# BCA501 : COMPUTER NETWORKS

**UNIT -1:**

Need of network. Network classifications-LAN, MAN , WAN, wireless networks & Internet. Data and signals-analog and digital,&#65533; periodic analog signals, digital signals, bit rate, baud rate, bandwidth .&#65533; Transmission impairments- attenuation distortion and noise.&#65533; Data communication protocols and standards, Network models - OSI model-layers and their functions. TCP/IP protocol suite.

**UNIT-2**

Bandwidth utilization Multiplexing:&#65533; FDM, TDM, spread spectrum. Transmission Media- guided media and unguided media. Switching: message, Circuit and packet switched networks, datagram networks, virtual- circuit networks.

**UNIT-3**

Hop to Hop Delivery. Error Detection and Correction &#65533;Type of Errors, Redundancy, Detection ,Correction, Forward Error and Retransmission. Coding -Block Coding(Parity Chek Code and Hamming Code) and Cyclic Codes.&#65533; Framing, flow and error control, Protocols - Noiseless channels (Simplest , Stop and Wait) and Noisy channels(Stop and Wait and Piggy Backing) .

**UNIT-4**

&#65533;Multiple Access Protocols .&#65533; Random Access-ALOHA, CSMA. Wired&#65533; LANs-IEEE standards, standard Ethernet, wireless LANs-Bluetooth, Wireless Lan- Cellular Telephony-Frequency Reuse Principle ,Transmitting, Receiving, Handoff, Hard Hand off, Soft Hand off, Roaming .&#65533; Cellular Telephony Generations &#65533;First, Second and Third generations. Satellite Networks &#65533;Geo, Meo,&#65533; Leo.

**UNIT-5**

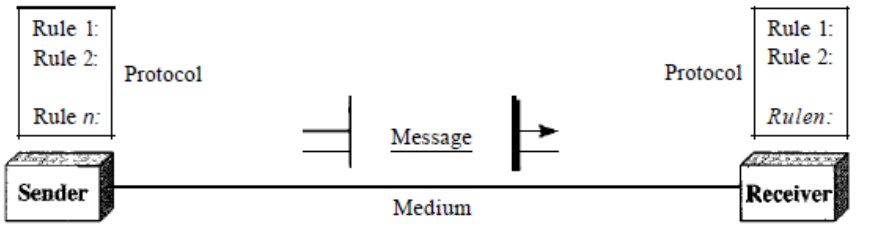
Host- To-Host&#65533; Communication . Network Level Logical addressing-IPv4 addresses, IPv6 addresses, Internet protocol-IPv4 andIPv6,&#65533; Process to Process&#65533; Delivery &#65533;Connectionless and Connection Oriented Service : UDP, TCP. Congestion control, quality of service. Client Server Programs. &#65533;Name space, domain name space, Remote logging, Electronic mail, file transfer.

***Book of study*** *:* Data communication and Networking (fourth edition)-B. A. Forouzan

**UNIT -1:**
Need of network. Network classifications-LAN, MAN , WAN, wireless networks & Internet. Data and signals-analog and digital,• periodic analog signals, digital signals, bit rate, baud rate, bandwidth .• Transmission impairments- attenuation distortion and noise.• Data communication protocols and standards, Network models - OSI model-layers and their functions. TCP/IP protocol suite.

A data communications system has five components.

*Five components of data communication*




The *message* is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
The *sender* is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
The *receiver* is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
The *transmission medium* is the physical path by which a message travels from sender to receiver. Some examples of transmission media
include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
A *protocol* is a set of rules that govern data communications. It represents
an agreement between the communicating devices.

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

## 1.Need of Network

There are several reasons why networking is essential to a business, institution or individual.

These benefits include:

1.**Information exchange** To exchange data and information between different individual users,

it is necessary to interconnect the individual users' computers.

**2.Resource sharing** The cost of computer has come down. However, the cost of a laser printer, bulk storage, and large enterprise software remains high. When computers are interconnected, there is a possibility that, users connected to the network may share the above mentioned resources. Printers, copiers and backup storages are shared among employees. This eliminates the need to buy

single IT assets for each employee. Unlike traditional desktops, you don't need frequent software installations. You only need to install updates and track performance.

3. **Central Data storage**

Computer networks pools their entire data to a central data storage server which can be made accessible to others.

With a central serve the number of storage servers needed is reduced which increase the efficiency of operations.

4. **Flexible operations**

Computer networks enable flexible operations. You can access your data from any device. This enhances free movement while accessing your data wherever you may be.

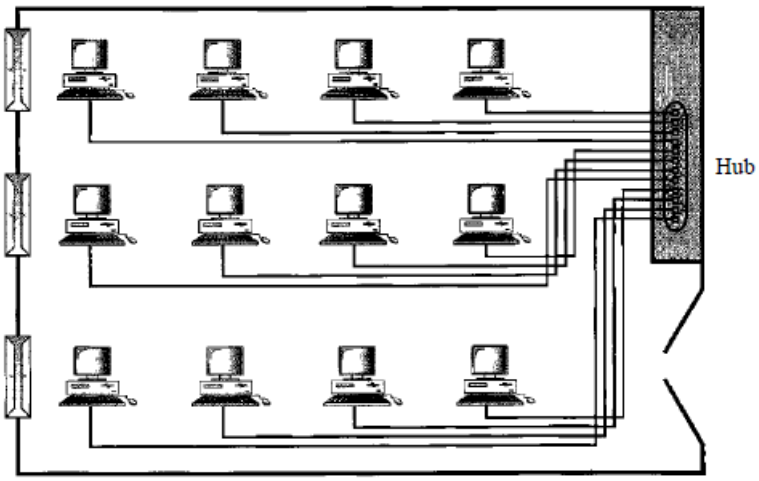
5**. Real Time communication**

Computer networking is a massive boon to the communication landscape. Networking allows you to send and receive text messages and files in real time. Information is available and easy to access from any device. You only need a reliable internet connection. Even if your device shuts down, you log in from a different device and access your data.

## 2.Network classifications

2.1 Classification based on the size (scale) of the Networks.

2.1.1 Local Area Network (LAN) : A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus of up to few kilometers in size. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Data rates of LANs are normally 100 or 1000 Mbps. The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI(Fiber Distributed Data Interface), and ATM LAN.




2.1.2 Metropolitan area networks (MAN) : MAN is designed to extend over the entire city. (Networks of a size in between a LAN and a WAN are normally referred to as metropolitan area networks and span tens of miles.) It may be means of connecting a number of LANs into a larger network.

It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

DQDB (Distributed Queue Dual Bus) or IEEE 802.6 standard has been adopted for them.

Examples :

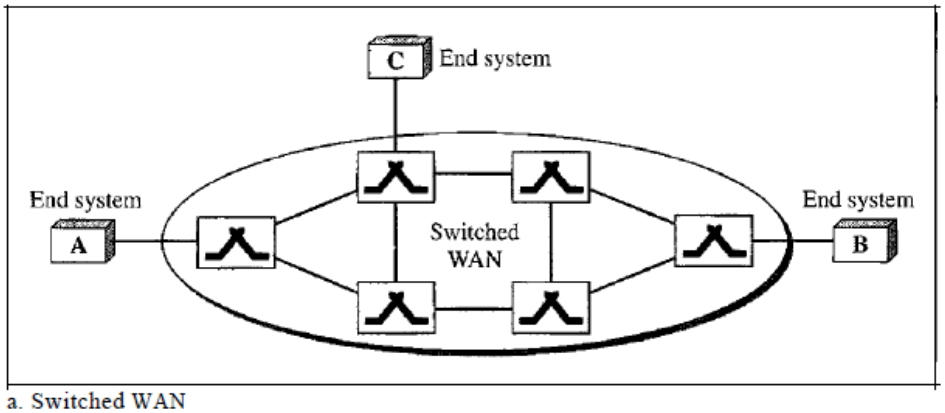
- Part of the telephone company network that can provide a high-speed DSL line to the customer.
- The cable TV network (It can also be used for high-speed data connection to the Internet.)

2.1.3 Wide area network (WAN) :

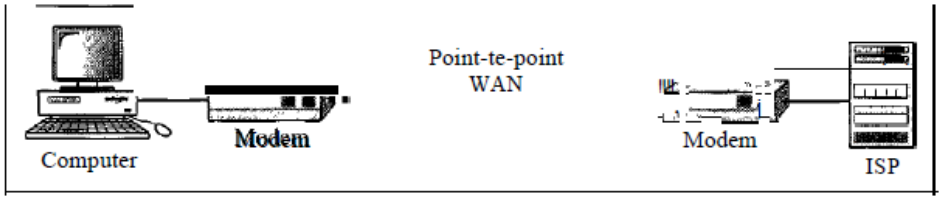
WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In contrast to LANs, WANs may utilize public, leased or private communication devices, usually in combinations, and can therefore span an unlimited number of miles.

Examples of WAN:

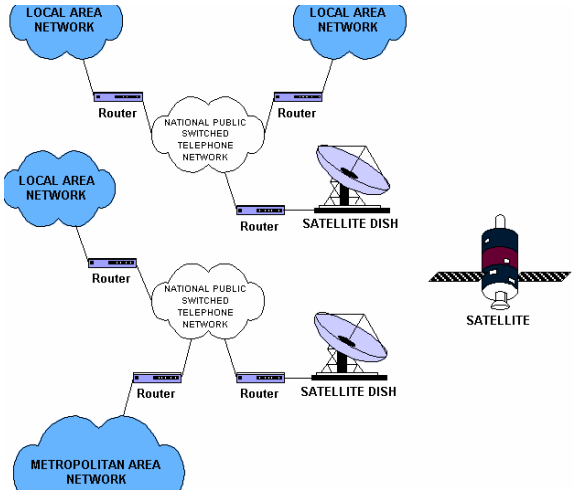
- X.25 (It is an earlier switched WAN)
- Frame Relay ( high-speed, more efficient network)
- Asynchronous transfer mode (ATM) network (It is a switched WAN, with fixed-size data unit packets called cells.)
- Wireless WAN (It is becoming more and more popular.)




a. Switched WAN



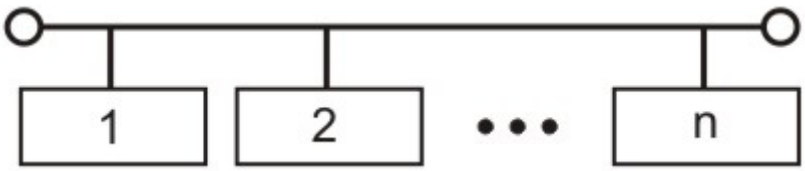

b. Point-to-point WAN



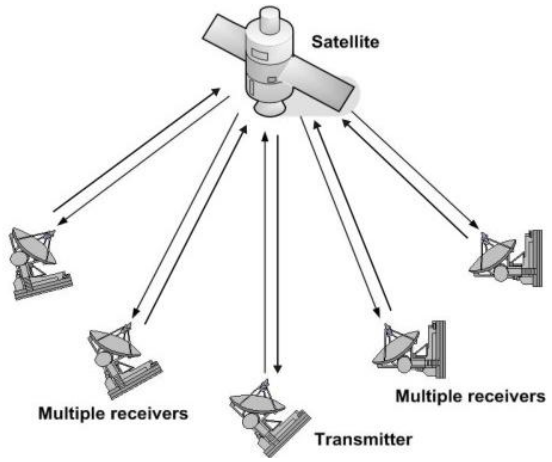

## 2.2 Classification of Computer networks based on transmission technologies:

### 2.2.1 Broadcast Networks

Broadcast network have a single communication channel that is shared by all the machines on the network. All the machines on the network receive short messages ( packets), sent by any machine. An address field within the packet specifies the intended recipient. Upon receiving a packet, machine checks the address field. If packet is intended for itself, it processes the packet; if packet is not intended for itself it is simply ignored.



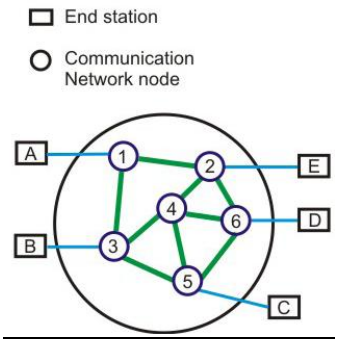

*Example of a broadcast network based on shared bus*




*Example of a broadcast network based on satellite communication*

This system generally also allows possibility of addressing the packet to all destinations (all nodes on the network). When such a packet is transmitted and received by all the machines on the network. This mode of operation is known as *Broadcast Mode*. Some Broadcast systems also supports transmission to a sub-set of machines, something known as *Multicasting*.

2.2.2. Point-to-Point Networks




*Communication network based on point-to-point communication*

The end devices that wish to communicate are called *stations*. The switching devices are called *nodes*. Some Nodes connect to other nodes and some to attached stations. It uses Frequency division multiplexing (FDM) or time division multiplexing (TDM) for node-to-node communication. There may exist multiple paths between a source-destination pair for better network reliability. The switching nodes are not concerned with the contents of data. They provide a switching facility that will move data from node to node until they reach the destination.

Smaller, geographically localized networks tend to use broadcasting, whereas larger networks normally use point-to-point communication.

## 3. Wireless networks

Wireless network refers to any type of computer network that is not connected by cables of any kind.

Wireless networks use radio waves to send information between computers.

The three most common wireless network standards are 802.11b, 802.11g, and 802.11a. A new standard, 802.11n, is expected to grow in popularity.

**Pros**

- It's easy to move computers around because there are no cables.
- Wireless networks are usually easier to install than Ethernet.

**Cons**

- Wireless is often slower than the other three technologies.
- Wireless can be affected by interference from things such as walls, large metal objects, and pipes. Also, many cordless phones and microwave ovens can interfere with wireless networks when they're in use.
- Wireless networks are typically about half as fast as their rated speed under all but ideal conditions.

## 3.1 Types of wireless Networks

### 3.1.1 Wireless LAN

A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method.
Two wireless technologies for LANs:
IEEE 802.11 wireless LANs ( wireless Ethernet) and
Bluetooth ( a technology for small wireless LANs)

### 3.1.2 Wireless MAN

Wireless Metropolitan Area Networks connects several wireless LANs.

- WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard.

### 3.1.3 Wireless WAN

Wireless wide area networks cover large areas. These networks can be used to connect branch offices of business or as a public internet access system. The wireless connections between access points are usually point to point microwave links.
3.1.4 Mobile devices networks
With the development of smartphones, cellular telephone networks routinely carry data in addition to telephone conversations:

- Global System for Mobile Communications (GSM): GSM is the most common standard and is used for a majority of cell phones.
- Personal Communications Service (PCS): PCS is a radio band that can be used by mobile phones in North America and South Asia.

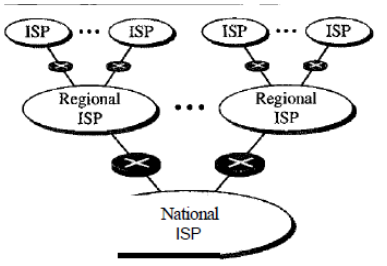
## 4. Internet

A network is a group of connected communicating devices such as computers and printers. When two or more networks are connected, they become an internetwork, or internet.

The most notable internet is called the **Internet** (uppercase letter I). It is a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. The Internet has come a long way since the 1960s.

The Internet today is made up of many wide- and local-area networks joined by connecting devices and switching stations. Today most end users who want Internet connection use the services of Internet service providers (lSPs). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government.




a. Structure of a national ISP

*International Internet Service Providers:* At the top of the hierarchy are the international service providers that connect nations together.

*National Internet Service Providers:* The national Internet service providers are backbone networks created and maintained. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* They normally operate at a high data rate (up to 600 Mbps).

*Regional Internet Service Providers:* Regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

*Local Internet Service Providers:* Local ISPs provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. A local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a non-profit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

## 5. Data and Signals

Data refers to information that conveys some meaning based on some mutually agreed up rules or conventions between a sender and a receiver. Today it comes in a variety of forms such as text, graphics, audio, video and animation.

Data can be analog or digital.

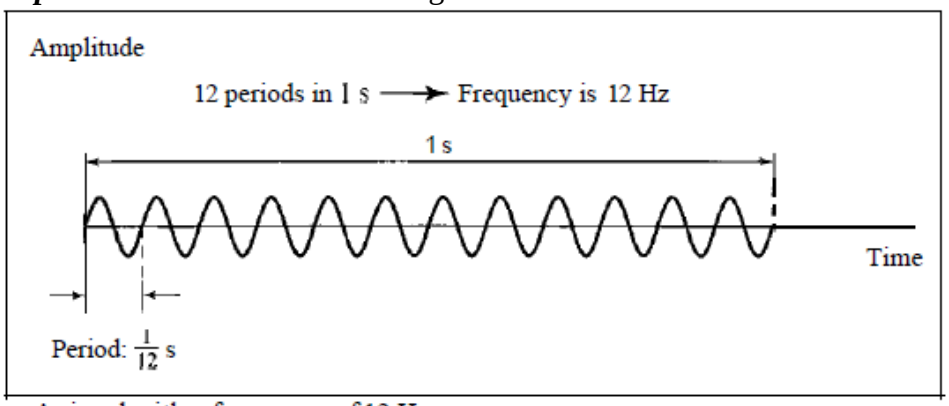
Generally, the data usable to a person or application are not in a form that can be transmitted over a network. To be transmitted, data must be transformed to electromagnetic signals. For example, a microphone converts voice data into voice signal, which can be sent over a pair of wire.

Signal : It is electrical, electronic or optical representation of data, which can be sent over a communication medium.

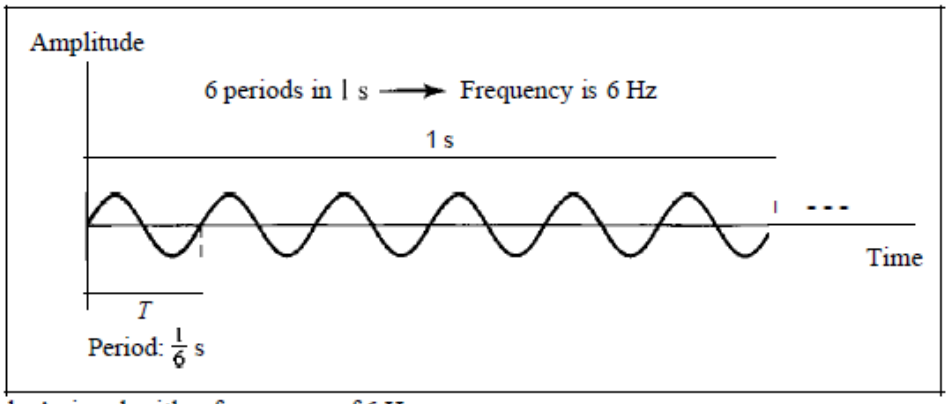
Signal Characteristics : A signal can be represented as a function of time, i.e. it varies with time. It can be also expressed as a function of frequency, i.e. a signal can be considered as a composition of different frequency components.

Thus, a signal has both time-domain and frequency domain representation.

***Amplitude*:** It is the value of the signal at different instants of time. It is measured in volts.



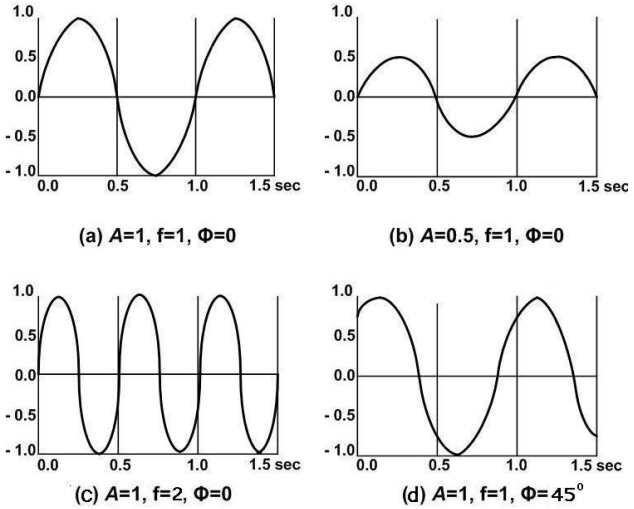

a. A signal with a frequency of 12 Hz




b. A signal with a frequency of 6 Hz

***Frequency*:** It is inverse of the time period, i.e. f = 1/T. The unit of frequency is Hertz (Hz) or cycles per second.

***Phase*:** It gives a measure of the relative position in time of two signals within a single period. It is represented by φ in degrees or radian.




*The phase angle φ indicated in the figure is with respect to the reference waveform shown in Fig.(a).*

## 5. 1. Analog And Digital Data

Analog data are continuous and take continuous values. Digital data have discrete states and take discrete values.

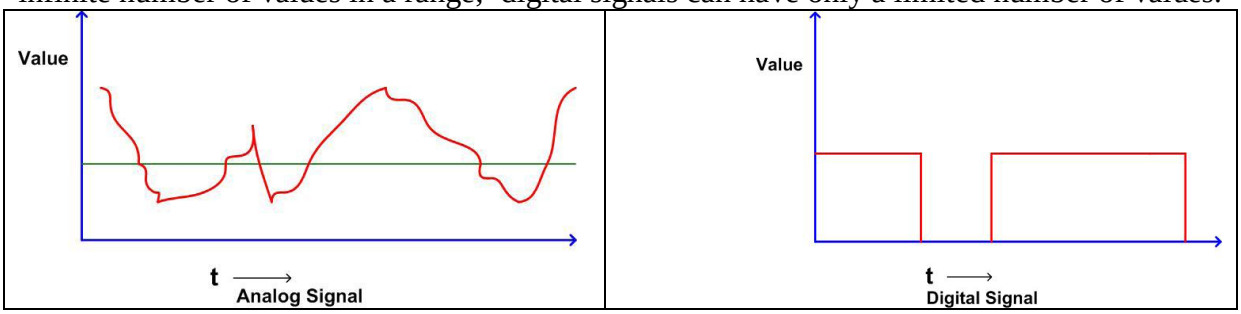
For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal.

Digital data take on discrete values. For example, data are stored in computer memory in the form of 0s and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

## 5.2. Analog and Digital Signals

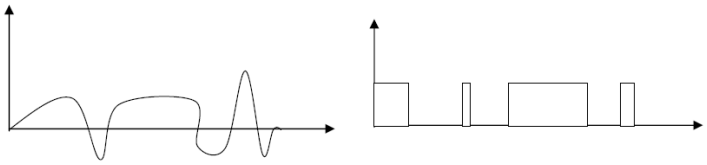
Like the data they represent, signals can be either analog or digital. Analog signals can have an infinite number of values in a range; digital signals can have only a limited number of values.




### 5.3. Periodic and nonperiodic Signals

A periodic 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**.

A nonperiodic (aperiodic) signal changes without exhibiting a pattern or cycle that repeats over time.



a). Analog aperiodic signal b). Digital aperiodic signal

Both analog and digital signals can be periodic or nonperiodic. In data communications, we commonly use periodic analog signals (because they need less bandwidth) and nonperiodic digital signals (because they can represent variation in data).

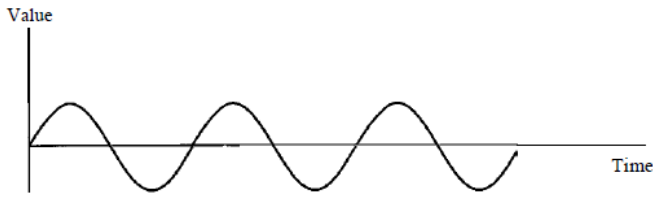
## 5.3.1 Periodic analog signals

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.

### *5.3.1.1. Sine Wave*

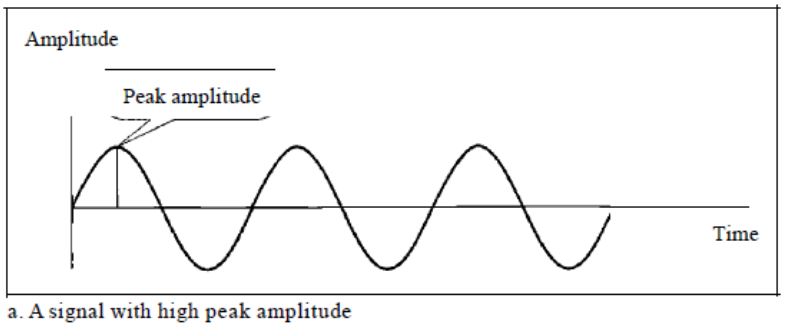
The sine wave is the most fundamental form of a periodic analog signal.
A sine wave can be represented by three parameters: the *peak amplitude*, the *frequency*, and the *phase.*

*A sine wave*

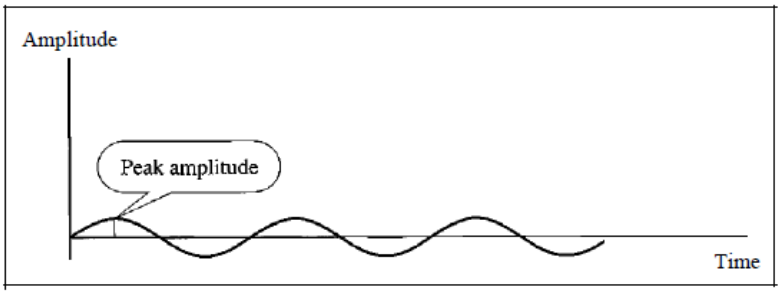



*Peak Amplitude*

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.*



a. A signal with high peak amplitude



b. A signal with low peak amplitude

*Period and Frequency*

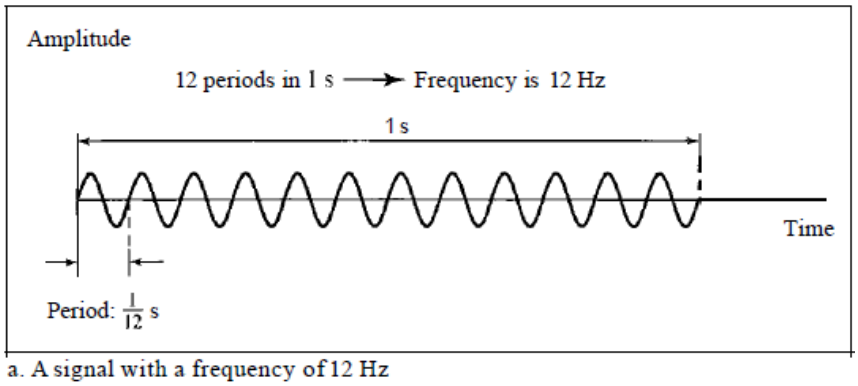
Period refers to the amount of time needs to complete 1 cycle.

Frequency refers to the number of periods in 1 s.

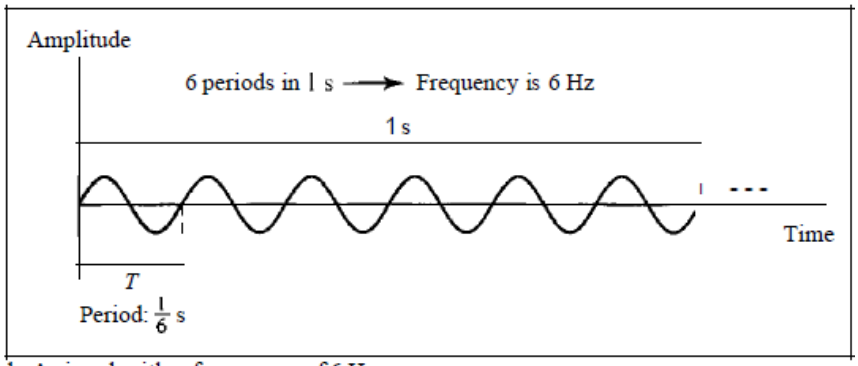
Period is formally expressed in seconds. Frequency is formally expressed in Hertz (Hz), which is cycle per second.

Period is the inverse of frequency, and frequency is the inverse of period.

$$Period = \frac{1}{Frequency}$$



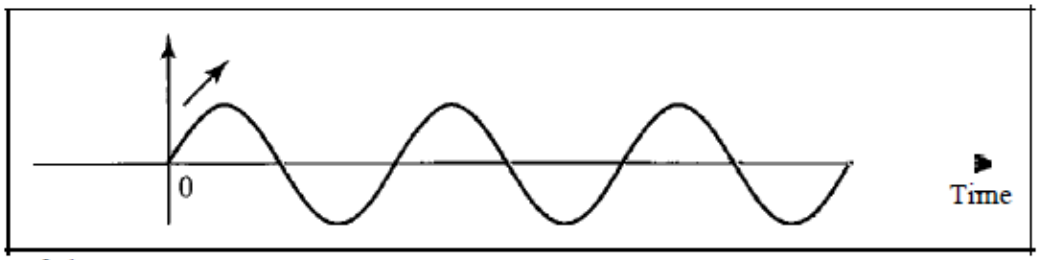

a. A signal with a frequency of 12 Hz



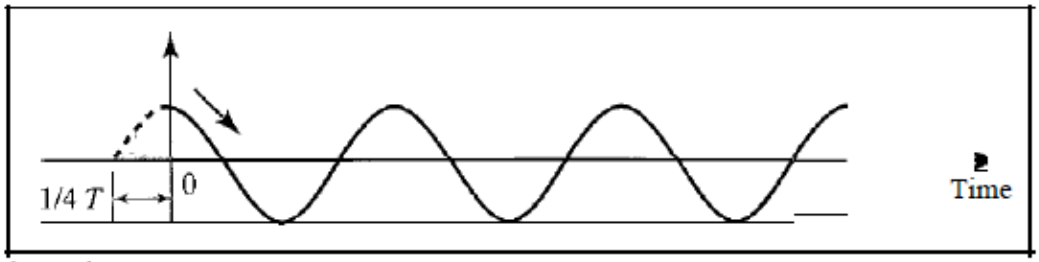

b. A signal with a frequency of 6 Hz

*Phase*: The term phase describes the position of the waveform relative to time 0.
It gives a measure of the relative position in time of two signals within a single period. It is represented by φ in degrees or radian. It indicates the status of the first cycle.

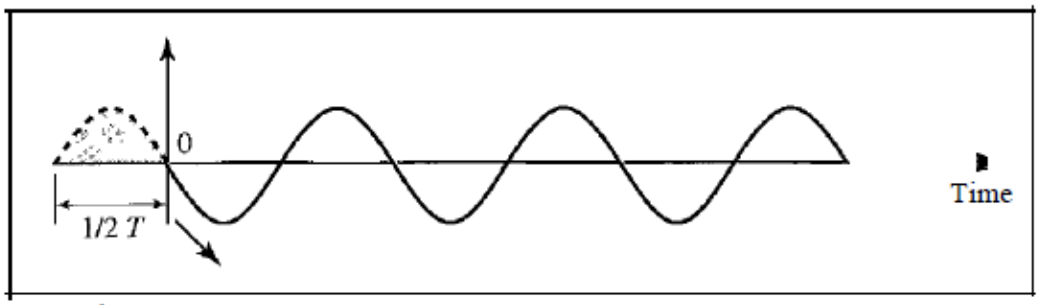
A phase shift of 360° corresponds to a shift of a complete period; a phase shift of 180° corresponds to a shift of one-half of a period; and a phase shift of 90° corresponds to a shift of one-quarter of a period




a. 0 degrees




b. 90 degrees




c. 180 degrees

*Wavelength :*

The wavelength is the distance a simple signal can travel in one period.

Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal.

$$Wavelength = Propagation\ speed \times Period = \frac{Propagation\ speed}{Frequency}$$

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal.

The wavelength is normally measured in micrometers (microns) instead of meters.

For example, the wavelength of red light (frequency =4 x 1014) in air is

$$Wavelength = \frac{Propagation\ speed}{Frequency} = \frac{3\times10^{8}}{4\times10^{14}} = 0.75\times10^{-6}\,m = 0.75\,\mu m$$

In a coaxial or fiber-optic cable, however, the wavelength is shorter (0.5 µm) because the propagation speed in the cable is decreased.

*5.3.2. Periodic composite signal* : A periodic composite signal can be decomposed into a series of simple sine waves with discrete frequencies- frequencies that have integer values (1, 2, 3, and so on).

**Digital signals,**

**5.4. Bit Rate** *The bit rate is the number of bits sent in 1second. It is expressed in bits per second (bps).*

## 5.5 baud rate

Bit rate and Baud rate, these two terms are often used in data communication. Bit rate is simply the number of bits (i.e., 0's and 1's) transmitted per unit time. While Baud rate is the number of signal units transmitted per unit time that is needed to represent those bits.

It is symbol that is transferred on a physical channel. Not bit. Symbol is the physical signals that is transferred over the physical medium to convey the data bits. Symbol is decided by the physical nature of the medium. While bit is a logical concept.
If you want to transfer data bits, you must do it by sending symbols over the medium. Baud rate describes how fast symbols change over a medium.

If we use only 2 symbols to transfer binary data, which means one symbol for 0 and another symbol for 1, that will lead to baud rate = bit rate..
If we can encode more bits into a symbol, we can achieve higher bit rate with the same baud rate. And this is when the baud rate < bit rate. This doesn't mean the transfer speed is slowed down. It actually means the transfer efficiency/speed is increased.

## 5.6 Bandwidth

Network bandwidth is the capacity of a wired or wireless network communications link to transmit the maximum amount of data from one point to another over a computer network or internet connection in a given amount of time -- usually, one second. Synonymous with capacity, bandwidth describes the **data transfer rate** Bandwidth is not a measure of network speed -- a common misconception. The more bandwidth a data connection has, the more data it can send and receive at one time. Bandwidth can be compared to the amount of water that can flow through a water pipe. The bigger the pipe, the more water can flow through it at one time. Bandwidth works on the same principle. So, the higher the capacity of the communication link, or pipe, the more data can flow through it per second. End users pay for the capacity of their network connections. Therefore, the greater the capacity of the link, the more expensive it is.
Bandwidth was originally measured in bits per second and expressed as bps. However, today's networks typically have much higher bandwidth than can be comfortably expressed by using such small units. Now it is common to see higher numbers that are denoted with metric prefixes, such as Mbps, (megabits per second), Gbps (gigabits per second), or Tbps (terabits per second)

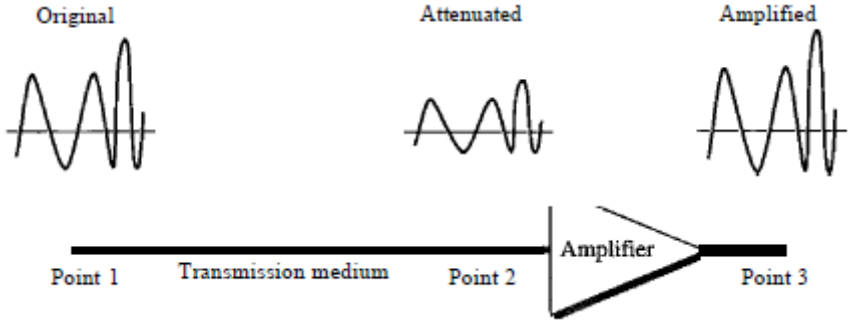
## 6. Transmission impairments-

Signal impairment is caused because the transmission media is not perfect. The signal at the beginning of the medium is not the same as the signal at the end of the medium. That means what is sent is not what is received.

Three causes of impairment are attenuation, distortion, and noise.

### 6.1 Attenuation

Attenuation means a loss of energy. When a signal travels through a medium, it loses some of its energy because of the resistance of the medium. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.




*Decibel*

The decibel (dB) measures the relative strengths of two signals or one signal at two different points. The decibel is negative if a signal is attenuated and positive if a signal is amplified.

$$dB = 10 \log_{10} \frac{P_2}{P_1}$$

Variables *PI* and *P2* are the powers of a signal at points 1 and 2, respectively.

The decibel in terms of voltage (power is proportional to the square of the voltage)

dB =20 $\log_{10}$ *(V2IV1).*

*Example 1.*

Suppose a signal travels through a transmission medium and its power is reduced to one-half.

This means that *P2 = P/2* In this case, the attenuation (loss of power) can be calculated as

10 $\log_{10}$ $P_2/P_1$ = 10 $\log_{10}$ 0.5 = -3 dB

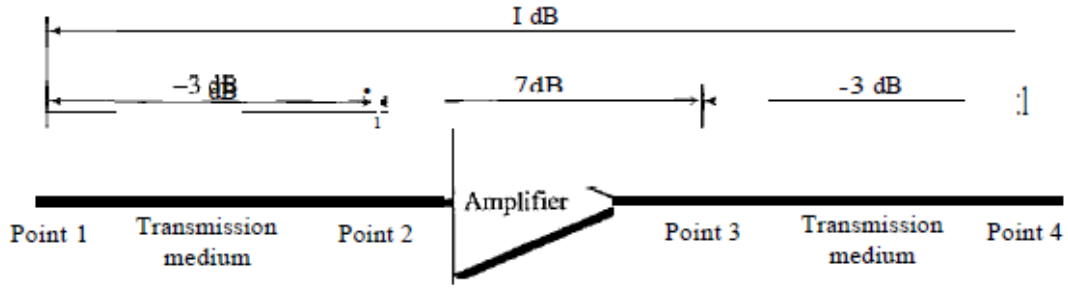
A loss of 3 dB (-3 dB) is equivalent to losing one-half the power.

*Example 2*

A signal travels through an amplifier, and its power is increased 10 times. Calculate the amplification (gain of power)

Example 3

In the following figure a signal travels from point 1 to point 4. The signal is attenuated by the time it reaches point 2. Between points 2 and 3, the signal is amplified. Again, between points 3 and 4, the signal is attenuated. We can find the resultant decibel value for the signal justby adding the decibel measurements between each set of points.



The decibel can be calculated as
dB=-3+7-3=+1
The signal has gained in power.

*Example 4*

Sometimes the decibel is used to measure signal power in milliwatts. In this case, it is referred to as dBm and is calculated as dBm = 10 loglO *Pm'* where *Pm* is the power in milliwatts. Calculate the power of a signal if its dBm =-30.

We can calculate the power in the signal as
dBm = 10 $\log_{10}$ *Pm* = -30

$\log_{lO}$ *Pm*:= -3 *Pm* =$10^{-3}$ mW

*Example 4*

The loss in a cable is usually defined in decibels per kilometer (dB/km).
Let loss in a cable is -0.3 dBlkm. If the signal at the beginning of the cable has a power of 2 mW, what is the power of the signal at 5 km?

The loss in the cable in decibels is 5 x (-0.3)= -1.5 dB. We can calculate the power as

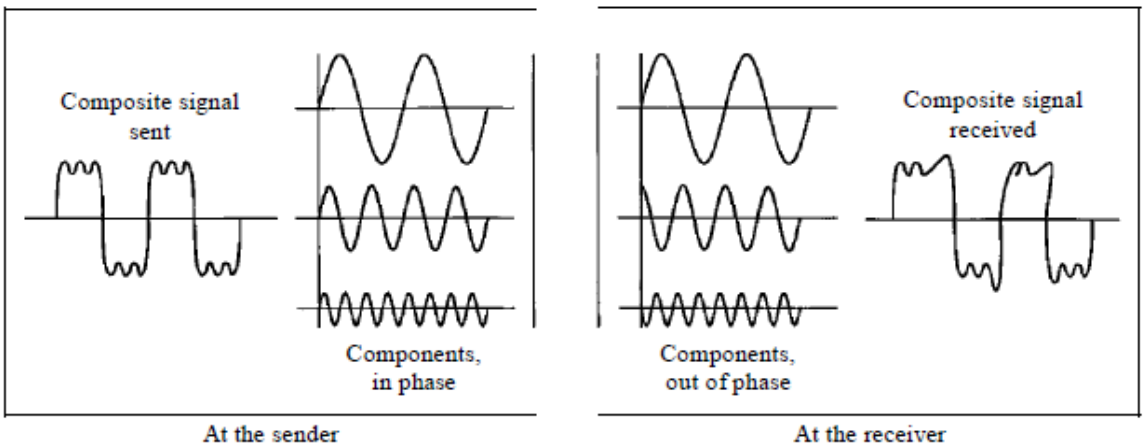
$$\text{dB} = 10 \log_{10} \frac{P_2}{P_1} = -1.5$$

$$\frac{P_2}{P_1} = 10^{-0.15} = 0.71$$

$$P_2 = 0.71 P_1 = 0.7 \times 2 = 1.4 \text{ mW}$$

## 6.2 Distortion

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration. In other words, signal components at the receiver have phases different from what they had at the sender.




## 6.3 Noise.

Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

- Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.
- Induced noise comes from sources such as motors and appliances.

- These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

- Crosstalk is the effect of one wire on the other.
  - One wire acts as a sending antenna and the other as the receiving antenna.
- Impulse noise is a spike (a signal with high energy in a very short time)
  - it comes from power lines, lightning, and so on

.

*Signal-to-Noise Ratio (SNR)* is defined as

$$SNR = \frac{\text{average signal power}}{\text{average noise power}}$$

(We need to consider the average signal power and the average noise power because these may change with time.)

SNR is actually the ratio of what is wanted (signal) to what is not wanted (noise).

- A high SNR means the signal is less corrupted by noise;
- a low SNR means the signal is more corrupted by noise.

SNR is the ratio of two powers, it is often described in decibel units, $SNR_{dB}$, defined as

$SNR_{dB} = 10\log_{10} SNR$

*Example*

The power of a signal is 10 μW and the power of the noise is 1 μW; what are the values of SNR and $SNR_{dB}$?

$$SNR = \frac{10{,}000\mu W}{1\mu W} = 10000$$

SNR = 10.000 μW = 10 000

$SNR_{dB} = 10 \log_{10} 10{,}000 = 10 \log_{10} 10^4 = 40$

*Example 3.32*

The values of SNR and $SNR_{dB}$ for a noiseless channel are

$$SNR = \frac{Signal power}{0} = \infty$$

$SNR_{dB} = 10 \log_{10} \infty = \infty$

We can never achieve this ratio in real life; it is an ideal.

## Data Flow

Communication between two devices can be **simplex, half-duplex, or full-duplex**.

**Simplex** In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive . Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

**Half-Duplex** In half-duplex mode, each station can both transmit and receive, but not at the same time. : When one device is sending, the other can only receive, and vice versa.The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies is an example for half-duplex systems. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

**Full-Duplex** In full-duplex (also called duplex), both stations can transmit and receive . In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions. One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

## 7. Data communication protocols and standards

An entity is anything capable of sending or receiving information. For communication to occur between entities in a network, the entities must agree on a protocol.
Protocols:

- A protocol is a set of rules that govern data communications.
- A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are syntax, semantics, and timing.
    - Syntax. The term syntax refers to the structure or format of the data. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
    - Semantics. The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
    - Timing. The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.
    - Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers.
        - 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: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").
        - De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use.
        - De jure. Those standards that have been legislated by an officially recognized body.

**Internet Standards**

An Internet standard is a thoroughly tested specification that is useful to those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a 6-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a Request for

Comment (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level, cooperation in the realms of scientific, technological, and economic activity.

## 8. Network models –

To reduce the design complexity, most of the networks are organized as a series of layers or levels, each one build upon one below it.

- The benefits of the layered models are modularity and clear interfaces, i.e. open architecture and comparability between the different providers' components.
- A basic principle is to ensure independence of layers by defining services provided by each layer to the next higher layer without defining how the services are to be performed. This permits changes in a layer without affecting other layers.
- The number of layers, functions and contents of each layer differ from network to network.
- The purpose of each layer is to offer certain services to higher layers, hiding the details of how the services are actually implemented.
- The basic elements of a layered model are services, protocols and interfaces.
    - A service is a set of actions that a layer offers to another (higher) layer.
    - Protocol is a set of rules that a layer uses to exchange information with a peer entity. These rules concern both the contents and the order of the messages used. In an n-layer architecture, layer n on one machine carries on conversation with the layer n on other machine. The rules and conventions used in this conversation are collectively known as the layer-n protocol.
    - Between each pair of adjacent layers there is an interface. The messages from one layer to another are sent through those interfaces. The interface defines which primitives operations and services the lower layer offers to the upper layer adjacent to it. (A clean-cut interface minimizes the amount of information passed between layers, makes it simpler to replace the implementation of one layer with a completely different implementation.)

Why Layered architecture?

1. To make the design process easy by breaking unmanageable tasks into several smaller and manageable tasks (by divide-and-conquer approach).

2. Modularity and clear interfaces, so as to provide comparability between the different providers' components.

3. Ensure independence of layers, so that implementation of each layer can be changed or modified without affecting other layers.

4. Each layer can be analyzed and tested independently of all other layers.

A set of layers and protocols is known as network architecture. The specification of architecture must contain enough information to allow an implementation to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. Neither the details of implementation nor the specification of interface is a part of network architecture.
A list of protocols used by a certain system, one protocol per layer, is called protocol stack

## 8.1 OSI model

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

## The OSI Reference Model includes seven layers:

## Layered Architecture

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). Each layer defines a family of functions distinct from those of the other layers. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

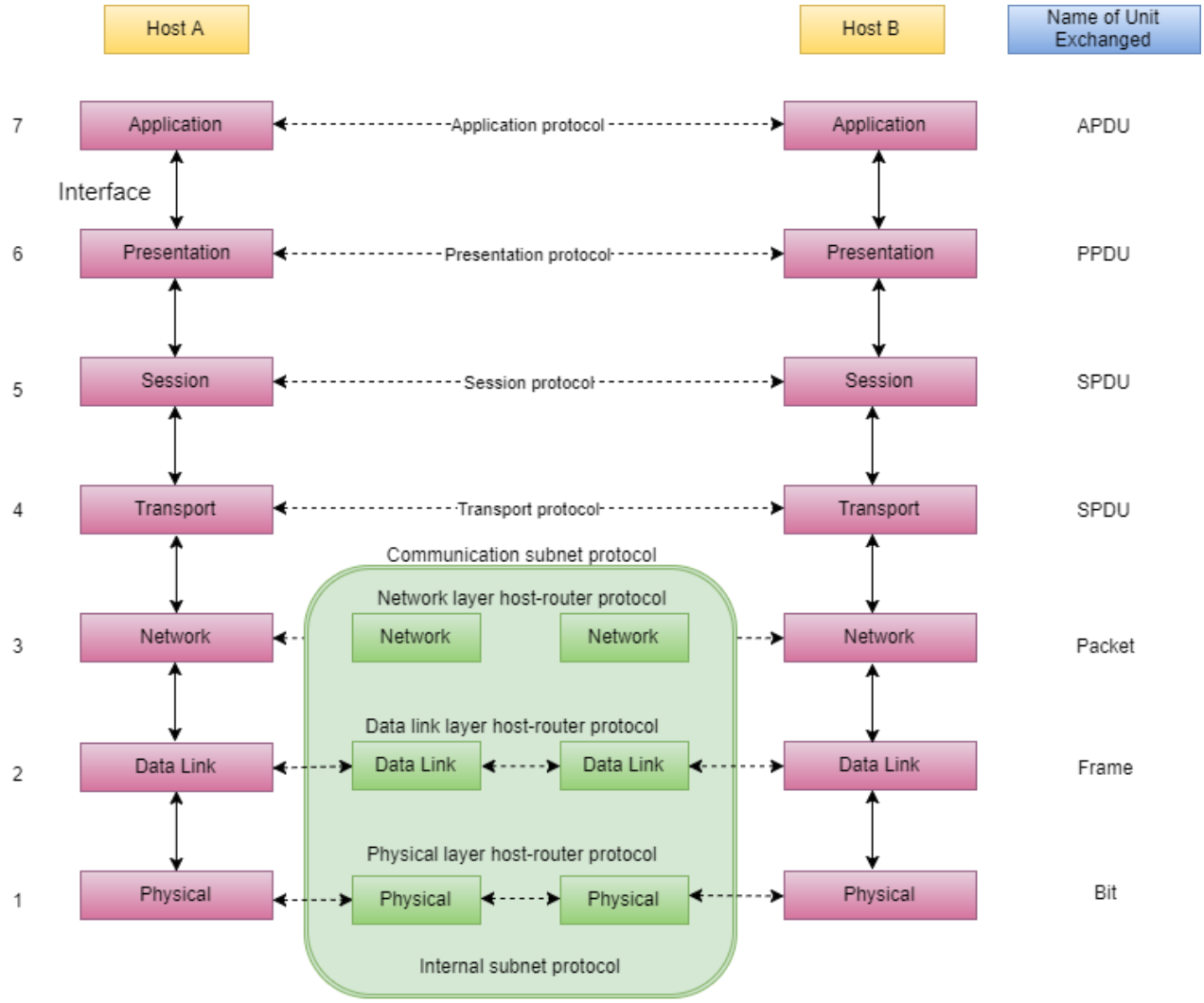
**Peer-to-peer processes** - The processes on each machine that communicate at a given layer are called peer-to-peer processes**.** Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

**Interfaces Between Layers** The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network.

### Organization of the Layers

The seven layers can be thought of as belonging to three subgroups. Layers I, 2, and 3-physical, data link, and network-are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.




At each layer, a header, or possibly a trailer, can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link. Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

## Encapsulation

Figure  reveals another aspect of data communications in the OSI model: encapsulation. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N - 1, the whole packet coming from level N is treated as one integral unit.

## Functions of each layer in the OSI model

7. Application Layer: The application layer enables the user, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
Specific services provided by the application layer include the following:

- Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services. This application provides the basis for e-mail forwarding and storage.
- Directory services. This application provides distributed database sources and access for global information about various objects and services.

6. Presentation Layer: The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

- Translation.
    - (The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.) The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- Encryption.
    - To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

5. Session Layer: The session layer is the network *dialog controller.*
It establishes, maintains, and synchronizes the interaction among communicating systems.
Provides name recognition and additional functions like security, which are needed to allow applications to communicate over the network.

- Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either halfduplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.
    - For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

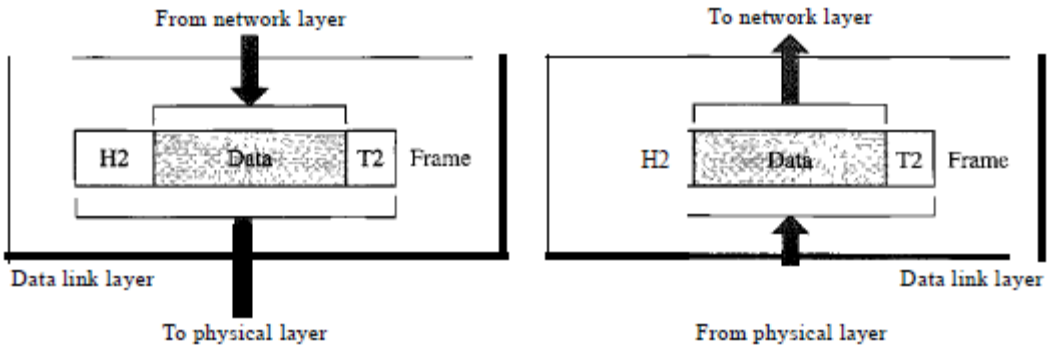
4. Transport Layer:
The transport layer is responsible for process-to-process delivery of the entire message.(A process is an application program running on a host.)

- Service-point addressing.
    - Process-to-process delivery means delivery from a specific process on one computer to a specific process on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address).
- Segmentation and reassembly. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- Connection control. The transport layer can be either connectionless or connection-oriented.
    - A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine, before delivering the packets. After all the data are transferred, the connection is terminated.
- Flow control.
    - flow control at this layer is performed end to end rather than across a single link.
- Error control.
    - error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission

3. Network Layer:

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). (If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.)
- Logical addressing.
    - (The physical addressing implemented by the data link layer handles the addressing problem locally.) If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.
- Routing.
    - responsible for finding a path through the network to the destination computer.

2. Data-Link Layer: This layer takes the data frames or messages from the Network Layer and provides error-free delivery of data between the two computers by using the physical layer. At the receiving computer, this layer receives the incoming data and sends it to the network layer for handling.




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

1. Physical Layer:

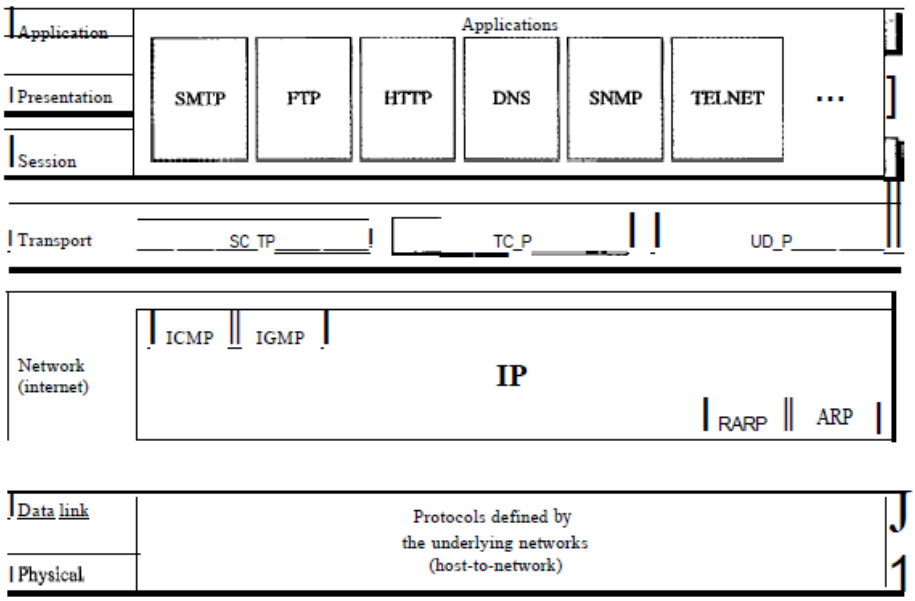
- Controls the transmission of the actual data over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- Defines the characteristics of the interface between the devices and the transmission medium.
- defines the type of transmission medium.
- Representation of bits.
    - The physical layer data consists of a stream of bits with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s are changed to signals).
- Data rate.
    - The transmission rate-the number of bits sent each second
    - defines the duration of a bit - how long it lasts.
- Synchronization of bits.
- Line configuration.
    - The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- Physical topology. The physical topology defines how devices are connected to make a network.

- Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

- Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.
  - In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

## 8.2 TCP/IP protocol suite.

TCPIIP protocol suite is made of five layers: physical,data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model are represented in TCPIIP by a single layer called the application layer




- TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- The layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.
- At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

**Physical and Data Link Layers**

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

- A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

**Network Layer**

- At the network layer (or the internetwork layer), TCP/IP supports the Internetworking Protocol.
- IP uses four supporting protocols: ARP,RARP, ICMP, and IGMP.

Internetworking Protocol (IP)

- The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- It is an unreliable and connectionless protocol-a best-effort delivery service.
    - The term best effort means that IP provides no error checking or tracking.
- IP transports data in packets called datagrams, each of which is transported separately.
    - Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Address Resolution Protocol

- The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.
    - (On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known. )

- Reverse Address Resolution Protocol
    - The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.
- Internet Control Message Protocol (ICMP)
    - The ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
    - ICMP sends query and error reporting messages.
- Internet Group Message Protocol
    - The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

**Transport Layer**

- Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP.
- IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.
- UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.
- User Datagram Protocol
    - It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
- Transmission Control Protocol

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

- Stream Control Transmission Protocol (SCTP)
  - TheSCTP provides support for newer applications such as voice over the Internet.
  - It is a transport layer protocol that combines the best features of UDP and TCP.

**Application Layer**

- The application layer in TCPIIP is equivalent to the combined session, presentation,and application layers in the OSI modeL
- Many protocols are defined at this layer.