BCA - SEMESTER V
CA5CRT14 : Computer Networks (Core)

Theory:3 hrs. per week
Credits:4

Unit 1: (10 hrs.)
Introduction to Networks, Data and signals-analog and digital, periodic analog signals, digital signals, bitrate, 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.

Unit 2: (10 hrs.)
Bandwidth utilization Multiplexing: 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: (12 hrs.)
Data link layer: Error Detection and Correction, Framing, flow and error control, Protocols – Noiseless channels (Simplest, Stop and Wait) and Noisy channels (Stop and Wait and Piggy Backing).
Multiple Access Protocols. Random Access-ALOHA, CSMA.
Wired LANs-IEEE standards, wireless LANs-Bluetooth, Cellular Telephony

Unit 4: (12 hrs.)
Network layer and Transport layer: Repeaters, Bridges, Gateways and routers.
Logical addressing – IPV4 and IPV6 addressing, Internet protocol - IPV4 and IPV6.
Connectionless and Connection Oriented Services: UDP and TCP. Congestion Control, Quality of Service.

Unit 5: (10 hrs.)
Application layer: HTTP, FTP, SMTP, DNS. Network security: Common Threats- Firewalls (advantages and disadvantages), Cryptography.

Book of study:

1. B. A. Forouzan - Data communication and Networking, Fourth edition-,TMH

2. Andrew S Tanenbaum - Computer Networks ,Fourth Edition, Prentice Hall of India.

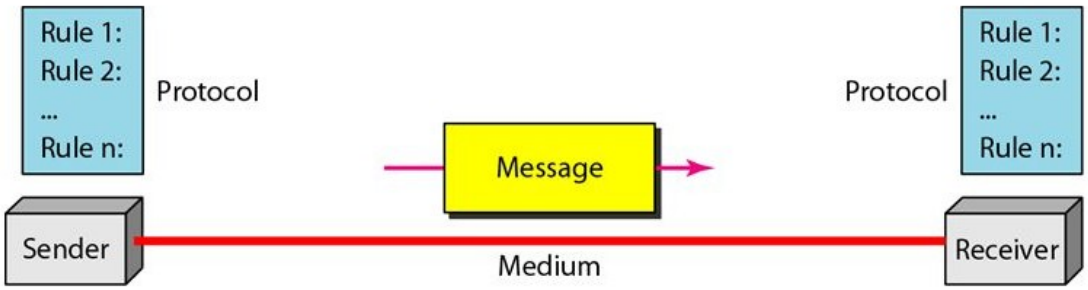
UNIT -1:
Introduction to networks. Data and signals-analog and digital, periodic analog signals, digital signals, bit rate, baud rate, bandwidth. Transmission impairments- attenuation distortion and noise.
Data communication protocols and standards, Network models - OSI model-layers and their functions. TCP/IP protocol suite.

DATA COMMUNICATION

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.
1. **Delivery**. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy**. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Components

A data communications system has five components (see Figure 1.1).

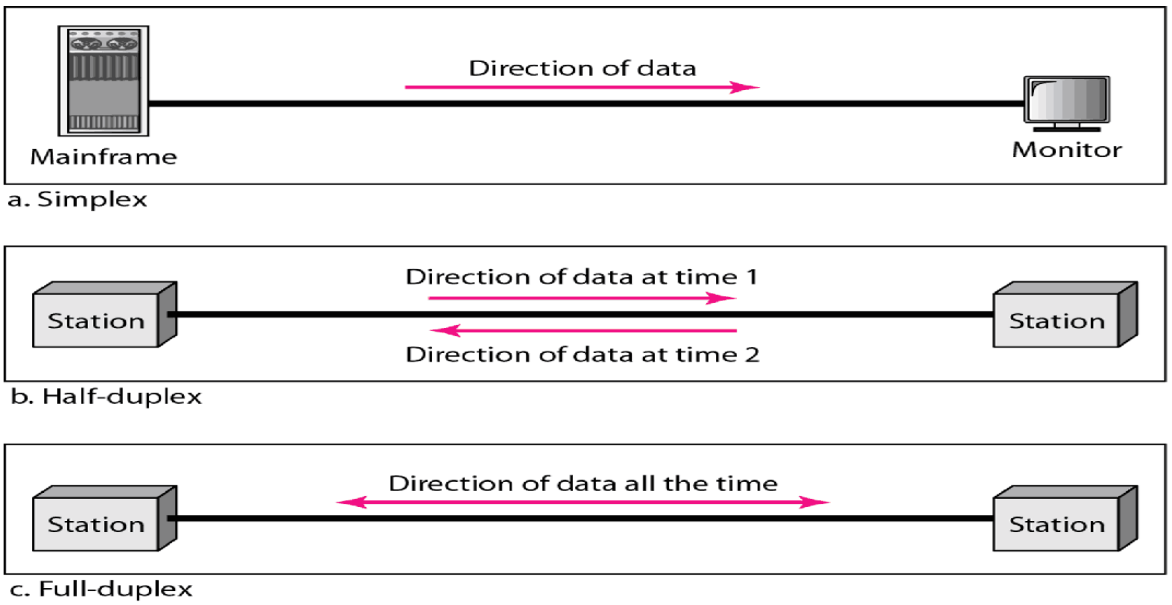


1. **Message.** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender.** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** 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.

5. **Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2



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 (see Figure 1.2a). 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 (see Figure 1.2b).
Walkie-talkies and CB (citizens band) radios are both 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 mode (also called duplex), both stations can transmit and receive simultaneously (see Figure 1.2c).
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 travelling 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.

Network

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.

Physical Structures

Network Attributes

Type of Connection

A network is two or more devices connected through links. A **link** is a communications pathway that transfers data from one device to another.

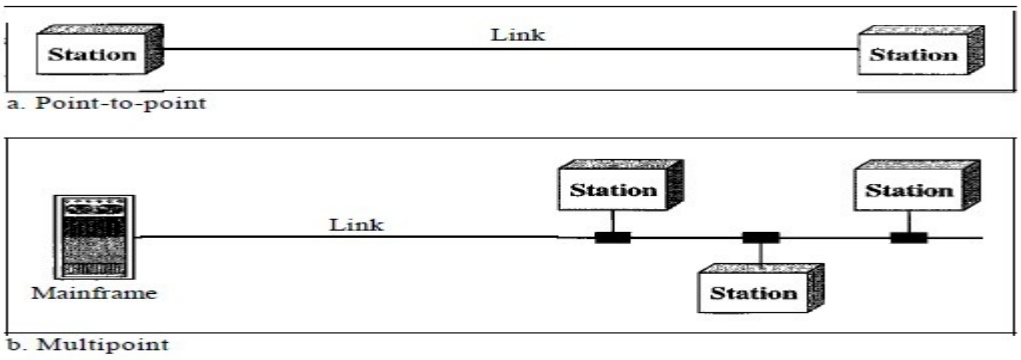
There are two possible types of connections:

- Point-To-Point
- Multipoint.

Point-to-Point :
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint :
A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b). In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

Types of connections: point-to-point and multipoint



.

Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically.:
Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
There are four basic topologies possible:

- Mesh
- Star
- Bus
- Ring (see Figure 1.4)

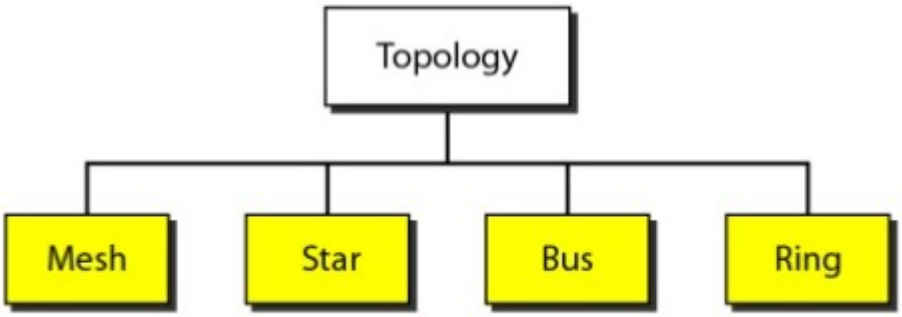


Figure 1.4-Categories Of topology

Mesh

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - I nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to *n* - 1 nodes. We need *n(n* - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.

In a mesh topology, we need *n(n* -1) /2 duplex-mode links.

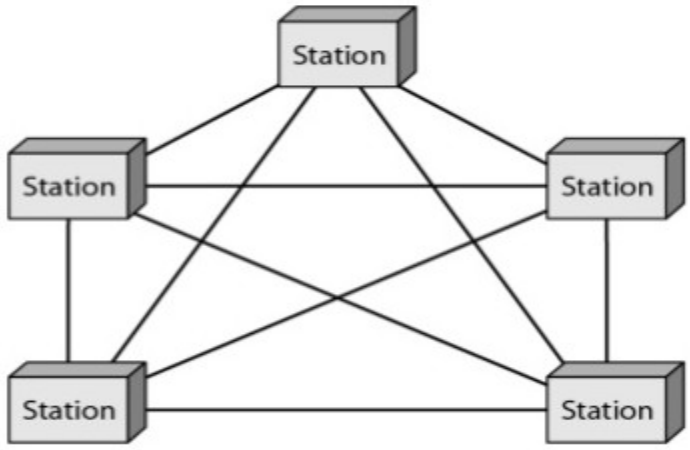


Figure 1.5 ***A fully connected mesh topology (five devices)***

Advantages over other network topologies

1. The use of dedicated links guarantees that each connection can carry its own data load, thus **eliminating the traffic problems** that can occur when links must be shared by multiple devices.
2. A mesh topology is **robust**. If one link becomes unusable, it does not incapacitate the entire system.
3. There is the advantage of **privacy or security**. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-point links make **fault identification and fault isolation easy**. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Main disadvantages
1. Since every device must be connected to every other device, installation and reconnection are difficult.
2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called **a hub.** The devices are not directly linked to one another. A star topology does not allow direct traffic between devices. The **controller** acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.6)

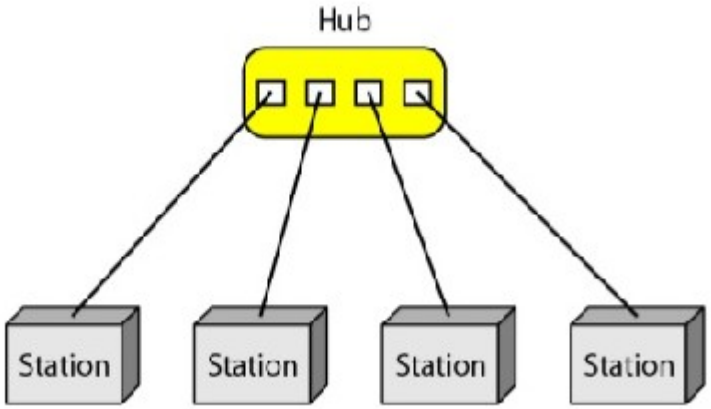
Advantages

- A star topology is **less expensive** than a mesh topology.
- In a star, each device needs only **one link and one I/O por**t to connect it to any number of others. This factor makes it **easy to install and reconfigure.**
- **Far less cabling** needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Other advantages include **robustness.** If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).
- The star topology is used in local-area networks (LANs) .High-speed LANs often use a star topology with a central hub.

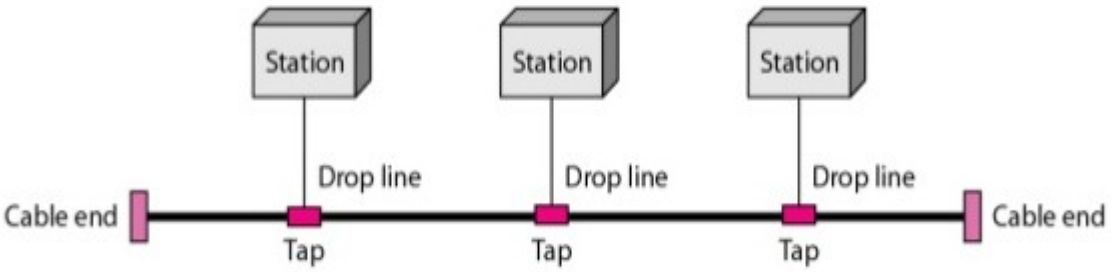
Figure 1.6 *A star topology connecting four stations*



Bus Topology

A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network (see Figure 1.7).
Nodes are connected to the bus cable by **drop lines and taps**. A **drop line** is a connection running between the device and the main cable. A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Figure 1.7 *A bus topology connecting three stations*



Advantages

- Ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

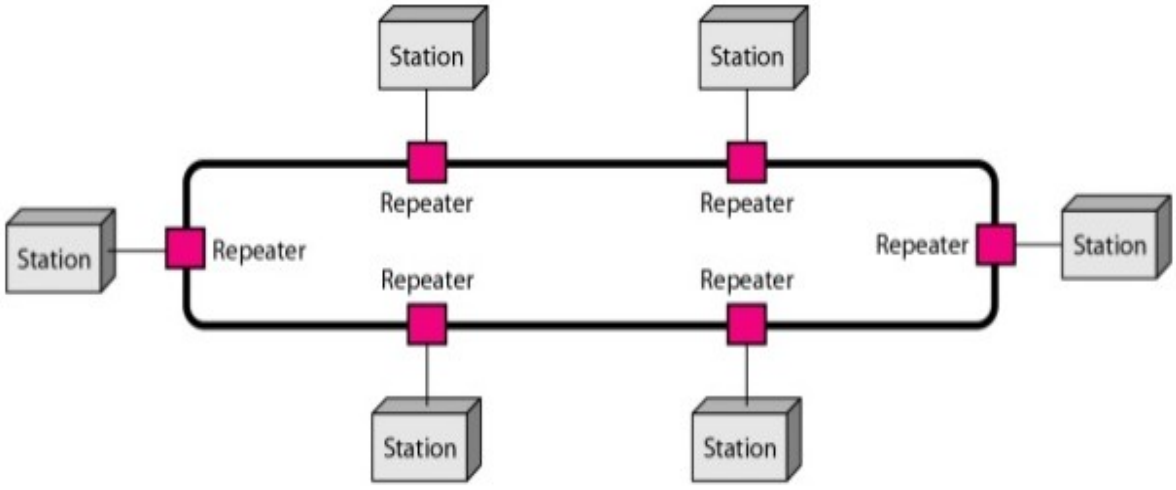
Disadvantages

- Disadvantages include **difficult reconnection and fault isolation.** A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.
- Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Figure 1.8 *A ring topology connecting six stations*



Advantages

- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbours (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified.
- Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

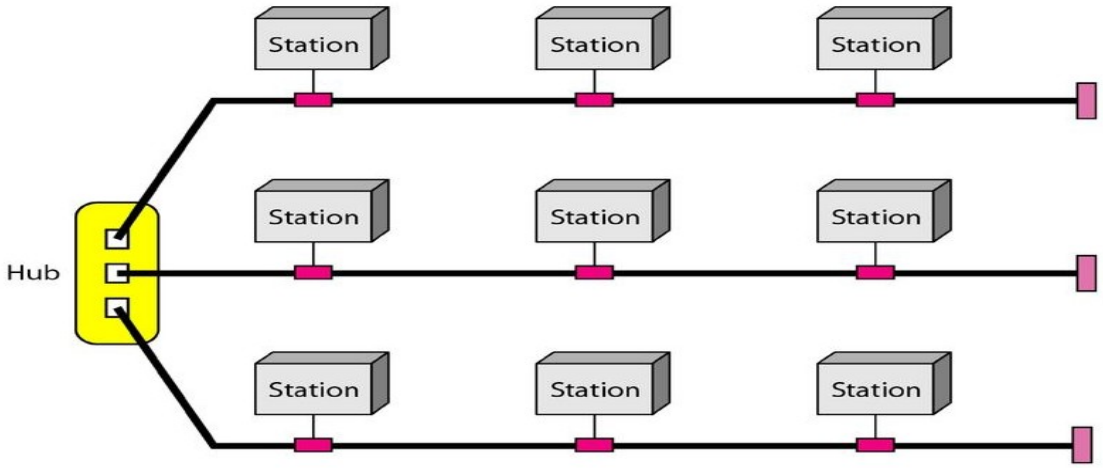
Disadvantage

- However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

Figure 1.9 A *hybrid topology: a star backbone with three bus networks*



Categories of Networks

Two primary categories:

- Local-area networks
- Wide-area networks.

The category into which a network falls is determined by its **size**. A LAN normally covers an area less than 2 mi; a WAN can be worldwide. Networks of a size in between are normally referred to as **metropolitan area networks** and span tens of miles.

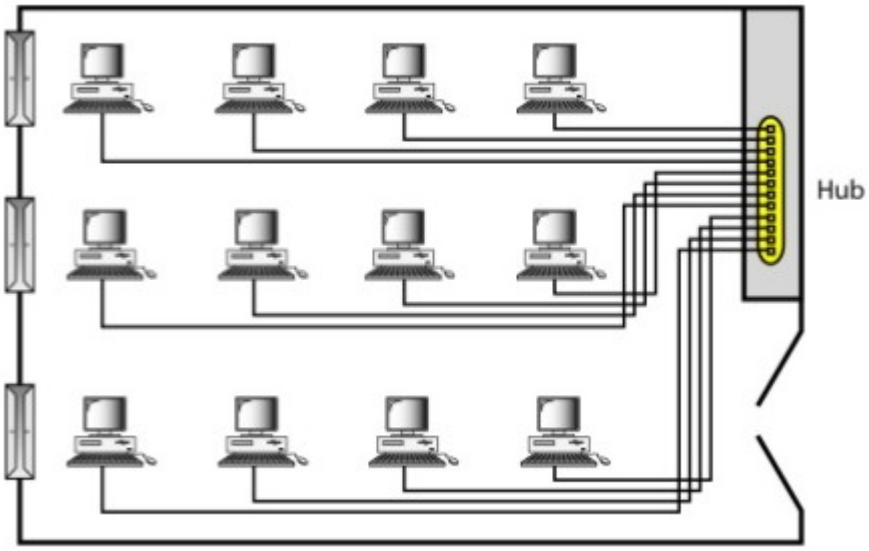
Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.10). Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometres.

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.

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.

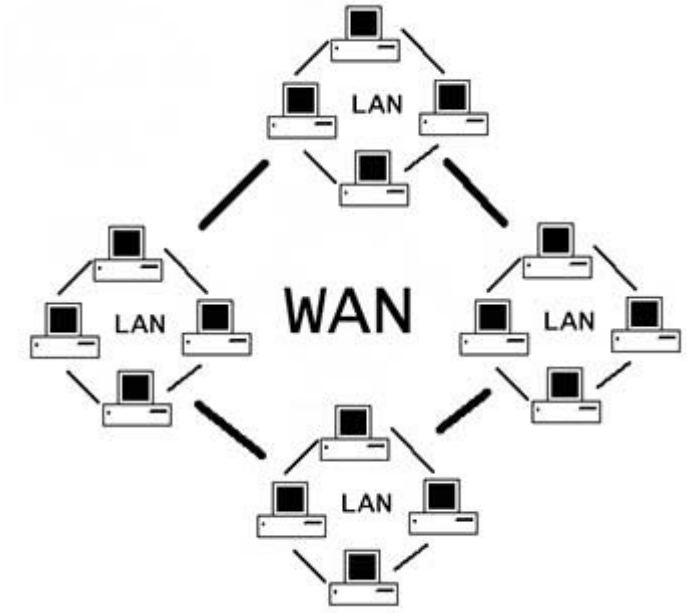
Figure 1.10 *An isolated IAN connecting* 12 *computers to a hub*



Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.



Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. 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.
A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

UNIT -1:

Introduction to networks. 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.

DATA

A data element is the smallest entity that can represent a piece of information (a bit). To be transmitted, data must be transformed to **electromagnetic signals.**

Data elements are what we need to send; signal elements are what we can send.

Data elements are being carried; signal elements are the carriers.

ANALOG AND DIGITAL

Both data and the signals that represent them can be either **analog or digital** in form.

Analog and Digital Data

Data can be **analog** or **digital.**

The term **analog data** refers to information that is continuous. For eg:an analog clock that has hour, minute, and second hands gives information in a continuous form.

Digital data refers to information that has discrete states. For eg: 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 a digital signal.

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

Analog and Digital Signals

An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value *A* to value *B,* it passes through and includes an infinite number of values along its path. A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0.

Analog and digital signals can be plotted on a pair of perpendicular axes. The **vertical axis** represents the **value or strength** of a signal. The **horizontal axis** represents **time**. Figure 3.1 illustrates an analog signal and a digital signal. The curve representing the analog signal passes through an infinite number of points. The vertical lines of the digital signal demonstrate the sudden jump that the signal makes from value to value.

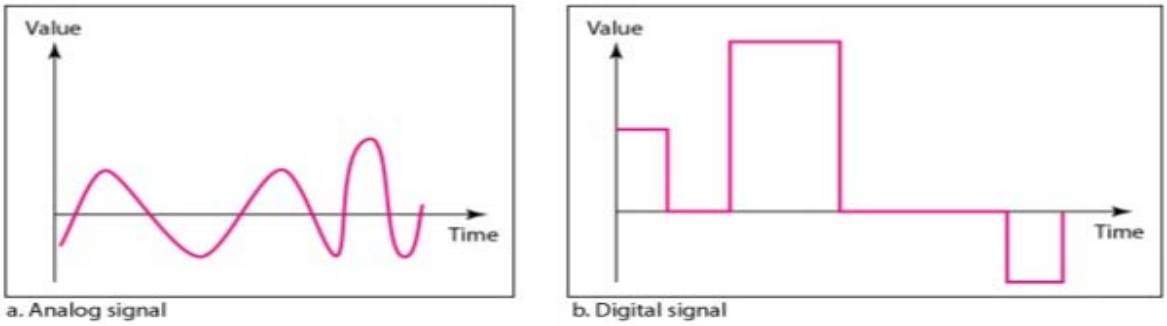


Fig 3.1 Comparison of analog and digital signals

Periodic and Non-periodic Signals

Both analog and digital signals can take one of two forms:

- ***periodic***
- ***non-periodic(aperiodic)***

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 **non-periodic signal** changes without exhibiting a pattern or cycle that repeats over time.
In data communications, we use periodic analog signals (because they need less bandwidth) and non-periodic digital signals (because they can represent variation in data).

PERIODIC ANALOG SIGNALS

Periodic analog signals can be classified as

1. **simple**
2. **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.

Sine Wave
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. Figure 3.2 shows a sine wave. Each cycle consists of a single arc above the time axis followed by a single arc below it.

A sine wave can be represented by three parameters:

- The *Peak Amplitude,*
- The *Frequency,*
- The *Phase.*

Figure 3.2 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.*

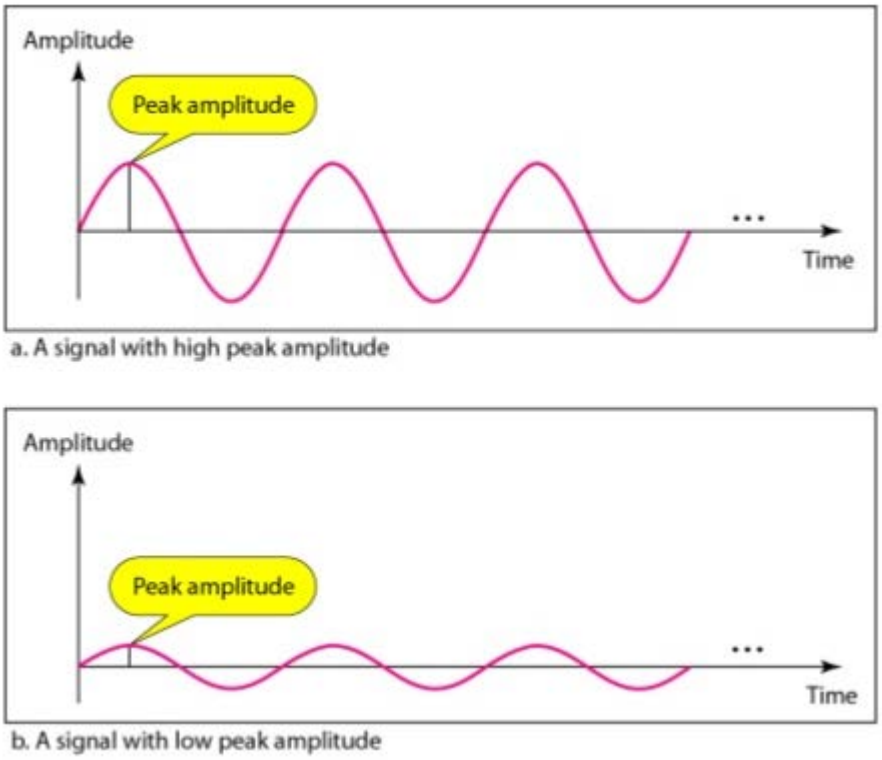


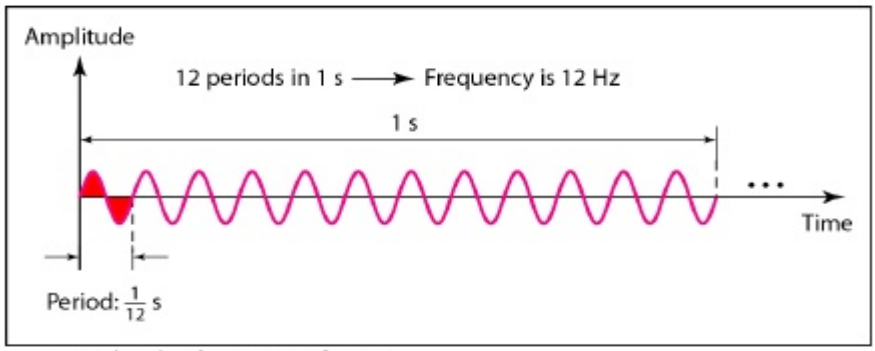
Figure 3.3 *Two signals with the same phase and frequency, but different amplitudes*

The peak value is equal to 2^{112} x rms value
.rms=root mean square

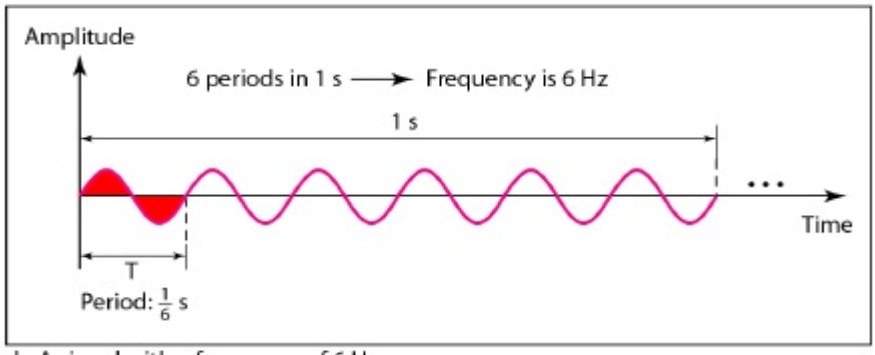
Period and Frequency

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.
Frequency refers to the number of periods in 1s. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

$$f=1/T \quad and \quad T=1/f$$



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

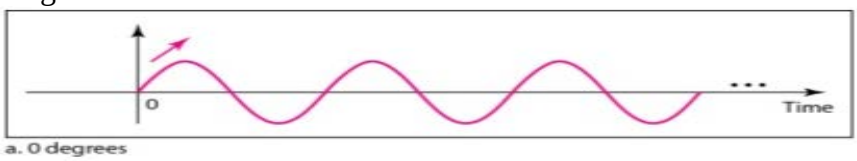
Figure 3.4 *Two signals with the same amplitude and phase, but different frequencies*

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

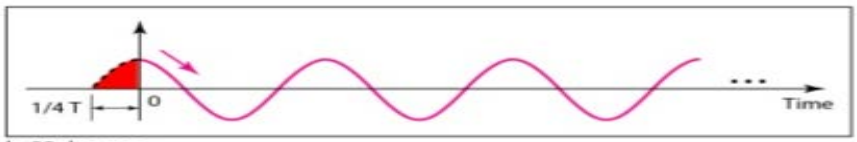
If a signal does not change at all, its frequency is zero. If a signal changes instantaneously, its frequency is infinite.

Phase

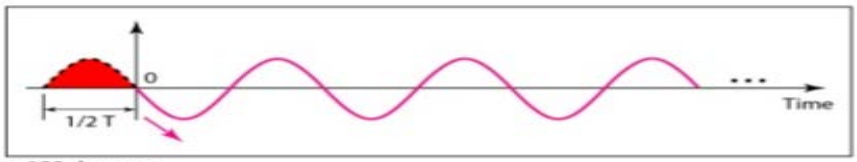
The term phase describes the position of the waveform relative to time 0. Phase is measured in degrees or radians.



a. 0 degrees



b. 90 degrees



c. 180 degrees

Wavelength

Wavelength binds the period or the frequency of a simple sine wave to the propagation speed of the medium.

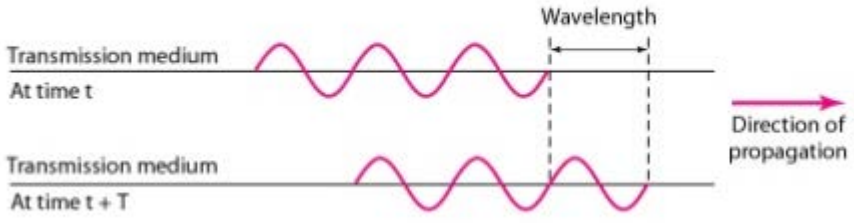


Figure 3.6 Wavelength and period

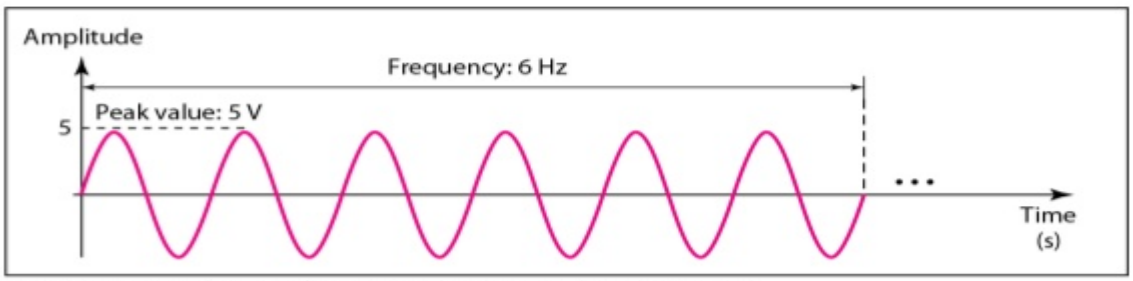
The frequency of a signal is independent of the medium, but the wavelength depends on both the frequency and the medium. Wavelength is a property of any type of signal.
The wavelength is the distance a simple signal can travel in one period.
Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. However, since period and frequency are related to each other, if we represent wavelength by A, propagation speed by c (speed of light), and frequency by*1*, we get

Wavelength =Propogation speed x Period= Propogation speed/frequency

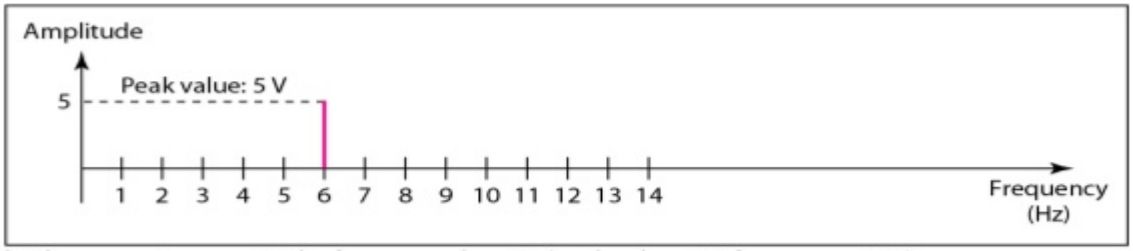
The wavelength is normally measured in micrometers (microns).

Time and Frequency Domains

The time-domain plot shows changes in signal amplitude with respect to time (it is an amplitude-versus-time plot).
A frequency-domain plot is concerned with only the peak value and the frequency.

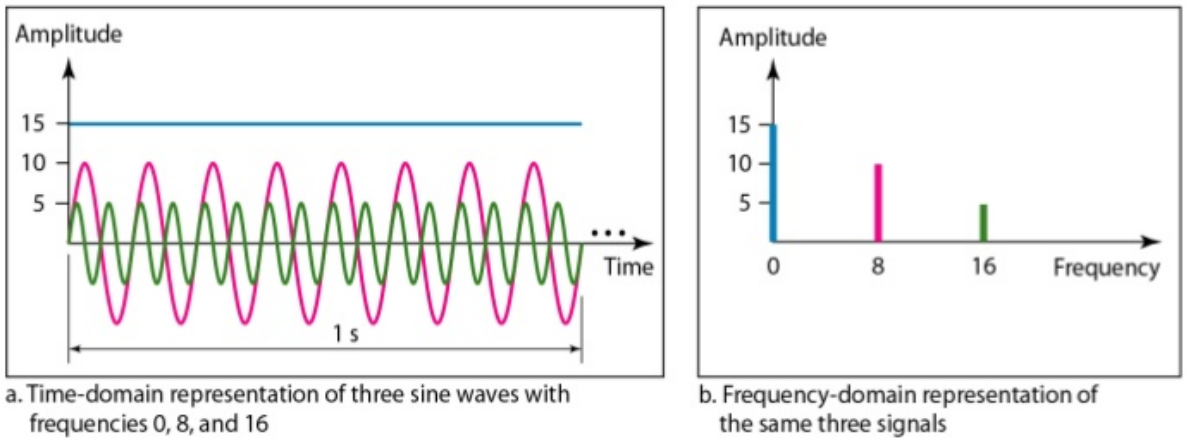


a. A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)



b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

Figure 3.7 The time-domain and frequency-domain plots of a sine wave



a. Time-domain representation of three sine waves with frequencies 0, 8, and 16

b. Frequency-domain representation of the same three signals

Figure 3.8 *The time domain and frequency domain of three sine waves*

Composite Signals

A composite signal is made of many simple sine waves. Any composite signal is 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 that have integer values (1, 2, 3, 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.

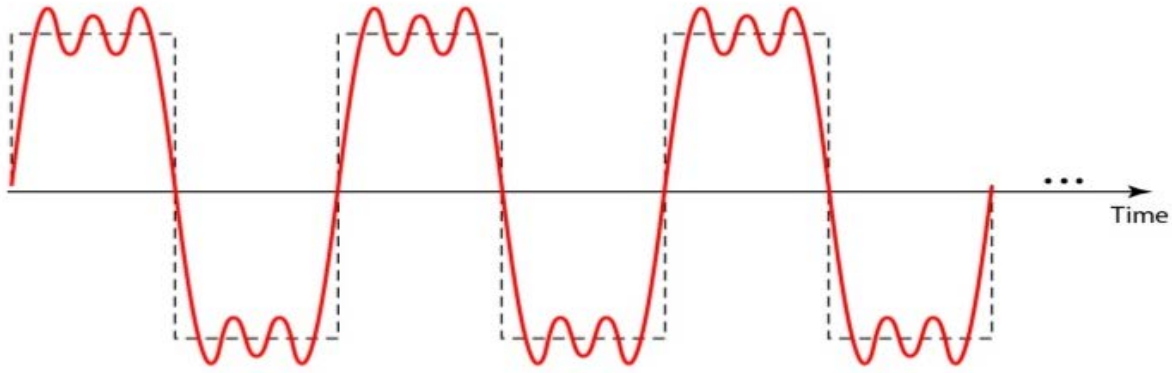


Figure 3.9 *A composite periodic signal*

It is very difficult to manually decompose this signal into a series of simple sine waves. However, there are tools, both hardware and software, that can help us do the job. Figure 3.10 shows the result of decomposing the above signal in both the time and frequency domains.

The amplitude of the sine wave with frequency *f* is almost the same as the peak amplitude of the composite signal. The amplitude of the sine wave with frequency *3f*is one-third of that of the first, and the amplitude of the sine wave with frequency *9f* is one-ninth of the first. The frequency of the sine wave with frequency *f* is the same as the frequency of the composite signal; it is called the fundamental frequency, or first harmonic. The sine wave with frequency 3fhas a frequency of 3 times the fundamental frequency; it is called the third

harmonic. The third sine wave with frequency *9f has* a frequency of 9 times the fundamental frequency; it is called the ninth harmonic.

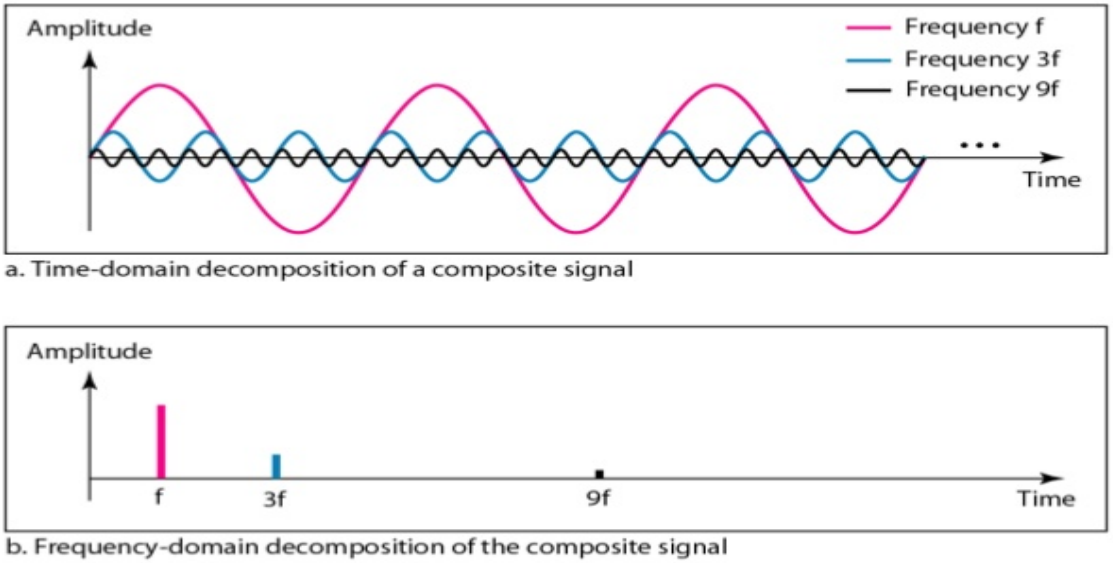


Figure 3.10 Decomposition of a composite periodic signal in the time and frequency domains

Bandwidth

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

The range of frequencies contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers. For example, if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 - 1000, or 4000.

Figure 3.12 shows the concept of bandwidth. The figure depicts two composite signals, one periodic and the other non periodic. The bandwidth of the periodic signal contains all integer frequencies between 1000 and 5000 (1000, 100I, 1002, ...). The bandwidth of the non-periodic signals has the same range, but the frequencies are continuous.

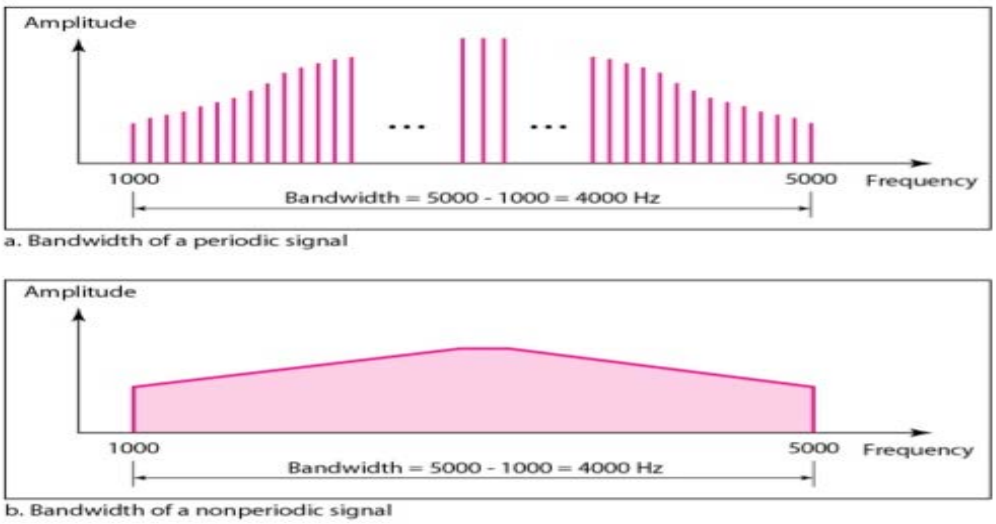


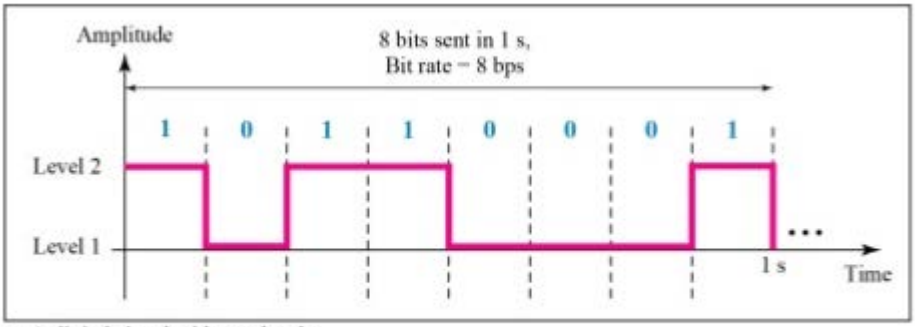
Figure 3.12 *The bandwidth of periodic and non periodic composite signals*

Let *f*h be the highest frequency *f*z the lowest frequency, and *B* the bandwidth then

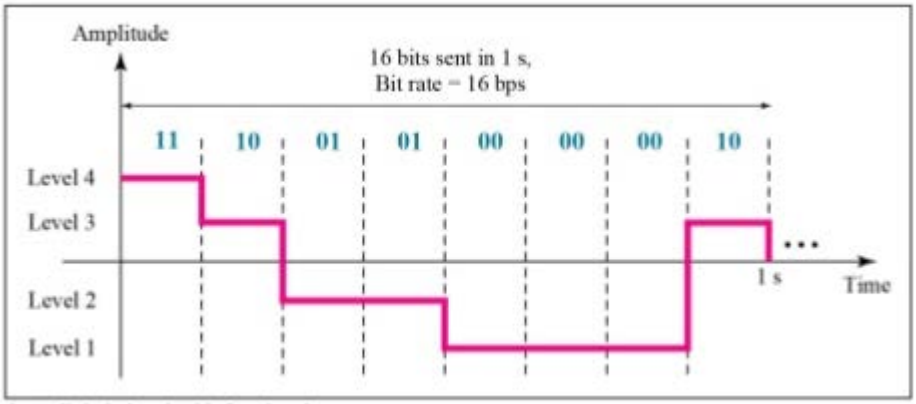
$$B = fh - fz$$

DIGITAL SIGNALS

A digital signal can have more than two levels. Generally 1 is for positive and 0 for negative.



a. A digital signal with two levels



b. A digital signal with four levels

Figure 3.16 *Two digital signals: one with two signal levels and the other with four signal levels*

We send 1 bit per level in part a of the figure and 2 bits per level in part b of the figure. In general, if a signal has *L* levels, each level needs *log2L* bits.

Bit Rate

The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). Figure 3.16 shows the bit rate for two signals.

Bit Length

The bit length is the distance one bit occupies on the transmission medium.

Bit length =propagation speed x bit duration

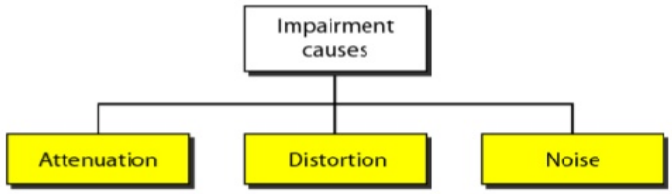
Baud Rate

The number of signal elements transmitted per second. A signal element consists of one or more bits.

Transmission impairments- attenuation distortion and noise

Transmission Impairments

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received.
Three causes of impairment are
1. Attenuation
2. Distortion
3. Noise



Attenuation

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal. Figure 3.26 shows the effect of attenuation and amplification.

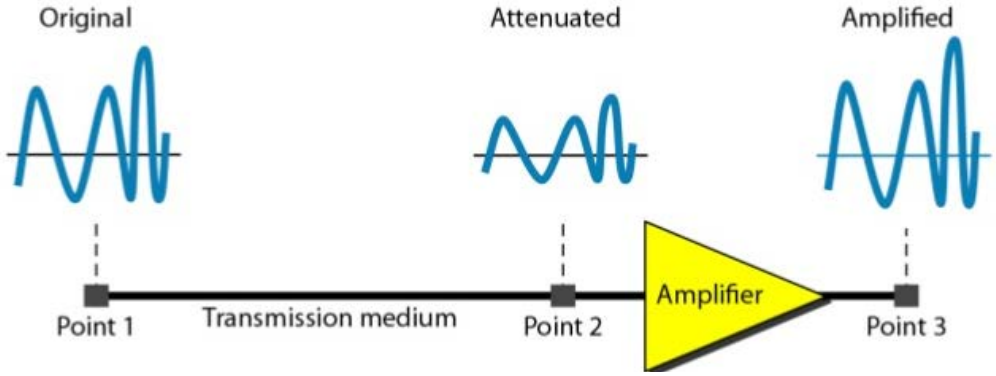


Figure 3.26 Attenuation

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.

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. Figure 3.28 shows the effect of distortion on a composite signal.

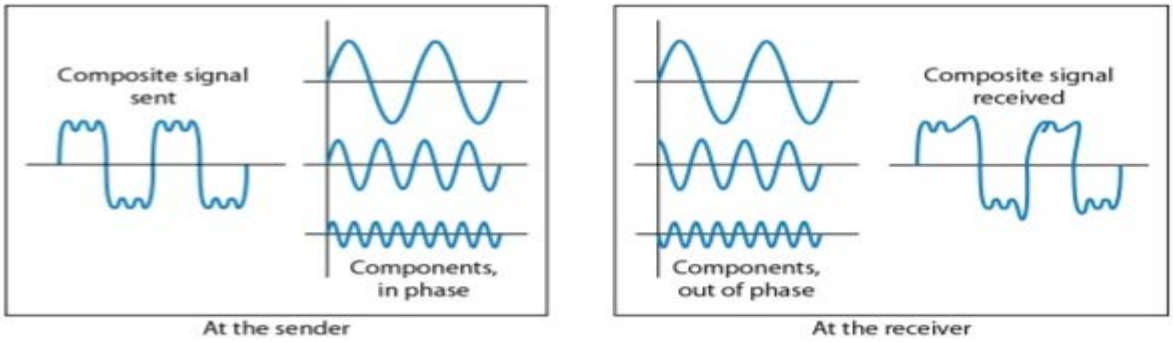


Figure 3.28 *Distortion*

Noise

Noise is another cause of impairment. Several types of noise, such as

- Thermal Noise
- Induced Noise
- Crosstalk
- 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) that comes from power lines, lightning, and so on. Figure 3.29 shows the effect of noise on a signal.

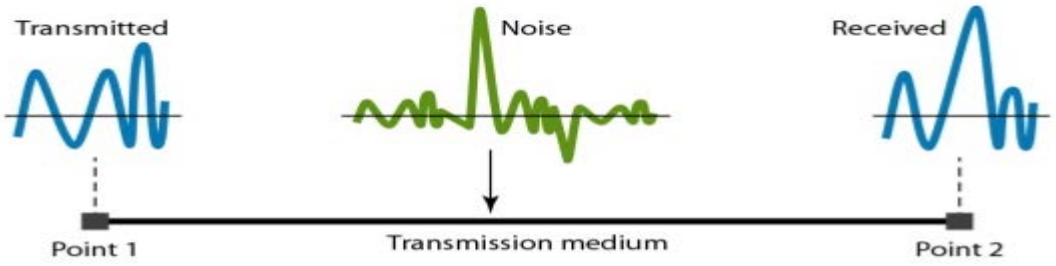


Figure 3.29 Noise

Signal-to-Noise Ratio (SNR)

It is the ratio of the signal power to the noise power. The signal-to-noise ratio is defined as

SNR=average signal power/average noise power

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. Because SNR is the ratio of two powers, it is often described in decibel units.

SNR_{dB}, defined as

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

Data communication protocols and standards

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
- Timing
  - **Syntax**. The term *syntax* refers to the **structure or format** of the data, meaning the order in which they are presented. 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

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 are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

Standards Organizations

Standards are developed through the cooperation of standards creation committees,forums, and government regulatory agencies.

Standards Creation Committees

o International Organization for Standardization (ISO). The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various

governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
o International Telecommunication Union-Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).

O American National Standards Institute (ANSI). Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.

O Institute of Electrical and Electronics Engineers (IEEE). The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

O Electronic Industries Association (EIA). Aligned with ANSI, the Electronic Industries Association is a non-profit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signalling specifications for data communication.

Forums
To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have developed **forums** made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies.

Regulatory Agencies
All communications technology is subject to regulation by government agencies such as the **Federal Communications Commission** (FCC) in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and international commerce as it relates to communications.

Internet Standards
An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by 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.

Network models - OSI model-layers and their functions.

A network is a combination of hardware and software that sends data from one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

OSI model
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

Purpose of OSI Model
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 not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

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.

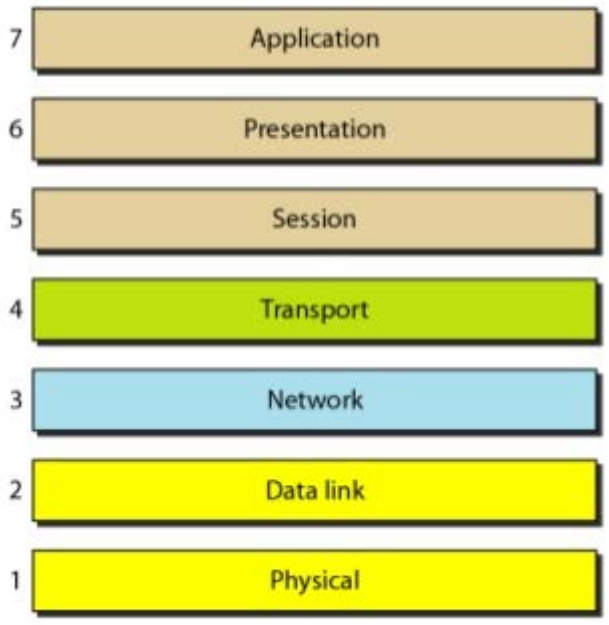


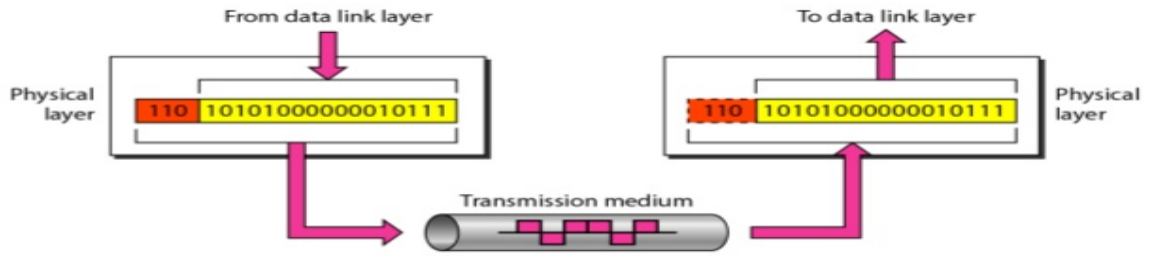
Figure 2.2 *Seven layers of the OSI model*

LAYERS IN THE OSI MODEL

Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure 2.5 shows the position of the physical layer with respect to the transmission medium and the data link layer.

Figure 2.5 ***Physical layer***



2.10

Figure 2.5 *Physical layer*

The physical layer is responsible for movements of individual bits from one hop (node) to the next.
The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium**.

The physical layer defines
1) the characteristics of the interface between the devices and the transmission medium.
2) the type of transmission medium.

- **Representation of bits.**

The physical layer data consists of a stream of bits (sequence of 0s or 1s) 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-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

- **Synchronization of bits**.

The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

- **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).

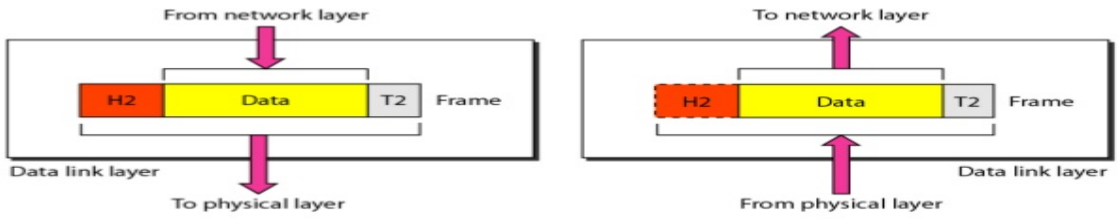
- **Transmission mode**.

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.

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 2.6 shows the relationship of the data link layer to the network and physical layers.

Figure 2.6 ***Data link layer***



2.12

Figure 2.6 *Data link layer*

The data link layer is responsible for moving frames from one hop (node) to the next. Other responsibilities of the data link layer include the following:

1)**Framing.**

The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

2) **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. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
3) **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.
4) **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.
5) **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.
Figure 2.7 illustrates hop-to-hop (node-to-node) delivery by the data link layer.

Figure 2.7 ***Hop-to-hop delivery***

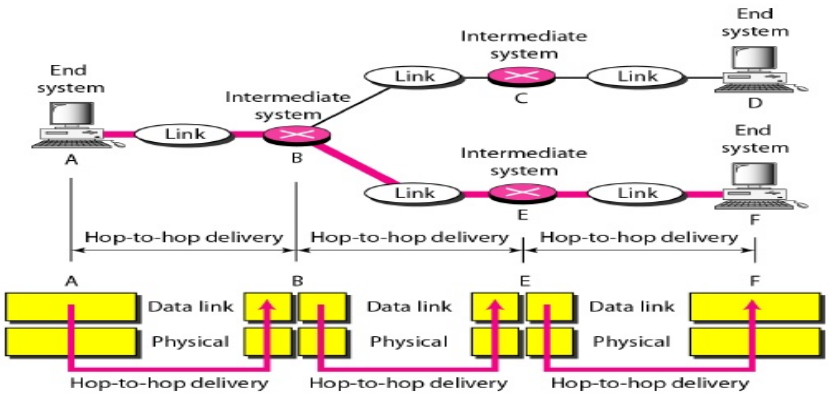


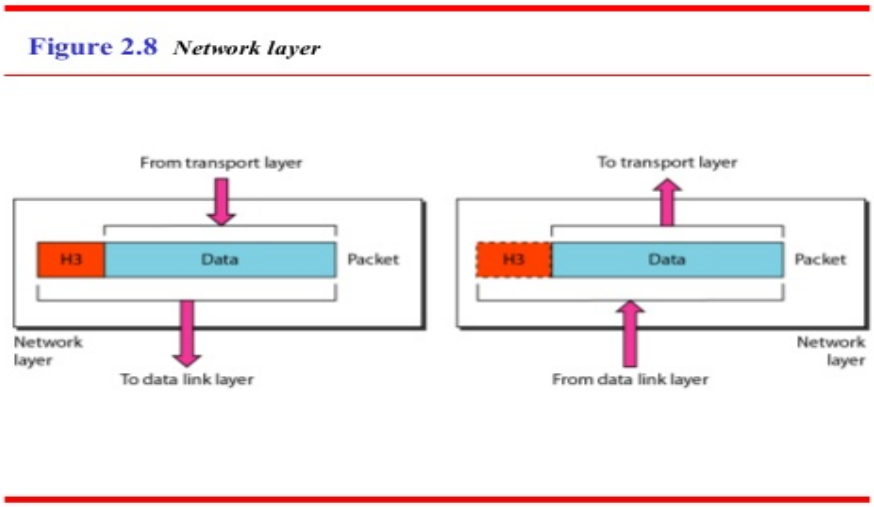
Figure 2.7 *Hop-to-hop delivery*

As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

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. Figure 2.8 shows the relationship of the network layer to the data link and transport layers.



2.15

Figure 2.8 *Network layer*

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

o **Logical addressing**.

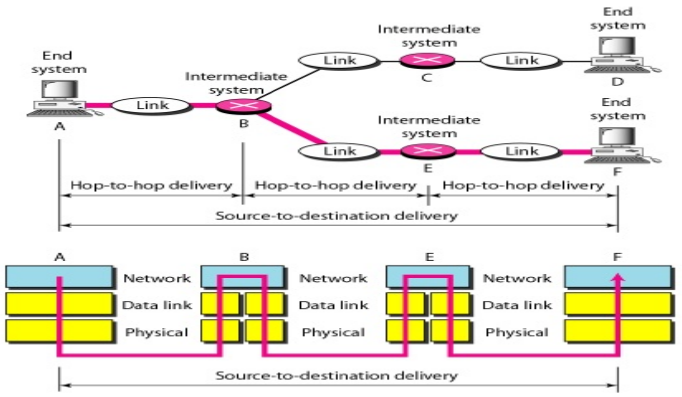
The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

o **Routing**.

When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Figure 2.9 illustrates end-to-end delivery by the network layer.

Figure 2.9 *Source-to-destination delivery*



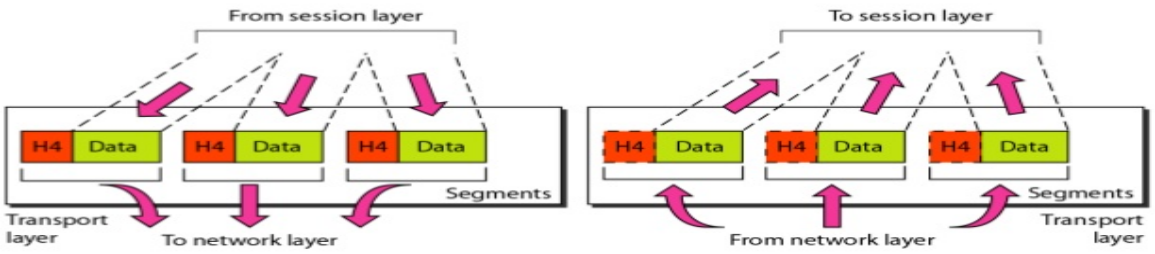
2.17

As the figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. Router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in turn, sends the packet to the network layer at F.

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. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 2.10 shows the relationship of the transport layer to the network and session layers.

Figure 2.10 *Transport layer*



2.18

The transport layer is responsible for the delivery of a message from one process to another.

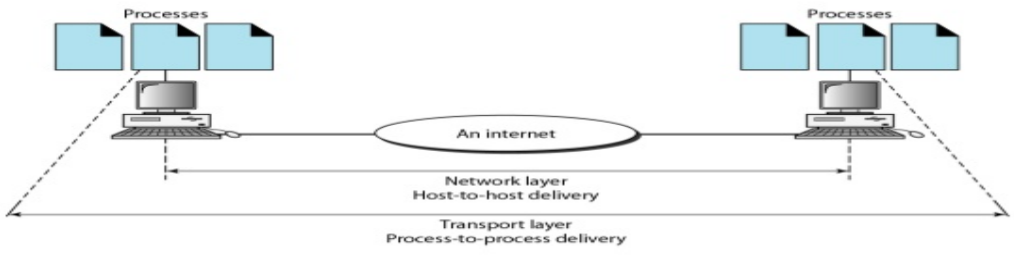
Other **responsibilities** of the **transport layer** include the following:

o **Service-point addressing**. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
o **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.
o **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 first before delivering the packets. After all the data are transferred, the connection is terminated.

o **Flow control**. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

o **Error control.** Like the data link layer, the transport layer is responsible for error control. However, 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.
Figure 2.11 illustrates process-to-process delivery by the transport layer.

Figure 2.11 ***Reliable process-to-process delivery of a message***



Session Layer

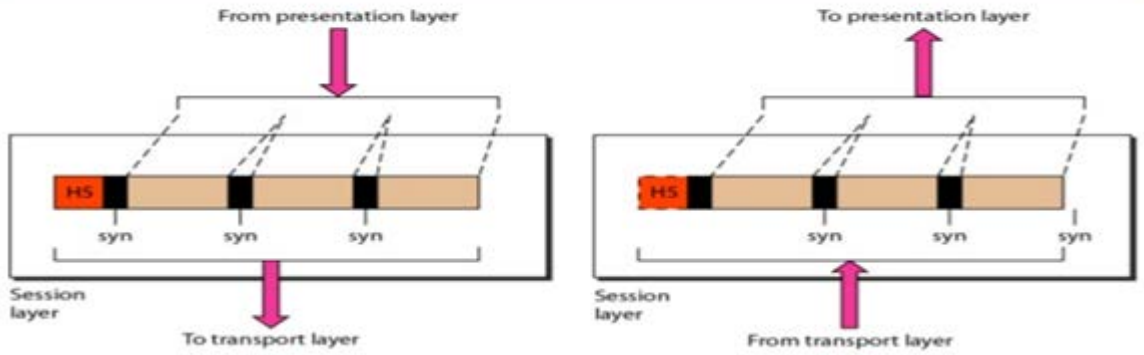
The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network ***dialog controller***. It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for **dialog control and synchronization.**
Specific responsibilities of the session layer include the following:

O **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 half duplex (one way at a time) or full-duplex (two ways at a time) mode.

O **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. Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.

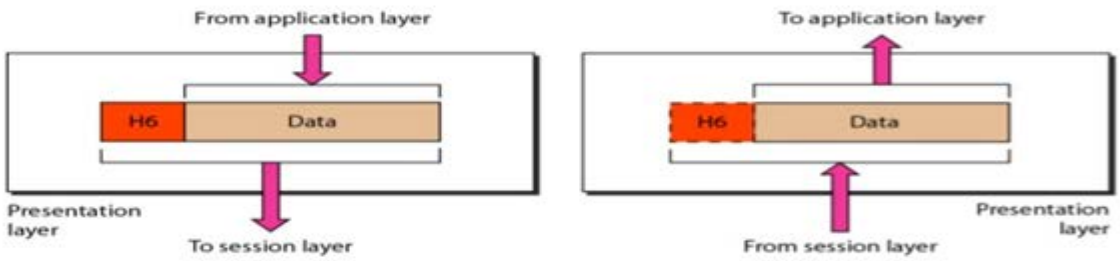
Figure 2.12 ***Session layer***



Presentation Layer

The presentation layer is concerned with the **syntax and semantics** of the information exchanged between two systems. Figure 2.13 shows the relationship between the presentation layer and the application and session layers.

Figure 2.13 ***Presentation layer***



The presentation layer is responsible for translation, compression, and encryption.
Specific responsibilities of the presentation layer include the following:

O **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. Because 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.

O **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.

O **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.

Application Layer

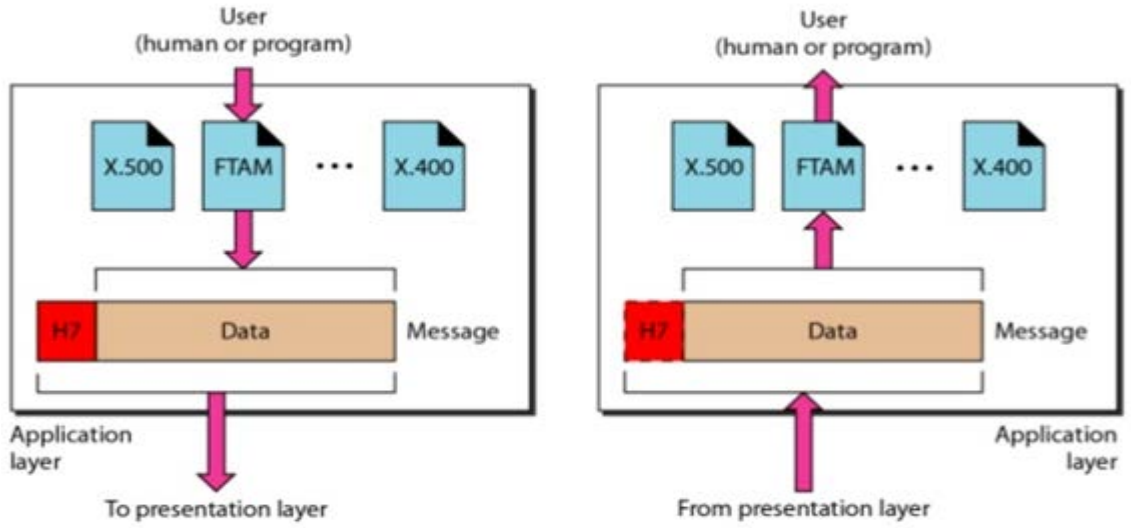
The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Figure 2.14 shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three:

- *X.4OO* (message-handling services)
- X.500 (directory services)
- file transfer,access, and management (FTAM).

The user in this example employs *X.4OO* to send an e-mail message.

Figure 2.14 ***Application layer***



The application layer is responsible for providing services to the user.

Specific services provided by the application layer include the following:

o **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. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

o **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.

o **Mail services.** This application provides the basis for e-mail forwarding and storage.

o **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

Summary of Layers

Figure 2.15 ***Summary of layers***

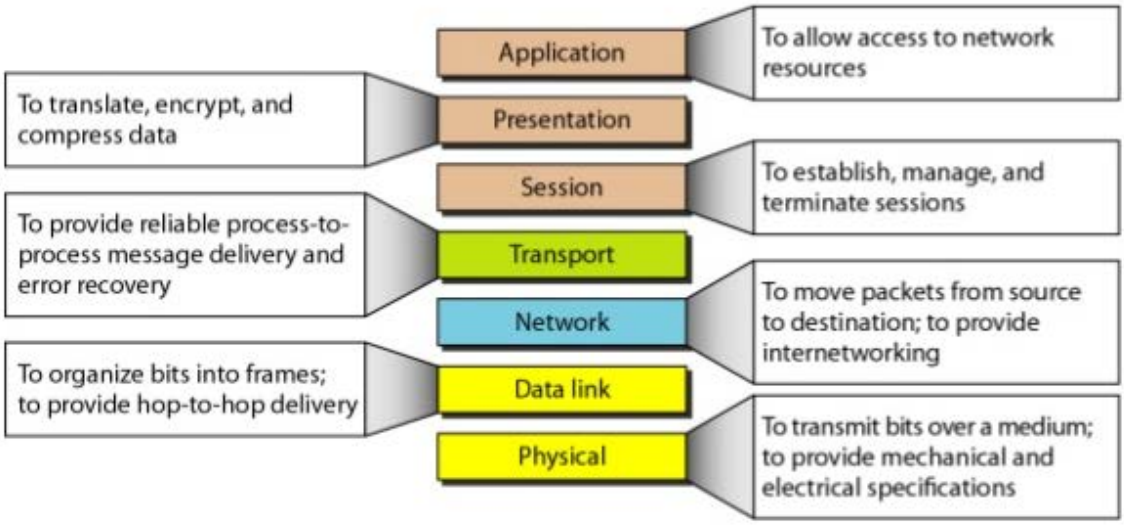


Figure 2.15 *Summary of layers*

TCP/IP PROTOCOL SUITE

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers:

1. Host-To-Network → Phy & Dat
2. Internet → network
3. Transport
4. Application. = part of session

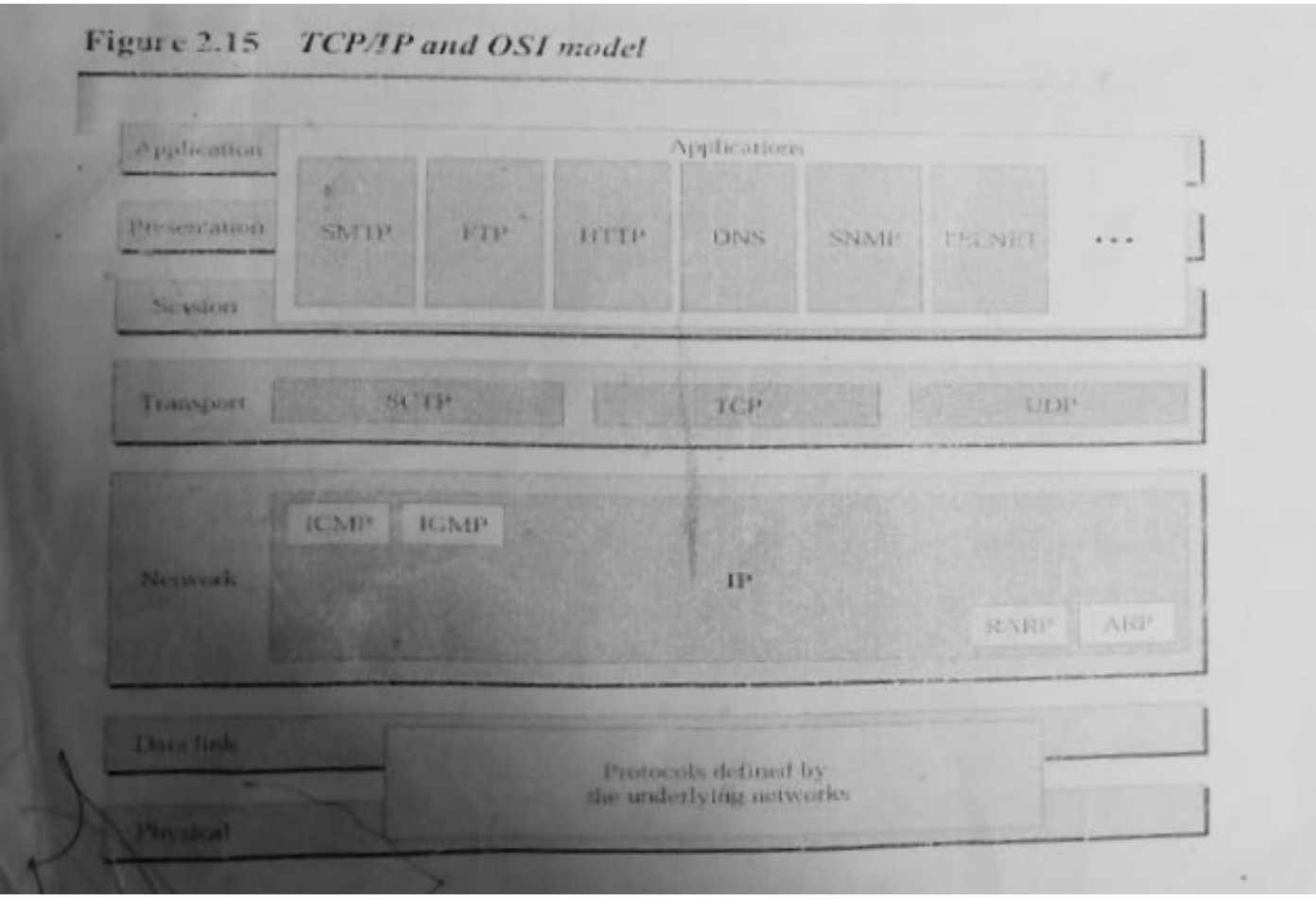
However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

Today TCP/IP protocol suite is thought of as a 5 layer model:

1. Physical,
2. Data Link
3. Network,
4. Transport
5. 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, however, are represented in TCP/IP by a single layer called the *application layer* (see Figure 2.16).

Figure 2.15 ***TCP/IP and OSI model***



TCP/IP is a **hierarchical protocol** made up of **interactive modules**, each of which provides a specific functionality but the modules are not necessarily interdependent.
Whereas the OSI model specifies which functions belong to each of its layers, 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)
- 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, *TCP/IP* does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a *TCP/IP* internetwork can be a local-area network or a wide-area network.

Network Layer
At the network layer (or, more accurately, the internetwork layer), *TCP/IP* supports the **Internetworking Protocol**. IP, in turn, 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 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

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.

The limited functionality of IP should not be considered a weakness, however. IP provides bare-bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

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

The Internet Control Message Protocol (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
- 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

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. 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

The 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, together with 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

The Stream Control Transmission Protocol (SCTP) 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 TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.