Network:

A network is a group of two or more computer systems linked together and ready to communicate each other or allows data to be transmitted from one machine to another. In other words, network is a group of computers connected by cable or other media so that they can share information/resources. Networked computers can share many things like printer, Internet, Drives, File and Folders, messages, modem etc.

Advantages of computer network:

1. **Sharing of resources** like files, data or hardware. (It provides all data & information to the users or computers connected to the computer network, without regarding their physical location. Computers on net can share printers, hard disks, files etc. Computers on net can communicate with one another. Multiple users simultaneously access a file without corrupting the data.)
2. **Reliability:** It improves the reliability of entire system by permitting other computers to take over the work of a machine, which is out of service. (If one system goes down, other will take care.)
3. **Faster and cheaper** communication (saves time and cost of message transfer)
4. **Centralized control:** Controlling of all the computers and resources is possible from the server.

Disadvantages of networking:

1. **Expensive**: Extra devices like NIC, Hubs, Cables, Modem etc are required
2. **Security of data**: data may be hacked and used by third party
3. **Needs technical knowledge**: skilled manpower is required.

Types of networks:

There are three types of networks:

1. LAN (Local Area Network)
2. MAN (Metropolitan Area Network)
3. WAN (Wide Area Network) or LHN (Long Haul Network)

LAN

Any collection of interconnected computers that is located within small area, like an office or a building is called Local Area Network (LAN).

- LANs are privately-owned network within a single building upto few kilometers in size (computer ownership of a single organization)
- Data and Hardware sharing between users
- Computers are connected through inexpensive cables (twisted-pair or co-axial cable)
- It transfers data at high speed (i.e. much faster than data can be transmitted over a telephone line)
- LAN architecture consists of cables, topology, protocol and network interface hardware.

MAN

MAN is a network that is larger than LAN. It is called metropolitan since it normally covers the area of a city or town. It provides network communication between different business houses or bank branches located at different areas or localities within the city. It might be either private or public. Many heterogeneous systems can be interconnected in this system. Computers are connected through telephone lines and modems. This network can use guided or unguided media. The range could be upto 100 kms. It has very high chances of data leakage or security break.

WAN or LHN

A WAN is a computer network that communicates over a long distance such as across a city or around the world. (That is, it spans a relatively large geographical area; spread over states or countries). For the data communication, they use telephone lines, microwave link or satellite communication channels rather than through a single physical cable. They are owned by different organizations. It is the combination of many different types of LAN and MAN networks, so it has massive amount of heterogeneous systems. For example: Internet

Transmission Media:

Transmission media are the means by which data is transmitted between the sending and receiving devices in a network. It can be divided into two broad categories: **Guided and Unguided**. Guided media provides the physical connection from one network device to another device. This includes: Twisted-Pair cable, Co-axial cable and Fiber Optic cable. Unguided media transmits wave signals without using physical connection. This type of communication is often referred as Wireless communication. Signals are normally broadcast through air and thus are available to anyone who has a device capable of receiving them. This includes Microwave system, Communication satellite systems and infrared system.

Copper wires:

Computer networks use wires as the primary medium to connect computers because wire is inexpensive and easy to install. Although wires can be made from various metals, many networks use copper because its low resistance to electric current means signal can travel farther. Thus, network professionals sometimes use the term copper as a synonym for wire.

Two basic wiring types: Twisted pair and Co-axial cable.

(i) Twisted Pair Wire:

Twisted pair cables are the oldest and still most common transmission line and consists of copper wires twisted into pairs. The pairs are twisted to minimize electrical noise (random unwanted signals picked up by the channel). They are inexpensive and easily available. They are used in telephone connections and most modern Ethernet networks for voice and data transmission. Actually, it can support low-noise data traffic to a great speed as 100 Mbps.

Twisted pair cable often is installed using a *Registered Jack 45* (RJ-45) connector. The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.

There are two types of twisted pairs:

1. Unshielded Twisted Pair (UTP) cables
2. Shielded Twisted Pair (STP) cables

Unshielded twisted pair (UTP) is a popular type of cable that consists of two unshielded wires twisted around each other, i.e., each of the eight individual copper wires in UTP cable is covered by an insulating material and the wires in each pair are twisted around each other. Due to its low cost, UTP cabling is used extensively for local area networks (LANs) and telephone connections. UTP cabling does not offer as high bandwidth or as good protection from interference as coaxial or fiber optic cables, but it is less expensive and easier to work with. UTP may support data transfer rates from 1 to 100Mbps at distances up to 100 m. 10 Mbps is the most common transmission rate in use today.

Shielded twisted pair (STP) is a cable that is wrapped in a metal sheath to provide extra protection from external interfering signals, i.e., each pair of wires is wrapped in a metallic foil. The four pairs of wires then are wrapped in an overall metallic foil. So, STP reduces electrical noise more than UTP. It is more expensive and difficult to install. In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals. Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks. It is capable of greater transmission speeds, up to 500 Mbps at 100m. The most common transmission rate is 16 Mbps.

Disadvantages:

Noise: i.e., random unwanted signals picked up by the channel

Distortion: i.e., changes to the shape of the signal caused by absorption of the signal and delays by the medium.

(ii) Co-axial cables:

Co-axial cables consist of a conductive wire (made up of copper) in inner layer, covered by an insulating material. The outer layer (over the insulating material) is also a conductive material that is in the form of mesh surrounding the insulating tube. A co-axial cable is capable of transmitting data from various workstations simultaneously. Coaxial cables are used in communication networks that require many simultaneous communication links. Each coaxial cable can provide more than 5000 links.

Coaxial cable supports 10 to 100 Mbps and is relatively inexpensive, although it is more costly than twisted pair on a per-unit length. However, coaxial cable can be cheaper for a physical bus topology because less cable will be needed. Coaxial cable can be cabled over longer distances than twisted-pair cable. For example, Ethernet can run approximately 100 meters using twisted-pair cabling. Using coaxial cable increases this distance to 500m.

They are a reliable medium of data transmission because of very little distortion or signal loss.

- They are used in cable TV and the medium of choice to connect computers and terminals located in nearby building, i.e., used generally in LAN.
- Coaxial cable is less expensive than fiber-optic cable, and the technology is well known; it has been used for many years for all types of data communication.

There are two types of coaxial cable. They are: Thicknet and Thinnet.

- The coaxial cable with thickness or diameter of 1 centimeter is referred to as Thicknet.
- Coaxial cable with an outside diameter of only 0.35 cm is referred to as Thinnet.

The most common connectors used with coaxial cable are BNC, *Bayonet Neil Concelman*, connectors. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector. BNC T-connectors are used to connect two cables to a network interface card (NIC).

(iii) Fiber optic cables:

Fiber optic cables transmit data in the form of light rays. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves over long distances. Hence, they are free from any outside interface like noise. A single optical fiber has the following parts:

- Core - Thin glass center of the fiber where the light travels
- Cladding - Outer optical material surrounding the core that reflects the light back into the core
- Plastic coating - Plastic coating that protects the fiber from damage and moisture

Hundreds of these optical fibers are arranged in bundles in optical cables. The bundles are protected by the cable's outer covering, called a jacket.

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
- Fiber optic cables are much thinner and lighter than metal wires.
- It is capable of transmitting data in huge volumes and high speeds.
- They are very expensive.
- The chances of data being corrupted through the transmitting line are very less

Optical Fibers come in two types:

1. Single-mode fibers have small cores and transmit infrared laser light.
2. Multi-mode fibers have larger cores and transmit infrared light from light-emitting diodes (LEDs).

Fiber optic cables use two different types of connectors:

The ***subscriber channel (SC)*** connector is used in cable TV. It uses a push/pull locking system.

The ***straight-tip (ST)*** connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.

(iv) Microwave system:

Microwave systems transmit high-speed radio signals in a line-of-sight path between relay stations (i.e., transmission from one antenna to another usually placed on top of buildings, towers, hills and mountain peaks). Microwave system transmits high-speed radio signals in a line of sight path between relay stations spaced approximately 25 to 35 miles apart. It has a much lower error rate and communication links can be made over large distance. Simply, Microwave transmission consists of high frequency radio waves that travel in straight line through the air rather than through wires. Networks using radio signal transmission do not require a direct physical connection between computers. Instead, each participating computer attaches to an antenna, which can both transmit and receive radio signals.

(v) Communication satellite:

Although radio transmissions do not bend around the surface of the earth, Radio frequency technology can be combined with satellites to provide communication across longer distance. Satellites have now become an integral part of the worldwide communications system. It is nothing more than microwave (radio) relay station. They have the capability of a direct line of sight path to almost the earth's entire surface. So, they can transmit high-speed microwave (or radio-signal) to the transmitters on the ground (earth). A ground station on one side of the ocean transmits a signal to the satellite, which then sends the signal to a ground station on the other side. A single satellite usually contains multiple transponders (device that consists of a radio receiver and transmitters that operate independently (typically six to twelve). Each transponder uses a different radio frequency, making it possible for multiple communications to proceed simultaneously. This uses satellites orbiting 22,000 miles above the earth for transmitting the data form relaying station at one end of the globe to the receiving station at the other end of the globe. It accounts for most long-distance international communications.

(vi) Infrared:

The wireless remote controls used with appliances such as televisions and stereos communicate with infrared transmissions. Infrared is limited to a small area (e.g., a single room), and usually requires that the transmitter be pointed toward the receiver. Infrared hardware is inexpensive compared to other mechanisms, and does into require an antenna.

Computer networks can use infrared technology for data communication. For example, it is possible to equip a large room with a single infrared connection that provides network access to all computers in the room. Computers can remain in contact with the network while they are moved within the room. Infrared networks are especially convenient for small, portable computers because infrared offers the advantages of wireless communication without requiring the use of antennas. Thus, a portable computer that uses infrared can have all communication hardware built in.

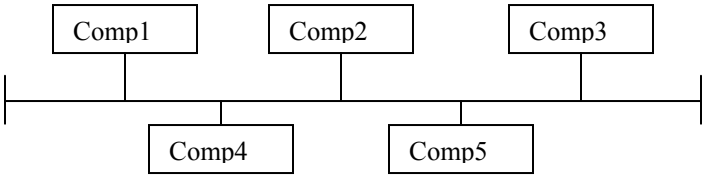
Network Topology:

Network Topology is the way of connecting the computer in LAN or way of cabling in networking. That is, the way in which the connections are made is called topology of the network. The major goal of topology is to find out the most economical and efficient way to connect all the users to the network resources. There are three basic network topology namely Bus topology, Star topology and Ring Topology.

1. **Bus Topology:** A bus topology is also known as linear topology. It consists of several computers that are attached to a common cable called a *bus or trunk*, which is a backbone for the network.

   Advantages:
   - It is a simple, reliable and easy to use
   - It is easy to extend (any number of computers can be connected by using a connector in the bus).
   - Since it uses co-axial cable, it is less expensive than other arrangement.

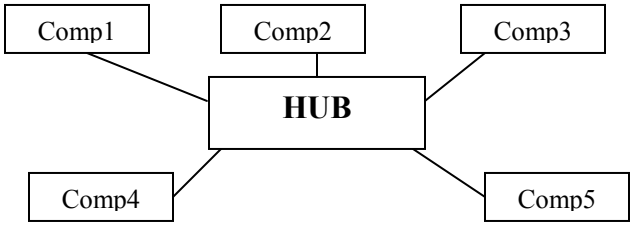
   Disadvantages:
   - If the cable fails, then the entire system fails to respond to the user.
   - Since the cable is one, fault finding and troubleshooting becomes very difficult.
   - Data traffic is high; Data collision is high



2. **Star Topology:** In star topology, all the computers are connected to a centrally located device called a "hub". This center node (hub) is connected to a powerful central computer known as server.

   Advantages:
   - It is flexible (Easy to add and remove computers)
   - Easy to find fault as it uses hub
   - The cable (one computer) failure does not halt the entire network

   Disadvantages:
   - It is more expensive than bus topology as it requires extra cables and other controlling devices.
   - Failure of the Hub or server makes the entire system disturbed

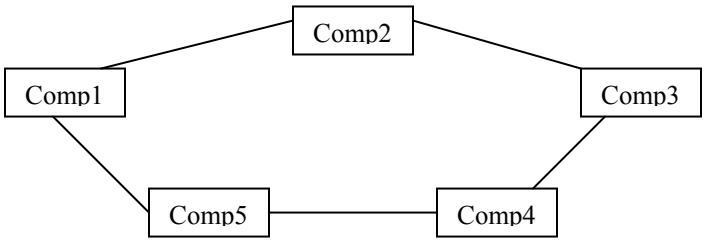


3. **Ring Topology:** In this topology, the cabling runs from computers to computers without any endpoint to form a loop, i.e., data flows in circular manner through the ring cable. It is based on peer-to-peer architecture. A ring topology passes data in only one direction. So the failure of one node can affect the entire network.

   Advantages:
   - Short cable length than star topology
   - There is no dependency on central node
   - Less chance of data collision as data travels

Disadvantages:

- Failure of any one computer on the network disturbs the entire system
- Not flexible (adding and removing the computers are difficult)
- Difficult to diagnose faults (whenever any terminal gets failed that will affect all others, so need to check a series of adjacent terminal)



4. Tree Topology:

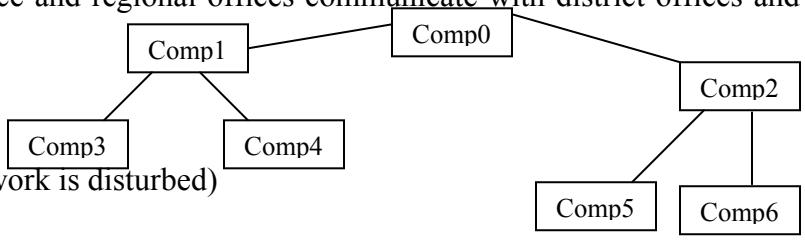
The tree topology arranges computers in a hierarchical structure in order to allow greater control and easier troubleshooting. So tree network is also known as Hierarchical network. The computer in upper level acts as server and at lower level acts as client. This type of network mostly used in the organization where headquarters communicate with regional office and regional offices communicate with district offices and so on.

Features:

It is Easy to extend

Dependent on root

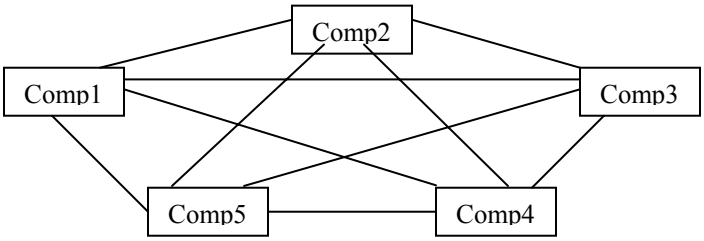
(If main device fails to operate, the entire network is disturbed)



5. Mesh Topology:

In mesh topology, every computer has a dedicated link to every other computer. If any of the computer is down then other computers can still continue to work. It is very much complex to implement and hard to find out the fault.

It is expensive, as it requires a lot of I/O ports



Network architecture:

Network architecture can be broadly classified into two types.

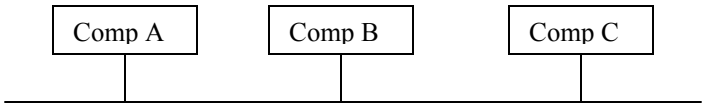
1. Peer-to-peer architecture (Point to point architecture)
2. Client-server (or server-based) architecture

Peer-to-Peer Architecture:

In peer-to-peer network, computers are connected individually in pair (one to one connection). There is no dedicated server. All the computers are equal, termed as peers. Each computer on the network has the capability to share data and resources with other computers. In other words there is no central authority that determines the network's resources sharing policy. Each user has the right to decide what he would or would not like to share. Each computer acts as both client and a server. This arrangement is suitable in small office network.

Advantages: inexpensive, easy setup, easy maintenance

Disadvantages: low security, scattering data.

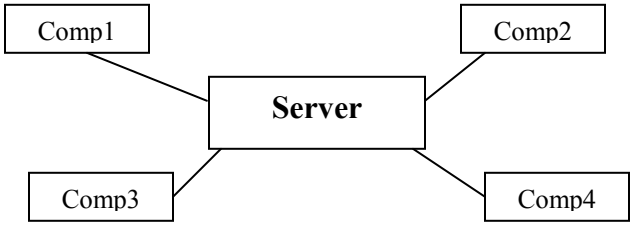


Structure of peer-to-peer

Client-Server architecture: (server-based)

This is a network architecture in which each computer on the network is either a client or a server. Each client (computer using central resources (server)) is connected to a centrally located dedicated computer called server. Servers are powerful computers, which provide services to other computers. They control data as well as printers and other resources that clients need to access. The server must be faster and more storage capacity to contain al the data, needs to be shared to the clients. There are different types or servers.

1. File servers: Managing files or disk drives
2. Print Server: To handle printing request.
3. Communication server: they are setup to handle remote users dialing into your network.
4. Mail Server: Specially setup to handle client's email
   Advantages: centralized security, easy accessibility.
   Disadvantages: dependent on an administrator, expensive server.



Client: computer that uses the services that a servers provides. The client is less powerful than server

Server: powerful computer that provides services to other computers on the net.

Protocol:

Protocols are a set of rules that control transmission (sending and receiving) of signals. In other words, it is a language of networking by which computers communicate with each other. Protocol defines a set of commands which one machine sends to another. If message is too large, protocol will split it up into several packets and make sure that they all arrive correctly. The most commonly used protocols are

1. TCP/IP: (Transmission Control Protocol/Internet Protocol)
   - Used in WAN and LAN
   - The Internet is based on TCP/IP
2. HTTP: (Hyper Text Transfer Protocol)
   - To transfer hypertext or web documents
   - Hypertext is text that is specially coded using standard system called HTML (Hyper Text Markup Language)
3. FTP: (File Transfer Protocol)
   - Part of TCP/IP
   - Enables files to be transferred between computers
4. Telnet: This protocol enables one computer to connect with another computer
5. NetBeui: (NetBios User Interface)
   - Mostly used in LAN.

OSI Reference Model (Seven-Layer Network Architecture)

All network are based on a theoretical model called the open system Interconnection model designed by ISO (International standard organization) in 1982. It is also known as ISO/OSI standard, which defines how network devices interact with each other, i.e, it describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI model works on a layer approach (conceptual model composed of seven layers), where each layer is responsible for performing certain network functions.
There are distinct seven layers.

7. Application Layer
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data- link Layer
1. Physical layer

1. Physical Layer: Physical layer is the lowermost layer of the model. It represents physical aspects (elements) of the network, i.e, basic network hardware. The network's transmission lines (the cables that connect all the computers of the network) connections are parts of the physical layer.
2. Data- Link Layer: this layer specifies how to organize into frames (the form of a packet that the underlying hardware accepts and delivers) and how to transmit frames over a network. This layer takes data fames or messages from the Network layer and provides for actual transmission. At the receiving computer, this layer receives the incoming data and sends it to network layer for handling. It provides error- free delivery of data between the two computers by using physical layer.
3. Network layer: this layer defines how addresses are assigned and how packets are forwarded from one end of network another. It is responsible for finding a path (route) through the netwrok to the destination (for addressing messages and data). So the data are sent to correct destination.
4. Transport layer: this layer is responsible for reliable transfer of information across the network. It ensures that the delivered (transmitted/received) data is error free, in sequence and with no loss or duplication.
5. Session layer: this layer specifies how to establish a communication session with a remote system. [It allows two applications to establish, use and disconnect a connection between them called a session]. This layer negotiates connections between processes or applications on different computers. As such, this layer handles details such as account names and passwords.
6. Presentation layer: this layer is responsible for text formatting and display code conversion (i.e., data displayed in red color by the sending device are also displayed in red by the receiving device). It is the layer that can change data itself (.doc, .xls, .bmp etc) are converted into same extension.
7. Application layer: highest layer of the OSI model and is the only layer that user will operate in. it acts as the interface between the actual software application and the communication process. It represents applications like E-mail, databases etc.

PSTN:

PSTN (Public Switching Telephone Network) is the system of communication used by telephone offices (Telecommunication office). It is general circuit switching system in which caller is linked with the receiver with the help of automated circuit switching through a copper wire as medium.

PABX:(or PBX):

PABX stands for private automatic branch exchange, a device for switching telephone calls within a building such as an office or factory. It is a system of telephone exchange being used by private offices as their private switching system. The fundamental principles of PABX switching are the same as those found in a much larger central office switch, which is used in the public network to switch telephone from the caller to receiver.

A dedicated telephone line (PSTN) is taken from telecommunication office and linked to the PABX system, which is distributed to different departments. Each department is given a unique extension number for switching.

Telex:

Telex is an old means of sending an electronic text message. A simple text message, normally created on a personal computer can be sent directly to another user on the networks in real time. Telex has retained many of its restrictions. The character set available to telex users is limited. The character set is limited to uppercase only, numbers and 13 special characters, which do not include £, $ or %. The transmission rate for telex is limited to 50 bps.

Teletex:

A new version of the old telex service, compatible with fax and able to send pictures as well as text it called teletex. Unlike telex, teletex operates on an A4 page format. Documents are prepared using word processor and are then transmitted directly to the receiving device's storage, which may be floppy or harddisk.

- Teletex operates at a much higher speed than telex (2400bps).
- Teletex also makes available a much larger character set with full upper and lowercase working.
- It is independent of a specific network

FAX (Facsimile) and E-Fax:

The machine, which makes copies of documents and sends them through telephone lines to another place, is called FAX machine. It can transmit text or graphics from source to destination in the same format.

In the office, a document or message can be created in one of three ways: using a typewriter, using a word processor or by hand. This document may contain images, signatures, text and other symbols. Facsimile works by using an optical reading head to scan the document and is converted to proper format for transmission by the fax modem and it is transmitted via a telephone wire. At the destination, such signal is again demodulated and converted into proper format by the destination fax machine. Nowadays the same function can be done using computer (instead of fax machine) and Internet, which is known as E-fax.

The speed of fax modem is measured by bps. The modem with high speed 56 kbps will be suitable for accessing the graphics.

Internet: (International Network)

Internet is an interconnection between several computers of different types belonging to various networks all over the world. It is the world's largest computer network, the network of networks, i.e. global network. The Internet offers access of data, graphics, sound, software, text, and people through a variety of services and tools for communication and data exchange.

Intranet:

Intranet is an Internet-like network within companies, i.e. it is a kind of internal web hosting (publishing) or internal networks within organization(s). It is not public, it is private network group and owned by a particular organization. Only those persons, who are authorized users of that organization, can only use this net. Generally, information regarding to a particular subject is kept in these nets. This technology also contains web sites for internal users, allowing employees to access often used forms, company news, announcements and clarifications. Network used by police or army headquarters are the examples of Intranet.

Networking Devices:

1. **Modems:**

The word modem stands for MOdulator/DEModulator. A modem is a device which converts the digital signals from a computer or transmission terminal at one end of a communications link into analog signals (Modulation), which can be transmitted over ordinary telephone lines. A modem at the other end of the communication line converts the transmitted data back into digital form at the receiving terminal (Demodulation)

The speed at which the modems can transfer data is measured in bits per second (bps). Most popular modems are of 33.6 kbps (kilo bits per second) or 56 kbps.

2. **HUB:**

- Hub is a device for connecting different computers on the network (generally star topology).
- It consists multiple ports
- It is non-intelligent device.
- It does not control data-traffic.
- Transfer speed is up to 100 mbps
- Share the speed between different computers
- May or may not contain cooler
- It operates at physical layer of OSI model

3. **Switch:**

- Switch is an intelligent device for connecting different computers on the network
- It operates on data link layer
- It can filter packets (data) ---> Hardware filtration
- It does not share bandwidth (so, fast)
- It consist processor, so cooler is needed

4. **Bridge:**

It is used to combine two different networks.
It is a connecting device between two or more hubs
It operates on physical and data link layer
Filtration is done by software (reduces unnecessary traffic problem)
Bridge is slower

5. **Repeater:**

- It operates on physical layer
- It increases the distance over which a network can extend
- It receives signals, amplifies them and sent it.
- If data travels beyond certain distance (100 m for twisted pair) without amplification, then it becomes weaker and after some time the signal will be destroyed. A repeater provides solution for such problem.

6. **Router:**

- It operates on Network layer
- Router is most intelligent interconnecting device
- It consists FIREWALL (ACL-->Access Control List)
- Main function is path determination and switching
- Router needs Internetworking operating software (IOS) to run configuration files

Switching:

A process of establishing a session and path with different network components is called switching. Data entering the network from a station are routed to the destination by being switched from node to node.

There are three types of switching techniques.

Circuit switching network:

It is a technology that describes a way the nodes switch the information from one link to another on the way from source to destination. Communication through circuit switching implies that there is a dedicated communication path between two stations. That path is a connected sequence of links between nodes. The most common example of circuit switching is the telephone network.

Message switching network:

With message switching, it is not necessary to establish a dedicated path between two stations. If a station wishes to send a message (a logical unit of information) it appends a destination address to the message. The message is then passed through the network from node to node. At each node, the entire message is received, stored and then transmitted to the next node. The term 'store and forward' is associated with message switching. This switching technique is also known as store and forward technique.

In circuit switching network, each ode is an electronic switching device, which transmits bits as fast as it receives them. A message-switching node is typically a computer, with sufficient storage to buffer messages as they come. A message is delayed at each node for the time required to receive all bits of the message plus a queuing delay waiting for an opportunity to retransmit to the next node.

Packet switching network:

In this technique, data are transmitted in the form of packets. Packet is a small, self-contained parcel data sent across a computer network. Each pack contains a header that identifies the sender and recipient and data to be delivered. For a larger message to be transmitted, the message is first broken into a series of packets. A packet contains a portion of user data and some control information. This information includes minimum information that the network requires to route the packet through the network and deliver it to the intended destination. At each node, the packets are received, examine the address, select the next node to which it shall transmit the packet and sends it on its way. Most modern networks are packet switching. Advantage over message switching is that first packet of multipacket message can be forwarded before the second one has fully arrived, reducing delay.

Circuit switching	**Message switching**	**Packet switching**
Dedicated transmission path	No dedicated path	No dedicated path.
Continuous transmission of data	Transmission of messages	Transmission of packets
Fast enough for interactive	Too slow for interactive	Fast enough for interactive
Data are not stored	Message may be stored	Packets may be stored until delivered.
Negligible transmission delay	Message transmission delay	Packet transmission delay.

Multiplexing:

Multiplexing is the process of combining the transmission from several devices into a single data stream that can be transmitted over a single communication channel. A multiplexer is a device that produces multiplexing. It is also used at the receiving end to separate the transmissions and send them back, in their original order for processing. A multiplexer allows the communication channels to transmit much more data at any one time, that what a single device can send. Multiplexers are more efficient and less expensive.