Chapter 1...

# Introduction to Data Communication

**Contents**



## 1.0 INTRODUCTION

- Data communications and computer networks are two of the fastest growing technological areas in today's modern world. This is because there is an almost unlimited demand for information transfer.
- Data communications and computer networks deals with data/information transmission. Data refers to the raw facts that are collected while processed data refers to information.
- Data can be represented in many ways such as a human voice, text, numbers, images (graphics), audio, and video etc.
- Data communication is a process of exchanging data or information between two devices (a sender and a receiver) through some kind of transmission medium such as co-axial cable or fiber optic cable (wired communication) and/or air (wireless communication).
- A communication involves the transfer/exchange of information. Communication means the transfer of information between humans, computers or machines in a meaningful way.
- Data communication can be defined, "the exchange of information between two computers capable of generating processing and interpreting data".
- The data communication process shown in Fig. 1.1.

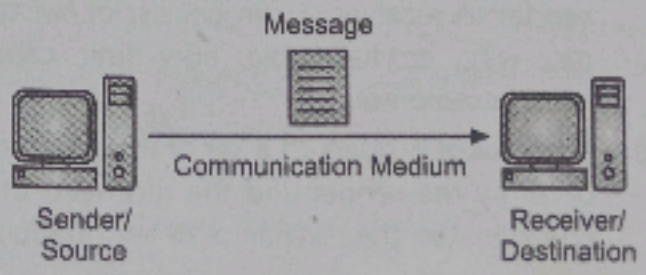



**Fig. 1.1: Communication between Two Computers**

- Fig. 1.1 shows communication between one computer (sender/source) sending a message to another computer (receiver/destination) over a wire or radio waves called as transmission media.
- The main objective of data communication and networking is to enable seamless exchange of data between any two points in the world. This exchange of data takes place over a computer network.

## 1.1 CONCEPT OF DATA COMMUNICATION

- Communication is the basic process of information exchange. Communication, whether between human beings or computer systems, involves transfer of information from a sender to a receiver.
- Communication is the conveyance of a message from one entity, called the source or transmitter or sender to another, called the destination or receiver, using a communication channel.
- Communication is defined as transfer of information, such as thoughts and messages between two entities. The process of sending or receiving data between two points of a computer networks is known as Data Communication.

**Definition of Data Communication:**

- Data communication is defined as, "the exchange of information (in the form of 0's and 1's) between two digital devices via some form of transmission medium". **OR**
- Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable (twisted-pair cable or co-axial cable) or wireless (air). **OR**
- "The transfer or exchange of information from one computer to another is known as Data Communication".

### 1.1.1 Process of Data Communication

- Data communication refers to the exchange of information/data between two devices through some form of wired or wireless transmission medium. It includes the transfer of data, the method of transfer and the preservation of the data during the transfer/exchange process.
- To initiate data communication, the communicating devices should be a part of a data communication system that is formed by the collection of physical equipment's (hardware) and programs (software).
- Fig. 1.2 shows process of data communication.
- A data communication process is made up of five components namely message, sender, receiver, transmission medium, and protocol are shown in Fig. 1.2.
- The **functions of each component in data communication** are as follows:
  1. The **message** is the information in the form of data to be communicated. It can consist of text, numbers, pictures, sound, video or any combination of these.
  2. The **sender** is the device that sends the data message. It can be computes, workstation, telephone handset, video camera and so on.
  3. The **receiver** is the device that receives the message. It can be computer, workstation, telephone handset, television and so on.
  4. The **transmission medium** is the physical path by which a message travels from sender to receiver. It can consist of twisted pair wire, coaxial cable, fiber-optic cable, laser or radio waves.
  5. A **protocol** is refers to a set of rules (agreed upon by the sender and the receiver) that co-ordinates the exchange of information.

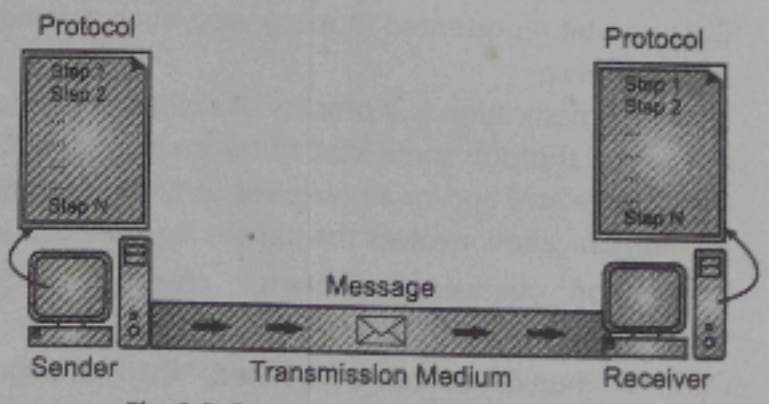



**Fig. 1.2: Process of Data Communication between Two Computers**

Without the protocol, the sender and the receiver cannot communicate. Both sender and receiver should follow the same protocol to communicate with each other.

## 1.1.2 Communications System

- The communications system provide a vehicle of carrying information from one point to another. A data communication system is the combination of hardware, software and data transfer links that make up a communication facility for transferring or exchanging data.
- Data communications is the movement of computer information from one point to another by means of electrical or optical transmission medium or air (often called data communications networks).
- The communication system transfers information from one place to another in the form of signal. There is a transmitter on one side and the receiver on the other. In between these, there is the channel as a medium to transmit information. It is shown in Fig. 1.3.

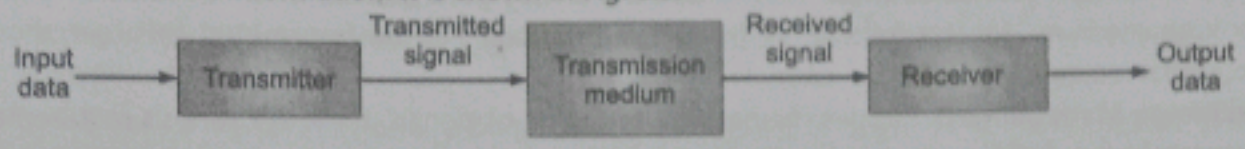



**Fig. 1.3: Simple Data Communication System**

## 1.1.3 Components of Data Communication

- In the case of sending and receiving messages or data from one place to another, we have many elements working together all these elements put together to work efficiently is known as a system. The communication system has the sole purpose of passing data or information in the most effective manner.
- A communication system itself can be either analog or digital (or a combination of two). The information can be transmitted in either in analog from or in digital form within the communication networks.
- For data communication to take place, the communicating devices must be part of a communication system. Fig. 1.4 shows components of data communication system.

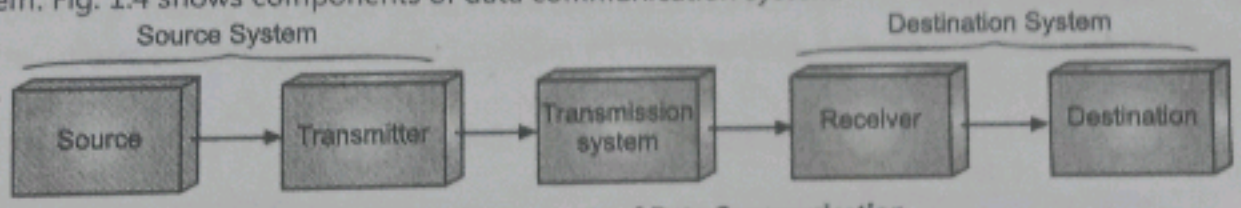


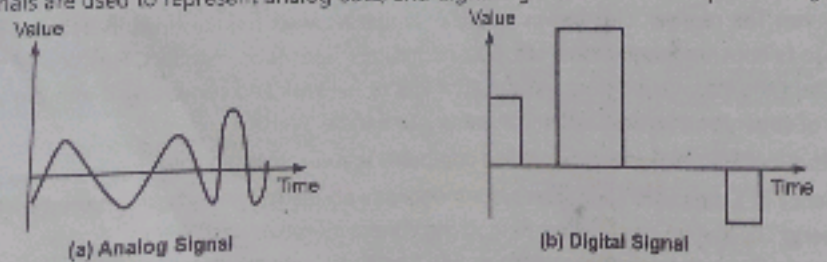

**Fig. 1.4: Components of Data Communication**

- Following are the building blocks (components) of Data Communication System:
  1. **Source:** Source generates the data which is to be transmitted. Examples of sources includes telephone terminal, personal computers, mainframes and so on.
  2. **Transmitter:** The transmitter, also known as the sender, is the device that originates the information transfer. Data from the source are not transmitted in the same form which are generated by source, transmitter converts and encodes the data so as to produce electromagnetic signals. Modem is used to convert incoming data stream into analog signals that can be handled by telephone network.
  3. **Transmission System:** It is a single transmission line or network connecting source and destination. Examples includes cabling, microwave, fiber optics, radio waves and so on.
  4. **Receiver:** The receiver, also known as the sink, that receives the information transfer. Receivers can include telephones, printer terminals, host computers, and video monitors. Function of the receiver is to accept the information from transmission line or network and converting it into digital data in the form of stream so that destination computer can handle the data.
  5. **Destination:** Destination is a device like computer that receives the data.
- The efficiency of a data communication system depends on the following basic **characteristics**:
  1. **Delivery:** The system must deliver data to the correct intended destination.
  2. **Accuracy:** The communication system should be deliver data accurately i.e. without any error.

3. **Timeliness:** The communication system must deliver data on time as required. Delay in data delivery might render data useless for the receiver.
4. **Jitter:** It is the variation in the packet arrival time. Uneven jitter may affect the timeliness of data being transmitted.
5. **Transmission System Utilization:** It is a measure of use of transmission facilities that are shared among the number of communicating devices. Various multiplexing techniques are used to share total capacity of transmission medium with number of users.
6. **Synchronization:** Receiver must be able to detect when transmission begins and when it ends. Synchronization between receiver and transmitter should be achieved using handshaking signals.
7. **Error Detection and Correction:** Transmitted signal may get distorted when it travels long distance through medium. For example, a file from one computer can be transmitted to other should be accompanied by error detection code.
8. **Exchange Management:** Besides the nature and timing of signals, there are various requirement for communication between two parties that comes under the term exchange management.
9. **Message Formatting:** Two parties should have some agreement about format of data to be exchanged or transmitted. Binary code for characters is to be adopted universally.

## 1.2 ANALOG SIGNAL AND DIGITAL SIGNAL

- The energy flow profile of particular representation of data is known as signal. Signals are electric or electromagnetic representations of data. Transmission is the communication of data by the propagation and processing of signals.
- A signal can be anything which conveys information. For example a picture of a person gives you information regarding whether he is short or tall, fair or black etc. Mathematically signal is defined as a function of one or more dependent variables that conveys information about the state of a system.
- Data is transmitted from one point to another point by means of electrical signals that may be in digital and analog form.
- Signals can be of two types namely, **Analog Signal** have infinite values in a range and **Digital Signal** have limited number of defined values.
- The term 'analog' means something that is continuous in nature. Analog data can have any value within a specified range. Analog data refers to information that is continuous. For example, sounds made by a human voice generates continuous waves in the air.
- The term 'digital' means something that is discrete in nature. Digital data can have only specified values that must be discrete in nature. Digital data refers to information that has discrete states. Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s.
- In data communication there are two types of transmission techniques namely analog transmission and digital transmission. **Analog transmission** is a means of transmitting analog signals (representing either analog or digital data) while the **digital transmission** is a means of transmitting digital signals (representing either analog or digital data).
- Analog signals are used to represent analog data, and digital signals are used to represent digital data.



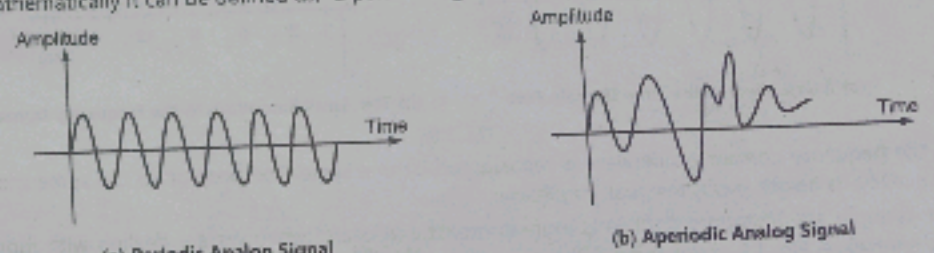

(a) Analog Signal (b) Digital Signal

Fig. 1.5: Types of Signals



### 1.2.1 Periodic and Aperiodic Signals

- An analog signal can take one of two forms namely, periodic or non-periodic (aperiodic).
  1. A **periodic analog signal** completes a pattern within a measurable time frame, called a **period**, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.
  2. A **nonperiodic analog signal** changes without exhibiting a pattern or cycle that repeats over time. In data communications, we commonly use periodic analog signals.
- A signal which repeats itself after a specific interval of time is called periodic signal. A signal is considered to be periodic signal when it is repeated over cycle of time or regular interval of time. This means periodic signal repeats its pattern over a period.
- A signal can be classified as periodic signal if it repeats itself after a time interval of T, Where T is called period of the signal.
- Mathematically a signal f(t) is said to be periodic if f(t + T) = f(t), where the T is the smallest positive non zero value of all possible values of constants T for which the equality holds then T is said to be period of f(t).
- For example, a sine wave is periodic wave which satisfies sin (0) = sin (2*n*Π + θ) where n = 0, + -1, + -2... But as per definition of period only 2*pi qualifies as period. Hence, sin (0) is said to be periodic with period 2*Π.
- A signal that does not repeats its pattern over a period is called aperiodic signal or non-periodic. Mathematically it can be defined as, "a periodic signal with infinite period".




(a) Periodic Analog Signal (b) Aperiodic Analog Signal

Fig. 1.6

- Periodic analog signals can be classified as simple or composite as explained below:
  1. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals.
  2. A composite periodic analog signal is composed of multiple sine waves.
- The sine wave is the most fundamental form of a periodic analog signal. When we visualize it as a simple, oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow.
- Fig. 1.7 shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.

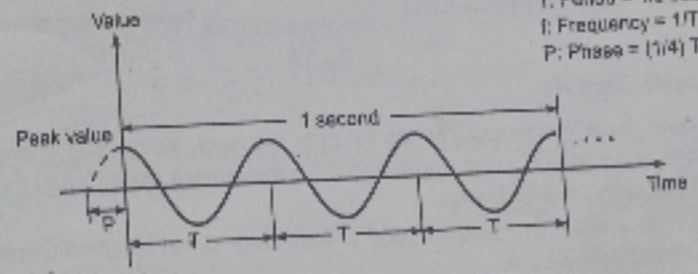
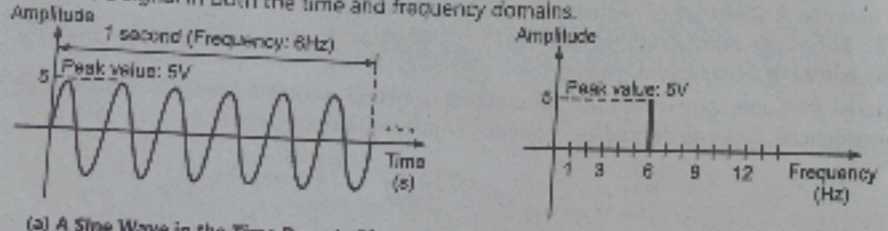



Fig. 1.7

- A sine wave can be represented by following parameters:
  1. The **peak amplitude** of a signal is the absolute value of its highest intensity, proportional to the energy it carries. For electric signals, peak amplitude is normally measured in volts.
  2. **Period** refers to the amount of time, in seconds, a signal needs to complete 1 cycle.
  3. **Frequency** measured in Hertz (Hz), refers to the number of periods in 1 second. Period and frequency are inverse of each other (f = 1/T).
  4. **Phase** describes the position of the waveform relative to time 0 and is measured in degrees or radians.
  5. The **wavelength** is the distance a simple signal can travel in one period. Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium.

## 1.2.2 Time and Frequency Domains

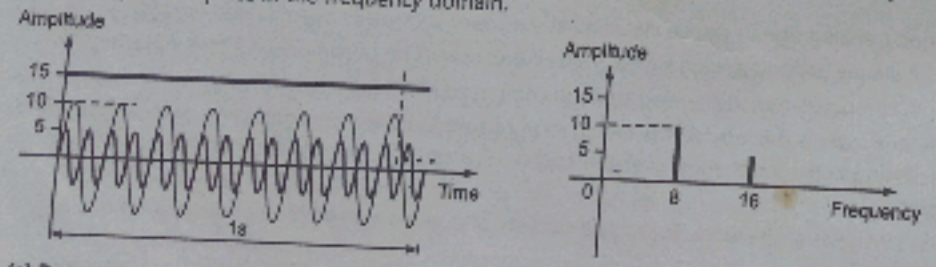
- A sine wave is comprehensively defined by its amplitude, frequency, and phase. We have been showing a sine wave by using what is called a time-domain plot, which shows changes in signal amplitude with respect to time while to show the relationship between amplitude and frequency, we can use a frequency-domain plot.
- Fig. 1.8 shows a signal in both the time and frequency domains.




(a) A Sine Wave in the Time Domain Plot (b) The Same Sine Wave in the Frequency Domain Plot

Fig. 1.8

- In the frequency domain, a sine wave is represented by one spike. The position of the spike shows the frequency; its height shows the peak amplitude.
- For example, the frequency domain is more compact and useful when we are dealing with more than one sine wave. Fig. 1.9 shows three sine waves, each with different amplitude and frequency. All can be represented by three spikes in the frequency domain.




(a) Representation of Time Domain Plot (b) Representation of Frequency Domain Plot

Fig. 1.9

## 1.2.3 Composite Signals

- Simple sine waves have many applications in daily life, such as sending energy from one place to another. However, if we had only one single sine wave to convey a conversation over the phone, it would make no sense and carry no information.
- We would just hear a buzz; we need to send a composite signal to communicate data. A composite signal is made of many simple sine waves.



- In the early 1900s, the French mathematician Jean-Baptiste Fourier showed that any composite signal is actually a combination of simple sine waves with different frequencies, amplitudes and phases.
- A composite signal can be periodic or non-periodic. A periodic composite signal can be decomposed into a series of simple sine waves with discrete frequencies-frequencies that are integral multiples of the fundamental frequency (1f, 2f, 3f and so on). A non-periodic composite signal can be decomposed into a combination of an infinite number of simple sine waves with continuous frequencies, frequencies that have real values.

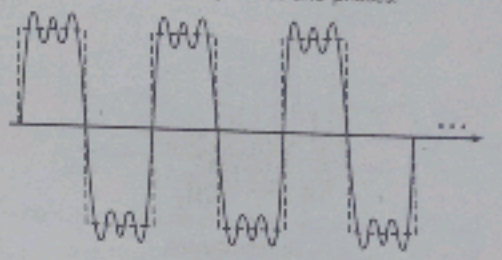
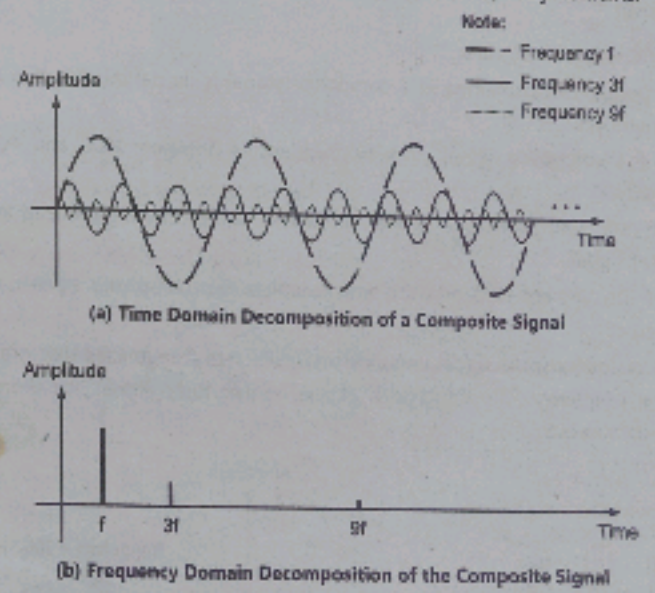


Fig. 1.10: Composite Periodic Signal

- A composite periodic analog signal is composed of multiple sine waves. A composite signal is a signal that is composed of other signals.
- Any composite signal is actually a combination of simple sine waves with different frequencies, amplitudes, and phases. Fig. 1.10 shows a periodic composite signal.

**Decomposition of Composite Signal:**

- It is very difficult to manually decompose this signal into a series of simple sine waves. Fig. 1.11 shows the result of decomposing the above signal in both the time and frequency domains.



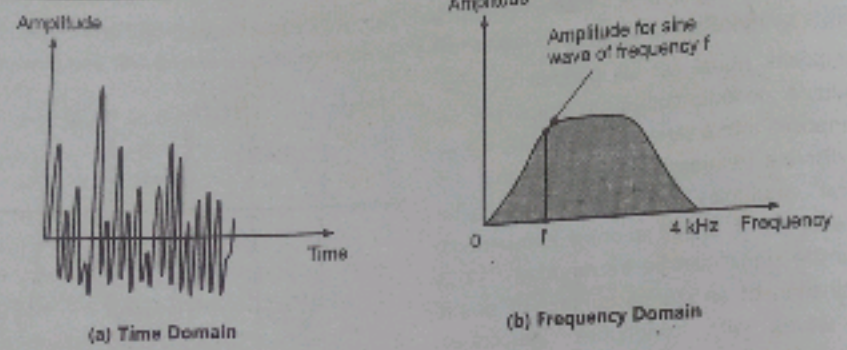

(a) Time Domain Decomposition of a Composite Signal

(b) Frequency Domain Decomposition of the Composite Signal

Fig. 1.11

**Decomposition of Non-periodic Signal:**

- Fig. 1.12 shows a non-periodic composite signal. It can be the signal created by a microphone or a telephone set when a word is pronounced.
- In this case, the composite signal cannot be periodic, because that implies that we are repeating the same word or words with exactly the same done.




(a) Time Domain (b) Frequency Domain

Fig. 1.12

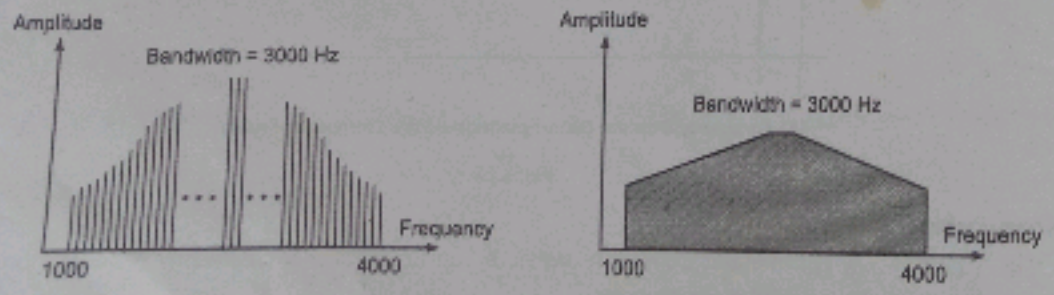
**Bandwidth of a Signal:**

- Bandwidth of a signal is defined as, "the portion of the electromagnetic spectrum occupied by a signal". **OR**

  We can also define the bandwidth of signal as, "the frequency range over which an information signal is transmitted".
- Bandwidth of analog and digital signals are calculated in separate ways; analog signal bandwidth is measured in terms of its frequency (Hz) but digital signal bandwidth is measured in terms of bit rate (bits per second, (bps)).

**1. Bandwidth of Composite Signals:**

- The range of frequencies contained in a composite signal is its bandwidth. It is normally a difference between two numbers.
- For example, if a composite signal contains frequencies between 1000 and 4000, its bandwidth is 4000 – 1000, or 3000.
- The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.
- Fig. 1.13 shows the concept of bandwidth which depicts two composite signals, one periodic and the other non-periodic.
- The bandwidth of the periodic signal contains many discrete frequencies that are integral multiples of the fundamental frequency. The bandwidth of the non-periodic signal has the same range, but the frequencies are continuous.




(a) Bandwidth of a Periodic Signal (b) Bandwidth of a Non-periodic Signal

Fig. 1.13: Bandwidth of Periodic and Non-periodic Composite Signals



**2. Bandwidth of Analog Signal:**

- Bandwidth of an analog signal is expressed in terms of its frequencies. It is defined as, "the range of frequencies that the composite analog signal carries." It is calculated by the difference between the maximum frequency and the minimum frequency.
- The signal shown in the Fig. 1.14 has a minimum frequency of $f_1$ = 30 Hz and maximum frequency of $f_2$ = 90 Hz. Hence, the bandwidth is given by, $f_2 - f_1 = 90 - 30 = 60$ Hz.

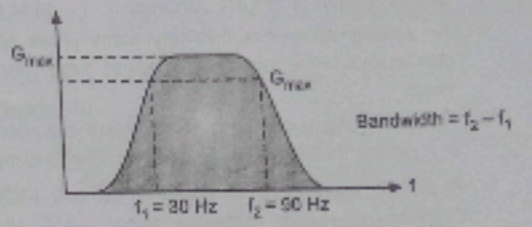



Fig. 1.14: Bandwidth of a Analog signal in Time Domain and Frequency Domain

**3. Bandwidth of a Digital Signal:**

- It is defined as, "the maximum bit rate of the signal to be transmitted". Basically, the bandwidth is the difference between the upper and lower frequency limits of the signal. Each of these signals (voice, music etc. signals) will have its own frequency range and this frequency range of a signal is known as its bandwidth.
- The range of voice signal is 300 Hz to 3400 Hz as shown in Fig. 1.15.

  Therefore, BW (Bandwidth) = $f_2 - f_1$ = 3400 – 300
  = 3100 Hz

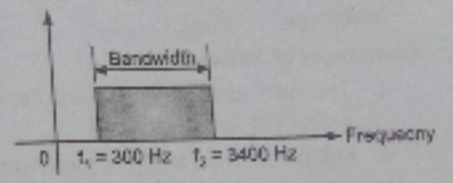



Fig. 1.15: Bandwidth of Voice Signal

**Signal Propagation:**

- Movement of signal through the channel wired or wireless is called as signal propagation. Fig. 1.16 shows a signal source, a communication channel and the destination of signal receiver.
- The signal containing the data or information is in the electric form and it is applied at point X of the conducting medium.
- The electrons in the conducting medium will transfer the charge to the adjacent electrons and the signal at point X gets transferred to Y and then to Z which is the receiving point, (See Fig. 1.16).
- The shape of the signal at the receiver i.e. point Z is almost same as that at the source i.e. point X, but the signal reaches point Z after a finite delay called **propagation delay**.

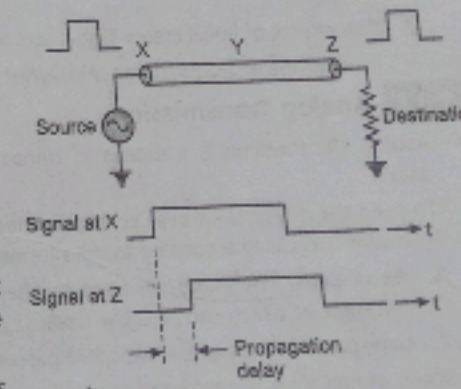



Fig. 1.16: Signal Propagation

- The signal in the Fig. 1.16 producing source can be a person talking on the computer producing a data signal. If we apply a signal at one end of the conducting medium then eventually this signal gets propagated to the other end of the medium.

## 1.3 ANALOG SIGNALS

- An electrical impulse or an electromagnetic wave which travels a distance to convey a message, can be termed as a signal in communication systems.

- A continuous time varying signal, which represents a time varying quantity can be termed as an Analog Signal. Signals which are continuous in time and amplitude are called analog signals.
- An analog signal has infinitely many levels of intensity over a period of time. An analog signal is a continuous wave form that changes smoothly over time. Analog signal is usually represented by sine wave.
- An analog signal can take on any value in a specified range of values. As the wave moves from value A to B, it passes through and includes an infinite number of values along its path.
- A simple example is Alternating Current (AC), which continuously varies between about +110 volts and −110 volts in a sine wave fashion 60 times per second.
- A more complex example of an analog signal is the time-varying electrical voltage generated when a person speaks into a dynamic microphone or telephone.

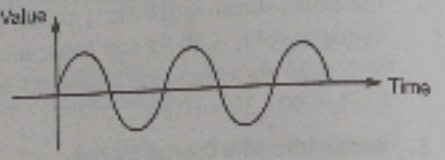


Fig. 1.17: Analog Signal

**Advantages of Analog Signals:**

1. The main advantage is the fine definition of the analog signal which has the potential for an infinite amount of signal resolution.
2. Compared to digital signals, analog signals are of higher density.
3. Analog signals are best suited for the transmission of audio and video.
4. They consumes less bandwidth than digital signals to carry the same information.
5. Analog signal is less susceptible to noise.

**Disadvantages of Analog Signals:**

1. The primary disadvantage of analog signaling is that any system has noise – i.e., random unwanted variation.
2. The effects of noise create signal loss and distortion.
3. Most of the analog systems also suffer from generation loss.

### 1.3.1 Analog Transmission

- Analog transmission is a means of transmitting analog signals, (representing either analog or digital data).
- To send the digital data over an analog media, it needs to be converted into analog signal. There can be following two cases according to data formatting:
  1. **Band-pass:** The filters are used to filter and pass frequencies of interest. A bandpass is a band of frequencies which can pass the filter.
  2. **Low-pass:** Low-pass is a filter that passes low frequencies signals.
- When digital data is converted into a bandpass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into bandpass analog signal, it is called analog-to-analog conversion.
- Analog transmission means of transmitting only analog signals. Data could be analog or digital, signal is always analog. Propagation could be over guided (wire/cable) or unguided medium (space, atmosphere).

#### 1.3.1.1 Digital-to-Analog Conversion

- The process of changing one or more the attributes of analog signal based on information in digital data is referred to as digital-to-analog conversion. It is also called as the modulation of the digital signal.
- Depending on whether the amplitude, frequency or phase of the carrier signal is modified, Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data.



- Fig. 1.18 shows the relationship between the digital information, the digital-to-analog modulating process, and the resultant analog signal. The digital-to-analog conversion is done by modem. Modem stands for modulator and demodulator.
- A modulator uses some coding scheme and converts a digital signal into an analog signal and demodulator converts the analog signal back into the digital signal.

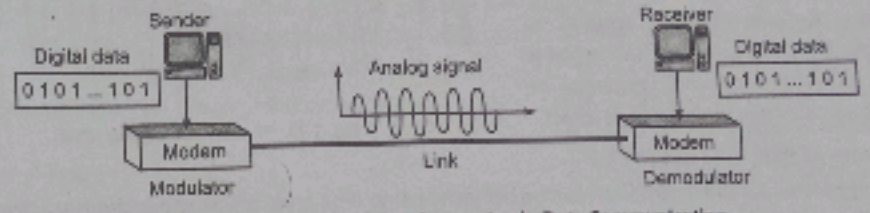


Fig. 1.18: Digital-to-Analog Conversion in Data Communication

- There are three kinds of digital-to-analog conversions possible as given below:

1. **Amplitude Shift Keying (ASK):**

- In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data, (See Fig. 1.19).
- When binary data represents digit 1, the amplitude is held otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

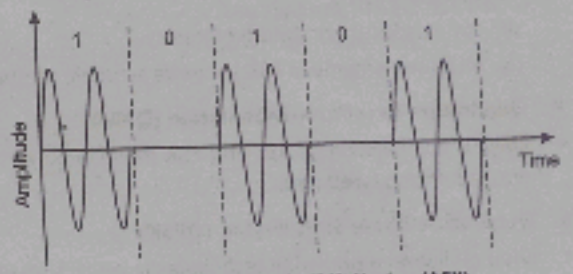


Fig. 1.19: Amplitude Shift Keying (ASK)

**Advantages of ASK:**

(i) Very simple to generate and detect.
(ii) ASK is a relatively low cost modulation technique.

**Disadvantages of ASK:**

(i) ASK is very sensitive to noise.
(ii) ASK has low quality of digital modulation.

2. **Frequency Shift Keying (FSK):**

- In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data, (See Fig. 1.20).
- FSK technique uses two frequencies, $f_1$ and $f_2$. One of them, for example $f_1$, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

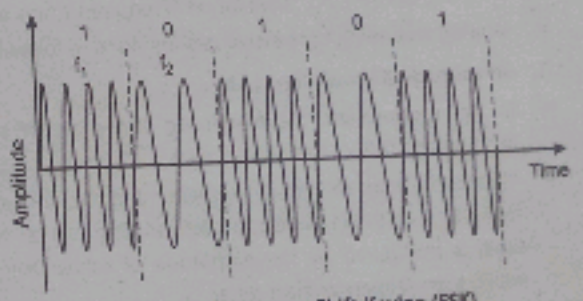


Fig. 1.20: Frequency Shift Keying (FSK)

**Advantages of FSK:**

(i) FSK has better noise immunity than ASK.
(ii) FSK is simple and easy to implement/generate.

**Disadvantages of FSK:**

(i) FSK require high bandwidth.
(ii) FSK is preferred only for the low speed modems.

**3. Phase Shift Keying (PSK):**

- In this conversion technique, the phase of the original carrier signal is altered to reflect the binary data. (See Fig. 1.21).
- When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

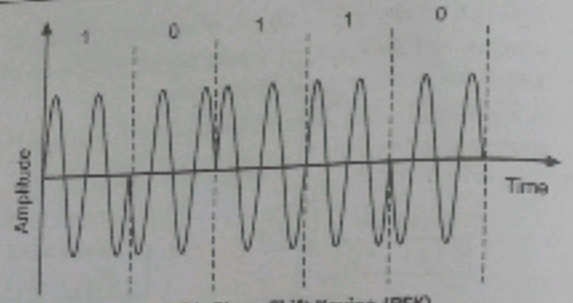



**Fig. 1.21: Phase Shift Keying (PSK)**

**Advantages of PSK:**

(i) High data rate of transmission can be achieved using high level of PSK modulations such as QPSK.

(ii) Efficient modulation technique as compared to ASK and FSK.

**Disadvantages of PSK:**

(i) PSK has lower bandwidth efficiency.

(ii) Multilevel scheme in PSK are more sensitive to phase variations.

**4. Quadrature Amplitude Modulation (QAM):**

- QAM is combination of ASK and PSK modulation techniques and is employed in order to minimize the errors in the received data.

**5. Quadrature Phase Shift Keying (QPSK):**

- It is a multilevel modulation techniques in which four phase shifts are used.
- QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams.
- The serial data is converted into parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

### 1.3.1.2 Analog-to-Analog Conversion

- Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used.
- Analog to analog conversion can be done in following three ways:

**1. Amplitude Modulation (AM):**

- In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.
- Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.
- In AM, the frequency and phase of carrier signal remain unchanged.

***Advantages of AM:***

(i) AM is simple and easy to implement.

(ii) AM waves requires low bandwidth.

(iii) AM waves can be travel in a long distance.

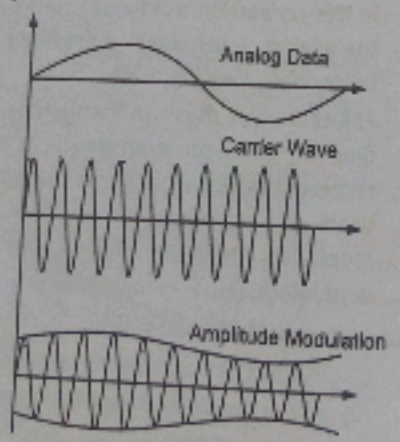



**Fig. 1.22: Amplitude Modulation (AM)**



**Disadvantages of AM:**

(i) AM is not efficient in terms of its use of bandwidth.

(ii) AM signal is not efficient in terms of its power uses.

**2. Frequency Modulation (FM):**

- In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).
- In FM the amplitude and phase of the carrier signal are not altered.

**Advantages of FM:**

(i) FM improves noise immunity.

(ii) FM requires low power for data transmission.

**Disadvantages of FM:**

(i) FM requires very large bandwidth.

(ii) FM has infinite number of data sidebands.

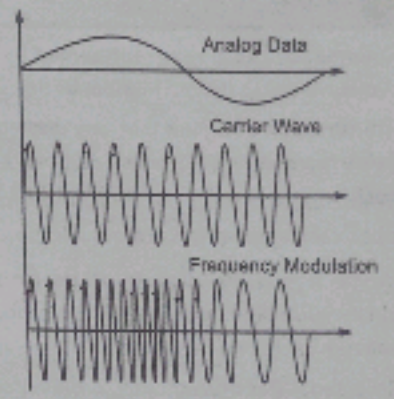



**Fig. 1.23: Frequency Modulation (FM)**

**3. Phase Modulation (PM):**

- In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.
- Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased.
- Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

**Advantages of PM:**

(i) PM increased immunity of noise.

(ii) PM provides higher data transmission rates.

**Disadvantages of PM:**

(i) PM requires more complex receiving hardware.

(ii) PM requires wide bandwidth.




**Fig. 1.24: Phase Modulation (PM)**

**Comparison of AM, FM and PM:**

| Sr. No. | Key Feature | AM | FM | PM |
|---|---|---|---|---|
| 1. | Bandwidth | Low | Wide | Wide |
| 2. | Spectrum complexity | Simple | Complex | Complex |
| 3. | Power efficiency | Poor | Good | Good |
| 4. | Ease of modulation/demodulation | Simple | Difficult | Moderate |
| 5. | Noise resistance | Low | High | High |
| 6. | Applications | Radio and TV broadcasting | Radio and TV | Data communication |

## 1.4 DIGITAL SIGNALS

- Information can also be represented by a digital signal. A digital signal is discrete in nature. Digital signal can have only a limited number of definite values, often as simple as 1 and 0.
- Transmission of signals that vary discretely with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.
- With copper cabling, the variable quantity is typically the voltage or the electrical potential. With fiber-optic cabling or wireless communication, variation in intensity or some other physical quantity is used.
- Digital signals use discrete values for the transmission of binary information over a communication medium such as a network cable or a telecommunications link.
- On a serial transmission line, a digital signal is transmitted 1-bit at a time. A '1' is represented by a positive voltage and a '0' is represented by a zero voltage.

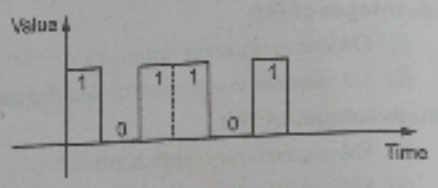



Fig. 1.25: Digital Signal

**Bit Rate:**

- Most digital signals are non-periodic and thus period and frequency are not appropriate characteristics. The term bit rate (instead of frequency) is used to describe digital signals.
- The bit rate is the number of bits sent in 1 second, expressed in bits per second (bps).
- **For example:** Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel? A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is given below:

$$100 \times 24 \times 80 \times 8 = 1,536,000 \text{ bps} = 1.536 \text{ Mbps}.$$

**Bit Length:**

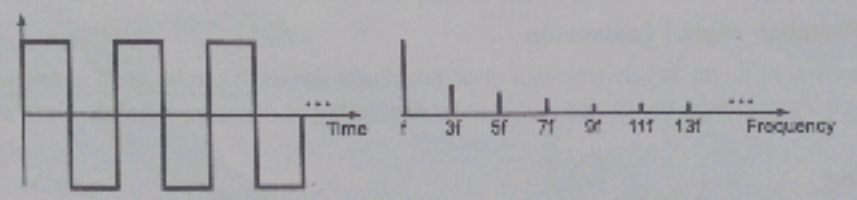
- The wavelength for an analog signal is the distance one cycle occupies on the transmission medium, while in a digital signal is the bit length.
- The bit length is the distance one bit occupies on the transmission medium.

$$\text{Bit Length} = \text{Propagation Speed} \times \text{Bit Duration}$$

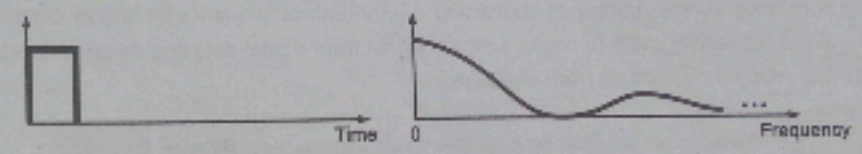
**Digital Signal as a Composite Analog Signal:**

- Based on Fourier analysis, a digital signal is a composite analog signal. The bandwidth is infinite.
- A digital signal, in the time domain, comprises connected vertical and horizontal line segments. A vertical line in the time domain means a frequency of infinity (sudden change in time); a horizontal line in the time domain means a frequency of zero (no change in time).
- Going from a frequency of zero to a frequency of infinity (and vice versa) implies all frequencies in between are part of the domain.
- Fourier analysis can be used to decompose a digital signal. If the digital signal is periodic, which is rare in data communications, the decomposed signal has a frequency domain representation with an infinite bandwidth and discrete frequencies. If the digital signal is non-periodic, the decomposed signal still has an infinite bandwidth, but the frequencies are continuous.






(a) Time and Frequency Domains of Periodic Digital Signal




(b) Time and Frequency Domains of Non-periodic Digital Signal

Fig. 1.26

**Advantages of Digital Signals:**

1. Digital signals are more secure.
2. Digital signals suffer less from noise because any errors can be detected and corrected using regenerators.

**Disadvantages of Digital Signals:**

1. Digital signals need more bandwidth to transmit the same information.
2. The transmitter and receiver have to synchronize very carefully so that the information makes sense.

### 1.4.1 Digital Transmission

- The digital transmission is a means of transmitting digital signals (representing either analog or digital data).
- A data communications network is designed to send information from one point to another and this information needs to be converted into either digital signal or an analog signal for transmission.
- Digital transmission means of transmitting both digital and analog signals. Usually assume the signal is carrying digital (or digitized) data.
- Can only be propagated a limited distance before attenuation distorts the signal and compromises the data integrity. A repeater retrieves the (digital) signal; recovers the (digital) data, e.g., a pattern of 1's and 0's; retransmits a new signal.
- A similar technique used for the analog signal where we assume that the data is digital or digitized; repeater recovers the (digital or digitized) data and amplifies only the data and retransmits.
- Fig. 1.27 shows digital transmission by a repeater.

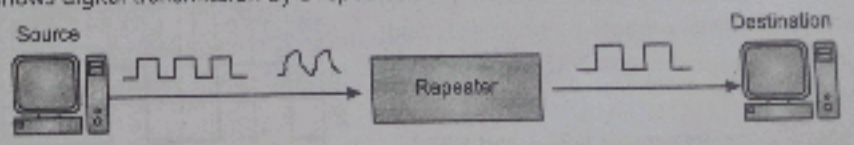



Fig. 1.27: Digital Transmission

- If data is digital, we need to use digital-to-digital conversion techniques, methods which convert digital data to digital signals. If data is analog, we need to use analog-to-digital conversion techniques, methods which change an analog signal to a digital signal.

### 1.4.1.1 Digital-to-Digital Conversion

- This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

**1. Line Coding:**

- The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.
- Line coding is defined as, the process of converting digital data or sequence of bits to digital signals. Encoder is used at the sender's end to create a digital signal from digital data and decoder is used at the receiver's end to recreate digital data from digital signal.

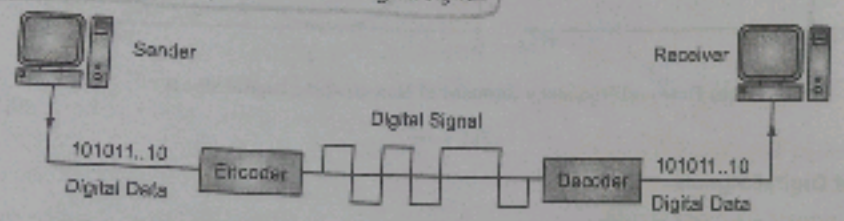



Fig. 1.28

- Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available as explained below:

**(i) Uni-polar Encoding:**

- Uni-polar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted.
- It is also called unipolar-non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.

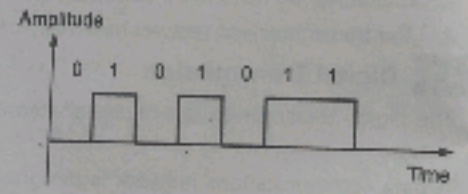



Fig. 1.29: Unipolar Encoding

**(ii) Polar Encoding:**

- Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types as given below:

**(a) Polar Non-Return to Zero (Polar NRZ):**

- It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.
- NRZ scheme has two variants namely, NRZ-L and NRZ-I.
- NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

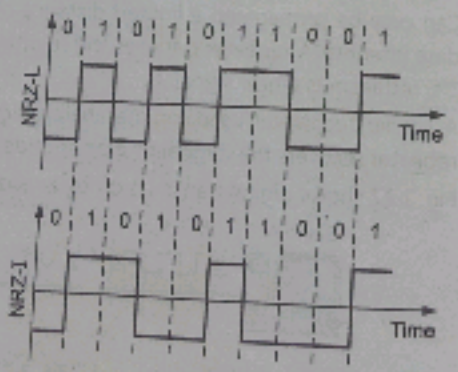



Fig. 1.30: Polar NRZ Encoding



**(b) Return to Zero (RZ):**

- Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.
- RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

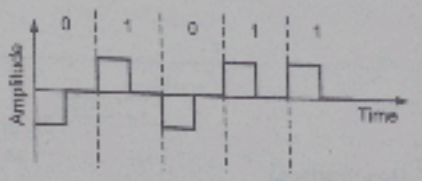



Fig. 1.31: RZ Encoding

**(c) Manchester:**

- This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

**(d) Differential Manchester:**

- This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

**(iii) Bipolar Encoding:**

- Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages.


Fig. 1.32: Bipolar Encoding

**Block Coding:**

- To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.
- Block coding is represented by slash notation, mB/nB. Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps namely Division, Substitution and Combination. After block coding is done, it is line coded for transmission.

### 1.4.1.2 Analog-to-Digital Conversion

- Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog-to-digital conversion.
- Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).
- PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps namely, Sampling, Quantization and Encoding.

**1. Sampling:**

- The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled.
- According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

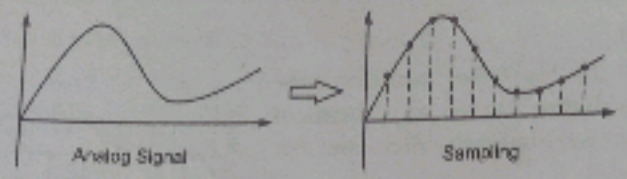



Fig. 1.33: Sampling

2. **Quantization:**

- Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance.

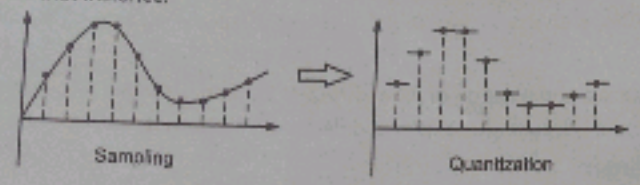



Fig. 1.34: Quantization

- The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

3. **Encoding:**

- In encoding, each approximated value is then converted into binary format.

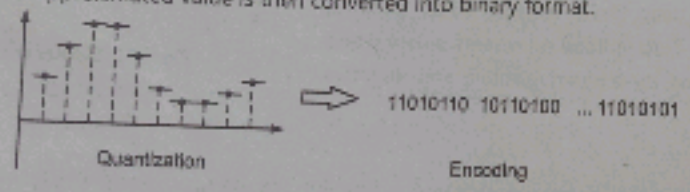
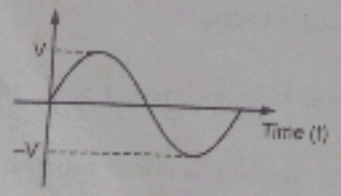
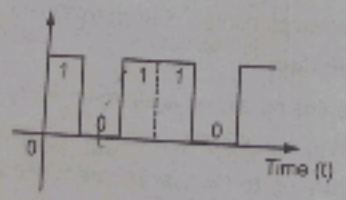



Fig. 1.35: Encoding

- Following table shows difference between analog and digital signals.

| Sr. No. | Terms | Analog Signal | Digital Signal |
|---|---|---|---|
| 1. | Basic | An analog signal is a continuous wave that changes over a time period. | A digital signal is a discrete wave that carries information in binary form. |
| 2. | Signal | Analog signal is a continuous signal which represents physical measurements. | Digital signals are discrete time signals generated by digital modulation. |
| 3. | Representation | An analog signal is represented by a sine wave.   | A digital signal is represented by square waves.   |

Contd..



| | | | |
|---|---|---|---|
| 4. | Description | An analog signal is described by the amplitude, period or frequency, and phase. | A digital signal is described by bit rate and bit intervals. |
| 5. | Range | Analog signal has no fixed range. | Digital signal has a finite range i.e. between 0 and 1. |
| 6. | Example | Human voice in air, analog electronic devices. | Computers, CDs, DVDs, and other digital electronic devices. |
| 7. | Flexibility | Analog hardware is not flexible. | Digital hardware is flexible in implementation. |
| 8. | Uses | Can be used in analog devices only. Best suited for audio and video transmission. | Best suited for Computing and digital electronics. |
| 9. | Applications | Thermometer | PCs, PDAs |
| 10. | Power | Requires large power. | Requires negligible power. |
| 11. | Cost | Low cost and portable. | Cost is high and not easily portable. |
| 12. | Impedance | Low. | High order of 100 megaohm. |
| 13. | Distortion | An analog signal is more prone to distortion. | A digital signal is less prone to distortion. |
| 14. | Adaptability | Are less adaptable to variety of use. | Are more adaptable to variety of use. |
| 15. | Medium of transmission | Wire/wireless. | Wire. |
| 16. | Type of values | Positive/negative (sine wave half cycles). | Positive values only. |
| 17. | Security | Non-encryption. | Encryption. |
| 18. | Capacity/ bandwidth | Low. | High. |
| 19. | Data storage | Stores data in the form of wave signal. | Stores data in the form of binary bits. |
| 20. | Bandwidth | Less bandwidth is require for transmission. | High bandwidth is require for transmission. |

## Practice Questions

1. What is data communication?
2. What is signal? Define it.
3. With the help of diagram describe process of data communication.
4. Describe the term signal propagation.
5. Enlist types of signals.

6. Define the following terms:
   (i) Data communication
   (ii) Message
   (iii) Bandwidth
   (iv) Protocol
   (v) Signal
   (vi) Bit rate.
7. What is periodic and aperiodic signals?
8. Explain the components of data communication with diagram.
9. What is meant by digital and analog signals?
10. State advantages and disadvantages of digital and analog signals.
11. Differentiate between analog and digital signals.
12. What is ASK? Explain in detail.
13. Explain the bandwidth of a signal in data communication.
14. Explain the term digital to analog conversion in detail.
15. Explain the term analog to analog conversion in detail.
16. Explain composite signal with decomposition.
17. Compare periodic and non-periodic signals.
18. Distinguish between analog and digital signals.

Chapter 2...

# Multiplexing and Access Techniques

**Contents**



## 2.0 INTRODUCTION

- Multiplexing is the process of combining multiple signals into one signal, over a shared medium. Multiplexing or (muxing) is a process to combine multiple signals (analog or digital) for transmission over a single line or media.
- Multiplexing (sometimes contracted to muxing) is a method by which multiple analog or digital signals are combined into one signal over a shared medium. In short, multiplexing combines multiple analog or digital signals bound for transmission through a single communication line or computer channel.
- A device that performs the multiplexing is called a multiplexer (MUX), and a device that performs the reverse process is called a de-multiplexer (DEMUX or DMX). Multiplexing methods are Frequency-Division Multiplexing (FDM) Time-Division Multiplexing (TDM) and Wavelength Division Multiplexing (WDM).
- The mechanism for exchange of information between different computer networks and network segments is called switching in networking. Switching is process to forward packets coming in from one port to a port leading towards the destination.

- There are basically three types of switching methods are available namely, Circuit Switching, Packet Switching and Message Switching. Access methods are multiplexing techniques that provide communications services to multiple users in a single-bandwidth wired or wireless medium.
- Communications channels, whether they are wireless spectrum segments or cable connections, are expensive. Communications services providers must engage multiple paid users over limited resources to make a profit.
- Access methods allow many users to share these limited channels to provide the economy of scale necessary for a successful communications business.
- The basic access or multiplexing methods includes Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and so on.

## 2.1 MULTIPLEXING

- Multiplexing is a process in which multiple data channels are combined into a single data or physical channel at the source. Multiplexing divides the physical line (medium) into logical segments called as channels.
- Multiplexing is the process where multiple channels are combined for transmission over a common transmission path.
- Multiplexing is a network that allows a number of simple and inexpensive terminals to share each communication line.

### 2.1.1 Many to One/One to Many

- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Fig. 2.1 shows the basic format of multiplexed system.
- Multiplexing is done using a device called Multiplexer (MUX) that combine n input lines to generate one output line i.e. (many to one).
- At the receiving end a device called Demultiplexer (DEMUX) is used that separate signal into its component signals i.e. one input and several outputs (one to many).
- In multiplexing, different channels carry data simultaneously over the same physical medium. Hardware equipment called multiplexer (or MUX) combine (or multiplexes) the inputs from different sources, and load them on different channels of a medium.
- The combined data traverses over the medium simultaneously. At the destination, a demultiplexer (also called DEMUX) separates (or demultiplexes) the signals and sends them to their different destinations.
- Networks use multiplexing for following two reasons:
  1. To make it possible for any network device to talk to any other network device without having to dedicate a connection for each pair. This requires shared media;
  2. To make a scarce or expensive resource stretch further e.g., to send many signals down each cable or fiber strand running between major metropolitan areas, or across one satellite uplink.
- Demultiplexing is the process of separating multiplexed data channels at the destination. Demultiplex (DEMUX) is the reverse of the multiplex (MUX) process combining multiple unrelated analog or digital signal streams into one signal over a single shared medium, such as a single conductor of copper wire or fiber optic cable.

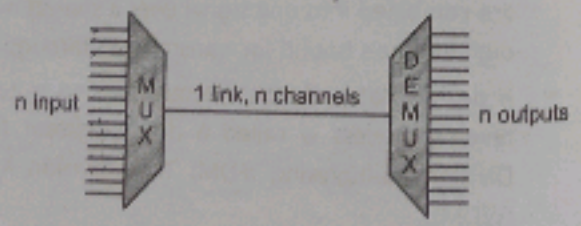



**Fig. 2.1: Multiplexing and Demultiplexing**

- Thus, demultiplex is reconverting a signal containing multiple analog or digital signal streams back into the original separate and unrelated signals.
- Fig. 2.1 shows Multiplexing and Demultiplexing concepts.



- Multiplexing is used in situations where the transmitting media is having higher bandwidth, but the signals have lower bandwidth. Hence there is possibility of sending a number of signals simultaneously. In this situation, multiplexing can be used.
- Multiplexing can be used to achieve the following goals:
  1. To send a large number of signals simultaneously.
  2. To reduce the cost of transmission.
  3. To make effective use of the available bandwidth.
- Multiplexing are of following forms:
  1. **Frequency Division Multiplexing (FDM):** FDM is an analog multiplexing technique that combines analog signals. Each signal is assigned a different frequency
  2. **Time Division Multiplexing (TDM):** TDM is a digital multiplexing technique for combining several low-rate digital channels into one high-rate one. Each signal is assigned a fixed time slot in a fixed rotation
  3. **Wavelength Division Multiplexing (WDM):** WDM is an analog multiplexing technique to combine optical signals. Each signal is assigned a particular wavelength; used on optical fiber.

**Advantages of Multiplexing:**

1. Simple and easy.
2. It reduces number of wires.
3. Large capacities and scalable.
4. It reduces circuit complexity and cost.
5. It simplifies logic design.
6. Inexpensive and signals may have varying speed.

**Disadvantages of Multiplexing:**

1. Complexity.
2. Bandwidth is wasted.
3. Added delays in switching ports.
4. Extra I/O ports required to control the multiplexer.

## 2.2 TYPES OF MULTIPLEXING

- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.
- Whenever, the transmission capacity of a medium linking two devices is greater than the transmission needs of the devices, the link can be shared in order to maximize the utilization of the link, such as one cable can carry a hundred channels of TV.
- Fig. 2.2 shows types of multiplexing.

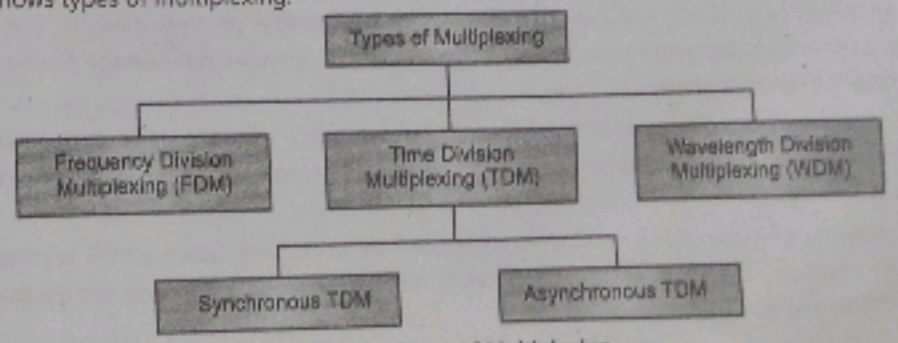



**Fig. 2.2: Types of Multiplexing**

## 2.2.1 Frequency Division Multiplexing (FDM)

- It is most popular and used extensively in radio and TV transmission. Here, the frequency spectrum is divided into several logical channels, giving each user exclusive possession of a particular frequency band. Fig. 2.3 shows basic concept of FDM.

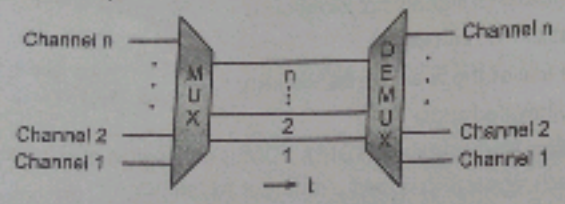



**Fig. 2.3: Basic Concept of FDM**

- Frequency Division Multiplexing (FDM) is a scheme in which numerous signals are combined for transmission on a single communications line or channel. It is analog multiplexing technique. Each signal is assigned a different frequency (sub channel) within the main channel. Its requires channel synchronization. FDM multiplexing technique is based on orthogonality of sinusoids.
- In FDM, signals to be transmitted must be analog signals. Thus digital signals need to be converted to analog form, if they are to use FDM.

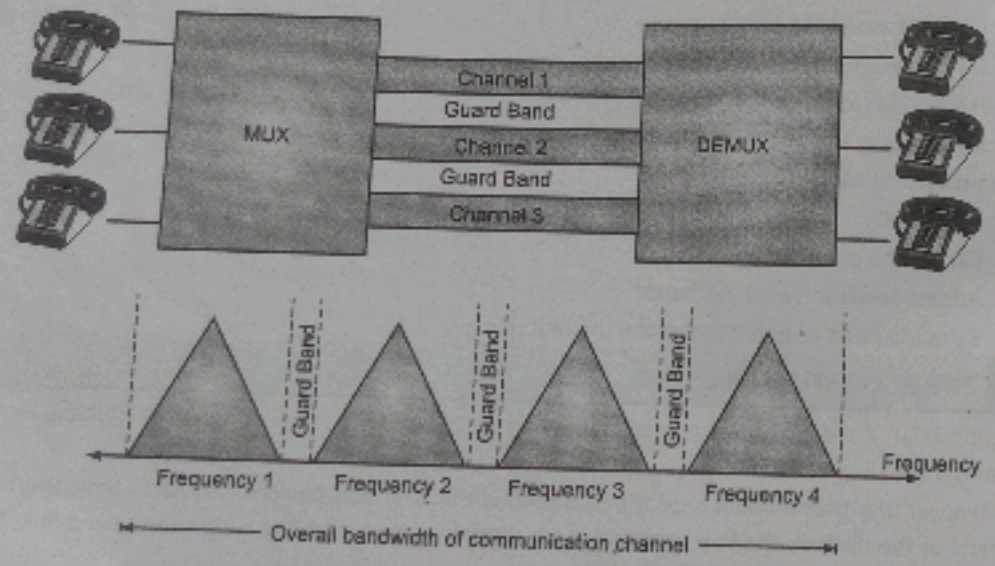
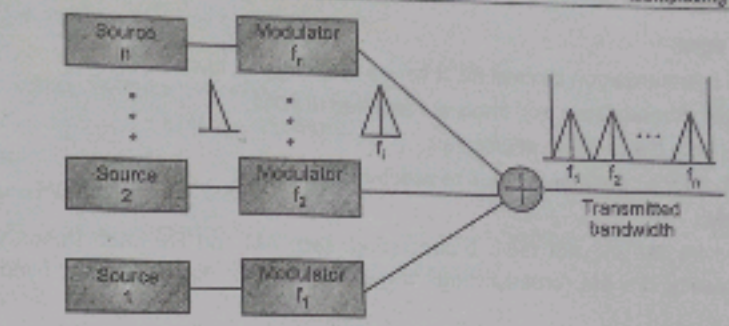


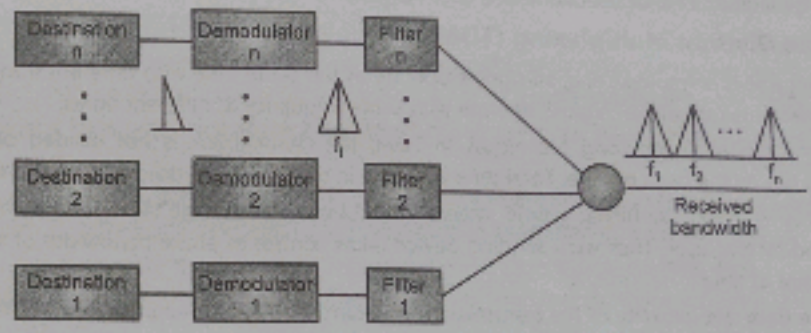

**Fig. 2.4: Frequency Division Multiplexing (FDM)**

- Basic approach is to divide the available bandwidth of a single physical medium into a number of smaller, independent frequency channels. Using modulation, independent message signals are translated into different frequency bands.
- All the modulated signals are combined in a linear summing circuit to form a composite signal for transmission. The carriers used to modulate the individual message signals are called sub-carriers, shown as $f_1$, $f_2$, ..., $f_n$ in Fig. 2.5 (a).
- At the receiving end the signal is applied to a bank of band-pass filters, which separates individual frequency channels. The band pass filter outputs are then demodulated and distributed to different output channels as shown in Fig. 2.5 (b).






**(a) FDM Multiplexing Process**




**(b) FDM Demultiplexing Process**

**Fig. 2.5**

- If the channels are very close to one other, it leads to inter-channel cross talk. Channels must be separated by strips of unused bandwidth to prevent inter-channel cross talk. These unused channels between each successive channel are known as guard bands as shown in Fig. 2.6.
- FDM are commonly used in radio broadcasts and TV networks.

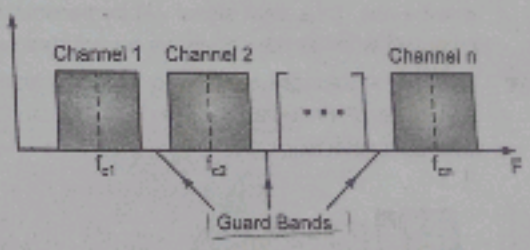



**Fig. 2.6: Use of Guard Bands in FDM**

- A typical analog Internet connection via a twisted pair telephone line requires approximately three kilohertz (3 kHz) of bandwidth for accurate and reliable data transfer.
- Each radio and TV station, in a certain broadcast area, is allotted a specific broadcast frequency, so that independent channels can be sent simultaneously in different broadcast area. For example, the AM radio uses 540 to 1600 KHz frequency bands while the FM radio uses 88 to 108 MHz frequency bands.
- Twisted-pair lines are common in households and small businesses. But major telephone cables, operating between large businesses, government agencies, and municipalities, are capable of much larger bandwidths.

**Advantages of FDM:**

1. In FDM a large number of signals (channels) can be transmitted simultaneously.
2. FDM does not need synchronization between its transmitter and receiver for proper operation.
3. Demodulation of FDM is easy.
4. FDM is inexpensive.

**Disadvantages of FDM:**

1. In FDM the communication channel must have a very large bandwidth.
2. Large number of modulators and filters are required in FDM.
3. FDM suffers from the problem of crosstalk.
4. All the FDM channels get affected due to wideband fading.

**Applications of FDM:**

1. FDM is used for FM and AM radio broadcasting. Each AM and FM radio station uses a different carrier frequency. In AM broadcasting, these frequencies use a special band from 530 to 1700 KHz.
2. FDM is used in television broadcasting.
3. First generation cellular telephone also uses FDM.

## 2.2.2 Time Division Multiplexing (TDM)

- In frequency division multiplexing, all signals operate at the same time with different frequencies, but in Time-division multiplexing all signals operate with same frequency at different times.
- TDM is the digital multiplexing technique. In TDM, the channel/link is not divided on the basis of frequency but on the basis of time. Total time available in the channel is divided between several users.
- Each user is allotted a particular a time interval called time slot or time slice during which the data is transmitted by that user. Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
- In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending or receiving devices.
- In TDM all the signals to be transmitted are not transmitted simultaneously. Instead, they are transmitted one-by-one. Thus, each signal will be transmitted for a very short time. One cycle or frame is said to be complete when all the signals are transmitted once on the transmission channel.
- The TDM system can be used to multiplex analog or digital signals, however it is more suitable for the digital signal multiplexing. The TDM signal in the form of frames is transmitted on the common communication medium.

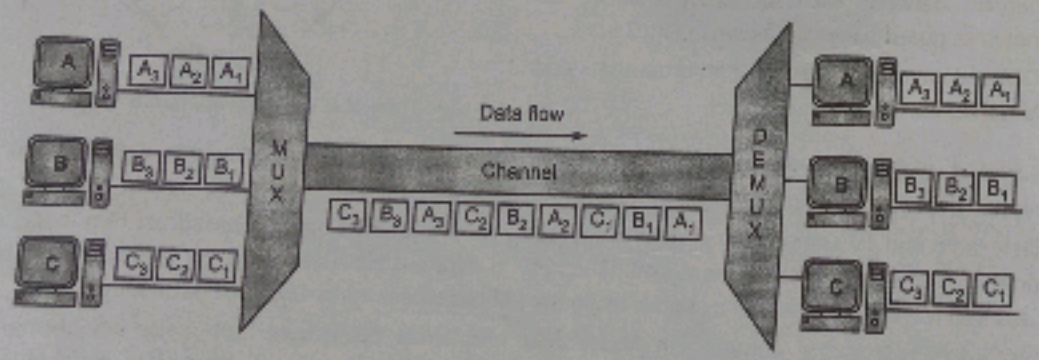



**Fig. 2.7: Time Division Multiplexing (TDM)**

***Advantages of Time Division Multiplexing:***

1. TDM systems are more flexible than FDM.
2. In TDM, the user gets full bandwidth of the channel in a particular time slot.
3. Time division multiplexing circuitry is not complex.
4. Problem of cross talk is not severe.



**Disadvantages of Time Division Multiplexing:**

1. Synchronization is required in time division multiplexing.
2. It is not much suitable for continues signals.
3. IN TDM extra guard time are necessary.
4. Complex to implement.

**Applications of Time Division Multiplexing:**

1. It used in ISDN (Integrated Services Digital Network) telephone lines.
2. It is used in PSTN (public switched telephone network).
3. It is used for some telephone system.
4. It is used in wire line telephone lines.

- Various types of time division multiplexing namely, Synchronous TDM and Asynchronous TDM.

**1. Synchronous TDM (STDM):**

- In synchronous TDM, each device is given same time slot to transmit the data over the link, irrespective of the fact that the device has any data to transmit or not. Hence the name Synchronous TDM.
- Synchronous TDM requires that the total speed of various input lines should not exceed the capacity of path.
- Each device places its data onto the link when its time slot arrives i.e. each device is given the possession of line turn by turn. If any device does not have data to send then its time slot remains empty.
- The various time slots are organized into frames and each frame consists of one or more time slots dedicated to each sending device. If there are n sending devices, there will be n slots in frame i.e. one slot for each device.
- As shown in Fig. 2.8, there are 3 input devices, so there are 3 slots in each frame.

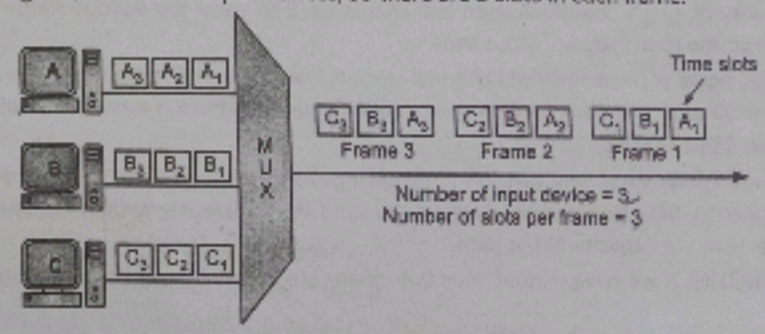



**Fig. 2.8: Synchronous TDM**

**Multiplexing and De-multiplexing Process in STDM:**

- In STDM every device is given the opportunity to transmit a specific amount of data onto the link. Each device gets its turn in fixed order and for fixed amount of time. This process is known as interleaving.
- We can say that the operation of STDM is similar to that of a fast interleaved switch. The switch opens in front of a device; the device gets a chance to place the data onto the link. Such an interleaving may be done on the basis of a bit, a byte or by any other data unit.
- In STDM, the interleaved units are of same size i.e. if one device sends a byte, other will also send a byte and so on.
- As shown in the Fig. 2.9 interleaving is done by a character (one byte). Each frame consists of four slots as there are four input devices. The slots of some devices go empty if they do not have any data to send.
- At the receiver, demultiplexer decomposes each frame by extracting each character in turn. As a character is removed from frame, it is passed to the appropriate receiving device.

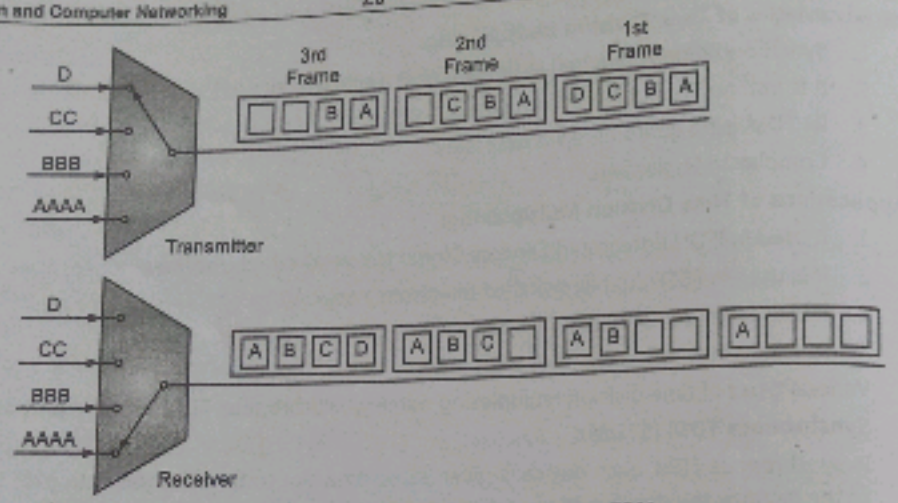



**Fig. 2.9: Multiplexing and Demultiplexing in Synchronous TDM**

**Advantages of Synchronous TDM:**

(i) Relatively simple.
(ii) An order is maintained.
(iii) Commonly used with ISDN (Integrated Services Digital Network).
(iv) No address information is required channel capacity should be large.

**Disadvantages of Synchronous TDM:**

(i) In TDM, the channel capacity cannot be fully utilized.
(ii) The capacity of single communication line that is used to carry the various transmission should be greater than the total speed of input lines.
(iii) If no input signal is present at one channel since a fixed time slot is assigned to each channel, that time slot for that channel does not carry any information and there is wastage of bandwidth.

**2. Asynchronous TDM (ATDM):**

- It is also known as statistical time division multiplexing. Asynchronous TDM is called so because is this type of multiplexing, time slots are not fixed i.e. the slots are flexible. Here, the total speed of input lines can be greater than the capacity of the path.
- In synchronous TDM, if we have n input lines then there are n slots in one frame. But in asynchronous it is not so.
- In asynchronous TDM, if we have n input lines then the frame contains not more than m slots, with m less than n ($m < n$). In asynchronous TDM, the number of time slots in a frame is based on a statistical analysis of number of input lines.

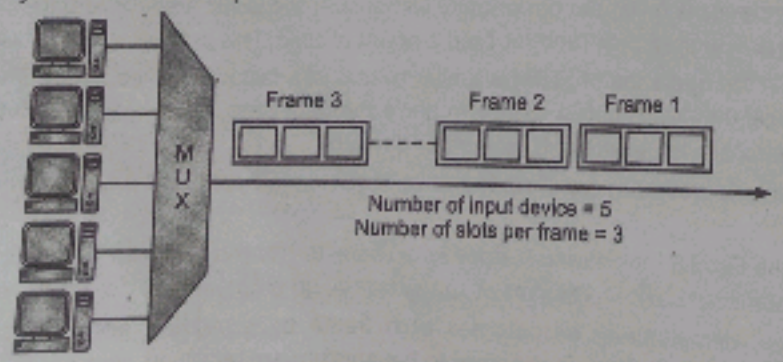



**Fig 2.10: Asynchronous TDM**



- In this system slots are not predefined; the slots are allocated to any of the device that has data to send. The multiplexer scans the various input lines, accepts the data from the lines that have data to send, fills the frame and then sends the frame across the link.
- If there are not enough data to fill all the slots in a frame, then the frames are transmitted partially filled.
- Asynchronous Time Division Multiplexing is depicted in Fig. 2.11. Here we have five input lines and three slots per frame.
  - In Case 1, only three out of five input lines place data onto the link i.e. number of input lines and number of slots per frame are same.
  - In Case 2, four out of five input lines are active. Here number of input line is one more than the number of slots per frame.
  - In Case 3, all five input lines are active.
- In all these cases, multiplexer scans the various lines in order and fills the frames and transmits them across the channel.
- The distribution of various slots in the frames is not symmetrical. In case 2, device 1 occupies first slot in first frame, second slot in second frame and third slot in third frame.

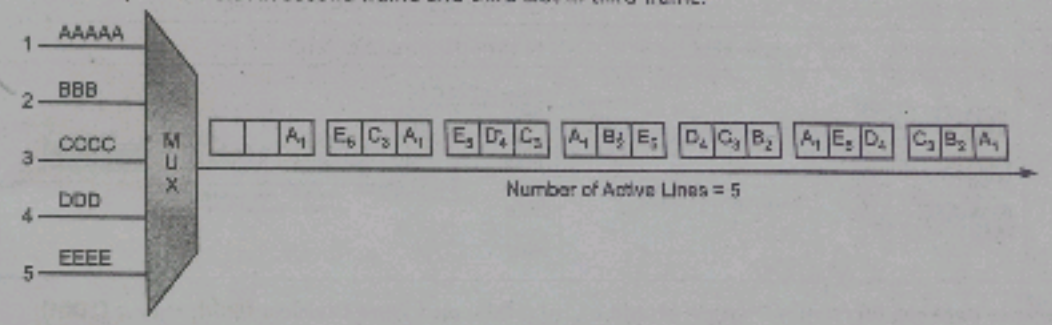



**Fig. 2.11**

**Advantages of ATDM:**

(i) In ATDM code utilization of communication channel.
(ii) TDM circuitry is not very complex.
(iii) Communication link of low capacity is used.
(iv) The problem of crosstalk is not severe.
(v) Full available channel bandwidth can be utilized for each channel.

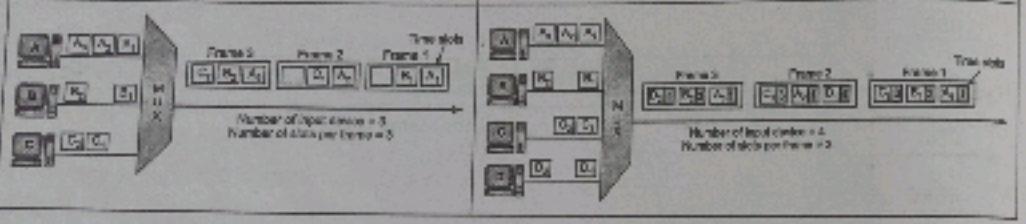
**Disadvantages of ATDM:**

(i) Frames have different sizes.
(ii) Requires buffer.
(iii) Address information is needed.

**Difference between Synchronous TDM and Asynchronous TDM:**

| Sr. No. | Synchronous TDM (STDM) | Asynchronous TDM (ATDM) or Statistical TDM |
|---|---|---|
| 1. | In synchronous TDM, the multiplexer allocates exactly the same slot to each device at all times, whether or not a device has something to transmit in contrast. | In ATDM if the device have nothing to transmit then its time slot is allotted to another device. |

Contd..

| | | |
|---|---|---|
| 2. | STDM requires a common clock signal at both the ends (sender and receiver). | ATDM does not require a common clock. |
| 3. | In synchronous TDM no. of slots in each frame are equal to no. of input lines. | In statistical TDM, no. of slots in each frame are less than the no. of input lines. |
| 4. | In synchronous TDM data flow of each input connection is divided into units and each input occupies one output time slot. | In statistical TDM slots are allotted dynamically. i.e. input line is given slots in output frame if and only if it has data to send. |
| 5. | Buffering is not done, frame is sent after a particular interval of time whether someone has data to send or not. | Buffering is done and only those inputs are given slots in output frame whose buffer contains data to send. |
| 6. | Synchronization bits are used at the beginning of each frame. | No synchronization bits are used. |
| 7. | Maximum bandwidth utilization if all inputs have data to send. | The capacity of link is normally is less than the sum of the capacity of each channel. |
| 8. | Supports high data transfer rate. | Slower data transfer rate. |
| 9. |  | |

**Difference between Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM):**

| Sr. No. | Frequency Division Multiplexing (FDM) | Time Division Multiplexing (TDM) |
|---|---|---|
| 1. | The signals which are multiplexed are added in the time domain. But they occupy different slots in the frequency domain. | The signals which are multiplexed can occupy the entire bandwidth in the time domain. |
| 2. | Synchronization is not required. | Synchronization is required. |
| 3. | FDM is usually preferred for analog signal. | TDM is preferred for digital signal and analog signals. |
| 4. | FDM require complex circuitry. | TDM circuitry is very simple to built. |
| 5. | FDM suffers from the cross talk immunity due to bandpass filter. | TDM is not sensitive for cross talk (noise immunity). |
| 6. | Due to wideband fading in the transmission medium, all the FDM channels are affected. | Only a few TDM channels will be affected due to fading. |
| 7. | Frequency is shared. | Times scale is shared. |
| 8. | Inference is high. | Interference is low. |
| 9. | In FDM total frequency bands are divided into several users e.g., television broad casting. | In TDM total available time is divided into several user e.g., telephone system. |

Contd..



| | | |
|---|---|---|
| 10. | Not Flexible. | TDM provides much better flexibility. |
| 11. | FDM requires guard bands for its operation. | TDM requires sync pulse for its operation. |
| 12. | FDM is less efficient compared to TDM. | TDM is more efficient and is widely used technique in multiplexing. |
| 13. | FDM is used in TV and RADIO broadcasting. | TDM is used in Pulse Code Modulation (PCM). |

### 2.2.3 Wavelength Division Multiplexing (WDM)

- The WDM is a multiplexing technique to combine optical signals. Optical fiber communications use WDM technique, to merge different wavelengths into a single light for communication.
- In short, WDM uses a single fiber to transmit multiple optical signals.
- In WDM, the available fiber-optic transmission channel is shared by a number of different light sources. WDM is conceptually quite similar to FDM.
- A prime application of WDM is the SONET (Synchronous Optical Network) standard developed in North America.
- Optical signals (in the form of light) at different optical wavelengths (colors) are combined by the multiplexer at the transmitter to form a single light to be transmitted through the high-speed fiber-optic cable and the splitting of the light sources is done by demultiplexer at the receiver.
- The combining and splitting of light sources are done by various optical devices, such as prism.
- A prism, which can turn different wavelengths into a single line, can be used at the output of MUX and input of DEMUX.

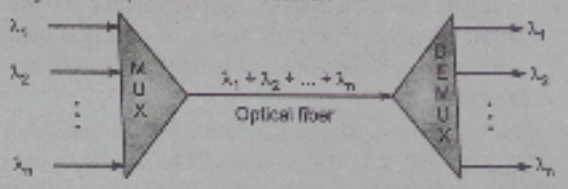



Fig. 2.12: WDM

**Advantages of WDM:**

1. Easier to reconfigure.
2. It provides higher bandwidth.
3. Simple to implement and High security.

**Disadvantages of WDM:**

1. Cost of system increases with addition of optical components.
2. Light wave carrying in WDM are limited to two-point circuit.

## 2.3 APPLICATIONS OF MULTIPLEXING

- Various applications of Multiplexing are given below:

**1. Telephone System:**

- Multiplexing has long been an essential tool of the telephone industry uses both FDM and TDM.

**2. Cable TeleVision (Cable TV):**

- It is a system of delivering television programming to consumers It has long carried multiplexed television channels, and late in the 20th century began offering the same services as telephone companies.
- The cable TV system uses fiber-optic cables to connect and multiplex different cable channels. Coaxial cables coming from individual premises are multiplexed in the junction boxes and converted to optical signals.

- Optical signals at the switching station are multiplexed, using WDM, to create wider bandwidth optical signals.

3. **IPTV (Internet Protocol TeleVision):**

- IPTV is also depends on multiplexing. It the delivery of television content over Internet Protocol (IP) networks.
- IPTV is defined as, multimedia services such as television/video/audio/text/graphics/data delivered over IP based networks managed to provide the required level of quality of service and experience, security, interactivity and reliability.
- IPTV services may be classified into Live television, Video on demand (VoD) and live media etc.

4. **Analog Broadcasting:**

- In FM broadcasting and other analog radio media, multiplexing is a term commonly given to the process of adding subcarriers to the audio signal before it enters the transmitter, where modulation occurs. (In fact, the stereo multiplex signal can be generated using time-division multiplexing, by switching between the two (left channel and right channel) input signals at an ultrasonic rate (the subcarrier), and then filtering out the higher harmonics.)
- Multiplexing in this sense is sometimes known as MPX, which in turn is also an old term for stereophonic FM, seen on stereo systems since the 1960s.

5. **Digital Broadcasting:**

- In digital television systems, several variable bit-rate data streams are multiplexed together to a fixed bitrate transport stream by means of statistical multiplexing. This makes it possible to transfer several video and audio channels simultaneously over the same frequency channel, together with various services.
- This may involve several standard definition television (SDTV) programmes (particularly on DVB-T, DVB-S2, ISDB and ATSC-C), or one HDTV, possibly with a single SDTV companion channel over one 6 to 8 MHz-wide TV channel. The device that accomplishes this is called a statistical multiplexer. In several of these systems, the multiplexing results in an MPEG transport stream.
- The newer DVB standards DVB-S2 and DVB-T2 has the capacity to carry several HDTV channels in one multiplex.

6. **Digital Radio:**

- In digital radio, a multiplex (also known as an ensemble) is a number of radio stations that are grouped together.
- A multiplex is a stream of digital information that includes audio and other data.

7. **Video Processing:**

- In video editing and processing systems, multiplexing refers to the process of interleaving audio and video into one coherent data stream. In digital video, such a transport stream is normally a feature of a container format which may include metadata and other information, such as subtitles.
- The audio and video streams may have variable bit rate. Software that produces such a transport stream and/or container is commonly called a statistical multiplexer or muxer.
- A demuxer is software that extracts or otherwise makes available for separate processing the components of such a stream or container.

## 2.4 DIFFERENT ACCESS TECHNIQUES

- Access techniques are based on multiplexing, that allows several data streams or signals to share the same communication channel or transmission medium.
- In this section we study different access techniques such as TDMA, FDMA, CDMA etc.



### 2.4.1 Frequency Division Multiple Access (FDMA)

- The FDMA channel access scheme is based on the Frequency Division Multiplexing (FDM) scheme, which provides different frequency bands to different data streams.

**Basic Idea:**

- Fig. 2.13 shows basic idea of FDMA.
- In FDMA, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.
- In other words, each band is reserved for a specific station, and it belongs to the station all the time. Each station also uses a bandpass filter to confine the transmitter frequencies. To prevent station interferences, the allocated bands are separated from one another by small guard bands.

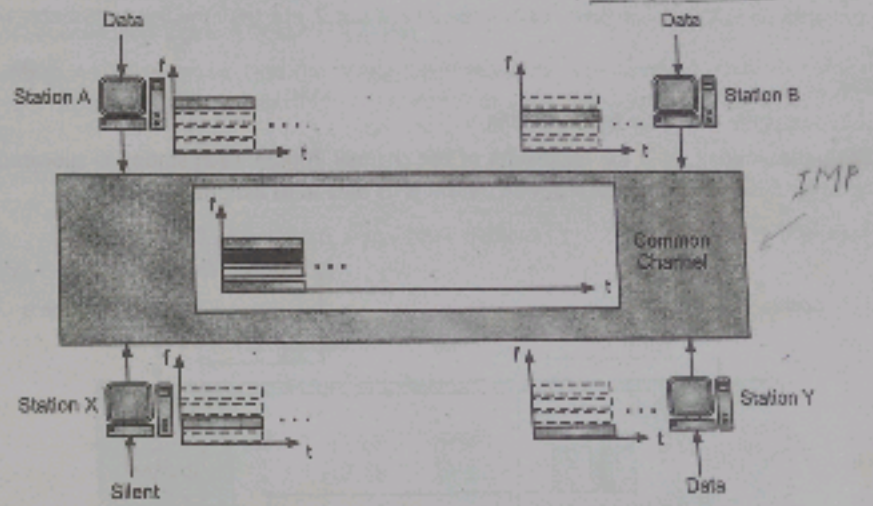



**Fig. 2.13: Concept of FDMA**

- In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands, (See Fig. 2.14).
- FDMA specifics a pre-determined frequency band for the entire period of communication. This means that stream data (a continuous flow of data that may not be packetized) can easily be used with FDMA.

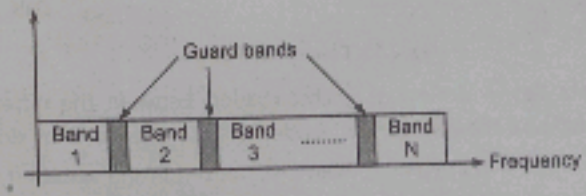



**Fig. 2.14: Channel Bandwidth divided in Bands**

- As shown in Fig. 2.14 there are 'N' bands which are non-overlapping. Each channel is assigned the frequency slot (band) permanently.

**Advantages of FDMA:**

1. In FDMA the channel bandwidth is utilized more efficiently.
2. No synchronization or codeword is required in FDMA.
3. The users in FDMA can transmit continuously without any interruption.

**Disadvantages of FDMA:**

1. Extra guard bands are required in FDMA to avoid interchannel interference.
2. Power efficiency is reduced in FDMA.

**Applications of FDMA:**

1. Used for wireline channels for voice and data transmission.
2. Used in telephone communication.

## 2.4.2 Time Division Multiple Access (TDMA)

- The TDMA channel access scheme is based on the Time Division Multiplexing (TDM) scheme. TDMA provides different time slots to different transmitters in a cyclically repetitive frame structure.
- For example, node 1 may use time slot 1, node 2 time slot 2, etc. until the last transmitter when it starts over.

**Basic Idea:**

- Fig. 2.15 shows the basic idea behind TDMA.
- In TDMA, the stations share the bandwidth of the channel in time. Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot.

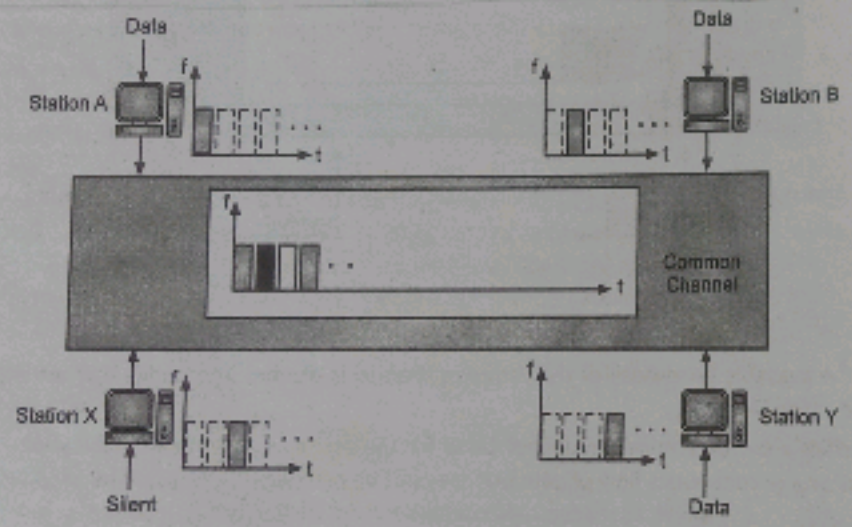



**Fig. 2.15: Concept of TDMA**

- The problem with TDMA lies in achieving synchronization between the different stations and each station in TDMA needs to know the beginning of its slot and the location of its slot.
- This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area. To compensate for the delays, we can insert guard times, (See Fig. 2.16).

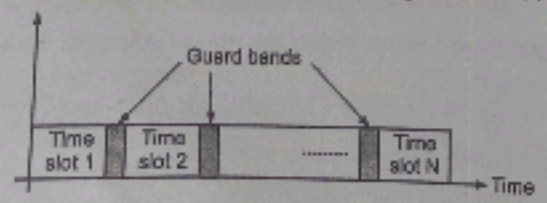



**Fig. 2.16: Time is divided in Slots**



**Advantages of TDMA:**

1. The user in TDMA gets full bandwidth of the channel in a particular time slot.
2. Most suitable technique for digital transmission.

**Disadvantages of TDMA:**

1. TDMA is not much suitable for continuous signals.
2. In TDMA extra guard times are necessary.
3. Synchronization is necessary in TDMA.

**Applications of TDMA:**

1. Used for voice and data transmission.
2. Used for transmission of bursty signals.

## 2.4.3 Code Division Multiple Access (CDMA)

- In CDMA method every user is assigned the unique code sequence. The signal is then spread across the complete frequency band with the help of the code. At the receiver, the signal is recovered with the help of same code.
- Since, the signals in CDMA spread over the complete frequency band, it is also called Spread Spectrum Multiple Access (SSMA).
- Access to the user is given randomly. Hence, signal transmissions from various overlap in time as well as frequency. Fig. 2.17 shows CDMA concept.

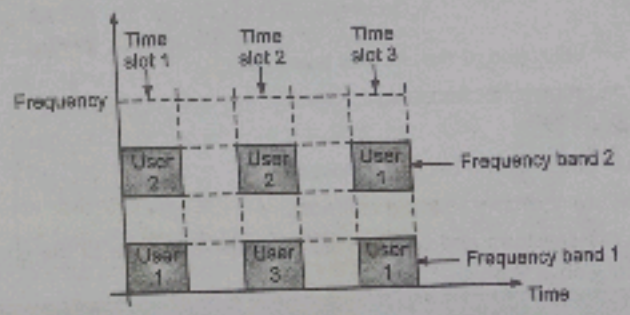



**Fig. 2.17: CDMA Transmission**

**Basic Idea:**

- Let us assume, we have four stations. A, B, X, and Y, connected to the same channel. The data from station A are $d_1$, from station 2 are $d_2$ and so on. The code assigned to the first station is $c_1$, to the second is and so on.
- We assume that the assigned codes have following two properties.
  1. If we multiply each code by another, we get 0.
  2. If we multiply each code by itself, we get 4 (the number of stations).
- With these two properties in mind, let us see how the above four stations can send data using the same common channel, as shown in Fig. 2.18.
- Station A multiplies its data by its code to get $d_1 \cdot c_1$. Station B multiplies its data by its code to get $d_2 \cdot c_2$ and so on. The data that go on the channel are the sum of all these terms, as shown in the box.
- Any station that wants to receive data from one of the other three multiplies the data on the channel by the code of the sender. For example, suppose stations A and B are talking to each other. Station B wants to hear what station A is saying. It multiplies the data on the channel by $c_1$, the code of station A.

- Because $(c_1 \cdot c_2)$ is 4, but $(c_2 \cdot c_1)$, $(c_3 \cdot c_1)$, and $(c_4 \cdot c_1)$ are all 0s, station B divides the result by 4 to get the data from station A. CDMA is based on coding theory and each station is assigned a code, which is a sequence of numbers called chips.

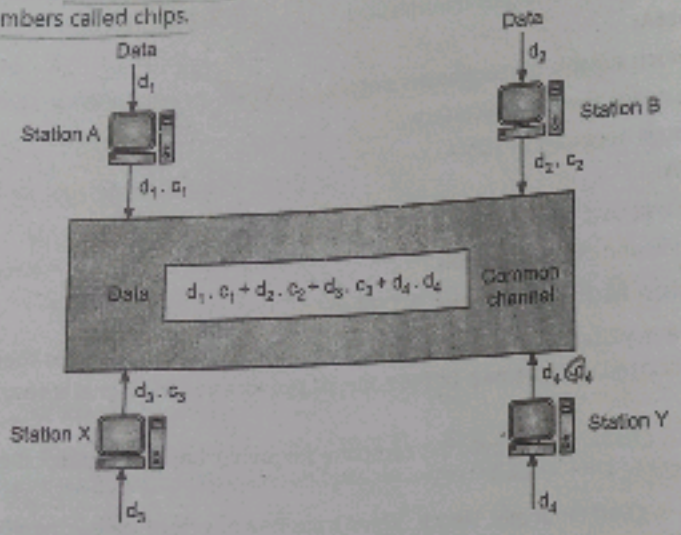



Fig. 2.18: Simple Idea of Communication with Code

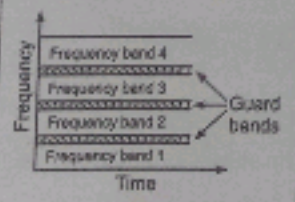
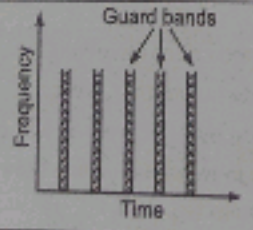
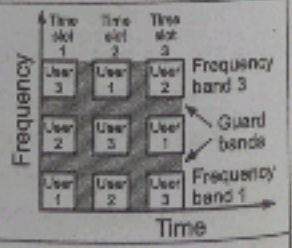
**Advantages of CDMA:**

1. In CDMA, maximum utilization of the channel takes place.
2. In CDMA, synchronization is not necessary.

**Disadvantages of CDMA:**

1. In CDMA Chance of data collision because of overlap.
2. In CDMA Protocols are necessary to avoid collision.

- CDMA also called spread-spectrum and code division multiplexing, one of the competing transmission technologies for digital Mobile Phones.

| Sr. No. | Parameter | FDMA | TDMA | CDMA |
|---|---|---|---|---|
| 1. | Technique | The overall 'bandwidth' of the channel is shared by multiple users. | The 'time' of the channel is shared by multiple users. | The 'time' as well as 'bandwitdh' of the channel is shared by multiple users. |
| 2. | Structure |   |   |   |
| 3. | Code word | No code word is required. | No code is required. | Code words or signature waveforms are required. |
| 4. | Guard times and bands | Guard bands are required. | Guard time are required. | Guard times and bands both are required. |

Contd..



| | | | | |
|---|---|---|---|---|
| 5. | Synchronization | No synchronization is required. | Time synchronization is essential. | No synchronization is required. |
| 6. | Power efficiency | Power efficiency is reduced. | Full power efficiency is possible. | Full power efficiency is possible. |

## 2.4.4 Wideband Code Division Multiple Access (WCDMA)

- WCDMA is a high speed 3G mobile wireless technology with capacity to offer higher data rate than CDMA. WCDMA is the leading 3G wireless standard in the world today.
- WCDMA has the capacity to easily handle bandwidth-intensive applications such as video, data, and image transmission necessary for mobile internet services.
- WCDMA (Wideband Code-Division Multiple Access), an ITU standard derived from Code-Division Multiple Access (CDMA), is officially known as IMT-2000 direct spread.
- WCDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices than commonly offered in today's market.
- WCDMA along with UMTS (Universal Mobile Telecommunications System) IMT-2000 CDMA Direct Spread is an air interface standard found in 3G mobile telecommunications networks.
- WCDMA was adopted as a standard by the International Mobile Telecommunications-2000 (IMT 2000) with the intention to create a global standard for real time multimedia services and international roaming.
- WCDMA is the air interface of the 3G UMTS (Universal Mobile Telecommunications System). The UMTS system has been deployed based on the existing GSM communication Core Network (CN) but with a totally new Radio Access Technology (RAT) in the form of WCDMA. Its radio access is based on FDD (Frequency Division Duplex).
- Current deployments are mainly at 2.1 GHz bands. Deployments at lower frequencies are also possible, such as UMTS900. UMTS supports voice and multimedia services.


Fig. 2.19

**Advantages of WCDMA:**

1. **Service Flexibility:** WCDMA allows each carrier of 5MHz to process mixed service from 8Kbps to 2Mbps. In addition, circuit switched service and packet switched service can be carried out in the same channel, and a single terminal is used to carry out multiple circuit and packet switched services, so as to realize genuine multimedia service. WCDMA supports services with different requirements (such as voice and packet data) and ensures high quality and perfect coverage.
2. **Spectrum Efficiency:** WCDMA can make highly efficient use of available radio spectrums. Because single cell multiplexing is adopted for WCDMA, no frequency planning is needed. Network capacity can be notably improved by using technologies of hierarchical cell structure, adaptive antenna array and coherent demodulation (bidirectional).
3. **Low Power Spectral Density:** As the signal is spread over a large frequency-band, the Power Spectral Density is getting very small, so other communications systems do not suffer from this kind of communications.
4. **Network Scale Economics:** When WCDMA wireless access is added to existing digital cellular network (such as European GSM) and the network is running in two systems, the same core network can be multiplexed and use the same base stations. The latest ATM mode i.e. micro-cell transmission

procedure is used for the links between WCDMA access network and GSM core network. Th method can process highly effective data packets, which can enhance the capacity of standard E1/T lines to 300 voice calls compared to 30 voice calls for that of existing network. It is estimated the about 50% transmission costs can be saved.

5. **Privacy:** Due to unknown random codes in WCDMA. The applied codes are unknown to a hostile user. This means that it is hardly possible to detect the message of another user.

**Disadvantages of WCDMA:**

1. **Cost:** WCDMA femtocells are more costly to develop than GSM, due to the reduced reuse of silicon when compared to a handset (only 15% in WCDMA).
2. **Complexity:** In addition, the components are more complex and thus, the raw materials are more expensive. The handsets are more costly and if carriers are going to offer family-type packages they will need to replace some of the handsets since, invariably, some users will still be on GSM.
3. **Interference:** It is far more difficult to accommodate interference in WCDMA networks.

## 2.4.5 LTE

- The Long-Term Evolution (LTE) is the next evolutionary step beyond 3G for mobile wireless communication.
- LTE is 4G (4th Generation) technology that aimed to provide better quality of service as compare to other 3G and WiMAX technology. LTE offers faster data rate transfer as compare to existing 3G network equipment's by using radio waves over the same bandwidth.
- LTE is the wireless data communications technology and a development of the GSM/UMTS standards. LTE is commonly marketed as 4G LTE and Advance 4G, but it does not meet the technical criteria of a 4G wireless service, as specified in the 3GPP Release 8 and 9 document series for LTE Advanced. LTE is also commonly known as 3.95G.
- LTE was started as a project in 2004 by telecommunication body known as the Third Generation Partnership Project (3GPP).
- LTE evolved from an earlier 3GPP system known as the Universal Mobile Telecommunication System (UMTS), which in turn evolved from the Global System for Mobile Communications (GSM).
- Even related specifications were formally known as the evolved UMTS terrestrial radio access (E-UTRA) and evolved UMTS terrestrial radio access network (E-UTRAN). First version of LTE was documented in Release 8 of the 3GPP specifications.
- A rapid increase of mobile data usage and emergence of new applications such as MMOG (Multimedia Online Gaming), mobile TV, Web 2.0, streaming contents have motivated the 3rd Generation Partnership Project (3GPP) to work on the Long-Term Evolution (LTE) on the way towards fourth-generation (4G) mobile.
- The main goal of LTE is to provide a high data rate, low latency and packet optimized radioaccess technology supporting flexible bandwidth deployments. Same time its network architecture has been designed with the goal to support packet-switched traffic with seamless mobility and great quality of service.

***LTE Network Architecture:***

- LTE network is referred to 4G network. This parallelism is due to higher speed offered by it. This is known as wireless broadband.
- The high-level network architecture of LTE is comprised of following three main components:
  1. User Equipment (UE).
  2. Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
  3. Evolved Packet Core (EPC).



- The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below in Fig. 2.20.

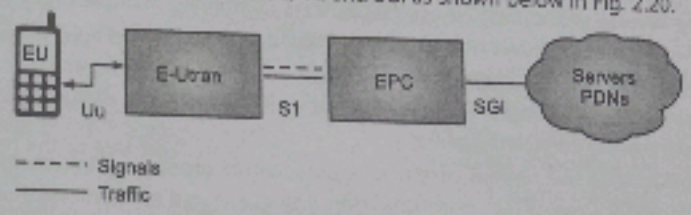



Fig. 2.20: Architecture of LTE

- LTE uses Orthogonal Frequency Division Multiplexing (OFDM) for the downlink i.e., from the base station to the terminal to transmit the data over many narrow band careers of 180 KHz each instead of spreading one signal over the complete 5MHz career bandwidth ie. OFDM uses a large number of narrow sub-carriers for multi-carrier transmission to carry data.
- Orthogonal frequency-division multiplexing (OFDM), is a frequency-division multiplexing (FDM) scheme used as a digital multi-carrier modulation method.
- OFDM meets the LTE requirement for spectrum flexibility and enables cost-efficient solutions for very wide carriers with high peak rates.

**Advantages of LTE:**

1. **Low Latency:** Time required to connect to the network is in range of a few hundred milliseconds and power saving states can now be entered and exited very quickly.
2. **High Throughput:** High data rates can be achieved in both downlink as well as uplink. This causes high throughput.
3. **High Data Rates:** As LTE supports MIMO, higher data rate can be achieved.
4. **FDD and TDD in the Same Platform:** Frequency Division Duplex (FDD) and Time Division Duplex (TDD), both schemes can be used on same platform.
5. **Superior End-user Experience:** Optimized signaling for connection establishment and other air interface and mobility management procedures have further improved the user experience. Reduced latency (to 10 ms) for better user experience.
6. **Seamless Connection:** LTE will also support seamless connection to existing networks such as GSM, CDMA and WCDMA.
7. **Plug and Play:** The user does not have to manually install drivers for the device. Instead system automatically recognizes the device, loads new drivers for the hardware if needed, and begins to work with the newly connected device.
8. **Simple Architecture:** Because of Simple architecture low Operating Expenditure (OPEX).

**Disadvantages of LTE:**

1. **High Cost:** The cost of setup of new network infrastructure and in case of network upgrades; new equipment's will be needed to be installed.
2. **Complex:** LTE network is completely new network which requires skilled users to make it operational.
3. **Additional Equipment:** LTE technology employs MIMO (Multiple Input Multiple Output) technology that raises the need to use additional antennas at network base stations for data transmission.

## 2.5 CONCEPT OF DEMULTIPLEXING AND ITS CIRCUIT

- Demultiplexing is the process of separating multiplexed data channels at the destination. Demultiplexing (DEMUX) is the reverse of the multiplex (MUX) process combining multiple unrelated analog or digital signal streams into one signal over a single shared medium, such as a single conductor of copper wire or fiber optic cable.
- Thus, demultiplex is reconverting a signal containing multiple analog or digital signal streams back into the original separate and unrelated signals.
- Demultiplex (DEMUX) is the reverse of the multiplex (MUX) process – combining multiple unrelated analog or digital signal streams into one signal over a single shared medium, such as a single conductor of copper wire or fiber optic cable.
- In demultiplexing process, we use filters to decompose the multiplexed signal into its constituent component signals. Then each signal is passed to an amplitude demodulation process to separate the carrier signal from the message signal. Then, the message signal is sent to the waiting receiver.
- The process of demultiplexing is shown in the Fig. 2.21.

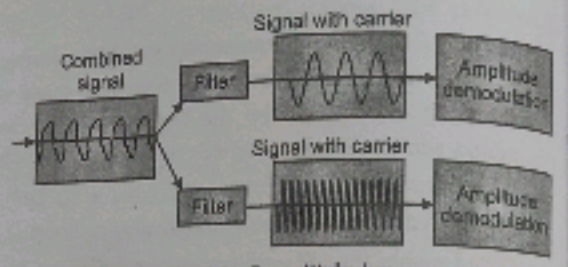



Fig. 2.21: Demultiplexing

**Circuit of Demultiplexer:**

- DEMUX are used to implement general-purpose logic systems. A demultiplexer takes one single input data line and distributes it to any one of a number of individual output lines one at a time. Demultiplexing is the process of converting a signal containing multiple analog or digital signals backs into the original and separate signals. A demultiplexer of $2^n$ outputs has n select lines.
- The demultiplexer is a combinational logic circuit designed to switch one common input line to one of several separate output line.

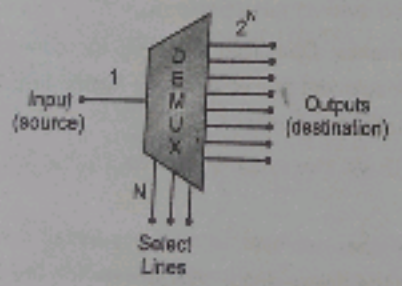



Fig. 2.22: Circuit of Demultiplexer

## 2.6 SWITCHING

- A network consists of many switching devices. In order to connect multiple devices, one solution could be to have a point to point connection in between pair of devices. But this increases the number of connection. The other solution could be to have a central device and connect every device to each other via the central device which is generally known as star topology.
- Both these methods are wasteful and impractical for very large network. The other topology also cannot be used at this stage. Hence, a better solution for this situation is switching.



- A switched network is made up of a series of interconnected nodes called switches.

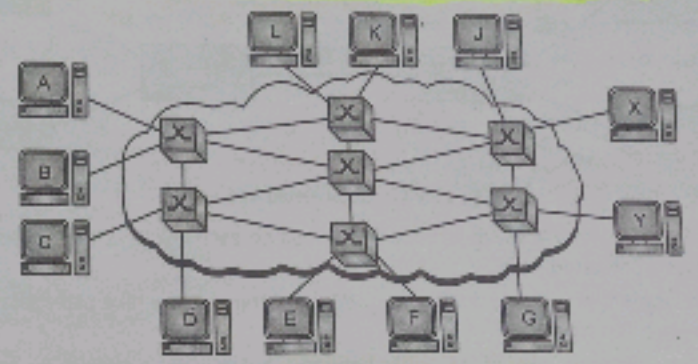



Fig. 2.23

- Switching is used for to send data along different routes. The data sent by sender before reaching its destination travels via numerous equipment's and nodes.
- The process by which these nodes forward data at one of its inputs to one of its outputs is known as switching. Switching is process to forward packets coming in from one port to a port leading towards the destination.

**Types of Switching Techniques:**

- There are basically three types of switching methods are available namely, Circuit Switching, Packet Switching and Message Switching.
- Out of three methods, circuit switching and packet switching are commonly used but the message switching has been opposed out in the general communication procedure but is still used in the networking application.

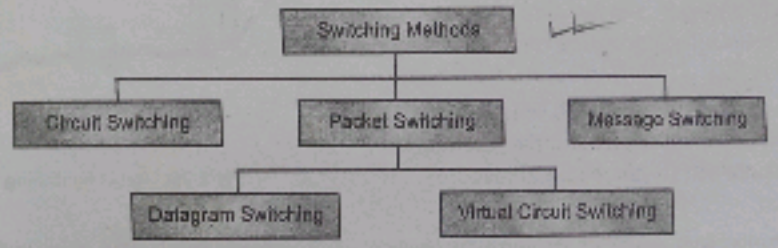



Fig. 2.24: Types of Switching

### 2.6.1 Circuit Switching

- Circuit switched network consists of a set of switches connected by physical links.
- In circuit switched network, two nodes communicate with each other over a dedicated communication path. There is a need of pre-specified route from which data will travel and no other data is permitted. Before starting communication, the nodes must make a reservation for the resources to be used during the communication.
- In this type of switching, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- The end systems, such as telephones or computers are directly connected to a switch. When system A needs to communicate with system B, system A needs to request a connection to system B that must be accepted by all switches as well as by B itself.

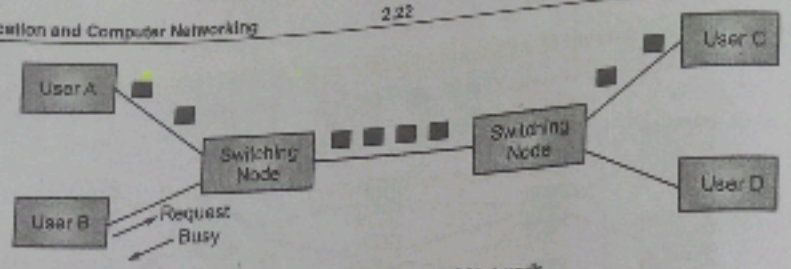



Fig. 2.25: Circuit Switched Network

- This is called as setup phase in which a circuit is reserved on each link, and the combination of circuits or channels defines a dedicated path.
- After the establishment of the dedicated circuit, the data transfer can take place.After all data has been transferred, the circuit is torn down.
- Circuit Switching is generally used in the public networks. It come into existence for handling voice traffic in addition to digital data. However, digital data handling by the use of circuit switching methods are proved to be inefficient.
- The network for circuit switching is shown in Fig. 2.26.
- In circuit switching the routing decision is made when the path is set up across the given network. After the link has been sets in between the sender and the receiver then the information is forwarded continuously over the provided link.
- After the link has been set between sender and receiver, information is forwarded continuously over the link. After the link has set up, no additional address information about receiver is required.
- In circuit switching, a dedicated path is established between sender and receiver which is maintained for entire duration of conversation.
- In circuit switching a dedicated link/path is established across the sender and the receiver which is maintained for the entire duration of conversation.

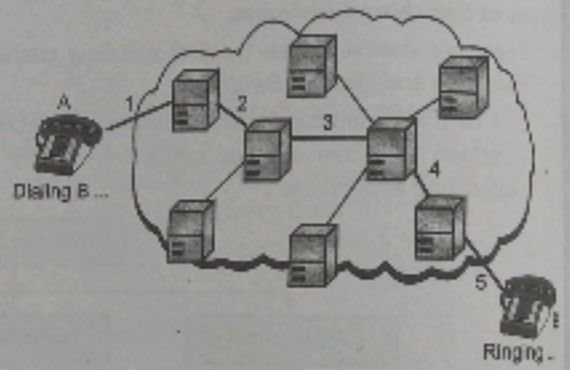



Fig 2.26: Circuit Switching

- Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.
- In circuit switching, routing (selection of path over network) is made when path is setup across the network.
- When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.
- Circuits can be permanent or temporary. Applications which use circuit switching may have to go through three phases:
  1. Establish a circuit,
  2. Transfer the data, and
  3. Disconnect the circuit.



**Advantages of Circuit Switching:**

1. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate.
2. Once, the circuit is established, data is transmitted without any delay as there is no waiting time at each switch.
3. Less expensive.
4. Fixed transit delays and throughput.
5. No loss of packets or out of order packets here as this is connection oriented network unlike packet switched network.

**Disadvantages of Circuit Switching:**

1. As is it designed for voice traffic, it is not suitable for data transmission.
2. Circuit switching usually done using a fixed rate stream (For example, 64 Kbps).
3. Circuit switched network does not provide flow control nor error control.
4. Dedicated channels require more bandwidth.
5. It is more expensive compare to other techniques due to dedicated path requirement.
6. Because connections are not shared, more links must be available to ensure new connections are not blocked.

## 2.6.2 Packet Switching

- In packet switching, messages are divided into packets of fixed or variable size and each of which includes a header with source, destination and intermediate node address information. Individual Packets in packet switching technique take different routes to reach their respective destination.
- By sending a large file in several small chunks over a network, packet switching minimizes the impact of data transmission errors.
- The size of packet is decided by the network and the governing protocol. Resource allocation for a packet is not done in packet switching. Resources are allocated on demand.
- The resource allocation is done on first-come, first-served basis. Each switching node has a small amount of buffer space to hold packets temporarily. If the outgoing line is busy, the packet stays in queue until the line becomes available.

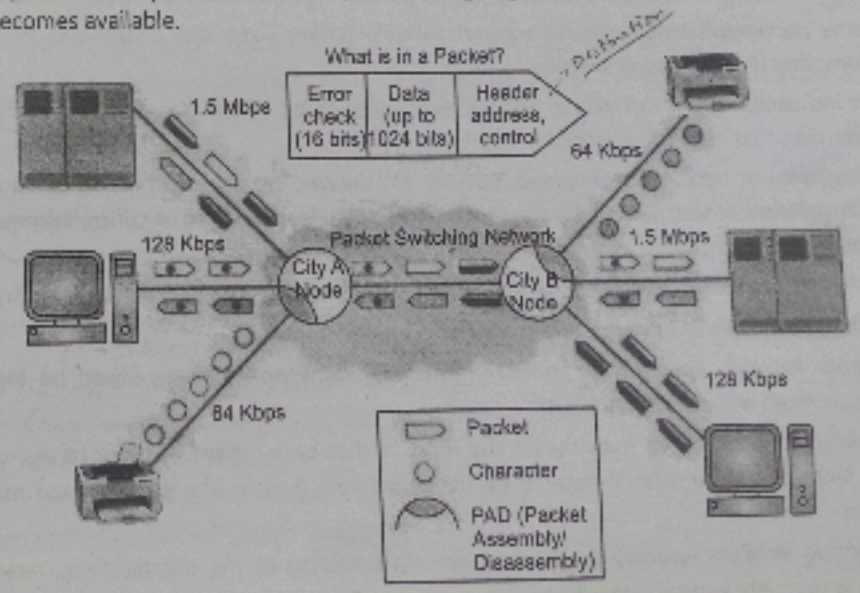



Fig. 2.27: Packet Switching

- The basic example of Packet Switching is the Internet. In Packet Switching, data can be fragmented into suitably-sized pieces in variable length or blocks that are called packets that can be routed independently by network devices based on the destination address contained certain "formatted" header within each packet.
- The packet switched networks allow sender and recipient without reserving the circuit. Multiple paths are existing between sender and recipient in a packet switching network. They does not require a call setup to transfer packets between sender and recipient.

**Advantages of Packet Switching:**

1. Packet Switching use digital network and enables digital data to be directly transmitted toward destination.
2. Better utilization of the network segments in terms of the usage of the network path.
3. Efficient for busty data and efficient used network paths.
4. Computers at each node allow dynamic data routing.
5. In packet switching, the quality of data transmission is kept high (error free).
6. As switching devices do not require massive secondary storage, costs are minimized to great extent. Hence packet switching is very cost effective technique.
7. Packets are rerouted in case of any problems (e.g. busy links or disabled links). This ensures reliable communication.
8. Many users can share the same channel simultaneously. Hence packet switching makes use of available bandwidth efficiently.

**Disadvantages of Packet Switching:**

1. Packet switching network cannot be used in applications requiring very little delay and higher quality of service e.g., reliable voice calls.
2. Protocols used in the packet switching are complex and require high initial implementation costs.
3. Variable transmission delays caused by packet processing and packet queues at packet switches.
4. Some packet-switching networks support variable packet sizes: this contributes to longer packet processing times at packet switches.
5. The inclusion of overhead data in packets means that data transmission efficiency and throughput is lower than that in circuit-switched networks.
6. If the network becomes overloaded, packets are delayed or discarded or dropped. This leads to retransmission of lost packets by the sender. This often leads to loss of critical information if errors are not recovered.
7. It is not secured if security protocols (e.g. IPsec) are not used during packet transmission.

**Connectionless Packet Switching or Datagram Packet Switching:**

- In datagram network, each packet routed individually by network devices based on the destination address contained within each packet.
- Due to each packet is routed individually, the result is that each packet is delivered out-of-order with different paths of transmission, it depend on the networking devices like (switches and routers) at any given time.
- After reaching recipient location, the packets are reassembling to the original form. Datagram packet switching is normally implemented in the network layer. Each packet carries a header that contains the full information about the destination.



- When the switch receives the packet, the destination address in the header of the packet is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

**Advantages of Datagram Packet Switching:**

1. No call setup phase required.
2. More flexible because routing can be used to avoid congested port of the network.
3. Cheaper in cost.

**Disadvantages Datagram Packet Switching:**

1. Packets are forwarded slowly as compare the virtual circuit approach.
2. Processing time request more at node.

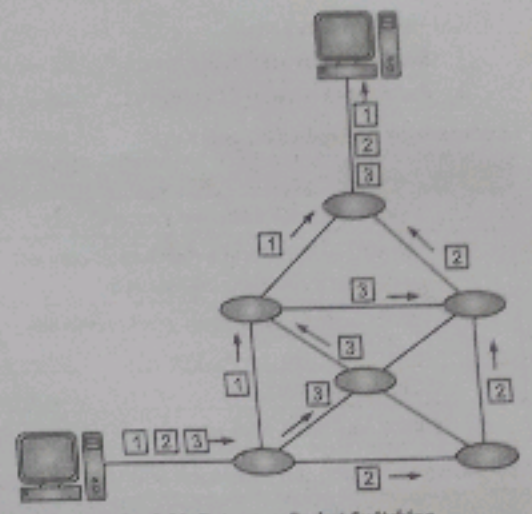


Fig. 2.28: Datagram Packet Switching

**Connection Oriented Packet Switching or Virtual Circuit Packet Switching:**

- In this type of Networking packets are send in sequential order over a defined route. Virtual circuit packet switching is normally done at the data link layer.
- Virtual circuit packet switching establishes a fixed path between a source and a destination to transfer the packets.
- A source and destination have to go through three phases in a virtual circuit packet switching:
  1. Setup phase.
  2. Data transfer phase.
  3. Connection release phase.
- A logical connection is established when a sender sends a setup request to the receiver and the receiver sends back an acknowledgement to the sender if the receiver agree.
- All packets belonging to the same source and destination travel the same path. The information is delivered to the receiver in the same order as transmitted by the sender.

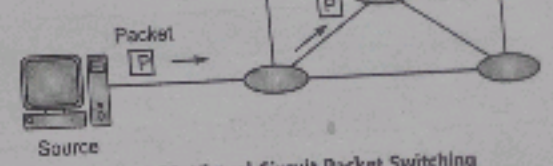



Fig. 2.29: Virtual Circuit Packet Switching

**Advantages of Virtual Packet Circuit Switching:**

1. Virtual circuit provides packet sequencing and error control.
2. Packet forwarding is fast and quick.
3. Multiple packets send by the same source to same destination.

**Disadvantages of Virtual Packet Circuit Switching:**

1. Loss of a node losses all circuits through that node so its is less reliable.
2. Less flexible than other approaches.
3. Cost is high than datagram approach.

**Virtual Circuit Approaches:**

1. **Switched Virtual Circuit (SVC):** SVC format is comparable to dial up lines in circuit switching.
2. **Permanent Virtual Circuit (PVC):** These are comparable to leased line in circuit switching.

**Comparison between SVC and PVC:**

| Sr. No. | SVC | PVC |
|---|---|---|
| 1. | SVC stands for Switched Virtual Circuit. | PVC stands for Permanent Virtual Circuit. |
| 2. | In SVC a source and a destination connect when data are being transferred. | In PVC a source and a destination may choose to have a PVC. |
| 3. | SVC creates a temporary short connection. | PVC creates a permanent and continuous connection. |
| 4. | Cheapest in cost. | Cost is high. |
| 5. | Examples: ATM, X.25, etc. | Examples: Frame Relay, X.25, etc. |

**Comparison of Datagram Approach and Virtual Circuit Packet Switching:**

| Sr. No. | Datagram Packet Switching | Virtual Circuit Packet Switching |
|---|---|---|
| 1. | All packets are free to go to any path on any intermediate router which is decided on the go by dynamically changing routing tables on routers. | First packet goes and reserves resources for the subsequent packets which as a result follow the same path for the whole connection time. |
| 2. | More flexible because of routing can be used to avoid congested port of the network. | Less flexible. |
| 3. | Slow in packet forwarding. | Packets are forwarded quickly. |
| 4. | More reliable. | Less reliable because loss of node losses all circuit through that node. |
| 5. | It is connectionless service. | It is connection-oriented service. |
| 6. | No circuits or path established. | Virtual circuit is established between source and destination before data transfer. |
| 7. | Out of order. | Sequential type of delivery. |
| 8. | No resource allocation required. | Resources are allocated on demand. |
| 9. | Unreliable. | Virtual circuits are highly Reliable. |
| 10. | Unpredictable delay. | High delay. |
| 11. | Example: Internet. | Example: X.25, Frame Relay. |
| 12. | Implementation is easy and cost efficient. | Implementation of virtual circuits is costly. |

## 2.6.3 Message Switching

- In message switching, it is not necessary to establish a dedicated path between transmitter and receiver.
- In this, each message is routed independently through the network. Each message carries a header that contains the full information about the destination.
- Each intermediate device receives the message and store it until the nest device is ready to receive it and then this message is forwarded to the next device. For this reason, a message switching network is sometimes called as Store and Forward Switching.



- Message switching is very slow because of store-and-forward technique. Message switches can be programmed with the information about the most efficient route as well as information regarding to the near switches that can be used for forwarding the present message to their required destination.

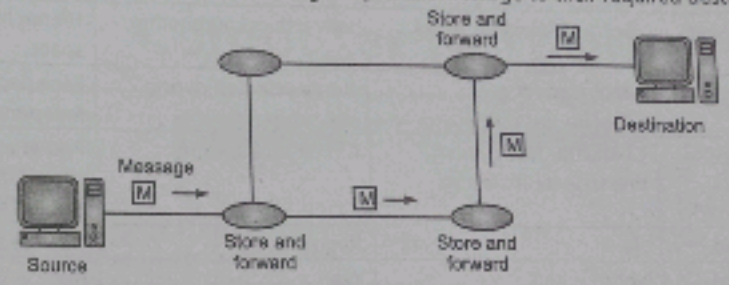



**Fig. 2.30: Message Switching**

- The storing and Forwarding introduces the concept of delay. For this reasons this switching is not recommended for real time applications like voice and video.

**Advantages of Message Switching:**

1. As more devices share the same channel simultaneously for message transfer, it has higher channal efficiency compare to circuit switching.
2. In this type, messages are stored temporarily en-route and hence congestion can be reduced to greater extent.
3. It is possible to incorporate priorities to the messages as they use store and forward technique for delivery.
4. It supports message lengths of unlimited size.
5. It does not require physical connection between source and destination devices unlike circuit switching.

**Disadvantages of Message Switching:**

1. The method is costly as store and forward devices are expensive. This is due to large storage disks requirements to store long messages for long duration.
2. Message switching type does not establish dedicated path between the devices. As there is no direct link between sender and receiver, it is not reliable communication.
3. This switching type is not compatible for interactive applications such as voice and video. This is due to longer message delivery time.

**Difference between Message Switching, Packet Switching and Circuit Switching:**

| Sr. No. | Parameter | Message Switching | Circuit Switching | Packet Switching |
|---|---|---|---|---|
| 1. | Concept | In message switching, each switch stores the whole message and forwards it to the next switch. Although, we don't see message switching at lower layers, it is still used in some applications like electronic mail (e-mail). | When you or your computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called circuit switching. | With this technology, packets are sent as soon as they are available. |

Contd.

| | | | | |
|---|---|---|---|---|
| 2. | Store and forward transmission | Yes. | No. | Yes. |
| 3. | Addressing | Geographical addresses. | Hierarchical numbering plan. | Hierarchical address space. |
| 4. | Routing | Manual routing. | Route selected during call setup. | Each packet routed independently. |
| 5. | Multiplexing | Character multiplexing, message multiplexing. | Circuit multiplexing. | Packet multiplexing shared media across networks. |
| 6. | Call setup | No. | Required. | Not needed. |
| 7. | Dedicated physical path | Not required. | Yes. | No. |
| 8. | Bandwidth available | -- | Fixed. | Dynamic. |
| 9. | Application | Telegraph network for transmission of telegrams. | Telephone network for bidirectional, real time transfer of voice signals. | Internet for datagram and reliable stream service between computers. |
| 10. | End Terminal | Telegraph, Teletype. | Telephone, modem. | Computer. |
| 11. | Information Type | Morse, Baudot, ASCII. | Analog voice or PCM digital voice. | Binary Information. |
| 12. | Transmission system | Digital data over different transmission media. | Analog and Digital data over different transmission media. | Digital data over differential transmission media. |

## Practice Questions

1. What is multiplexing?
2. Explain circuit switching with example.
3. What is packet switching? State its advantages and disadvantages.
4. Write short note on: Message switching.
5. What is meant by switching?
6. What are the types of multiplexing?
7. Explain the term FDM in detail.
8. What is TDM?
9. Explain datagram and virtual circuit networks in detail.
10. What are the types of TDM?
11. Define the terms: (i) Multiplexing, (ii) Switching.
12. Explain WDM in detail.
13. With the help of diagram describe TDM.
14. Compare FDM and TDM.
15. Compare circuit, packet and message switching.
16. Explain FDMA in detail.
17. What is TDMA? State its advantages and disadvantages.
18. Describe CDMA diagrammatically.
19. Write short note on: LTE.

❖❖❖

*Chapter* **3...**

# Computer Network

**Contents**



## 3.0 INTRODUCTION TO COMPUTER NETWORK

- The world is surging toward a digital revolution where computer networks mediate every aspect of modern life, from paying bills to buying real estate, and from reading a book to watching a film.
- Continued growth of the global Internet is one of the most interesting and exciting phenomena in networking. Just over twenty years ago, the Internet was a research project that involved a few dozen sites. Today, the Internet has grown into a production communication system that reaches hundreds of millions of web sites.
- The processing of all types of digital information signals with the help of digital computers has revolutionized the concept of information exchange. Today, the entire world is brought closer by the global computer networking. This has made the job of disseminating information faster and more efficient.
- A group of computers and other devices such as printers, modems etc., connected together is called a network. The interconnected computers can share resources, which called networking.
- Networking is linking of two or more different entities together to form a group or network to perform some specific task. A computer network provides the facility of information exchange/transfer among the computers, connected to it.

## 3.1 NETWORKS

- A network is nothing more than two or more computers connected by a cable or by a wireless radio connection so that they can exchange information.
- A network is a set of devices, (often referred to as nodes) connected by communication media links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- The links connecting the devices are often called communication channels. The term channel refers to a communication path between two communicating devices. It can be either refer to the physical medium (wire/cables).

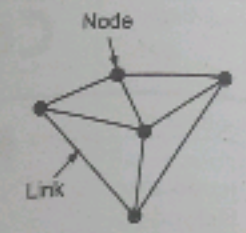



**Fig. 3.1: A Typical Network**

- A network provides the ability of resource sharing to its users such that users of any computers (working under any environment) connected via a network can access the data, programs, resources (hard disks, printers, modems, etc.), peripheral devices, electronic mail (e-mail), software, etc., regardless of their physical locations.

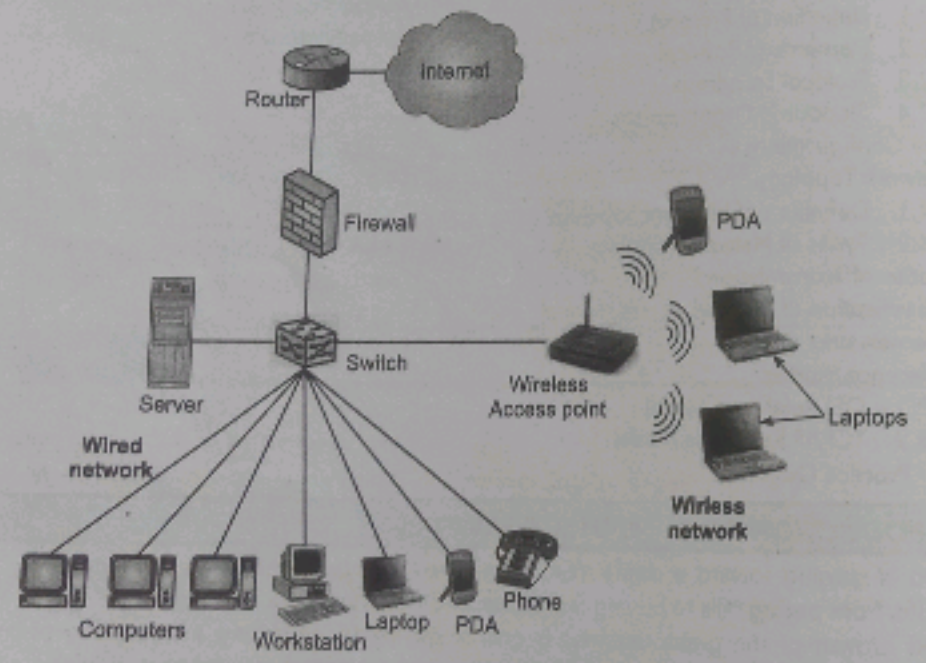



**Fig. 3.2: Computer Network (Wired and Wireless)**

- **Network services** are the thing that a network can do. The major networking services are:
  1. ***File Services:*** This includes file transfer, storage, data migration, file update, synchronization and achieving.
  2. ***Printing Services:*** This service produces shared access to valuable printing devices.
  3. ***Message Services:*** This service facilitates email, voice mails and coordinate object oriented applications.
  4. ***Application Services:*** This services allows to centralize high profile applications to increase performance and scalability.
  5. ***Database Services:*** This involves coordination of distributed data and replication.



### 3.1.1 Definition of Computer Network

- "Two or more computers connected together through a communication media (coaxial cable, fiber optics or satellite) is called as computer network". **OR**
- A computer network is defined as, "a set of electronically connected computers which can share information and resources among themselves". **OR**
- A network as, "an interconnected collection of autonomous computers". Two computers are said to be interconnected if they are capable of exchanging information.

### 3.1.2 Need of Computer Network

- A computer network, often simply referred as network, is a collection of computers and devices connected by communication channels that facilitate communication among users and allow users to share resources with other users.
- Computer networking is the very important and crucial part of Information Technology (IT). Millions of computers are networked together to form the Internet.
- Networking plays an important role in every kind of organization form small to medium sized, in banks, multinational companies, stock exchanges, airports, hospitals, police stations, post offices, colleges, universities and even in the home in short networking plays an important role everywhere where computers are used.
- We need computer network for following reasons:
  1. Sharing of information and data over the geographically wide areas.
  2. Communication from one computer to the other computer.
  3. Sharing the resources such as printers among the network users.
  4. Exchange of data and information amongst the data and users, via the network.
  5. Sharing of expensive software's and database.

### 3.1.3 Characteristics of Computer Network

- The following characteristics should be considered in computer network design and ongoing maintenance:
  1. **Availability:** Availability is typically measured in a percentage based on the number of minutes that exist in a year. Therefore, uptime would be the number of minutes the network is available divided by the number of minutes in a year.
  2. **Cost:** Includes the cost of the network components, their installation, and their ongoing maintenance.
  3. **Reliability:** Defines the reliability of the network components and the connectivity between them. Mean Time Between Failures (MTBF) is commonly used to measure reliability.
  4. **Security:** Includes the protection of the network components and the data they contain and/or the data transmitted between them.
  5. **Speed:** Includes how fast data is transmitted between network end points, (the data rate).
  6. **Scalability:** Defines how well the network can adapt to new growth, including new users, applications, and network components.
  7. **Topology:** Describes the physical cabling layout and the logical way data moves between components.
  8. **Integration:** All the components of the network work in a coordinated manner for a seamless user experience.
  9. **Sharing:** Computer networks enable sharing of files, software, hardware resources and computing capabilities.

### 3.1.4 Components of Computer Network

- Computer networks components comprise both physical parts as well as the software required for installing computer networks, both at organizations and at home.
- The hardware components are the server, client, peer, transmission medium, and connecting devices. The software components are operating system and protocols.
- There are different components of a computer network. The most essential components of a simple network are listed below:

1. **Server:** Servers are high-configuration computers that manage the resources of the network. Servers are faster computers that run various software's, store and process information and also provide a human interface for the users to be able to use the networked computers. The basic function of a server is that provides services to the other computers on the network.
2. **Client:** Computer that uses the services that a server provides. Clients are computers that request and receive service from the servers to access and use the network resources. The client is less powerful than server.
3. **Nodes:** Nodes are the computers on the network, which are provided to the users to carry out their tasks using the network.
4. **Transmission Media:** A physical connection between the devices on a network. Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fiber optic cables etc., or unguided media like radio waves, microwaves, infra-red waves etc.
5. **Network Adopter:** Network adopter or Network Interface Card (NIC) is a circuit board with the components necessary for sending and receiving data. It is plugged into one of the available slots on the PC and transmission cable is attached to the connector on the NIC.
6. **Network Operating System (NOS):** The network requires some software to control all the information transfer activity on the network, like the traffic police to control the traffic. The software called NOS handles these tasks. Networks, which are more complex, require network devices like hubs, switches and routers to carry out different network function.
7. **Resources:** Anything available to a client on the network is considered as a resource. Printers, data, fax devices and other network devices and information are resources.
8. **User:** Any person that uses a client to access resources on the network.
9. **Protocols:** A protocol is a rule or guideline followed by each computer for data communication. A network protocol is usually an agreed-upon or standardized set of rules used for transmitting data and/or establishing communication between them. Protocols are the languages that computers use to talk to each other on a network.
10. **Connecting Devices:** Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are Routers, Bridges, Hubs, Repeaters, Gateways, Switches etc.

### 3.1.5 Advantages and Disadvantages of Computer Network

- **Advantages of Computer Network:**

1. **File Sharing:** The major advantages of a computer network is that allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he/she is authorized.
2. **Resource Sharing:** A computer network provides a cheaper alternative by the provision of resource sharing. All the computers can be interconnected using a network, and just one modem and printer can efficiently provide the services to all users.



3. **Inexpensive Set-up:** Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses.
4. **Flexible Handling:** A user can log on to a computer anywhere on the network and access his/her files. This offers flexibility to the user as to where he/she should be during the course of his/her routine.
5. **Increased Storage Capacity:** Since, there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent.
6. **Easy Communication:** It is very easy to communicate through a network. People can communicate efficiently using a network with a group of people. They can enjoy the benefit of emails, instant messaging, telephony, video conferencing, chat rooms, etc.
7. **Speed:** Sharing and transferring files within networks is very rapid (fast), depending on the type of network. This will save time while maintaining the integrity of files.
8. **Flexible Access:** Access of files from computers throughout the world, and 24 × 7 environment.

- **Disadvantages of Computer Network:**

1. **Security Concerns:** One of the major drawbacks of computer networks is the security issues that are involved.
2. **Expensive to Build:** Building a network is a complex and time consuming for large scale organizations.
3. **Virus and Malware:** Viruses can spread on a network easily, because of the inter-connectivity of workstations.
4. **Lack of Robustness:** If the main file server of a computer network breaks down, the entire system or network becomes useless.
5. **Needs an Efficient Handler:** The technical skills and knowledge required to operate and administer a computer network.
6. **Lack of Independence:** Since, most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.

### 3.1.6 Applications of Computer Network

- Various applications of computer networks are listed below:

1. **Marketing and Sales:** Computer networks are used extensively in both marketing and sales organizations. Marketing professionals use them to collect, exchange, and analyze data related to customer needs and product development cycles. Sales application includes tele-shopping, which uses order-entry computers or telephones connected to order processing network, and online-reservation services for hotels, airlines and so on.
2. **Financial Services:** Today's financial services are totally depended on computer networks. Application includes credit history searches, foreign exchange and investment services, and electronic fund transfer, which allow user to transfer money without going into a bank (An Automated Teller Machine (ATM) is an example of electronic fund transfer automatic pay-check is another).
3. **Manufacturing:** Computer networks are used in many aspects of manufacturing including manufacturing process itself. Two of them that use network to provide essential services are Computer-Added Design (CAD) and Computer-Assisted Manufacturing (CAM), both of which allow multiple users to work on a project simultaneously.
4. **Directory Services:** Directory services allow list of files to be stored in central location to speed worldwide search operations.

5. **Information Services:** A Network information services includes bulletin boards and data bank... World Wide Web (WWW) site offering technical specification for a new product is an inform... service.
6. **Electronic Data Interchange (EDI):** EDI allows business information, including documents such ... purchase orders and invoices, to be transferred without using paper.
7. **Electronic Mail:** Probably it's the most widely used computer network application.
8. **Teleconferencing:** Teleconferencing allows conference to occur without the participants being ... the same place. Applications include simple text conferencing (where participants communicate ... through their normal keyboards and monitor) and video conferencing where participants can e... see as well as talk to other fellow participants.
9. **E-Commerce:** Computer networks have paved way for a variety of business and commerc... transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or s... items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investmen... electronically.

## 3.2 PROTOCOLS

- A protocol is a set of rules that governs data communication. Protocol is very important for networki... without protocol communication cannot occur.
- A protocol defines what is to be communicated, how it is to be communicated and when it is to b... communicated. Both sender and receiver should follows the same protocol to communicate data.

**Functions of Protocols:**

1. Protocol defines data sequencing rules. It also defines data routing rules which the most effici... path between the source and destination.
2. Protocol defines data formatting rules which group of bits or characters within packet consti... data, control, addressing, or other information.
3. Protocol defines flow control of information or data.
4. Protocol defines error control rules are designed to detect errors in messages and to ensu... transmission of correct messages.
5. Protocol defines precedence and order of transmission rules ensure that all the nodes get a chan... to use the communication lines and other resources of the network based on the priorities assigne... to them.
6. Protocol defines connection establishment and termination rules that define how connections ar... established, maintained and terminated when two nodes of a network want to communicate wi... each other.
7. Protocol defines data security and privacy that built into most communication software packages.

- The most common protocols are, Ethernet, LocalTalk, Token Ring, FDDI, ATM and so.

### 3.2.1 Definition of Protocol

- A protocol is defined as, "a set of rules that governs the communications between computers or ... network."
- A protocol is, "a formal set of rules, conventions and data structure that governs how computers an... other network devices exchange information over a network." Network protocols define the rules an... procedures for the network communications.
- "A set of rules or standards designed to enable computers to connect with one another over a netwo... and to exchange information with as little error as possible."

28/04/23 9:04 AM



### 3.2.2 Elements of Protocol

- A protocol defines the following basic elements:

1. **Syntax (What is to be communicated?):** The syntax of protocol defines the structure or format of data. This means that the order in which it is to be sent is decided. A protocol could define that the first 16 bits of a data transmission must always contain the receiver's address.
2. **Semantics (How it is to be communicated?):** Protocol semantics defines the interpretation of the data that is being sent. For example: The semantics could define that if the last two bits of the receiver's address field contain a 00, it means that the sender and the receiver are on the same network.
3. **Timing (When it should be communicated?):** Timing refers to an agreement between the sender and the receiver about the data transmission rates and duration.

### 3.2.3 Protocol Standards

- Standards are necessary in our daily life. Every thing that we use in our daily life has some common features, some standards. Standards are also necessary in data communication to ensure interconnectivity and interoperability between various networking hardware and software components.
- Without standards we would have proprietary products creating isolated islands of users which cannot interconnect.
- In data communication, standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and also in guaranteeing national and international inter-operability of data and telecommunications technology and processes.
- Standards provide guidelines to manufacturers, vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.
- Data communication standards fall into two categories namely de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation") as explained below:

**1. De facto Standards:**

- This category includes standards that have not been approved formally by some authority but have been accepted as standards because of their widespread use.
- For example, the UNIX operating system has largely been used in computer science departments of most universities and thus has been adopted as the standard.
- De facto data communication standards can be further divided into proprietary and non-proprietary standards as explained below:

(I) **Proprietary Standards** are invented and owned by an organization who first uses them, and which gain popularity. Proprietary standards is closed, because they close-off communication with devices/systems of other vendors.

(II) **Non-proprietary Standards** are those that are developed by an organization/ committee/group, which become popular and vendors start supporting them. Non-proprietary standards are open because anybody adhering to those automatically gains access to all others following those standards.

**2. De jure Standards:**

- The De jure standards are formally declared as legal standards by recognized standardization authorities.
- The De jure are the standards that have been legislated by an official body. These De jure standards are usually led by governments or government appointed agencies.

### 3.2.4 Standards Organizations

- Standards organizations can be classified into three categories namely, Standards creation committees, Forums, and Regulatory agencies.

1. **Standards Creation Committees:** There are lot of organizations serving as standards creation committees. Some of them are listed below:

   (i) **American National Standards Institute (ANSI):** ANSI is a private non-profit organization that does not have any direct ties with the US federal government. Generally, all ANSI projects are undertaken for the social benefit of the US citizens. Professional groups, regulatory bodies, government, and consumer groups represent ANSI.

   (ii) **Electronic Industries Association (EIA):** EIA is a non-profit organization that is aligned with ANSI. EIA focus is public awareness and lobbying for standards. The main contributions to the data communications technology are the development of interfaces for physical connections and electronic signal specifications for data communications.

   (iii) **International Telecommunications Union-Telecommunications Standards Sector (ITU-T):** ITU-T was earlier known as the Consultative Committee for International Telegraphy and Telephony (CCITT). ITU-T was formed by the United Nations in response to the demands from some nations who were developing their own national standards for data communications in the early 1970s and which led to issues of incompatibility with each other.

   (iv) **Institute of Electrical and Electronics Engineers (IEEE):** IEEE is the biggest professional engineering body in the world. IEEE focus areas are developments in the areas of electric and electronic engineering and radio sciences. IEEE also covers the development and adoption of international computer and communications standards.

   (v) **International Standards Orgnization (ISO):** ISO is a well-known multi-national standards body. Open Systems Interconnection (OSI) model as a networking protocol is a major contribution of the ISO to the data communications world. Most members of ISO are their respective government representatives. ISO created in 1947, the ISO is a non-profitable standards creation organization. Members from over eighty developed nations actively represent the ISO.

2. **Forums:**

- The main drawback of standards committees are notorious for the slow pace of developments and decision-making.
- Forums generally concentrate on a particular technology, and this specialization helps them achieve a great amount of throughput with contributions from a variety of forum members.
- User groups, industry representatives, university students, and experts come together and set up forums to address the various issues and concerns of data communications technology, and come up with standards from time to time.

**Examples of Forums:**

(i) Internet Society (ISOC), (ii) Internet Engineering Task Force (IETF),
(iii) Frame Relay Forum, and (iv) ATM Forum.

3. **Regulatory Agencies:**

- Government appointed agencies, for example, Federal Communications Commission (FCC) of the US are always involved in regulating standards. These Government appointed agencies help protect the interests of the general public in areas such as radio, television and wired communications.
- Every portion of communications technology must be approved by FCC before it can be sold in the market.
- FCC periodically reviews the rates changed by service providers, technical specifications of communication hardware and divides and allocates ratio frequencies, etc.



## 3.3 LINE CONFIGURATIONS

- A network is two or more devices connected through a link. A link is a physical communication pathway that transfer data from one device to another. Devices can be a computer, printer or any other device that is capable to send and receive data.
- Line configuration refers to the way two or more communication devices attached to a link. Link configuration defines the attachment of communication devices to a link. For communication to occur, two devices must be connected in same way to the same link at the same time.
- There are two possible line configurations namely, Point to Point Line Configuration and Multipoint Line Configuration.

1. **Point to Point Line Configuration:**

- In point to point line configuration there is a dedicated link between the communicating devices.
- The link is totally reserved for transmission specifically for those two devices. Most point to point connections are established with cable or wire though satellite or microwave links are also possible.
- For example, operating any device such as television using a remote control establishes a point to point connection between the device and the remote control.

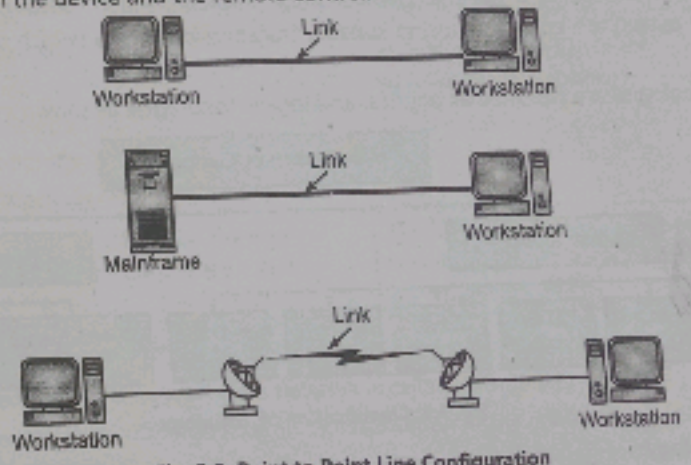



Fig. 3.3: Point to Point Line Configuration

2. **Multipoint Line Configuration**

- It is also called multidrop line configuration. In this line configuration two or more devices share a single link.
- In a multipoint line configuration, a single link is shared between two or more devices, i.e., there is no dedicated link between the communicating devices (as shown in Fig. 3.4.).
- If the shared link can be utilized by many devices simultaneously, it is known as a spatially shared connection whereas if devices need to take turns to utilize the link, it is known as a timeshared connection.

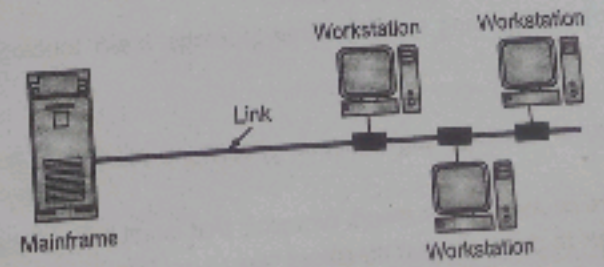



Fig. 3.4: Multipoint Line Configuration

## 3.4 NETWORK TOPOLOGY

- A network topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network.
- Network topology refers to layout of a network and how different nodes in a network are connected to each other and how they communicate.
- A topology is geometric arrangement of computers and its devices in a network. The word "topology" comes from topos, which is Greek for "place". Topology is the map of a network i.e. a topology is the layout of connected devices.
- Network topology describe the ways in which the elements of a network are mapped. They describe the physical and logical arrangement of the network nodes.
- Topology refers to the way in which the network of computers is connected. Each topology is suited for specific tasks and has its own advantages and disadvantages.
- The choice of topology is dependent upon type and number of equipment being used, planned applications and rate of data transfer required, response time, and cost.
- Topology can be defined as the geometrically interconnection pattern by which the stations (nodes/computers) are connected using suitable transmission media (which can be point-to-point and broadcast).
- Network topologies are classified as physical and logical topologies as shown in Fig. 3.5.

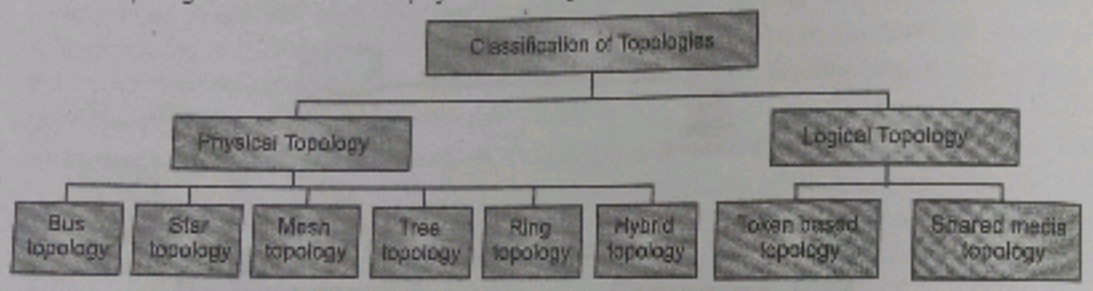



Fig. 3.5: Classification of Topology

**1. Physical Topology:**

- Physical topology mentions the physical design of a network including the devices, location and cable installation.
- A physical topology describes the placement of network nodes and the physical connections between them.
- The physical topology of a network refers to the configuration of cables, computers, and other peripherals.
- It describes the actual layout of the network transmission media. This includes the arrangement and location of network nodes and they are connected.
- Bus topology, star topology, ring topology, tree topology, mesh topology, etc. are the examples of physical topologies.

**2. Logical Topology:**

- It is also called as signal topology. Logical topology refers to the nature of the paths the signals follow from node to node.
- Logical topologies are bound to the network protocols that direct how the data moves across a network. Logical topology refers to the paths that messages take to get from one place on the network to another place.



- The two most common types of logical topologies are broadcast and token passing.
- For example, in a logical diagram of your office network, you may show a connection between city A and city B. But in the actual physical network, your data may go through switching points in several other cities as well. The logical path is a high-level representation; the physical path is the actual route.

**Difference between Physical Topology and Logical Topology:**

| Sr. No. | Physical Topology | Logical Topology |
|---|---|---|
| 1. | **Definition:** Physical topologies refer to the physical layout of devices and network media. | **Definition:** Logical topologies refer to the logical paths in which data accesses the media and transmits packets across it. |
| 2. | How the wires are connected. | How the data is transferred. |
| 3. | Physical topology defines how the nodes of the network are physically connected. | Logical topology dedicated connections between certain selected source-destination pairs using the underlying physical topology. |
| 4. | Types include:<br>(i) Bus topology<br>(ii) Ring topology<br>(iii) Star topology<br>(iv) Tree topology<br>(v) Mesh topology | There are two main types of logical topologies:<br>(i) Shared media topology<br>(ii) Token-based topology. |
| 5. | A physical topology describes the way in which the devices are connected together. | The logical topology describes how the devices communicate or the shape of the communication path. |

### 3.4.1 Definition of Network Topology

- The way of connecting the computers in a network is called as topology. **OR**
- The topology of a network is "the geometric representation of the relationship of all the links and linking devices (nodes) in a network". **OR**
- Network topology is defined as "the physical interconnection between various elements on computer network, such as links and nodes". **OR**
- A topology is a usually "schematic description of the arrangement of a network, including its nodes and connecting lines (links)".
- Selecting an appropriate topology for your deployment environment depends upon several factors. When you select a topology pattern, consider the following factors:
  1. Current Hardware.
  2. Size of the Network.
  3. Budget Limitations.
  4. Need for reliability.
  5. Bandwidth capacity.
  6. Scalability and Ease installation.
  7. Ease of Troubleshooting.

### 3.4.2 Types of Topology

- The way in which the connections are made is called the topology of the computer network.
- Fig. 3.5 shows different categories or types of topologies in computer network.

## 3.4 NETWORK TOPOLOGY

- A network topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network.
- Network topology refers to layout of a network and how different nodes in a network are connected to each other and how they communicate.
- A topology is geometric arrangement of computers and its devices in a network. The word "topology" comes from topos, which is Greek for "place". Topology is the map of a network i.e. a topology is the layout of connected devices.
- Network topology describe the ways in which the elements of a network are mapped. They describe the physical and logical arrangement of the network nodes.
- Topology refers to the way in which the network of computers is connected. Each topology is suited to specific tasks and has its own advantages and disadvantages.
- The choice of topology is dependent upon type and number of equipment being used, planned applications and rate of data transfer required, response time, and cost.
- Topology can be defined as the geometrically interconnection pattern by which the stations (nodes/computers) are connected using suitable transmission media (which can be point-to-point and broadcast).
- Network topologies are classified as physical and logical topologies as shown in Fig. 3.5.

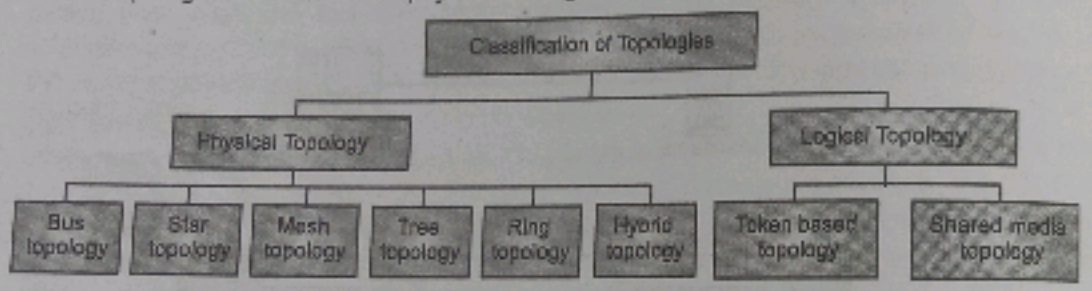



**Fig. 3.5: Classification of Topology**

### 1. Physical Topology:

- Physical topology mentions the physical design of a network including the devices, location and cable installation.
- A physical topology describes the placement of network nodes and the physical connections between them.
- The physical topology of a network refers to the configuration of cables, computers, and other peripherals.
- It describes the actual layout of the network transmission media. This includes the arrangement and location of network nodes and they are connected.
- Bus topology, star topology, ring topology, tree topology, mesh topology, etc. are the examples of physical topologies.

### 2. Logical Topology:

- It is also called as signal topology. Logical topology refers to the nature of the paths the signals follow from node to node.
- Logical topologies are bound to the network protocols that direct how the data moves across a network. Logical topology refers to the paths that messages take to get from one place on the network to another place.



- The two most common types of logical topologies are broadcast and token passing.
- For example, in a logical diagram of your office network, you may show a connection between city A and city B. But in the actual physical network, your data may go through switching points in several other cities as well. The logical path is a high-level representation; the physical path is the actual route.

**Difference between Physical Topology and Logical Topology:**

| Sr. No. | Physical Topology | Logical Topology |
|---|---|---|
| 1. | **Definition:** Physical topologies refer to the physical layout of devices and network media. | **Definition:** Logical topologies refer to the logical paths in which data accesses the media and transmits packets across it. |
| 2. | How the wires are connected. | How the data is transferred. |
| 3. | Physical topology defines how the nodes of the network are physically connected. | Logical topology dedicated connections between certain selected source-destination pairs using the underlying physical topology. |
| 4. | Types include:<br>(i) Bus topology<br>(ii) Ring topology<br>(iii) Star topology<br>(iv) Tree topology<br>(v) Mesh topology | There are two main types of logical topologies:<br>(i) Shared media topology<br>(ii) Token-based topology. |
| 5. | A physical topology describes the way in which the devices are connected together. | The logical topology describes how the devices communicate or the shape of the communication path. |

### 3.4.1 Definition of Network Topology

- The way of connecting the computers in a network is called as topology. **OR**
- The topology of a network is "the geometric representation of the relationship of all the links and linking devices (nodes) in a network". **OR**
- Network topology is defined as "the physical interconnection between various elements on computer network, such as links and nodes". **OR**
- A topology is a usually "schematic description of the arrangement of a network, including its nodes and connecting lines (links)".
- Selecting an appropriate topology for your deployment environment depends upon several factors. When you select a topology pattern, consider the following factors:
  1. Current Hardware.
  2. Size of the Network.
  3. Budget Limitations.
  4. Need for reliability.
  5. Bandwidth capacity.
  6. Scalability and Ease installation.
  7. Ease of Troubleshooting.

### 3.4.2 Types of Topology

- The way in which the connections are made is called the topology of the computer network.
- Fig. 3.5 shows different categories or types of topologies in computer network.

**1. Bus Topology:**

- In networking, a topology that allows all network nodes to receive the same message through the network cable at the same time is called as bus topology.
- In this type of network topology, all the nodes of a network are connected to a common transmission medium having two endpoints.
- All the data that travels over the network is transmitted through a common transmission medium known as the bus or the backbone of the network.
- When the transmission medium has exactly two endpoints, the network topology is known by the name 'linear bus topology'.
- A network that uses a bus topology is referred to as a "Bus Network".

**Working of Bus Topology:**

- Fig. 3.6 shows bus topology. The central cable is the backbone of the network and is known as Bus (thus the name). Every workstation or node communicates with the other device through this Bus.
- A signal from the source is broadcasted and it travels to all workstations connected to bus cable. Although the message is broadcasted but only the intended recipient, whose MAC address or IP address matches, accepts it.
- If the MAC/IP address of machine does not match with the intended address, machine discards the signal.
- A terminator is added at ends of the central cable, to prevent bouncing of signals. A barrel connector can be used to extend it.

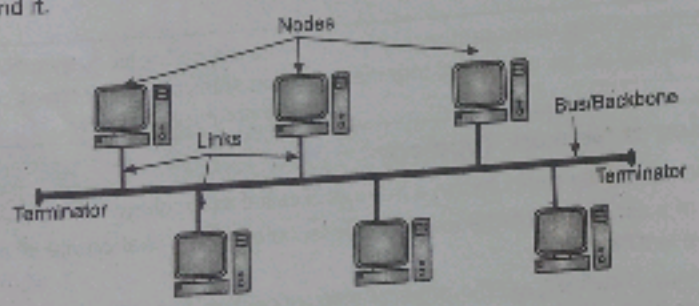



Fig. 3.6: Bus Topology

**Features of Bus Topology:**

1. It transmits data only in one direction.
2. Every device is connected to a single cable in bus topology.

**Advantages of Bus Topology:**

(i) It is cost effective and cabling cost is less than other topologies.
(ii) Easy to install and set-up. It is very easy to connect a computer or peripheral to a bus.
(iii) Requires less cabling length, so cheaper.
(iv) Any one computer or device being down does not affect the others.
(v) Fast as compare to ring topology and sufficient for small network.
(vi) Easy to expand joining two cables together.

**Disadvantages of Bus Topology:**

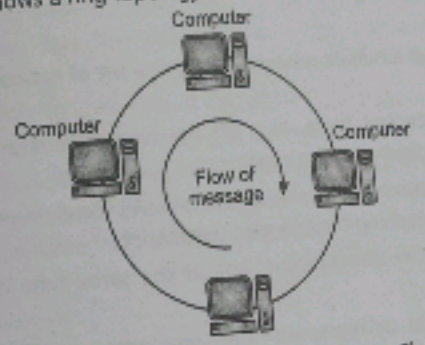
(i) Cable has a limited length, so it cannot connect a large number of computers.
(ii) A fault or break in the bus cable stops all data transmission. Difficult to identify the problem if the entire network shuts down.



(iii) Collision may occur.
(iv) Terminators are required at both ends of the backbone cable.
(v) If network traffic is heavy or nodes are more the performance of the network decreases.

**2. Ring Topology:**

- Ring topology is a network topology that is set-up in circular fashion. 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.
- Each node in this topology contains repeater. A signal passes node to node, until it reaches its destination. If a node receives a signal intended for another node its repeater regenerates the signal and passes it.
- Token is a special three byte frame that travels around the ring network. It can flow clockwise or anticlockwise. Ring topology is a point to point network.
- 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.
- The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each network node, it is called Dual Ring Topology.
- 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.
- In a ring network, the data and the signals that pass over the network travel in a single direction. Fig. 3.7 shows a ring topology.



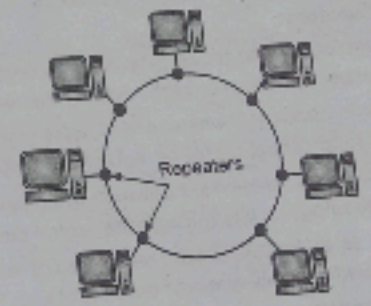




Fig. 3.7: Ring Topology

**Working of Ring Topology:**

- In ring topology network arrangement, a signal is transferred sequentially using a 'token' from one node to the next. If a node wants to transmit, it "grabs" the token, attaches data and a destination address to it, and then sends it around the ring.
- The token travels along the ring until it reaches its destination. Once, token reaches destination, receiving computer acknowledges receipt with a return message to the sender. The sender then releases the token for the token for use by another computer.
- A signal from the source is broadcasted and it travels to all workstations connected to bus cable. Although the message is broadcasted but only the intended recipient, whose MAC address or IP address matches, accepts it.
- If the MAC/IP address of machine does not match with the intended address, machine discards the signal.

- A terminator is added at ends of the central cable, to prevent bouncing of signals. A barrel connector can be used to extend it.

**Advantages of Ring Topology:**

(i) Require less cabling.
(ii) Less expensive.
(iii) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision.
(iv) Each computer has equal access to resources.
(v) There is no need for network server to control the connectivity between workstations.
(vi) Even when the load on the network increases, its performance is better than that of Bus topology.
(vii) Fault isolation is simplified.
(viii) Good communication over long distance.
(ix) Handles high volume of traffic.

**Disadvantages of Ring Topology:**

(i) Traffic is unidirectional.
(ii) Network is highly dependent on the wire which connects different components.
(iii) Failure of one computer disturbs the whole network.
(iv) Slow in speed.
(v) Adding or deleting the computers disturbs the network activity.
(vi) Reconfiguration is needed to add one node; whole network must be down first.
(vii) Difficult for troubleshooting the ring.

**3. Star Topology:**

- Star topology is one topology in which a central unit called a hub or concentrator host a set of network cables that radiate out to each node on the network.
- Unlike bus topology, where nodes were connected to central cable, here all the workstations are connected to central device i.e. hub or concentrator with a point-to-point connection.
- The data that is transmitted between the network nodes passes across the central hub. All the data on the star topology passes through the central device before reaching the intended destination.
- Hub acts as a junction to connect different nodes present in Star Network, and at the same time it manages and controls whole of the network.
- A distributed star is formed by the interconnection of two or more individual star networks. The centralized nature of a star network provides a certain amount of simplicity while also achieving isolation of each device in the network.

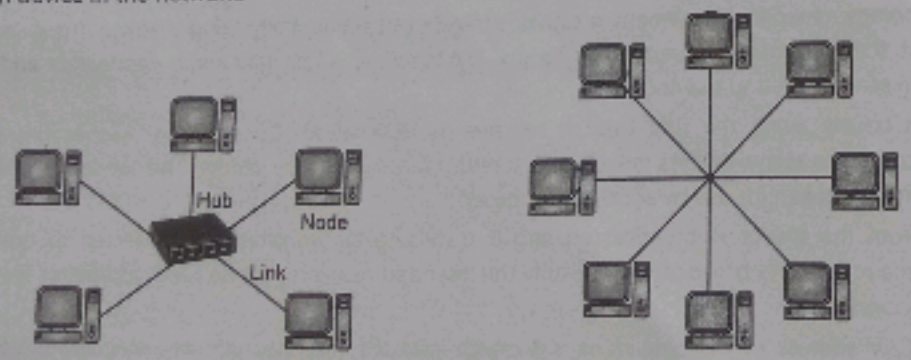



**Fig. 3.8: Star Topology**



**Advantages of Star Topology:**

(i) Easy to install, reconfigure and wire.
(ii) Centralized management. It helps in monitoring the network.
(iii) Robustness i.e. if one link fails, only that link is affected.
(iv) Fast as compare to ring topology.
(v) Multiple devices can transfer data without collision.
(vi) Eliminates traffic problem.
(vii) No disruptions to the network then connecting or removing devices.
(viii) It is easy to detect the failure and troubleshoot it.
(ix) Supported by several hardware and software venders.

**Disadvantages of Star Topology:**

(i) If central node (hub or switch) goes down, then entire network goes down.
(ii) More cabling is required than bus topology.
(iii) More expensive than bus topologies because of the cost of the concentrators (hub or switch).
(iv) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

**4. Mesh Topology:**

- In a mesh network topology, each of the network node, computer and other devices, are interconnected with one another.
- Every node not only sends its own signals but also relays data from other nodes. In fact, a true mesh topology is the one where every node is connected to every other node in the network.
- In this type of network, each node may send message to destination through multiple paths. While the data is travelling on the Mesh Network it is automatically configured to reach the destination by taking the shortest route which means the least number of hops.
- This type of topology is very expensive as there are many redundant connections, thus it is not mostly used in computer networks. It is commonly used in wireless networks.

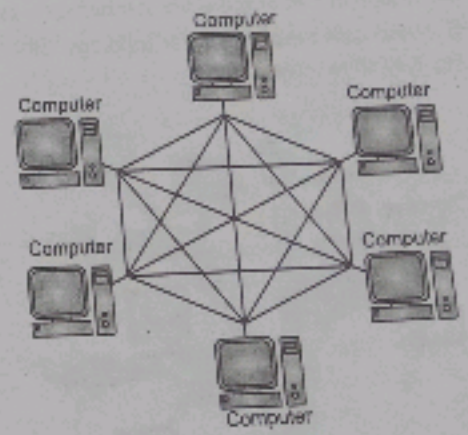



**Fig. 3.9: Mesh Topology**

- A mesh topology employs one of two connection arrangements, full mesh topology or partial mesh topology.
  - **(i) In a full mesh network,** each network node is connected to every other node in the network. Due to this arrangement of nodes, it becomes possible for a simultaneous transmission of signals from one node to several other nodes.
  - **(ii) In a partially connected mesh network,** only some of the network nodes are connected to more than one node. This is beneficial over a fully connected mesh in terms of redundancy caused by the point-to-point links between all the nodes.
- The nodes of a mesh network require possessing some kind of routing logic so that the signals and the data travelling over the network take the shortest path during each of the transmissions.

**Advantages of Mesh Topology:**

(i) Mesh topology is robust. If one link becomes unusable, it does not affect other systems.
(ii) Eliminates traffic problem.
(iii) Each connection can carry its own data load due to dedicated link.
(iv) Privacy or security because of dedicated line.
(v) Point-to-point link make fault identification and troubleshooting easy.

**Disadvantages of Mesh Topology:**

(i) More cables are required than other topologies.
(ii) Overall cost of this network is too high as compared to other network topologies.
(iii) Installation and reconfiguration is very difficult because each device must be connected to every other device.
(iv) Set-up and maintenance of this topology is very difficult.
(v) Expensive due to hardware requirements such as cables and input/output ports.

**5. Tree Topology:**

- As its name implies in this topology devices make a tree structure. Tree topology integrates the characteristics of star and bus topology.
- In tree topology, the number of star networks are connected using Bus. This main cable seems like a main stem of a tree, and other star networks as the branches.
- It is also called expanded star topology. Ethernet protocol is commonly used in this type of topology. Fig. 3.10 shows tree topology.

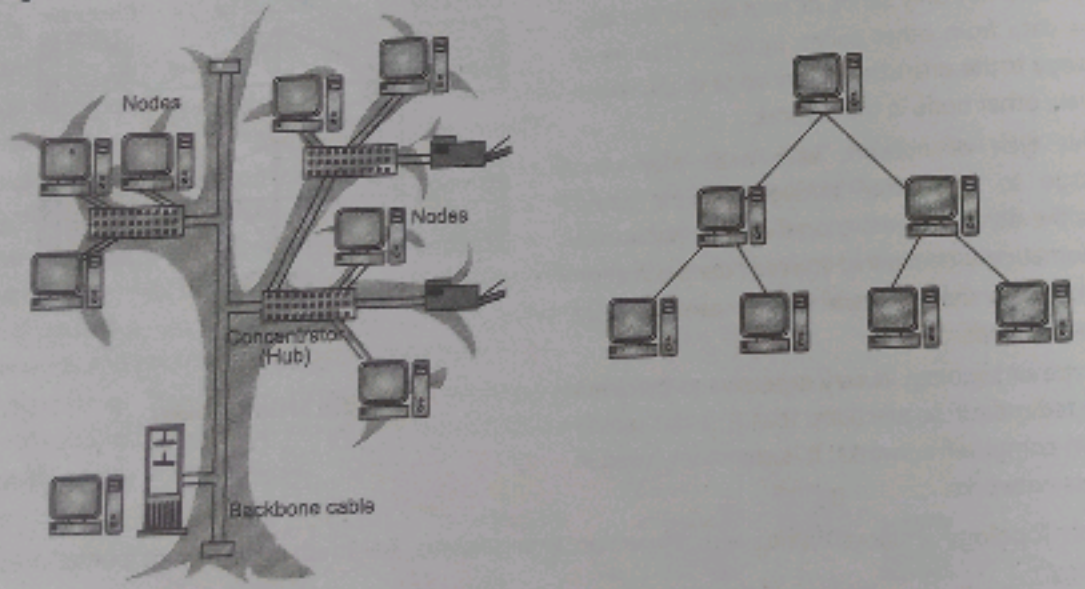



**Fig. 3.10: Tree Topology**

- A tree topology can also combine characteristics of linear bus and star topologies. It consists of groups of star-configure workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network and enable schools to configure a network to meet their needs.

**Advantages of Tree Topology:**

(i) Easy to install and wire.
(ii) Fast as compare to other topologies.



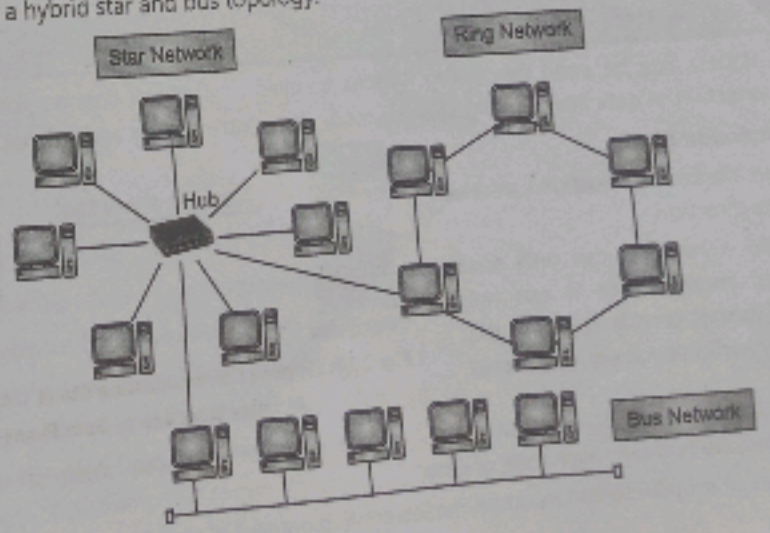
(iii) Multiple devices can transfer data without collision.
(iv) Eliminates traffic problem.
(v) Increase the distance of a signal can travel between network devices.
(vi) No disruptions to the network then connecting or removing devices.
(vii) Easy to detect faults and to remove parts.
(viii) Supported by several hardware and software vendors.
(ix) It allows the network to isolate and priorities communications form different computers.
(x) Each node in the network having a specific fixed number nodes connected to it at the next lower level hierarchy.

**Disadvantages of Tree Topology:**

(i) Because of its basic structure, tree topology, relies heavily on the main bus cable, if it breaks whole network is crippled.
(ii) More expensive than bus topologies because of the cost of the concentrators (hub or switch).
(iii) The cabling cost is more.
(iv) As more and more nodes and segments are added, the maintenance becomes difficult.
(v) Scalability of the network depends on the type of cable used.
(vi) Failure in the central hub brings the entire network to a halt.

**6. Hybrid Topology:**

- Hybrid, as the name suggests, is mixture of two different things. A hybrid topology is combination of two or more network topologies.
- A combination of two or more different topologies makes for a hybrid topology. This combination of topologies is done according to the requirements of the organization. In other words, the topology that combines more than one topology is called hybrid topology.
- Hybrid topology is used to connect a network that is divided into smaller sections also known as segments.
- Two common examples for hybrid network are star ring network and star bus network.
  - (i) **A star-ring network** consists of two or more star topologies connected using a Multistation Access Unit (MAU) as a centralized hub.
  - (ii) **A star-bus network** consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).
- Fig. 3.11 shows a hybrid star and bus topology.



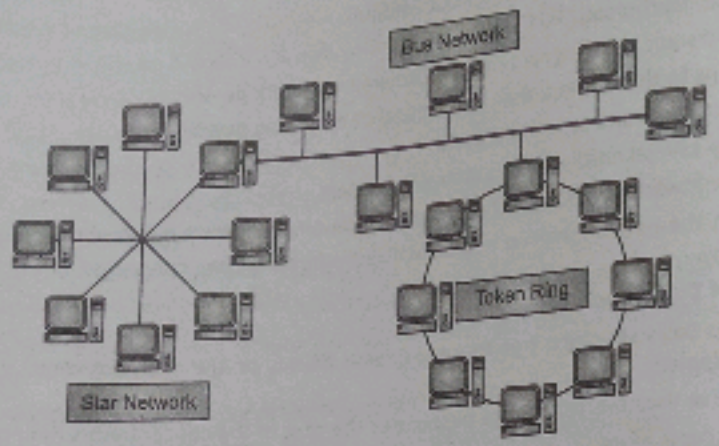



Fig. 3.11: Hybrid Topology

**Advantages of Hybrid Topology:**

(i) Unlike other networks, fault detection and troubleshooting is easy in this type of topology.

(ii) It is easy to increase the size of network by adding new components, without disturbing existing architecture.

(iii) Hybrid network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.

(iv) Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while their weaknesses are neutralized.

**Disadvantages of Hybrid Topology:**

(i) One of the biggest drawback of hybrid topology is its design. It's not easy to design this type of architecture and it's a tough job for designers.

(ii) Configuration and installation process needs to be very efficient.

(iii) The hubs used to connect two distinct networks, are very expensive.

(iv) As hybrid architectures are usually larger in scale, they require a lot of cables, cooling systems, sophisticate network devices, etc.

## 3.5 MODES OF TRANSMISSION

- The direction of data flow between two linked devices is called as mode of communication. There are three types of direction of data flow namely, simplex mode, half-duplex mode and full-duplex mode.

**1. Simplex Transmission Mode:**

- In simplex mode, the communication can take place in only one direction.
- In simplex mode, a terminal can only send data and cannot receive it or it can only receive data but cannot send it. It means that in this mode communication is uni-directional.

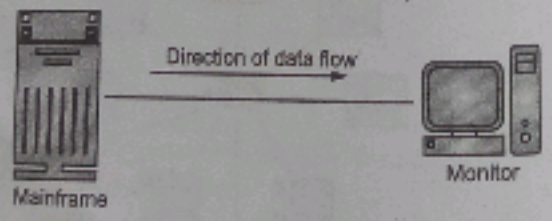



Fig. 3.12: Simplex Communication Mode (Mainframe to Monitor Direction of Data Flow)

- Today, simplex mode of data communication is not popular, because most of the modern communications require two-way exchange of data.
- The some examples of simplex communication modes are Radio and T.V. transmissions.



- In computer system, the keyboard, monitor and printer are examples of simplex devices. The keyboard can only be used to enter data into computer, while monitor and printer can only accept (display/print) output.

**Advantages of Simplex Transmission Mode:**

(i) Very simple and easy communication method.

(ii) Cheaper in cost.

**Disadvantages of Simplex Transmission Mode:**

(i) Only allows for communication in one direction.

(ii) Simplex transmission are not often used because it is not possible to send back error to the transmit end.

**2. Half Duplex Transmission Mode:**

- In half duplex mode, the communication can take place in both directions, but only in one direction at a time.
- In this mode, data is sent and received alternatively. It is like a one-lane bridge where two-way traffic must give way in order to cross the other. In half-duplex mode, at a time only one end transmits data while other end receives. In addition, it is possible to perform error detection and request the sender to re-transmit information.
- The Internet browsing is an example of half duplex mode. When we issue a request to download a web document, then that document is downloaded and displayed before we issue another request.

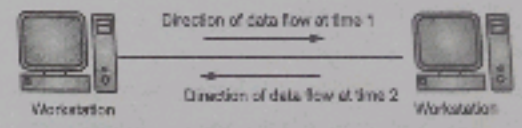



Fig. 3.13: Half Duplex Communication Mode

- A walkie-talkie operates in half duplex mode. It can only send or receive a transmission at any given time. It cannot do both at the same time.

**Advantages of Half Duplex Transmission Mode:**

(i) Enables to two way communication.

(ii) Low cost than full duplex communication mode.

**Disadvantages of Half Duplex Transmission Mode:**

(i) Only one device can transmit at a time.

(ii) High cost than simplex mode.

**3. Full Duplex Transmission Mode:**

- In full duplex mode, the communication can take place in both directions simultaneously, i.e. at the same time on the same channel. Full-duplex mode is the fastest directional mode of communication.
- The telephone communication system is an example of full-duplex communication mode.

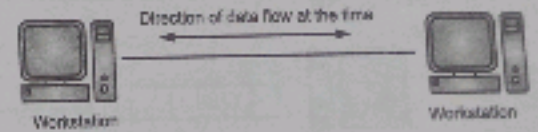



Fig. 1.14: Full Duplex Communication Mode

**Advantages Full Duplex Transmission Mode:**

(i) Enables tow-way communication simultaneously.

(ii) Fastest method of data communication.

**Disadvantages Full Duplex Transmission Mode:**

(i) More expensive and complex method.

(ii) Two bandwidth channels is required for data transmission.

**Types of Data Transmission/Communication:**

- Data transmission means transferring of data or information from one computer to another computer using a transmission medium such as coaxial cable, fiber-optic etc.
- Types of data transmission modes are explained below.

**1. Parallel Transmission (Communication):**

- In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines. Parallel transmission is shown in Fig. 3.15.
- Parallel transmission is used for short distance communication.
- Parallel transmission is commonly used to transfer data from computer to printer. The printer is connected to the parallel port of computer and parallel cable that has many wires is used to connect the printer to computer.

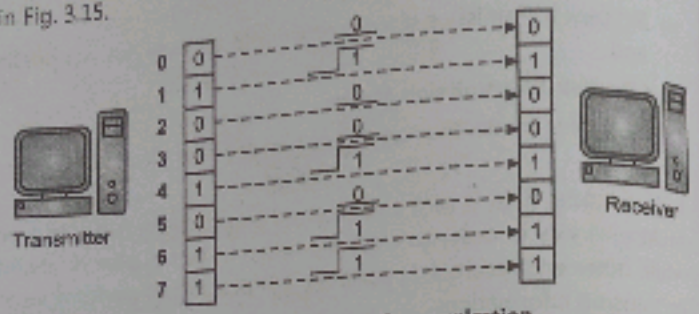



Fig. 3.15: Parallel Data Communication

**Advantages:**

(i) Fastest method for data transmission because of the data bits will be transmitted simultaneously.

(ii) It does not require high frequency for operation.

**Disadvantages:**

(i) Cost is high.

(ii) Requires separate lines for each bit of word.

**2. Serial Transmission (Communication):**

- In serial data transmission, bits of data flow in sequential order through single communication line. Serial transmission is used for long distance communication.
- Serial data transmission is shown in Fig. 3.16.
- Serial transmission is typically slower than parallel transmission, because data is sent sequentially in a bit-by-bit fashion. Serial mouse uses serial transmission mode in computer.

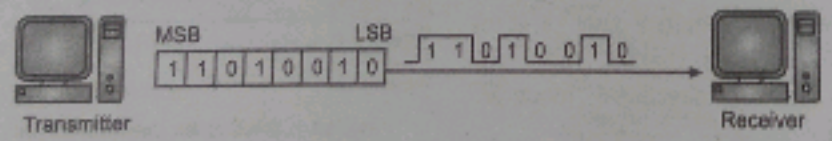



Fig. 3.16: Serial Data Transmission

**Advantages:**

(i) Only one communication wire required.

(ii) Cheaper than parallel data transmission.

**Disadvantages:**

(i) Speed of data transfer is slow.

(ii) It requires high frequency for data transmission operations.



**Difference between Serial Communication and Parallel Communication:**

| Sr. No. | Factors | Serial Communication | Parallel Communication |
|---|---|---|---|
| 1. | Number of bits transmitted at one clock pulse. | One bit. | n bits. |
| 2. | Number of lines required to transmit n bits. | One line. | n lines. |
| 3. | Speed of data transfer. | Slow. | Fast. |
| 4. | Cost of transmission. | Low as one line is required. | Higher as n lines are required. |
| 5. | Application | Long distance communication between two computers. | Short distance communication like computer to printer. |

- There are two types of serial transmission namely, synchronous and asynchronous both these transmissions use 'bit synchronization'. Bit synchronization is a function that is required to determine when the beginning and end of the data transmission occurs.

**(i) Synchronous Communication:**

- In this type of transmission, data is transmitted block-by-block or word-byword simultaneously. Each block in this transmission may contain several bytes of data.
- In synchronous transmission, a special communication device known as synchronized clock is required to schedule the transmission of information. This special communication device or equipment is expensive.

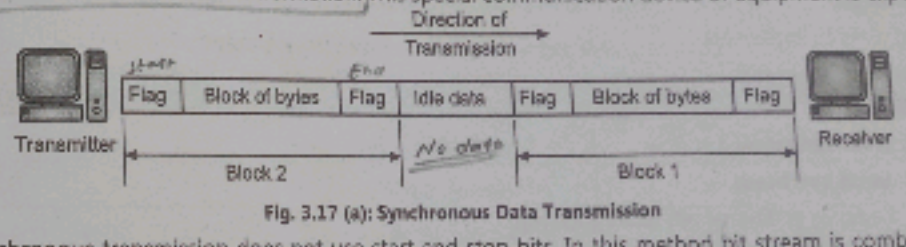



Fig. 3.17 (a): Synchronous Data Transmission

- Synchronous transmission does not use start and stop bits. In this method bit stream is combined into longer frames that may contain multiple bytes. There is no gap between the various bytes in the data stream, (see Fig. 3.17 (b)).

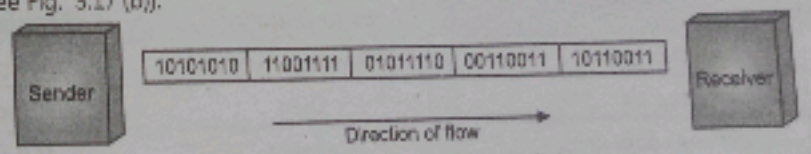



Fig. 3.17 (b): Synchronous Transmission

- In the absence of start and stop bits, bit synchronization is established between sender and receiver by 'timing' the transmission of each bit. Since, the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information.
- In order to receive the data error free, the receiver and sender operates at the same clock frequency. Synchronous transmission is used for high speed communication between computers.

**Advantages:**

(a) Speed of data transmission is very high.

(b) Lower overhead and thus greater throughput.

**Disadvantages:**

(a) Expensive and complex data transmission method.

(b) Requires proper synchronization.

- The communication network established for the purpose of connecting computer devices of personal use is known as the PAN (Personal Area Network).
- Fig. 3.21 shows typical PAN. Personal area networks may be wired with computer buses such as USB and FireWire.
- A Wireless Personal Area Network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth.


Fig. 3.21: PAN

**Advantages of PAN:**

(i) PAN network is easy to use. No advanced setup is required.
(ii) PAN network is secured because all the devices are authorized before data sharing.
(iii) Many devices can be connected to one device at the same time in a PAN.
(iv) PAN is an inexpensive way of communication.
(v) A person can move devices as it is a wireless network and data exchange is not affected. That means PAN is portable as well.

**Disadvantages of the PAN:**

(i) PAN has slow data transfer rate.
(ii) PAN is used in digital devices such as smart phones, PDA, laptops, tablets etc. which are costly.
(iii) Signal range is maximum 10 meters which makes limitation for long distance sharing.

**2. CAN (Campus Area Network)**

- A Campus Area Network (CAN) is used to connect buildings across campuses of colleges or Universities.
- A CAN is actually a type of Local Area Network (LAN). It is larger than a LAN but smaller than a Metropolitan Area Network (MAN).
- Fig. 3.22 shows typical CAN. Fig. 3.22 shows an example of the CAN is the networking between school, library and hostel. School management can access to library and hostel data through the network. Any student with login access can search the book by connecting its computer with the library. Similarly, school staff can check hostel data through their computers.

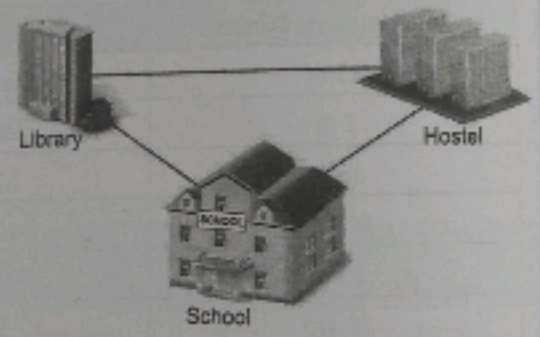



Fig. 3.22: CAN

- CAN is a network that connects two or more LANs but that is limited to a specific and contiguous geographical area such as a college campus, industrial complex, or a military base.
- A CAN is also known as a Corporate Area Network (CAN). CAN is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area (1 km to 5 km).
- A Campus Area Network (CAN) is a network of multiple interconnected Local Area Networks (LAN) in a limited geographical area. A CAN is smaller than a Wide Area Network (WAN) or Metropolitan Area Network (MAN).
- CAN is a computer network made up of an interconnection of Local Area Networks (LANs) within a limited geographical area.

**Advantages of CAN:**

(i) CAN are economical and Cost effective way for data transmission.
(ii) CAN is simple and easy to implement.
(iii) Helpful for universities and corporate organization to work from any block and receive the same speed of data transfer.



**Disadvantage of CAN:**

(i) CAN covers small geographical area 1 km to 5 km.

**3. LAN (Local Area Network):**

- Local Area Network (LAN) is privately-owned networks covering a small geographic area (less than 1 km), like a home, office, building or group of buildings (example, campus).
- LAN is a group of computers and associated peripheral devices connected by a communications channel, capable of sharing files and other resources among several users.
- LAN transmits data with a speed of several megabits per second (106 bits per second). The transmission medium is normally coaxial cables.
- LAN links computers, i.e., software and hardware, in the same area for the purpose of sharing information.
- Usually LAN links computers within a limited geographical area because they must be connected by a cable, which is quite expensive.
- People working in LAN get more capabilities in data processing, work processing and other information exchange compared to stand-alone computers.
- Fig. 3.23 shows simplest form of LAN that connect two computers together.

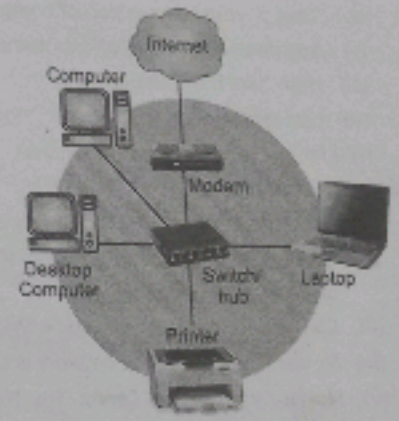



Fig. 3.23: A Local Area Network (LAN)

- A network which consists of less than 500 interconnected devices across several buildings, is still recognized as a LAN shown in Fig. 3.24.

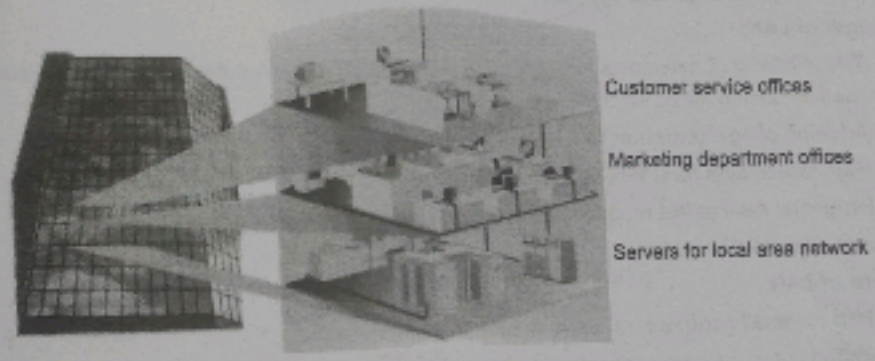



Fig. 3.24

- LAN are widely used for connecting personal computers and workstation in companies offices and factories to share resources.
- Because of this information exchange most of the business and government organizations are using LAN.
- A LAN is a high-speed data network that covers a relatively small geographic area less than 1 km and it typically connects workstations, personal computers, printers, servers, and other devices.
- LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications.
- LAN have data rate 10 to 100 Mbps.

- A MAN can support both data and voice and may be related to the Local Cable Television Network (CATV).
- MAN is a high-speed network that connects local area networks in a metropolitan area. A MAN employs one or two cables and does not contain switching elements, which simplifies the design.
- A public, high-speed network, capable of voice and data transmission over a distance of up to 80 kilometers, (50 miles).
- The best example of MAN is cable television. In their early systems a large antenna was placed on top of hill and signal was then piped to subscriber.
- A MAN is smaller than a Wide Area Network (WAN) but larger than a Local Area Network (LAN). MAN is designed to extend over an entire city.
- Multiple local area networks (LANs) that are connected on a campus or industrial complex using a high-speed backbone.
- Multiple networks that are connected within the same city to form a citywide network for a specific government or industry. Any network bigger than a LAN but smaller than a wide area network (WAN) is called as MAN.
- Fiber Distributed Data Interface (FDDI) is a good network technology for building a MAN.

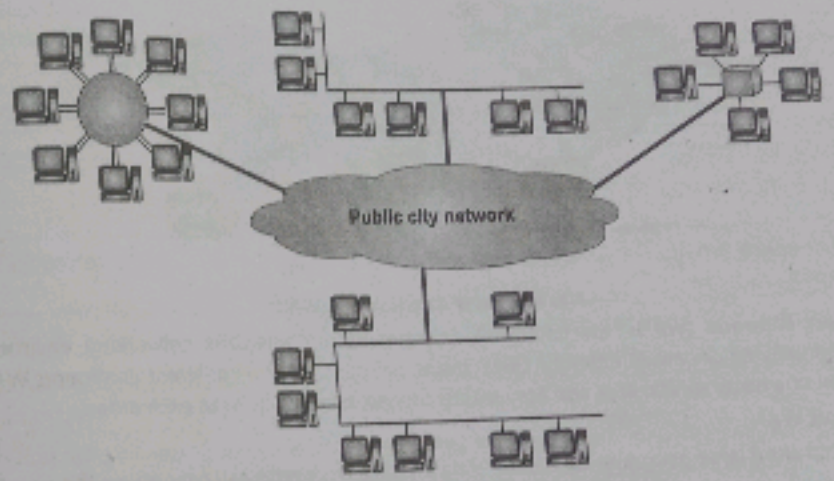



Fig. 3.25: Metropolitan Area Network (MAN)

**Advantages of MAN:**

(i) MAN spans large geographical area than LAN.
(ii) MAN falls in between the LAN and WAN therefore, increases the efficiency of handling data.
(iii) MAN time saves the cost attached to establish a wide area network.
(iv) MAN offers centralized management of data.
(v) MAN enables you to connect many fast LANs together.

**Disadvantages of MAN:**

(i) Implementation of MAN requires high cost.
(ii) If MAN becomes bigger then it becomes difficult to manage it. This is due to a security problem and other extra configuration.
(iii) In MAN there are high chances of attacking hackers on the network compared to LAN. So data may be leaked.
(iv) To setup MAN it requires technical people that can correctly setup MAN.



**Characteristics of LAN:**

(i) Every computer has the potential to communicate with any other computers of the network.
(ii) The reliability of network is high because the failure of the computer in the network does not affect the functioning for other computers.
(iii) High degree of interconnection between computers.
(iv) Easy physical connection of computers in a network.
(v) Inexpensive medium of data transmission.
(vi) High data transmission rate.
(vii) Less expensive to install.
(viii) Peripheral devices can be shared.

**Components of LAN:**

(i) **Workstations:** Workstations may allow data to be stored locally or remotely on a file server.
(ii) **Servers:** A server is a computer that provides the data, software and hardware resources that are shared on the LAN.
(iii) **Clients:** A client is any machine that requires something from a server.
(iv) **Nodes:** Each PC on the network is called a node.
(v) **Network Interface Cards:** The Network Interface Card (NIC), or LAN adapter, functions as an interface between the computer and the network cabling, so it must serve two masters.
(vi) **Connectors:** Connectors used with TP (Twisted-Pair) included RJ-11 and RJ-45 modular connectors in current use by phone companies.
(vii) **Network Operating System:** The Network Operating System (NOS) software acts as the command center, enabling all of the network hardware and all other network software to function together as one cohesive, organized system.

**Advantages of LAN:**

(i) The reliability of network is high because the failure of one computer in the network does not affect the functioning for other computers.
(ii) Addition of new computer to network is easy.
(iii) High rate of data transmission is possible.
(iv) Peripheral devices like magnetic disk and printer can be shared by other computers.
(v) Less expensive to install.

**Limitations of LAN:**

(i) Used for small geographical areas (less than 1 km).
(ii) Limited computers are connected in LAN.
(iii) Special security measures are needed to stop users from using programs and data that they should not have access to network.
(iv) Networks are difficult to set up and need to be maintained by skilled technicians.
(v) 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.

**4. MAN (Metropolitan Area Network):**

- MAN (Metropolitan Area Network) which is a network covering a larger area than LAN, say a network of all computers within a city.
- A MAN may be owned and operated by a single organization but is used by a larger number of individuals and organizations. A MAN can cover a group of corporate offices or a town or city and can be either privately or publicly owned.

**5. WAN (Wide Area Network):**

- Wide Area Network is a long-distance communications network that covers a wide geographic area, such as a state or country or even the whole world.
- A wide area network is a network that spans a large geographical area, the most common example being the Internet.
- A WAN is contrasted to smaller Local Area Networks (LANs) and Metropolitan Area Networks (MANs). LANs are home or office networks, while a MAN might encompass a campus or service residents of a city, such as in a citywide wireless or WiFi network.
- The Internet is a public WAN, but there are many ways to create a business model or private WAN. A private WAN is essentially two or more LANs connected to each other.
- A WAN provides long-distance transmission of data, voice, image, and video information over large geographical areas that may comprise a country, or even whole world.
- WAN containers a collection of machines intended for running user programs. We will follow traditional usage and call there machine host.
- A geographically distributed network composed of Local Area Networks (LANs) joined into a single large network using services provided by common carriers.

**Fig. 3.26: Wide Area Network (WAN)**

- Wide Area Networks (WANs) are commonly implemented in enterprise networking environments in which company offices are in different cities, states, or countries or on different continents.WAN's span more than one geographical area and are used to connect remote offices to each other.

***Advantages of WAN:***

(i) WAN covers a large geographical area so long distance businesses can connect on the one network.

(ii) WAN shares software and resources with connecting workstations.

(iii) Messages can be sent very quickly to anyone else on the network. These messages can have pictures, sounds, or data included with them, (called attachments).

(iv) 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.

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

***Disadvantages of WAN:***

(i) WANs are expensive and generally slow.

(ii) WANs need a good firewall to restrict outsiders from entering and disrupting the network.

(iii) Setting up a network can be an expensive and complicated experience. The bigger the network the more expensive it is.

(iv) 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.

(v) Slow speed than LAN and MAN.



**Difference between LAN, MAN and WAN:**

| Sr. No. | Parameter | LAN | WAN | MAN |
|---|---|---|---|---|
| 1. | Stand for | Local Area Network. | Wide Area Network. | Metropolitan Area Network. |
| 2. | Meaning | A computer network that interconnects computers within a limited area such as residence, office building, school or laboratory. | A computer network that interconnects user with computer resources in a geographical area larger than LAN but smaller than WAN. | A computer network that extends over a large geographical area. |
| 3. | Area covered | Covers small geographical area i.e. within the building, school (within 1 km to 10 km). | Covers large geographical area, like country, state etc., (beyond 100 km). | Covers larger area than LAN and smaller than WAN like campus. (with in 90 km). |
| 4. | Bandwidth | High bandwidth for data transfer. | Low bandwidth for data transfer | Bandwidth is moderate for data transfer. |
| 5. | Error rates | Lowest. | Highest. | Moderate. |
| 6. | Ownership | Owned by private companies or individuals. | Established under distributed ownership. | Ownership can be private or public. |
| 7. | Equipment cost | Uses inexpensive equipment. | Uses most expensive equipment. | Uses moderately expensive equipment. |
| 8. | Design | Easier to design and maintain. | Difficult and complicated to design and maintain. | Difficult and complicated to design and maintain. |
| 9. | Example | Offices, Cyber Café. | Internet. | ATM, FDDI etc. |
| 10. | Data transfer rate | Higher data transfer speeds with 10, 100, and 1000 Mbps high speed Ethernet. | Low data transfer rates between 10 to 20 Mbps. | Speed can go up to 100 Mbps. |
| 11. | Set-up cost | Lower setup cost due to inexpensive devices. | Higher setup cost than LAN and MAN. | Moderate installation costs. |

## 3.7 INTERNETWORKS

- An internetwork is a collection of individual networks connected by networking devices and that function as a single large network. The public Internet is the most common example which is a single network that connects millions of computers.
- Internetworking refers to the industry and products that are involved in the design, implementation, and administration of internetworks.
- An internetwork may be defined as, a network of computer communication networks every authorized member of which could communicate with every other authorized member (node) directly or indirectly.
- It may consist of several local, metropolitan or wide area networks interconnected via a LAN, M... WAN oriented communication technology, depending upon the specific context of use.

- When two or more networks are connected, they become an internetwork, or internet as shown in Fig. 3.27, the boxes labeled R represent routers. Individual networks are joined into internetwork by the use of internetworking devices. These devices which include routers, gateways etc.

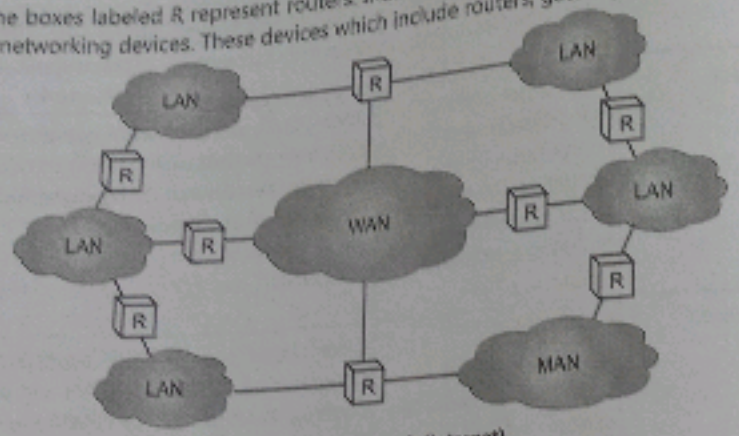



**Fig. 3.27: Internetwork (Internet)**

- Two architectural models are commonly used to describe the protocols and methods used in internetworking namely, Open System Interconnection (OSI) reference model and TCP/IP model.
- There are three units of Internetworking as explained below:
  1. An **Intranet** is a private network that is contained within an enterprise and is designed in a way that links together different IT systems, hardware, databases and other resources. An Intranet uses TCP/IP, HTTP and other Internet protocols and in general looks like a private version of the Internet.
  2. **Extranet** is a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's very lowest level of Internetworking, usually enforced in an exceedingly personal area.
  3. **Internet** is a selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks.

## 3.8 REFERENCE MODELS

- A reference model in networking is a conceptual layout that describes how communication between devices should occur. For efficient communication, the reference model identifies the tasks involved in inter-computer communication and divides them in logical groups called layers, with each layer performing a specific function.
- A communication system designed in such a manner is referred to as layered architecture. Reference model offers a means of standardization which is acceptable worldwide. Since, people using the computer network are located over a wide physical range.
- In order to provide communication among heterogeneous devices, we need a standardized model i.e. a reference model, which would provide us way how these devices can communicate regardless their architecture.
- The purpose of the reference model was to define an architectural framework that defines the logical communication tasks that are required to move information between different computer systems.
- The two reference models are OSI model and TCP/IP reference model. The OSI model consists of seven layers while TCP/IP consist of four layers.



### 3.8.1 OSI Reference Model

- In 1978, the International Organization for Standardization (ISO) developed an architecture that would allow the devices of different manufacturers to work together to communicate with different operating systems.
- In 1984, the ISO architecture became an international standard known as the Open Systems Interconnection (OSI) reference model. This architecture determines how hardware, software, topologies, and protocols exist and operate on a network.
- The OSI model consists of seven separate but related layers namely, physical, data link, network, transport, session, presentation and application layers.
- Open Systems Interconnection (OSI) model is a reference model developed by ISO (International Organization for Standardization) in 1984.
- OSI model logically groups the functions and sets rules, called protocols, necessary to establish and conduct communication between two or more parties. The model consists of seven functions, often referred to as layers.
- OSI reference model is a logical framework for standards for the network communication. Today many network communication protocols are based on the standards of OSI model.
- OSI defines standards by which computers can communicate together. OSI is simply a set of protocols which govern the various aspects of networking.
- The Reference Model defined by OSI is also an excellent model to understand how networks work. In the OSI model the network/data communication is defined into seven layers. Each layer of OSI model provides services for the next higher layer.
- Each layer communicates logically with its associated layer on the other computer. The layer boundaries should be chosen to minimize the information. Flow across the interfaces.
- In OSI model the packets are sent from one layer to another in the order of the layers, from top to bottom on the sending computer and then in reverse order on the receiving computer. Each layer of OSI model performs a unique, generic, and well-defined function.
- Fig. 3.28 shows OSI reference model.

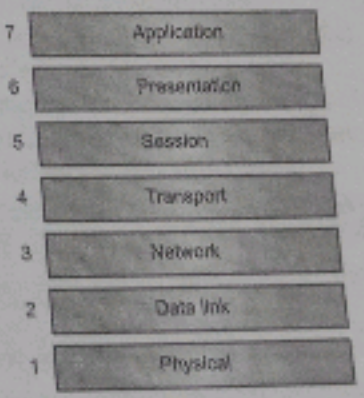



**Fig. 3.28: OSI Model**

- Layer boundaries are designed so that the amount of information flowing between any two adjacent layers is minimized. This is accomplished by having each layer within an open system use the services provided by the layer below. Conversely, each layer provides a sufficient number of services to the layer immediately above it.

**Functions of Each Layer in the OSI Model:**

1. **Physical Layer:**

- The lowest layer of the OSI model (Layer 1) is referred as physical layer. Physical layer deals with the mechanical and electrical specifications of the interface and transmission medium.

**Functions of Physical Layer:**

(i) **Data Encoding:** Physical layer modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

(a) What signal state represents a binary 1 or 0?

(b) How the receiving station knows when a "bit-time" starts.

(c) How the receiving station delimits a frame.

(ii) **Physical Medium Attachment, Accommodating various possibilities in the Medium:**
   (a) Will an external transceiver (MAU) be used to connect to the medium?
   (b) How many pins do the connectors have and what is each pin used for?

(iii) **Transmission Technique:** It determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

(iv) **Physical Medium Transmission:** It transmits bits as electrical or optical signals appropriate for the physical medium, and determines:
   (a) What physical medium options can be used.
   (b) How many volts/db should be used to represent a given signal state, using a given physical medium.

(v) **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both transmitter as well as receiver thus providing synchronization at bit level.

(vi) **Provides Physical Characteristics of Interfaces and Medium:** Physical layer manages the way a device connects to network media.

(vii) **Bit rate control:** Physical layer defines the transmission rate i.e. the number of bits sent in one second. Therefore it defines the duration of a bit.

(viii) **Line Configuration:** Physical layer also defines the way in which the devices are connected to the medium. Two different line configurations are used point to point configuration and multipoint configuration. To activate, maintain and deactivate the physical connection.

(ix) **Transmission Mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are simplex, half-duplex and full-duplex.

(x) **Physical Topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh.

(xi) **Multiplexing:** Physical layer can use different techniques of multiplexing, in order to improve the channel efficiency.

(xii) **Circuit Switching:** Physical layer also provides the circuit switching to interconnect different networks.

- The major protocols used by this layer include Bluetooth, OTN (Optical Transport Network), DSL, IEEE.802.11, IEEE.802.3, and TIA 449.

**2. Data Link Layer:**

- The second layer is referred to as the data link layer. This layer defines how frames of information are constructed. Generally this mean defining how bytes are combined into units called frames.
- Data link layer sends data frames from the Network layer to the Physical layer. The transmission of the data over the communication medium is the responsibility of this layer. The 0s and 1s that are used in the communication are grouped into logical encapsulation called frames.
- Data Link layer consists of following two sub-layers:

**(i) Logical Link Control (LLC) Sub layer:**

- LLC sub layer provides interface between the media access methods and network layer protocols such as Internet protocol which is a part of TCP/IP protocol suite.
- LLC sublayer determines whether the communication is going to be connectionless or connection-oriented at the data link layer.



**(ii) Medium Access Control (MAC) Sub layer:**

- MAC sub layer is responsible for connection to physical media. At the MAC sublayer of Data link layer, the actual physical address of the device, called the MAC address is added to the packet.
- Such a packet is called a Frame that contains all the addressing information necessary to travel from source device to destination device.

**Functions of Data Link Layer:**

(i) **Link Establishment and Termination:** It establishes and terminates the logical link between two nodes.

(ii) **Physical Addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

(iii) **Frame Traffic Control:** Data link layer tells the transmitting node to "back-off algorithm" when no frame buffers are available.

(iv) **Frame Sequencing:** It transmits/receives frames sequentially.

(v) **Frame Acknowledgment:** Data link layer provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

(vi) **Frame Delimiting:** Data link layer creates and recognizes frame boundaries.

(vii) **Frame Error checking:** Data link layer checks received frames for integrity.

(viii) **Media Access Management:** It determines when the node "has the right" to use the physical medium.

(ix) **Flow Control:** It is the traffic regulatory mechanism implemented by Data Link layer that prevents the fast sender from drowning the slow receiver. If the rate at which data is absorbed by receiver is less that the rate produced in the sender, the data link layer imposes this flow control mechanism.

(x) **Error Control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames. It also deals with the problem of duplicate frame, thus providing reliability to physical layer.

(xi) **Access Control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

(xii) **Feedback:** After transmitting the frames, the system waits for the feedback. The receiving device then sends the acknowledgement frames back to the source providing the receipt of the frames.

- The protocols are used by the Data Link Layer includes Point-to-Point Protocol (PPP), Point-to-Point High-Level Data Link Control (HDLC), Serial Line Internet Protocol (SLIP), Spanning Tree Protocol (STP,) Address Resolution Protocol (ARP), IEEE.802.3, ARCNET etc.

**3. Network Layer:**

- The third layer is in the OSI Model the network layer. This layer defines how packets of data are constructed.
- Network layer is responsible for addressing messages and translating logical addresses and names into physical addresses. It determines the route from the source to the destination computer.

**Functions of Network Layer:**

(i) **Subnet Traffic Control:** Network layer routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

(ii) **Logical-physical Address Mapping:** It translates logical addresses, or names, into physical addresses.

(iii) **Subnet Usage Accounting:** It has accounting functions to keep track of frames forwarded by subnet intermediate systems.

(iv) **Internetworking:** One of the main responsibilities of network layer is to provide internetworking between different networks. It provides logical connection between different types of network. It is because of this layer, we can combine various different networks to form a bigger network.

(v) **Logical Addressing:** Large number of different networks can be combined together to form bigger networks or internetwork. In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. Such an address distinguishes each device uniquely and universally.

(vi) **Routing:** When independent networks or links are combined together to create internet works, multiple routes are possible from source machine to destination machine. The network layer protocols determine which route or path is best from source to destination. This function of network layer is known as routing. Routes frames among networks.

(vii) **Packetizing:** The network layer receives the data from the upper layers and creates its own packets by encapsulating these packets. The process is known as packetizing. This packetizing in done by Internet Protocol (IP) that defines its own packet format.

(viii) **Fragmentation:** Fragmentation means dividing the larger packets into small fragments. The maximum size for a transportable packet in defined by physical layer protocol. For this, network layer divides the large packets into fragments so that they can be easily sent on the physical medium. If it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

- The network layer uses protocols such as Internet Protocol (IP), Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), Internet Protocol Security (IPsec), Internetwork Packet Exchange (IPX), Routing Information Protocol (RIP) etc.

**4. Transport Layer:**

- Layer 4 of the OSI model is the transport layer. Transport layer is responsible for packet creation.
- Transport layer ensures that packets are delivered error free, in sequence with no losses or duplications. Transport layer provides flow control, error handling, and solves transmission problems.
- Transport layer provides following two types of services:
  - (i) In **Connection Oriented Transmission** the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is also known as reliable transport method. Because connection oriented transmission requires more packets be sent across network, it is considered a slower transmission method.
  - (ii) In **Connectionless Transmission** the receiver does not acknowledge receipt of a packet. Sending device assumes that packet arrive just fine. This approach allows for much faster communication between devices.

***Functions of Transport Layer:***

(i) **Segmentation of Message into Packet and Reassembly of Packets into Message:** It accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

(ii) **Message Acknowledgment:** It provides reliable end-to-end message delivery with acknowledgments.



(iii) **Message Traffic Control:** It tells the transmitting station to "back off" when no message buffers are available.

(iv) **Session Multiplexing:** It multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions.

(v) **Service Point Addressing:** The purpose of transport layer is to delivery message from one process running on source machine to another process running on destination machine. It may be possible that several programs or processes are running on both the machines at a time. In order to delivery the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process on destination machine.

(vi) **Flow Control:** Like data link layer, transport layer also performs flow control. Transport layer makes sure that the sender and receiver communicate at a rate they both can handle. Therefore flow control prevents the source from sending data packets faster than the destination can handle. Here, flow control is performed end-to-end rather than across a link.

(vii) **Error Control:** Like data link layer, transport layer also performs error control. Here error control is performed end-to-end rather than across a single link. The sending transport layer ensures that the entire message arrives at the receiving transport layer without error (damage, loss or duplication). Error correction is achieved through retransmission.

- Some protocols used by transport layer includes Datagram Congestion Control Protocol (DCCP), Stream Control Transmission Protocol (SCTP), Internetwork Packet Exchange/ Sequenced Packet Exchange (IPX/SPX), Structured Stream Transport (SST), User Datagram Protocol (UDP) etc.

**5. Session Layer:**

- The session layer is the 5th layer of the OSI model. Session layer establishes, maintains the interactions between communicating system.
- Session layer allows two applications running on different computers to establish use and end a connection called a Session. Session layer performs name recognition and security.
- The session layer allows users on different machines to establish sessions between them. Sessions offers various services, including dialogue control.

**Functions of Session Layer:**

(i) **Session Establishment, Maintenance and Termination:** It allows two application processes on different machines to establish, use and terminate a connection, called a session.

(ii) **Session Support:** It performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging and so on.

(iii) **Dialog Control:** Dialog control is the function of session layer that determines which device will communicate first and the amount of data that will be sent. When a device is contacted first, the session layer is responsible for determining which device participating in the communication will transmit at a given time as well as controlling the amount of data that can be sent in a transmission. This is called dialog control. The types of dialog control that can take place include simplex, half duplex and full duplex.

(iv) **Dialog Separation or Synchronization:** The session layer is also responsible for adding checkpoint or markers within the message. This process of inserting markers to the stream of data is known as dialog separation.

- The protocols used in session layer includes Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), Network Basic Input Output System (NetBIOS), PAP (Password Authentication Protocol), Sockets Direct Protocol (SDP) etc.

**6. Presentation Layer:**

- The 6th layer of OSI modal is the Presentation layer. It serves as a translator layer of the OSI model and it is responsible for data conversion and encryption.
- The presentation layer may translate data from a format used by the application layer into a common format at the sending station, and then translate the common format to a format known to the application layer at the receiving station.

**Functions of Presentation Layer:**

(i) **Translations:** Different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependant format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependant format.

(ii) **Encryption:** The process of rendering a message (or data) unusable to all but the intended recipients, who have the ability to decrypt it.

(iii) **Compression:** Reduces the number of bits to be transmitted. Saves network bandwidth.

- The presentation layer uses protocols Multipurpose Internet Mail Extensions (MIME) Network News Transfer Protocol (NNTP), Transport Layer Security (TLS) and Secure Sockets Layer (SSL) etc.

**7. Application Layer:**

- Application layer is top most layer (Layer 7) of OSI model.
- Application layer provides the interface and services that supports user applications and provides general access to the network. Application layer serves as a window for applications to access network services.

***Functions Application Layer:***

(i) **Network Virtual Terminal:** It allows a user to log on to a remote host.

(ii) **File Transfer, Access and Management (FTAM):** This application allows a user to access files in a remote computer (to make changes or read data), to retrieve files from a remote computer, and to manage or control files in a remote computer.

(iii) **Mail Service:** This application provides the basis for e-mail forwarding and storage.

(iv) **Remote Logins:** This layer allows logging into a host which is remote.

(v) **Network Abstraction:** Provides an abstraction of the underlying network to an end user and an application.

(vi) **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

- Application layer uses protocols such as Secure Shell (SSH), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Reverse Address Resolution Protocol (RARP), Bootstrap Protocol (BOOTP), Simple Network Management Protocol (SNMP), Border Gateway Protocol (BGP), Hypertext Transfer Protocol (HTTP) etc.
- The main **benefits of the OSI model** include the following:

1. Helps users understand the big picture of networking.



2. Helps users understand how hardware and software elements function together.
3. Makes troubleshooting easier by separating networks into manageable pieces.
4. Defines terms that networking professionals can use to compare basic functional relationships on different networks.
5. Helps users understand new technologies as they are developed.
6. Aids in interpreting vendor explanations of product functionality.

**Layered Architecture of the OSI Model:**

- Each interface defines what information and services a layer must provide for the layer above it. Fig. 3.29 shows layered architecture of OSI model.

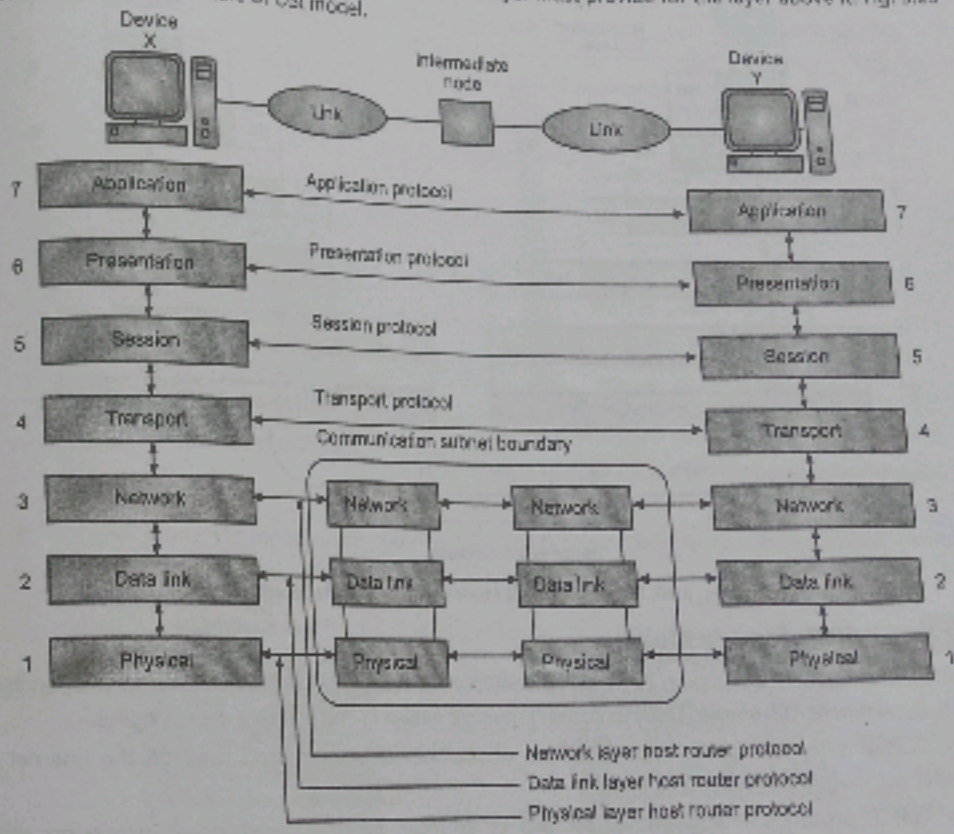



**Fig. 3.29: Layered Architecture of the OSI Model**

- Layer 1, 2, and 3 are the network support layers; they deal with physical aspect of moving data from one device to another (such as electrical specification, physical connection). Layer 4, ensures end-to-end reliable data transmission. Layers 5, 6, and 7 are user support layer.
- The upper OSI layers are almost always implemented by software; lower layers are a combination of hardware and software, except physical layer, which is mostly hardware.
- This layered approach was selected as a basis for the OSI Reference Model to provide flexibility and open-ended capability through defined interfaces.
- The interfaces permit some layers to be changed while leaving other layers unchanged. In principle, as long as standard interfaces to the adjacent layers are adhered to, an implementation can still work.

- For example, a system implementation could use either HDLC or local area network protocols as the data link layer. Similarly, a particular layer such as the presentation layer, can be implemented as a null layer for the time being. This means the layer is functionally empty, providing only the mandatory interfaces between the upper and lower layers, (application and session layers respectively).

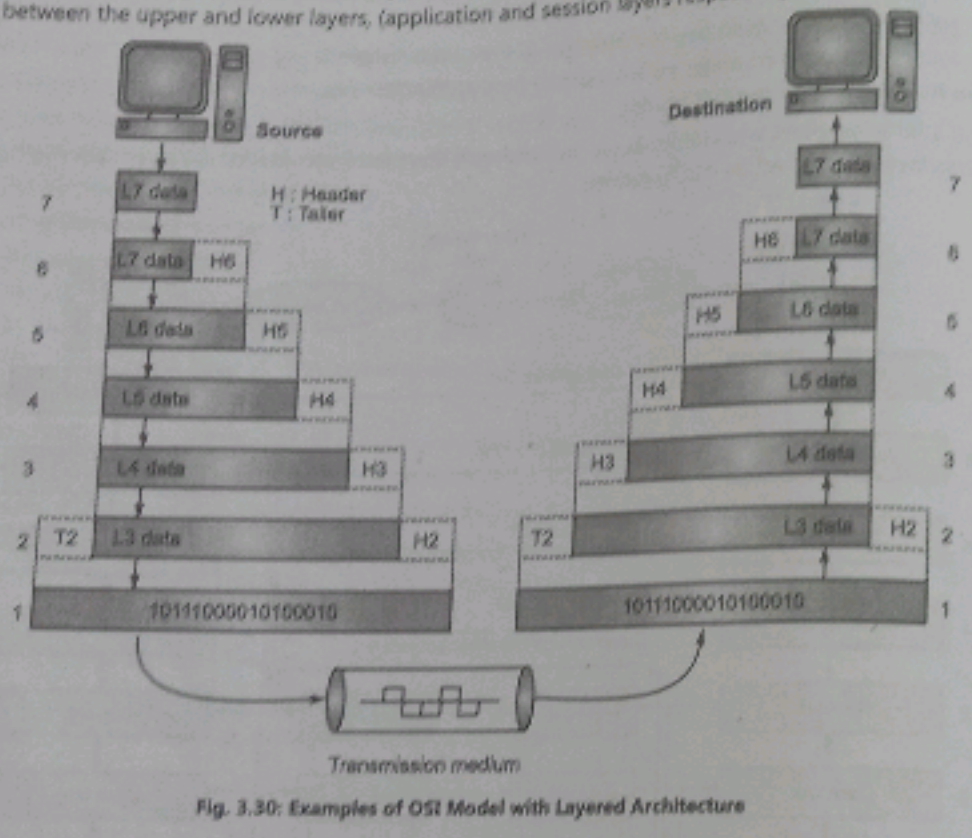



**Fig. 3.30: Examples of OSI Model with Layered Architecture**

## 3.8.2 TCP/IP Reference Model

- TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP model was developed by the U.S. Department of Defense (DoD) to connect multiple networks and preserve data integrity.
- The TCP/IP is the conceptual model and set of communications protocols used on the Internet and similar computer networks.
- The TCP/IP protocol suite is named for two of its most important protocols Transmission control protocol (TCP) and Internet protocol (IP). The TCP/IP protocol suite establishes the technical foundation of the Internet.
- TCP/IP protocol suite also called as Internet protocol suite. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.
- TCP/IP protocol model came after the OSI model and the numbers of layers in TCP/IP differ from that of the OSI model. TCP/IP model comprises of four layers, namely, network access (also called host-to-network layer), Internet, transport and application layers.
- The network access layer of TCP/IP model corresponds to the combination of physical and data link layers of OSI model. The Internet layer corresponds to the network layer of OSI model and the application layer performs tasks of session, presentation and application layers of OSI model with the transport layer of TCP/IP performing a part of responsibilities of session layer of OSI model.



**Layered Structure of TCP/IP:**

- TCP/IPs an industry-standard protocol suite for wide area networks (WANs) developed in the 1970s and 1980s by the U.S. Department of Defense (DoD).
- TCP/IP is not one protocol, but is a suite of many protocols. The protocols define applications, transport controls, networking, routing, and network management.
- The TCP/IP is a set of protocols, or a protocol suite, that defines how all transmission are exchanged across the Internet.
- Fig. 3.31 shows TCP/IP reference model. It is a hierarchical model, i.e. there are multiple layers and higher layer protocols are supported by lower layer protocols. TCP/IP protocol architecture is shown in Fig. 3.32.

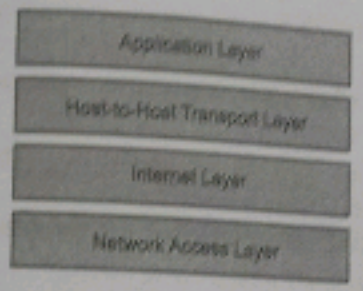



**Fig. 3.31**

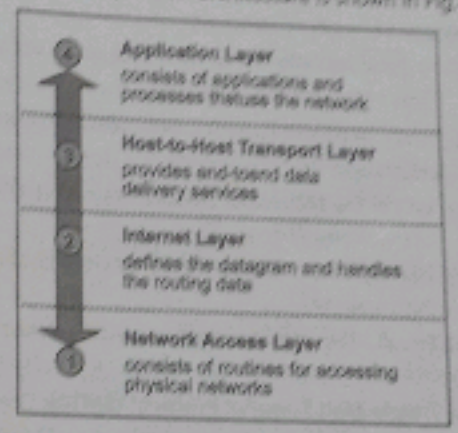



**Fig. 3.32: Layers in the TCP/IP Protocol Architecture**

- TCP/IP is a four layer model. Each layer of the TCP/IP protocol suite has its associated component protocols.

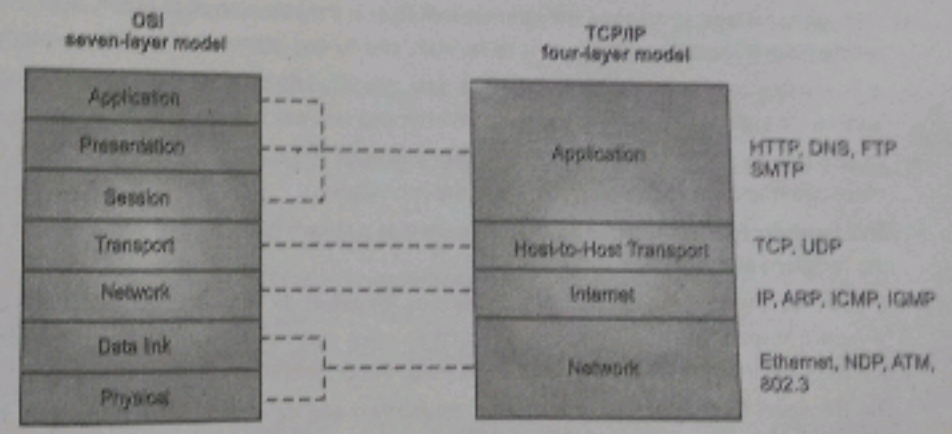



**Fig. 3.33: OSI Model and TCP/IP Model**

- Layers in TCP/IP reference model are explained below:

**1. Application Layer:**

- The top/highest layer in the Internet reference model is the application layer. This layer provides functions for users or their programs, and it is highly specific to the application being performed.

- Application layer provides the services that user applications use to communicate over the network, and it is the layer in which user-access network processes reside. These processes include all of those that users interact with directly, as well as other processes of which the users are not aware.
- This layer includes all applications protocols that use the host-to-host transport protocols to deliver data. Other functions that process user data, such as data encryption and decryption and compression and decompression, can also reside at the application layer.
- The application layer also manages the sessions (connections) between cooperating applications. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

**Functions of Application Layers:**

(i) It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

(ii) The functions such as LOGIN or password checking are also performed by the application layer.

**Application Layer Protocols:**

**(i) HTTP:** The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.

**(ii) File Transfer Protocol (FTP):** A protocol that enables a client to send and receive complete files from a server.

**(iii) Telnet:** The protocol that lets you connect to another computer on the Internet in a terminal emulation mode.

**(iv) Simple Mail Transfer Protocol (SMTP):** One of several key protocols that are used to provide e-mail services.

**(v) Domain Name System (DNS):** The protocol that allows you to refer to other host computers by using names rather than numbers.

**2. Host-to-Host Transport Layer:**

- The protocol layer just above the internetwork layer is the host-to-host transport layer. The primary job of the host-to-host transport layer is to facilitate end-to-end communication over an internetwork.
- It is responsible for providing end-to-end data integrity and provides a highly reliable communication service for entities that want to carry out an extended two-way conversation.
- In addition to the usual transmit and receive functions, the host-to-host transport layer uses open and close commands to initiate and terminate the connection.
- This layer accepts information to be transmitted as a stream of characters, and it returns information to the recipient as a stream.
- The service employs the concept of a connection (or virtual circuit). A connection is the state of the host-to-host transport layer between the time that an open command is accepted by the receiving computer and the time that the close command is issued by either computer.
- The transport layer is where sessions are established and data packets are exchanged between hosts. Two core protocols are found at this layer:

**Functions of Transport Layer:**

(i) It uses TCP and UDP protocol for end to end transmission.

(ii) TCP is reliable and connection oriented protocol.

(iii) TCP also handles flow control.

(iv) The UDP is not reliable and a connection less protocol also does not perform flow control.



**Transport Layer Protocols:**

**(i) Transmission Control Protocol (TCP):** Provides reliable connection oriented transmission between two hosts. TCP establishes a session between hosts, and then ensures delivery of packets between the hosts.

**(ii) User Datagram Protocol (UDP):** Provides connectionless, unreliable, one-to-one or one-to-many delivery.

**3. Internet Layer:**

- The Internet layer of TCP/IP is associated with the network layer of the OSI model. In the Internet reference model, the layer above the network access layer is called the internetwork layer.
- This layer is responsible for routing messages through internetworks. Two types of devices are responsible for routing messages between networks. The first device is called a gateway, which is a computer that has two network adapter cards.
- This computer accepts network packets from one network on one network card and routes those packets to a different network via the second network adapter card. The second device is a router, which is a dedicated hardware device that passes packets from one network to a different network.

**Internet Layer Protocols:**

**(i) The Internet Protocol (IP)** is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.

**(ii) The Address Resolution Protocol (ARP)** is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.

**4. Network Access Layer:**

- The network access layer is the lowest layer in the Internet reference model. It defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
- This layer contains the protocols that the computer uses to deliver data to the other computers and devices that are attached to the network.
- The protocols like Ethernet, ATM, Neighbor Discovery Protocol (NDP), 802.3 etc. at this layer perform three distinct functions:
  - (i) They define how to use the network to transmit a frame, which is the data unit passed across the physical connection.
  - (ii) They exchange data between the computer and the physical network.
  - (iii) They deliver data between two devices on the same network.
- Unlike higher level protocols, the network access layer protocols must understand the details of the underlying physical network, such as the packet structure, maximum frame size, and the physical address scheme that is used.
- Understanding the details and constraints of the physical network ensures that these protocols can format the data correctly so that it can be transmitted across the network.
- Ethernet is one example protocol at the TCP/IP network interface layer. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

**OSI Reference Model vs TCP/IP Reference Model:**

| Sr. No. | OSI Reference Model | TCP/IP Model |
|---|---|---|
| 1. | OSI refers to Open Systems Interconnection. | TCP refers to Transmission Control Protocol/ Internet Protocol. |
| 2. | OSI model had Seven (7) layers. | TCP/IP model has Four (4) layers. |
| 3. | OSI is less reliable. | TCP/IP is more reliable. |
| 4. | Developed by ISO (International Standard Organization). | Developed by Department of Defense (DoD). |
| 5. | OSI is a conceptual model. | TCP/IP is a client-server model, i.e. when the client requests for service it is provided by the server. |
| 6. | OSI model is useful in describing networks, but protocols are too general. | TCP/IP model is weak, but protocols are specific and widely used. |
| 7. | Protocol Independent Standard. | Protocol dependent standard. |
| 8. | Protocols are hidden in OSI model and are easily replaced as the technology changes. | Replacing protocol is not easy. |
| 9. | OSI follows a Horizontal approach. | TCP/IP follows a vertical approach. |
| 10. | OSI Model follows a bottom-up approach. | TCP/IP follows top to bottom approach |
| 11. | In OSI model, model was developed before the development of protocols. | In TCP/IP model, Protocol were developed first and then the model was developed. |
| 12. | OSI has strict boundaries. | TCP/IP does not have very strict boundaries. |
| 13. | Model describes any type of network. | Model only describes TCP/IP which is not useful for describing any other networks. |
| 14. | Network layer supports both connection oriented and connectionless service. | Network layer supports only connectionless service. |
| 15. | OSI model represents and ideal. | TCP/IP network model represents reality in the world. |
| 16. | In OSI model, transport layer guarantees delivery of packets. | In TCP/IP model, transport layer does not Guarantees delivery of packets. |
| 17. | Transport layers supports only connection oriented service. | Transport layers supports both Connection oriented and connectionless service. |
| 18. | Separate session and presentation layer | Combines the session and presentation layer in the application layer. |



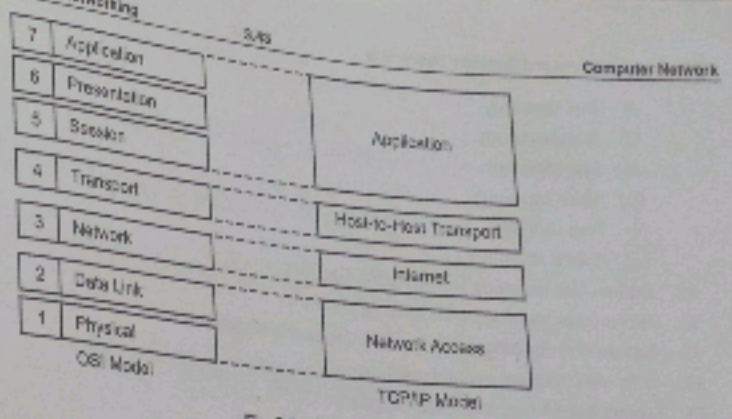



Fig. 3.34

## Practice Questions

1. What is network?
2. What is computer network?
3. Define the terms: Network and Computer Network.
4. What is meant by transmission mode?
5. Explain the components of computer network with diagram.
6. What is meant by simplex mode of transmission? State its advantages and disadvantages.
7. What is meant by half-duplex mode transmission? State its advantages and disadvantages.
8. What is meant by full-duplex mode transmission? State its advantages and disadvantages.
9. Describe the term parallel transmission in detail.
10. Describe the term serial transmission with advantages.
11. Describe the term protocols in detail.
12. Explain the asynchronous communication mode.
13. Explain the synchronous communication mode with suitable diagram.
14. Explain the most common useful protocols.
15. Elaborate the term standard organizations.
16. Describe the various standards for protocol.
17. What is meant LAN? State its advantages and disadvantages.
18. What is meant MAN? State its advantages and disadvantages.
19. What is meant WAN? State its advantages and disadvantages.
20. Compare LAN, MAN and WAN.
21. What is meant by reference model?
22. Enlist types of reference models.
23. Explain network architecture diagrammatically.
24. What is TCP/IP?
25. What is OSI meant by OSI model and TCP/IP model
26. With the help of diagram describe OSI model.
27. List out various layers of OSI model.
28. What is network topology?
29. Define the following topologies with their advantages and disadvantages.

(i) Bus topology.
(ii) Ring topology.
(iii) Star topology.
(iv) Mesh topology.
(v) Tree topology.
(vi) Hybrid topology.

30. Explain bus topology with suitable diagram.
31. Explain star topology with suitable diagram.
32. Explain ring topology with its advantages and disadvantages.
33. With neat diagram explain mesh topology.
34. Explain hybrid topology with diagram.
35. Describe tree topology in detail.
36. Explain TCP/IP model diagrammatically.
37. List out various layers as TCP/IP.
38. Enlist functions of each layer in OSI model.
39. Enlist functions of each layer in TCP/IP model.
40. Compare OSI model and TCP/IP model.

❖❖❖

*Chapter* **4...**

# Transmission Media and Network Devices

**Contents**

## 4.0 INTRODUCTION

- Media is the general term used to describe the specific data path that forms the physical channel between sender (source) and receiver (destination).
- Communication medium refers to the physical channel through which data is sent and received. In short, communication media is a pathway that carries the information/data from sender to receiver.
- Data is sent in the form of voltage levels which make up the digital signal. A digital signal consists of 0s and 1s; essentially, a 1 corresponds to a high voltage, while a 0 corresponds to a low voltage.
- Communication media is broadly classified into two groups Wired or Guided Media or Bounded Transmission Media (twisted pair cable, co-axial cable and fiber optical cable etc.) and Wireless or Unguided Media or Unbounded Transmission Media (Microwave, Radio wave, Infrared etc.).
- Switching and multiplexing are both techniques we use to make data communication more economical and scalable. Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.
- Computer networking devices, are physical devices which are required for communication and interaction between devices on a computer network.
- Computer networking devices are units that mediate data in a computer network and are also called as network equipment. Networking devices may include gateways, routers, bridges, modems, switches, hubs, and repeaters and so on.

## 4.1 CONCEPT OF TRANSMISSION MEDIA

- Transmission media means a communication signal is carried from one computer system to another. The physical path over which the information flows from transmitter to receiver is called the transmission medium/communication media.
- The transmission medium is usually free space, metallic cable or fiber-optic cable.

***Need of Transmission/Communication Media:***

1. Transmission media are needed for interacting with the devices.
2. Without transmission media communication cannot take place.
3. Communication media is the middle part of sender and receiver.
4. Transmission media is needed for faster communication.
5. It is needed for reliable delivery of data with efficient methods.
6. Transmission media is needed for secure transmission of data.

**Definition of Transmission Media:**

- A transmission medium can be defined as, "anything that can carry information from a source to a destination". **OR**
- We can define transmission medium as, "the physical path between transmitter and receiver in a data transmission system."
- Fig. 4.1 shows transmission of data from sender to receiver through a medium.

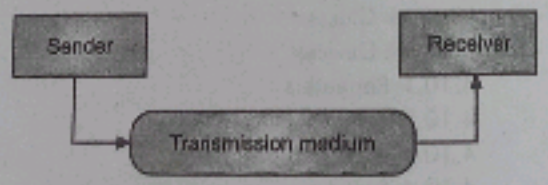



**Fig. 4.1: Transmission of Data from Sender to Receiver through a Medium**

***Criteria to Selection of Transmission Media:***

- For selecting communication/transmission media following factors are considered:
  1. **Transmission Rate** refers to the speed or data transmission rate.
  2. **Bandwidth** is the measure of the capacity of the transmission medium to transmit data. The bandwidth of a cable is determined by cable length (short cable generally can accommodate greater bandwidth than a long cable) and Frequency (high-frequency frequency signals can deteriorate more and higher frequency means higher bandwidth).
  3. **Attenuation** is a measure of how much a signal weakens as it travels through a medium. Attenuation refers to loss of energy as signal propagates outwards. The amount of energy lost depends on frequency.
  4. **No. of Users (Density)** is the concurrent number of users supported/connected by the communication media.
  5. **Noise Absorption** refers to the susceptibility of the media to external electrical noise that can cause distortion of data signal.
  6. The **cost** of the transmission media.
  7. The **data security** capabilities provided by the transmission media.
  8. The communication medium should be **flexible** in order to expand network, the need for extra equipment or devices.
  9. The consistency of transmission media (effect of weather conditions) is **reliable**.
  10. **Radiation** refers to the leakage of signal from the medium due to undesirable electrical characteristics of the medium.
- Fig. 4.2 shows categories of transmission media.



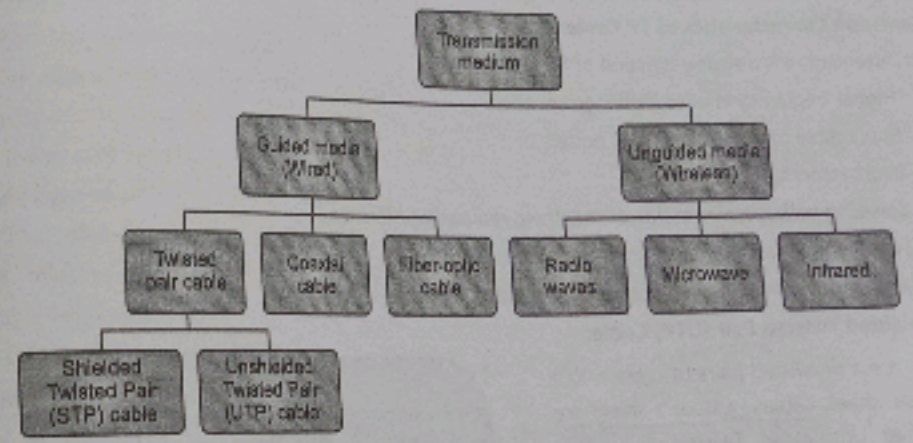



**Fig. 4.2: Categories of Transmission Media**

### 4.1.1 Guided Transmission Media

- Guided transmission media uses a cabling system that guides the data signals along a specific path. Guided media also known as bounded media which, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

#### 4.1.1.1 Twisted Pair (TP) Cable

- Twisted pair cable is the most common type of cable used in data communication. It is reliable, flexible and cost effective.
- The least-expensive and most widely-used guided transmission medium is twisted pairs. A twister pair consists of two conductors (normally copper). Each with its own plastic insulation, twisted together as shown in Fig. 4.3.