What is Data Communication?

Data communications means 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).

Characteristics of Data Communications:

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.

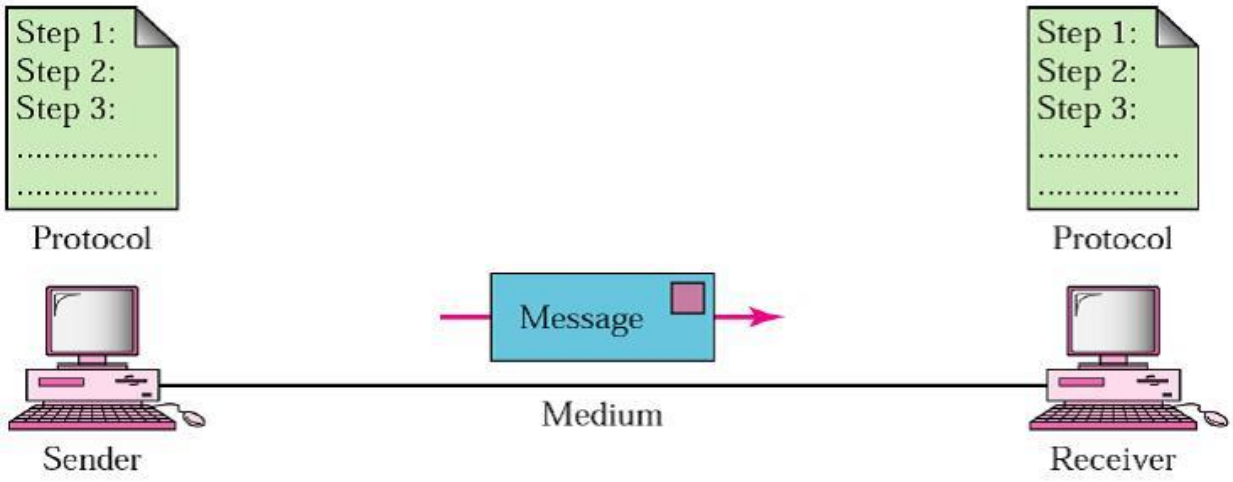
4. Jitter:

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 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Components of Data Communication

The different components of Data communication are shown in the following figure.



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:

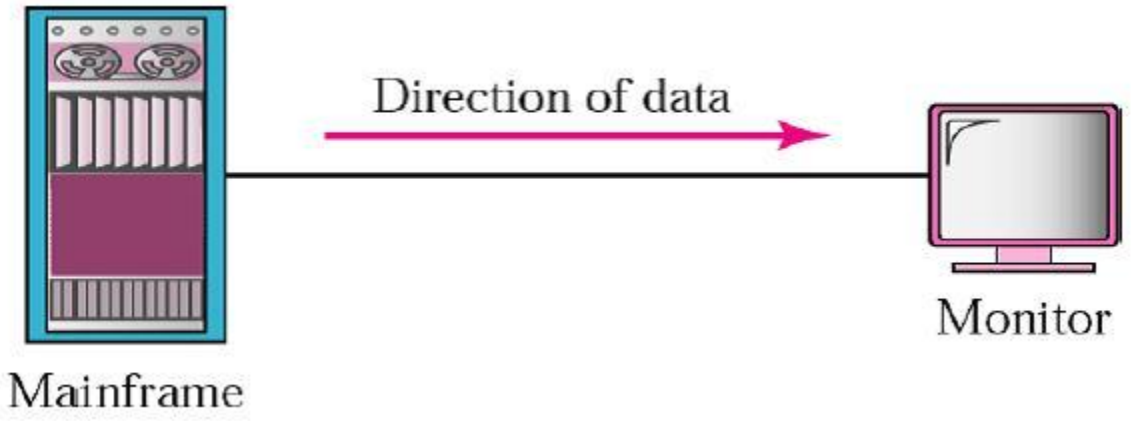
A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Different Data Flow Directions

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

1. Simplex:

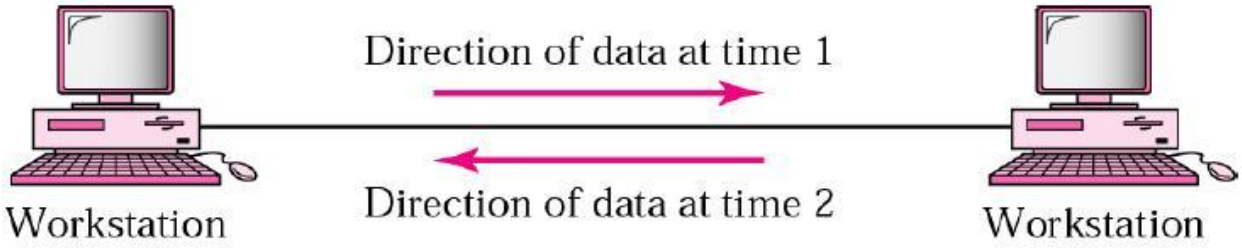
In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive which can be represented in the following figure.



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.

2.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 which will represent in the following figure.



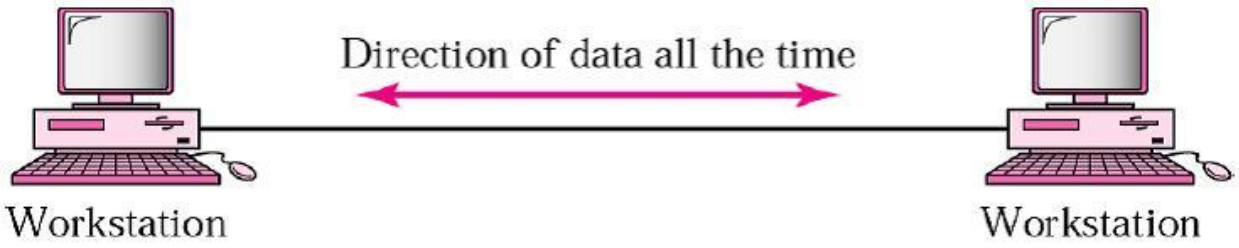
The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.

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 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.

3.Full-Duplex:

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously as shown in the following figure.



The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. 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 the 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.

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.

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance

Performance can be measured in many ways, including transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Reliability

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure

Security

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Network Physical Structures

We have said that a network is a two or more devices connected together and that a path is set up for communication to be reached between the two.

Now we will discuss the physical connections for Networks.

There are two possible connection types when it comes to Networks Point-to-point or Multipoint

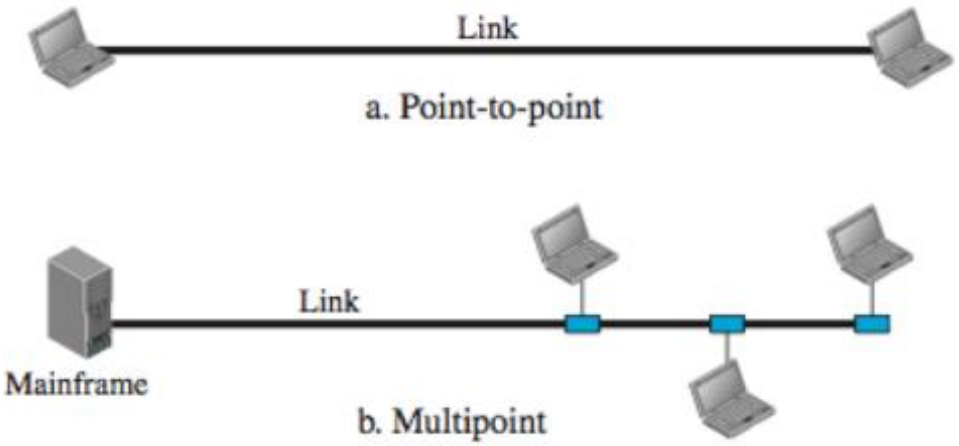
Point-to-point connections –

- provides a dedicated link or 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 microwave or satellite links, are also possible.
- Changing the T.V with a remote is a point-to-point connection between the remote control and the television.

Multipoint connections –

- more than two devices are sharing a link

- The entire capacity of the link is either shared spatially or temporally.
- This means either every computer shares a specific space of the link or each computer shares the link for a specific time when being used



Networks all have a physical topology.

Physical Topology – the way a network is laid out physically.

Two or more devices connect to a link

Two or more links form a topology.

A linking device in a network is called a node.

There are four basic types of topologies available.

Mesh –

every device has a dedicated point-to-point link to every other device.

In a mesh topology, each physical link carries information only between the two devices that it connects.

If it is a duplex connection, you only need half the physical links, since each link travels both ways.

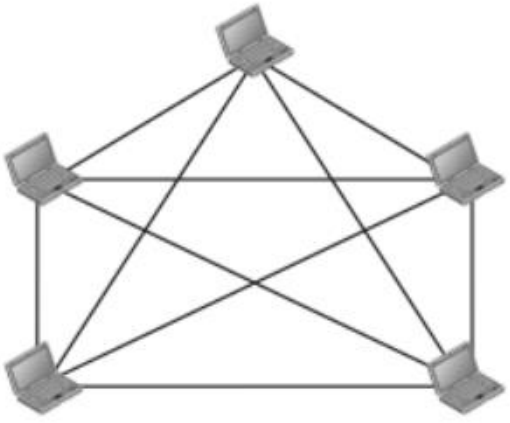
Advantages of a Mesh topology

- Avoid traffic since each link can carry its own data and none are being shared
- If one link breaks, the rest of the network is still functional
- Privacy since only the dedicated device receives the message.
- Easy to detect a problem in the network by discovering which device is having problems and examining the link that connects to it.

Disadvantages of a Mesh topology

- A lot of cables are needed
- Too many cables too much cost
- Too many cables not enough physical space

$n = 5$
10 links.



Star –

- each device is connected to a hub through a dedicated point-to-point link.
- The devices are not directly linked to each other.
- If one device wants to send data to another, it sends it first to the hub, which then forwards the data to the other connected device.

<u>Advantages of a Star topology</u>

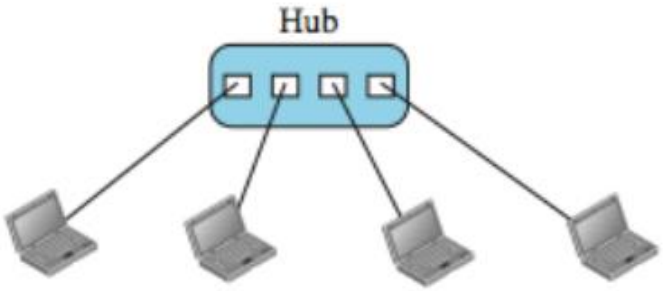
• Less expensive than mesh

• Easy to install, easy to configure

• If one link fails the network can still function

<u>Disadvantages of a Star topology</u>

• Everything depends on the hub



Bus – Multipoint connection.

- One long cable acts as a backbone; other devices are connected through a drop line and a tap in the link.
- Drop line – a connection running between a device and a main cable.

- Tap – a physical device that punctures the cable and connects to it.
- The longer the cable and the more taps it has the weaker the signal becomes.
- Taps should be a short distance from each other.

<u>Advantages of a Bus topology</u>

• Easy to install

• Minimal Cable

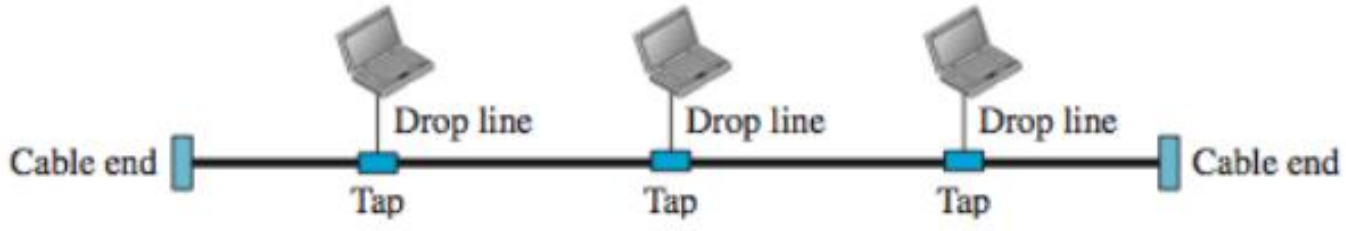
<u>Disadvantages of a Bus topology</u>

• Difficult reconnection

• Difficult to find the problem

• Difficult to add new devices

• Break stops all transmission of data



Ring –

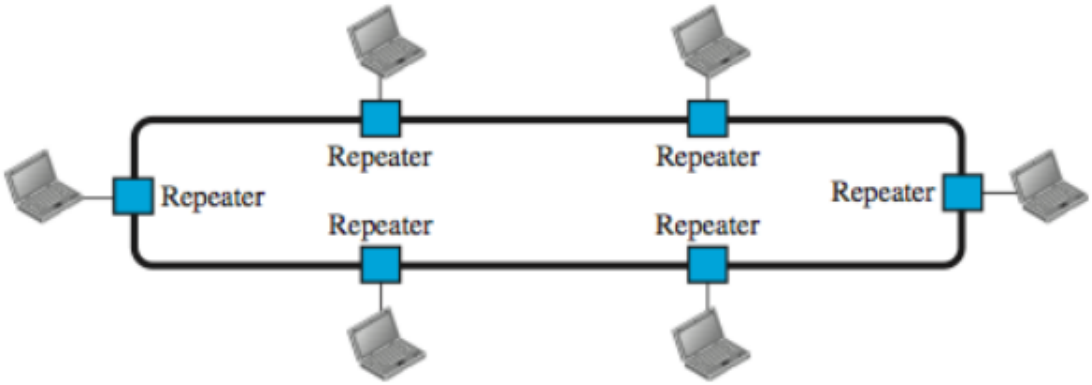
- devices in a ring topology has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction from device to device until the destination is reach.
- Each device has a repeater that passes the data received that is intended for another device along.

Advantages of a Ring topology

- Easy to install
- Easy to reconfigure
- Easy to detect a problem

Disadvantages of a Ring topology

- Break means the whole system is dead



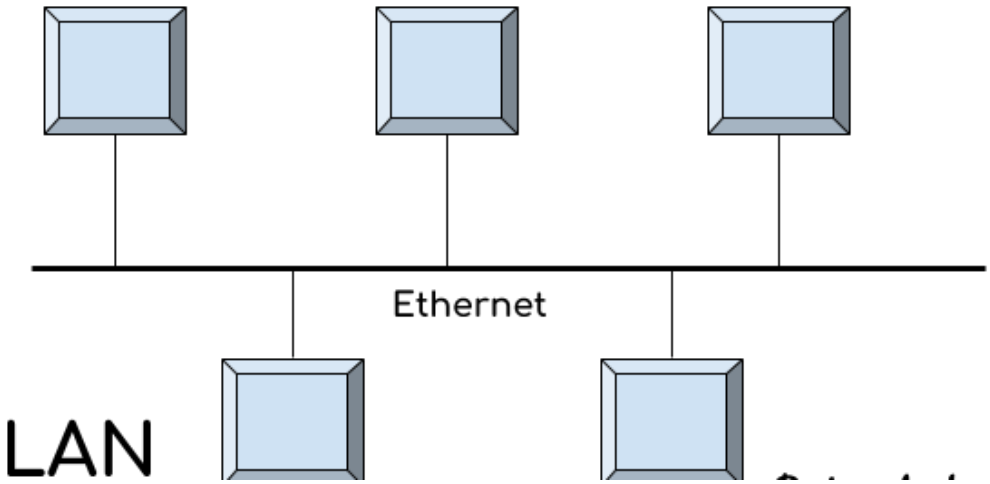
Categories of Networks
Today when we speak of networks, we are generally referring to two primary categories:
local-area networks and wide-area networks. The category into which a network
falls is determined by its size. A LAN normally covers an area less than 2 mi; aWAN can
be worldwide. Networks of a size in between are normally referred to as metropolitanarea
networks and span tens of miles.

There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)

2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

Local Area Network (LAN)

Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

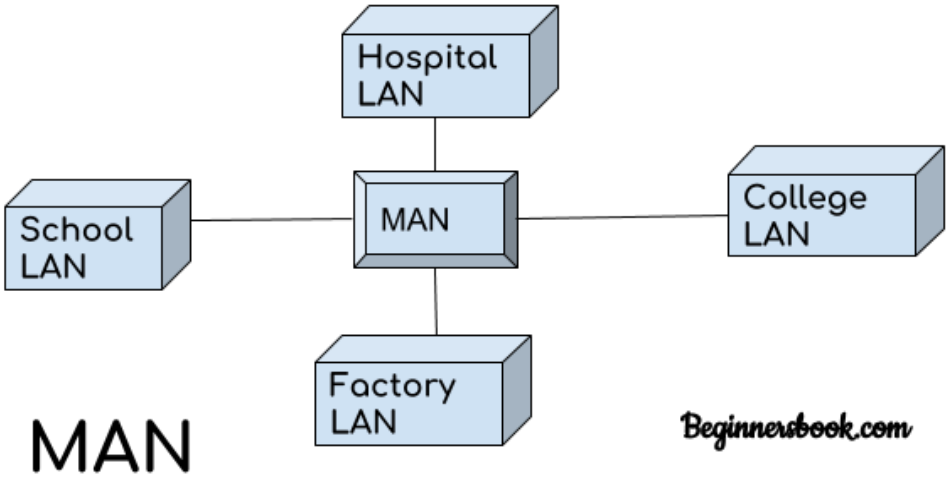


Metropolitan Area Network (MAN)

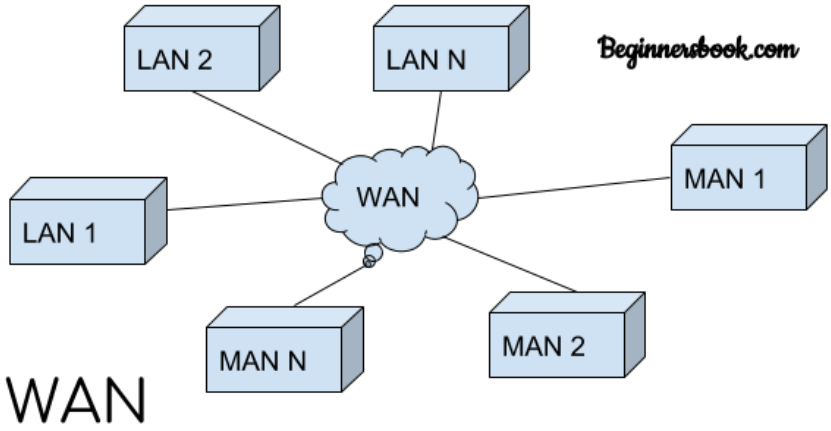
MAN network covers larger area by connections LANs to a larger network of computers.

In Metropolitan area network various Local area networks are connected with each other through telephone lines.

The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.



Wide area network (WAN)



Wide area network provides long distance transmission of data.

the size of the WAN is larger than LAN and MAN.

A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN.

Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Protocols and Standards

I.Protocols:

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information.

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.

1.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.

2.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?

3.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.

II. Standards:

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications. Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

a.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.

b.De jure:

Those standards that have been legislated by an officially recognized body are de jure standards.

Summary:

- Data communications are the transfer of data from one device to another via some form of transmission medium.
- A data communications system must transmit data to the correct destination in an accurate and timely manner.
- The five components that make up a data communications system are the message, sender, receiver, medium, and protocol.
- Text, numbers, images, audio, and video are different forms of information.
- Data flow between two devices can occur in one of three ways: simplex, half-duplex,or full-duplex.
- A network is a set of communication devices connected by media links.
- In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link.
- Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.
- A network can be categorized as a local area network or a wide area network.
- A LAN is a data communication system within a building, plant, or campus, or between nearby buildings.
- A WAN is a data communication system spanning states, countries, or the whole world.
- A protocol is a set of rules that govern data communication; the key elements of a protocol are syntax, semantics, and timing.