# DATA COMMUNICATION AND NETWORKING

## DATA COMMUNICATION

*Data communication* refers to the process of transmitting data signal from one place to another through a communication media.

The basic components of a data transmission system are:

(a) A central computer.
(b) Terminal devices.
(c) Telecommunications link between the central computer & the terminal devices.

### Terms used in data communication

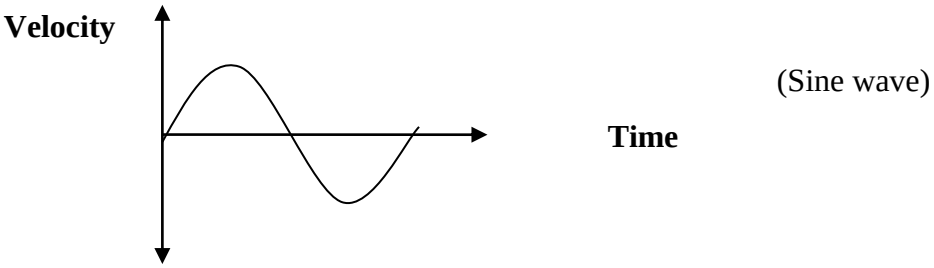
#### Data signal:

A data signal is a voltage level in the circuit which represents the flow of data.

In data communication, there are 2 types of data signals; *Digital* and *Analog*.

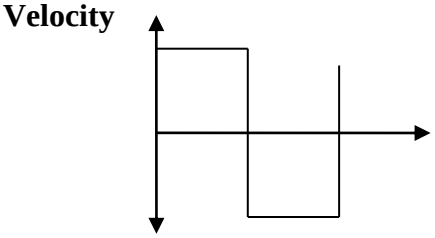
*Analog data* is made up of continuous waveforms, while *digital data* is made up of a non-continuous discrete waveform.

***Analog data signal***




(Sine wave)

***Digital data signal***




(Rectangular waved)

#### Signal modulation and demodulation:

This is the process of converting data signals to a form that can be transmitted over a transmission medium.

E.g., a modem converts a digital signal to an analog signal, which can be transmitted over analogue telephone lines. This process is called *modulation*. A modem at the receiving end converts the analogue signal into a digital signal, a process known as *demodulation*.

#### Multiplexing and Demultiplexing:

*Multiplexing* is the process of sending *multiple data signals* over the same medium, e.g., a wire conductor can be made to carry several data signals either simultaneously or at different times.

*Demultiplexing* is the process of separating the multiplexed signals at the receiving end.

Illustration:

Town A has 10 computers which want to communicate with 10 other computers in town B. In a normal case, it will need a direct cable linking each of the computers in town A to its partner in town B. However, if multiplexing is used, the computers can be made to share a single cable laid between the two towns, hence, saving cost.

The different data signals have different frequencies on the cable; hence, they do not interfere with one another.

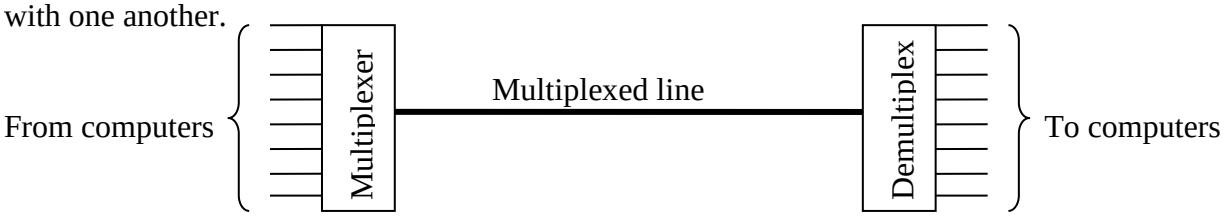



Fig.: A multiplexed link

**Frequency (f):**

Frequency of a wave is the number of cycles made by the wave in 1 second. Frequency is measured in units called ***Hertz*** (***Hz***); where 1 Hz is equivalent to 1 cycle/second.

**Baud:**

This is the unit to measure the speed of transmission. Generally, 1BAUD is 1bit/second.

**Baud rate:**

This is the rate at which data is transferred or transmitted. It is measured in Bits per second (bps).

**Band:**

The rate of change of a signal on a transmission line.

**Bandwidth:**

A *Bandwidth* is the maximum amount of data that a transmission medium can carry at any one time. E.g., a certain cable may have a bandwidth of 100 Mbps (Mega bits per second).

**Guardband:**

This is the range of frequency that is used to separate two channels.

**Baseband signal:**

This is a digital signal that is generated and applied to the transmission medium directly without modulation.

**Note**. A baseband signal utilizes the full capacity of the transmission medium; hence, at any one time, only one signal can be sent. However, multiple signals can be sent at different times, if they are multiplexed.

**Broadband transmission:**

This is where an analog signal is sent over the transmission medium using a particular frequency. This means that, several data signals can be sent at the same time through the same medium, but at different frequencies so as to prevent them from overlapping.

**Attenuation:**

*Attenuation* is the decrease in magnitude and energy of a signal as it progressively moves along a transmission medium.
If the signal is not boosted, it will totally be lost along the way, and may never reach the destination.

Attenuation (or signal loss) is usually corrected by placing signal amplifiers (also called ***repeater stations***) along the medium at appropriate distances in order to receive the weak signal, clean it, amplify it, then retransmit it.

## Modes of data communication

There are 3 modes of data communication:

**(a).** Simplex.
**(b).** Half duplex.
**(c).** Full duplex.

### Simplex transmission:

This is where communication is only in one direction (as in radio or television broadcast). The listener or viewer cannot communicate back through the radio or television receiver back to the broadcaster.

### Half duplex transmission:

This refers to communication in both directions, but one direction at a time.
A sender must first send the data before the recipient can reply, e.g., if two police officers are communicating using a 'walkie talkie' radio, one has to say "*over*" to mark the end of every statement in order for the other to respond.

### Full duplex transmission:

This is where communication occurs in both directions simultaneously (as in computers that are sending & receiving data on a network).

### Factors to consider when selecting a data transmission system

1. Cost of each type of data transmission method.
2. Distance between the computer & the terminal.
3. Whether data should be transmitted direct to the computer online.
4. Type of data transmission system to be used, i.e., whether the data transmission will be 1-way or 2-way.
5. Volume of data to be processed; and whether it is batched at particular times, or whether it is collected individually and required to be processed immediately.
6. Speed of transmission required.
   In many cases, it is acceptable to use the ordinary Postal service, Kenyan rail, or a private Courier service.
7. Accuracy and reliability required.

## Data communication (Transmission) media.

A ***data communication medium*** is a physical pathway used for carrying data signals & information from one point to another.

Data communication media can be divided into two:

**(a).** Communication using cable (bound media).
**(b).** Wireless communication (unbounded media).

### Communication using cables (bounded media).

In bounded media, data signals are transmitted from the source to the destination through a cable.

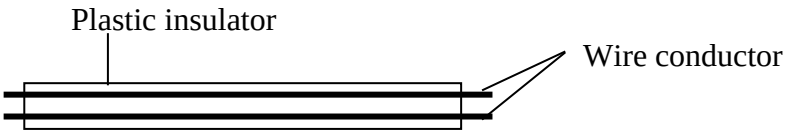
There are 4 major types of bounded transmission media, namely:

**1.** Two-wire open lines cables.

**2.** Twisted pair cables.
**3.** Coaxial cables.
**4.** Fibre optic cables.

### Two-wire open lines cables.

Two-wire open lines cables are made up of 2 parallel copper wires separated by a plastic insulator.




The *Plastic insulator* is meant to reduce signal interference called **Crosstalk**. However, the linear nature of the wires allows an electromagnetic field to build around them during heavy data transmission, which may cause interference to the signal.

The wires also capture/pick unwanted environmental frequencies, e.g., radio waves, hence causing ***noise*** in the transmission channel.

Two-wire open lines cables are used in telecommunication network to transmit voice (analogue) signals.

### Twisted pair cables.

A twisted pair cable is made up of 2 insulated copper wires twisted around each other in a spiral pattern.

The twisting prevents electromagnetic fields from developing around the two wires as they transmit data.

Twisted pair cables can be used to transmit both voice & data signals (i.e., analogue & digital signals).

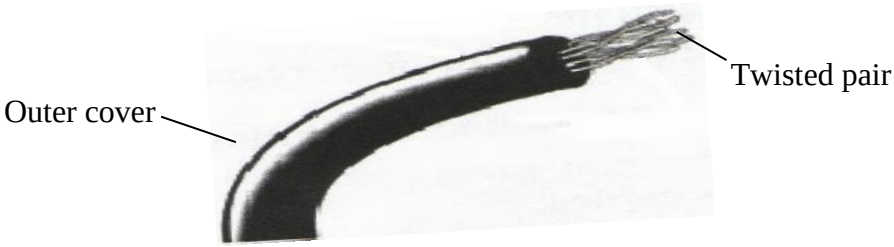
#### *Types of twisted pair cables.*

The 2 common types of twisted pair cables are:

**(i).** Unshielded twisted pair (UTP).
**(ii).** Shielded twisted pair (STP).

#### Unshielded twisted pair (UTP) cables.

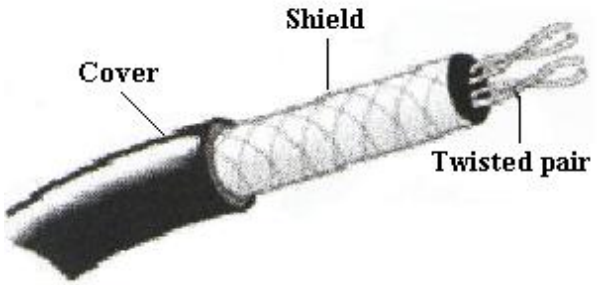
UTP cables do not have a shield that prevents electromagnetic interference (also called '***Electric noise***') from the environment.




UTP cable is prone to noise & signal interference, and therefore, not suitable for environments that are electrically 'noisy'.
Noise may come from lightening sparks, radio signal, or radiations from spark plugs in motor vehicles.

**Shielded twisted pair (STP) cables.**

In STP cables, a braided shield is wrapped around the wires to protect them from noise.




Twisted pair cables are grouped into 5 categories according to the type of data transmitted, and the maximum rate of transmission.

| Category | Speed (max. limit) | Suitable for transmitting |
|---|---|---|
| 1 | Less than 1 Mbps (i.e., Megabits per second) | Voice |
| 2 | 1 Mbps | Data |
| 3 | 16 Mbps | Data |
| 4 | 20 Mbps | Data |
| 5 | 100 Mbps | Data |

**Advantages of Twisted pair cables.**

1. Can support high data rates (bandwidth) of up to 100 Mbps.
2. Telephone systems use UTP, which is present in most buildings. Therefore, it is easier to setup network media because; connection is readily available.
3. Installation equipment is cheap & readily available.
4. It is cheap because; of mass production for telephone use.

**Disadvantages of Twisted pair cables.**

1. They suffer from high attenuation. Therefore, for every cable length of 90m, a "**Repeater**" is needed to amplify (restore) the signal.
2. It is sensitive to electromagnetic interference & eavesdropping.
3. It has low data transmission rates as compared to other cables.

## Coaxial cables.

A Coaxial cable resembles the cable that is used to connect television antenna to a television set.

The cable has;

**1.** A central *copper core* (which is either solid or stranded wires).

The diameter of the centre core determines the attenuation rate. If the core is thin, then the attenuation rate will be higher.

**2.** An *insulator* (a dielectric material) surrounding the copper core.

**3.** A hollow *braid* (mesh conductor) surrounding the insulator. The braid is made of copper or aluminium, and serves as the ground for the carrier wire.

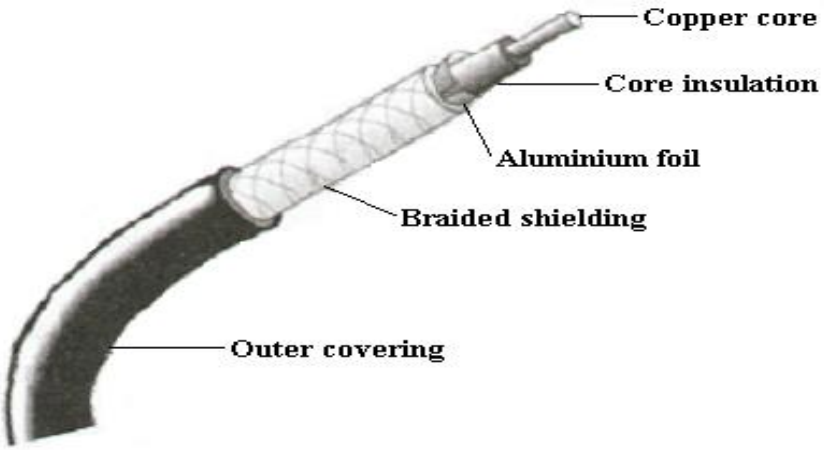
**4.** A *shield* which covers the braid making the core more resistant to electromagnetic interference.

The braid together with the insulator & the foil shield protects the carrier wire from Radio Frequency Interference (RFI) and Electromagnetic Interference (EMI).

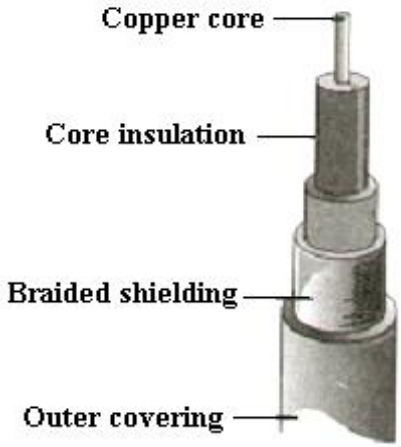
Coaxial cables have bandwidths of up to *1 Gbps* (Gigabits per second). Hence, they can be used to link/connect different networks between buildings, and route trunk calls in telecommunication companies.

***The Two types of coaxial cables.***

**(i).** *Thin coaxial cable (Thinnet)*: - it has 1 dielectric insulator around the core.




**(ii).** *Thick coaxial cable (Thicknet)*: - it has 2 dielectric insulators around the core, and is thicker than the thinnet.




**Advantages of coaxial cables.**

1. They are very stable even under high loads.
2. They have a large bandwidth (up to 1Gbps) compared to twisted pair cables.
3. They can carry voice, data and video signals simultaneously.
4. They are more resistant to radio and electromagnetic interference than twisted pair cables.

**Disadvantages of coaxial cables.**

1. Thick coaxial cable is hard to work with.
2. They are relatively expensive to buy & install compared to twisted pair cables.

## Fibre optic cables.

A fibre optic cable uses light to transmit data signals from one point to another on the network.

A ***Light Emitting Diode*** (***LED***) is used at the source/transmitter (sending computer) to convert electrical signals to light signals which are then send along the cable. At the receiving computer, a ***photosensitive*** device is then used to convert the light signals back to electric signals that can be processed by the computer.

A fibre optic cable is made up of;

1. **The Core**.
   This is the central part of the cable, and is made of a hollow transparent plastic or glass.
2. **Cladding**.
   This is a single protective layer surrounding the core.

The Cladding is able to bend light rays, (i.e., when light tries to travel from the core to the cladding, it is redirected back to the core).

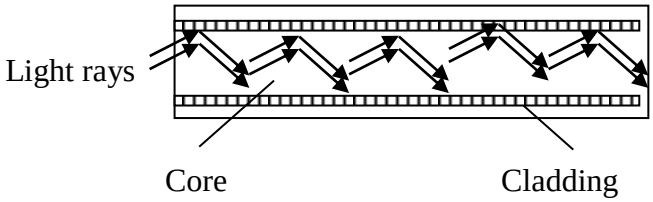
3. **Buffer**.
   It surrounds the cladding. Its main function is to strengthen the cable.
4. **The Jacket**.
   It is the outer covering of the cable.

**Light transmission along a fibre optic cable.**

The light signal travels along the core through a process referred to as ***Total internal reflection***.

The process that causes total internal reflection is called **Refraction**. *Refraction* is the bending of light when it crosses the boundary of two mediums that have different densities.

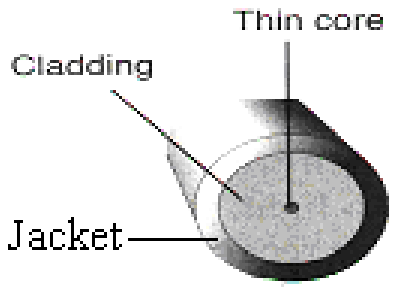
Therefore, when light signal is inserted into the cable, it tries to cross from the core to the cladding. The light is bent back into the core, hence spreads along the length of the cable.




***Types of fibre optic cables.***

**(i). Single mode fibre optic cable**.

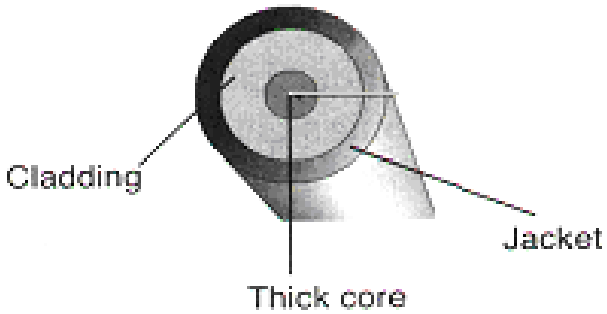
The single mode fibre has a very narrow centre core. This implies that, the light in the cable can take only one path through it.




- It has a very low attenuation rate, and is preferred for long distance transmission.
- It has a very high bandwidth of 50 Gigabits per second.
- It is very expensive, and requires very careful handling during installation.

**(ii). Multimode fibre optic cable.**

A multimode fibre has a thicker centre core than the single mode fibre.




- It allows several light signals (rays) to be sent through the cable at the same time. Hence, there are high chances of the signal being distorted.

- It has a high attenuation rate, and is usually used for shorter distance transmission.

**Advantages of fibre optic cable.**

1. It is immune to electromagnetic interference, and eavesdropping.
2. It is fast and supports high bandwidth.
3. It has low attenuation; hence, a long distance can be covered.
4. It does not generate electrical signals; hence can be used in dangerous (highly flammable) places.
5. It is smaller & lighter than copper cables; hence, suitable for situations where space is limited.

**Disadvantages of fibre optic cable.**

1. Requires expensive connectivity devices and media.
2. Installation is difficult because the cable must be handled carefully.
3. It is relatively complex to configure.
4. A broken fibre optic cable is difficult & expensive to repair.

## Review questions.

**1.** Define the term Transmission media.
**2.** **(a).** Give two advantages of coaxial cables.
**(b).** Explain the importance of the wire braid in coaxial cable.
**3.** Distinguish between Thinnet and Thicknet coaxial cables.
**4.** Define the term Pitch as used in twisted pair cabling.
**5.** **(a).** Give two advantages of fibre optic media.
**(b).** Differentiate between single mode and multimode fibre optic cables.

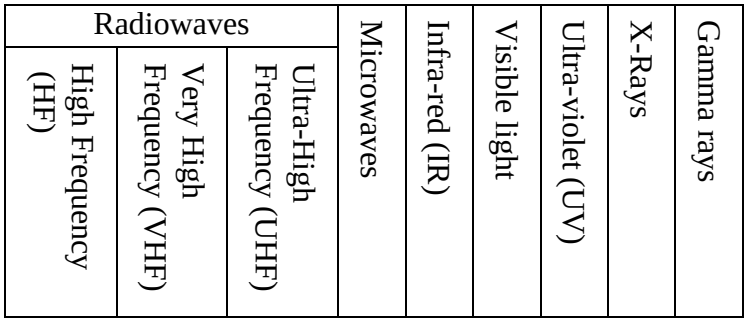
## Wireless communication (unbounded media)

*Wireless* (*unbounded*) *media* is a type of media that is used to transmit data from one point to another *without using physical connections*.
In this case, a transmitting *antenna* & a receiver *aerial* are used to facilitate the communication.

Examples of wireless communication media include:

**1.** Microwaves.
**2.** Radiowaves.
**3.** Infrared transmission.
All these waves use different frequencies of the electromagnetic spectrum, and travel at the speed of light.

Below is a diagrammatic representation of the electromagnetic spectrum

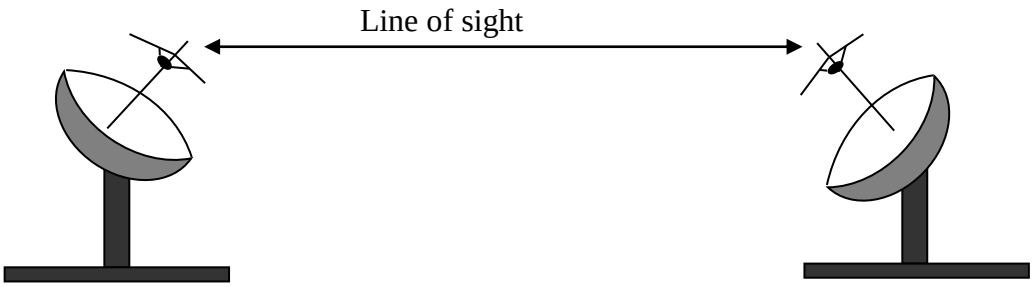


| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $10^6$ Hz | $10^7$ Hz | $10^8$ Hz | $10^{10}$ Hz | $10^{13}$ Hz | $10^{15}$ Hz | $10^{16}$ Hz | $10^{20}$ Hz | $10^{22}$ Hz |

## Microwave transmission

Microwave frequencies have a small wavelength, and can easily release their energy in water as heat. This is why they are used in making domestic kitchen appliances, e.g., microwave ovens.

In networking, microwaves are suitable for *point-to-point* transmissions, whereby a signal is directed through a focused beam from the transmitter to the receiver station.

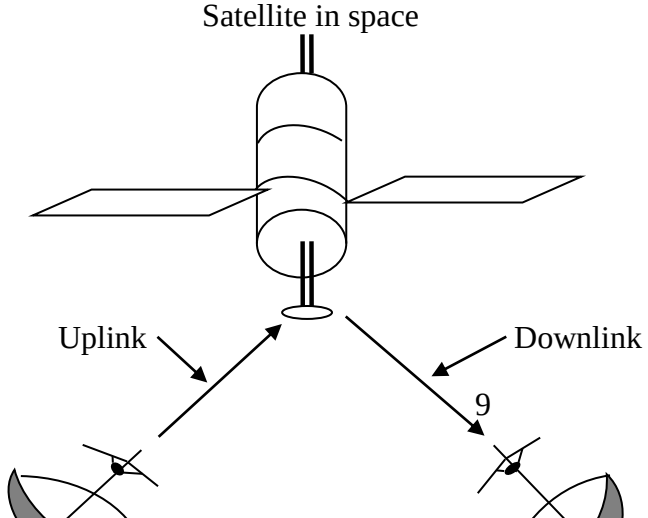



## Satellite communication

A Satellite is a microwave relay station. The microwave earth stations have parabolic dishes with an antenna fixed on them in order to focus a narrow beam towards the satellite in space.

A satellite transmission system has 3 main components:

1. ***Transmitter earth station*** - it sets up an *uplink* to the satellite in order to transmit data.
2. A ***Satellite*** that is somewhere in an orbit. It receives, amplifies, and retransmits the signal to a receiving earth station through a *downlink* frequency.
   The downlink & the uplink frequency are usually different. This is to prevent the downlink signal from interfering with the uplink signal.
3. ***Receiving earth station*** - receives the signal sent by the satellite on the other side of the globe.



Transmitter earth station

Receiving earth station

A communication satellite is usually launched into space about 36,000 km above the earth in such a manner that its speed is almost equal to the rotation speed of the earth. This makes the satellite appear as if it is stationary in space. Such types of satellites are called ***geostationary*** satellites.

**Advantages of using satellites**

1. A satellite is convenient because; it provides a large constant line of sight to earth stations. This means that, there is no need to keep on moving the parabolic dish so as to track the line of sight.
2. The satellite transmits the signal to many recipient earth stations. This is because; the transmitted signal spreads out in all directions to form a *Point to Multipoint* transmission.

**Very Small Aperture Terminal (VSAT)**

A *VSAT* is a very small satellite dish used both in data, radio, and TV communication.

It can be set up at home or in a small business. It enables direct access to satellite communication instead of having to go through state-owned or licensed satellite gateways.

The dish has an antenna that receives the satellite signals. The signals are decoded using a *decoder* which is plugged directly to a television set or a computer.

**Radio communication**

Radio waves are used in radio and television broadcasts.

Radio waves travel just like surface water waves, i.e., they start from a central point and spread outwards in all directions.
As they travel outwards, their energy spreads outwards over the covered area. The waves are radiated into the atmosphere by a radio frequency antenna at constant velocity.

The figure below shows a typical radio waves link between two separate geographical locations.

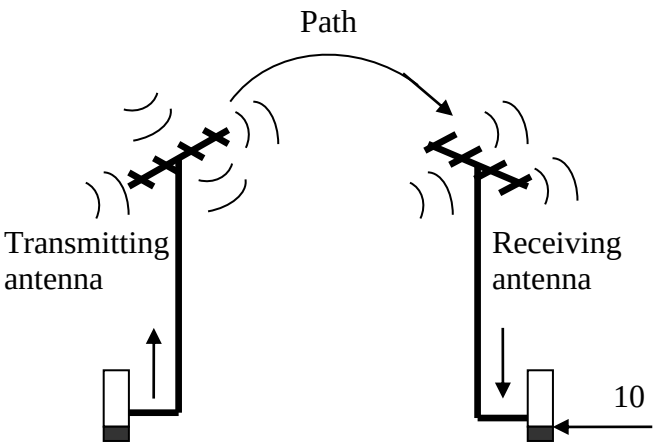



Fig.: A typical radio transmitter and receiver link

Radio waves can be of:

- High frequency (HF).
- Very high frequency (VHF).
- Ultra-high frequency (UHF).

**High frequency (HF) radio waves**

The *High frequency* radio wave signal is transmitted by directing it to the *ionosphere* of the earth. The ionosphere reflects it back to the earth's surface, and the receiver then picks the signal.

*Disadvantage of HF communication*

– The signal can be intercepted by unauthorized parties.

**Very High frequency (VHF) radio waves**

They are transmitted along the earth's surface. However, since the earth is somehow curved, the signal tends to attenuate at the horizons of mountains and buildings. This means that, *repeater stations* have to be built on raised areas in order to receive, amplify, and propagate the signal from one area to another.

**Note**. The range of VHF is limited, however, it is preferred to HF because; it is possible to make a VHF wave follow a narrower & more direct path to the receiver.

**Ultra-High frequency (UHF) radio waves**

The UHF radiowaves use the *line of sight principle* used by the VHF waves. This means that, there should be no barrier between the sending & the receiving aerial. However, they require smaller aerials.

*For example;*

The Television aerial for VHF is bigger than the one for UHF radio waves. This is because; UHF radio waves can be made to follow a narrower & a more direct path to the receiver than VHF radio waves.

## *The Bluetooth technology*

This is a worldwide and short range radio transmission technology that allows all personal, hand-held devices to be able to communicate with each other through wireless technology.

It enables people to use hand-held communication devices such as mobile phones & Personal Digital Assistants (PDA's) to access the Internet.

The main component in Bluetooth is a small *low power* two-way radio transceiver, which can be inserted in small devices.

Bluetooth enabled devices use a network called the *Wireless personal area network* (*WPAN*) or *piconet*.

## Infrared transmission

Communication through infrared waves (signals) is achieved by having infrared transmitters & receivers (*transceivers*) within a line of sight in the same room. This is because; infrared signals cannot penetrate obstacles like walls and ceilings. However, the signal can be reflected off these surfaces until they reach their destination.

*For example;*

Most mobile phones have an infrared transceiver. Once activated, two people in the same room can send messages to each other on their mobile phones without going through the mobile service provider; hence avoid being charged.

In computer networking environment, infrared technology can be used to connect devices in the same room to each other without the need for cables, e.g., a computer and a printer. However, the computer's infrared transceiver must maintain a line of sight with the one for the printer.

**Advantages of wireless communication.**

1. Wireless medium is flexible in operation, i.e., devices can be moved around without losing access to the network.
2. Wireless networks can span large geographical areas easily.
3. Wireless communication can take place via satellite even in very remote areas that do not have high cost physical infrastructure like telephone lines.

**Disadvantages of wireless communication.**

1. The initial cost is very high.
2. It is relatively difficult to establish or configure.

## Review questions.

**1.** Distinguish between radio and microwave transmission.
**2.** Describe an electromagnetic spectrum.
**3.** State two advantages of satellite communication.
**4.** Give one application area of Infrared transmission.
**5.** Describe the VSAT technology.
**6.** Explain the concept of a geostationary satellite.
**7.** Explain the *line of sight principle* in wireless communication.

## Communication devices

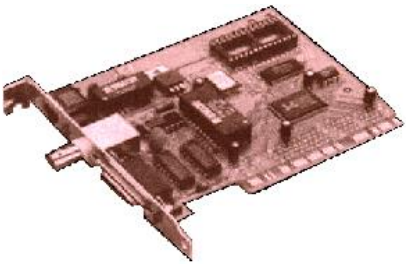
For a network to be fully operational, communication devices are required, and act as interfaces between the **Terminal devices**.
*Terminal equipments* are the devices at both ends of the communication link, e.g., computers.

Some of the data communication devices are:

### 1. Network Interface cards (NIC)

A NIC acts as a physical connection (link/interface) between the computer & a properly terminated transmission cable.

A NIC is plugged into an empty expansion slot on the motherboard, and has ports at the back in which the terminated end of a network cable can be plugged.



### 2. A Modem and a Codec

A *Modem* converts a digital signal to analogue form so that it can be transmitted over an analogue media.

A *Codec* converts an analogue signal to digital form so that it can be transmitted over a digital medium.

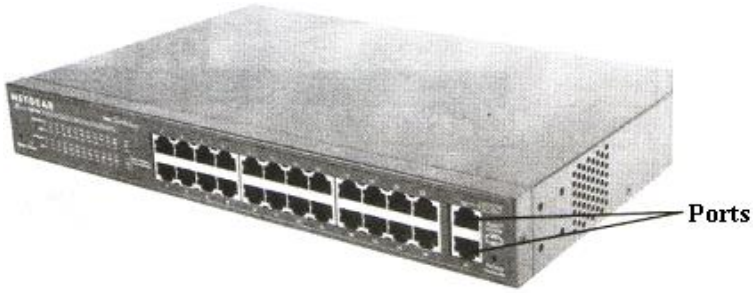
A modem can be *external*, an *add-on card* or built on the motherboard.


Fig.: An external modem

## 3. Hub (Concentrator)

A *Hub* is a component that connects computers on a network, and is able to relay signals from one computer to another on the same network.

A Hub usually connects networks that have the same set of communication software usually called *Protocols*.




A Hub transmits signals by broadcasting them to all the computers on the network. After the signal is broadcasted, the computer whose address is on the message then picks the message from the network.

Several hubs can be connected together one after another to expand a network.

**Intelligent hubs**

*Intelligent hubs* are able to monitor the way computers are communicating on the network, and keep the information in their own database called *management information base (MIB)*. The network server can then use this information to fine-tune the network.

- Intelligent hubs also manage a network by isolating computers that are not functioning properly.

## 4. Bridges

This is a network device that selectively determines the appropriate network segment for which a message is meant to be delivered. It does this through address filtering.

***Purpose of using a Bridge***

a). It can divide a busy network into segments to reduce network traffic.
b). To extend the length & number of workstations that a segment can support.
c). To reduce overall traffic flow by allowing broadcasts only in the destination segment of the network.
The bridge makes sure that packets that are not meant for a particular segment are not broadcast in that segment.

## 5. Repeater

A *Repeater* receives a signal from one segment of a network, cleans it to remove any distortion, boosts it, and then sends it to another segment.
It therefore, enables the network to eliminate attenuation problems.

**Note**. Repeaters can easily be used to expand a network. This is because; they broadcast the same message to other network segments.

## 6. Routers

A *Router* connects different networks, and directs the transfer of data packets from source to destination.

**Note**. Routing depends on network addresses. Each network has a unique address (or identifier) called the ***IP address***.

The router will receive a packet of data from another router on the network, and check the network address of the destination. If the address is the same as the one on which the router is, the router will then read the address of the host and then pass the data packet to the destination, otherwise the packet will be routed to the next network address.

**NB**: Network addressing has been made possible because of the use of a special interconnecting protocol called the ***Internet Protocol*** (***IP***).

## 7. Gateways

A *Gateway* is any device that can be configured to provide access to a Wide Area Network or the Internet.

**Note**. A gateway may be a router, or a computer configured to provide access to the Internet.

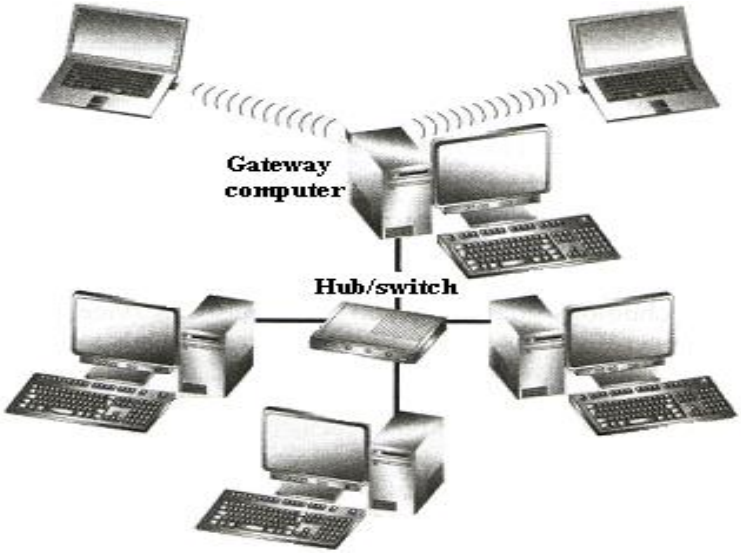



Fig.: A gateway PC connecting a LAN to a WAN

## 8. Switches

Unlike a hub, a *Switch* forwards a data packet directly to the terminal equipment on the network without broadcasting. It does this by connecting the two nodes *point-to-point* as if they were linked by a direct cable.

**Note**. Some hubs can also act as switches. Such a hub is referred to as a ***switching hub***.

- Switches are more expensive than hubs. This means that, one switch may be used as a bridge to connect several hubs. This reduces collision problems caused by broadcasts.

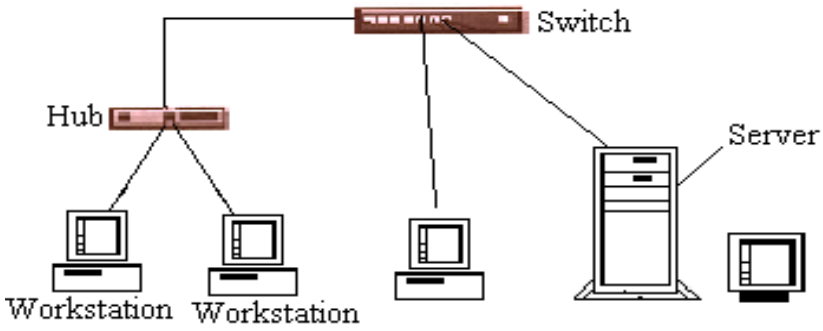



Fig. A switch on a Local area network

## Wireless communication devices

For a long time, networks have been implemented using tangible transmission media like cables. However, since the cost of wireless technology has gone down & the quality of service increased, companies & individuals are now using wireless segments in their communications with the aim of extending the capability of wired networks.

The most common devices (components) used in wireless communication are: *Access Points (AP)*, and *Wireless antennae*.

### 1. Access points (AP)

An *Access point* is an entry point into a bounded network.

It is used by people who have wireless devices such as Personal Digital Assistants (PDA's), Laptops, and computers with wireless links.

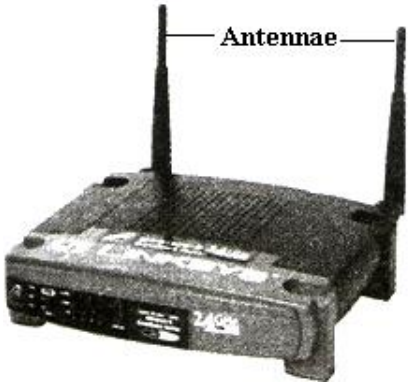



Fig. 3.0: Wireless access point

### 2. Wireless antennae

The Access point should have antennae so as to detect wave signals in the surrounding. The waves may be *Radio waves*, *microwaves* or *infrared waves*.
Most Access points have 2 antennae so that the one that receives the best signal at any particular time can be used.

## Personal Computer Memory Card International Association (PCMCIA) card

A PCMCIA is a card inserted into a device such as a Personal Digital Assistant (PDA) or a laptop in order to enable wireless communication between the device and a wired network server.

Fig.: The PCMCIA card used to connect a device to a wireless LAN

### Review questions.

1. Describe at least five devices used in data communications.
2. Explain the function of a NIC in networking.
3. **(a).** Explain the importance of a gateway on a network.
   **(b).** Differentiate between a router and a gateway.
4. Why is a Switch preferred to a hub on the network?
5. What is the function of a Repeater on a network?
6. Give one disadvantage of a Hub on a network.

## Definition of terms used in Networking

### Network

A *Network* can be defined as a collection of *independent entities* that are arranged in such a manner as to exchange data, information or resources.

*Examples of networks:*

- Road network: - this is the interconnection of roads in a country, continent or throughout the world. Road networks facilitate the transfer of goods & services from one area to another.
- Telephone network (voice networks): - it includes the many lines that criss-cross a country, and enables people to communicate.
- Railway network.
- Nervous system.

### Computer Network

A *computer network* can be defined as a collection 2 or more computers connected together using transmission media (e.g., telephone cables, or Satellites) for the purpose of communication and sharing of resources.

Usually there can be from 2 to hundreds or even thousands of computers on the network. Apart from computers, other devices such as Printers, plotters, fax machines, modems, etc can also be connected to the network.

The term **Transmission media** refers to any physical or non-physical link between 2 or more computers, and in which a signal can be made to flow from source to destination.

**Network Server.**

Computer networks usually have one computer reserved as the "**Mother**" of all the other computers on the network.

A ***Server*** is a powerful computer that provides services (shared resources) to the other computers on the network. It enables information, resources & network devices to be shared by users on a computer network.

Network servers;

i). Have a higher hard disk & main memory (RAM) capacity than the other computers on the network.
ii). Store & run a special program called the *server software* (network operating system), which controls computers on the network.

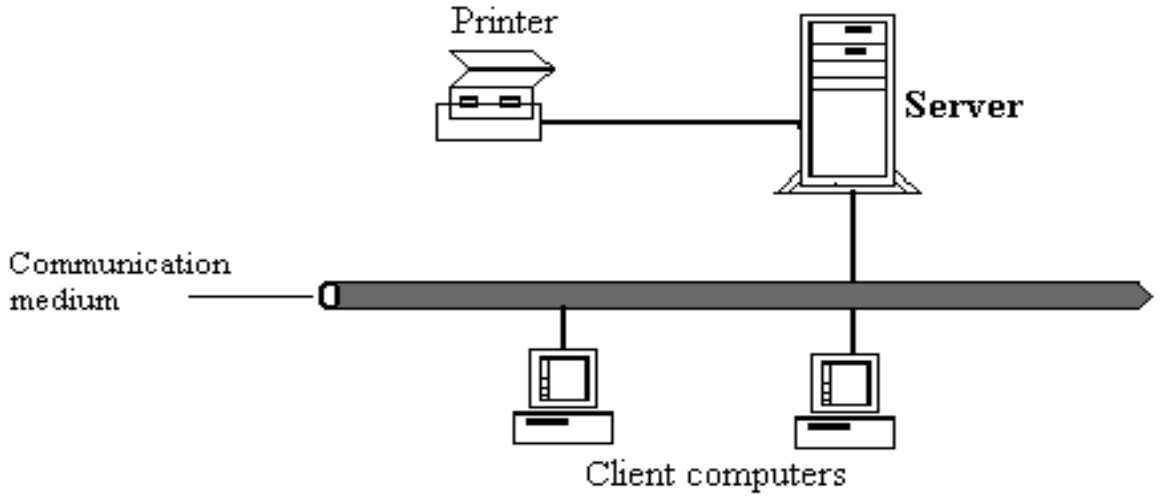
**Clients (workstations)**

***Clients*** (also referred to as *Workstations*) are Personal Computers (PCs) attached to the network, on which the network users do their work. They are used by network users to send their requests to the server.

Clients;

i). Are usually less powerful than the server, and use the resources provided by the Server.
ii). Have their own operating systems and files.
The PCs can be IBM or compatible running MS-DOS, OS/2, Windows, etc.

The figure below shows a server on a network.




**PURPOSE OF NETWORKING**

Some of the reasons for setting up computer networks include:

**1). Resource sharing**

A *Network resource* refers to any component that can be attached to the network for access by users.

Some of the shared resources include:

i). Application programs.
ii). Data and information.
iii). Messages.
iv). Graphics.
v). Files.
vi). Computer processing power.
vii). Network Printers
viii). Fax machines
ix). Modems
x). Storage devices (optical drives).
xi). Communication ports.
xii). Disk space

Users whose computers are connected to a network can, for example, share their files, exchange mails, send faxes, schedule meetings, and print documents from any point on the network. This centralized access to data & information leads to less waste of time, and hence greater productivity.

**2). Remote communications**

*Remote communication* refers to the transmission of data signals between two communication devices located at different geographical locations.
E.g., using remote communication, one can work from home just as if he/she is in the office.

It is mainly through remote communications that people can be able to share ideas, and pass messages over the Internet.

A computer that tries to access resources from another computer on the network is called a ***remote client***, while the computer being accessed is called a ***remote host***.

Remote communication has been made possible by use of wireless transmission media such as *radio waves, microwave,* and *satellite.*

**3). Distributed processing facilities**

*Distributed processing* refers to the act of running the same programs or databases on different computers, which are on the same network but placed in separate locations.

Each computer has its own local peripherals, e.g., disks, printers, terminals, etc.

*For example;*

In a large organization, each branch office has its own server that stores data, information, and other resources required for their daily operations.
This implies that, files reside on the user's computer rather than on a central computer, and are only transmitted periodically to update the central computer.

***Advantages of distributed processing.***

1. Failure of the central computer does not affect the operations of the other terminals.
2. Processing load is shared equally; hence, no time wastage.
3. There is faster access of data as each machine can process & store its data.
4. It doesn't need powerful and expensive servers for data storage.
5. It can accommodate users with variety of needs.

***Disadvantages of distributed processing.***

1. It is more susceptible to virus, as any user could introduce an infected file and spread it throughout the network.
2. Developing an effective back up plan is more difficult when users store data in their individual systems.
3. File management (organization) is difficult as the files are stored in different locations.

**4). Cost effectiveness**

The initial cost of purchasing and laying down of networks components may be expensive. However, the savings experienced and the value added to service delivery make networks cost effective.

- Networks greatly increase the efficient use of scarce resources. E.g., a large organization with many stand alone computers will need a printer for each computer. However, if the computers are networked, only one printer is used.
- Computer networks have also enhanced daily communication, i.e., they have made the flow of information from one place to another easy. Users can send mails (e.g., e-mails) to each other, without having to bear the cost of stamp duty or delivery charges. Similarly, company executives can hold electronic *video conferences,* thus reducing the traveling costs.

**5). Reliability**

A computer network is reliable especially when communicating or accessing information:

**i).** Data can be transferred with minimum errors from source to destination.
**ii).** Incase one computer breaks down; the user can still access data & information from the other computers using another computer on the network.

**LIMITATIONS (DISADVANTAGES) OF NETWORKING**

**1). Security issues**

Data & information held on a network is open to many people across the world, and can easily be accessed illegally. In addition, when information is sent over the network from one place to another, it can be tapped or listened to by unauthorized parties.

**2). High initial cost**

The initial cost of buying network hardware & software is very high.

**3). Moral and cultural effects**

Large networks such as the Internet have chat rooms and messaging services. These enable underage children to meet peers and adults on the *net*, some of whom may have bad intentions.

Access to pornographic and other negative material on the Internet has made the fight against social problems such as HIV/AIDS, bad sexual behaviour, and drug abuse more complicated.

**4). Spread of terrorism and drug trafficking**

The Internet makes it easy for terrorists and drug traffickers to operate. This is because; they use information networks for their business communications.

**5). Over-reliance on networks.**

Most organizations have done away with manual operations. This means that, all business processes, and the society depend on computer networks. Therefore, if by any chance the network fails or goes down, then many systems in the society will stop working.

## Review questions.

**1.** List four network systems that are not computer-based networks.
**2.** Define the following terms:
   **(a).** Computer network.
   **(b).** Data communication.
**3.** Differentiate between:
   **(a).** A baseband and broadband signal.
   **(b).** A Network server and a workstation.
   **(c).** Remote client and remote host.
   **(d).** Half duplex and full duplex transmissions.
**4.** State the factors to be considered while selecting a data transmission system.
**5.** Give four advantages and two disadvantages of networking.
**6.** (a) Explain the concept of distributed processing in networking.
   (b) State 3 advantages and 2 disadvantages of distributing processing.
**7.** Why is a network more reliable than stand alone computers?
**8.** What do you understand by the following terms in networking:
   (i). Baud.
   (ii). Baud rate.
   (iii). Bandwidth.
   (iv). Resource.
**9.** What name do we give to each of the following:
   **(a).** The computer that is dedicated to serving requests from other computers in a network.
   **(b).** The computers that sends requests.

## TYPES OF COMPUTER NETWORKS

Computer networks are usually classified according to size. The three most common types of networks are:

1. Local Area Network (LAN).
2. Metropolitan Area Network (MAN).
3. Wide Area Network (WAN).

### Local Area Network (LAN).

This is a computer network that is formed whenever computers are connected together in a relatively small geographical area, e.g., in one building or a school.

LAN is the smallest size of network & it normally covers an area within the radius of 10M – 3 Km.

LAN is usually owned by one organization. However, one LAN can be connected to other LANs over any distance via data transmission lines or wireless media.

A LAN connects several Personal Computers to a ***Server computer***. The server computer makes available the resources requested by the other computers (workstations) on a network.

In most LANs, each workstation has its own CPU which it uses to execute programs, but still the workstation user can also access data & devices anywhere on the network.

***Advantages of LANs.***

**1).** They enable many users to share expensive devices such as Laser printers, as well as data. However, the no. of computers that can be connected & the distance to be covered is limited.
**2).** Have Low cost (requires less expensive equipment).
**3).** Enable users to communicate with each other, by sending messages or engaging in chat sessions.
**4).** LANs transmit data at very fast rates. They are much faster than data transmitted over telephone lines.
**5).** Small error counts (low error rates).

## Metropolitan Area Network (MAN).

A MAN is made up of many LANs connected together.

It covers a metropolitan (medium-sized geographical) area, e.g., a town or an entire city, within a radius of 5 – 50 Km.

*Characteristics of MAN*

- Larger than LAN.
- Slower than LAN, but faster than WAN with data rates of 100MBps & above.
- Are more expensive than LANs, since special equipment is needed to connect the different networks together.
- Prone to few errors (moderate error rates).

## Wide Area Network (WAN).

This is the largest size of network.

A WAN covers a large geographical area such as an entire country, a continent, or even the whole world.

It consists of many LANs and MANs connected together to form one large network such as the Internet.

*Characteristics of WAN*

– They cover an unlimited (a very large) geographical area, e.g., can cover the whole world.
– They are expensive to build since it requires special equipment for connection.
– Their transmission links are also expensive.
– Long distance transmission.
– Have low data transfer rates compared to LANs (i.e., they are slower than LANs & MANs)
– More prone to errors (very high possible error rates compared to LANs and MANs).

**Differences between a Local Area Network and a Wide Area Network.**

1. LAN is limited to a small geographical distance.
2. Data transmission speed in LANs is higher.
3. Cost of data transmission in LANs is small.

4. There are less transmission errors in LANs.

### Review questions.

**1.** Describe THREE major data communication models.
**2.** Explain the three most common types of computer networks in use today.
**3.** Describe a Wide area network.
**4.** List THREE differences between Wide Area Network and Local Area Network.
**5.** Determine the type of a network characterized by:
   **(a).** connection between computers, printers and other resources using UTP cables.
   **(b).** over 250 computers connected to share resources in a city.

## ELEMENTS (COMPONENTS) OF NETWORKING

A computer network is made up of several standard components, which can be classified into three (3) major categories, namely:

**1.** Data communication media.
**2.** Communication devices.
**3.** Networking software.

## Network software

Network software can be classified into 2 main groups:

**1.** Network Operating systems.
**2.** Network Protocols.

### Network Operating systems

These are operating systems specifically designed to enable the networked computers to respond to service requests.
Servers run on a network operating system.

#### *Functions of network operating systems*

A network operating system performs the following network related functions:

**1.** Provides access to network resources, e.g., printers and folders.
**2.** Enables nodes on the network to communicate efficiently with each other.
**3.** Enables the various processes on the network to communicate with one another.
**4.** Responds to requests from application programs running on the network.
**5.** Supports network services such as network card drivers & protocols.
**6.** Maintains security, ensuring that only users authorized to use the computer system are allowed access to it.
**7.** Produces logs, i.e., a record of all the programs as they are run.
**8.** Organises the use of storage, since this has to be shared among different users.
**9.** Works out the resources used by each program. If the user is paying for the service, then the computer works out the cost of running the program & charges the appropriate account.

Network OS are normally designed as Multi-user operating systems that run the network server program.

Examples of network operating systems are:

– UNIX - Windows NT
– Linux - Windows 2000
– Novell NetWare - Windows 2003

### Protocols

*Protocols* are a set of rules and procedures that govern the communication between two different devices or people.

E.g., a diplomat from a foreign country must adhere to the set rules and procedures of communication when representing his country in the host country.

In computer networking, ***Protocols*** are the rules and technical procedures that govern communication between the different computers on the network.

### How Protocols work

The data transmission process over the network is divided into steps, and at each step, a certain action takes place.
In addition, each step has its own rules and procedures as defined by the network protocols. The work of these protocols is usually coordinated through ***protocol layering*** so as to ensure that there are no conflicts or incomplete operations.

## The Open Systems Interconnection (OSI) reference model.

Interconnecting of the various hardware & software products from different manufacturers together into a single network requires that the equipment must be able to communicate and work with each other.

The *OSI* reference model defines standard (uniform) methods which enable different systems to interoperate with each other and to be portable across one another.
Network protocols are usually designed using the OSI reference model. To facilitate communication between application processes located on different computers, the model groups similar computer communication protocols into 7 layers, each performing specific functions.

| | Layer | Function |
|---|---|---|
| **7.** | Application layer | This is where user applications are run. It provides network services such as file sharing, distributed processing, file transfer, and network management to users. It also generates requests for transmission of data or opening of received information |
| **6.** | Presentation layer | Defines data formats to be exchanged & adds formatting, display and encryption information to the data being sent. |
| **5.** | Session layer | Sets up data transmission sessions between two communicating devices on the network. |
| **4.** | Transport layer | Manages data transfer over the network to ensure reliability. It ensures that data units are delivered free of errors, in sequence, and without loss or duplication. |
| **3.** | Network layer | Serves the Transport layer by adding address information to the data packets, and routing it to its destination. |
| **2.** | Data link layer | Prepares data for going onto the communication medium on the physical layer. Adds error checking & correction information to the data. |
| **1.** | Physical layer | Transmits raw data packets via the network card through the transmission media in form of bits. Converts frames to electronic signals and vice versa. |

***Protocols at the Application layer:***

They provide services to application programs such as the ***E-mail editor program*** that enables composing or reading of e-mail messages.

Examples of protocols at the Application layer include:

1. *Simple Mail Transfer Protocol* (*SMTP*) - an Internet protocol for transferring e-mails.
2. *File Transfer Protocol (FTP)* – an Internet protocol for transferring files.

3. *Apple Talk and Apple Share* – a networking protocol standard for Apple computers.

***Protocols at the Transport layer:***

They ensure that data is passed between computers more reliably.

Examples of protocols at the Transport layer include:

1. *Transmission Control Protocol* (*TCP*) – enables delivery of sequenced data over the network.
2. *Sequential Packet Exchange (SPX)* – used in Novell networks for sequenced data.
3. *NetBEUI* – used in Microsoft and IBM networks to establish communication sessions between computers in LANs.
4. *Apple Transaction Protocol (ATP)* – it is a communication session and data transport protocol used in Apple computers.

***Protocols at the Network layer:***

They provide link services, e.g., they handle addressing and routing information, error checking and retransmission of requests.

Examples of protocols at the Network layer include:

1. *Internet Protocol* (*IP*) – it does packet forwarding and routing.
2. *Internetwork Packets Exchange* – This is a NetWare's protocol for packet forwarding and routing.

### Review questions.

1. List two types of network software.
2. Outline four functions of network operating system.
3. List four examples of network operating systems.
4. Outline the seven open systems interconnection (OSI) reference model layers.
5. Explain the importance of the Physical layer in the open systems interconnection (OSI) reference model.
6. **(a).** Define the term protocol.
   **(b).** Give three examples of protocols used in networking.

## Network Topologies

The term network *Topology* refers to the way in which computers, cables, and other devices have been arranged in the network.

It can also refer to how data is passed from one computer to another in the network.

### Logical and physical topologies

Network topology can be viewed in 2 ways; *Logical* or *Physical*.

**Logical (Signal) topology**

*Logical topology* deals with the way data passes from one device to the next on the network.

Examples of logical topologies are:

(a). Ethernet.
(b). Token ring.

***Ethernet topology***

In Ethernet topology, all computers listen to the network media, and a particular computer can only send data when none of the others is sending.

***Token ring topology***

In Token ring topology, a special package for data called a *token* goes around the network. The computer whose address is on the data held in the token picks it up, reads the data, and then

releases the token. The token can then be captured by another computer which needs to transmit data.

## Physical topology

*Physical topology* refers to the physical arrangement of components on the network.

Examples of physical topologies are:

(a). Star topology.
(b). Bus topology.
(c). Ring topology.
(d). Mesh topology.
(e). Tree (Hierarchical) topology.

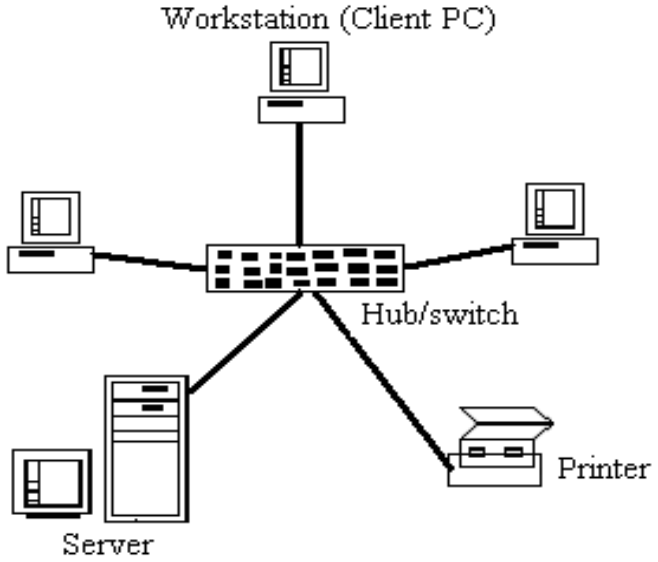
The choice of the topology to adopt depends on factors such as *Reliability*, *Expandability*, and *Performance*.

## Star topology

Star topology consists of computers and other devices, each connected to a common central server called the **Hub**. However, to connect to the central machine, each computer uses a separate cable.

Nodes communicate across the network by passing data signals through the hub, i.e., any two computers (workstations) in the network communicate through the central machine.

When the hub receives data from a transmitting computer, it broadcasts the message to all the other nodes on the network.




**Advantages of Star topology.**

1. Allows key networking resources such as concentrators & servers to be centralized.
2. Easy to configure.
3. Enhances operational survivability.

   The hub isolates the network cables from each other. Even if a wire between a workstation and the hub breaks or develops a bad connection, the rest of the network remains operational.
4. Simple to control.
5. It can be extended easily, since a workstation is simply connected to the hub.
6. Provides flexibility in adding or deleting devices.

   The wiring hubs increase the flexibility for growth. Addition & removal of nodes does not involve cutting and joining of cables.
7. Easier to troubleshoot.

When something goes wrong with the network, the administrator can troubleshoot it from the wiring hub.

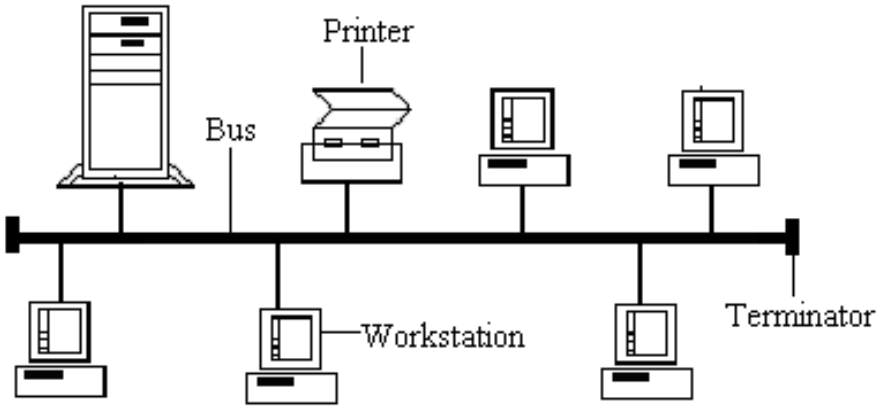
8. The Hub can support multiple types of cables.

**Disadvantages of Star topology.**

**1.** If the central switch node (Hub) fails, it may bring down the entire network.
**2.** It is costly because; each workstation is connected to the central concentrator by is own dedicated cable (i.e., it requires a lot of cables).
**3.** Installation is time consuming, because each node forms a segment of its own.
**4.** May require a special device for signal regeneration across the network.

**Bus topology (Daisy-chain topology)**

In Bus topology, all the devices in the network are connected directly, through appropriate interfacing hardware, to a single transmission cable called the ***Bus*** (or ***Backbone***) on which information is broadcast.




Bus topology uses Coaxial cable as transmission medium. The cable can carry only one message at a time and each workstation on the network must be able to know when it can and cannot transmit using this cable.

A ***Terminator*** is attached to each end of the cable to avoid signals from bouncing back and forth on the cable causing signal distortion.

For communication to take place, data is addressed to a particular computer & put in the cable in the form of electronic signal. As the data passes along the cable, each workstation checks whether the data is addressed to it. If the address in the data matches that of the machine, it picks up the data and processes it.

Bus topology doesn't need any special equipment such as switches or repeaters to amplify the signal.

**Advantages of Bus topology.**

**1.** Easy to install.
**2.** Inexpensive (less costly) because; it does not require a complete cable length per computer.
**3.** Can easily be extended.
**4.** It allows the workstations to communicate independently (separately) of each other.
**5.** Failure of one station on the network does not affect the operations on the bus.

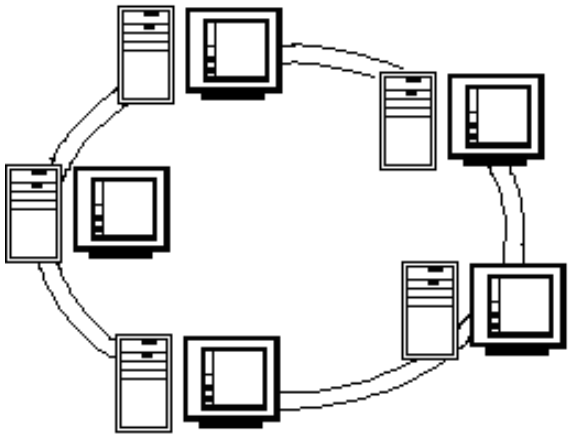
**Disadvantages of Bus topology.**

**1.** A cable break in each section brings down the whole network.
**2.** The performance degrades since there is no signal integration.
**3.** Troubleshooting the cable fault can be quite difficult because; the fault could be anywhere on the cable.

4. Only a limited number of computers can be connected to the cable. This is because; each computer is listening to the cable in order to transmit. This means that, if the number of computers increase, there will be more collision as the workstations compete for transmission.

### Ring topology

In a ring topology, the computers are connected to one another in the shape of a closed loop using a single cable.



Data flows from one computer to another in one direction, and each computer actively participates in data transfer from one station to the other. In other words, each workstation acts as a booster by regenerating and retransmitting the signals around the network to its neighbour.

A token is used to exchange data from one station to another. A ***token*** can be viewed as an envelope or a bag where data is placed for transmission and carried around the network.

#### Advantages of Ring topology.

1. They use a short length cable.
2. Simple to install.
3. Provides high performance for many users.
4. Provides an orderly network in which every device has access to the token and can transmit data.

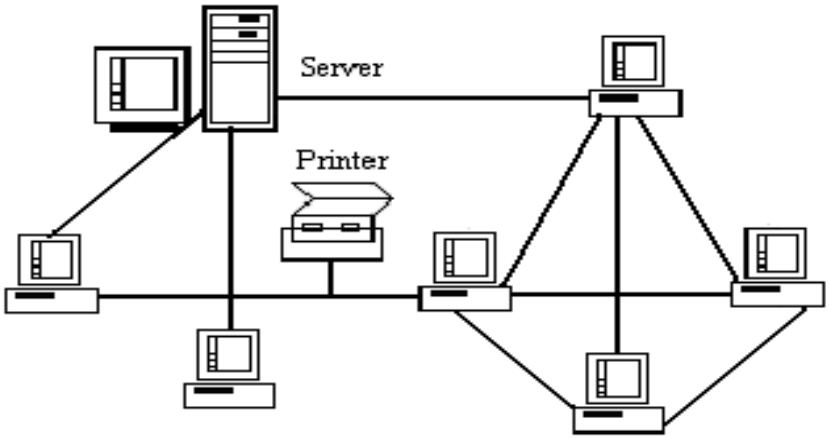
#### Disadvantages of Ring topology.

1. Failure of one computer or the cable will affect the rest in the entire network.
2. Modification is difficult because; adding or removing a device can disrupt the entire network.
3. Troubleshooting can be difficult.

### Mesh topology

Mesh topology uses separate cables to connect each device to every other device on the network providing a straight communication path.

It is mostly used in Wide Area Networks where there are many paths between different locations.




**Advantages of Mesh topology.**

1. It is fast.
2. Failure on one node will not cause communication breakdown.
3. Easy to troubleshoot cable problems. If two machines are not communicating, the administrator will only check the cable between them.
4. Enhances flexibility in communication.
5. Enhances fault tolerance provided by redundant/ excessive links.

**Disadvantages of Mesh topology**

1. Difficult and expensive to install and maintain.
2. Very costly as it requires large amounts of cables (or redundant links).
3. Difficult to add more nodes when the network is large.
4. Difficult to isolate faults due to lack of a central control point.

## Tree (Hierarchical) topology

This is a hybrid topology where groups of star-configured networks are connected to a linear bus (backbone).

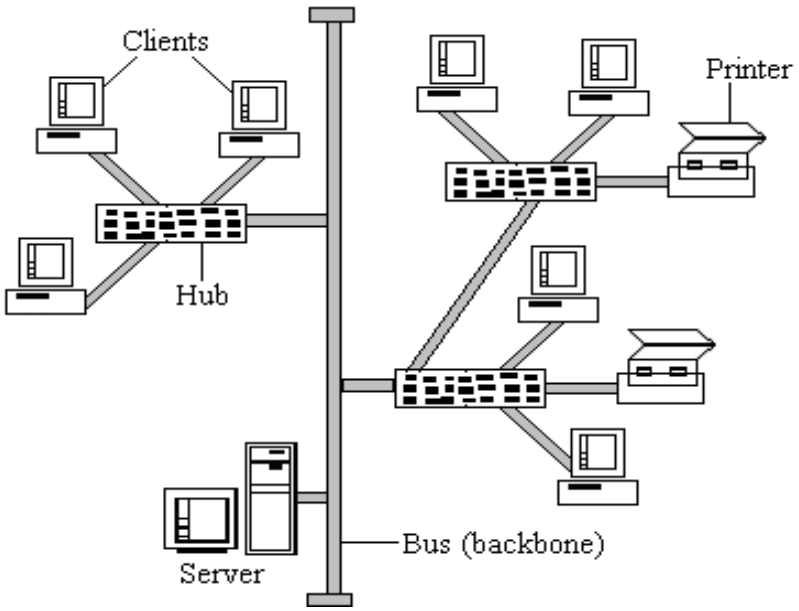



Fig. 3.6: Tree topology

## Review questions.

1. What is a computer network topology?
2. Distinguish between Logical and Physical network topology.
3. Using appropriate diagrams, describe any three types of physical network topologies.

## COMMUNICATION OF DATA IN A NETWORK.

Data in a network travels from one computer to the other using laid down rules known as **Protocols**. The protocols used depend on the way the computers are connected together on the network.

Generally, there are 2 broad ways in which computers communicate with one another in a network, namely:

**(i).** Point-to-point communication.
**(ii).** Broadcast communication.

**Point-to-point communication.**

In point-to-point, the network contains numerous cables or telephone lines, each one connecting a pair of computers.

The message is received at each intermediate computer in whole, stored there until the required output line is free, and then forwarded.

A network using this principle is called a *point-to-point* or *store-and-forward network*.

**Broadcast communication.**

In broadcast, there is a single communication channel shared by all computers. In this case, the messages sent by any computer are received by all other computers.

Something in the message itself must specify for whom it is intended. After receiving a message not intended for itself, a computer just ignores it.

### Review questions.

**1.** As regards to communication within a computer network, what do you understand by the following terms:
(a) Point-to-point
(b) Broadcast (2 marks)

## NETWORK MODELS

A *Network model* describes how the computer processes information on the network.

Data can be processed by a Client, a central Server or by all the computers on the network.

### 1). Centralized computer model.

Very large computers, usually mainframes, are connected with terminals. The users input & output data using the terminals, while the processing is done by the central computer (mainframe).

**Advantages of Centralized model**

(i). Data is kept in one location, ensuring that every user is working with the same information.
(ii). It is easier to back up data since the information is stored on only one Server.
(iii). Easier to maintain security. It is only the server which needs to be secured since the terminals have no data.
(iv). The terminals do not require floppy drives as all work is stored on a Server.
(v). Chances of computer being affected by viruses are very minimal as no diskettes are being used.
(vi). It less costly.
Although the Server has to be very powerful with a lot of storage space, the terminals are inexpensive as they don't require real processing or storage capability of their own.

**Disadvantages of Centralized model**

(i). It is very slow as it is the server alone, which does all the processing.
(ii). In case where the users have varied needs, it would be difficult to meet these needs in a centralized computing network as each user application needs to be set up separately.
(iii). Connection is difficult. All the computers have to be connected on a central place.

### 2). Distributive computing

In this model, data is stored and processed on the local workstation. Computers acting as ***Stand alone systems*** are connected together for increased functionality.

A **Stand alone** is a computer which is not connected to any other computer equipment other than its own Printer.

**Advantages of Distributive Computing model.**

(i). Each machine processes and stores its data; hence, data is accessed faster.
(ii). It doesn't need powerful and expensive servers for data storage.
(iii). It can accommodate users with variety of needs.

**Disadvantages of Distributive Computing model.**

(i). It is more susceptible to virus, as any user could introduce an infected file and spread it throughout the network.
(ii). It is more difficult to develop an effective back up plan, since each user stores data in his/her individual system.
(iii). File management (organization) is difficult as the files are stored in different locations.

### 3). Collaborative model.

In this model, all computers can share processing power across the network. Applications can be written to use the processing on the computers to complete job more quickly.

**Advantages of Collaborative model.**

(i). It is faster to complete a task as users are not limited to processing power of one system.
(ii). Variety of users can be accommodated on a collaborative network.

**Disadvantages of Collaborative model.**

(i). Viruses can easily be transmitted through the network.
(ii). Backing up of the data is difficult.
(iii). File synchronization is difficult.

## CATEGORIES OF NETWORKS

### 1. Peer-to-Peer network.

A **Peer** is a computer that acts both as the client and a server.

In this network, all the connected computers are equal & each machine acts as both client and Server. This means that, there is no central storage area for information & no dedicated central Server.

No system administrator. Therefore, the user of each computer determines what data & resources the computer will shares with other computers on the network.

Peer-to-peer networks are appropriate in an environment where:
- There are 10 or less users.
- The users are located in a general area.
- Security is not an issue, e.g. in Bulletin boards.

**Advantages of Peer-to-peer networks.**

(i). It is small & inexpensive.
(ii). It is easier to maintain.
(iii). It is easier to setup.

**Disadvantages of Peer-to-peer networks.**

(i). It is difficult to locate information stored in the connected computers due to *Shared level security*.
(ii). Difficult to update documents and files.
(iii). It is expensive to train staff on how to share resources, as each user is an administrator.
(iv). It is difficult to maintain security, as it is the user's responsibility to ensure that only authorized individuals can access their data.
(v). It is more tedious as the user has to memorize password for resources, and in case of any change, they have to inform others.

**2. Server-based networks**.

In this network, there is usually a Server, e.g. a company which is dedicated to handle files and/or information for clients, make & service requests from network clients, and ensure security of files and directories for them.

Server-based networks require a network operating system.

**Advantages of Server based networks.**

(i). There is security since the Server controls the resources the clients need to access.
(ii). It can support a large number of users.
(iii). The server can be optimized to hand out information as fast as possible.
(iv). Fewer connections are required by the clients to get the resources.
(v). Easier to maintain backup for files (synchronization of files).
(vi). Cost effective as client workstations don't need large hard disk (storage capacity).

**Disadvantages of Server based networks.**

(i). It is dependent on a Network administrator.
(ii). Requires servers, which are expensive.

## Review questions.

**2.** How does each of the following networking models operate?
(i). Centralized computing.
(ii). Collaborative computing.
(iii). Distributed computing.

## Network Security

In networking, there are several ways of protecting your data and information from intruders. They include: *Share level* and *User level security*.

**Share level security**

This model of security is mostly used in peer-to-peer networks. The user can decide which resources to give for sharing.
Most Windows operating systems such as Windows 9X provide such kind of security.

**User-level security**

The User level security is used on server-based networks.

A network administrator assigns accounts to users, i.e., each user is provided with a unique name and a password which he/she can use to access network resources.