresses through 3 phases: authorization, transaction and update. During first phase, the user agent sends a username and password to authenticate the user. During second phase, the user agent retrieves messages. During third phase, the client issues the quit command to end the POP3 session.

IMAP4

Internet Message Access Protocol, a protocol for retrieving e-mail messages. The latest version, IMAP4 is similar to POP3 but supports some additional features. For example, with IMAP4, you can search through your e-mail messages for keyboards while the messages are still on mail server. You can choose which messages to download to your machine. IMAP was developed at Stanford University in 1986. It is more powerful and complex. It provides extra functions such as:

1) User can check the e-mail header before downloading the mail.
2) User can search the contents of the email for a specific string of characters before downloading.
3) User can partially download e-mail.
4) User can create, delete or rename mailbox on mail server.
5) User can create a hierarchy of mailboxes in a folder for email storage.

MIME

Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages so they can be sent over the internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio and video files via the internet mail systems. In addition, MIME supports messages in character sets other than ASCII. MIME was defined in 1992 by the Internet Engineering Task Force (IETF).

SMTP can send messages only in 7-bit ASCIT format. SMTP has limitation that it cannot be used for languages that are not supported by 7-bit ASCII characters. MIME is supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME is not a mail protocol and cannot replace SMTP it is only an extension to SMTP. Whenever transmission of non-ASCII data at that time MIME and SMTP both are required.

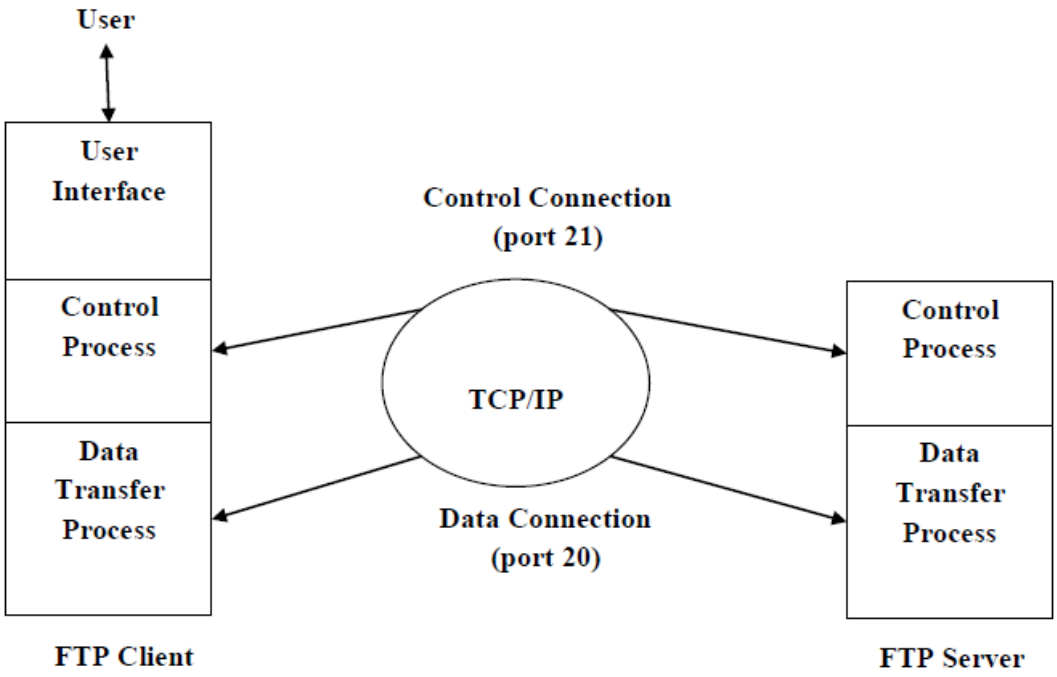
FTP

FTP stands for File Transfer Protocol. FTP is a standard mechanism provided by TCP/IP model for copying a file from one computer to another. Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. File Transfer Protocol, the protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring web pages from a server to user's browser and SMTP for transferring electronic mail across the Internet in that, like these technologies. FTP uses the internet's TCP/IP protocols to enable data transfer.

FTP is most commonly used to download a file from server using the internet or to upload a file to server (e.g. uploading a web page file to a server). Transferring a file from one system to another system suffers from many problems like two systems may use different OS, two systems may use different file name conventions, two systems may have different ways to represent text and data, and two systems may have different directory structures. All of these problems have been solved by FTP.

FTP creates two connections between client and server one connection is used for data transfer and other for control information (Commands and response). Control connection uses very simple rules of communication. We need to transfer only one line of command or one line of response at a time. Data connections, on the other hand needs more complex rules due to variety of data type transferred.

The control connection is made between the control processes. The data connection is made between the data transfer processes. Control connection is maintained during the entire interactive FTP session. The data connection is opened and closed for each file transferred. Port 21 used for the control connection and Port: 20 used for data connection.



TFTP (Trivial File Transfer Protocol)

When we need to simply copy a file without need of all functions of FTP protocol. For Example, when a diskless computer is booted, we need to download files from servers. So, at that time we do not need all the sophistication problems solution provided by FTP. We just require protocol to copy file from one computer to another. Reading file in TFTP means copying file from the server site to client site.

Writing file in TFTP means copying file from client site to server site. TFTP does not have authorization (FTP have authorization). TFTP client and server use UDP protocol instead of TCP. TFTP uses the User Datagram Protocol (UDP) and provides no security features. It is often used by servers to boot devices like routers. TFTP is less powerful than FTP. Code for TFTP requires less memory than the code for FTP.

HTTP

HTTP is said to be a connectionless protocol and is used to interconnect web pages. HTTP stands for Hyper Text Transfer Protocol. WWW is about communication between web clients and servers. Communication between client computers and web servers is done by sending HTTP Requests and receiving HTTP Response. HTTP has some built-in request methods as follows:

Method	Action
GET	Request to read a web page
HEAD	Request to read a web page's header
POST	Sends some information from the client to the server
PUT	Request to store a web page
DELETE	Remove the web page

.

Communication between clients and servers is done by requests and responses:

1) A client (a browser) sends an HTTP request to the web.
2) A web server receives the request.
3) The server runs an application to process the request.
4) The server returns an HTTP response (output) to the browser.
5) The client (the browser) receives the response