UNIT-1 INTRODUCTION TO NETWORK

Introduction:Networks:

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

- **Performance:** Performance can be measured in many ways, including transit time and response time.
  - **Transit time** is the amount of time required for a message to travel from one device to another.
  - **Response time** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.
- **Reliability:** In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.
- **Security:** Network security issues include protecting data from unauthorised access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Need Uses and Advantages of network

Benefits of computer networks Setting up a computer network is a fast and reliable way of sharing information and resources within a business. It can help you make the most of your IT systems and equipment.

ADVANTAGES OF COMPUTER NETWORKING MAIN BENEFITS OF NETWORKS INCLUDE:

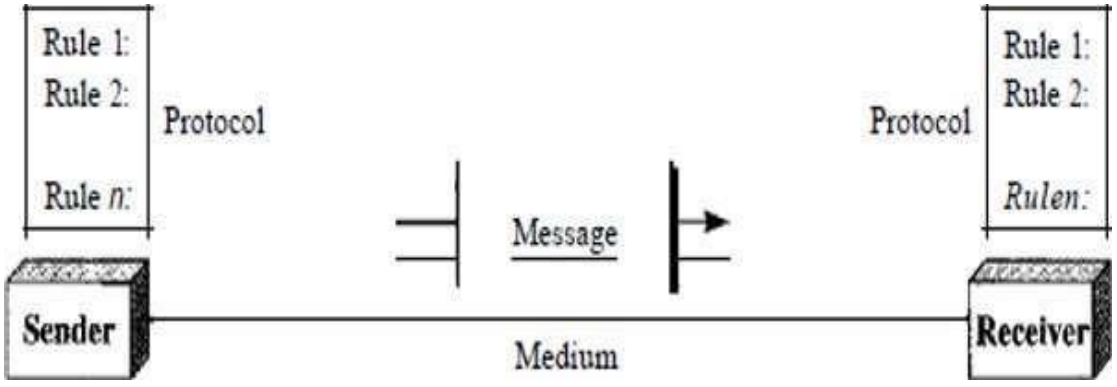
1. File sharing - you can easily share data between different users, or access it remotely if you keep it on other connected devices.
2. Resource sharing - using network-connected peripheral devices like printers, scanners and copiers, or sharing software between multiple users, saves money.
3. Sharing a single internet connection - it is cost-efficient and can help protect your systems if you properly secure the network.
4. Increasing storage capacity - you can access files and multimedia, such as images and music, which you store remotely on other machines or network-attached storage devices.

DISADVANTAGES OR CONS OF HAVING A NETWORK

1. Purchasing the network cabling and file servers can be expensive.
2. Managing a large network is complicated, requires training and a network manager usually needs to be employed.
3. If the file server breaks down the files on the file server become inaccessible. Email might still work if it is on a separate server. The computers can still be used but are isolated.
4. Viruses can spread to other computers throughout a computer network.
5. There is a danger of hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, eg a firewall.

DATA COMMUNICATION:

Component:



- **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
- **Receiver.** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- **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
- **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.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divide into three types:

1. **Simplex Communication:** It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data usinga keyboard, listing music using a speaker, etc.
2. **Half Duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.
3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

1.2 TYPES OF NETWORK:

Clients-Servers, Peer based and Hybrid Networks

CLIENT-SERVER MODEL

- The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients.

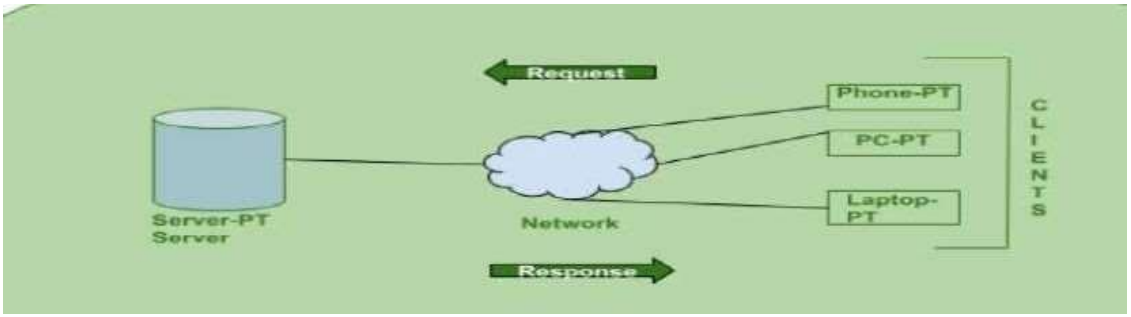
• In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client.
• Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

HOW THE CLIENT-SERVER MODEL WORKS?

The client server computing works with a system of request and response. The client sends a request to the server and the server responds with the desired information.

Client: In the digital world a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: In this digital world a Server is a remote computer which provides information (data) or access to particular services.



ADVANTAGES OF CLIENT-SERVER MODEL:

1. Centralised system with all data in a single place.
2. Cost efficient requires less maintenance cost and Data recovery is possible.
3. The capacity of the Client and Servers can be changed separately.

DISADVANTAGES OF CLIENT-SERVER MODEL:

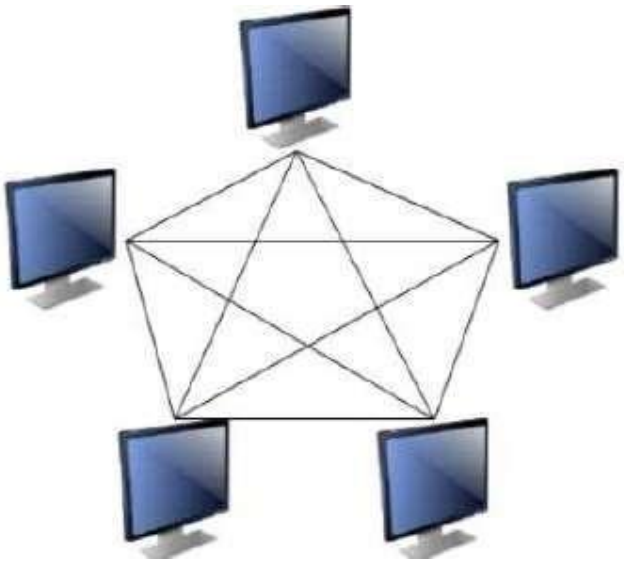
1. Clients are prone to viruses, Trojans and worms if present in the Server oruploaded into the Server.
2. Server are prone to Denial of Service (DOS) attacks.
3. Data packets may be spoofed or modified during transmission.
4. Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

PEER COMPUTER

A computer is called a peer computer when it has rights of both server and client in other words it works both as client and server

PEER TO PEER COMPUTING

- The peer to peer computing architecture contains computers that are equal participants in data sharing.
- All the tasks are equally divided between all the computers.
- The computers interact with each other as required as share resources.A diagram to better understand peer to peer computing is as follows



CHARACTERISTICS OF PEER TO PEER COMPUTING

The different characteristics of peer to peer networks are as follows

- Peer to peer networks are usually formed by groups of a dozen or lesscomputers.
- These computers all store their data using individual security but also share data with all the other nodes.
- The nodes in peer to peer networks both use resources and provideresources.
- So, if the nodes increase, then the resource sharing capacity of the peer to peer network increases. This is different than client server networks where the server gets overwhelmed if the nodes increase.
- Since nodes in peer to peer networks act as both clients and servers, it is difficult to provide adequate security for the nodes. This can lead to denial ofservice attacks.

- Most modern operating systems such as Windows and Mac OS contain software to implement peer to peer networks.

ADVANTAGES OF PEER TO PEER COMPUTING

Some advantages of peer to peer computing are as follows −

- Each computer in the peer to peer network manages itself. So, the network is quite easy to set up and maintain.
- In the client server network, the server handles all the requests of the clients. This provision is not required in peer to peer computing and the cost of the server is saved.
- It is easy to scale the peer to peer network and add more nodes. This only increases the data sharing capacity of the system.
- None of the nodes in the peer to peer network are dependent on the others for their functioning.

DISADVANTAGES OF PEER TO PEER COMPUTING

Some disadvantages of peer to peer computing are as follows −

- It is difficult to backup the data as it is stored in different computer systems and there is no central server.
- It is difficult to provide overall security in the peer to peer network as each system is independent and contains its own data.

HYBRID NETWORKS

- Hybrid networks are the networks that are based on both peer-to-peer & client-server relationship.
- Hybrid networks incorporate the best features of workgroups in peer-to-peer networks with the performance, security and reliability of server-based networks.
- Hybrid networks still provide all of the centralized services of servers, but they also allow users to share and manage their own resources within the workgroup.

ADVANTAGES OF HYBRID NETWORK

1. Client Server application are still centrally located and managed.
2. Users can assign local access to resources in their computers.
3. Workgroups can manage resources without requiring assistance from network administrator.

DISADVANTAGES OF HYBRID NETWORK

1. Users may need to remember multiple passwords.
2. Files can be duplicated and changes overwritten between the computers with the shared folder and the Server.
3. Files saved on the workstation are not backed up.

Different topologies:Physical Structure:

TYPE OF CONNECTION:

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

There are two possible types of connections:

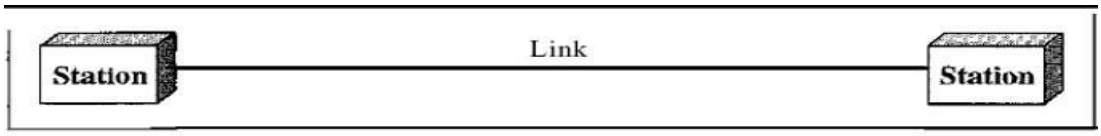
1) point-to-point and
2) multipoint.

Point-to-Point:

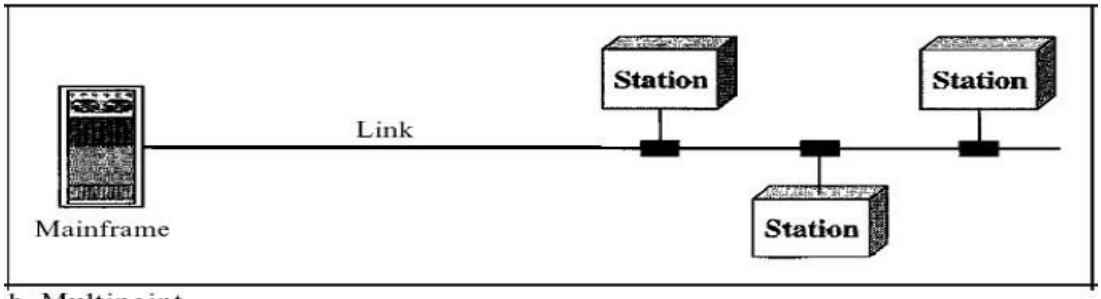
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint:

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.



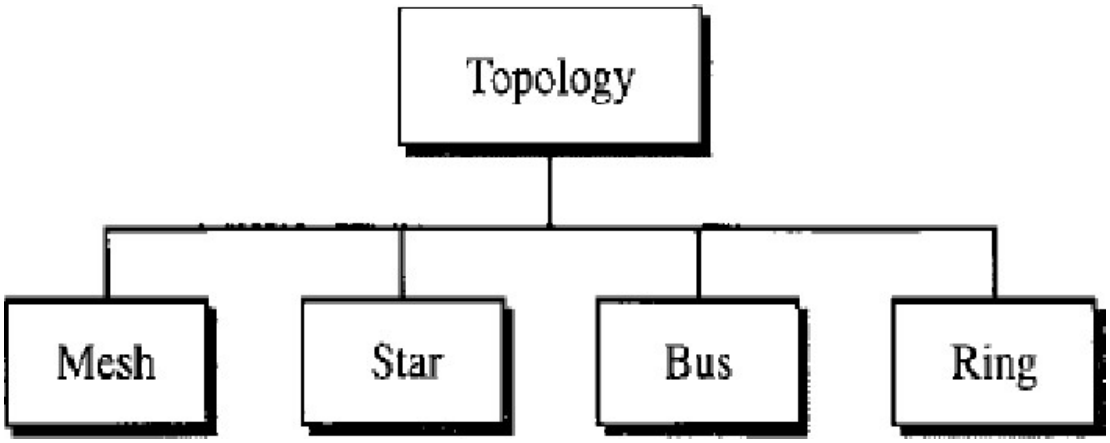
a. Point-to-point



b. Multipoint

Physical Topology

The term physical topology refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

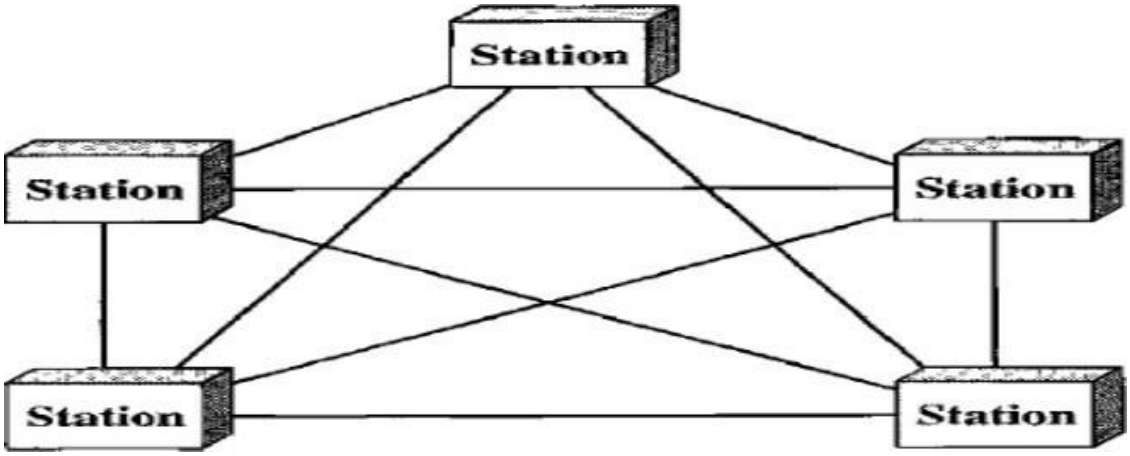


MESH TOPOLOGY:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.

In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links. To accommodate that many links, every device on the network must have n – 1 input/output ports to be connected to the other n - 1 stations.



ADVANTAGES:

1. *No traffic problems:*

The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

2. *ROBUST:*

A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

3. *HIGH PRIVACY OR SECURITY.*

When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users fromgaining access to messages.

4. *EASY FAULT IDENTIFICATION AND FAULT ISOLATION*

point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

DISADVANTAGES:

1. Large amount of cable requirement.

because every device must be connected to every other device**.**

2. *INSTALLATION AND RECONNECTION ARE DIFFICULT.*

To add or remove a system requires lots of connection to beadded or removed.

3. *MORE AVAILABILITY OF SPACE.*

The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

4. *EXPENSIVE*

The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

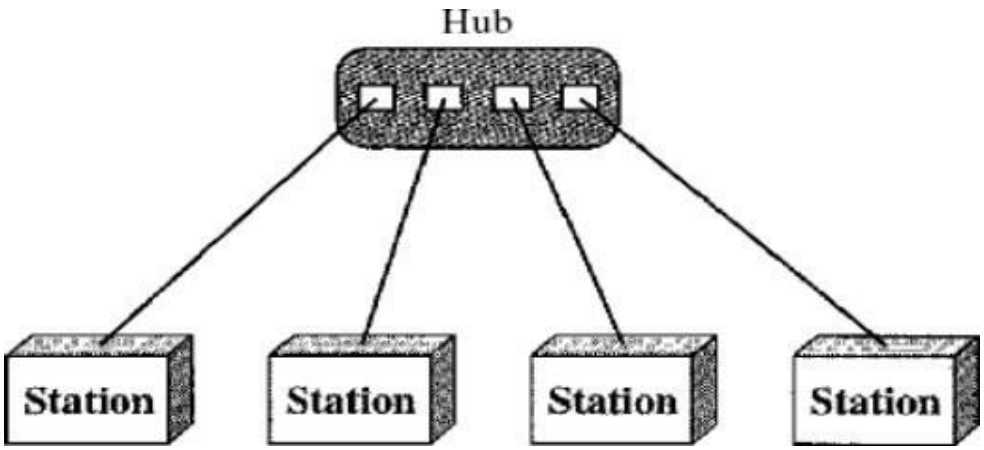
- *MESH TOPOLOGY MAJOR USE*

As a backbone connecting the main computers of a hybrid network that can include several other topologies.

STAR TOPOLOGY:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device

wants to send data to another, it sends the data to the controller, which then relays the data to the other connected devices. .



ADVANTAGES:

- Star topology is less expensive than a mesh topology
- Easy to install and reconfigure.additions, moves, and deletions involve only one connection: between that device and the hub.
- Robust technology.

If one link fails, only that link is affected. All other links remain active.

- Easy fault identification and fault isolation

As long as the hub is working, it can be used to monitor link problems and bypass defective links.

DISADVANTAGES:

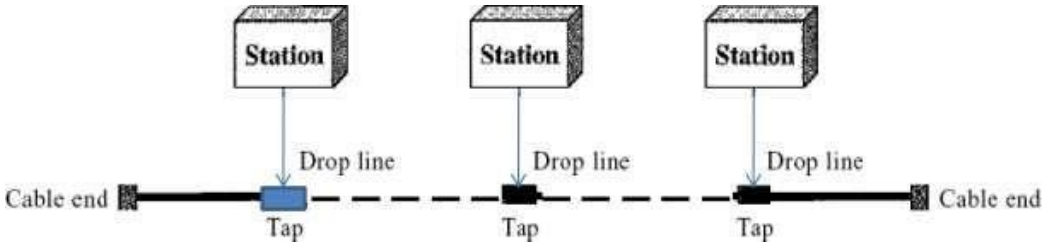
- Dependency on hub.

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole systemis dead.

- Often more cabling is required in a star than in some other topologies (such as ring or bus).

BUS TOPOLOGY:

A bus topology is **multipoint** toplogy . One long cable acts as a backbone to link all the devices in a network as shown



- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the

sheathing of a cable to create a contact with the metallic core.

- As a signal travels along the backbone, some of its energy is transformed into heat.

Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages:

- Ease of installation
- Bus uses less cabling than mesh or star topologies

Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths

Disadvantages :

- Difficult reconnection and fault isolation
- Signal reflection at the taps can cause degradation in quality

- Not a robust technology

  a fault or break in the bus cable stops all transmission

- Creates noise

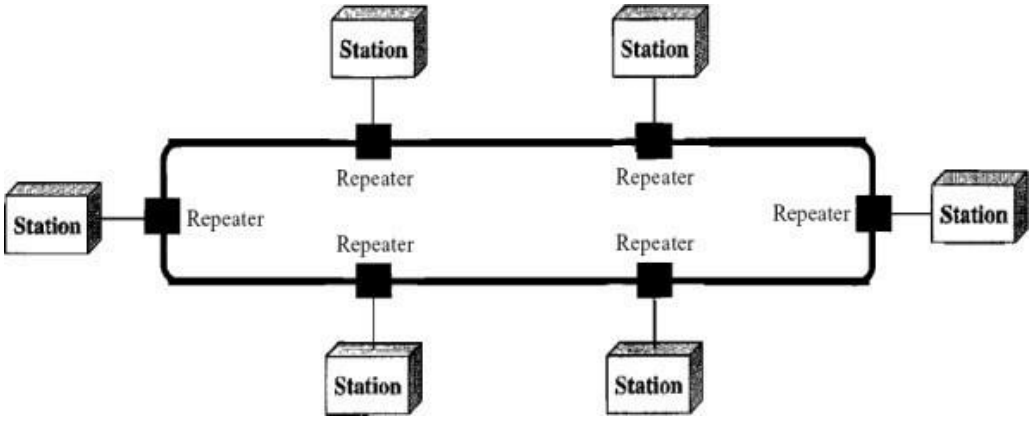
  The damaged area reflects signals back in the direction of origin, creating noise in both directions

WHERE IT IS USED?

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular.

RING TOPOLOGY

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



Advantages:

- Relatively easy to install and reconfigure

  Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.

- Fault isolation is simplified

Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

- unidirectional traffic can be a disadvantage
- Not a robust technology.

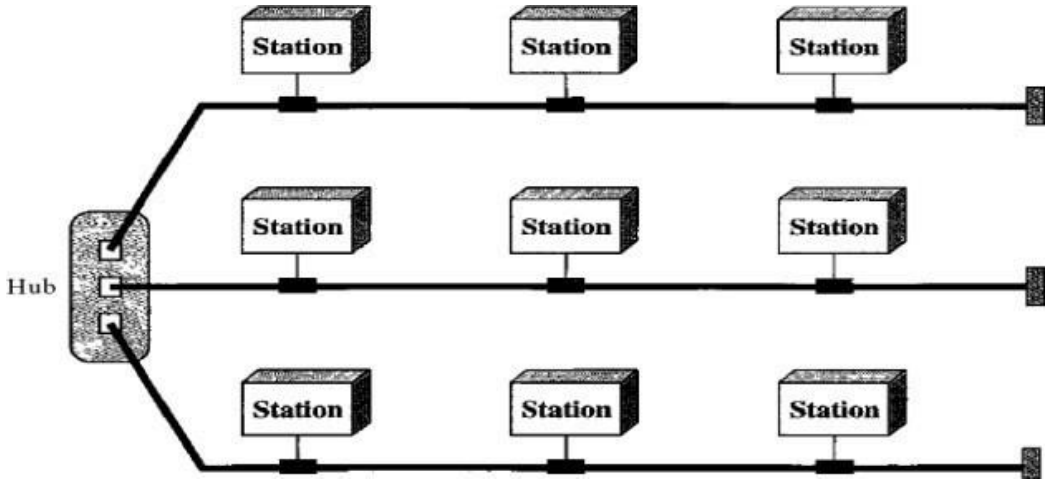
A break in the ring (such as a disabled station) can disable the entire network

HYBRID TOPOLOGY

Star-bus topology (Tree Topology)

Tree Topology is a topology which has a tree structure in which all the computers are connected like the branches which are connected with the tree. In Computer Network, tree topology is called a combination of a Bus and Star network topology.Tree network topology is considered to be the simplest topology in all the topologies which is having only one route between any two nodes on the network.

We can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure.



Advantages:

- This topology provides a hierarchical as well as central data arrangement of the nodes.
- The other nodes in a network are not affected if one of their nodes gets damaged or does not work.
- Tree topology provides easy maintenance and easy fault identificationcan be done.

Disadvantages:

- This network is very difficult to configure as compared to the other network topologies.
- Due to the presence of a large number of nodes, the network performance of tree topology becomes a bit slow.
- Requires a large number of cables compared to star and ring topology**.**

CATEGORIES OF NETWORKS

- *LOCAL AREA NETWORKS:*

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometres in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

1. Their size

   LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management.

2. Their transmission technology

   LANs may use a transmission technology consisting of a cable to which all the machines are attached

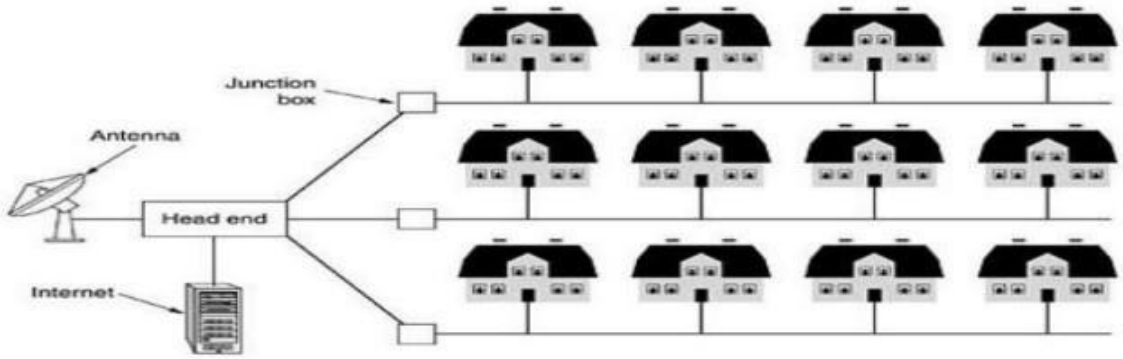
3. Their topology.

   lan can use any topology like bus or ring

METROPOLITAN AREA NETWORK (MAN):

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. a MAN might look something like the system shown in Fig. In this figure both television signals and Internet are fed into the centralised head end for subsequent distribution to people's homes. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardised as IEEE 802.16.

Metropolitan area network based on cable TV.



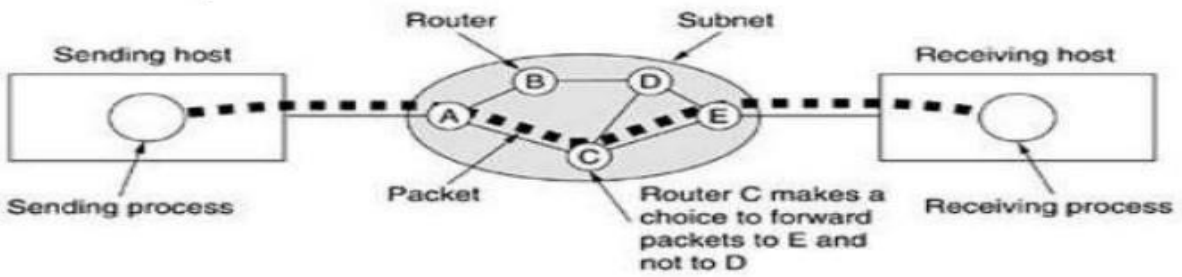
WIDE AREA NETWORK (WAN).

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements

1. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links.
2. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet
3. Nearly all wide area networks (except those using satellites) have store-and-forward subnets.

stream of packets from sender to receiver.



In this figure, all the packets follow the route ACE, rather than ABDE or ACDE. In some networks all packets from a given message must follow the same route; in others each packed is routed separately. Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually Routed.

DEFINITIONS:

INTERNET:

- It is a worldwide/global system of interconnected computer networks. It uses the standard Internet Protocol (TCP/IP). Every computer in Internet is identified by a unique IP address. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location**.**

INTRANET:

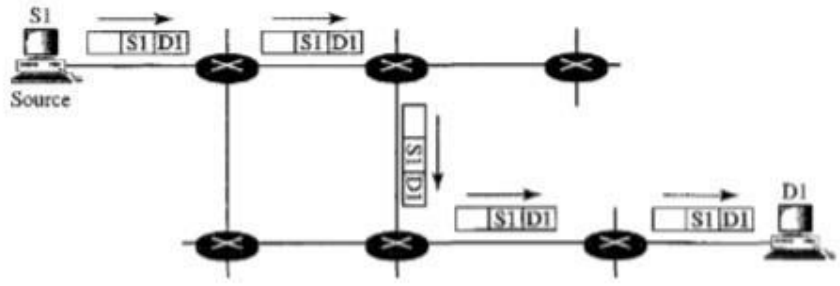
- Intranet is the system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. Usually each organization has its own Intranet network and members/employees of that organization can access the computers in their intranet.

UNICAST:

- In unicast communication, there is one source and one destination. The relationship between the source and the destination is one-to-one. In this type of communication, both the source and destination addresses, in the IP

datagram, are the unicast addresses assigned to the hosts (or host interfaces, to be more exact.

Figure 22.33 *Unicasting*



- A unicast packet staI1s from the source S1 and passes through routers to reach the destination D1. In unicasting, when a router receives a packet, it forwards the packet through only one of its interfaces (the one belonging to the optimum path) as defined

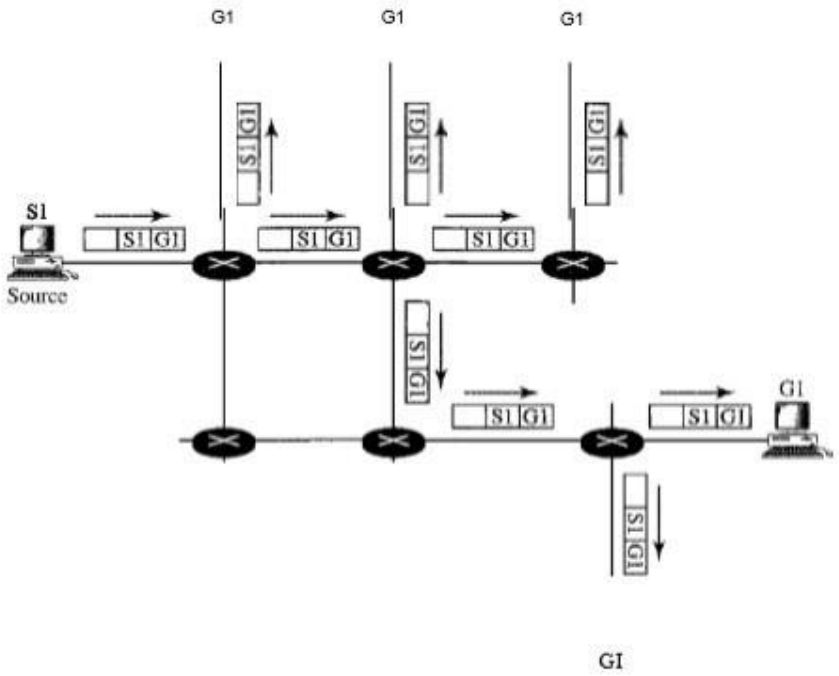
in the routing table. The router may discard the packet if it cannot find the destination address in its routing table.

- In unicasting, the router forwards the received packet through only one of its interfaces.

MULTICAST:

- In multicast communication, there is one source and a group of destinations. The relationship is one-to-many. In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations. The group address identifies the members of the group.

Figure 22.34 *Multicasting*



- A multicast packet starts from the source S1 and goes to all destinations that belong to group G1. In multicasting, when a router receives a packet, it may forward it through several of its interfaces.
- In multicasting, the router may forward the received packet through several of its interfaces.

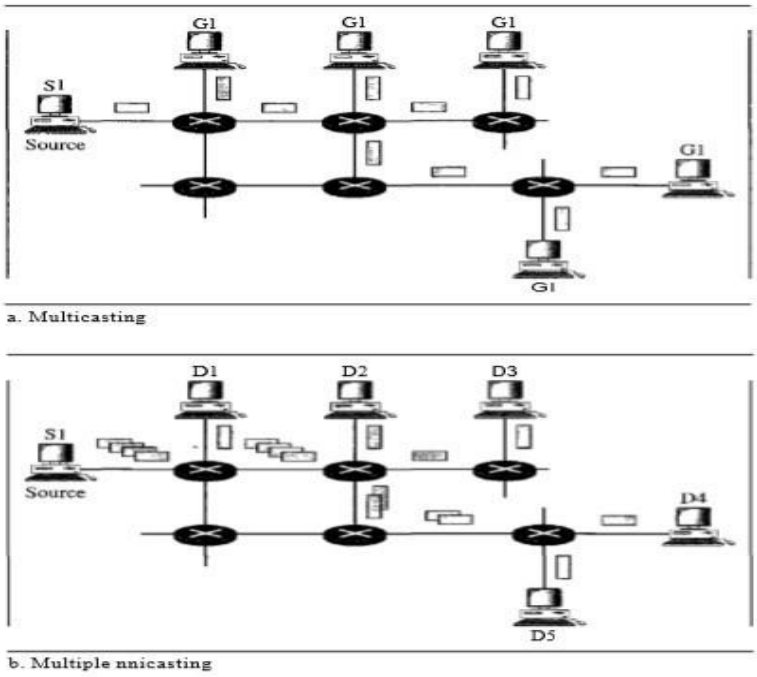
BROADCAST:

- In broadcast communication, the relationship between the source and the destination is one-to-all. There is only one source, but all the other hosts are the destinations. The

Internet does not explicitly support broadcasting because of the huge amount of traffic it would create and because of the bandwidth it would need. Imagine the traffic generated in the Internet if one person wanted to send a message to everyone else connected to the Internet.

Multicasting Versus Multiple Unicasting

Figure 22.35 *Multicasting versus multiple unicasting*



- Multicasting starts with one single packet from the source that is duplicated by the routers. The destination address in each packet is the same for all duplicates. Note that only one single copy of the packet travels between any two routers.
- In multiple unicasting, several packets start from the source. If there are five destinations, for example, the source sends five packets, each with a different unicast destination address. Note that there may be multiple copies travelling between two routers. For example, when a person sends an e-mail message to a group of people, this is multiple unicasting. The e-mail software creates replicas of the message, each with a different destination address and sends them one by one. This is not multicasting; it is multiple unicasting.

UNIT-2 INTERNET & INTRANET

Concept of Internet And IntranetInternet:

The Internet is used to connect the different networks of computers simultaneously. It is a public network therefore anyone can access the internet. On the internet, there are multiple users and it provides an unlimited amount of information to the users.

Intranet:

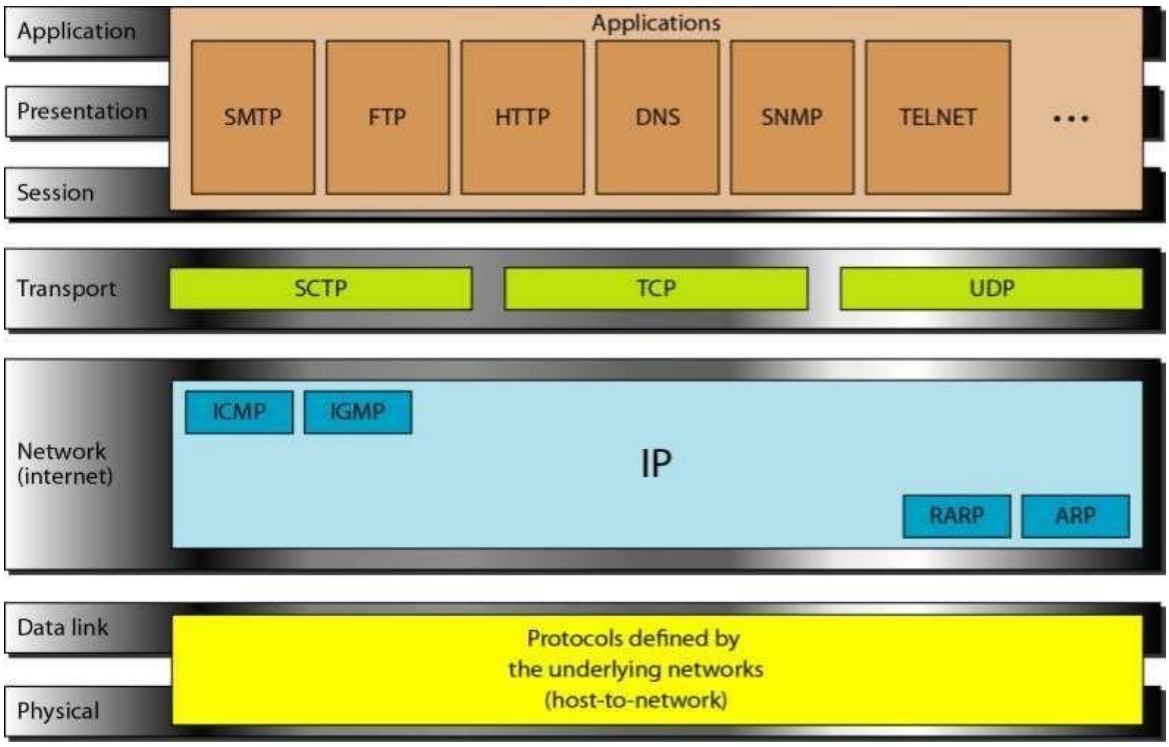
Intranet is the type of internet that is used privately. It is a private network therefore anyone can't access the intranet. On the intranet, there is a limited number of users and it provides a piece of limited information to its users.

Working of Internet & its architecture:

The Internet is called the network of networks. It is a global communication system that links together thousands of individual networks. In other words, internet is a collection of interlinked computer networks, connected by copper wires, fiber-optic cables, wireless connections, etc. As a result, a computer can virtually connect to other computers in any network. These connections allow users to interchange messages, to communicate in real time.

Architecture of the Internet:

Internet architecture is a meta-network, which refers to a congregation of thousands of distinct networks interacting with a common protocol. In simple terms, it is referred to as an internetwork that is connected using protocols. Protocol used is TCP/IP.
The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.



Working of Intranet & its Architecture:

- The intranet is a private network that belongs to a particular organization. It is designed for the exclusive use of an organization and its associates, such as employees, customers, and other authorized people.
- It offers a secure platform to convey information and share data with authorized users. Confidential information, database, links, forms, and applications can be made available to the staff through the intranet.
- So, it is like a private internet or an internal website that is operating within an organization to provide its employees access to its information and records. Each computer in intranet is identified by a unique IP Address.
- It is based on internet protocols (TCP/IP) and is protected from unauthorized access with firewalls and other security systems. The firewall monitors the incoming and outgoing data packets to ensure they don't contain unauthorized requests.
- So, users on the intranet can access the internet, but the internet users can't access the intranet if they are not authorized for it. Furthermore, to access the intranet, the authorized user is required to be connected to itsLAN (Local Area Network).

HOW INTRANET WORKS?

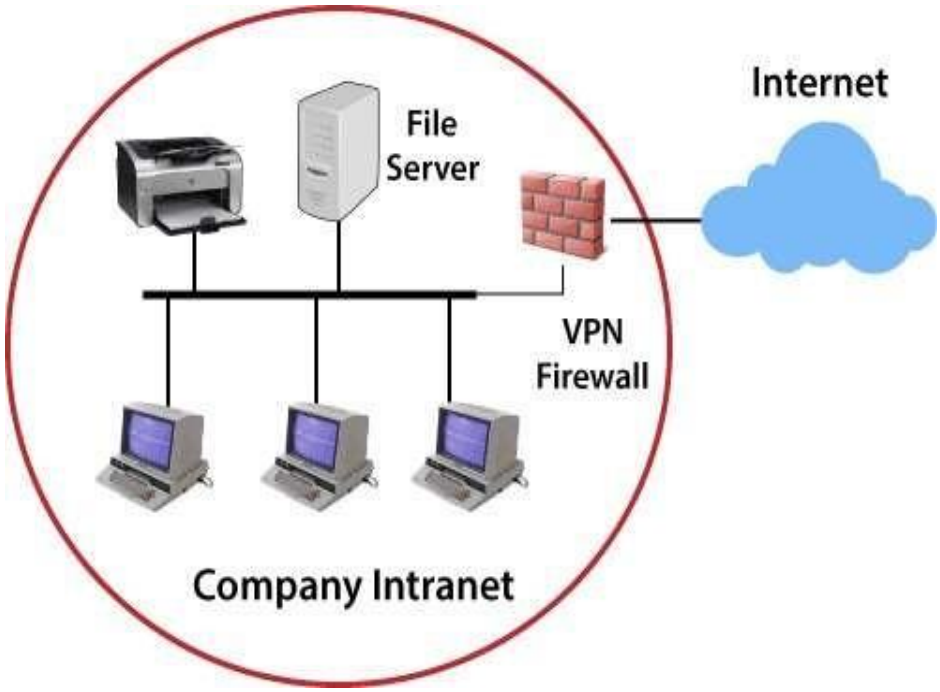
Intranet basically comprises three components:

1) a web server,
2) an intranet platform, and
3) applications.

The web server is hardware that contains all the intranet software and data. It manages all requests for files hosted over the server and finds the requested files and then delivers it to the user's computer.

The intranet platform, which is software, allows communication tools, collaboration apps, and databases to work seamlessly with each other.

The applications are required to enable users to work smoothly. They are the computing tools that allow users to do their work, communicate, and coordinate with each other and retrieve and store information.



The user who wants to access the intranet is required to have a special network password and should be connected to the LAN. A user who is working remotely can gain access to the intranet through a virtual private network (VPN) that allows them to sign in to the intranet to accessthe information.

EXAMPLE OF INTRANET:

Educational Intranet: It is generally found in a school, college, etc., For example, a school intranet is intended to allow teaching staff to communicate with each other and get information about upcoming updates such as exam dates, schools functions, holidays, etc.

Health Care Intranet: In the healthcare sector, in big hospitals, the Intranet helps health care professionals to work as a team to provide proper care and treatment to their patients. Doctors can share reports, treatment procedures, bills and claims can be settled easily without moving from onedepartment to another department.

ADVANTAGES:

1) It is cheap and easy to implement and run, and is more safe than theinternet.
2) It provides a secure space to store and develop applications to support business operations.
3) Information is shared in real-time, or updates are reflected immediately to all the authorized users.
4) It can work with mobile devices, which means it can provide information that exists on intranet directly to mobile devices of employees such as phones, tablets, etc.

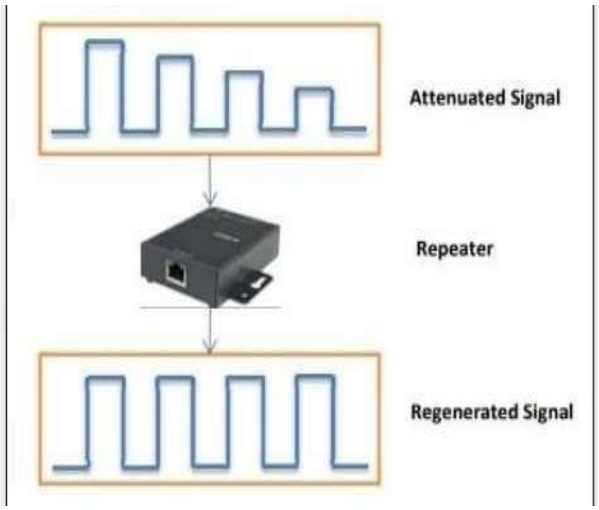
DISADVANTAGES:

1) It may be costly to set up an Intranet due to hidden costs and complexity.
2) If the firewall does not work properly or not installed, it can be hacked by someone High-security passwords are required, which cannot be guessed byoutside users
3) There is always a fear of losing control over the intranet
4) Sometimes document duplication may happen which can cause confusion among employees

NETWORK DEVICES TERMINOLOGIES:

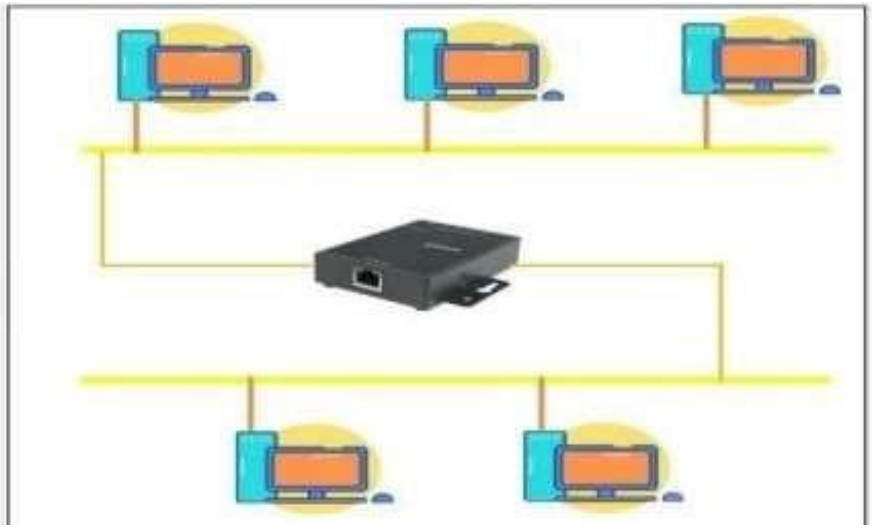
HUB, MODEM, SWITCH, ROUTERS, GATEWAYS, ACCESS POINTREPEATER

- Repeaters are network devices operating at physical layer of the OSImodel
- Repeaters amplify or regenerate an incoming signal before retransmitting it.
- They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



WHY ARE REPEATERS NEEDED?

- When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated(reduced) by installing repeaters at certain intervals.
- Repeaters amplifies the attenuated signal and then retransmits it. Digital repeaters can even reconstruct signals distorted by transmission loss. So, repeaters are popularly incorporated to connect between two LANs thus forming a large single LAN. This is shown in the following diagram −



ADVANTAGES OF REPEATERS

1. Repeaters are simple to install and can easily extend the length or the coverage area of networks.
2. They are cost effective.
3. Repeaters don't require any processing overhead. The only time they need to be investigated is in case of degradation of performance.
4. They can connect signals using different types of cables.

DISADVANTAGES OF REPEATERS

1. Repeaters cannot connect dissimilar networks.
2. They cannot differentiate between actual signal and noise.
3. They cannot reduce network traffic or congestion.
4. Most networks have limitations upon the number of repeaters thatcan be deployed.

Note: **Repeaters** Traditionally, any discussion of networking comp onents would include repeaters, but today repeaters are a little outdated.

HUB:

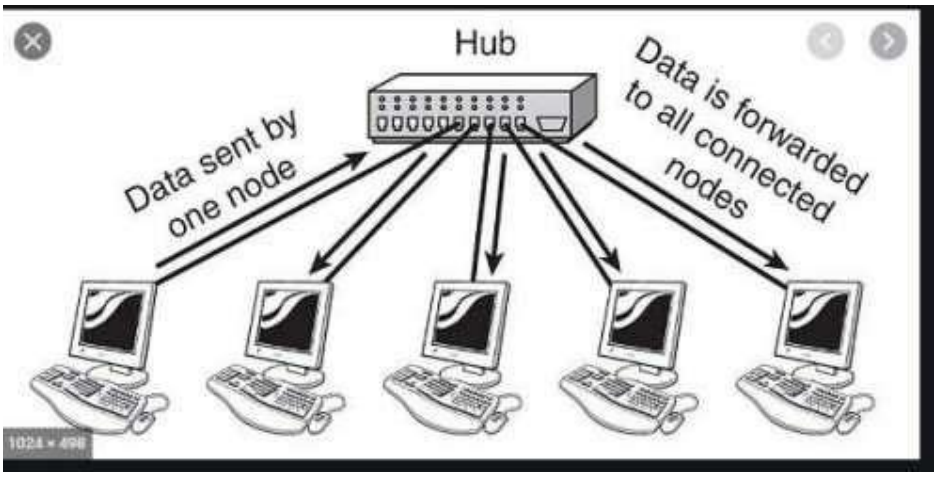
- Hubs are network devices operating at physical layer of the OSImodel
- Computers connect to a hub via a length of twisted-pair cabling
- hub to be connected to another hub to create larger networks which is called cascading, done through BNC connectors.
- The **BNC connector** (initialism of Bayonet Neill–Concelman) is a miniature quick connect/disconnect radio frequency connector usedfor coaxial cable.

- Typically hub can connect from 8 to 24 connections together.
- There are three types of hubs:

1) Active hub
2) Passive Hub and
3) Intelligent hub .

- ACTIVE HUB :
  Active regenerate a signal before forwarding it to all the ports on the device and requires a power supply. Small workgroup hubs normally use an external power adapter, but on larger units the power supply is built in.
- PASSIVE HUBS:
  which today are seen only on older networks, do not need power and they don't regenerate the data signal. It is just a connector that connects the wires coming from different branches.
- INTELLIGENT HUB
  regenerates the signal ,performs network management and intelligent path selection.

  FUNCTIONS:
- like repeater hubs can also regenerate signal
- The basic function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub. This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices
- Due to the inefficiencies of the hub system and the constantly increasing demand for more bandwidth, hubs are slowly but surely being replaced with switches.



WHAT IS THE DIFFERENCE BETWEEN A HUB AND A REPEATER?

- Repeater has two ports: one for incoming signal and another one for "boosted" outgoing signal. Hub is able to join more than two signals. It takes the signal, "boosts" it, and transmits to all its ports. Typically hub can connect from 8 to 24 connections together.

ADVANTAGES:

- It supports various types of Network Media.
- It is very cheap that anyone can use it.
- Using the Hub does not make any difference in Network performance.
- Many different media types can be easily connected with Hub.

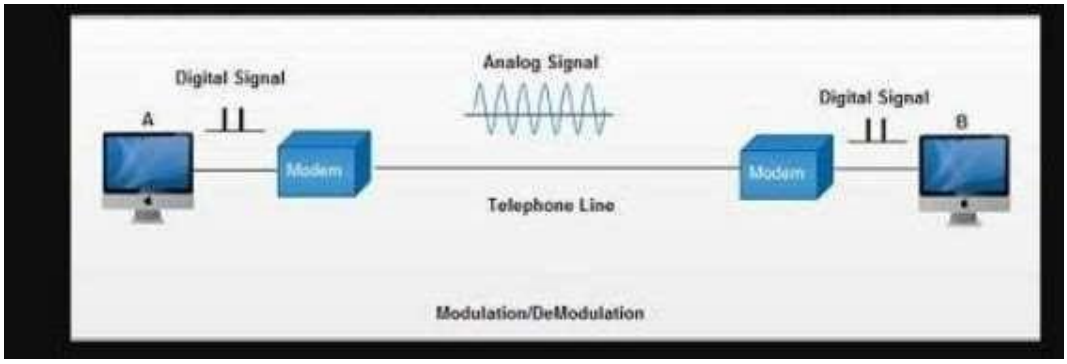
DISADVANTAGES:

- Network cannot Reduce traffic.
- It can not select Network's Best Path.
- The Hub network cannot be divided into the Segment.
- There is no mechanism of any kind to reduce network traffic**.**

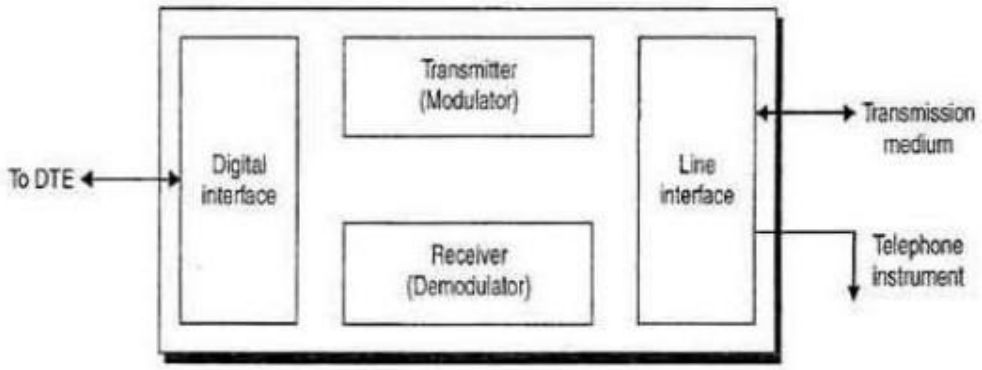
MODEM:

- Modem is abbreviation for Modulator – Demodulator.
- Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.

- When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.



- The modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier. This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.



Building blocks of a modem

- The transmission medium between the two modems can be dedicated circuit or a switched telephone circuit. If a switched telephone circuit is used, then the modems are connected to the local telephone exchanges. Whenever data transmission is required connection between the modems is established through telephone exchanges.
- The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − modulator and demodulator.

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

Digital Data Waveform

Analog Data Waveform

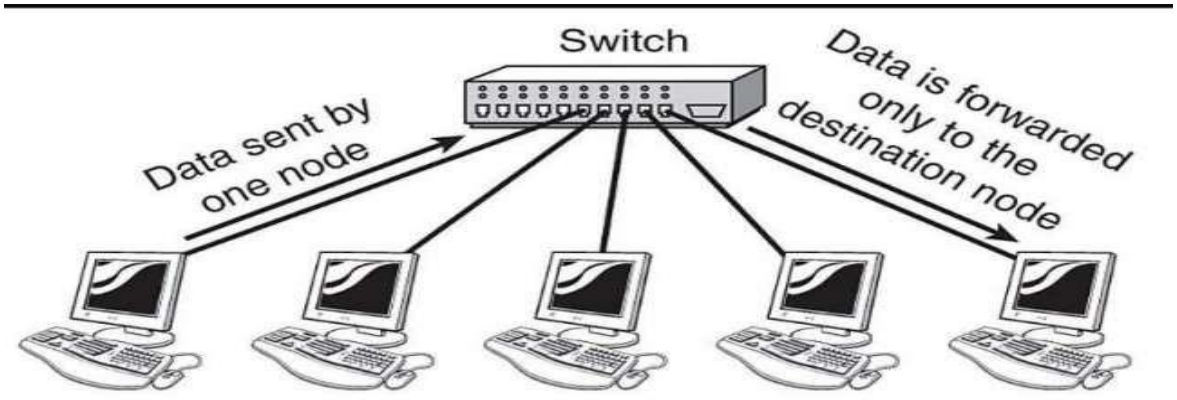
- Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.
- Depending on direction of data transmission, modem can be of these types –
  - **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digitaldevice (demodulator).
  - **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
  - **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

- ADVANTAGES:
  - More useful in connecting LAN with the internet
  - Speed depends on the cost
  - A modem is most probably widely used in data communication roadway
  - A modem converts that the digital signal into an analog signal

- DISADVANTAGES:
  - Acts just as an interface between LAN and internet
  - No traffic maintenance is present
  - Slow speed when compared to the hub
  - A modem is not understood the intermediate process
  - A limited number of a system can be connected
  - The modem does not know about the own destination path

SWITCH:

- It can perform in both the second and the third layer of the OSI Model, the Data-Link and the Network layer respectively.
- **Layer 2 switch:** While in the Data-Link layer, it can successfully perform the task of a Switch by forwarding all the frames to the required devices using the MAC Addresses.
- **Layer3 switch:** Furthermore, it can also perform the task of a Router; it can receive data Packets and successfully forward them to their destination IP Addresses to make sure that they reach their destination.
- Rather than forwarding data to all the connected ports like hub, a switch forwards data only to the port on which the destination system is connected. It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine the correct port. A MAC address is a unique number that is stamped into every NIC. By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically.
- Switches can also further improve performance over the performance of hubs by using a mechanism called full-duplex . In full-duplex mode it can send and receive data on the connection at the same time. In a full-duplex connection, the maximum data throughput is double that for a half-duplex connection.



- SWITCHING METHODS

Switches use three methods to deal with data as it arrives:

- **Cut-through**—In a cut-through configuration, the switch begins to forward the packet as soon as it is received. No error checking is performed on the packet, so the packet is moved through quickly. The downside of cut-through is that because the integrity of the packet is not checked, the switch can propagate errors.
- **Store-and-forward**—In a store-and-forward configuration, the switch waits to receive the entire packet before beginning to forward it. It also performsbasic error checking.
- **Fragment-free**—Building on the speed advantages of cut-through switching, fragment-free switching works by reading only the part of the packet that enables it to identify fragments of a transmission.
- As you might expect, the store-and-forward process takes longer than the cut-through method, but it is more reliable. In addition, the delay caused by store-and-forward switching increases with the packet size. The delay caused by cut-through switching is always the same—only the address portion of the packet is read, and this is always the same size, regardless of the size of the data packet. The difference in delay between the two protocols is high. On average, cut-through switching is 30 times faster than store-and-forward switching.
- It might seem that cut-through switching is the obvious choice, but today's switches are fast enough to be able to use store-and-forward switching and still deliver high performance levels.

- Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

BENEfiTS OR ADVANTAGES OF SWITCHES

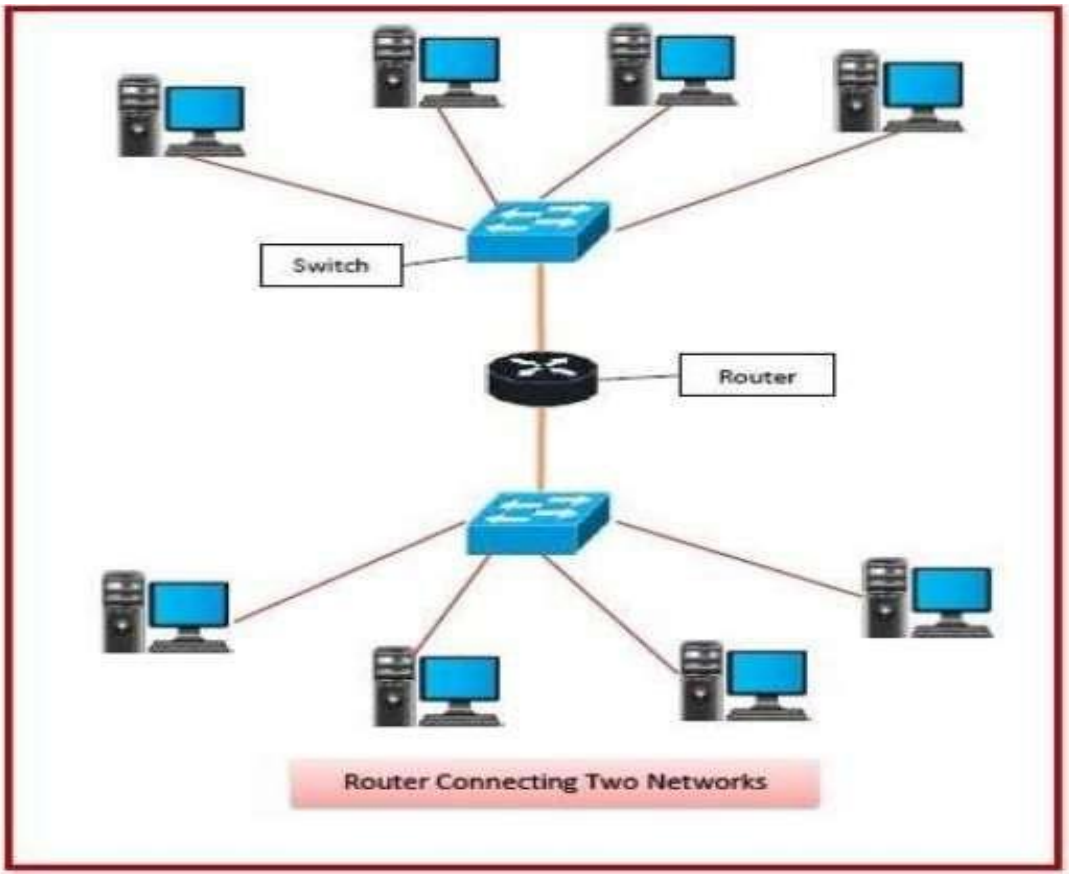
- They increase the available bandwidth of the network.
- They help in reducing workload on individual host PCs.
- They increase the performance of the network.
- Networks which use switches will have less frame collisions. This is due to the fact that switches create collision domains for each connection.
- Switches can be connected directly to workstations.

DRAWBACKS OR DISADVANTAGES OF SWITCHES

- They are more expensive compared to network bridges.
- Network connectivity issues are difficult to be traced through the networkswitch.
- Broadcast traffic may be troublesome.
- If switches are in random mode, they are vulnerable to security attacks e.g. spoofing IP address or capturing of ethernet frames.
- Proper design and configuration is needed in order to handle multicast packets.
- While limiting broadcasts, they are not as good as routers.

ROUTERS:

- Routers are networking devices operating at layer 3(Network layer) or a network layer of the OSI model.
- They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.



ROUTING TABLE

The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

A routing table typically contains the following entities −

1. IP addresses and subnet mask of the nodes in the network
2. IP addresses of the routers in the network
3. Interface information among the network devices and channels

ROUTING TABLES ARE OF TWO TYPES −

Static Routing Table − Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.

Dynamic Routing Table − Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

FUNCTIONS OF A ROUTER:

1) Forwarding –

Router receives the packets from its input ports, checks it header, performs some basic functions like checking checksum and then looks upto the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.

2) Routing –

Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table which is made using different algorithms by the router only.

TYPES OF ROUTERS

A variety of routers are available depending upon their usages. The main types of routers are −

1) WIRELESS ROUTER −
They provide WiFi connection WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.

2) BROADBAND ROUTERS −
They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by theInternet Service Provider (ISP).

3) CORE ROUTERS −
They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used byISP and communication interfaces.

4) EDGE ROUTERS −
They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external
networks, and are suitable for transferring data packets acrossnetworks.
There are two types of edge routers, subscriber edge routers andlabel edge routers.

BENEfiTS OR ADVANTAGES OF ROUTERS

- It provides connections between different network architectures such as ethernet & token ring etc.
- It can choose the best path across the internet work using dynamicrouting algorithms.

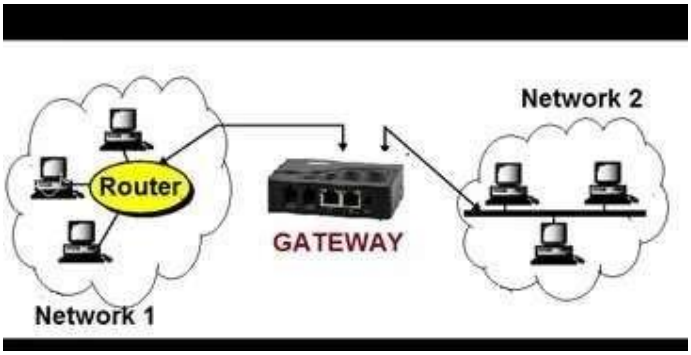
- It can reduce network traffic by creating collision domains and also by creating broadcast domains.
- It provides sophisticated routing, flow control and traffic isolation.
- They are configurable which allows network manager to make policy based on routing decisions.

DRAWBACKS OR DISADVANTAGES OF ROUTERS

- They operate based on routable network protocols.
- They are expensive compared to other network devices.
- Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
- They are slower as they need to analyze data from layer-1 throughlayer-3.
- They require considerable amount of initial configurations.
- They are protocol dependent devices which must understand the protocol they are forwarding.

GATEWAYS:

- Gateway is normally a computer that operates in all five layers of internet or seven layers of OSI model.
- It can be used as a connecting device between two networks that use different models.
- A gateway is **a network node used in telecommunications that connects two networks with different transmission protocols together**. Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.
- For example,One network using OSI model and another using the Internet model. We can connect these two different networks by gateway.
- Gateway is also called protocol translator.
- A gateway takes an application message,reads it and interprets it.
- In the network for an enterprise ,a computer server acting as a gateway node is often also acting as a proxy server and a firewall server .So Gateways can also provide security.
- The gateway (or default gateway) is implemented at the boundary of a network to manage all the data communication that is routed internally or externally from that network.
- Gateways serve as the entry and exit point of a network; all the data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths.Generally ,a router is configured to work as a gateway device in computer networks.
- The Primary Goal of Gateway is to translate with one protocol then onto the next, while the Router is to Route traffic starting with one network then onto the next.



ACCESS POINT:

In computer networking, a **wireless access point** (**WAP**), or more generally just **access point** (**AP**), is a networking hardware device that allows other wireless-capable devices to connect to a wired network.

As a standalone device, the AP may have a wired connection to a router, but, in a wireless router, it can also be an integral component of the router itself.

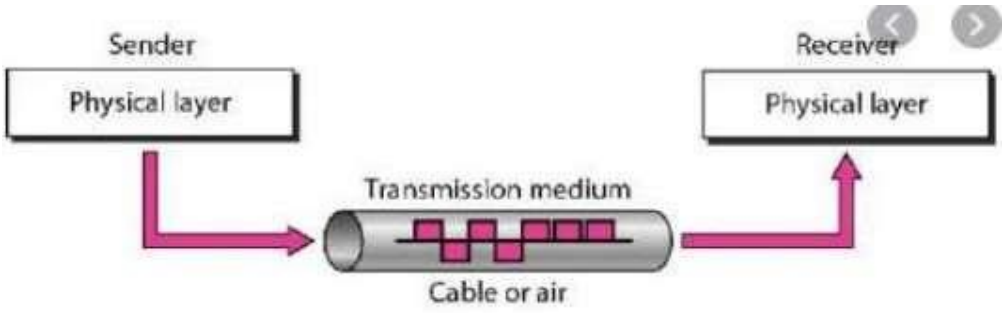
It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.

wireless access point

An access point is a wireless network device that acts as a portal for devices to connect to a local area network. Access points are used for extending the wireless coverage of an existing network and for increasing the number of users that can connect to it.

TYPES OF CABLES: CO-AXIAL, UTP, FIBER OPTIC CABLE TRANSMISSION MEDIA

- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable, orfiber-optic cable.
- The information is usually a signal that is the result of a conversion of data from another form

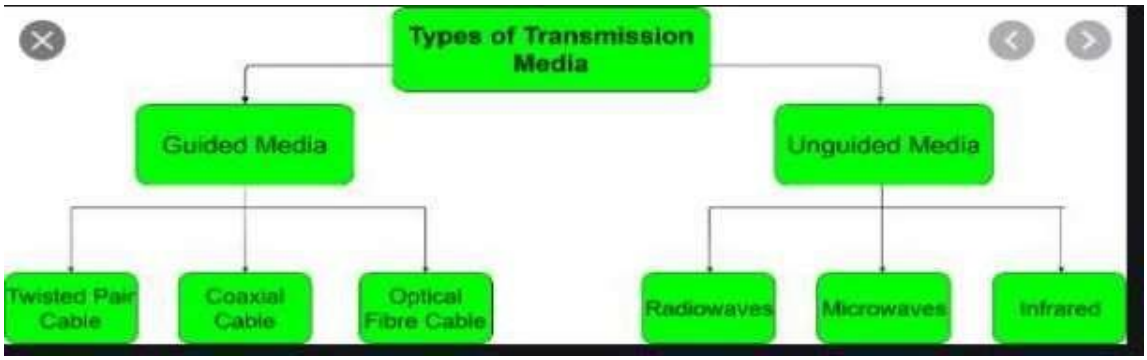


GUIDED AND UNGUIDED MEDIA

- In telecommunications, transmission media can be divided into twobroad categories:

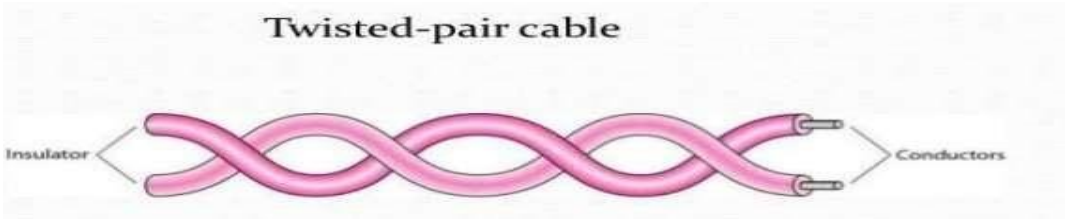
- GUIDED AND
- **Unguided**
- Guided media, which are those that provide a conduit from one device to another,include twisted-pair cable, coaxial cable, and fiber-optic cable.

1. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
2. Optical fiber is a cable that accepts and transports signals in the form of light.
3. Unguided medium is free space



TWISTED-PAIR CABLE(GUIDED MEDIA)

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure

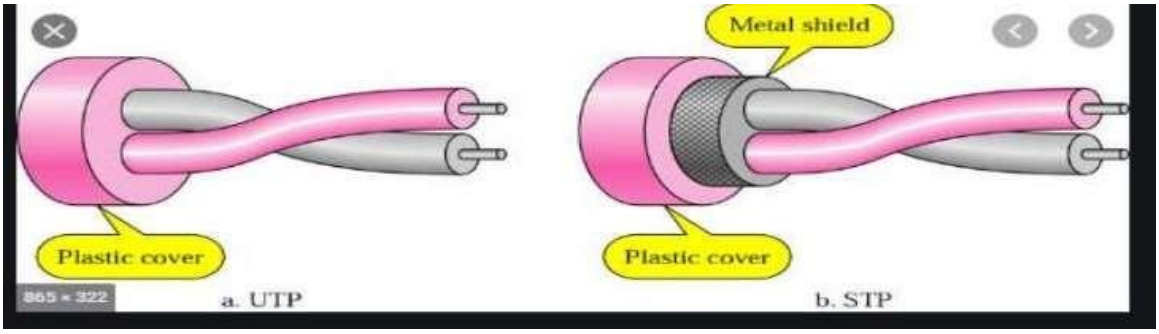


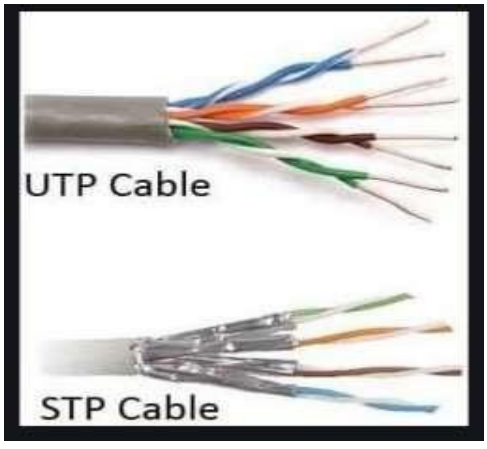
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference
- In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.
- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver
- By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.

- Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out.
- More the turns in the wire per foot more the noise will be reduced
- Analog and digital both the signals can be transmitted using this media.
- This cable is of two types:
  - Shielded Twisted Pair(STP) and
  - Unshielded Twisted Pair(UTP)

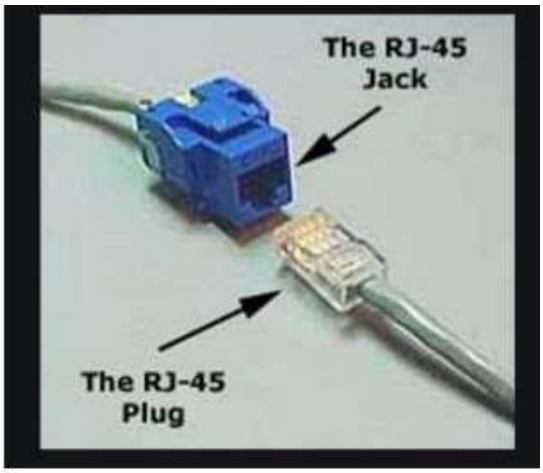
SHIELDED TWISTED PAIR(STP)

- The STP cable is covered by a mesh due to which it is more secure and also the transmission rate is high
- Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk
- It is bulkier and more expensive.





The connector of twisted pair is RJ45



APPLICATION

- Twisted-pair cables are used in telephone lines to provide voice anddata channels
- The DSL (digital subscriber line)lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local-area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

ADVANTAGES OF TWISTED-PAIR CABLE

- It is cheap and easy to install.
- Greater transmission rate.
- Capacity is high.

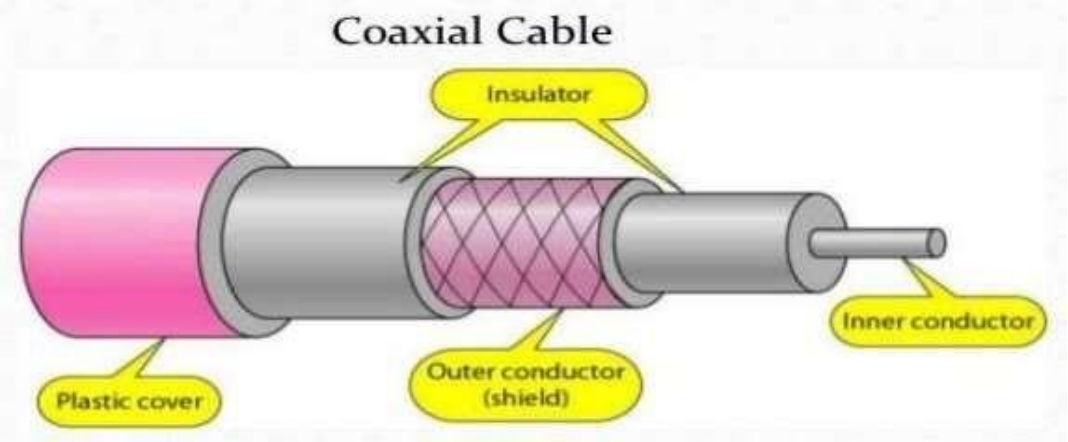
DISADVANTAGES OF TWISTED-PAIR CABLE

- Higher attenuation rate.
- Shielded cable is costlier than coaxial and unshielded cable.
- Useful in a short distance (due to attenuation).

COAXIAL CABLE(GUIDED MEDIA)

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable
- coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two

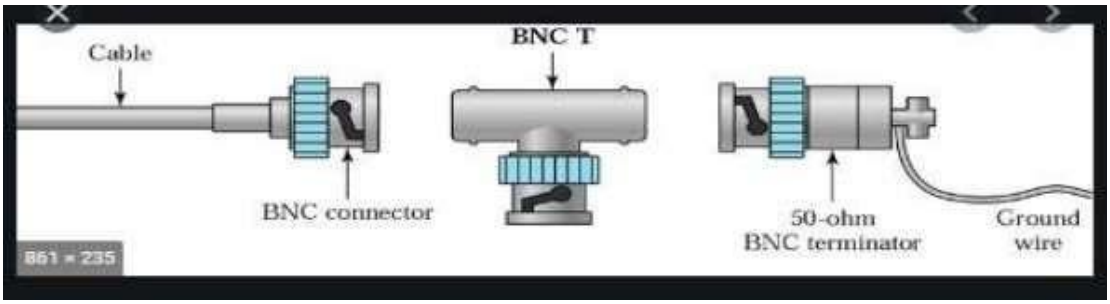
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is

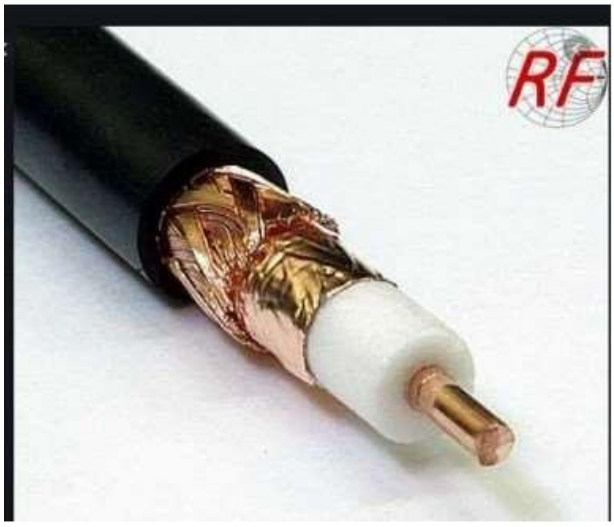


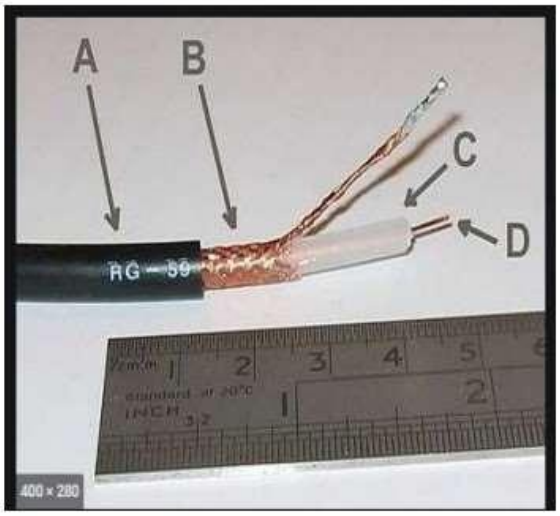
protected by a plastic cover

Coaxial Cable Connectors

- To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector.
- Three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.
- The BNC connector is used to connect the end of the cable to a device, such as a TV set.
- The BNC T connector is used in Ethernet network to branch out to a connection to a computer or other device.
- The BNC terminator is used at the end of the cable to prevent the reflection of the signal.







APPLICATION

- Coaxial cable was widely used in analog telephone networks
- Cable TV networks also use coaxial cables.
- In the traditional cable TV network, the entire network used coaxialcable
- Common application of coaxial cable is in traditional Ethernet LANseg. 10base5

ADVANTAGES OF COAXIAL CABLE

- Transmission speed is high.
- Bandwidth is high.
- Its shielding is better than twisted pair cable.

DISADVANTAGES OF COAXIAL CABLE

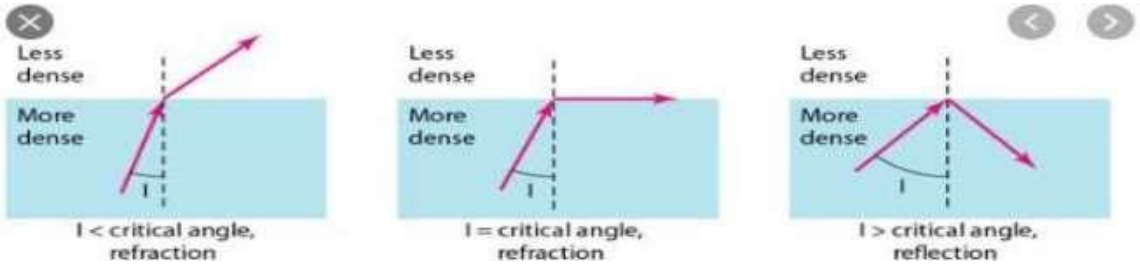
- Expensive than twisted pair.
- The signal weakens rapidly and requires the frequent use ofrepeaters.

FIBER-OPTIC CABLE(GUIDED MEDIA)

- A fiber-optic cable is made of glass or plastic and transmits signalsin the form of light.
- A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications.
- Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.
- Fiber optic cables carry communication signals using pulses of light generated by small lasers.
- To know about fiber optics we will first study the property of light

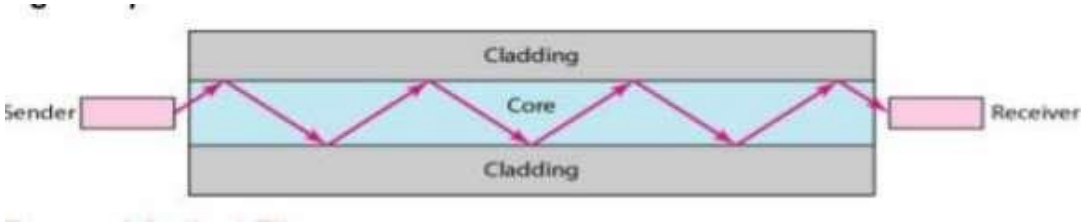
SOME PROPERTIES.

- Light travels in a straight line as long as it is moving through a singleuniform substance
- If a ray of light traveling through one substance suddenly enters another (less or more dense) substance, its speed changes abruptly,causing the ray to change direction.



- if the angle of incidence is less than the critical angle then we say that there is refraction.
- When the angle of incidence becomes greater than the critical angle, a new phenomenon occurs called reflection.
- If the angle of incidence is equal to the critical angle, the light bends along the interface
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding insteadof being refracted into it.

See Figure



• Information is encoded onto a beam of light as a series of on-off flashes that represent 1 and 0 bits.

PROPAGATION MODES

• Current technology supports 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

• Current technology supports two modes for propagating light along optical channels, each requiring fiber with different physical characteristics: **Multimode and Single Mode.**

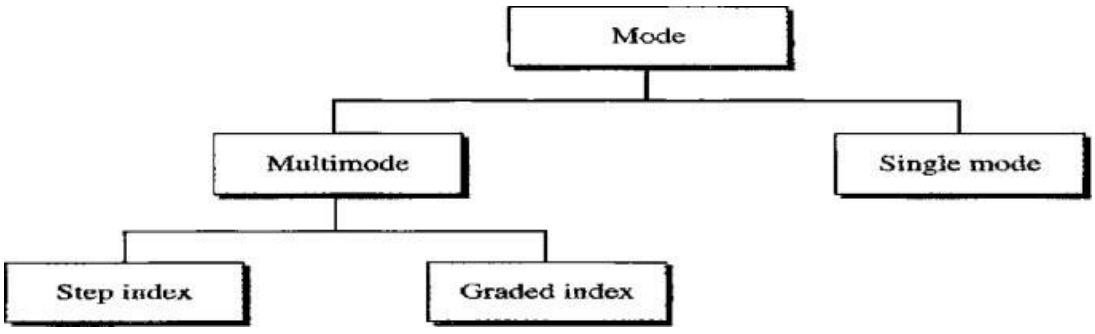
• Single mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

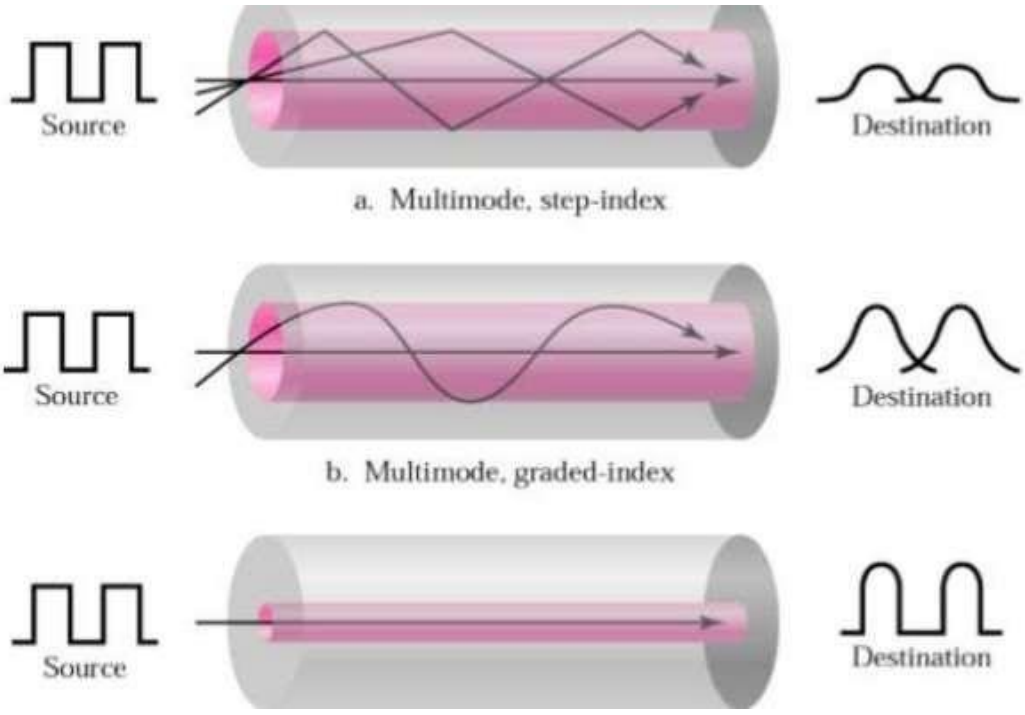
• Multimode: In this case multiple beams from a light source move through the core in different paths.

MULTIMODE, IN TURN, CAN BE IMPLEMENTED IN TWO FORMS: STEP-INDEX ORGRADED INDEX

• **In multimode step-index fiber**, the density of the core remains constant from the center 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 cladding. At the interface there is an abrupt change to a lower density that alters the angle of the beam's motion.

• **In a multimode graded-index fiber** the density is highest at the center of the core and decreases gradually to its lowest at the edge.





TYPES OF OPTICAL FIBER

There are two basic types of fiber: multimode fiber and single-mode fiber.

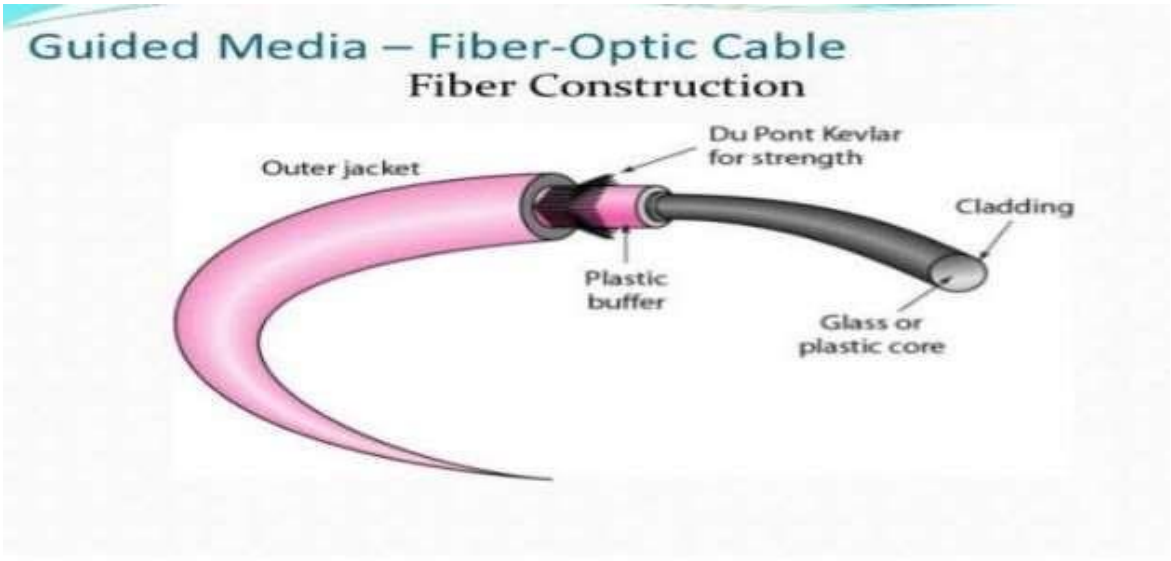
a) Multimode fiber is best designed for short transmission distances, and is suited for use in LAN systems and video surveillance.

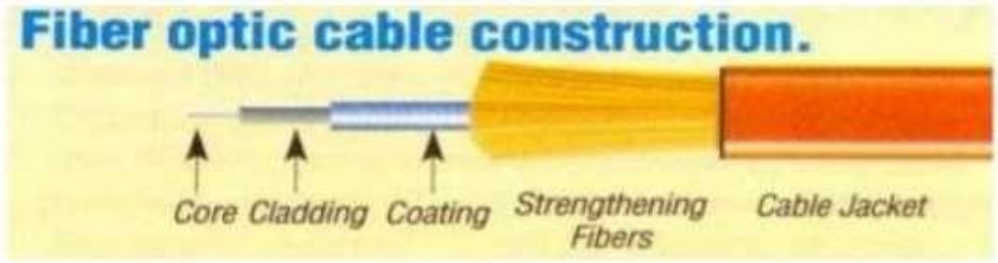
b) Single-mode fiber is best designed for longer transmission distances, making it suitable for long-distance telephony and multichannel television broadcast systems.

CABLE COMPOSITION

Figure shows the composition of a typical fiber-optic cable.

- The outer jacket is made of either PVC or Teflon.
- Inside the jacket are Kevlar strands to strengthen the cable.(Kevlar is a strong material used in the fabrication of bulletproof vests).
- Below the Kevlar is another plastic coating to cushion the fiber.



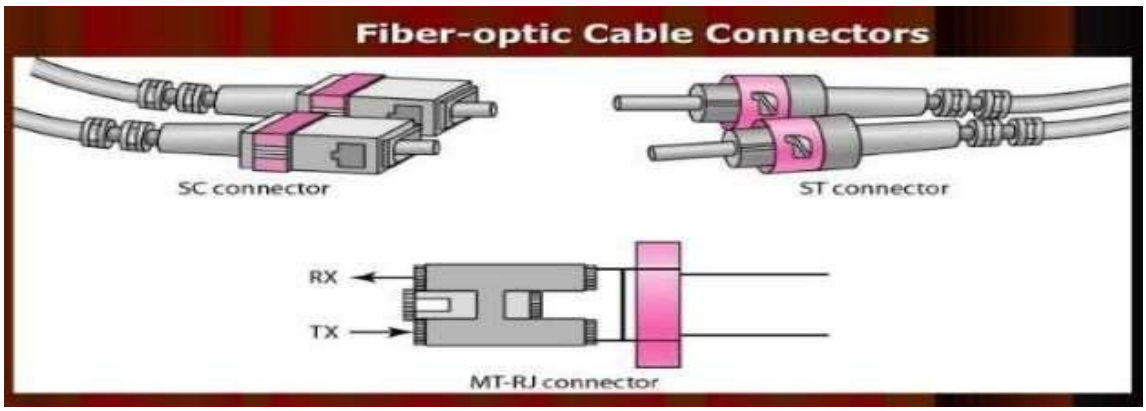


• The fiber is at the center of the cable, and it consists of cladding and core.

FIBER-OPTIC CABLE CONNECTORS

There are three types of connectors for fiber-optic cables

- The subscriber channel (SC) connector is used for cable TV.The straight-tip (ST) connector is used for connecting cable tonetworking devices.
- MT-RJ is a connector that is the same size as RJ45.



ADVANTAGES AND DISADVANTAGES OF OPTICAL FIBERADVANTAGES

1. Higher bandwidth:

   Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

2. Less signal attenuation:
   Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
3. Immunity to electromagnetic interference:
   Electromagnetic noise cannot affect fiber- optic cables.
4. Resistance to corrosive materials:
   Glass is more resistant to corrosive materials than copper.
5. Light weight:
   Fiber-optic cables are much lighter than copper cables.
6. Greater immunity to tapping:
   Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

DISADVANTAGES

There are some disadvantages in the use of optical fiber.

1. Installation and maintenance:

   Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

2. Unidirectional light propagation:
   Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. Cost:

   The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

UNIT:3 MOBILE AD HOC NETWORK

3.2 Concepts of OSI layers

THE OSI REFERENCE MODEL:

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has seven layers.

The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

- Open Systems Interconnection (OSI).
  - Developed by the International Organization for Standardization (ISO).
  - Model for understanding and developing computer-to-computer communication architecture that is flexible, robust and interoperable.
  - It is not a protocol.
  - Developed in the 1980s.
  - Divides network architecture into seven layers.
  - Each layer performs a subset of the required communication functions
  - Each layer relies on the next lower layer to perform more primitivefunctions
  - Each layer provides services to the next higher layer
  - Changes in one layer should not require changes in other layers

The 7 layers of osi model are

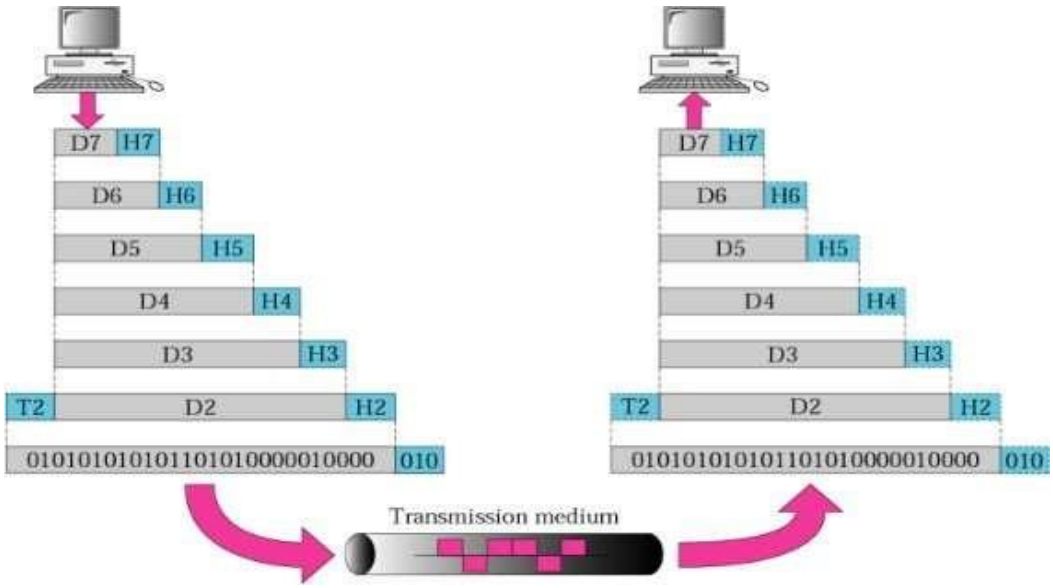
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Datalink
1 Physical

USER SUPPORT LAYERS

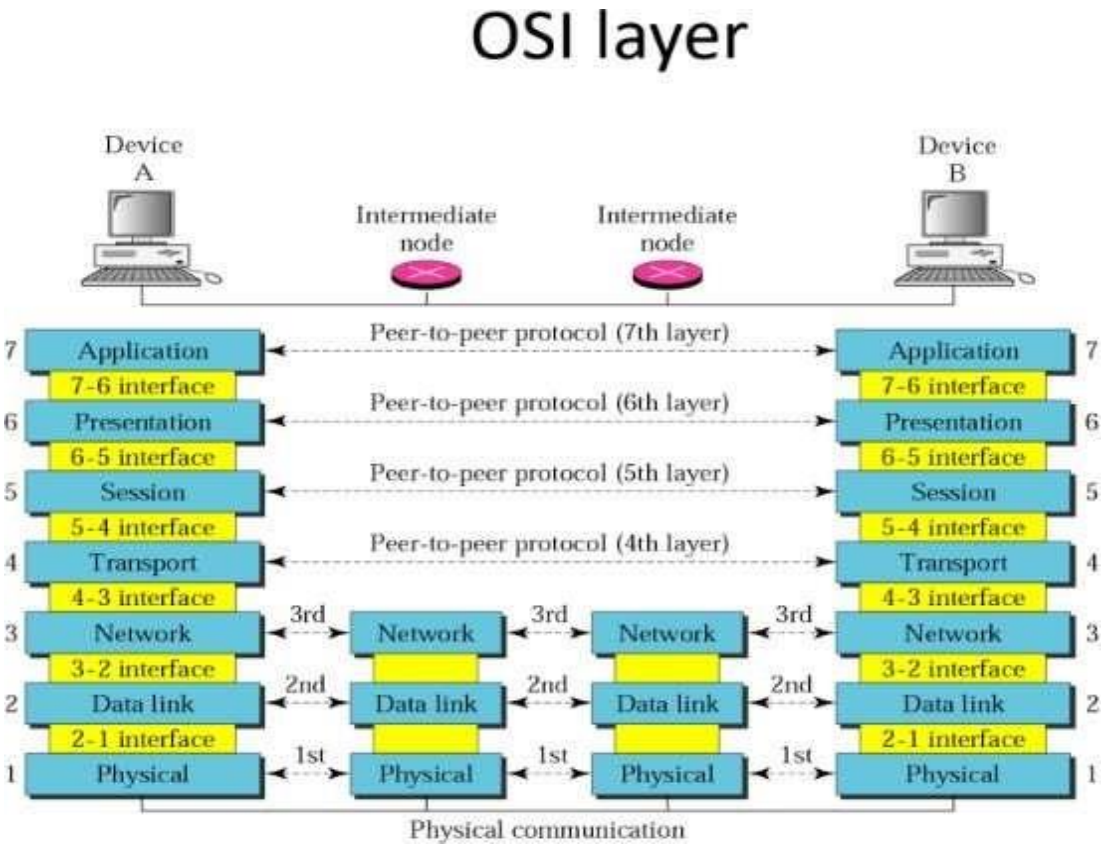
NETWORK SUPPORT LAYERS

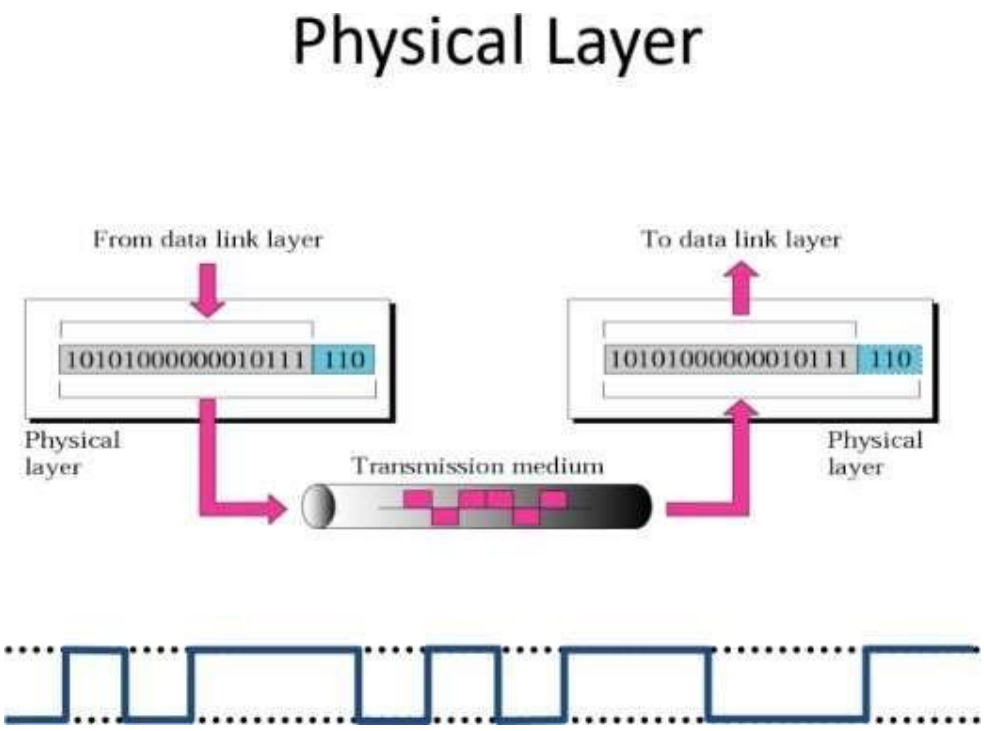
- Layers I, 2, and 3-physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability amongunrelated software systems.
- Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upperlayers can use.

An exchange using the OSI modelENCAPSULATION



- Sender side encapsulation:
  - Figure, which gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, andso on.
  - The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a header, or possibly a trailer, can be added to the data unit.
  - Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported alonga physical link.
- Receiver side decapsulation:
  - Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
  - By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

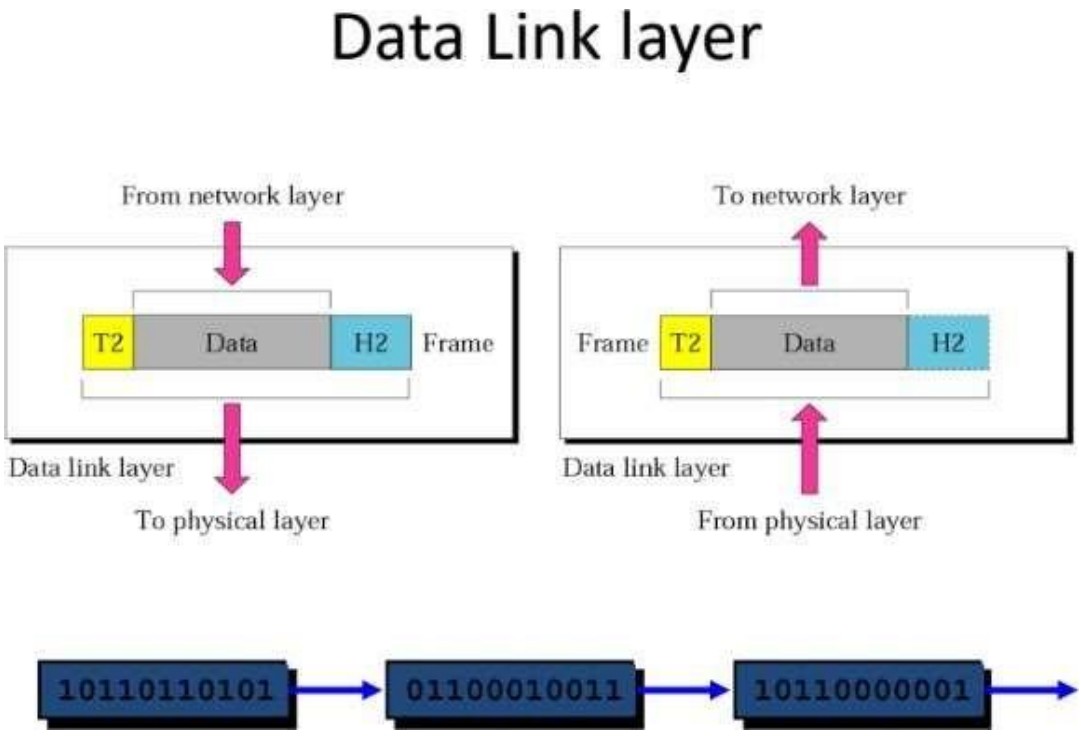




Layer 1: Physical Layer

Responsibility:

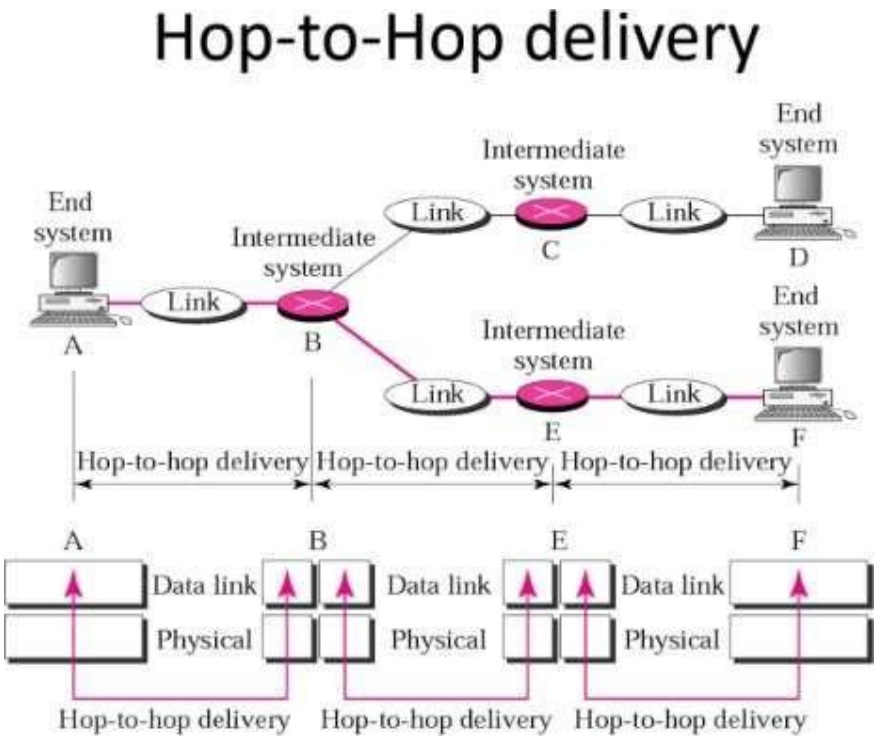
1. Physical characteristics of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
2. Representation of bits: The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. The physical layer defines the type of encoding (how Os and Is are changed to signals).
3. Data rate:The transmission rate-the number of bits sent each second-is also defined by the physical layer
4. Synchronization of bits :, the sender and the receiver clocks must be synchronized.
5. Line configuration: concerned with the connection of devices to the media whether it is a point-to-point configuration or multipointconfiguration
6. Physical topology: whether the topology used is star,bus,mesh ,ring or hybrid topology
7. Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex



LAYER 2: DATA LINK LAYER

Responsibility:

1. Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
2. Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
3. Flow control:If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism.
4. Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. . Error control is normally achieved through a trailer added to the end of the frame.
5. Access control:When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

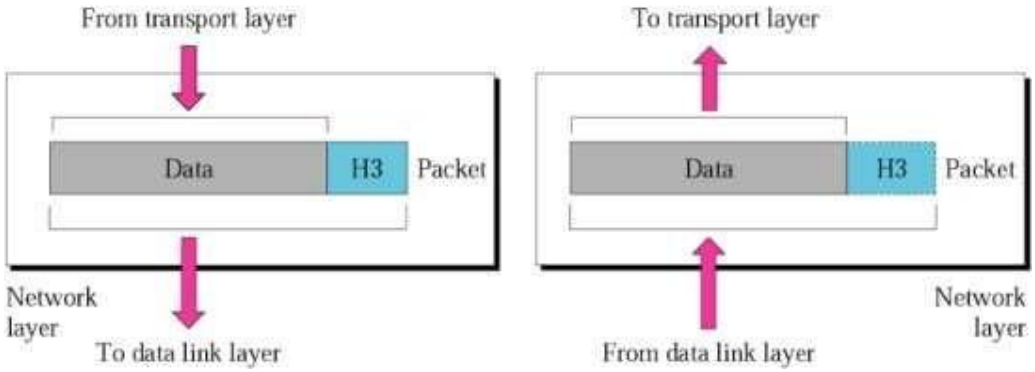


HOP TO HOP DELIVERY

As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made.

- First, the data link layer at A sends a frame to the data link layer at B (arouter).
- Second, the datalink layer at B sends a new frame to the data link layerat E.
- Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers.
- The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of theframe.

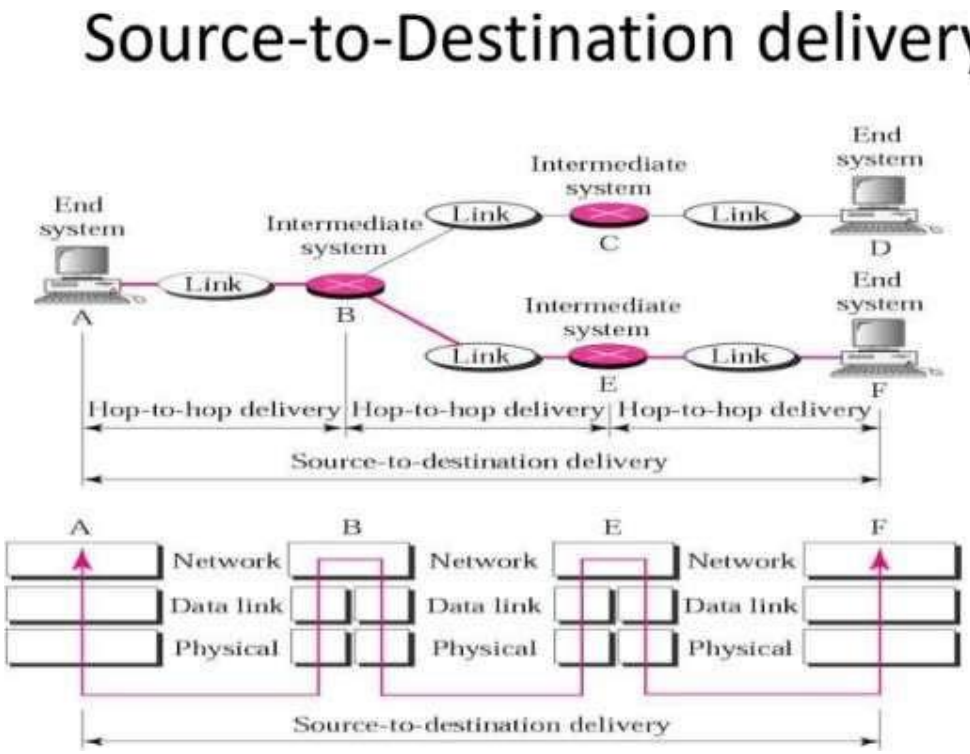
Network Layer



LAYER 3: NETWORK LAYER

RESPONSIBILITY

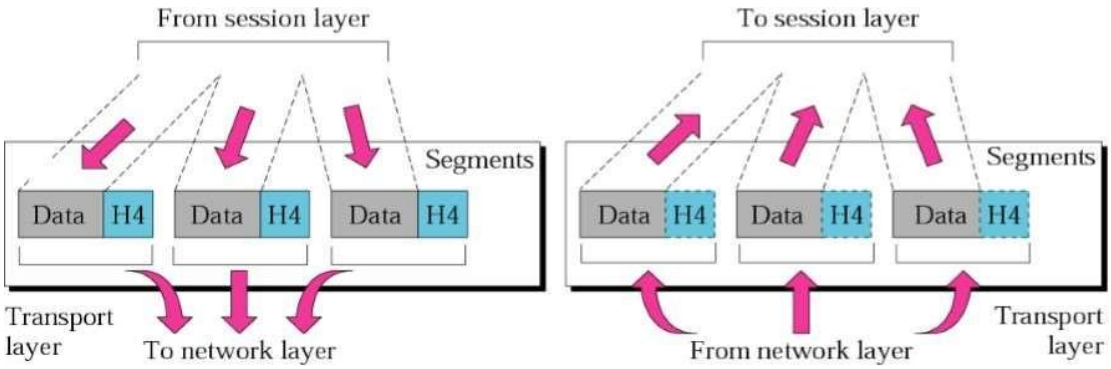
1. source-to-destination delivery of a packet : If the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery
2. Logical addressing: If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver
3. Routing : independent networks or links are connected to create internetworks(network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. This is one of the main mechanism of network layer



Hop to hop delivery in network layer

As the figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B,therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.

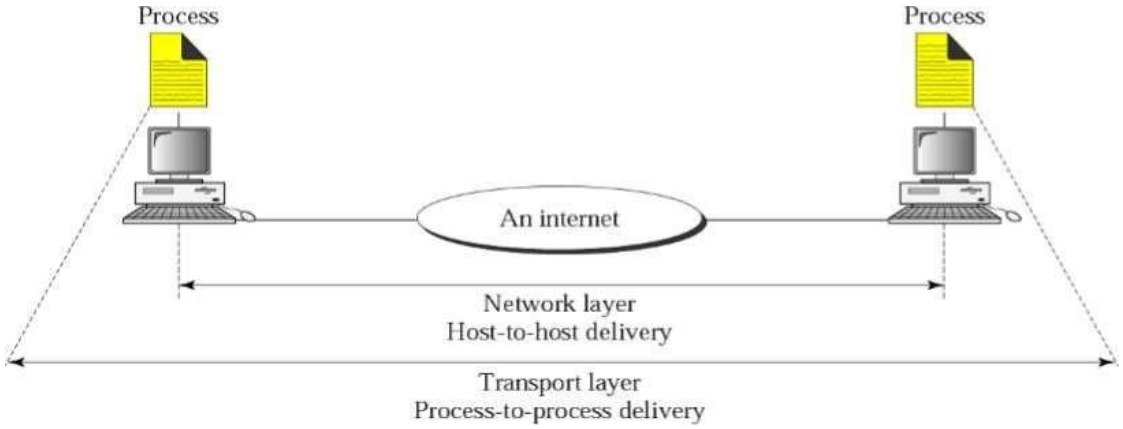
Transport Layer



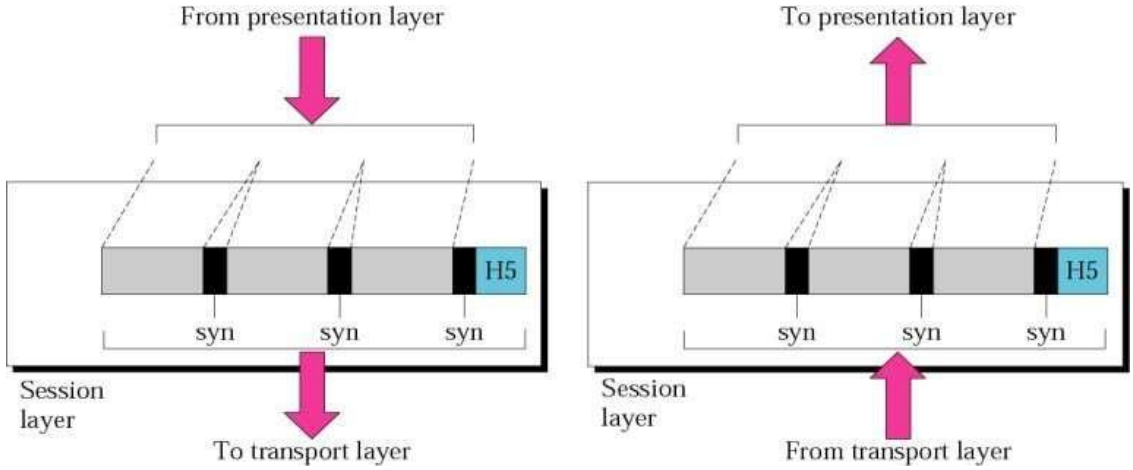
RESPONSIBILITY:

1) Process-to-Process delivery :Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other computer.Network layer ensures that the delivery is made to the correct system whereas transport layer ensures delivery made to the correct process of the correct system.
2) service-point address (or port address): To ensure that the packet reaches the correct process of the correct destination the transport layer header includes a address called as port number(16 bit).
3) Segmentation and reassembly: A message is divided into transmittable segments with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission
4) Connection control :The transport layer can be either connectionless or connection - oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
5) Flow control: Flow control at this layer is performed end to end that is process to process
6) Error control: error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Reliable process-to-process delivery of a message



Session Layer



Layer 5: Session Layer

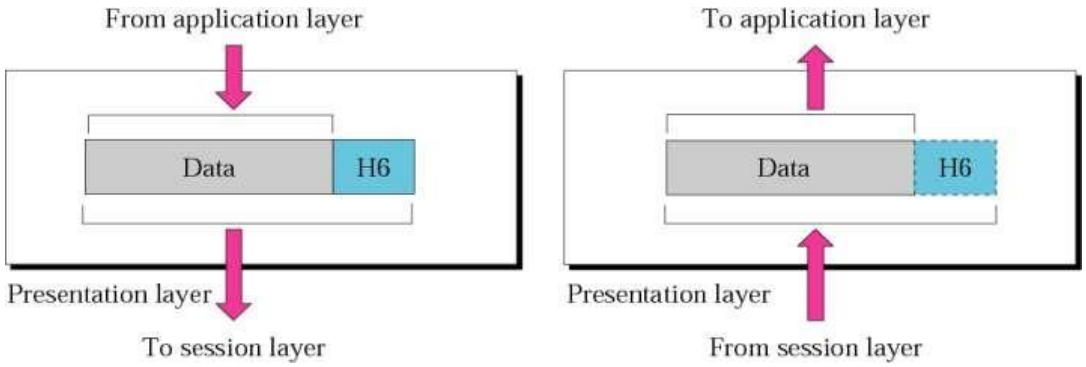
Responsibility:

1. Dialog control :The session layer allows two systems to enter into a dialog. It establishes, maintains, and synchronizes the interaction among communicating systems. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two waysat a time) mode.

2. Synchronization:The session layer allows a process to add checkpoints, or syn-Chronization points, to a stream of data.

For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need notbe resent.

Presentation Layer



LAYER 6 :PRESENTATION LAYER

Responsibility:

1. Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted.

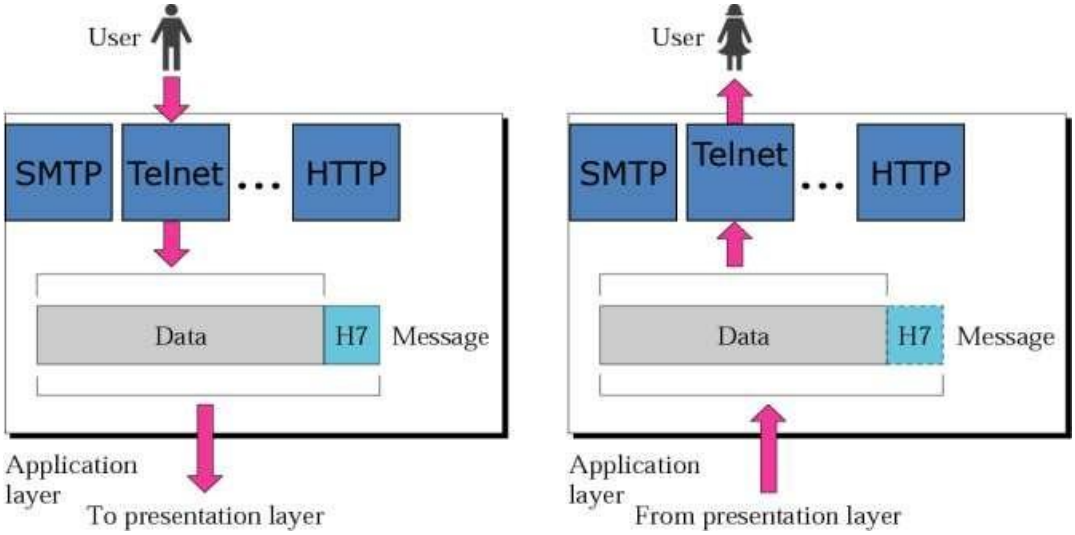
Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

2. Encryption : To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over thenetwork.

3. Decryption reverses the original process to transform the message back to its original form

4. Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video

APPLICATION LAYER



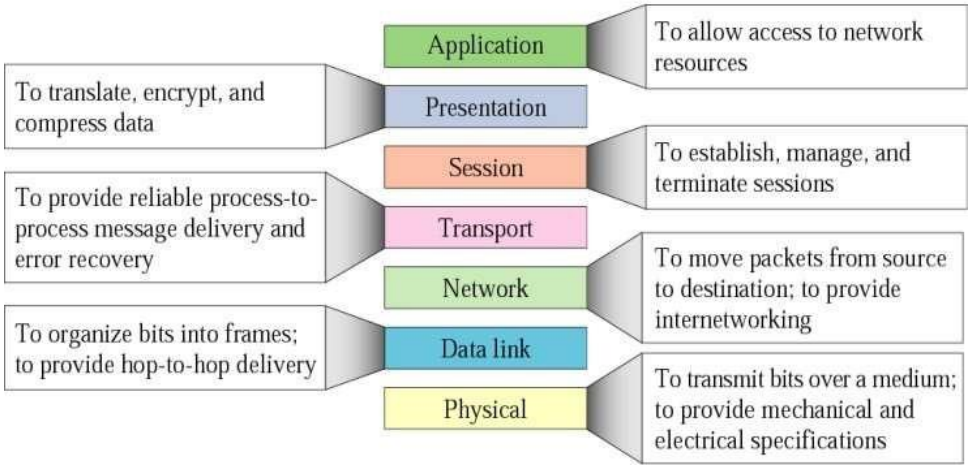
LAYER 7: APPLICATION LAYER

Responsibility:

1. Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
2. File transfer, access, and management.: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
3. Mail services. This application provides the basis for e-mail forwarding andstorage.

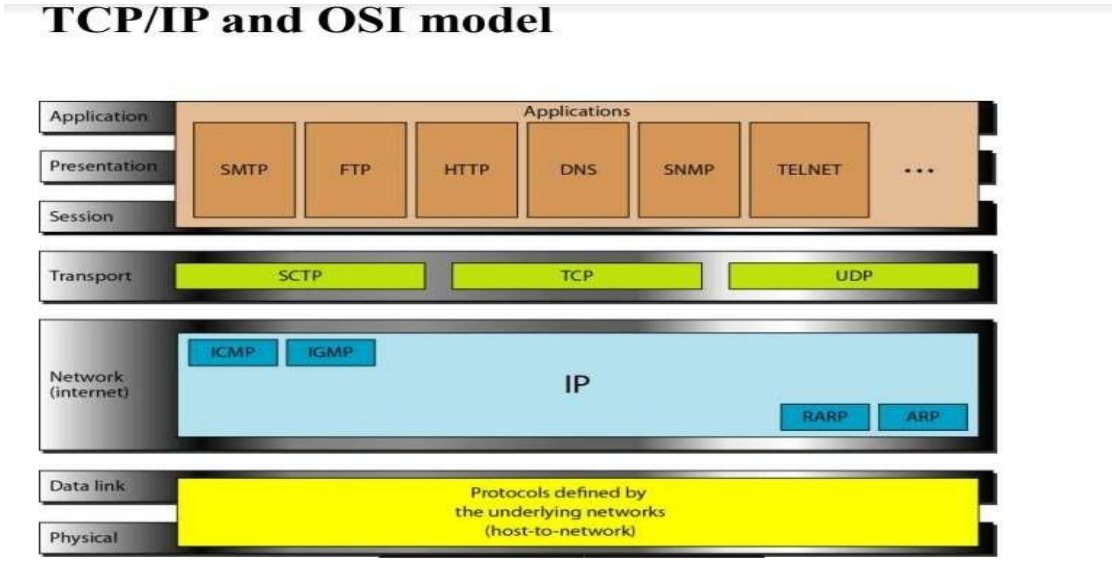
4 Directory services. This application provides distributed database sources and access for global information about various objects and services.

Summary



TCP/IP PROTOCOL SUITE

- The layers in the TCP/IP protocol suite do not exactly match those in theOSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI,we can say that the TCP/IP protocol suite is made of five layers: physical, data link,network, transport, andapplication.



PHYSICAL AND DATA LINK LAYERS

At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols

NETWORK LAYER

TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

1. **INTERNETWORKING PROTOCOL (IP):**

- It is an unreliable and connectionless protocol-a best-effort delivery service
- The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
- IP transports data in packets called datagrams
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.
- The limited functionality of IP should not be considered a weakness, however IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allowsfor maximum efficiency

2. **ADDRESS RESOLUTION PROTOCOL(ARP)**
3. **ON A TYPICAL PHYSICAL NETWORK, SUCH AS A LAN, EACH DEVICE ON A LINK IS**

identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

4. **REVERSE ADDRESS RESOLUTION PROTOCOL(RARP)**

The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted

5. **INTERNET CONTROL MESSAGE PROTOCOL(ICMP)**

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

6. **INTERNET GROUP MESSAGE PROTOCOL(IGMP)**

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients

TRANSPORT LAYER

1 User Datagram Protocol(UDP)

The User Datagram Protocol (UDP) is the simpler of the two standard TCPIIP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

2. TRANSMISSION CONTROL PROTOCOL(TCP)

• The transmission Control Protocol (TCP) provides full transport-layer services to applications. • TCP is a reliable transport protocol. • The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. • At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. • Each segment includes a sequence number for reordering and also includes an acknowledgment number for the segments received. •Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers

STREAM CONTROL TRANSMISSION PROTOCOL(SCTP)

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet

APPLICATION LAYER

The application layer in TCPI/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer few are shown in the figure.

UNIT-4 IMPORTANT PROTOCOLS OF NETWORK LAYERS

4.1 CONCEPTS OF DATA PACKETS AND DATAGRAM

Data packet

A data packet is a unit of data made into a single package that travels along a given network path. Data packets are used in Internet Protocol (IP) transmissions for data that navigates the Web, and in other kinds of networks.

A packet is a basic unit of communication over a digital network.

A packet is also called a datagram, a segment, a block, a cell or a frame, depending on the protocol used for the transmission of data. When data has to be transmitted, it is broken down into similar structures of data before transmission, called packets, which are reassembled to the original data chunk once they reach their destination.

DATAGRAM

There are two types of network transmission techniques, circuit switched network and packet switched network.

Circuit Switch vs Packet Switch

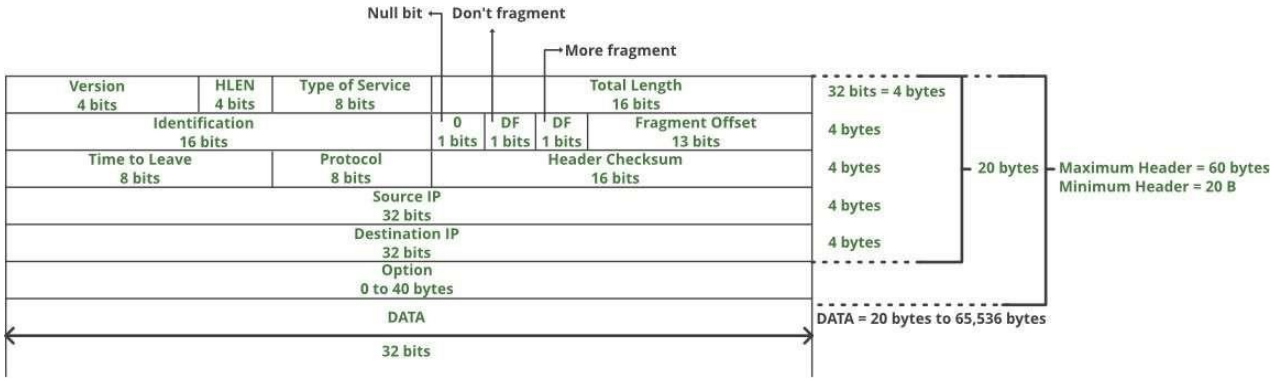
In circuit switched network, a single path is designated for transmission of all the data packets. Whereas in case of a packet-switched network, each packet may be sent through a different path to reach the destination.

In a circuit switched network, the data packets are received in order whereas in a packet switched network, the data packets may be received out of order.

The packet switching is further subdivided into Virtual circuits and Datagram.

IPV4 DATAGRAM :

Packets in the IPv4 layer are called datagrams.



A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4

HLEN: IP header length (4 bits), defines the total length of the datagram header.The minimum value for this field is 5 and the maximum is 15.

Type of service: This field, previously called service type, is now called differentiated services. Low Delay, High Throughput, Reliability (8 bits). the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.

Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.

Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits). If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order).As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. When fragmentation of a message occurs, this field specifies the offset, or position, in the overall message where the data in this fragment goes. It is specified in units of 8 bytes (64 bits). The first fragment has an offset of 0

Time to live: It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.Specifies how long the datagram is allowed to "live" on the network, in terms of router hops. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

Protocol: An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered.

Header Checksum: 16 bits header checksum for checking errors in the datagram header

Source IP address: 32 bits IP address of the sender

Destination IP address: 32 bits IP address of the receiver

Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

Data: The data to be transmitted in the datagram, either an entire higher-layer message or a fragment of one.

CONCEPTS AND PURPOSE OF VARIOUS PROTOCOLS:

Purpose of Presentation layer

Function of presentation layer explained in OSI MODEL

PRESENTATION LAYER PROTOCOLS AND THEIR PURPOSE:

SSL, HTTP, FTP, Telnet

SSL: SECURE SOCKETS LAYER

SSL stands for Secure Sockets Layer. It is the standard security technology (a protocol) that offers secure communication between web servers and browsers (web clients) over an insecure network, such as the internet. It maintains the privacy and integrity of the data exchanged between a web server and browsers.

The web server is required to have an SSL certificate to establish a secure SSL connection. SSL encrypts network connection segments which are above the transport layer, which is a component of network connection above the program layer.

SSL works through an asymmetric cryptographic mechanism, in which the web browser creates a public key and a private key. The public key, which is called certificate signalling request (CSR), is placed in a data file. The private key is generated for the recipient only.

It makes the data, which is shared between users and sites, impossible to read. It uses encryption algorithms to scramble data in transit, to prevent hackers from reading it. This data may be your bank login id and password, credit card details, social media login details, and other financial information, etc. For example, when you shop online, the details you share with the websites remain safe.

SSL is the predecessor of Transport Layer Security (TLS), a protocol for the secure transmission of internet data. TLS (Transport Layer Security) is an updated and more secure version of SSL. You can see the HTTPS (Hypertext Transfer Protocol Secure) in the URL of a website, which is secured by an SSL certificate. To see the details of the certificate, you can click on the lock symbol on the browser bar to the left of the URL.

Internet Engineering Task Force has discontinued both SSL 2.o and 3.0 in 2011 and 2015 respectively and replaced them by the Transport Layer Security (TLS) protocol.

Benefits of SSL:

- Data integrity: The data can't be tempered as it is not sent as a plain text, so even if it is intercepted, it could not be decoded.
- Data privacy: The privacy of data is maintained using a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol, and SSL Alert Protocol. So, confidential information, such as social security number, credit card number, login details, can betransmitted securely.
- Client-server authentication: It uses the standard cryptographic technique to authenticate the client and server.

HTTP

- HTTP stands for HyperText Transfer Protocol.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use it in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

FEATURES OF HTTP:

- Connectionless protocol: HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.

- Media independent: HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- Stateless: HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

FTP (FILE TRANSFER PROTOCOL) :

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

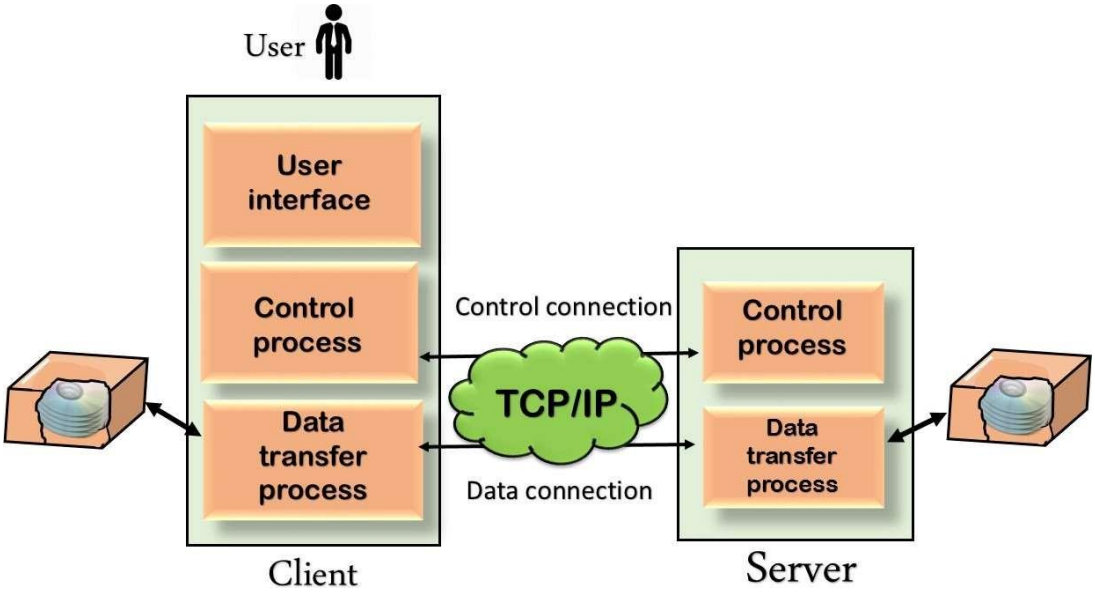
OBJECTIVES OF FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

WHY FTP?

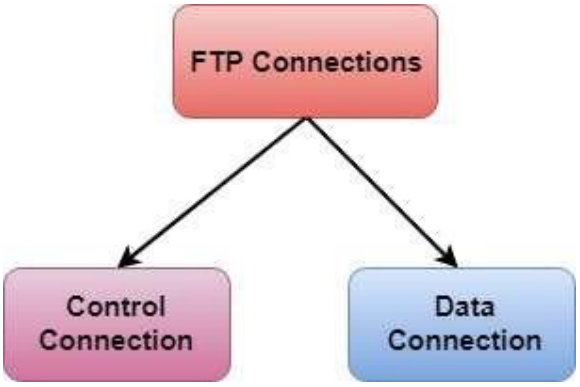
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



- Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.

- Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

ADVANTAGES OF FTP:

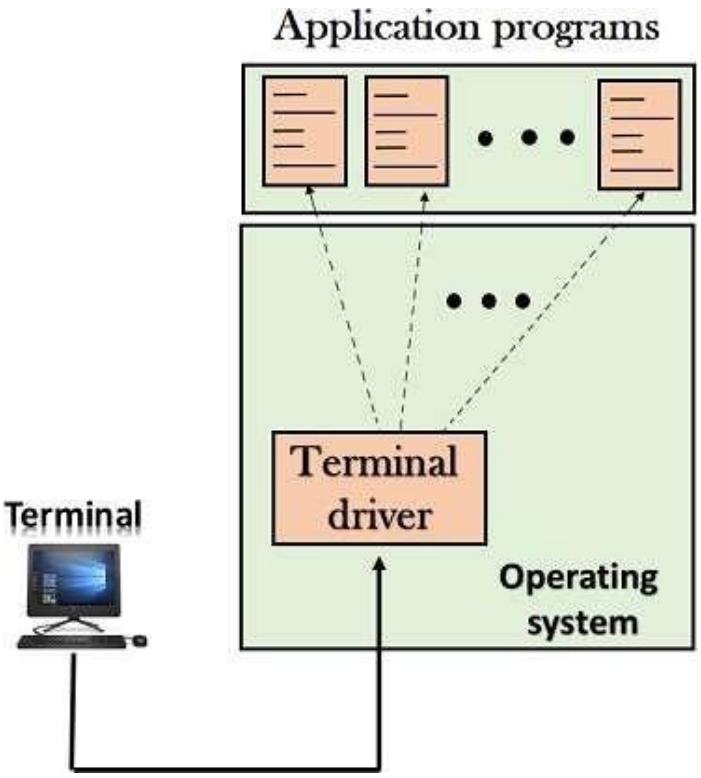
- Speed: One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- Efficient: It is more efficient as we do not need to complete all the operations to get the entire file.
- Security: To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- Back & forth movement: FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

DISADVANTAGES OF FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

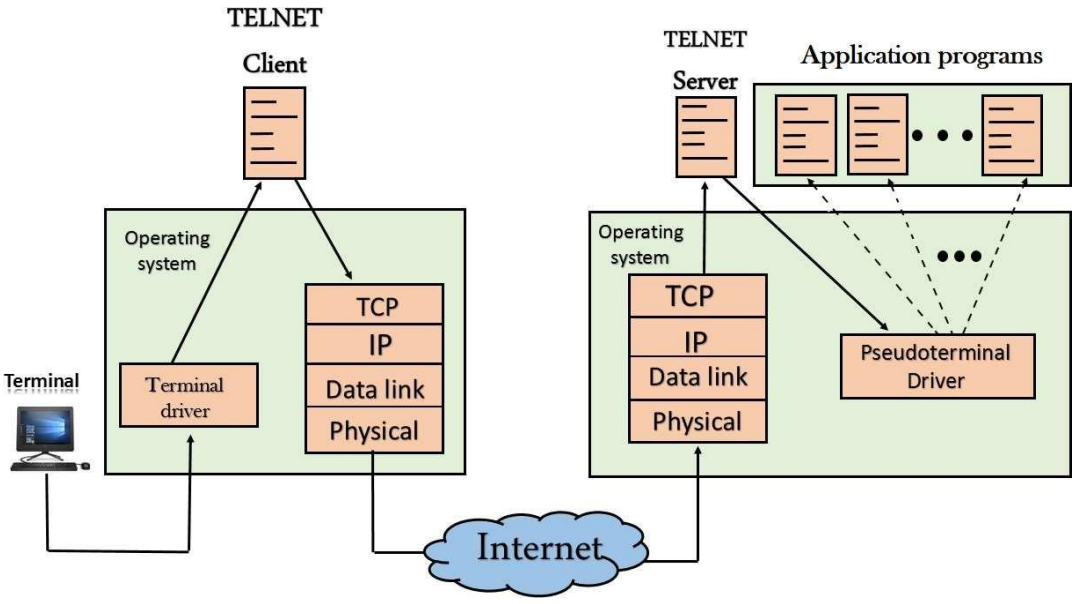
TELNET

- a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**.
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side.
- There are two types of login:Local Login



- When a user logs into a local computer, then it is known as local login.

Remote login



- When the user wants to access an application program on a remote computer, then the user must perform remote login.

HOW REMOTE LOGIN OCCURSAT THE LOCAL SITE

The user sends the keystrokes to the terminal driver, the characters are then sent to the TELNET client. The TELNET client which in turn, transforms the characters to a universal character set known as network virtual terminal characters and delivers them to the local TCP/IP stack

AT THE REMOTE SITE

The commands in NVT forms are transmitted to the TCP/IP at the remote machine. Here, the characters are delivered to the operating system and then pass to the TELNET server. The TELNET server transforms the characters which can be understandable by a remote computer. However, the characters cannot be directly passed to the operating system as a remote operating system does not receive the characters from the TELNET server. Therefore it requires some piece of software that can accept the characters from the TELNET server. The operating system then passes these characters to the appropriate application program.

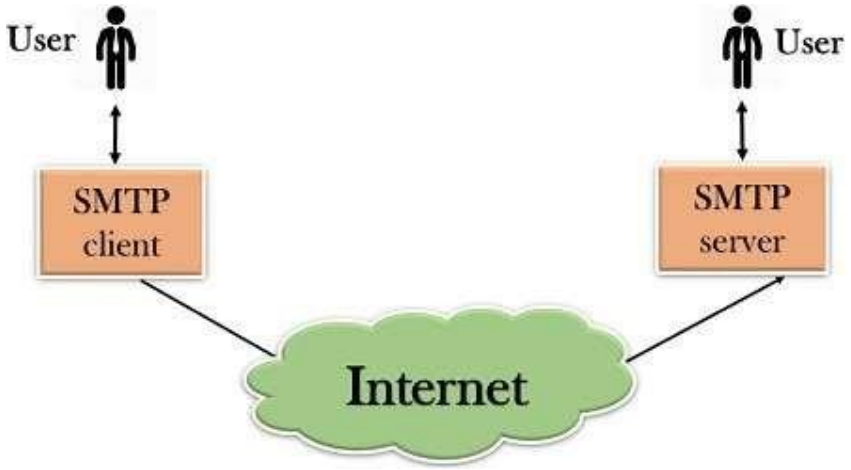
CONCEPTS OF APPLICATION LAYER PROTOCOLS AND TERMINOLOGIES: 4.2.3.1 SMTP, DNS (DOMAIN NAME SERVER), POP (POST OFFICE PROTOCOL)

SMTP

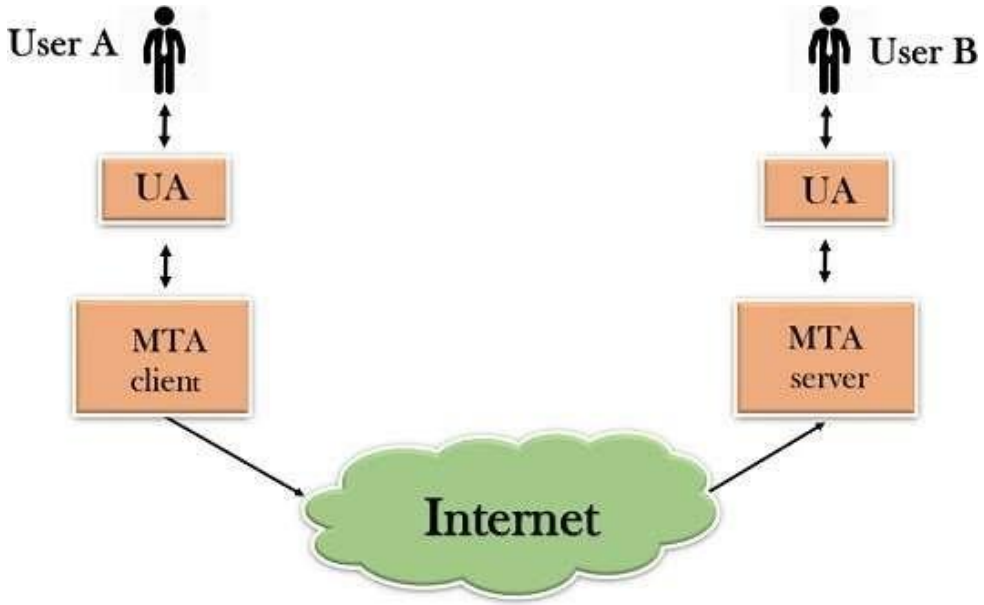
- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.

- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

Components of SMTP



- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



Working of SMTP

1. Composition of Mail: A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. Submission of Mail: After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. Delivery of Mail: E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name.

   If the domain name of the recipient's email address is different from the sender's domain name, the MTA will find the target domain.Once the record is located in Domain name System, MTA connects to the exchange server to relay the message.

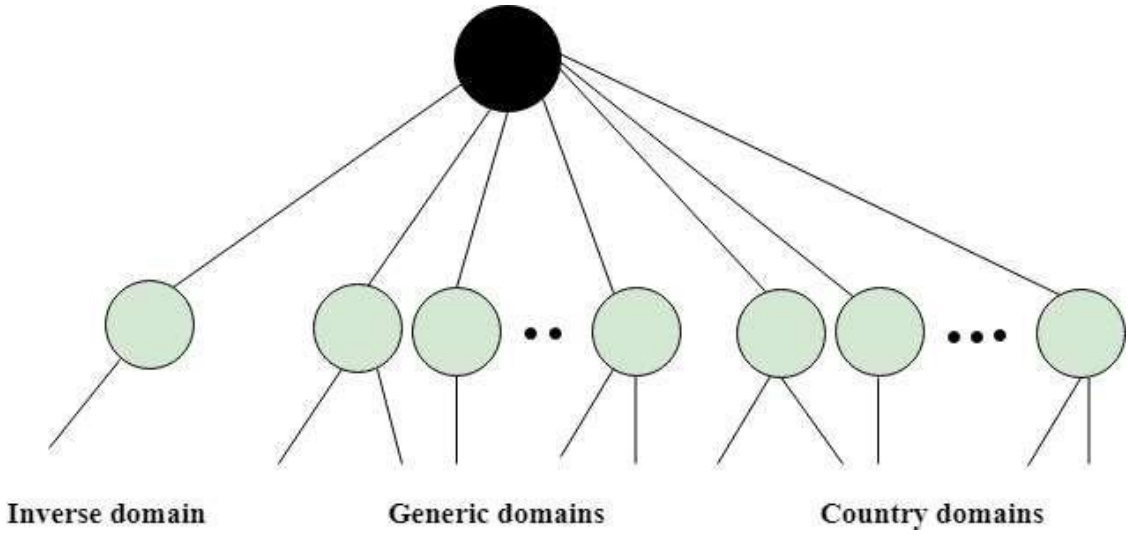
4. Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.

- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com.
- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

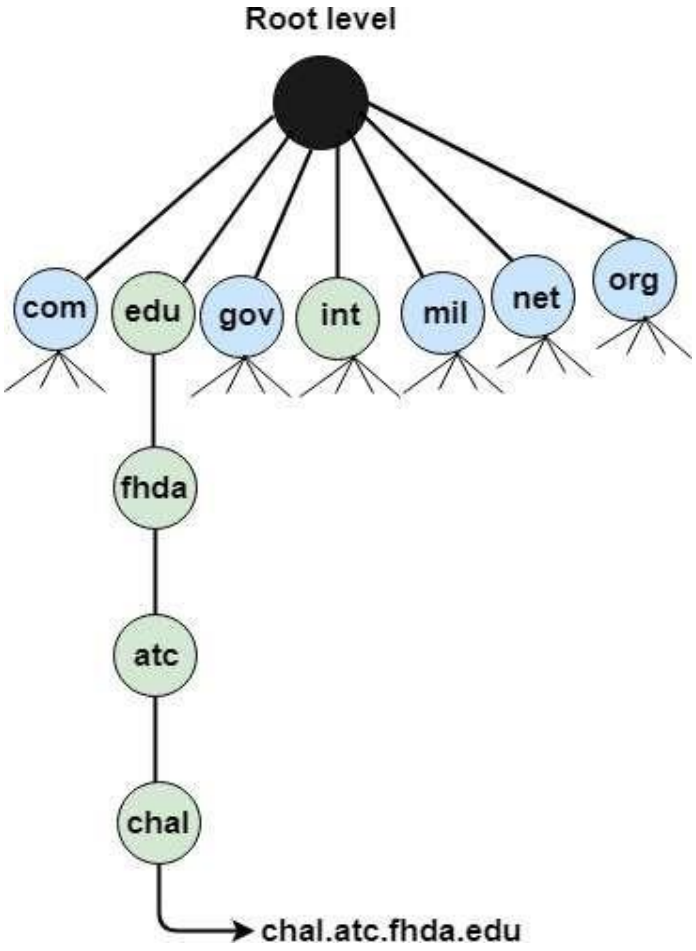


Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNSdatabase.
- It uses three-character labels, and these labels describe the organizationtype.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions

info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofitorganizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

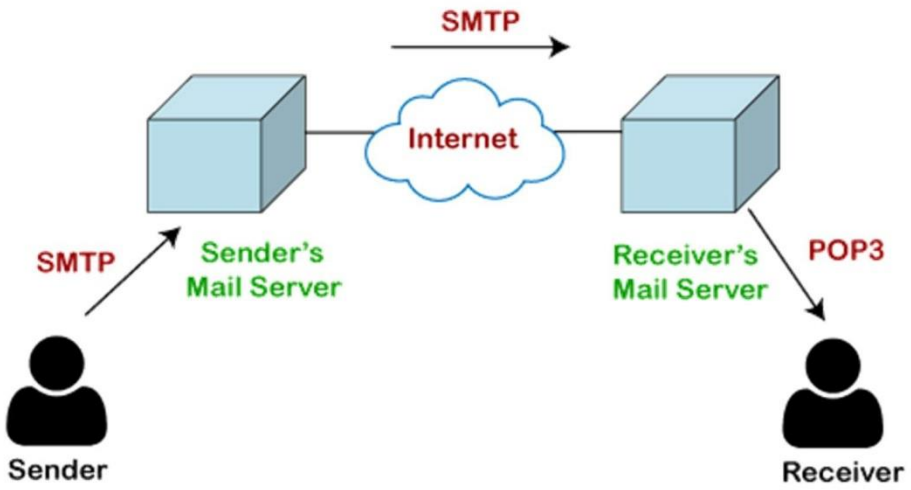
Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMTP is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

How is mail transmitted?



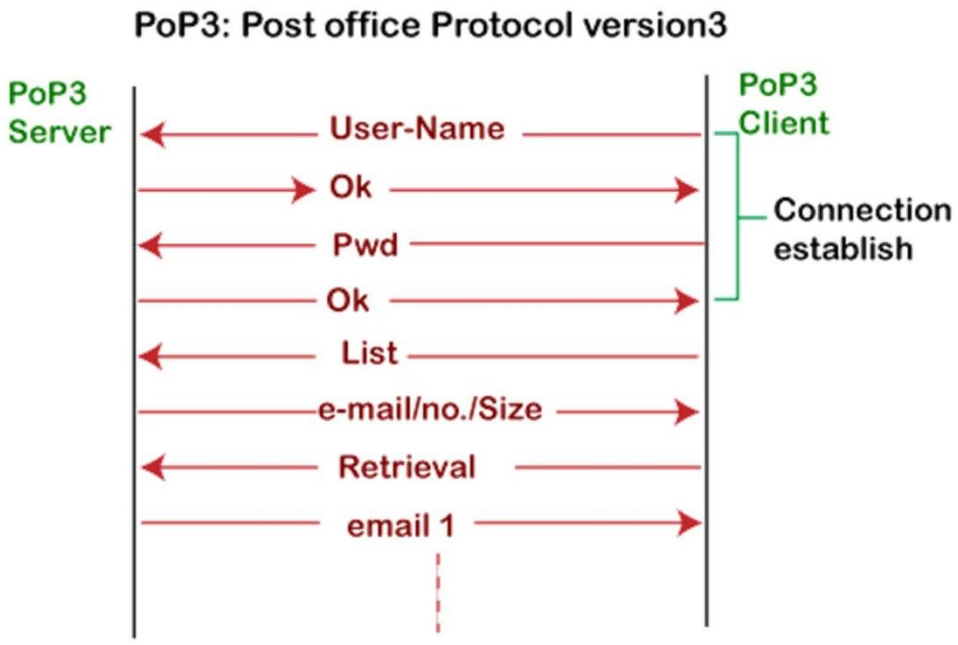
Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.

Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

What is POP3?

The POP3 is a simple protocol and having very limited functionalities. In the case of the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.

Let's understand the working of the POP3 protocol.



To establish the connection between the POP3 server and the POP3 client, the POP3 server asks for the user name to the POP3 client. If the username is found in the POP3 server, then it sends the ok message. It then asks for the password from the POP3 client; then the POP3 client sends the password to the POP3 server. If the password is matched, then the POP3 server sends the OK message, and the connection gets established. After the establishment of a connection, the client can see the list of mails on the POP3 mail server. In the list of mails, the user will get the email numbers and sizes from the server. Out of this list, the user can start theretrieval of mail.

Advantages of POP3 protocol

The following are the advantages of a POP3 protocol:

- It allows the users to read the email offline. It requires an internet connection only at the time of downloading emails from the server. Once the mails are downloaded from the server, then all the downloaded mails reside on our PC or hard disk of our computer, which can be accessed without the internet. Therefore, we can say that the POP3 protocol does not require permanent internet connectivity.
- There is no limit on the size of the email which we receive or send.
- It is a simple protocol so it is one of the most popular protocols used today.
- It is easy to configure and use.

Disadvantages of POP3 protocol

The following are the advantages of a POP3 protocol:

- If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
- Transferring the mail folder from the local machine to another machine can be difficult.
- Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.
- The email folder which is downloaded from the mail server can also become corrupted.

Internet Protocol IPv4)

Internet Protocol hierarchies contain several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IPaddresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotteddecimal notation of IP Address:

The number of networks and the number of hosts per class can be derived by this formula:

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved forBroadcast IP.

CLASS A ADDRESS

The first bit of the first octet is always set to 0 *zero*. Thus the first octet ranges from 1 – 127, i.e.

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x isreserved for loopback IP addresses.
The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).
Class A IP address format is thus:
0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

CLASS B ADDRESS

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.
Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is
255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses. Class B IP address format is:
10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH**Class C Address**

The first octet of Class C IP address has its first 3 bits set to 110, that is:

11000000 – 11011111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses. Class C IP address format is:
110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH**Class D Address**

11100000 – 11101111
224 – 239

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

CLASS E ADDRESS

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Difference between http and https

S.No.	HTTP	HTTPS
1.	HTTP stands for HyperText Transfer Protocol.	HTTPS for HyperText TransferProtocol Secure.
2.	In HTTP, URL begins with "http://".	In HTTPs, URL starts with "https://".
3.	HTTP uses port number 80 for communication.	HTTPsuses 443 port number for communication.
4.	HTTPis considered to be unsecure.	HTTPs is considered as secure.
6.	In HTTP, Encryption is absent.	Encryption is present in HTTPS.
7.	HTTP does not require any certificates.	HTTPS needs SSL Certificates.
8.	HTTP does not improve search ranking	HTTPS helps to improve search ranking
9.	HTTP faster than HTTPS	HTTPS slower than HTTP
10.	HTTPdoes not use data hashtags to secure data.	HTTPS will have the data before sending it and return it to its original state on the receiver side.

UNIT-5 MAIL SERVICES

Application Layer services:

Services of Application Layers

- **Network Virtual terminal:** An application layer allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which in turn, talks to the host. The remote host thinks that it is communicating with one of its own terminals, so it allowsthe user to log on.
- File Transfer, Access, and Management (FTAM): An application allows a user to access files in a remote computer, to retrieve files from a computer and to manage files in a remote computer. FTAM defines a hierarchical virtual file in terms of file structure, file attributes and the kind of operations performed on the files and their attributes.
- **Addressing:** To obtain communication between client and server, there is a need for addressing. When a client made a request to the server, the request contains the server address and its own address. The server response to the client request, the request contains the destination address, i.e., client address. To achieve this kind of addressing, DNS is used.
- **Mail Services:** An application layer provides Email forwarding andstorage.
- **Directory Services:** An application contains a distributed database that provides access for global information about various objects and services.

CONCEPTS OF EMAIL

What is E-mail?

E-mail is defined as the transmission of messages on the Internet. It is one of the most commonly used features over communications networks that may contain text, files, images, or other attachments. Generally, it is information that is stored on a computer sent through a network to a specified individual orgroup of individuals.
Email messages are conveyed through email servers; it uses multiple protocols within the TCP/IP suite. For example, SMTP is a protocol, stands for simple mail transfer protocol and used to send messages whereas other protocols IMAP or POP are used to retrieve messages from a mail server. If you want to login to your mail account, you just need to enter a valid email address, password, and the mail servers used to send and receive messages.

WORKING OF EMAIL ACCOUNT AND SERVICES

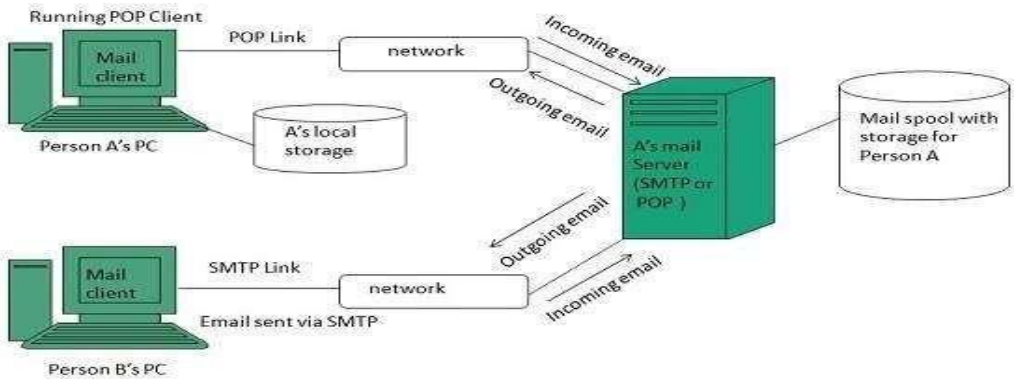
When an individual writes a message, it's usually done in an email client like Outlook in a web-based service like Gmail.

In both cases, whether the message is created by an email client or by an automated system, it is specially formatted to be transmitted over the Internet using a standard called "Simple Mail Transfer Protocol" (SMTP).

The sender's mail server (technically called a "Mail Transfer Agent," or MTA) looks up the "@domain.com" portion of the recipient's email address in a Domain Name System (DNS) server to determine which destination mail server (referred to as a "Mail Exchanger," or MX) it should contact to deliver the message.

The sending and receiving servers communicate using the SMTP protocol. The receiving server accepts the message so that it can be delivered to the recipient.

The recipient's email client retrieves the message using standards like the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) to download the message so it can be read.



URL AND URL TYPES (ABSOLUTE, RELATIVE)

URL stands for Uniform Resource Locator. Any internet location available on server is called a web URL, web address or website. Each website or webpage has a unique address called URL. e.g., the website of **geeksforgeeks** website has an address or URL called https://www.geeksforgeeks.org/

Basic Structure of URL

type: It specifies the type of the server in which the file is located. **address:** It specifies the address or location of the internet server. **path:** It specifies the location of the file on the internet server.

Types of URL: URL gives the address of files created for webpages or other documents like an image, pdf for a doc file, etc.

There are two types of URL:

- Absolute URL
- Relative URL

Absolute URL: This type of URL contains both the domain name and directory/page path. An absolute URL gives complete location information. It begins with a protocol like "http://" and continues, including every detail. An absolute URL typically comes with the following syntax.

protocol://domain/path

For web browsing, absolute URL's are types in the address bar of a web browser. For example, if it is related to our project page link of **geeksforgeeks** website, the URL should be mentioned as https://www.geeksforgeeks.org/computer-science-projects/ this gives the complete information about the file location path.

Note: The protocol may be of following types.http://, https://, ftp://, gopher://, etc.

Relative URL: This type of URL contains the path excluding the domain name.

Relative means "in relation to", and a relative URL tells a URL location on terms of the current location. Relative path is used for reference to a given link of a file that exist within the same domain.

Let us assume a web developer setting up a webpage and want to link an image called "geeksforgeeks.jpg".

<img src="geeksforgeeks.jpg">

It would internally be interpreted like the following.

<img src="./geeksforgeeks.jpg">

The dot(.) before the "/" in the *src* attribute is a "special character". It means the location should be started from the current directory to find the file location.

CASE STUDY OF EMAIL:

From sender to receiver (Mailer, Mail Server, Mailbox)

E-mail System

E-mail system comprises of the following three components:

- Mailer
- Mail Server
- Mailbox

Mailer

It is also called mail program, mail application or mail client. It allows us to manage, read and compose e-mail.

Mail Server

The function of mail server is to receive, store and deliver the email. It is must for mail servers to be Running all the time because if it crashes or is down, email can be lost.

Mailboxes

Mailbox is generally a folder that contains emails and information about them.

Working of E-mail

Email working follows the client server approach. In this client is the mailer i.e. the mail application or mail program and server is a device that manages emails.

Following example will take you through the basic steps involved in sending and receiving emails and will give you a better understanding of working of email system:

Suppose person A wants to send an email message to person B.

Person A composes the messages using a mailer program i.e. mail client and then select Send option.

The message is routed to Simple Mail Transfer Protocol to person B's mail server.

The mail server stores the email message on disk in an area designated for person B.

The disk space area on mail server is called mail spool.

Now, suppose person B is running a POP client and knows how to communicate with B's mail server.

It will periodically poll the POP server to check if any new email has arrived for B.As in this case, person B has sent an email for person B, so email is forwarded over the network to B's PC. This is message is now stored on person B's PC.
The following diagram gives pictorial representation of the steps discussed above:

FUNCTIONALITY AND USE OF PROTOCOLS AT DIFFERENT LAYERS

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server.
ALREADY DISCUSSED ONLY A SUMMARY IS PROVIDED BELOWSMTP
SMTP stands for Simple Mail Transfer Protocol. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.
Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IPnetwork.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

IMAP
IMAP stands for Internet Message Access Protocol. It was first proposed in 1986. Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

Comparison between POP and IMAP

S.N	POP	IMAP
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.
4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.

6	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e. attachment.
7	POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

CASE STUDY OF LOCATING WEBSITE:

URL AND LOCATING URL

A URL is located in the address bar or search bar at the top of the browser window. The URL is always visible in the desktop computers and laptop unless your browser is being displayed in full screen. In most of the smartphones and tablets, when you scroll down the page, the URL will disappear and only show the domain when visible. To visible the address bar, you need to scroll up the page. And, if only the domain is shown and you want to see full address, tapping on the address bar to show the full address.

STEPS AND PROTOCOLS INVOLVED IN ACCESSING URL

URL protocols include HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) for web resources, mail to for email addresses, FTP for files on a File Transfer Protocol (FTP) server, and telnet for a session to access remote computers.Concepts of search engine and purpose.

A search engine is a software program that provides information according to the user query. It finds various websites or web pages that are available on the internet and gives related results according to the search.

A search engine is an internet-based software program whose main task is to collect a large amount of data or information about what is on the internet, then categorize the data or information and then help user to find the required information from the categorized information. Google, Yahoo, Bing are the most popular Search Engines.

How do search engines work?

Search engines are generally working on three parts that are crawling, indexing, and ranking

1. Crawling: Search engines have a number of computers programs that are responsible for finding information that is publicly available on the internet. These programs scan the web and create a list of all available websites. Then they visit each website and by reading HTML code they try to understand the structure of the page, the type of the content, the meaning of the content, and when it was created or updated.

2. Indexing: Information identified by the crawler needs to be organized, Sorted, and Stored so that it can be processed later by the ranking algorithm. Search engines don't store all the information in your index, but they keep things like the Title and description of the page, The type of content, Associated keywords Number of incoming and outgoing links, and a lot of other parameters that are needed by the ranking algorithm. If your website is not in their index it will not appear for any searches this also means that if you have any pages indexed you have more chances of appearing in the search results for a related query.

3. Ranking: Ranking is the position by which your website is listed in any Search Engine. (There are three steps in which ranking works).

- **Step 1:** Analyze user query – This step is to understand what kind of information the user is looking for. To do that analyze the user's query by breaking it down into a number of meaningful keywords.
- **Step 2:** Finding matching pages – This step is to look into their index and find the best matching pages, for example, if you search dark wallpaper then it gives you the result of images, not text.
- **Step 3:** Present the results to the users – A typical search results page includes ten organic results in most cases it is enriched with other elements like paid Ads, direct answers for specific queries, etc.