## A] INTRODUCTION TO COMPUTER NETWORKS:

Each of the past three centuries has been dominated by a single technology. The 18th century was the era of the great mechanical systems accompanying the Industrial Revolution. The 19th century was the age of the steam engine.

During the 20th century, the key technology was information gathering, processing, and distribution. Among other developments, the installation of worldwide telephone networks, the invention of radio and television, the birth and unprecedented growth of the computer industry, and the launching of communication satellites.

As a result of rapid technological progress, these areas are rapidly converging and the differences between collecting, transporting, storing, and processing information are quickly disappearing. As our ability to gather, process, and distribute information grows, the demand for ever more sophisticated information processing grows even faster.

Although the computer industry is still young compared to other industries (e.g., automobiles and air transportation), computers have made spectacular progress in a short time. During the first two decades of their existence, computer systems were highly centralized, usually within a single large room.

A medium-sized company or university might have had one or two computers, while large institutions had at most a few dozen. The idea that within twenty years equally powerful computers smaller than postage stamps would be mass produced by the millions was pure science fiction.

The merging of computers and communications has had a profound influence on the way computer systems are organized. The concept of the "computer center" as a room with a large computer to which users bring their work for processing is now totally obsolete.

The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large number of separate but interconnected computers do the job. These systems are called computer networks.

The term "computer network" to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used. Networks come in many sizes, shapes and forms. Although it may sound strange that, neither the Internet nor the World Wide Web is a computer network.

The Internet is not a single network but a network of networks and the Web is a distributed system that runs on top of the Internet.

**Characteristics of Computer Network:**

The primary purpose of a computer network is to share resources:

1. You can play a CD from one computer while sitting on another computer
2. You may have a computer that doesn't have a DVD or BluRay (BD) player. In this case, you can place a movie disc (DVD or BD) on the computer that has the player, and then view the movie on a computer that lacks the player
3. You may have a computer with a CD/DVD/BD writer or a backup system but the other computer doesn't have it. In this case, you can burn discs or make backups on a computer that has one of these but using data from a computer that doesn't have a disc writer or a backup system
4. You can connect a printer (or a scanner, or a fax machine) to one computer and let other computers of the network print (or scan, or fax) to that printer (or scanner, or fax machine)
5. You can place a disc with pictures on one computer and let other computers access those pictures
6. You can create files and store them in one computer, then access those files from the other computer(s) connected to it.

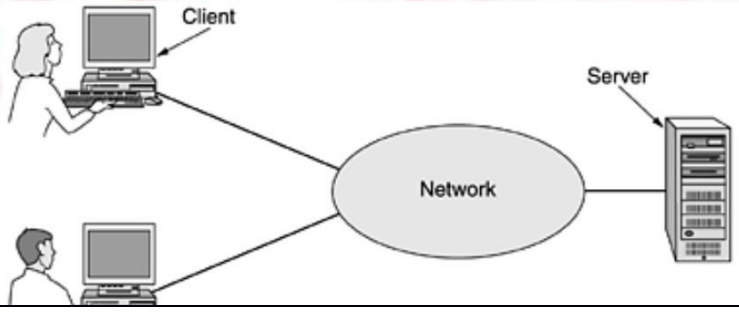
**Uses of Computer Networks:**

1. **Business Applications**

The issue is resource sharing, and the goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. An obvious and widespread example is having a group of office workers share a common printer. None of the individuals really needs a private printer, and a high-volume networked printer is often cheaper, faster, and easier to maintain than a large collection of individual printers.

However, probably even more important than sharing physical resources such as printers, scanners, and CD burners, is sharing information. Every large and medium-sized company and many small companies are vitally dependent on computerized information. Most companies have customer records, inventories, accounts receivable, financial statements, tax information, and much more online. If all of its computers went down, a bank could not last more than five minutes. A modern manufacturing plant, with a computer-controlled assembly line, would not last even that long. Even a small travel agency or three-person law firm is now highly dependent on computer networks for allowing employees to access relevant information and documents instantly.

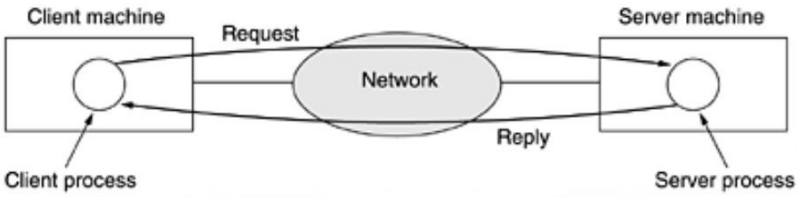
For smaller companies, all the computers are likely to be in a single office or perhaps a single building, but for larger ones, the computers and employees may be scattered over dozens of offices and plants in many countries. In the simplest of terms, one can imagine a company's information system as consisting of one or more databases and some number of employees who need to access them remotely. In this model, the data are stored on powerful computers called servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called clients, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing. The client and server machines are connected by a network.



**A network with two clients and one server.**

This whole arrangement is called the client-server model. It is widely used and forms the basis of much network usage. It is applicable when the client and server are both in the same building, but also when they are far apart. For example, when a person at home accesses a page on the World Wide Web, the same model is employed, with the remote Web server being theserver and the user's personal computer being the client. Under most conditions, one server can handle a large number of clients.

**The client-server model involves requests and replies.**




Many companies is doing business electronically with other companies, especially suppliers and customers. For example, manufacturers of automobiles, aircraft, and computers, among others, buy subsystems from a variety of suppliers and then assemble the parts. Using computer networks, manufacturers can place orders electronically as needed. Being able to place orders in real time reduces the need for large inventories and enhances efficiency.

Another goal that is starting to become more important is doing business with consumers over the Internet. Airlines, bookstores, and music vendors have discovered that many customers like the convenience of shopping from home. Consequently, many companies provide catalogs of their goods and services online and take orders on-line. This sector is expected to grow quickly in the future. It is called e-commerce.

2. **Home Applications**

Some of the more popular uses of the Internet for home users are as follows:

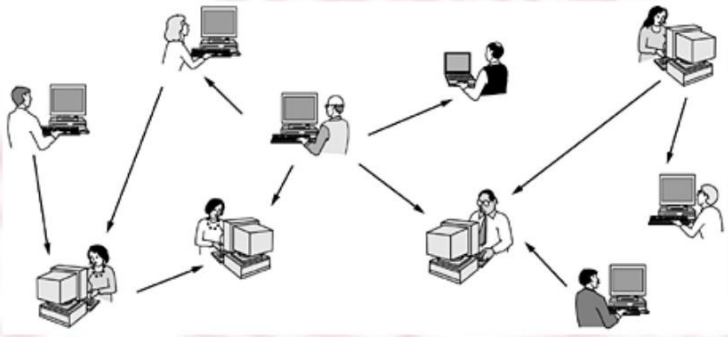
- Access to remote information.
- Person-to-person communication.

- Interactive entertainment.
- Electronic commerce.

Access to remote information comes in many forms. It can be surfing the World Wide Web for information or just for fun. Information available includes the arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel, and many others. Many newspapers have gone on-line and can be personalized. The next step beyond newspapers (plus magazines and scientific journals) is the on-line digital library. Many professional organizations, such as the ACM (www.acm.org) and the IEEE Computer Society (www.computer.org), already have many journals and conference proceedings on-line.

The second broad category of network use is person-to-person communication, basically the 21st century's answer to the 19th century's telephone. E-mail is already used on a daily basis by millions of people all over the world and its use is growing rapidly. It already routinely contains audio and video as well as text and pictures. Worldwide newsgroups, with discussions on every conceivable topic, are already commonplace among a select group of people, and this phenomenon will grow to include the population at large. These discussions, in which one person posts a message and all the other subscribers to the newsgroup can read it, run the gamut from humorous to impassioned. Another type of person-to-person communication often goes by the name of peer-to-peer communication, to distinguish it from the client-server model. In this form, individuals who form a loose group can communicate with others in the group. Every person can communicate with one or more other people; there is no fixed division into clients and servers.

**peer-to-peer system there are no fixed clients and servers.**



The third category is entertainment, which is a huge and growing industry. The killer application is video on demand. A decade or so hence, it may be possible to select any movie or television program ever made, in any country, and have it displayed on your screen instantly. Live television may also become interactive, with the audience participating in quiz shows, choosing among contestants, and so on.

The fourth category is electronic commerce in the broadest sense of the term. Home shopping is already popular and enables users to inspect the on-line catalogs of thousands of companies. Some of these catalogs will soon provide the ability to get an instant video on any product by just clicking on the product's name. After the customer buys a product electronically but cannot figure out how to use it, on-line technical support may be consulted.

One area that virtually nobody foresaw is electronic flea markets (e-flea?). On-line auctions of second-hand goods have become a massive industry. Unlike traditional e-commerce, which follows the client-server model, on-line auctions are more of a peer-to-peer system, sort of consumer-to-consumer.

Computer networks may become hugely important to people who are geographically challenged, giving them the same access to services as people living in the middle of a big city. Telelearning may radically affect education; universities may go national or international. Telemedicine is only now starting to catch on (e.g., remote patient monitoring) but may become much more important.

### 3. Mobile Users

Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest-growing segments of the computer industry. Many owners of these computers have desktop machines back at the office and want to be connected to their home base even when away from home or en route. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless networks.

People on the road often want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, surf the Web, access remote files, and log on to remote machines. And they want to do this from anywhere on land, sea, or air. For example, at computer conferences these days, the organizers often set up a wireless network in the

conference area. Anyone with a notebook computer and a wireless modem can just turn the computer on and be connected to the Internet, as though the computer were plugged into a wired network. Similarly, some universities have installed wireless networks on campus so students can sit under the trees and consult the library's card catalog or read their e-mail.

Wireless networks are important to the military. If you have to be able to fight a war anywhere on earth on short notice, counting on using the local networking infrastructure is probably not a good idea. It is better to bring your own. Although wireless networking and mobile computing are often related, they are not identical.

On the other hand, some wireless computers are not mobile. An important example is a company that owns an older building lacking network cabling, and which wants to connect its computers. Installing a wireless network may require little more than buying a small box with some electronics, unpacking it, and plugging it in. This solution may be far cheaper than having workmen put in cable ducts to wire the building.

A whole different application area for wireless networks is the expected merger of cell phones and PDAs into tiny wireless computers. A first attempt was tiny wireless PDAs that could display stripped-down Web pages on their even tinier screens.

Since the network operator knows where the user is, some services are intentionally location dependent. For example, it may be possible to ask for a nearby bookstore or Chinese restaurant. Mobile maps are another candidate. So are very local weather forecasts. No doubt many other applications appear as these devices become more widespread.

**4. Social Issues**

The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks is newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The trouble comes when newsgroups are set up on topics that people actually care about, like politics, religion, etc. Views posted to such groups may be deeply offensive to some people. Furthermore, messages need not be limited to text. High-resolution color photographs and even short video clips can now easily be transmitted over computer networks.

Another fun area is employee rights versus employer rights. Many people read and write e-mail at work. Many employers have claimed the right to read and possibly censor employee messages, including messages sent from a home computer after work. Not all employees agree with this.

Another key topic is government versus citizen. The FBI has installed a system at many Internet service providers to snoop on all incoming and outgoing e-mail for nuggets of interest to it. The government does not have a monopoly on threatening people's privacy. The private sector does its bit too. For example, small files called cookies that Web browsers store on users' computers allow companies to track users' activities in cyberspace and also may allow credit card numbers, social security numbers, and other confidential information to leak all over the Internet.

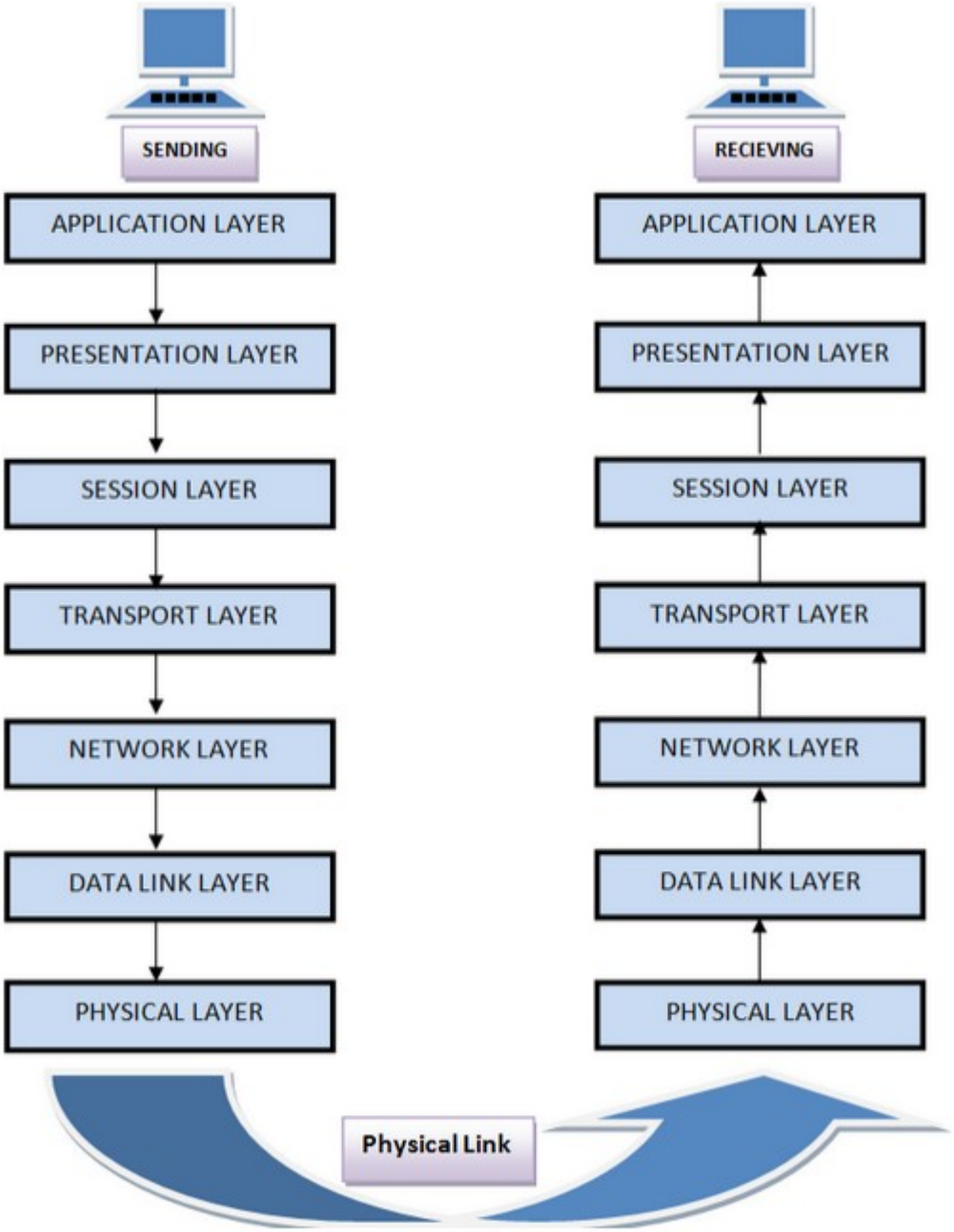
Along with the good comes the bad. The Internet makes it possible to find information quickly, but a lot of it is ill-informed, misleading, or downright wrong. The medical advice you plucked from the Internet may have come from a Nobel Prize winner or from a high school dropout.

Identity theft is becoming a serious problem as thieves collect enough information about a victim to obtain get credit cards and other documents in the victim's name. Finally, being able to transmit music and video digitally has opened the door to massive copyright violations that are hard to catch and enforce.

## ISO/OSI Model in Communication Networks

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other. ISO has developed this. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.


SENDING
APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER
RECIEVING
APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER
Physical Link

**Feature of OSI Model :**

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

**Functions of Different Layers :**

**Layer 1: The Physical Layer :**

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

**Layer 2: Data Link Layer :**

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

**Layer 3: The Network Layer :**

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

**Layer 4: Transport Layer :**

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

**Layer 5: The Session Layer :**

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

**Layer 6: The Presentation Layer :**

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.

3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It perfroms Data compression, Data encryption, Data conversion etc.

**Layer 7: Application Layer :**

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

**Merits of OSI reference model:**

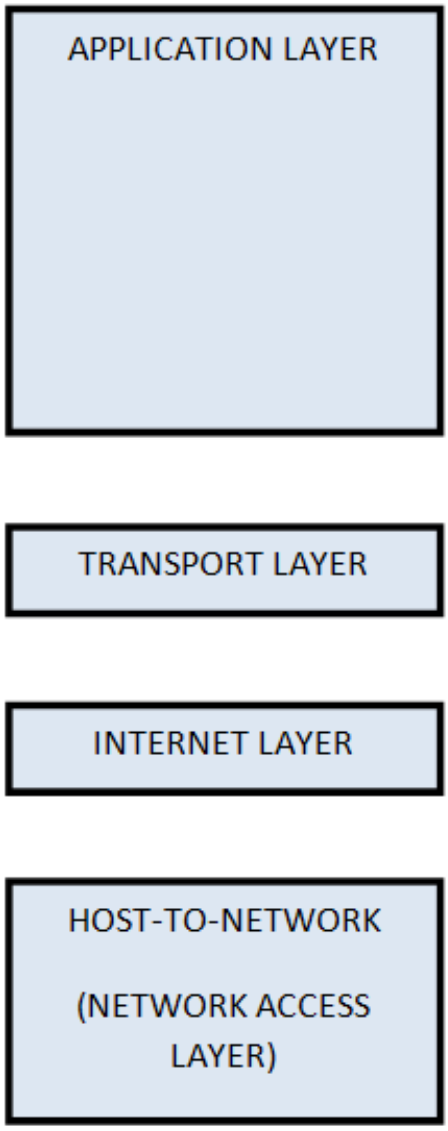
1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

**Demerits of OSI reference model:**

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

## The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.




**Overview of TCP/IP reference model**

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

**Description of different TCP/IP protocols**

**Layer 1: Host-to-network Layer**

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

**Layer 2: Internet layer**

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

**Layer 3: Transport Layer**

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

**Layer 4: Application Layer**

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

**Merits of TCP/IP model**

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

**Demerits of TCP/IP**

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

## Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

| OSI(Open System Interconnection) | TCP/IP(Transmission Control Protocol / Internet Protocol) |
|---|---|
| 1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user. | 1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network. |
| 2. In OSI model the transport layer guarantees the delivery of packets. | 2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable. |
| 3. Follows vertical approach. | 3. Follows horizontal approach. |
| 4. OSI model has a separate Presentation layer and Session layer. | 4. TCP/IP does not have a separate Presentation layer or Session layer. |
| 5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool. | 5. TCP/IP model is, in a way implementation of the OSI model. |
| 6. Network layer of OSI model provides both connection oriented and connectionless service. | 6. The Network layer in TCP/IP model provides connectionless service. |
| 7. OSI model has a problem of fitting the protocols into the model. | 7. TCP/IP model does not fit any protocol |
| 8. Protocols are hidden in OSI model and are easily replaced as the technology changes. | 8. In TCP/IP replacing protocol is not easy. |
| 9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent. | 9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent. |
| 10. It has 7 layers | 10. It has 4 layers |

## Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

### 1) Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

7. Its frequency range is 0 to 3.5 kHz.
8. Typical attenuation is 0.2 dB/Km @ 1kHz.
9. Typical delay is 50 µs/km.
10. Repeater spacing is 2km.

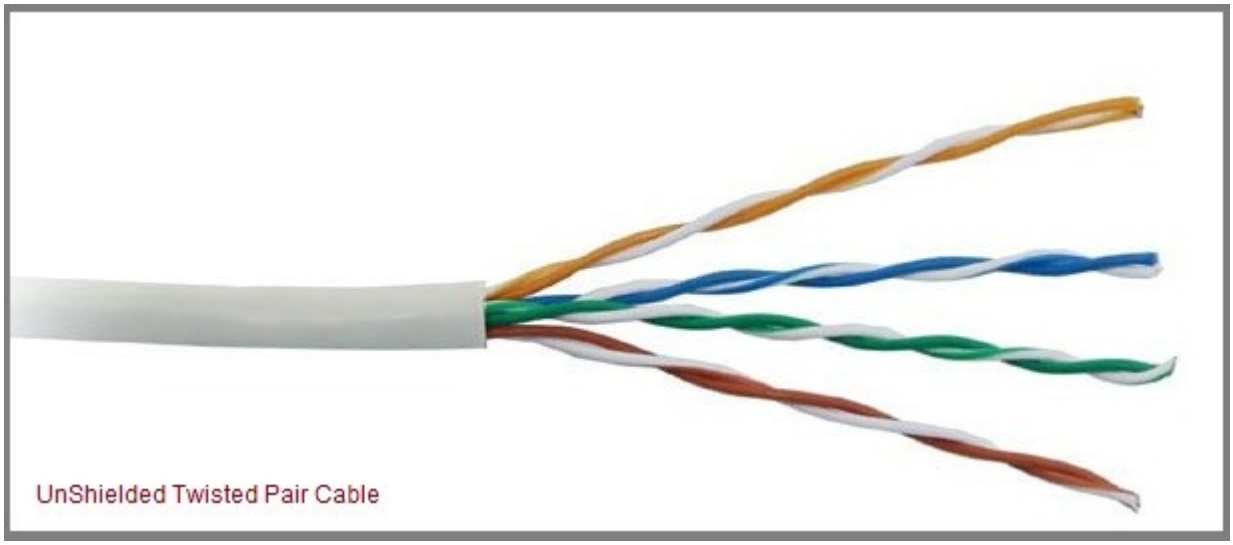
Twisted Pair is of two types :

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

### Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.




Categories of UTP:

CAT 5

1. 100 MHz Bandwidth
2. 24.0 dB Attenuation
3. 100 ohms Impedance
4. Used for high-speed data transmission
5. Used in 10BaseT (10 Mbps) Ethernet & Fast Ethernet (100Mbps)

**CAT 5e**

1. 150 MHz Bandwidth
2. 24.0 dB Attenuation
3. 100 ohms Impedance
4. Transmits high-speed data
5. Used in Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) &
6. 155 Mbps ATM

7. For runs of up to 90 meters
8. Solid core cable ideal for structural installations (PVC or Plenum)
9. Stranded cable ideal for patch cables
10. Terminated with RJ-45 connectors

## CAT 6

1. 250 MHz Bandwidth
2. 19.8 dB Attenuation
3. 100 ohms Impedance
4. Transmits high-speed data
5. Used in Gigabit Ethernet (1000 Mbps) & 10 Gig Ethernet (10000Mbps)

| | CAT5 | CAT5e | CAT6 |
|---|---|---|---|
| Frequency | 100 MHz | 100 MHz | 250 MHz |
| Attenuation (min. at 100 MHz) | 22 dB | 22 dB | 19.8 dB |
| Characteristic Impedance | 100 ohms = 15% | 100 ohms = 15% | 100 ohms = 15% |
| NEXT (min. at 100 MHz) | 32.3 dB | 35.3 dB | 44.3 dB |
| PS-NEXT (min. at 100 MHz) | NA | 32.3 dB | 42.3 dB |
| EL-FEXT (min. at 100 MHz) | NA | 23.8 dB | 27.8 dB |
| PS-ELFEXT (min. at 100 MHz) | NA | 20.8 dB | 24.8 dB |
| PS-ANEXT (min. at 500 MHz) | -- | -- | -- |
| PS-AELFEXT (min. at 500 MHz) | 16 dB | 20.1 dB | 20.1 dB |
| Return Loss (min. at 100 MHz) | 16 dB | 20.1 dB | 20.1 dB |
| Delay Skew (max. per 100m) | NA | 45 ns | 45 ns |
| Networks Supported | 100BASE-T | 1000BASE-T | 1000BASE-TX |

**Advantages :**

1. Installation is easy
2. Flexible
3. Cheap
4. It has high speed capacity,
5. 100 meter limit
6. Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

**Disadvantages :**

1. Bandwidth is low when compared with Coaxial Cable
2. Provides less protection from interference.

**Shielded Twisted Pair Cable**

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

**Advantages :**

1. Easy to install
2. Performance is adequate
3. Can be used for Analog or Digital transmission
4. Increases the signalling rate
5. Higher capacity than unshielded twisted pair
6. Eliminates crosstalk

**Disadvantages :**

1. Difficult to manufacture
2. Heavy

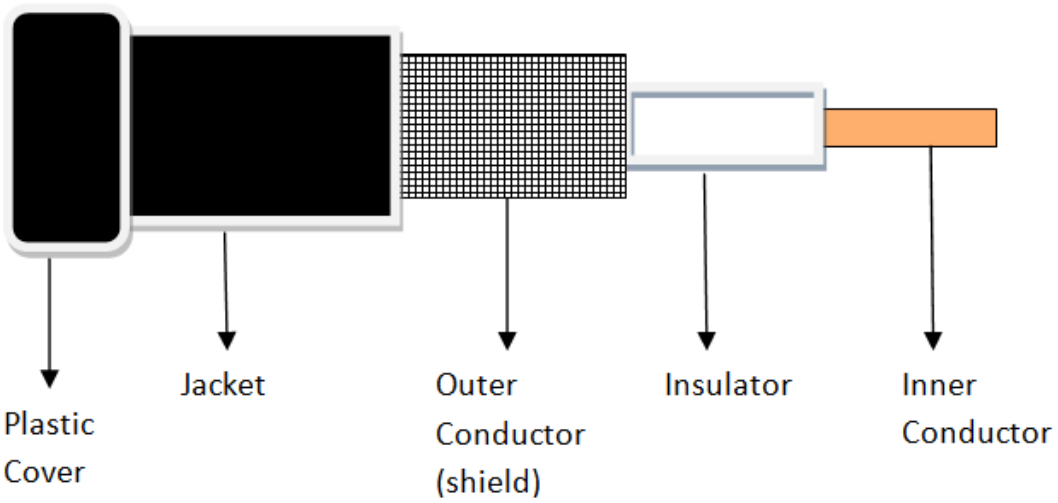
**2) Coaxial Cable**

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

1. 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
2. 50-Ohm RG-58 : used with thin Ethernet
3. 75-Ohm RG-59 : used with cable television
4. 93-Ohm RG-62 : used with ARCNET. There are two types of Coaxial cables :




**BaseBand**

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

**BroadBand**

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

**Advantages :**

1. Bandwidth is high
2. Used in long distance telephone lines.
3. Transmits digital signals at a very high rate of 10Mbps.
4. Much higher noise immunity
5. Data transmission without distortion.
6. The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

**Disadvantages :**

1. Single cable failure can fail the entire network.

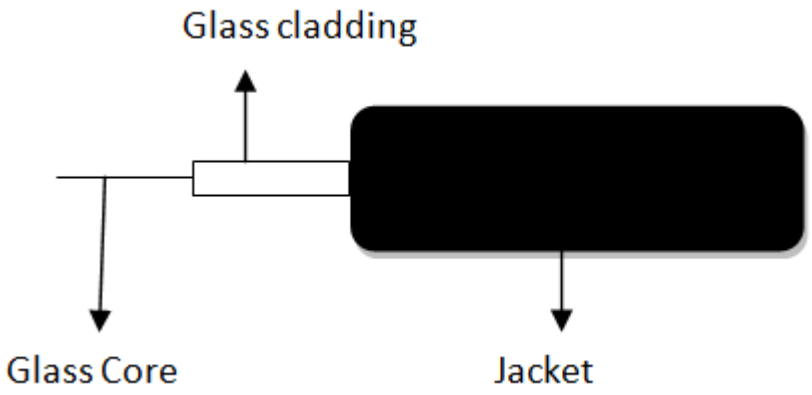
2. Difficult to install and expensive when compared with twisted pair.
3. If the shield is imperfect, it can lead to grounded loop.

**3) Fiber Optic Cable**

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**




Advantages :

1. Provides high quality transmission of signals at very high speed.
2. These are not affected by electromagnetic interference, so noise and distortion is very less.
3. Used for both analog and digital signals.

**Disadvantages :**

1. It is expensive
2. Difficult to install.

3. Maintenance is expensive and difficult.
4. Do not allow complete routing of light signals.

## UnBounded/UnGuided Transmission Media:

Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them. Types of unguided/ unbounded media are discussed below :

1. Radio Transmission
2. MicroWave Transmission

**1) Radio Transmission:**

Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications.

**Types of Propogation**

Radio Transmission utilizes different types of propogation :

1. **Troposphere :** The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet planes, wind is found here.
2. **Ionosphere :** The layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

**2) Microwave Transmission:**

It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

**Advantages of Microwave Transmission**

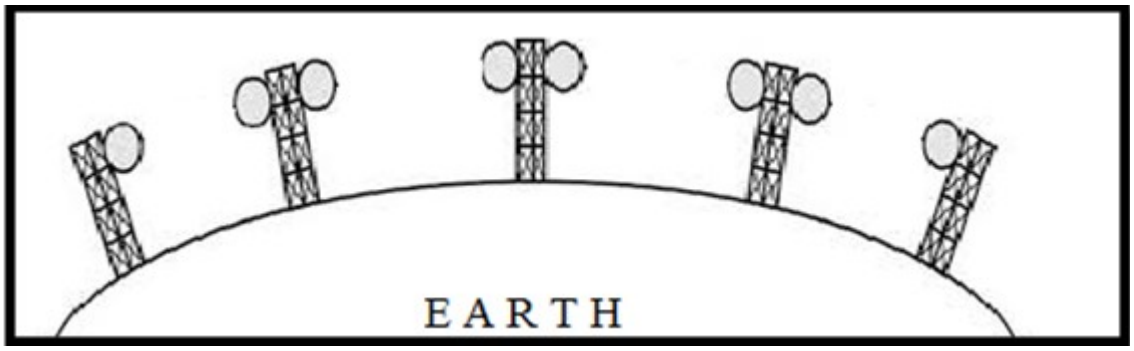
1. Used for long distance telephone communication
2. Carries 1000's of voice channels at the same time

**Disadvantages of Microwave Transmission**

1. It is Very costly

**3) Terrestrial Microwave:**

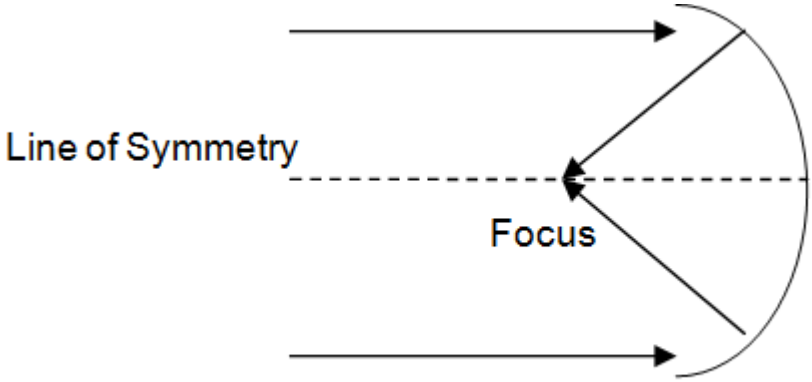
For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world




There are two types of antennas used for terrestrial microwave communication :

**1. Parabolic Dish Antenna**

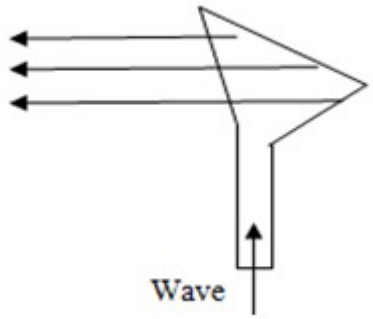
In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.




**2. Horn**

**Antenna**

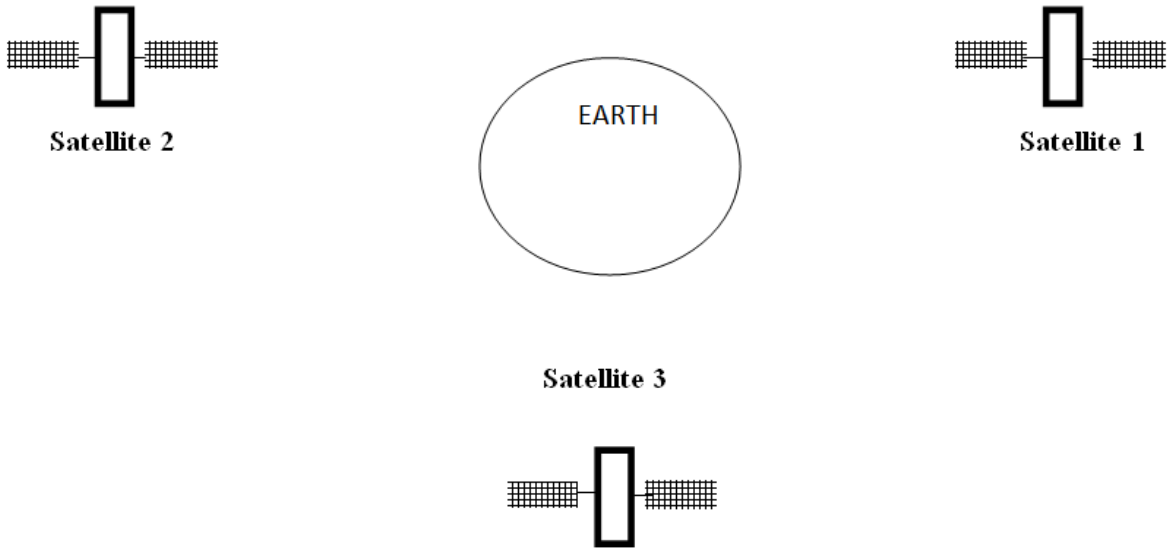
It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.




**4)Satellite Microwave:**

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 36000KM above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.




**Features of Satellite Microwave :**

1. Bandwidth capacity depends on the frequency used.
2. Satellite microwave deployment for orbiting satellite is difficult.

**Advantages of Satellite Microwave :**

1. Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
2. A single microwave relay station which is visible from any point.

**Disadvantages of Satellite Microwave :**

1. Satellite manufacturing cost is very high
2. Cost of launching satellite is very expensive
3. Transmission highly depends on whether conditions, it can go down in bad weather.

## Types of Networks

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

- Storage area network, or SAN
- Enterprise private network, or EPN
- Virtual private network, or VPN

Let's look at each of these in a bit more detail.

### Personal Area Network

A **personal area network**, or **PAN**, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

This type of network provides great flexibility. For example, it allows you to:

- Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.

- Upload a photo from your cell phone to your desktop computer.
- Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.


**PAN-Advantages**

- The pan is a personal network of one or two person so there is no risk of any leak of data.

**PAN-Disadvantages**

- The network it can only travel straight up to 10mts and if in different rooms then only 2mts.
- In the case of infrared the infra red sensor bust be in a straight line otherwise it won't communicate.
- Transmission speed is slow to moderate.

## Local Area Network

A **local area network**, or **LAN**, consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.

The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.

LANs are typically used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same office, but you would not want somebody just walking outside to be able to send a document to the printer from their cell phone! If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN.

**LAN Advantages**

Cost reductions through sharing of information and databases, resources and network services.

• Increased information exchange between different departments in an organization, or between individuals.

• The trend to automate communication and manufacturing process.

**LAN Disadvantages**

- Special security measures are needed to stop users from using programs and data that they should not have access to;

• Networks are difficult to set up and need to be maintained by skilled technicians.

• If the file server develops a serious fault, all the users are affected, rather than just one user in the case of a stand-alone machine.

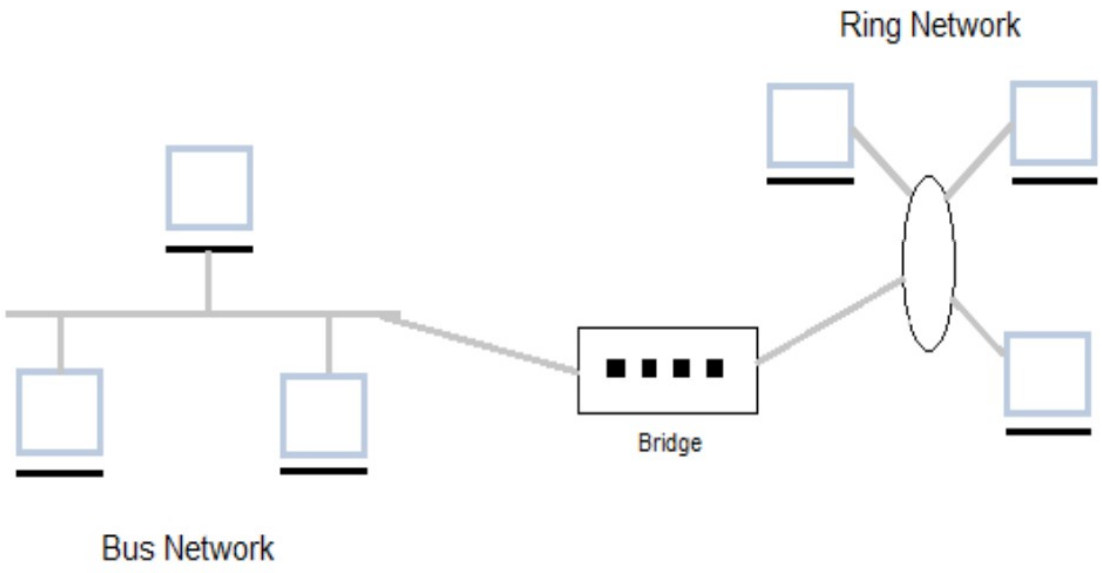
**Applications**

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.

- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.

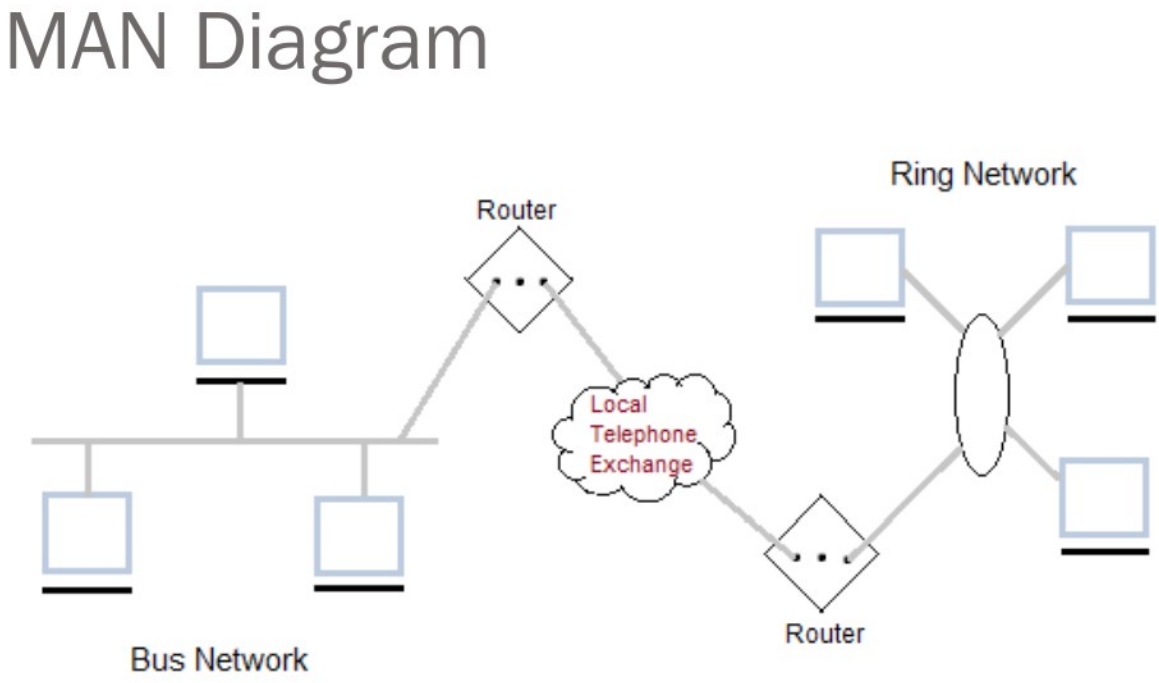
- Sharing common resources like printers etc are some common applications of LAN.

LAN Diagram



## Metropolitan Area Network

A **metropolitan area network**, or **MAN**, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.




**MAN-Advantages**

- It provides a good back bone for a large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both direction simultaneously.
- A Man usually encompasses several blocks of a city or an entire city.

**MAN-Disadvantages**

- More cable required for a MAN connection from one place to another.

- It is difficult to make the system secure from hackers and industrial espionage (spying) graphical regions.

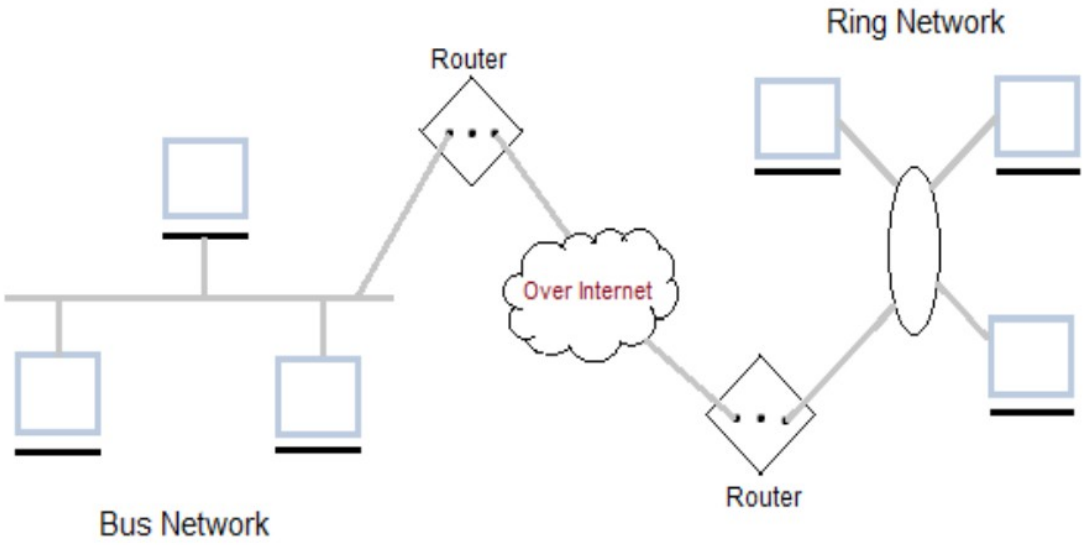
**MAN Applications**

- The MAN can be used to provide services including
- telecoms,
- Internet access,
- television and
- CCTV to businesses and citizens in these metropolitan areas.

## Wide Area Network

A **wide area network**, or **WAN**, occupies a very large area, such as an entire country or the entire world. A WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is the best-known example of a public WAN.

# WAN Diagram




**WAN Advantages**

•Covers a large geographical area so long distance businesses can connect on the one network.

•Shares software and resources with connecting workstations.

•Messages can be sent very quickly to anyone else on the network

•Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.

•Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

**WAN Disadvantages**

•Need a good firewall to restrict outsiders from entering and disrupting the network

•Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.

•Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.

•Security is a real issue when many different people have the ability to use information from other computers.

•Protection against hackers and viruses adds more complexity and expense.

## Network Devices:

### Hubs

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use **twisted pair cabling** to connect devices.

They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received.

They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

**Hub falls in two categories:**

**Active Hub:** They are smarter than the passive hubs. They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as '**repeaters'**.

**Passive Hub:** They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.


## Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive.

**Hub** works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it.

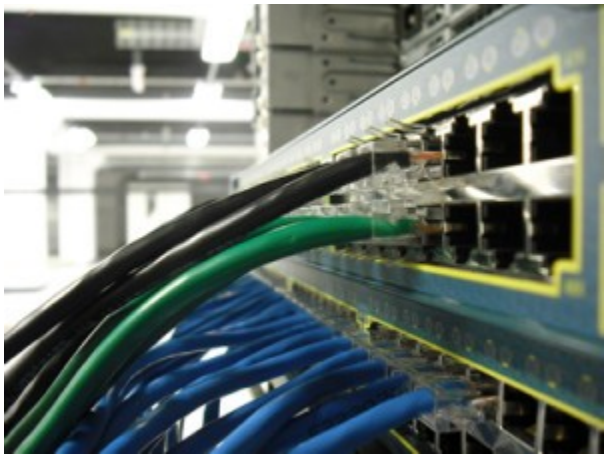
Since the transmission of data signals are well defined in a **switch** hence the network performance is consequently enhanced. Switches operate in **full-duplex** mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode.

The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps. Performance improvements are observed in networking with the extensive usage of switches in the modern days.

The following method will elucidate further how data transmission takes place via switches:

- **Cut-through transmission**: It allows the packets to be forwarded as soon as they are received. The method is prompt and quick but the possibility of error checking gets overlooked in such kind of packet data transmission.
- **Store and forward**: In this switching environment the entire packet are received and 'checked' before being forwarded ahead. The errors are thus eliminated before being propagated further. The downside of this process is that error checking takes relatively longer time consequently making it a bit slower in processing and delivering.

- **Fragment Free**: In a fragment free switching environment, a greater part of the packet is examined so that the switch can determine whether the packet has been caught up in a collision. After the collision status is determined, the packet is forwarded.



## Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them.

It connects two local-area networks; two physical LANs into larger logical LAN or two *segments* of the same LAN that use the same protocol.

Apart from building up larger networks, bridges are also used to segment larger networks into *smaller* portions.

The bridge does so by placing itself between the two portions of two physical networks and controlling the flow of the data between them. Bridges nominate to forward the data after inspecting into the MAC address of the devices connected to every segment.

The forwarding of the data is dependent on the acknowledgement of the fact that the destination address resides on some other interface. It has the capacity to block the incoming flow of data as well.

Today **Learning bridges** have been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network. This is a leap in the development field of manually recording of MAC addresses.

**Types of Bridges:**

There are mainly three types in which bridges can be characterized:

- **Transparent Bridge:** As the name signifies, it appears to be transparent for the other devices on the network. The other devices are ignorant of its existence. It only blocks or forwards the data as per the MAC address.
- **Source Route Bridge:** It derives its name from the fact that the path which packet takes through the network is implanted within the packet. It is mainly used in Token ring networks.
- **Translational Bridge:** The process of conversion takes place via Translational Bridge. It converts the data format of one networking to another. For instance Token ring to Ethernet and vice versa.

**Advantages of using a bridge**

– Extend physical network

– Reduce network traffic with minor segmentation

– Creates separate collision domains

– Reduce collisions

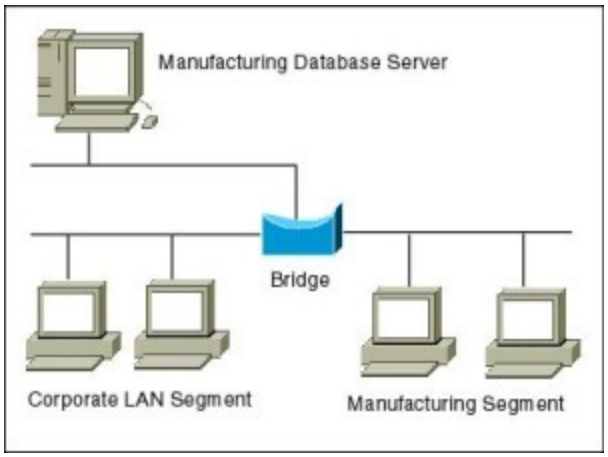
– Connect different architecture

**Disadvantages of using bridges**

– Slower that repeaters due to filtering

– Do not filter broadcasts

– More expensive than repeaters




## Routers

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process *logical* addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol.

It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.

**Functionality:**

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

**Routing tables** play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*. The two ways through which a router can receive information are:

- **Static Routing**: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.
- **Dynamic Routing**: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

**Advantages of Routers**

-provide sophisticated routing, flow control, and traffic isolation

-are configurable, which allows network manager to make policy based on routing decisions

-allow active loops so that redundant paths are available

**Disadvantages of Routers**

– are protocol-dependent devices that must understand the protocol they are forwarding.

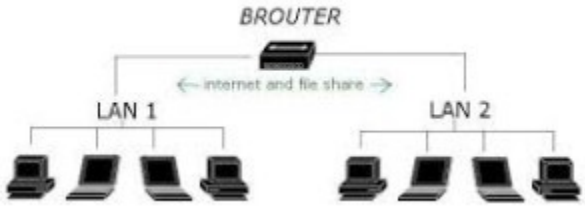
– can require a considerable amount of initial configuration.

– are relatively complex devices, and generally are more expensive than bridges.


## Brouters

Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a *bridge* when forwarding data between networks, and serving as a *router* when routing data to individual systems.

Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.




## Gateway

• Interchangeably used term router and gateway. Connect two networks above the network layer of OSI model.

Are capable of converting data frames and network protocols into the format needed by another network.

• Provide for translation services between different computer protocols.

• Transport gateways make a connection between two networks at the transport layer.

• Application gateways connect two parts of an application in the application layer, e.g., sending email between two machines using different mail formats • Broadband-modem-router is one e.g. of gateway.

**Access Point**

In computer networking, a wireless access point (WAP) is a networking hardware device that allows a Wi-Fi device to connect to a wired network. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

# Comparison of Hub and Switch

| Basis for Comparison | Hub | Switch |
|---|---|---|
| Layer | Physical layer. Layer 1 devices | Data Link Layer. Layer 2 |
| Function | To connect a network of personal computers together, they can be joined through a central hub. | Allow to connect multiple device and port can be manage, Vlan can create security also can apply |
| Data Transmission | Electrical signal or bits | Frame (L2 Switch) Frame & Packet (L3 switch) |
| Ports | 4/12 ports | Switch is multi port Bridge. 24/48 ports |
| Device Type | Passive Device (Without Software) | Active Device (With Software) & Networking device |
| Used in | LAN | LAN |
| Transmission Mode | Half duplex | Half/Full duplex |
| Broadcast Domain | Hub has one Broadcast Domain. | Switch has one broadcast domain |
| Definition | An electronic device that connects many network device together so that devices can exchange data | A network switch is a computer networking device that is used to connect many devices together on a computer network. A switch is considered more advanced than a hub because a switch will on send msg to device that needs or request it |
| Speed | 10Mbps | 10/100 Mbps, 1 Gbps |

# Comparison of Switch and Bridge

| Switch | Bridge |
|---|---|
| A switch when compared to bridge has multiple ports. | Bridge has a single incoming and outgoing port. |
| Switches can perform error checking before forwarding data. | A bridge maintains a MAC address table for both LAN segments it is connected to. |
| Switches are very efficient by not forwarding packets that error-ed out or forwarding good packets selectively to correct devices only. | Bridge filters traffic on the LAN by looking at the MAC address. |
| Switches can support both layer 2 (based on MAC Address) and layer 3 (Based on IP address) depending on the type of switch. | Bridge looks at the destination of the packet before forwarding unlike a hub. |
| Usually large networks use switches instead of hubs to connect computers within the same subnet. | It restricts transmission on other LAN segment if destination is not found. |
| | Bridges are used to separate parts of a network that do not need to communicate regularly, but need to be connected. |

# Routers versus Bridges

- Priority
  - » Routers can treat packets according to priorities
  - » Bridges treat all packets equally.
- Error Rate
  - » Network layers have error-checking algorithms that examines each received packet.
  - » The MAC layer provides a very low undetected bit error rate.
- Security
  - » Both bridges and routers provide the ability to put "security walls" around specific stations.
  - » Routers generally provide greater security than bridges because
    - – they can be addressed directly and
    - – they use additional data for implementing security.

## Manchester and Differential Manchester Encodings:

**Encoding**

1. Coding is the process of embedding clocks into a given data stream and producing a signal that can be transmitted over a selected medium.
2. Transmitter is responsible for "encoding" i.e. inserting clocks into data according to a selected coding scheme.
3. Receiver is responsible for "decoding" i.e. separating clocks and data from the incoming embedded stream.
4. A signal needs to be manipulated in such a way so that it contains identifiable changes that are recognizable to the sender and receiver.
5. There are 4 possible encoding techniques that can be used on the data: Digital-to-digital, Digital-to-Analog, Analog-to-analog, Analog-to-digital.

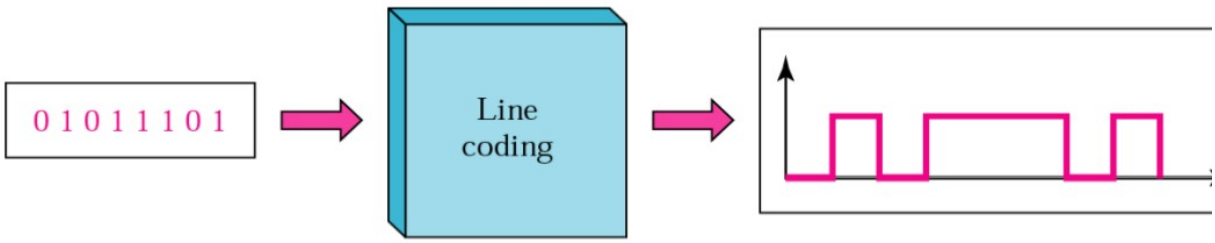
**Digital-to-Digital Encoding**

•The binary signals created by your computer (DTE) are translated into a sequence of voltage pulses that can be sent through the transmission medium.

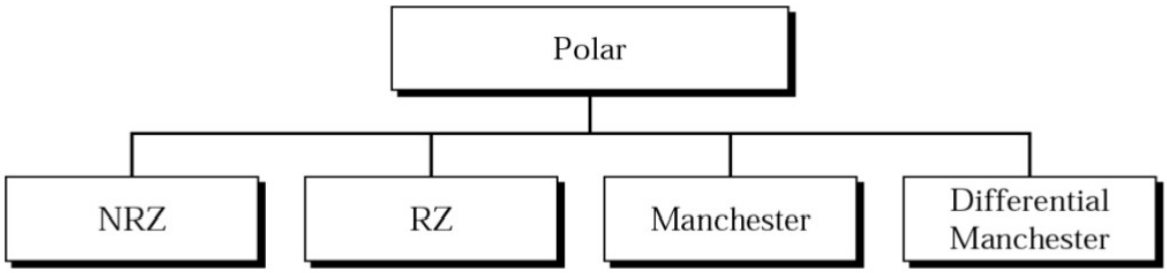
•Binary signals have two basic parameters: amplitude and duration.

•As the number of bits sent per unit of time increases, the bit duration decreases.

•The three most common methods of encoding used are: unipolar , polar , and bipolar.



# POLAR ENCODING

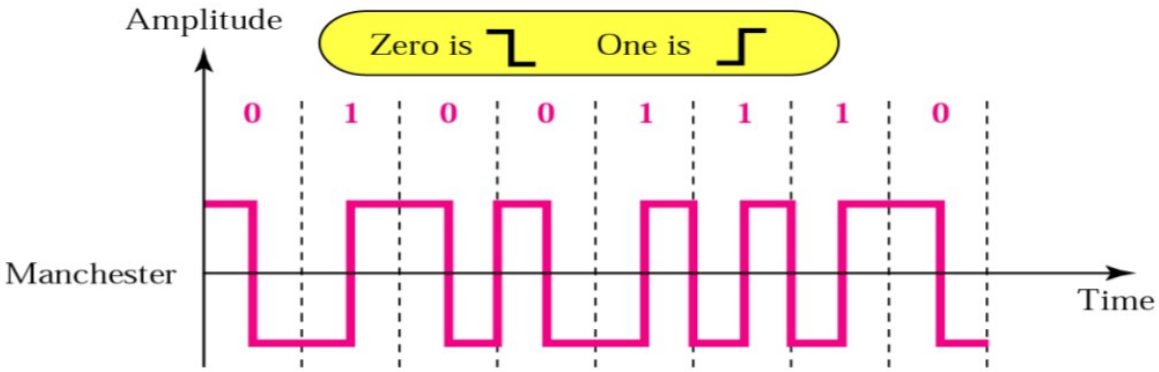



***Polar encoding uses two voltage levels (positive and negative).***

**Manchester (or diphase or biphase encoding)**

1. This code is self-clocking.
2. Provides a transition for every bit in the middle of the bit cell. This transition is used only to provide clocking.
3. +ve to -ve transition for a "0" bit
4. -ve to +ve transition for a "1" bit
5. Residual DC component is eliminated by having both polarities for every bit.
6. This scheme is used in Ethernet and IEEE 802.3 compliant LANs

# Manchester Encoding

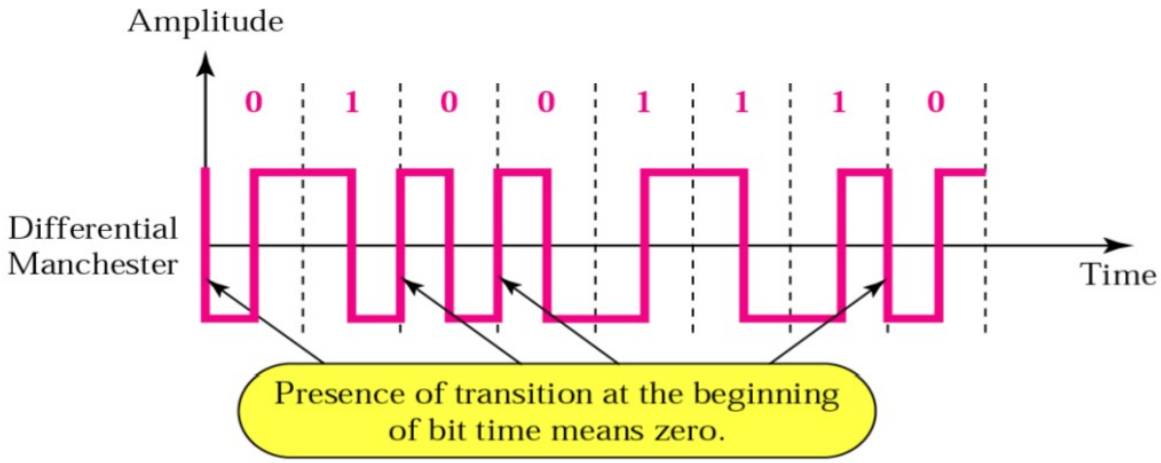



***In Manchester encoding, the transition at the middle of the bit is used for both synchronization and bit representation.***

**Differential Manchester Coding**

- Code is self-clocking
- Transition for every bit in the middle of the bit cell
- Transition at the beginning of the bit cell if the next bit is " 0 "
- NO Transition at the beginning of the bit cell if the next bit is " 1 "
- Used in Token Ring or IEEE 802.5-compliant LANs.

## Differential Manchester encoding




*In differential Manchester encoding, the transition at the middle of the bit is used only for synchronization. The bit representation is defined by the inversion or noninversion at the beginning of the bit.*

## IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS):

# IEEE 802 Standards

| Number | Topic |
|---|---|
| 802.1 | Overview and architecture of LANs |
| 802.2 ↓ | Logical link control |
| 802.3 * | Ethernet |
| 802.4 ↓ | Token bus (was briefly used in manufacturing plants) |
| 802.5 | Token ring (IBM's entry into the LAN world) |
| 802.6 ↓ | Dual queue dual bus (early metropolitan area network) |
| 802.7 ↓ | Technical advisory group on broadband technologies |
| 802.8 † | Technical advisory group on fiber optic technologies |
| 802.9 ↓ | Isochronous LANs (for real-time applications) |
| 802.10 ↓ | Virtual LANs and security |
| 802.11 * | Wireless LANs |
| 802.12 ↓ | Demand priority (Hewlett-Packard's AnyLAN) |
| 802.13 | Unlucky number. Nobody wanted it |
| 802.14 ↓ | Cable modems (defunct: an industry consortium got there first) |
| 802.15 * | Personal area networks (Bluetooth) |
| 802.16 * | Broadband wireless |
| 802.17 | Resilient packet ring |

**IEEE 802.11 Wireless LAN Standard**

1. IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11 in 1997
2. Scope of IEEE 802.11 is limited to Physical and Data Link Layers.

**IEEE 802.11 Standards**

- 802.11a (OFDM Waveform)
- 802.11b
- 802.11g
- 802.11n
- 802.11ac
- 802.11ad
- 802.11af
- 802.11ah
- 802.11ai
- 802.11aj
- 802.11aq
- 802.11ax

# Physical Media of 802.11 Standard

| | |
|---|---|
| Frequency-hopping spread spectrum | • Operating in 2.4 GHz ISM band<br>• Lower cost, power consumption<br>• Most tolerant to signal interference |
| Direct-sequence spread spectrum | • Operating in 2.4 GHz ISM band<br>• Supports higher data rates<br>• More range than FH or IR physical layers |
| Infrared | • Lowest cost<br>• Lowest range compared to spread spectrum<br>• Doesn't penetrate walls, so no eavesdropping |

**What is meant by Spread Spectrum?**

1. Spread spectrum is a form of wireless communications in which the frequency of the transmitted signal is varied . This results in a much greater bandwidth than the signal
2. This technique decreases the potential interference to other receivers while achieving privacy.
3. Two types of Spread Spectrum- FHSS and DSSS

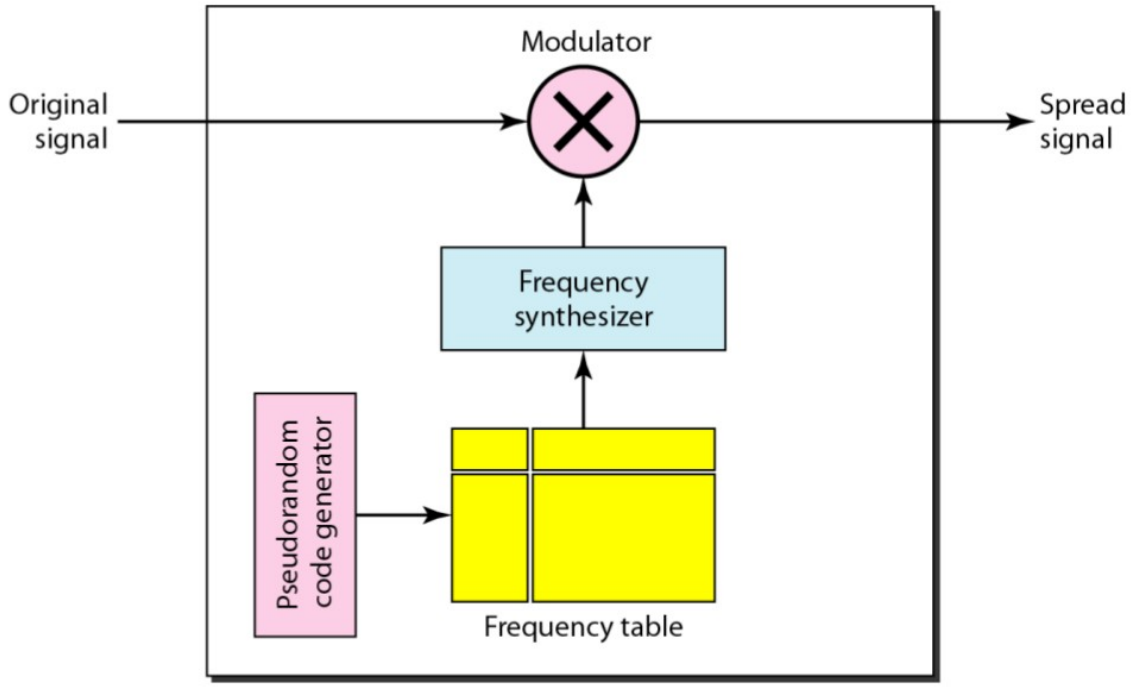
**Frequency Hopping Spread Spectrum (FHSS)**

- Signal is broadcast over seemingly random series of radio frequencies
- Signal hops from frequency to frequency at fixed intervals
- Receiver, hopping between frequencies in synchronization with transmitter, picks up message

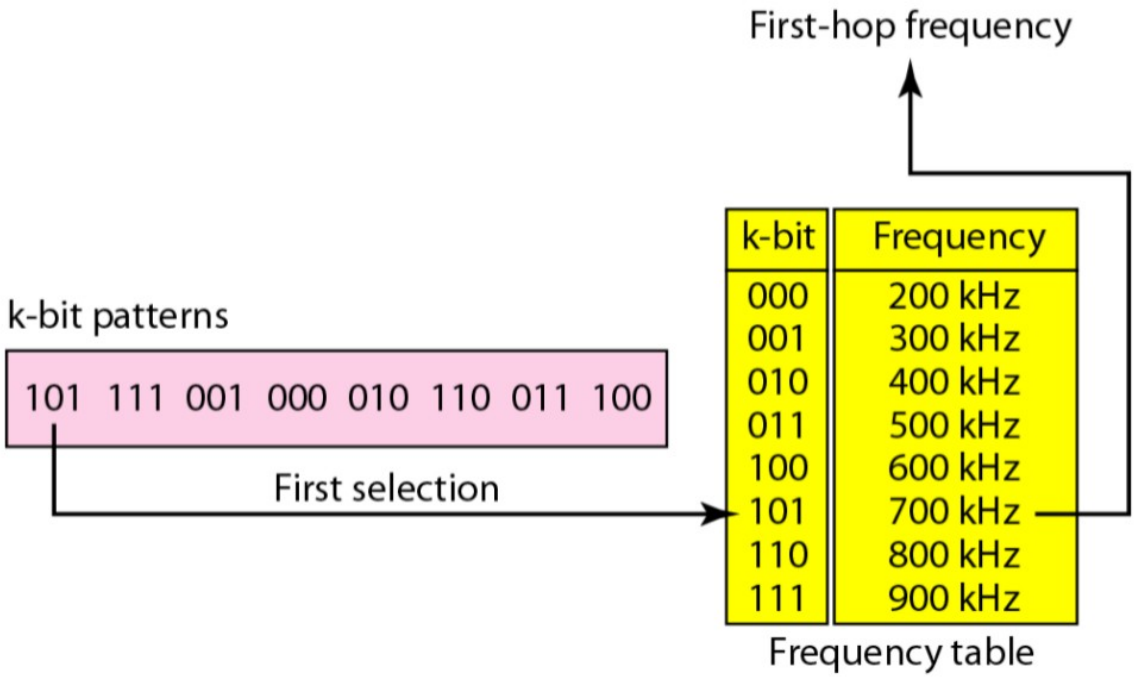
**Advantages**

1. Efficient utilization of available bandwidth
2. Eavesdropper hear only unintelligible blips
3. Attempts to jam signal on one frequency succeed only at knocking out a few bits

## Frequency hopping spread spectrum (FHSS)



## Frequency hopping spread spectrum (FHSS)



**Direct Sequence Spread Spectrum (DSSS)**

- Each bit in original signal is represented by multiple bits in the transmitted signal
- Spreading code spreads signal across a wider frequency band
- DSSS is the only physical layer specified for the 802.11b

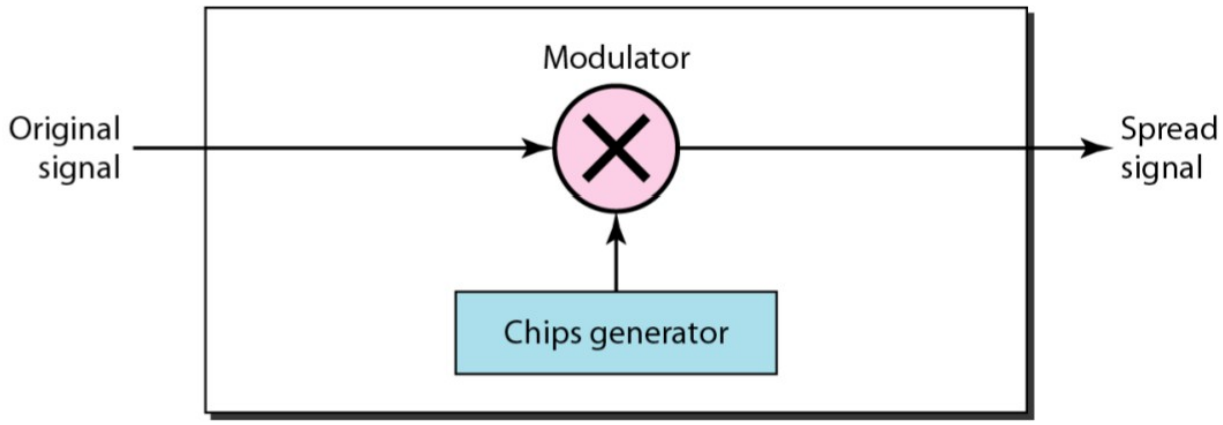
**specification**

802.11a and 802.11b differ in use of chipping method

802.11a uses 11-bit barker chip

802.11b uses 8-bit complimentary code keying (CCK) algorithm

## Direct Sequence Spread Spectrum (DSSS)



## FHSS Vs DSSS

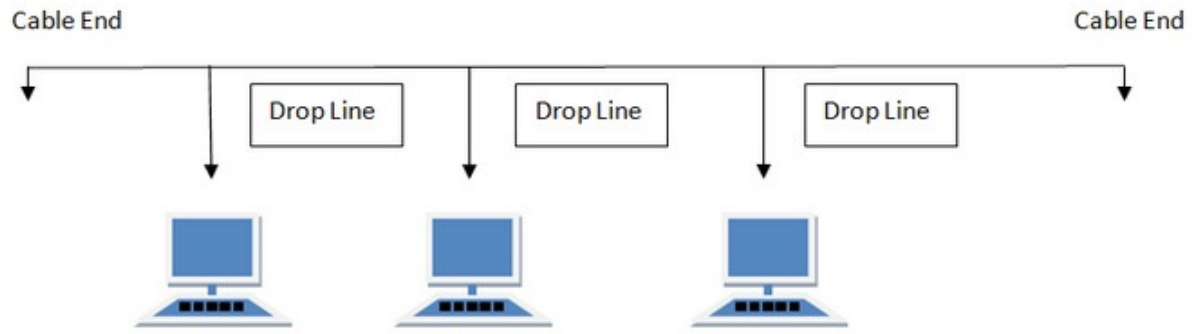
- FH systems use a radio carrier that "hops" from frequency to frequency in a pattern known to both transmitter and receiver
  - Easy to implement
  - Resistance to noise
  - Limited throughput (2-3 Mbps @ 2.4 GHz)
- DS systems use a carrier that remains fixed to a specific frequency band. The data signal is spread onto a much larger range of frequencies (at a much lower power level) using a specific encoding scheme.
  - Much higher throughput than FH (11 Mbps)
  - Better range
  - Less resistant to noise (made up for by redundancy – it transmits at least 10 fully redundant copies of the original signal at the same time)

## Types of Network Topology:

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

**BUS Topology:**

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.



**Features of Bus Topology**

7. It transmits data only in one direction.
8. Every device is connected to a single cable

**Advantages of Bus Topology**

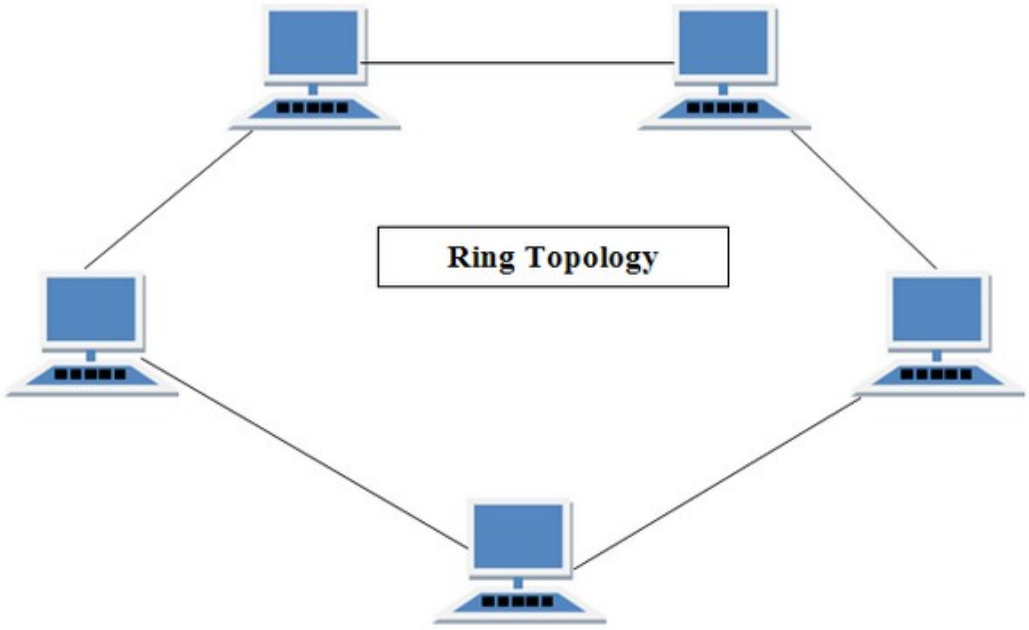
3. It is cost effective.
4. Cable required is least compared to other network topology.
5. Used in small networks.
6. It is easy to understand.
7. Easy to expand joining two cables together.

**Disadvantages of Bus Topology**

7. Cables fails then whole network fails.
8. If network traffic is heavy or nodes are more the performance of the network decreases.
9. Cable has a limited length.
10. It is slower than the ring topology.

**RING Topology**

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.




**Features of Ring Topology**

3. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
4. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
5. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
6. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

**Advantages of Ring Topology**

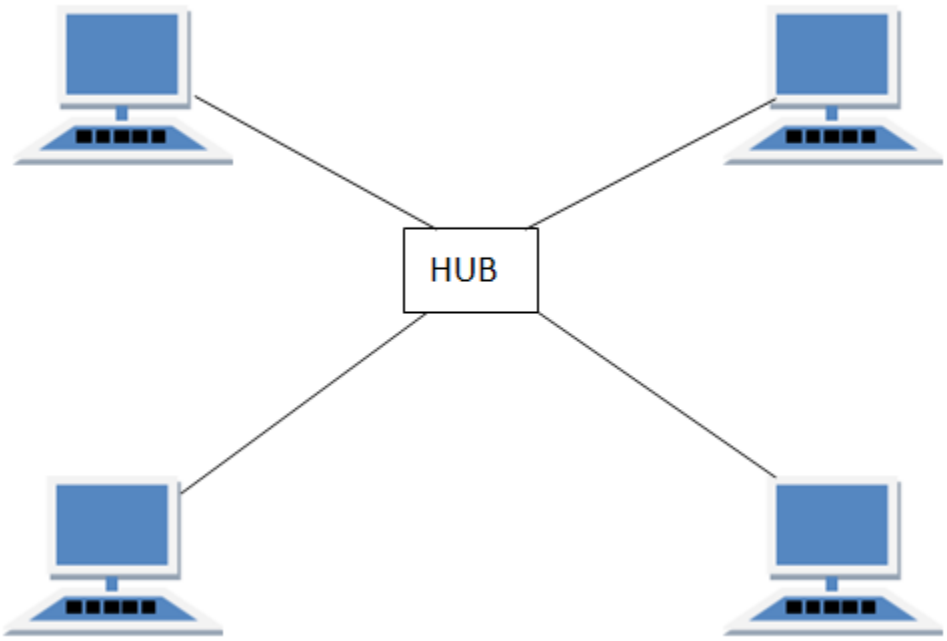
5. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
6. Cheap to install and expand

**Disadvantages of Ring Topology**

7. Troubleshooting is difficult in ring topology.
8. Adding or deleting the computers disturbs the network activity.
9. Failure of one computer disturbs the whole network.

**STAR Topology**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.




**Features of Star Topology**

4. Every node has its own dedicated connection to the hub.
5. Hub acts as a repeater for data flow.
6. Can be used with twisted pair, Optical Fibre or coaxial cable.

**Advantages of Star Topology**

4. Fast performance with few nodes and low network traffic.

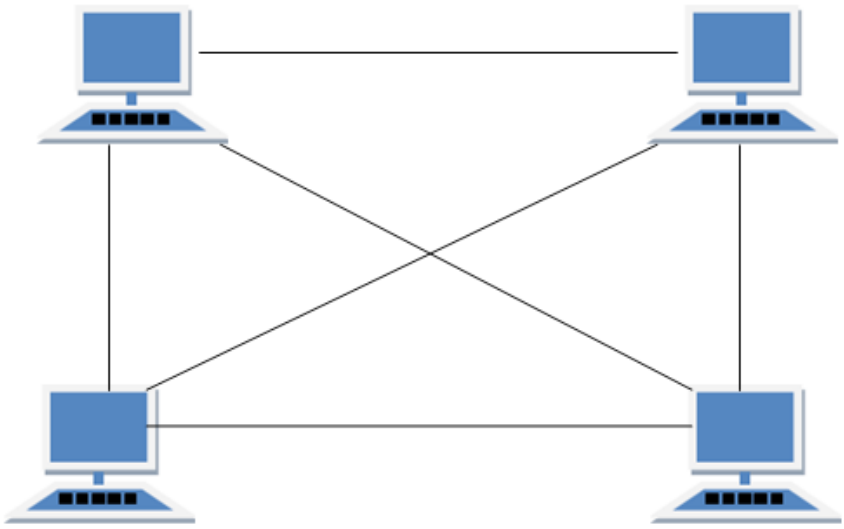
5. Hub can be upgraded easily.
6. Easy to troubleshoot.
7. Easy to setup and modify.
8. Only that node is affected which has failed, rest of the nodes can work smoothly.

**Disadvantages of Star Topology**

5. Cost of installation is high.
6. Expensive to use.
7. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
8. Performance is based on the hub that is it depends on its capacity

**MESH Topology**

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.



There are two techniques to transmit data over the Mesh topology, they are :

3. Routing
4. Flooding

**Routing**

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

**Flooding**

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

**Types of Mesh Topology**

3. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
4. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

**Features of Mesh Topology**

3. Fully connected.
4. Robust.
5. Not flexible.

**Advantages of Mesh Topology**

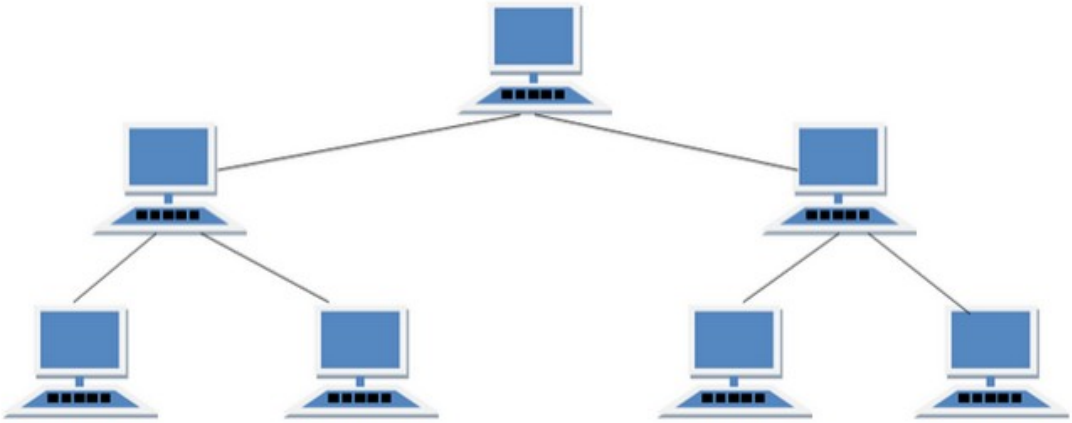
3. Each connection can carry its own data load.
4. It is robust.
5. Fault is diagnosed easily.
6. Provides security and privacy.

**Disadvantages of Mesh Topology**

2. Installation and configuration is difficult.
3. Cabling cost is more.
4. Bulk wiring is required.

**TREE Topology**

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



**Features of Tree Topology**

3. Ideal if workstations are located in groups.
4. Used in Wide Area Network.

**Advantages of Tree Topology**

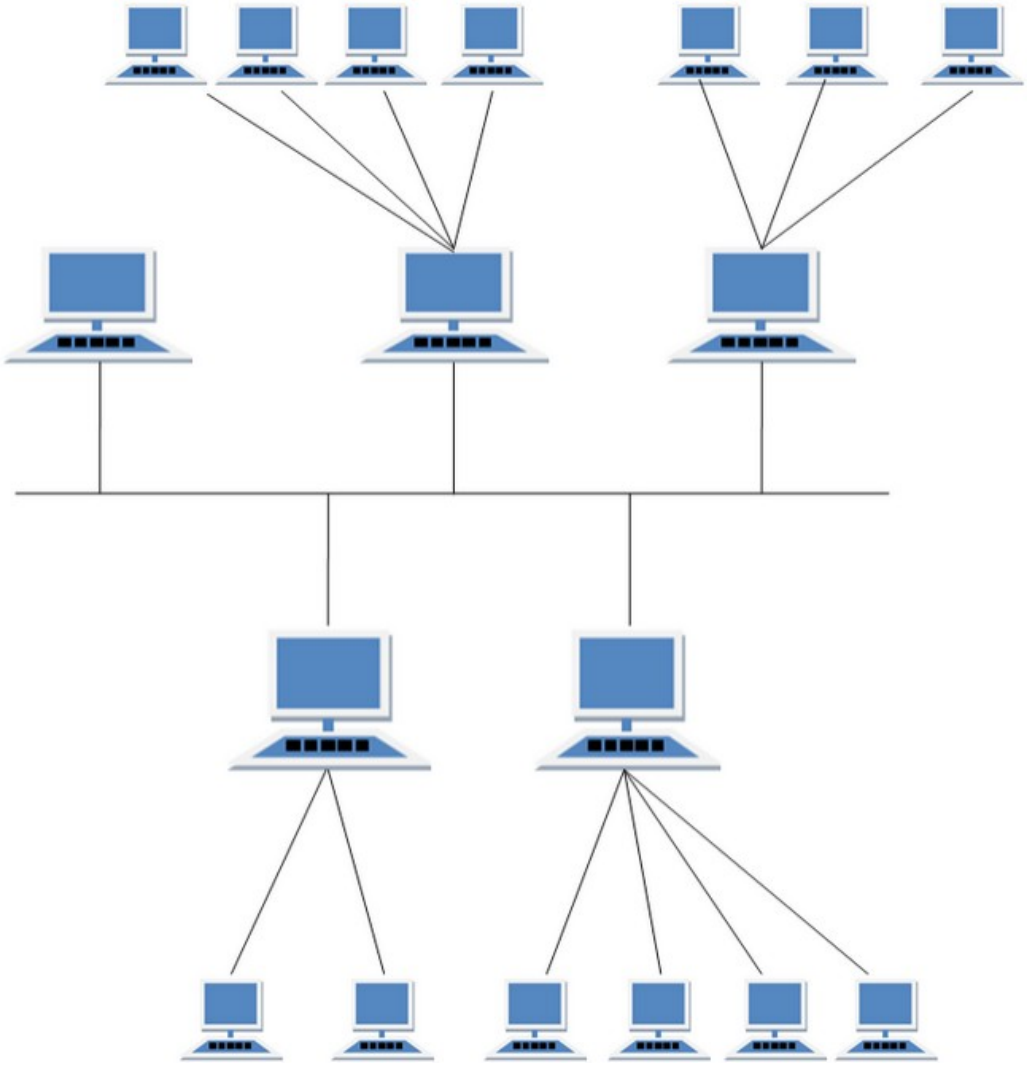
3. Extension of bus and star topologies.
4. Expansion of nodes is possible and easy.
5. Easily managed and maintained.
6. Error detection is easily done.

**Disadvantages of Tree Topology**

4. Heavily cabled.
5. Costly.
6. If more nodes are added maintenance is difficult.
7. Central hub fails, network fails.

**HYBRID Topology**

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



**Features of Hybrid Topology**

6. It is a combination of two or topologies
7. Inherits the advantages and disadvantages of the topologies included

**Advantages of Hybrid Topology**

6. Reliable as Error detecting and trouble shooting is easy.
7. Effective.
8. Scalable as size can be increased easily.
9. Flexible.

**Disadvantages of Hybrid Topology**

11. Complex in design.
12. Costly

Note: Material for this Notes are taken from Internet and books and only being used for student reference