TH-2 DATA COMMUNICATION & COMPUTER NETWORK

Theory : 4 Period Per Week
Total Period : 60 Periods
Examination : 3 Hours

I.A : 20 Marks
Term End Exam : 80 Marks
Total marks : 100 Marks

Chapter wise distribution of Periods with total Periods

SL.NO	Topics	Periods
1.	NETWORK & PROTOCOL	08
2.	DATA TRANSMISSION & MEDIA	08
3.	DATA ENCODING	08
4.	DATA COMMUNICATION & DATA LINK CONTROL	08
5.	SWITCHING & ROUTING	10
6.	LAN TECHNOLOGY	10
7.	TCP / IP	08
	TOTAL	60

Detailed Contents:

Unit-1 : Network & Protocol
- 1.1 Data communication
- 1.2 Networks
- 1.3 Protocol & Architecture, standards, OSI, TCP / IP

Unit-2 : Data transmission & media
- 2.1 Data transmission concepts and terminology
- 2.2 Analog and digital data transmission
- 2.3 Transmission impairments, channel capacity
- 2.4 Transmission media, guided transmission, wireless transmission

Unit-3 : Data encoding
- 3.1 Data encoding
- 3.2 Digital data digital signals,
- 3.3 Digital data analog signals
- 3.4 Analog data digital signals
- 3.5 Analog data analog signals

Unit-4 Data communication & data link control
4.1 Asynchronous and synchronous transmission
4.2 Error detection
4.3 Line configuration
4.4 Flow control
4.5 Error control
4.6 Multiplexing
4.7 FDM Synchronous TDM
4.8 Statistical TDM

Unit-5 Switching & Routing
5.1 Circuit switching network
5.2 Packet switching Principle
5.3 X.25
5.4 Routing in packet switching
5.5 Congestion
5.6 Effects of Congestion, Congestion control
5.7 Traffic management
5.8 Congestion control in Packet switching network.

Unit-6 LAN Technology
6.1 Topology and transmission media
6.2 LAN Protocol Architecture
6.3 Medium Access control
6.4 Bridges, Hub, switch
6.5 Ethernet (CSMA/CD), Fiber channel
6.6 Wireless LAN Technology

Unit-7 TCP/IP
7.1 TCP/IP Protocol suite
7.2 Basic Protocol Functions
7.3 Principle of internet working
7.4 Internet Protocol Operations
7.5 Internet Protocol

BOOKS RECOMMENDED :

Sl NO	Name of Authors	Title of the book	Name of the Publisher
01	W. Stallings	Data communication & Computer Network	PHI
02	M. Bhatia	Introduction to Computer Network	Univ. S. Press
03	Forouzen	Data communication & network	TMH

Lecturer - Jyotiprakash Behera
Mob :- 7008140500
E-mail :- Jyotiprakash.522@gmail.com

CHAPTER-1 NETWORK & PROTOCOL

1.1 DATA COMMUNICATIONS

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Topics discussed in this section:

(i) Components of a data communications system.

(ii) Data Flow.

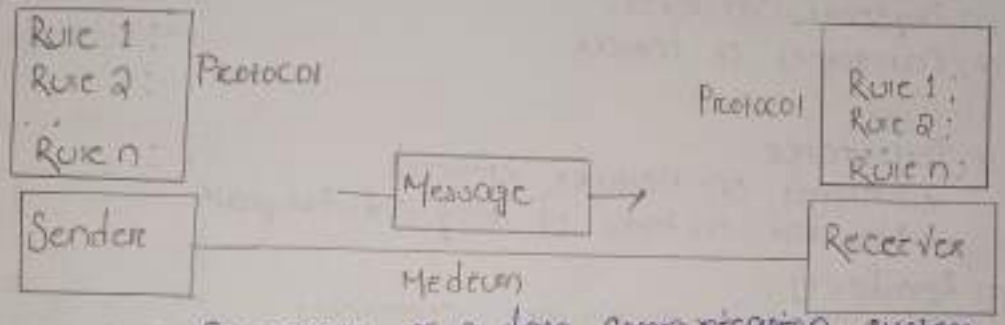
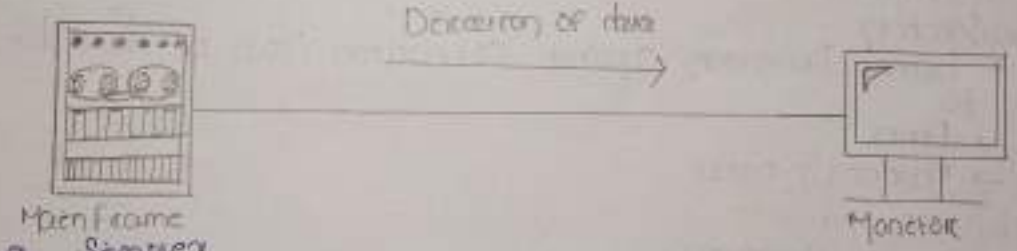
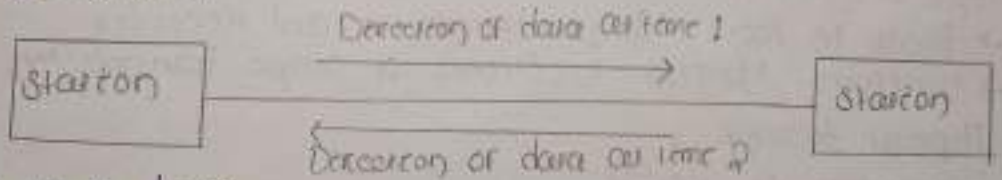


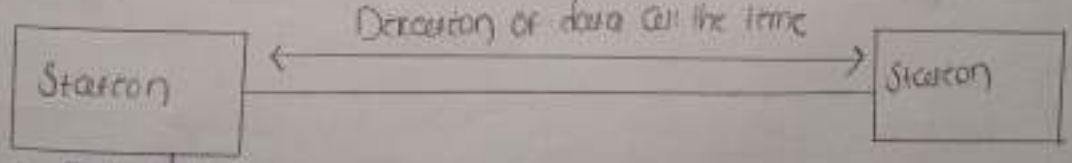
Figure 1.1 Components of a data communication system



a. Simplex



b. Half-duplex



c. Full-duplex

Figure 1.2 Data Flow (Simplex, half-duplex and full-duplex)

1.2 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 link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Topics discussed in this section:

(i) Network Criteria.
(ii) Physical Structures.
(iii) Categories of network.

Network Criteria

(i) Performance
→ Depends on network elements
→ Measured in terms of delay and throughput

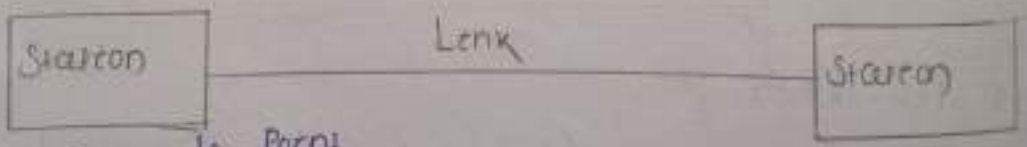
(ii) Reliability
→ Failure rate of network components
→ Measured in terms of availability / robustness

(iii) Security
* Data Protection against corruption / loss of data due to
→ Errors
→ Malicious users

Physical Structure

(i) Type of Connection
→ Point to point - Single transmitter and receiver
→ Multipoint - Multiple recipients of single transmission

(ii) Physical topology
→ Connection of device
→ Type of transmission - unicast, multicast, broadcast



a. Point - to - Point

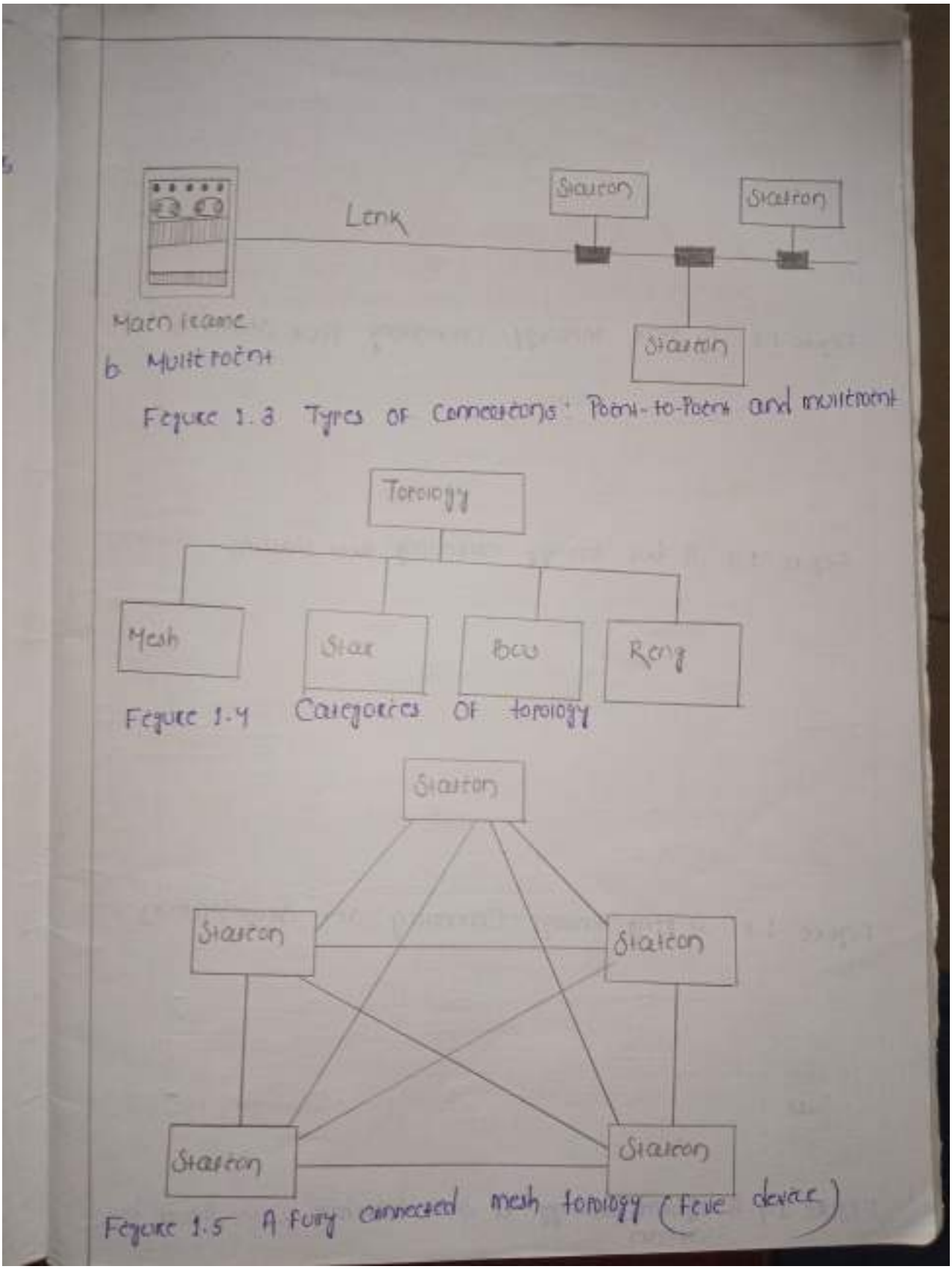
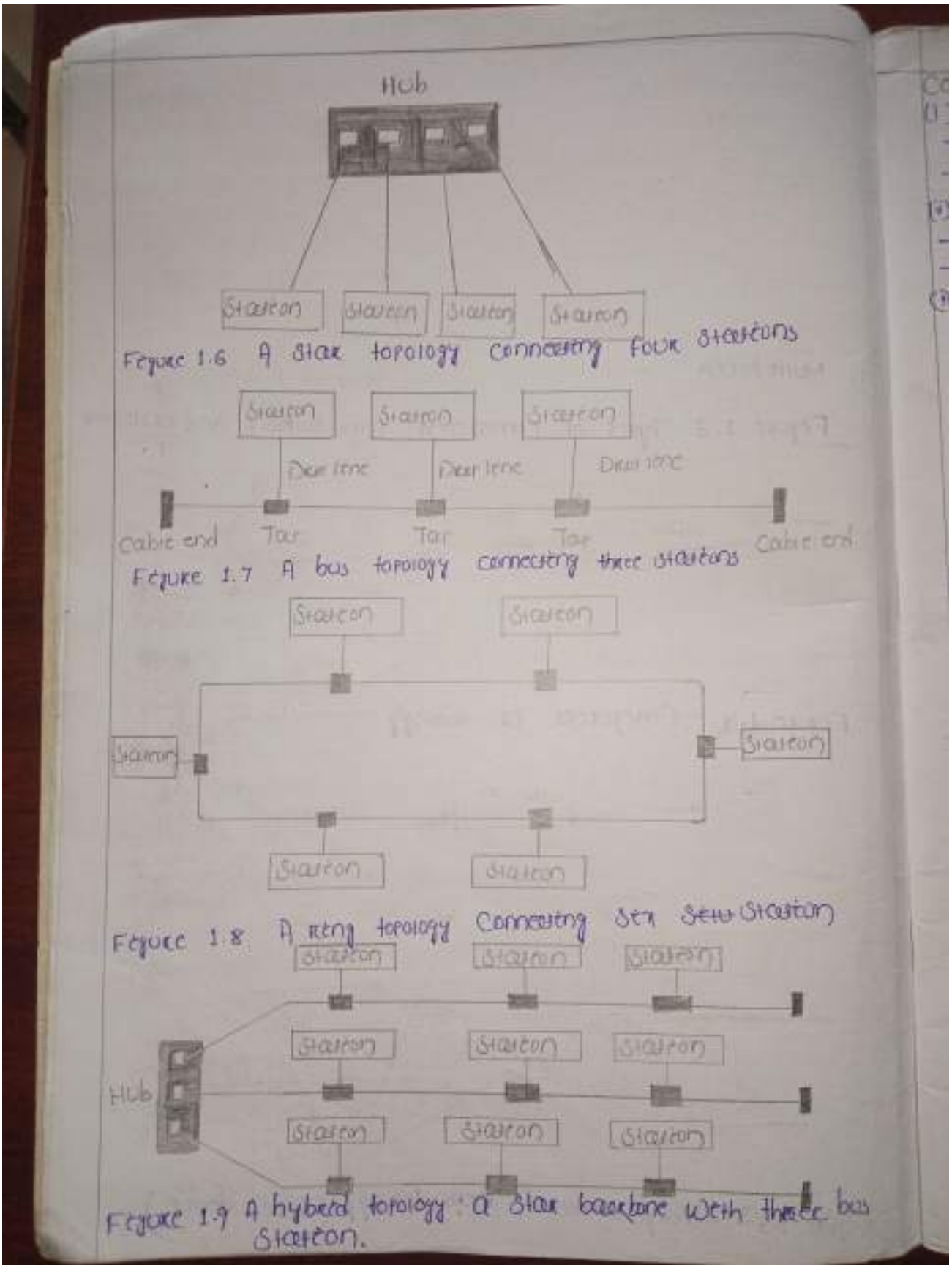


Figure 1.3 Types of connections: Point-to-Point and multipoint

Figure 1.4 Categories of topology

Figure 1.5 A fully connected mesh topology (five devices)


Hub
Station
Station
Station
Station
Figure 1.6 A star topology connecting four stations
Station
Station
Station
Cable end
Tap
Tap
Tap
Cable end
Figure 1.7 A bus topology connecting three stations
Station
Station
Station
Station
Station
Station
Figure 1.8 A ring topology connecting ten stations
Station
Station
Station
Station
Station
Station
Station
Station
Station
Hub
Figure 1.9 A hybrid topology: a star backbone with three bus stations.

Categories of Network

(i) Local Area Network (LANs)
→ Short distances
→ Designed to provide local interconnectivity

(ii) Wide Area Network (WANs)
→ Long distances
→ Provide connectivity over large areas

(iii) Metropolitan Area Network (MANs)
→ Provide connectivity over areas such as a city, a campus

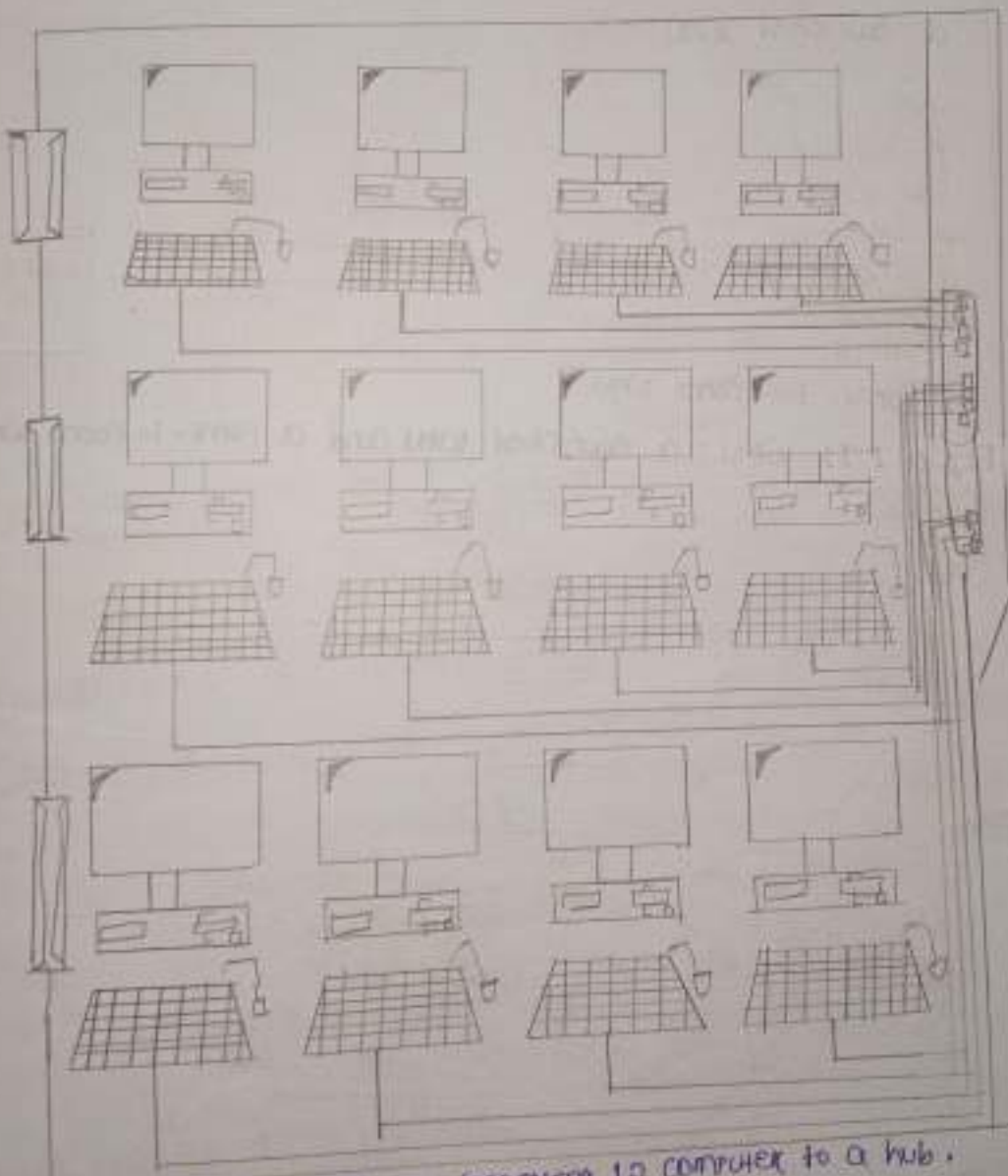
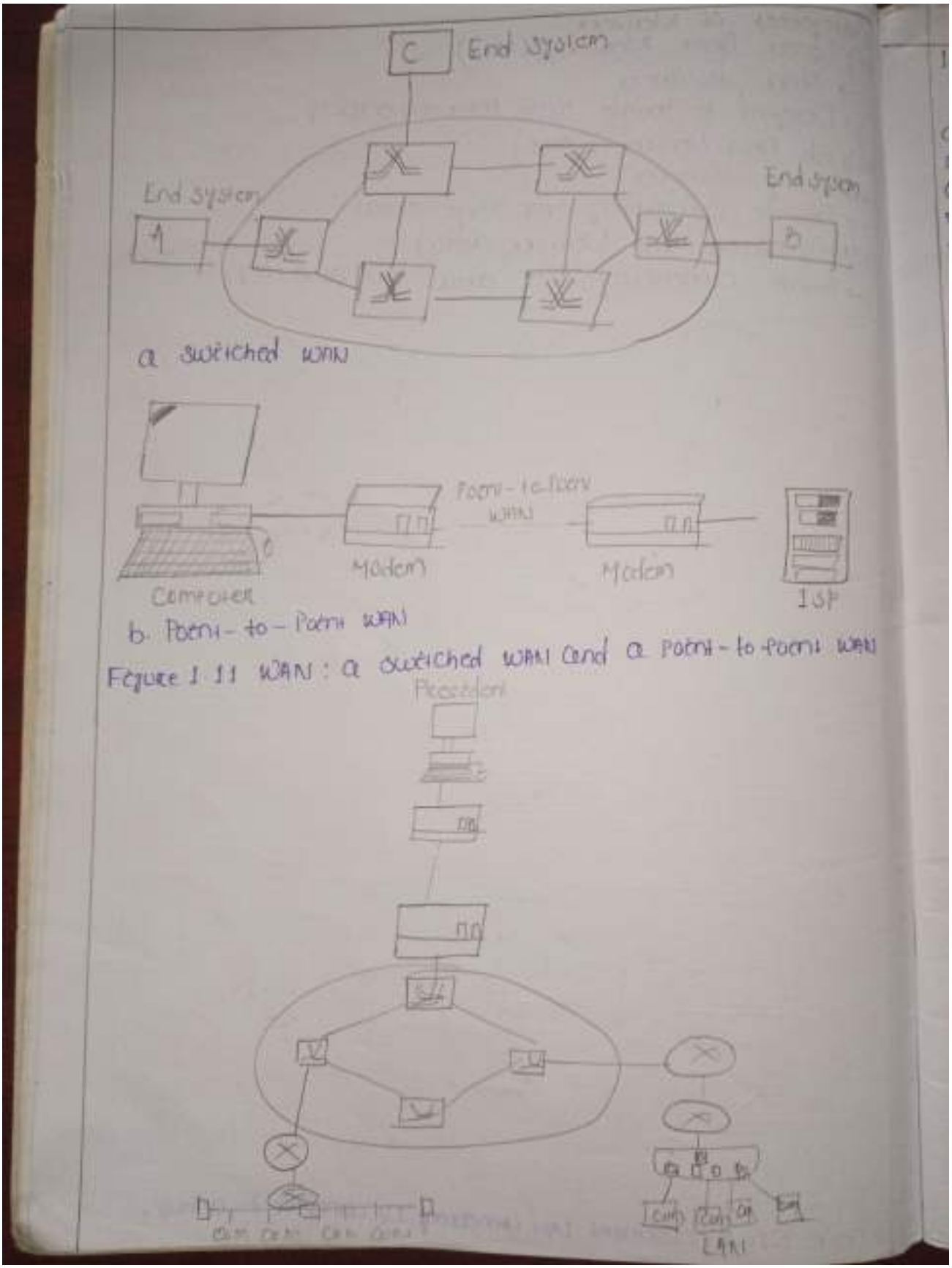


Figure 1.10 An interconnected LAN connecting 12 computer to a hub.



a switched WAN

b. Point-to-Point WAN

Figure 1.11 WAN: a switched WAN and a point-to-point WAN

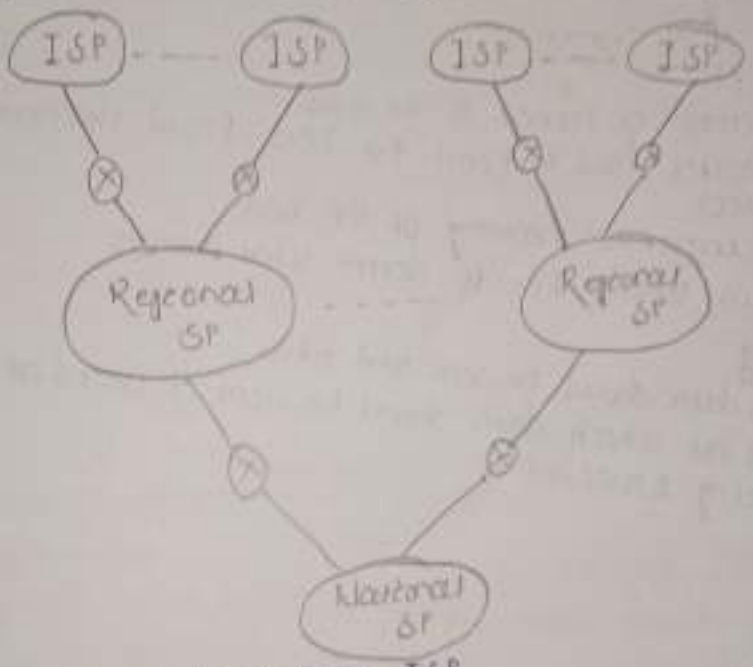
1.3 The Internet

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

Topics discussed in this section:

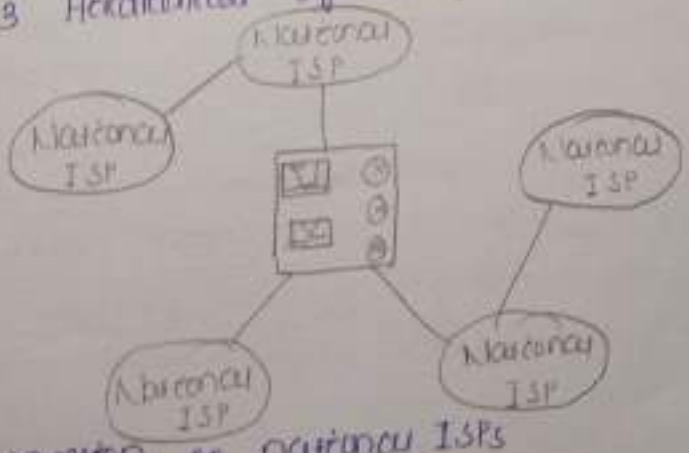
Organization of the Internet

Internet Service Providers (ISPs)



a. Hierarchical of a national ISP

Figure 1.13 Hierarchical organization of the Internet



b Interconnection of national ISPs

1.4 PROTOCOLS

A Protocol is synonymous with rule. It consists of a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Topics discussed in this section:

(i) Syntax
(ii) Semantics
(iii) Timing

Elements of a Protocol

(i) Syntax:
→ Structure or format of the data
→ Indicates how to read the bits - field delineation

(ii) Semantics
→ Interprets the meaning of the bits
→ knows which fields define what action

(iii) Timing
→ When data should be sent and what
→ Speed at which data should be sent or speed at which it is being received.

Unit-1 NETWORK AND PROTOCOL

1.1 DATA COMMUNICATION :

Introduction of data communication :-

In data communications, data generally are deemed as information that is stored on digital form. Data communications is the process of transferring digital information between two or more points. Information is deemed as the knowledge or intelligence, Reception & Processing of digital information. For data communication to occur, the communicating device must be part of a communication system made up to combination of hardware (Physical equipment) & software (programs).

The effectiveness of a data communication system depends on four fundamental characteristics. There are :

(i) Delivery
(ii) Accuracy
(iii) Timeliness
(iv) Jitter

A data communication system has five components.
There are : (i) Sender
(ii) Receiver
(iii) Transmission medium
(iv) Protocol
(v) Message

* **Delivery :-**
The system must deliver data to the correct destination. data must be received by the intended device or user & only by that device or user.

* **Accuracy :**
The system must deliver the data accurately data that have been altered in transmission and left uncorrected are unusable.

* **Timeliness :**
The system must deliver data in a timely manner data delivered late are useless. In the case of video & audio, timely delivery means delivery data as they are produced, and without significant delay. This kind of delivery is called real time transmission.

* Jitter :

The system Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or audio or video packets. For eg: packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

* Message :

The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio & video.

* Sender :

The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera and so on.

* Receiver :

The receiver is the device that receives ~~that~~ the message. It can be a computer, workstation, telephone handset, television & so on.

* Transmission Medium :

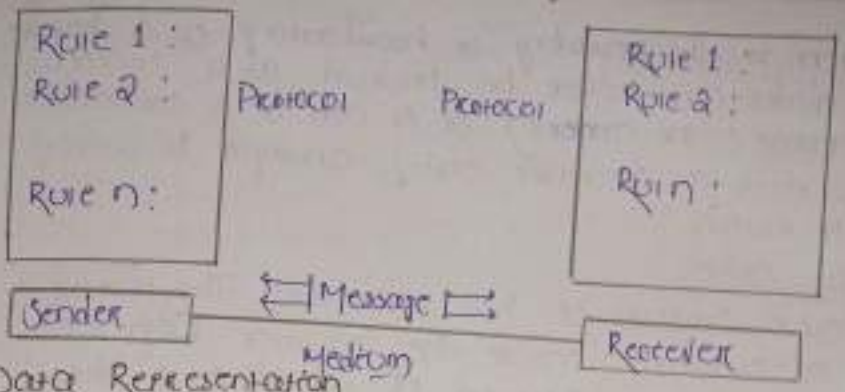
The transmission medium is the physical path by which a message travels from sender to receiver. Some example of transmission medium include twisted pair wire, coaxial cable, fibre-optic cable & radio waves.

* Protocol :

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

* A data communication system has five components.

Five Components of data communication :-



* Data Representation

Information today comes in different forms such as text, numbers, image, audio & video.

(i) Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different set of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.

(ii) Number

Number are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operation. Appendix B discuss several different numbering system.

(iii) Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixel (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

(iv) Audio

Audio refers to the recording or broadcasting of sound or music. Audio by nature different from text, numbers or image. It is continuous, not discrete.

(v) Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (example: TV camera) or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

* Co-axial Cable

Co axial cable consists of two conductors. The inner conductor is contained inside the insulator with the other conductor weaves around it providing a shield. An insulating protective coating called a jacket covers the outer conductor. The outer shield protects the inner conductor from outside electrical signals. Distance between the outer conductor & inner conductor plus the type of material used for insulating the inner conductor determine the cable properties.

Transmission modes in computer networks

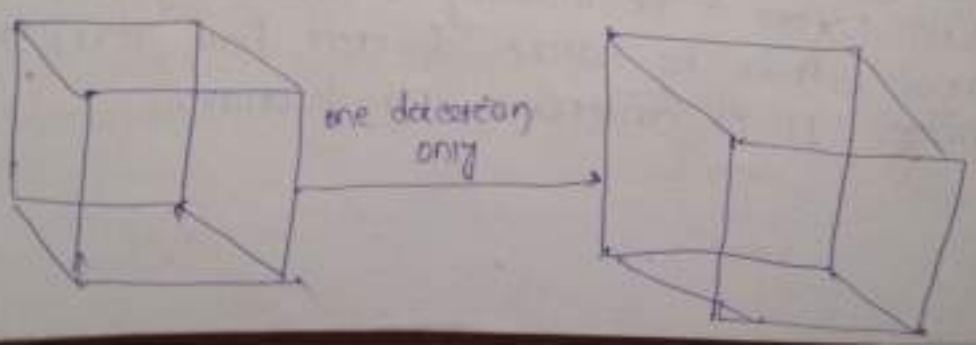
There are 3 types of transmission modes which are:

(i) Simplex mode
(ii) Half duplex mode
(iii) Full duplex mode

(i) Simplex Mode

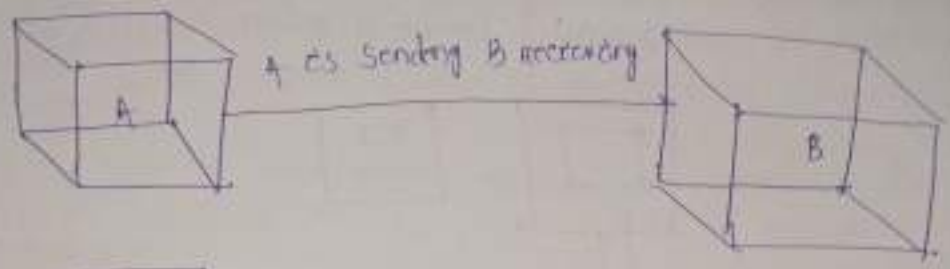
The communication is unidirectional, as on a one way street. Only one of the two devices on a link transmits; the other can only receive.

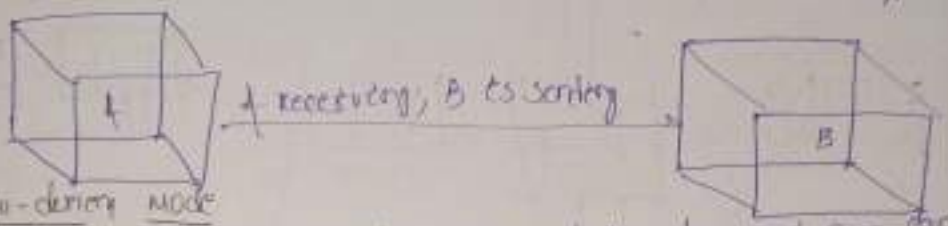
Keyboard and traditional monitors are examples of simplex device. The keyboard can only introduce input, the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.



(ii) Half-duplex mode

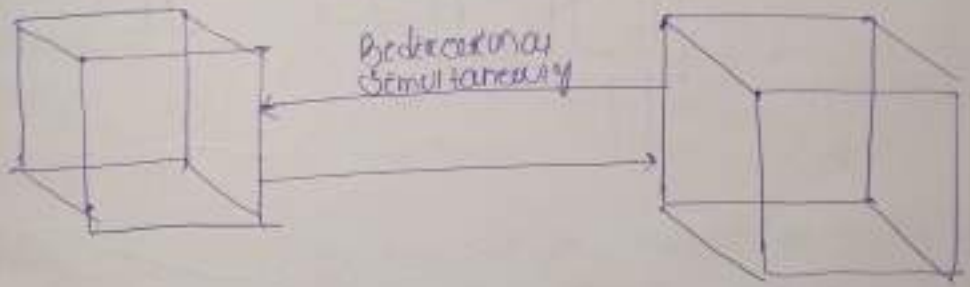
In half-duplex mode, sender can send the data and also can receive the data but one at a time. It is two-way directional communication but once at a time.





(iii) Full-duplex mode

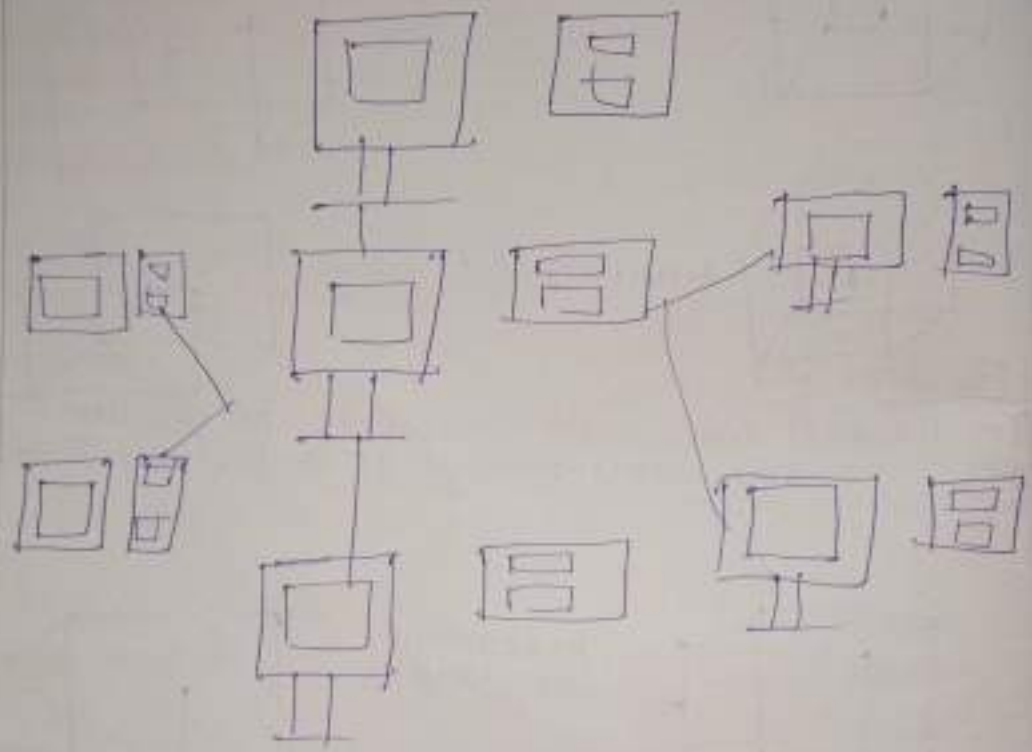
In full duplex mode, sender can send the data and also can receive the data simultaneously. It is two-way directional communication simultaneously.



1.2 NETWORK:

A network consist of two or more computers that are linked in order to share resource (such as Printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams.

- Distributed Processing:
Most network use distributed processing in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computers or workstation) handle a subset.



- Networking Criteria:
A network must be able to meet a certain number of criteria. The most important of these are ~~perf~~ performance, Reliability and Security.

(i) Performance:

Performance can be measured in many ways including transit and response time. Transmit time is the amount of the required for a message to travel from one device to another. Response time is the elapsed time between an enquiry and a response. The performance of a network depends on a network 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 performance is often evaluated by two networking metrics: throughput and delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

(ii) Reliability:

In addition of accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

(iii) Security:

Network security issues include protecting data from damage and development, and implement policies and procedure for recovery from breaches and data losses.

→ LAN:

A local area network (LAN) is a collection of device connected together in one physical location, such as a building office or large ranging from a home network with thousand of users and devices in an office or school.

Regardless of size, a Lan's single defining characteristics is that it connect devices that can are in a single, limited area. A Lan comprises cables, access points, switches routers and other components the enable devices to connect to internal services, web servers, and other Lans via wide area networks. The advantages of lan are the same as those for any group of devices networked together.

The device can use a single internet connection, share files with one another, print to shared printers and be accessed and even controlled by one another.

→ WAN :-

Wide area network (WAN) is a collection of (LAN) or other networks that communicate with one other. A WAN is essentially a network, with the internet the world's largest WAN.

Today there are several type of WAN is built for a variety of use cases that touch virtually every aspect of modern life. WAN orchestration use a variety of techniques, including duplication compression, protocol optimization traffic shaping and local caching these techniques ensure packet delivery and traffic control on a given delivery network bandwidth to grow or shrink dynamically as needed.

→ MAN :-

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and town, or any given large area with multiple buildings. A MAN is large than wide area network (WAN). MAN do not have to be in urban areas; the term "metropolitan" implies the size of the network not the demographics of the area that it serves.

→ DIFFERENCE BETWEEN LAN & WAN:

LAN	WAN
→ LAN stands for local area network	→ WAN stands for wide area network.
→ LAN's ownership is private	→ WAN ownership is public.
→ The speed of LAN is high (more than WAN).	→ where the speed of WAN is (slower than LAN)
→ The propagation delay is short in LAN.	→ where the propagation delay in WAN is long (longer than LAN).
→ There is less congestion in LAN.	→ while there is more congestion in WAN.
→ There is more fault tolerance in LAN.	→ where there is less fault tolerance in WAN.

1.3 OPEN SYSTEM INTERCONNECTION (OSI):

International standard organization (ISO) establishes a committee in 1977 to develop architecture for computer communication and the OSI model is the result of this effort. In 1984, the open systems interconnection (OSI) reference model was approved as an international standard for communications architecture.

The OSI reference model divides the problems of moving information between computers over a network medium into seven smaller and more manageable problems.

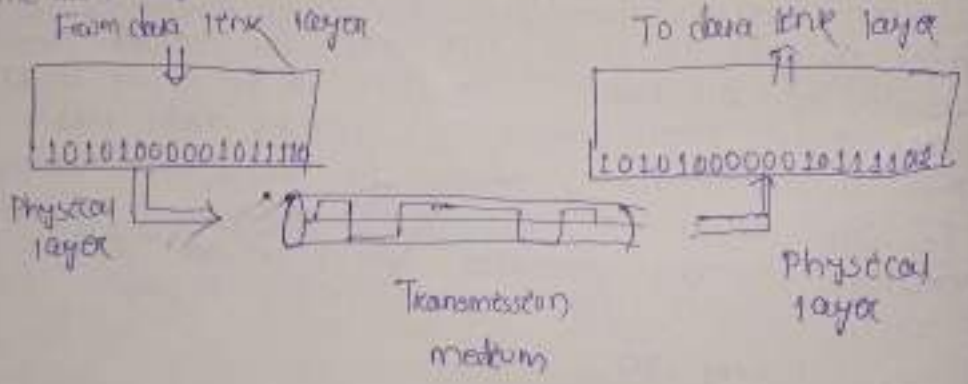
The seven layers are:

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. Data link
7. Physical

Physical layer the physical layer is responsible for transmitting individual bits from one node to the next:

The Physical layer is the lowest layer of the OSI hierarchy and coordinates the functions required to transmit a bit stream over a physical medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission over.

The physical layer specifies the type of transmission medium and the transmission mode (simplex, half duplex, full duplex) and the physical, electrical, functional and procedural standards for accessing data communication network. transmission media depending defined by the physical layer include metallic cable, optical fibre cable or wireless radio-wave propagation. The physical layer also encodes the correct signal used to propagate the data signals between nodes in the network.



Data-Link layer the data link layer is responsible for transmitting frames one nodes to the next:

The data link layer enforces the physical layer, a raw transmission facility, to a reliable link and is responsible for node to node delivery. It makes the physical layers appears error free to the upper layer (network layers). The data link layer packages data from the physical layer into group coded blocks,

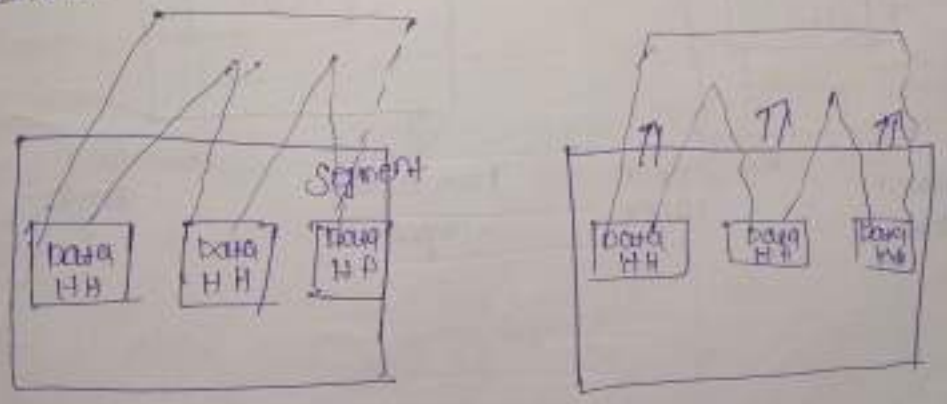
Frames as Packets. If Frame are to be distributed to different systems, on the networks, the data link layer adds a header to the Frame to define the Physical address to of the sender (Source address) and / or receiver (destination address) of the Frame. The data link layer provides flow control, access control and error control.

Network layer is responsible for the delivery of individual packets from the source host to the destination host:-

The network layer provides device that enables data to be routed between devices on an environment using multiple network, subnetwork or both. This is responsible for addressing message and data so they are sent to correct destination, and for translating logical addressing and names (like a machine name FLAME into Physical address) this layer is also responsible for finding a path through the network to the destination computer.

Transport layer is responsible for delivery of a message from one process to another:-

The transport layer controls and ensure the end to end integrity of the data message propagated through the network between two devices, providing the reliable, transport transfer of data between two end points.



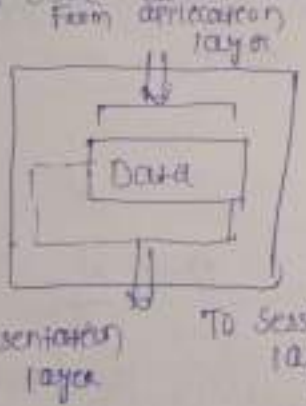
Transport layer responsibilities includes message reading, segmenting, error recovery and two type of basic services to an other layers network connection oriented and connectionless

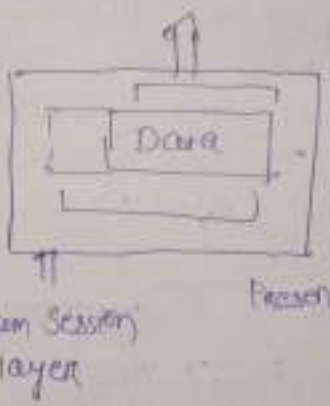
Session layer (responsible for dialog control and synchronization)

Session layer, some time called the dialog controller provides mechanism for controlling the dialogue between the two end system. It defines how to start, control and end conversations (called sessions) between applications, and end connections. Session layer protocols provide the required connections entities at the application layer.

Presentation layer (responsible for translation, compression and encryption) :-

The presentation layer provides independence to the application process by addressing any code or syntax conversion necessary to present the data to the network in a common communication format. It specifies how end user applications should format the data.





The presentation layer translated between different data formats and protocols presentation function include data file formatting, encoding, encryption

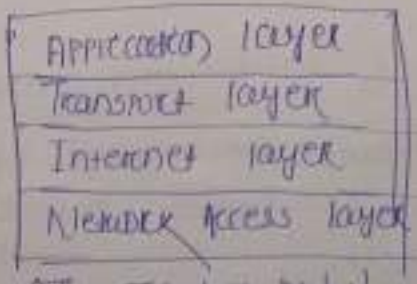
and decryption of data messages: dialogue procedures, data compression algorithms, synchronization, interruption and termination.

Application layer (responsible for providing service to the users):

The application layer is the highest layer on the hierarchy and is analogous to the general manager of the network by provides access to the OSI environment. The application layer provides distributed information access and control and the sequence of activities within and application and also the sequence of events between the computers application and the user of another application.

1. Physical layer: Transmits, raw bit stream over the physical medium.
2. Data link layer: Defines the format of data on the network.
3. Network layer: Decides which physical path the data will take.
4. Transport layer: Transmits data using transmissions protocols including TCP & UDP.
5. Session layer: Maintains connections and is responsible for controlling ports and sessions.
6. Presentation layer: Ensure that data is in a usable format and is where data encryption occurs.
7. Application layer: Human computers interaction layer, where application can access the network services.

TCP/IP MODEL



(The TCP/IP model)

TCP/IP reference model has only 4 layers. They are: (i) Network layers
(ii) Internet layers
(iii) Transport layers
(iv) Application layers

Layer-1: Network layers
(i) Lowest layer of the all
(ii) Protocol is used to connect to the host, so that the packets can be sent over it
(iii) Packets from host to host and network to network

Layer-2: Internet layers
(i) Selection of a packet switching network which is based on a connectionless internet work layer is called a internet layer.
(ii) It is the layer which holds the whole architecture together
(iii) It helps the packet to travel independently destination
(iv) Order on which packets are received is different from the way they are sent
(v) IP (Internet Protocols) is used in this layers.
(vi) The various function performed by the internet layer are ① delivery IP packets ② performing routing ③ avoiding congestion.

Layer-3 Transport layer
(i) It decides if data transmission should be on parallel path or single path.
(ii) Functions such as multiplexing, something or splitting on the data is done by transport layer.
(iii) The application can read and write to the transport layer.
(iv) Transport layer adds heads on formation to the data
(v) Transport layer breaks the message (data) into small unit so that they are ~~hurted~~ handled more efficiently by the network layers.

(vi) Transport layer also arrange the packets to be sent, in sequence.

Layer-4: Application layer

The TCP/IP specification described a lot of application that way at the top of the protocol stack. Some of them were talent FTP, SMTP, DNS etc.

(i) TALENT :- It stands for file type management system a remote computer communication protocol which allows connecting to a machines and run application on it.

(ii) FTP (File transfer protocol) :- It is a protocol, that allows file transfers amongst computer users connected over a network. It is a reliable, simple and efficient.

(iii) SMTP (simple mail transfer protocol) :- It is a protocol, which is used to transport electronic mail between a source and destination, directly via a network.

(iv) DNS (Domain name server) :- It resolves an IP address into a textual address for hosts connected over a network.

(v) It allow terminals to carry conversation.

(vi) It defines two end to end protocols : TCP and UDP.

TCP (Transmission control protocol) :

It is a reliable connection oriented protocol which handles byte-stream from source to destination without error and flow control.

UDP (User Datagram protocol)

It is a unreliable connectionless protocol that does not want TCP's sequencing and flow control.

Examples :- One-shot request-reply kind of service.

Merits of TCP/IP Model

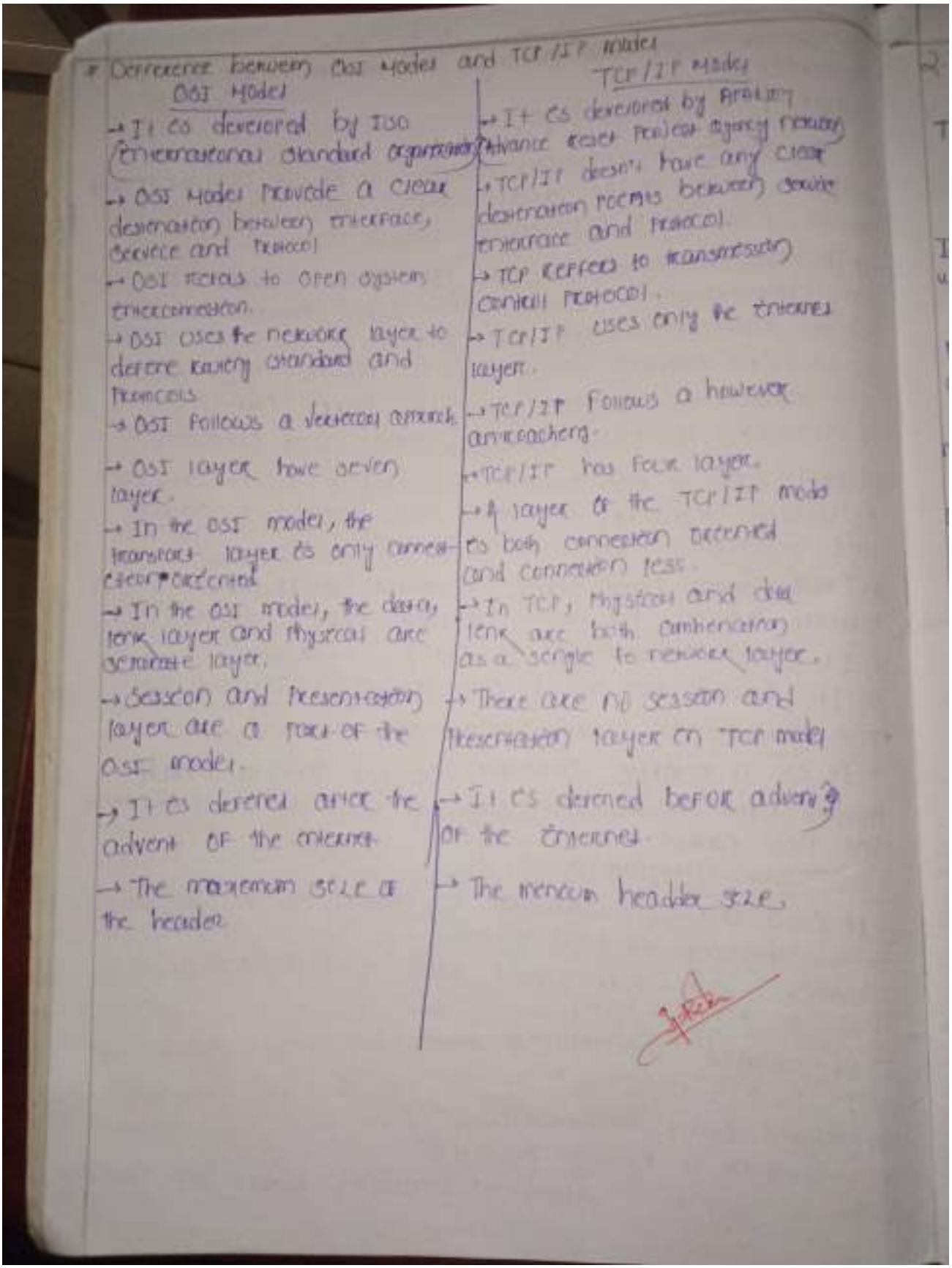
(i) It operational independency.

(ii) It is scalable.

(iii) Client / server architecture.

(iv) Supports no of routing protocols.

(v) Can be used to establish a connection between two computers.



* Difference between OSI Model and TCP/IP Model

OSI Model	TCP/IP Model
→ It is developed by ISO (International Standard Organization)	→ It is developed by Advance Research Project Agency (ARPA)
→ OSI Model provide a clear distinction between interface, service and protocol	→ TCP/IP doesn't have any clear distinction between service interface and protocol.
→ OSI refers to Open System Interconnection.	→ TCP refers to Transmission Control Protocol.
→ OSI uses the network layer to define routing standard and protocols.	→ TCP/IP uses only the internet layer.
→ OSI follows a vertical approach.	→ TCP/IP follows a horizontal approach.
→ OSI layer have seven layer.	→ TCP/IP has four layer.
→ In the OSI model, the transport layer is only connection oriented.	→ A layer of the TCP/IP model is both connection oriented and connection less.
→ In the OSI model, the data link layer and physical are separate layer.	→ In TCP, physical and data link are both combination as a single to network layer.
→ Session and Presentation layer are a part of the OSI model.	→ There are no session and Presentation layer in TCP model
→ It is define after the advent of the internet.	→ It is defined before advent of the internet.
→ The minimum size of the header	→ The minimum header size.

Data Transmission Concept And Terminology

2.1 Data transmission occurs between transmitter and receiver.

Transmission media may be classified as:

(i) guided

(ii) unguided

In both cases, communication is in the form of electromagnetic waves.

Guided media, the waves are guided along a physical path.

Examples of guided media are: twisted pair, coaxial cable, and optical fibre.

Unguided media provide a means for transmitting electromagnetic waves but do not guide them; examples are propagation through air, vacuum and sea water.

(i) Point-to-point:

It provides a direct link between two devices and both these are the only two devices.

(ii) Multipoint:

Guided configuration, more than two devices share the same medium.

Interface from transmission to receive with intermediate devices other than computer or resources use to increase signal strength.

Simplex Mode:

In simplex mode, the communication is unidirectional, as in a one-way street, only one of the two device on a link can transmit the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.

Examples keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

Duplex Mode -
In Full duplex mode, both stations can transmit and receive simultaneously. In Full-duplex mode signals going in one direction share the capacity of the link with signals going in other direction, the sharing can occurs in two ways either the link must contain two physically separate transmission path, one for sending and other for receiving.

OR

The capacity is divided between signals travelling in both directions. Full-duplex mode is used when communication in both direction is required all the time. The capacity of the channel, however must be divided between the two direction.

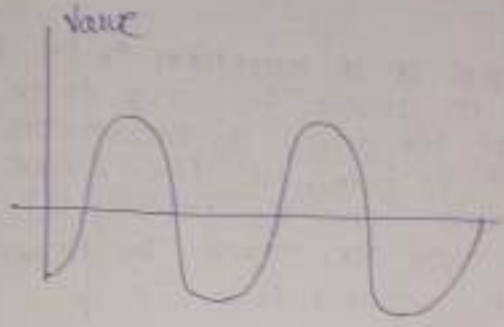
Example: Telephone network in which there is communication between two person by a telephone.

Half-duplex mode -
In half-duplex mode, each station can both transmit and receive, but not at same time. when one device is sending, the other can only receive, and vice versa. The half duplex mode is used in cases where there is no need for communication in both direction at the same time. The entire capacity of the channel can be utilized for each direction.

2.2 SIGNAL :-
Information converted into an electrical form suitable for transmission is called a signal.
There are two type of signal
(i) Analog
(ii) Digital

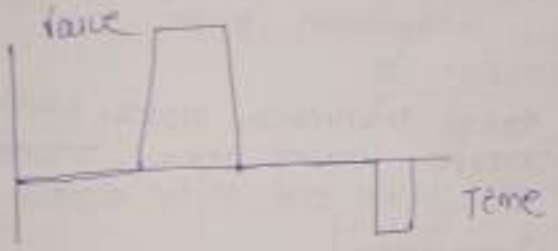
Analog signal -
Analog data refers to information that is continuous.
Examples, an analog clock that has hour, minute and second hands gives information in a continuous form, the movement of the hands are continuous. An analog signal has infinitely many levels of intensity over a period of time, as the wave moves from value

A to B, it passes through and includes an infinite number of values analog is path.



Digital signal -

Digital data refers to information has discrete states. Digital data take on discrete values. For example, data are stored on computer memory in the form of 0's and 1's.



Periodic

A periodic signal completes a pattern within a measurable time frame, called period, and repeats that pattern over subsequent identical periods.

The completion of one one full pattern is called a cycle. Both analog and digital signals can take one of two forms Periodic or nonperiodic.

Non Periodic

Signals non periodic signal changes without exhibiting a pattern or cycle that repeats over time.

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.

Frequency:

The time of one cycle of a waveform is its period, which is measured in seconds. Frequency is the number of cycles completed per second. The measurement unit for frequency (F) is the hertz, Hz. 1 Hz = 1 cycle per second. The measurement unit for frequency (F) is the hertz, Hz. 1 Hz = 1 cycle per second. The frequency of the signal can be calculated from $T = \frac{1}{F}$

Phase (ϕ):

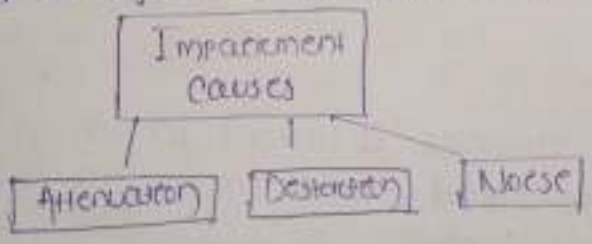
The phase of the signal is measured in degrees or radians with respect to a reference point. A phase shift of 180 degrees corresponds to a shift of half a cycle.

Wavelength:

Wavelength is another characteristics of a signal travelling through a transmission media.

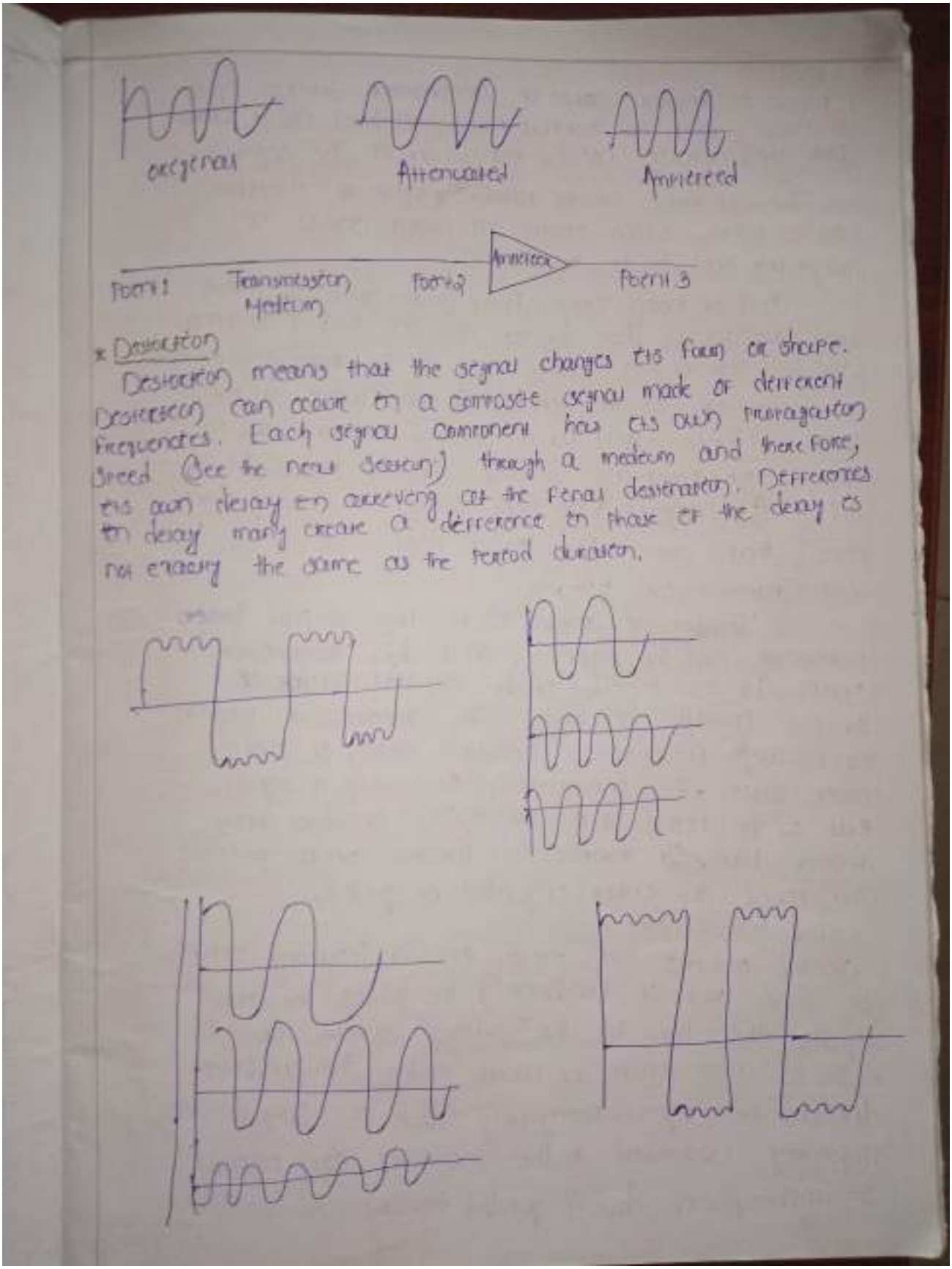
TRANSMISSION IMPAIRMENT

Signals travel through transmission media, which are not perfect. The imperfect causes signals impairment. This means that the signal at the end of the medium.



* Attenuation

Attenuation means loss of energy. When a signal, simple or composite, travels through a medium, it losses 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.



* 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 (see the next section) through a medium and therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

Noise: Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk and impulse noise, may corrupt the signal.

Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

Induced noise comes from sources such as motor and appliances. These devices act as 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.

2.4 Transmission Media

Transmission media is the physical path between transmitter and the receiver, in a data transmission system. It is in inside the physical layer of the OSI Protocol hierarchy. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form. Transmission media can be generally categorized as either unguided or guided.

Guided transmission Media

Guided transmission media uses a "cabling system" (or some sort of conductor) the guides the data signals as are bound by the "cabling" system. Guided media is also known as bound media. The conductor directs the signal propagating down it. Only devices physically connected to the medium can receive signal. Propagation down a guided transmission medium.

* Three Examples of guided transmission media are Twisted pair, coaxial cable and optical fibre.

Unguided transmission media:

Unguided transmission media consists of a means for the data signals to travels but nothing to guide them along a specific path. The data signal are not bound to a cabling media and as such are often called unbound media. Unguided transmission media are wireless system. Signals propagating down an unguided transmission medium are available to anyone who has a device capable of receiving them.

Twisted Pair transmission line

A twisted-pair (TP) transmission lines is formed by twisted two insulated conductors around each other. Usually a number of pairs of these wires are put together into a cable. The cable many contain more than a hundred pairs of wires for long-distances communications. Twisted pair wires are the most common media in a telephone network. These wires support both analog and digital signals and can transmit the signal data at a speed of 10 Mbps over a short distance. The twisting of wires with different twisting lengths reduces the effect of cross talk and low-frequency interference.

Twisted Pair Cable

The two basic types of twisted pair transmission lines discussed are unshielded twisted pair (UTP) & shielded twisted pair (STP).

Unshielded twisted pair UTP cable

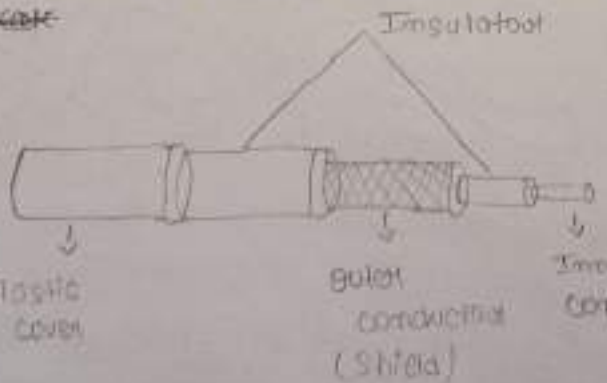
An UTP cable consists of two copper wires where as each wire is separately encapsulated in PVC (Poly Vinyl Chloride) insulation. Bandwidth can be improved by controlling the number of twists per foot & also the manner in which individual pairs are twisted around each other.

Shielded twisted pair (STP) cable

STP cable is a parallel two-wire transmission line consisting of two copper conductors separated by a solid dielectric method. The wires and dielectric are encased in a conductive-material sleeve called foil. If the sleeve is woven into a mesh, it's called braid.

* Physical Description

Coaxial cable, like twisted pair, consists of two conductors but is constructed differently to permit it to operate over a wider range of frequencies. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor. The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield. A single coaxial cable has a diameter of from 0.4 to about 1 in. Because of its shielded concentric construction, coaxial cable is much less susceptible. Coaxial cable can be used over longer distance & supports more stations on a shared line than twisted pair.



Application :-
(i) Television distribution
(ii) Long-distance telephone transmission
(iii) Short-term computer system links
(iv) Local area network

Optical Fibre

* Physical description

An optical fibre is a thin (2 to 125 μm), flexible medium capable of conducting an optical ray. Various glasses & plastics can be used to make optical fibers. The lowest losses have been obtained using fibres of ultra pure fused silica. Ultra pure fibre is difficult to manufacture; higher-loss multicomponent glass fibres are more economical & still provide good performance. Plastic fibre is even less costly and can be used for short-haul links, for which moderately high losses are acceptable.

An optical fibre cable has a cylindrical shape and consists of three concentric sections: the core, the cladding and the core is the inner most section and consists of one or more very thin strands, or fibres, made of plastic, glass or plastic. Each fibre is surrounded by its own cladding, a glass or plastic coating that has optical properties different from those of the core. The outermost layer surrounding one or a bundle of cladded fibers, is the jacket. The jacket is composed of plastic and other materials layered to protect against moisture, abrasion, crushing and other environmental dangers.

Application :-
(i) Long-haul trunks
(ii) Metropolitan trunks

* Radio waves

Radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

* Application:

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, marine radio, cordless phones and paging are examples of multicasting.

* Microwaves:

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional when an antenna transmits microwaves, they can be narrowly focused. This means that the sending & receiving antennas need to be aligned

Application:

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender & the receiver. They are used in cellular phones satellite networks.

* Infrared:

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls

Application :

The infrared band, around 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The infrared data association (IrDA), an association for promoting the use of infrared waves.

UNIT-3 DATA ENCODING

* Data Encoding :-

Encoding is the process of using various patterns of voltage or current levels to represent 1s and 0s of the digital signals on the transmission link. The common types of line encoding are unipolar, polar, Bipolar and Manchester.

* Encoding techniques :-

The data encoding technique is divided into the following types, depending upon the type of data conversion.

(i) Analog data to Analog signals
(ii) Analog data to digital signals
(iii) Digital data to digital signals
(iv) Digital data to Analog signals

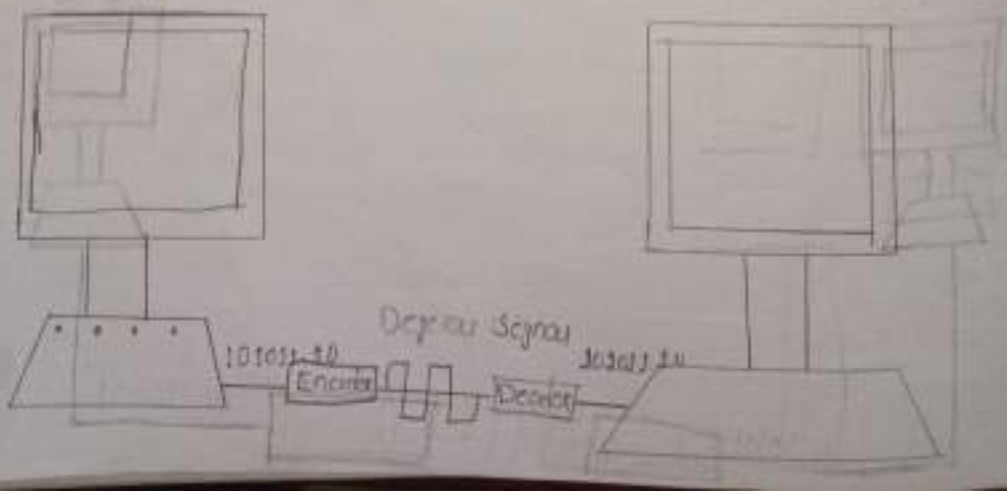
3.2

* Digital-to-digital conversion :-

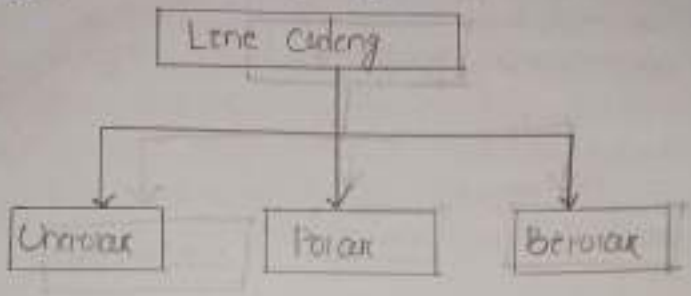
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding & block coding. For all communications, line coding is necessary where as block coding is optional.

→ Line coding

The process for converting digital data into digital signal is said to be line coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

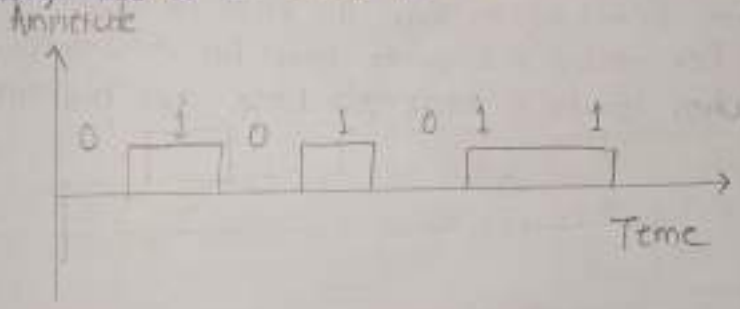


Digital signal is denoted by discrete signal, which represents digital data. There are 3 types of line coding.



(i) Unipolar Encoding :-

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



(ii) Polar Encoding :-

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types. Polar non return to zero (Polar NRZ) it uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative values represents 0. It is also NRZ because there is no rest condition. NRZ scheme has two variants there are : NRZ-L & NRZ-I

NRZ-L changes voltage levels at when a different bit is encountered where as NRZ-I changes voltage when a 1 is encountered.

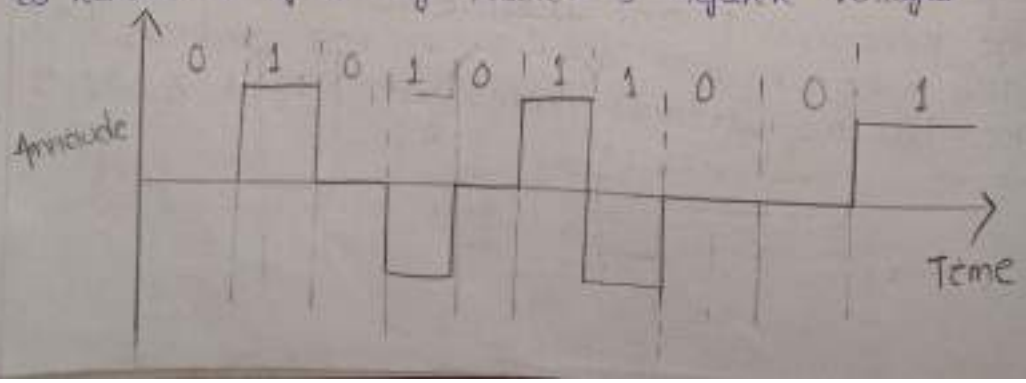
• Return to Zero (RZ) :-

Problem with NRZ is that the receiver cannot conclude when a bit ended & when the next bit is started, in case when sender & receiver's clock are not synchronized

RZ uses 3 voltage levels, positive voltage to represent 1, negative to represent 0 & zero voltage for none. Signal change during bits not between bits.

(iii) Bipolar Encoding

Bipolar encoding uses three voltage levels, +ve, -ve & zero. Zero voltage represents binary zero & bit one is represented by altering positive & negative voltages



• Manchester :-

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

Differential manchester this encoding scheme is a combination of RZ & NRZ-I. It also transists at the middle of the bit but changes phase only when 1 is encountered.

3.3

* Digital-to-Analog Conversion :-

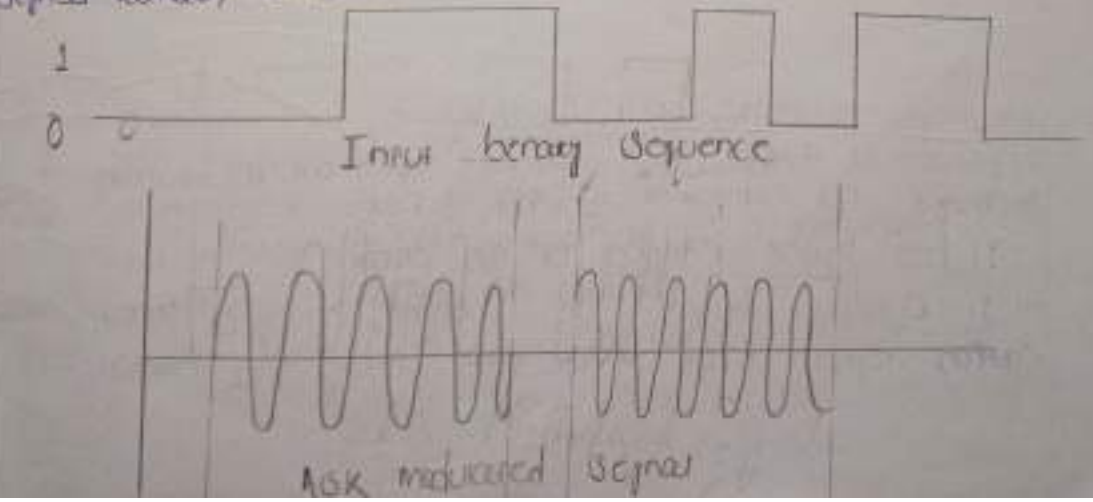
When data from one computer is sent to another via some analog carrier, it is first converted into analog signals.

Analog signals are modified to reflect digital data. An analog signal is characterized by its amplitude, frequency & phase. There are 3 kinds of digital-to-analog conversion.

• Amplitude Shift Keying

Amplitude shift keying is a technique in which carrier signal is analog and data to be modulated is digital. The amplitude of analog carrier signal is modified to reflect binary data.

The binary signal when modulated gives a zero value when the binary data represents zero while gives the carrier output when data is one. The frequency & phase of the carrier signal remain constant.



Advantages of amplitude shift keying

(i) It can be used to transmit digital data over optical fibre.

(ii) The receiver & transmitter have a simple design which also makes it comparatively inexpensive.

(iii) It uses lesser bandwidth as compared to FSK thus it offers high bandwidth efficiency.

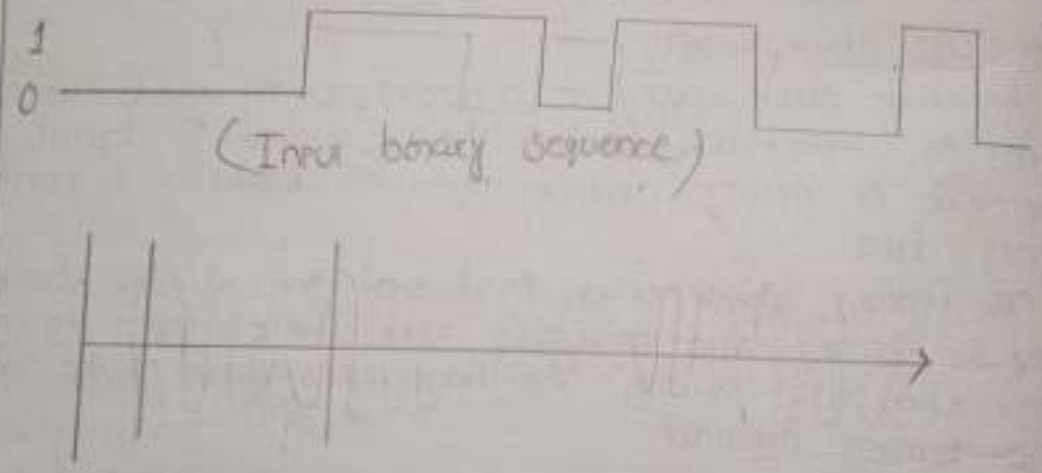
Disadvantages of amplitude shift keying

(i) It uses larger bandwidth as compared to ASK thus it offers less bandwidth efficiency.

(ii) It has lower power efficiency.

• Phase shift keying

In this modulation the phase of the analog carrier signal is modified to reflect binary data. The amplitude & frequency of the carrier signal remain constant.



Advantages of phase shift keying :-

(i) It is a more power different efficient modulation technique as compared to ASK & FSK.

(ii) It has lower chances of an error.

(iii) It allows data to be carried along a communication signal much more efficiently as compared

Disadvantages of Phase Shift Keying:

(i) It offers low bandwidth efficiency.
(ii) The detection & recovery complexities of binary data is very complex.
(iii) It is a non coherent reference signal.

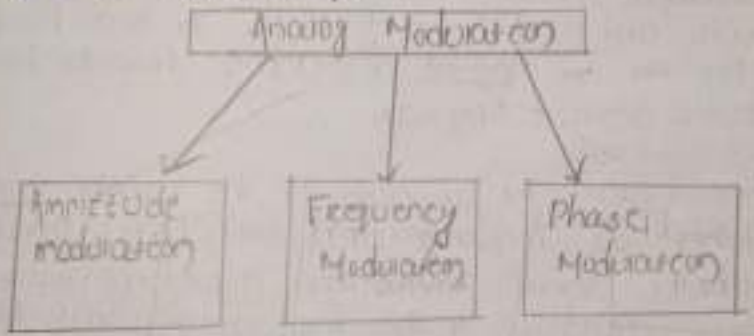
Quadrature Phase Shift Keying:

QPSK carries the phase to represent two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two substreams. The serial data is converted in to parallel in both sub-streams & then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

9.5

• Analog-to-Analog Conversion

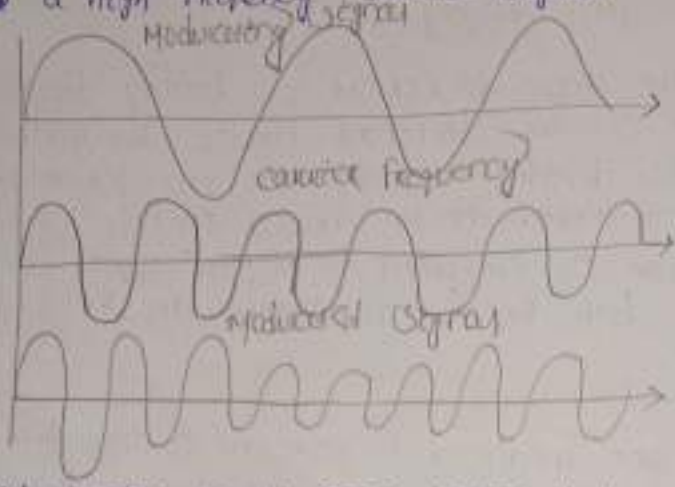
Analog signals are modified to represent analog data. This conversion is also known as analog modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways.



• Amplitude Modulation

In this modulation, the amplitude of the carrier signal is modified to represent the analog data. Amplitude modulation is the process of changing the amplitude of a relatively high frequency carrier signal in proportion to the instantaneous value of the modulating signal (Information). AM modulators are two-input devices, one of them is a single, relatively

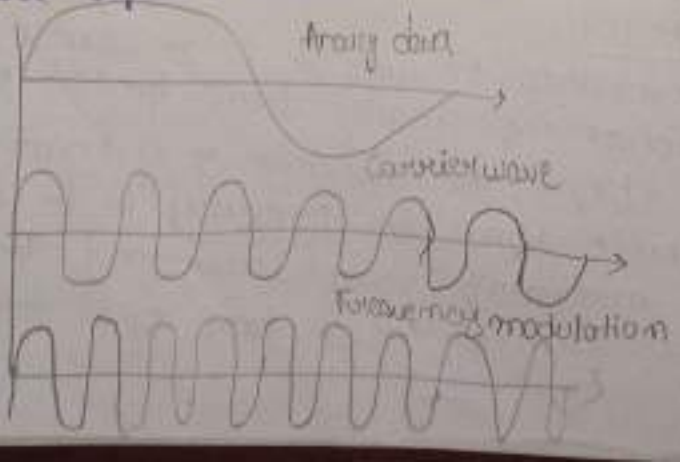
high frequency carrier signal of constant amplitude & the second is the relatively low frequency information signal. The following figure shows generation of AM waveform when a single-frequency modulating signal acts on a high frequency carrier signal.



Advantages of AM are simple to implement, needs a circuit with very few components & inexpensive. The disadvantages include inefficient power usage & use of bandwidth and also prone to noise. The total bandwidth required for AM can be determined from the bandwidth of the audio signal: $B_{AM} = 2B$.

- Frequency Modulation

In this modulation, the amplitude of the carrier signal varies. Whereas as frequency modulation (FM), the frequency of the carrier signal varies in accordance with the instantaneous amplitude of the modulating signal. Hence, in frequency modulation, the amplitude & the phase of the carrier signal remains constant.



The frequency of the modulated wave increases, when the amplitude of the modulating or message signal increases. Similarly, the frequency of the modulated wave decreases, when the amplitude of the modulating signal decreases. Note that, the frequency of the modulated wave remains constant if it is equal to the frequency of the carrier signal, when the amplitude of the modulating signal is zero.

5.4

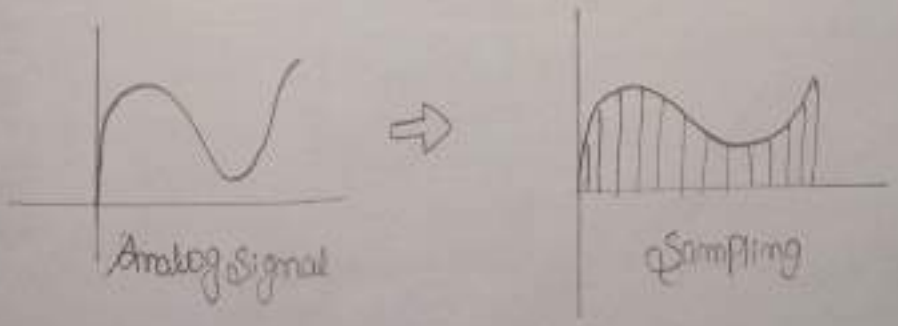
* Analog to digital Conversion :-

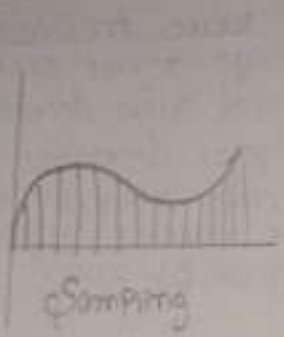
Microphone creates analog voice and camera creates analog video, which are treated as analog data. To transmit this analog data over digital signals, we need analog to digital conversion. Analog data is a continuous stream of data in the wave form where as digital data is discreate. To convert analog wave into digital data, we use pulse code modulation (PCM). PCM is one of the most commonly used method to convert analog data into digital form.

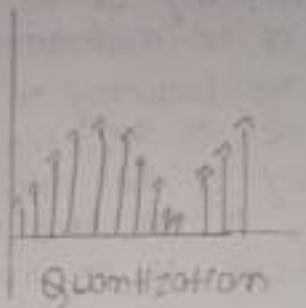
It involves three steps :-

(i) Sampling
(ii) Quantization
(iii) Encoding

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

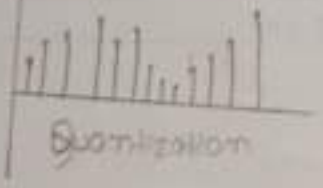


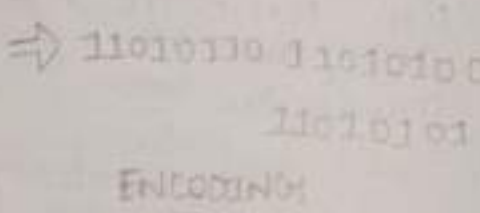




Summery, yields discrete form of continuous analog signal. Every discrete patterns shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value & the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

• Encoding:





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

UNIT-4 DATA COMMUNICATION & DATA LINK CONTROL

Asynchronous and Synchronous Transmission

* Asynchronous Transmission :-

In asynchronous transmission, data is transmitted character by character.

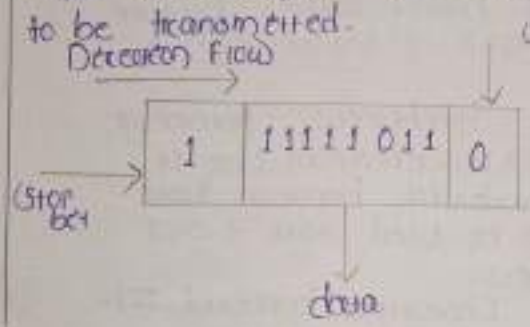
There are irregular gaps between characters in this transmission.

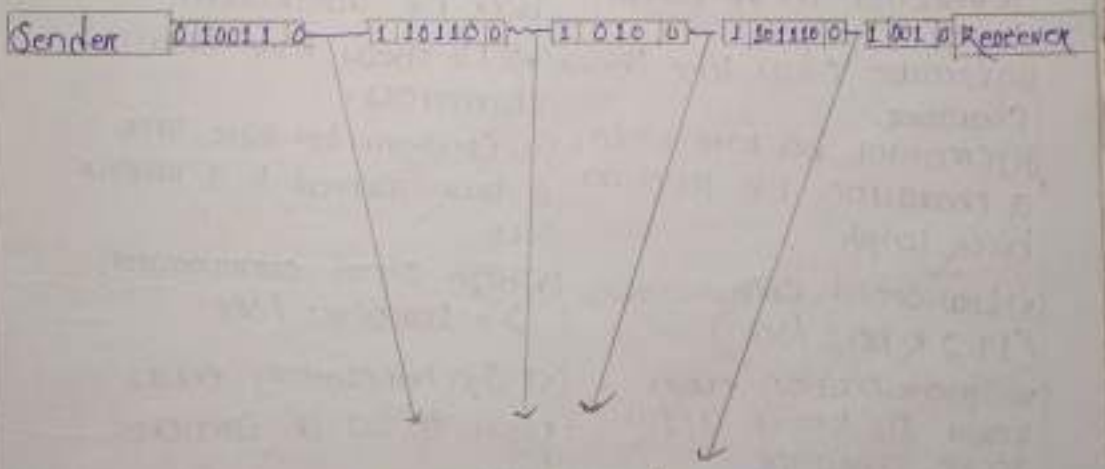
It is cheaper to ~~implement~~ implement because data is not sent before it is sent.

It uses a special start signal.

This signal is transmitted at the beginning of each message.

The start signal is sent, when the character is about to be transmitted.





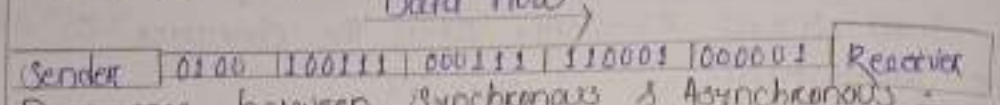
Irregular gaps between data units

* Synchronous Transmission :-

In the synchronous transmission mode, the same data is transmitted by block by block. Each block may consist of many characters. It uses clock to control the timing between data being sent.

A large amount of information can be terms at a single time with this type of transmission.

There are regular gap between sender and receiver.



Difference between Synchronous & Asynchronous :-

Asynchronous Transmission	Synchronous Transmission
(i) Start & stop bits reduce efficiency.	(i) Non-efficient use of bandwidth because there is no used start & stop bits.
(ii) A character can be transmitted on the random times.	(ii) Characters buffered into block for transmission.
(iii) Variable idea time between character.	(iii) No idea time between characters.
(iv) Constant bit rate within a character. No limit on block length.	(iv) Constant bit rate over a block limited to a maximum size.
(v) Low speed communication (19.2 K bits/sec)	(v) High speed communication >= 1 mbites/sec
(vi) Synchronization errors result in loss of only a single character.	(vii) Synchronization errors result in loss of complete block.

* ERROR :-

A station cannot guarantees that the data received by one device are identical to the data transmitted by another. Data can be corrupted during transmission. For reliable communication, error must be detected and corrects are implemented either at the data link layer or transport layer of the OSI model.

- Types of Error :-

Error can be categorized as three types.

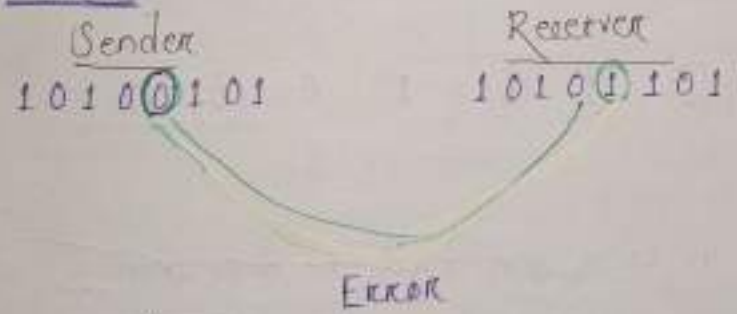
They are; (i) Single bit error
(ii) Parallel bit error
(iii) Burst bit error

(i) Single bit error :-

In a single bit error zero (0) is changes to 1 or 1 changes to zero (0).

Only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1.

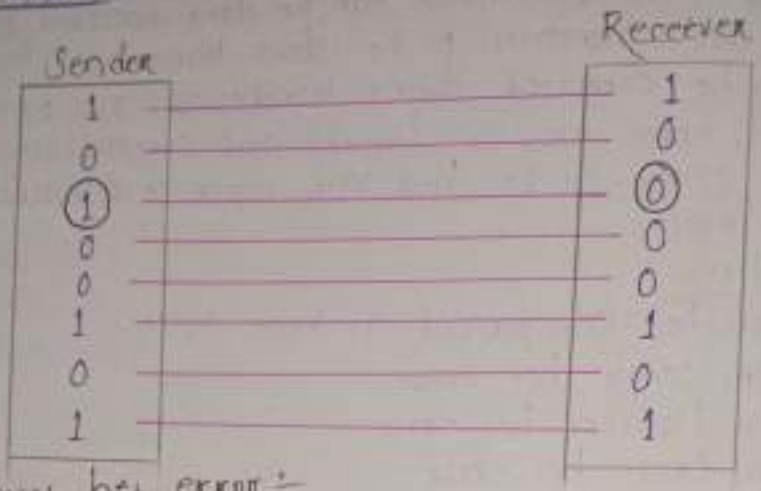
EXAMPLE :-



(ii) Parallel bit error :-

In parallel bit error 0(zero) is changes to 1 or 1 changes to 0 (zero) bit identify by parallely. Only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1.

EXAMPLE :



(iii) Burst bit error :-

Burst bit error means that two or more bits in data unit have changed from 1 to 0 or 0 to 1.

EXAMPLE :

Sender :-

0	1	0	1	1	0	1	0

Receiver :-

0	0	1	0	1	0	0	0

* CHECK SUM :

Step-1 :-

To calculate the check sum divide the data into sections.

Step-2 :-

Add the sections together after number using 1's complement arithmetics.

Step-3 :-

Take the complement of the final sum that is the check sum.

Step-4 :-

After 1's complement of a number that will be added in the parity bit.

EXAMPLE :-

10101001 , 00111001

10101001
00111001

11100010 → 1's complement → 00011101

Receiver

10101001 00111001

00011101

(Sender accepts (Send the data)

* CRC (Cyclic Redundancy check) :-

→ The redundancy bits is used by CRC are derived decoding the data units by error-determined division.

→ The remainder in the CRC.

Data (M(x))
Polynomial - Remainder
Generator(G(x))

EXAMPLE

G(x) - Generated Polynomial - x^4+x^2+1

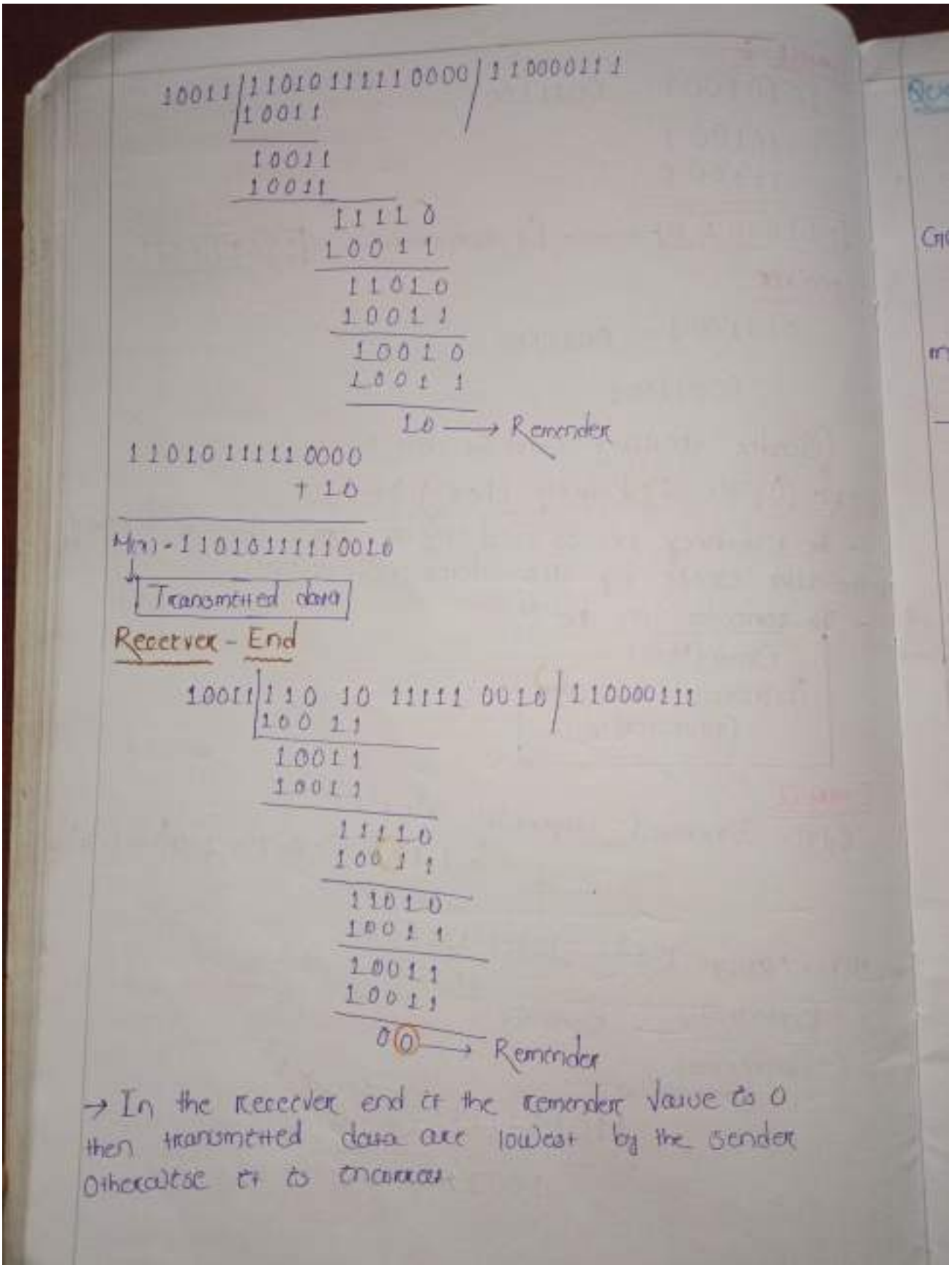
$= 1x^4+0.x^3+0.x^2+1.x^1+1.x^0$

= 10011

M(x) - Message Reader - 11010111111

$$\frac{\text{Data}(M(x))}{\text{Polynomial generated}(G(x))} = \text{Remainder}$$

$$= \frac{11010111110000}{10011}$$


10011 | 11010 11111 0000 | 11000111
10011
10011
10011
1111 0
10011
11010
10011
10010
10011
10 → Remainder
11010 11111 0000
+ 10
M(x) - 11010 11111 0010
Transmitted data
Receiver - End
10011 | 110 10 11111 0010 | 11000111
100 11
10011
10011
1111 0
10011
11010
10011
10011
10011
00 → Remainder
→ In the receiver end if the remainder value is 0 then transmitted data are lowest by the sender otherwise it is incorrect.

Question :-

$G(x) = x^4 + x^3 + x^2 + 1$

$M(x) = 11110001011$

$T(x) = ?$

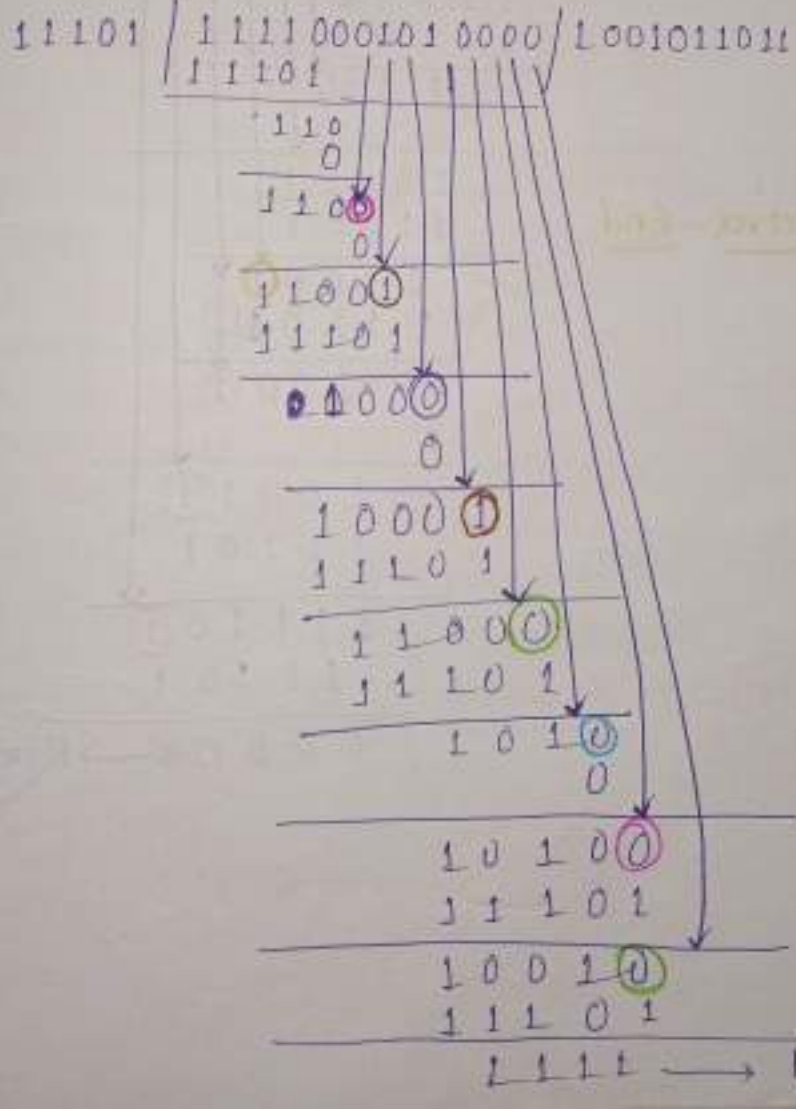
$G(x) = x^4 + x^3 + x^2 + 1$

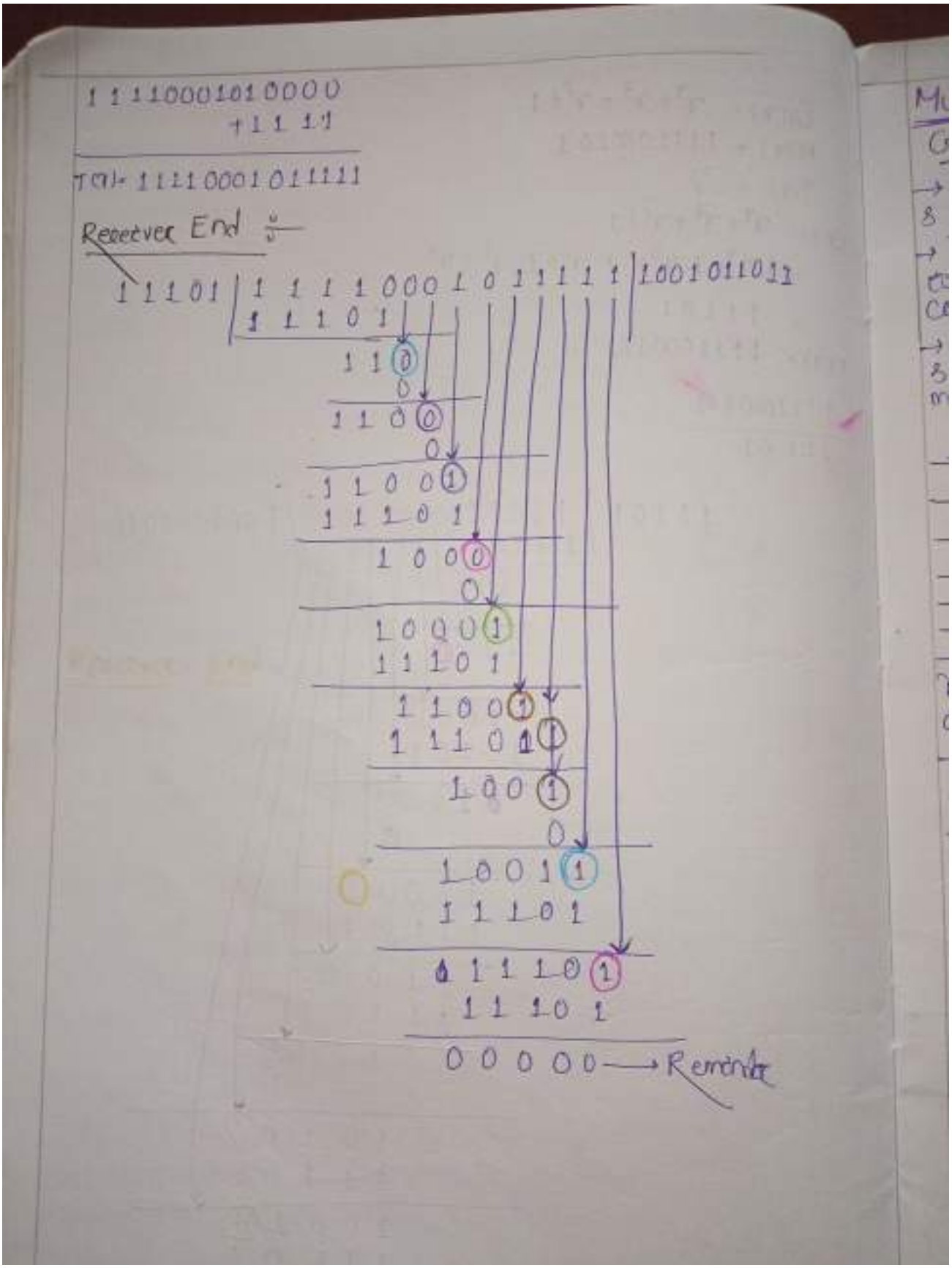
$= 1.x^4 + 1.x^3 + 1.x^2 + 0.x^1 + x^0$

$= 11101$

$m(x) = 11110001011$

11110001011
11101




1 1 1 1 0 0 0 1 0 1 0 0 0 0
+ 1 1 1 1
T(x) = 1 1 1 1 0 0 0 1 0 1 1 1 1 1
Receiver End :-
1 1 1 0 1 | 1 1 1 1 0 0 0 1 0 1 1 1 1 1 | 1 0 0 1 0 1 1 0 1 1
1 1 1 0 1
1 1 0 0
1 1 0 0
1 1 1 0 1
1 0 0 0
1 0 0 0
1 1 1 0 1
1 1 0 0
1 1 1 0 1
1 0 0 1
1 1 1 0 1
1 1 1 0 1
1 1 1 0 1
0 0 0 0 0 → Remainder

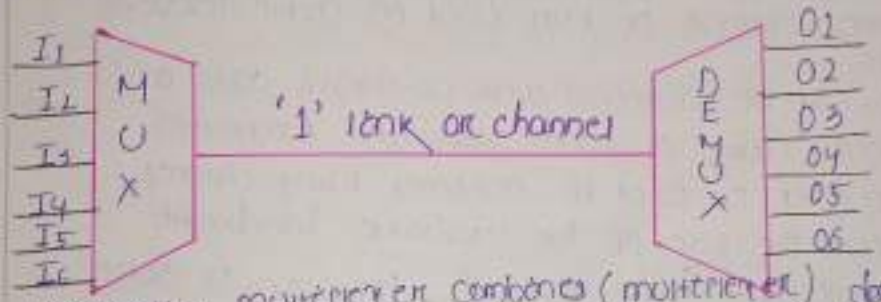
Multiplexing :-

(General definition)

→ Multiplexing is resource sharing over a time between sender & receiver.

→ In the communication and computer networks, multiplexing is a method by which multiple analog or digital signal are combined into one signal over a share medium.

→ A device that perform the multiplexing is called multiplexer (MUX) & a device that perform reverse process that is called de-multiplexer (DEMUX)



→ Basically, multiplexer combines (multiplexer) data from the 'n' input lines & transmission over a single data link (channel or medium).

→ The Demultiplexer separates the data channel, and delivery data to the corresponding output line.

+ Some multiplexing techniques are :-

(i) Frequency division multiplexing (FDM)

(ii) Time division multiplexing (TDM)

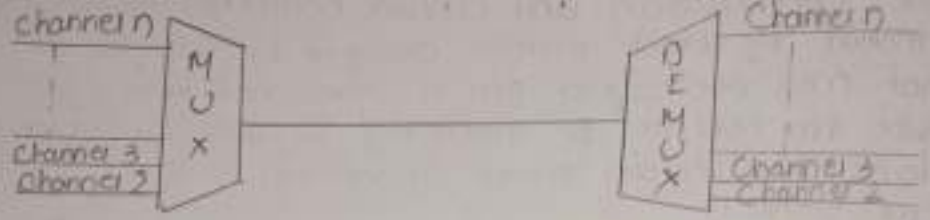
Then TDM is 2 types. They are :-

(i) Synchronous TDM

(ii) Asynchronous & Statistical TDM.

(i) FREQUENCY DIVISION MULTIPLEXING (FDM):-

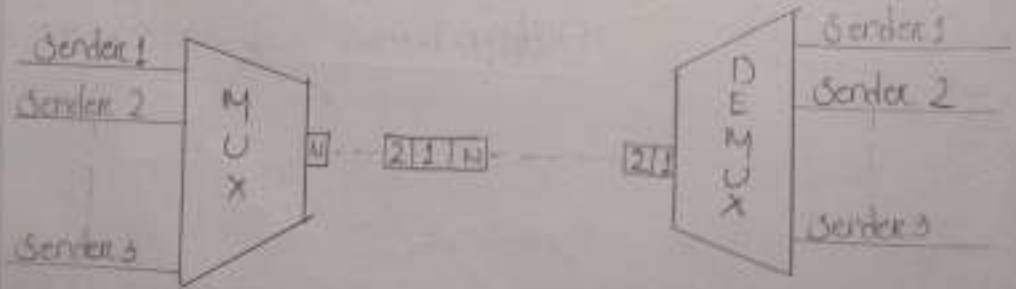
→ It can be used with the analog signal.
→ A number of signals are combined simultaneous on the same medium.



→ A common example of FDM used in cable television, radio etc.
→ And this can be achieved with co-axial cable and fibre optical cable or radio wave and microwaves.
→ A multiplexer is used to combines many channel to maximize the use of the available bandwidth and de-multiplexed back into the television or other, book will allocate the channel that the receiver wants to watch.

(ii) TIME DIVISION MULTIPLEXING (TDM):-

→ It usually used with digital signal or analog signal carrying digital data as well as analog data.
→ Data from various sources are combined in frame.
→ Each frame consists of a set of time slots.
→ Each source is assigned one or more time slots per frame.



Time devision multiplexer is two types. They are

(a) Synchronous TDM

(b) Asynchronous TDM

(1) Synchronous TDM :-

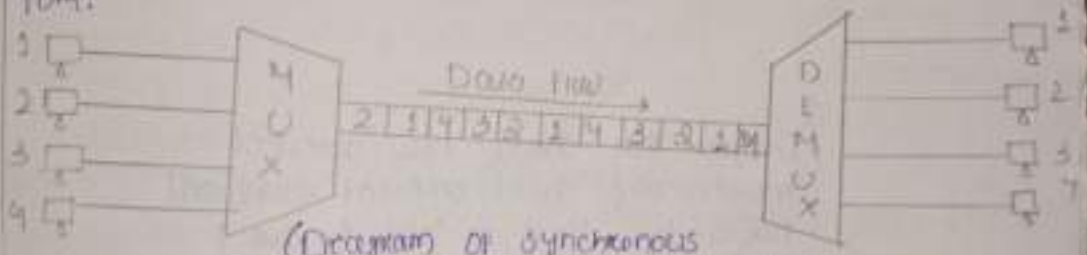
→ TDM is a broad concept that arrises in many forms.

→ It is widely used together through out the internet.

→ Below figure shown items being in round robbing fashion.

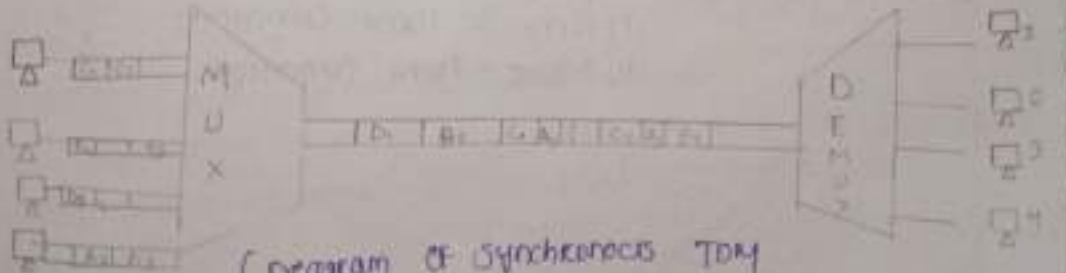
→ Here no gaps occured between bits of a communication system uses a synchronous transmission.

→ When TDM is applied to synchronous networks no gap occurs between items the result is known as synchronous TDM.



(Diagram of synchronous TDM with 4 senders)

→ The problem of synchronous TDM is unfilled slots.



(Diagram of synchronous TDM system leaving slots unfilled when a source doesn't have a data item ready on time)

4.8 (b)

Asynchronous TDM / STATISTICAL TDM :

→ Asynchronous TDM is designed to avoid the wastage in Synchronous TDM.

→ The term asynchronous means flexible but not fixed here.

→ In asynchronous system if we have n-input lines the frame contains a fixed number of atleast n-times slots.

→ One techniques to increase the overall data rate is known as statistical TDM or asynchronous TDM.

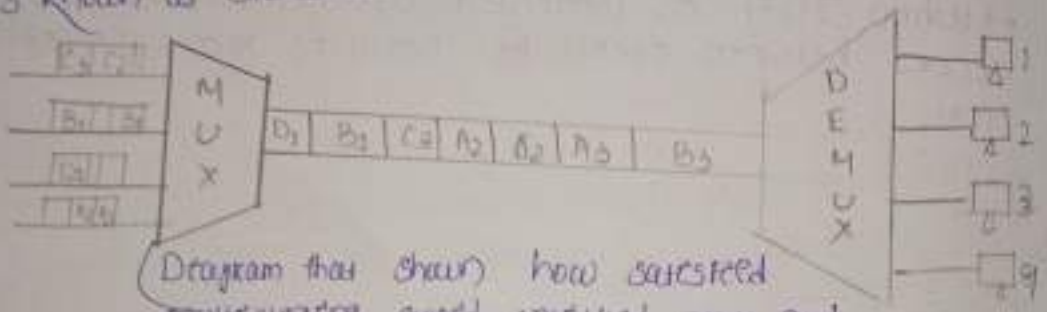


Diagram that shows how statistical multiplexing avoid unfilled slots and takes less time to send the data)

4.8

Line configuration :-

→ A network is nothing but a connection made through connection link and between two or more devices.

→ Device can be computer, printer or any devices that is capable to send and receive data.

→ There are two way to connect the devices

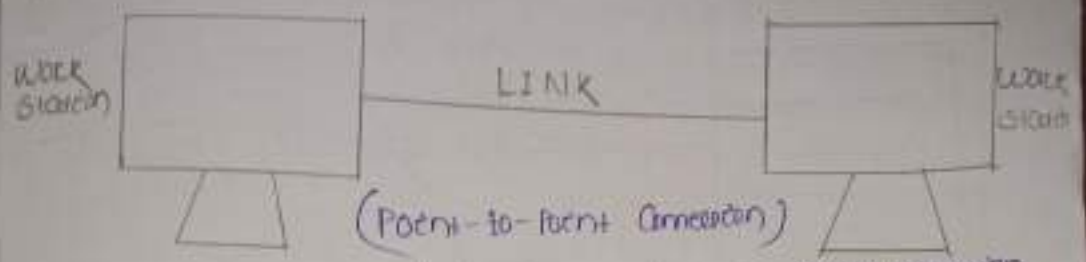
(i) Point-to-Point connection

(ii) Multi-Point connection

(i)

(ii)

(i) POINT-TO-POINT CONNECTION :-



(Point-to-Point Connection)

→ It is a protocol which is used as a communication link between two devices and it is simple to establish.

→ The common example for point-to-point connection is a computer connected by telephone line. We can connect the two devices by means of pairs of wires or using microwave or satellite link.

Example :-

Point-to-Point connection between remote control and television for changing the channel.

(ii) MULTI-POINT CONNECTION :-

→ It is also called multi-drop configuration. In this connection more than two devices and one link.

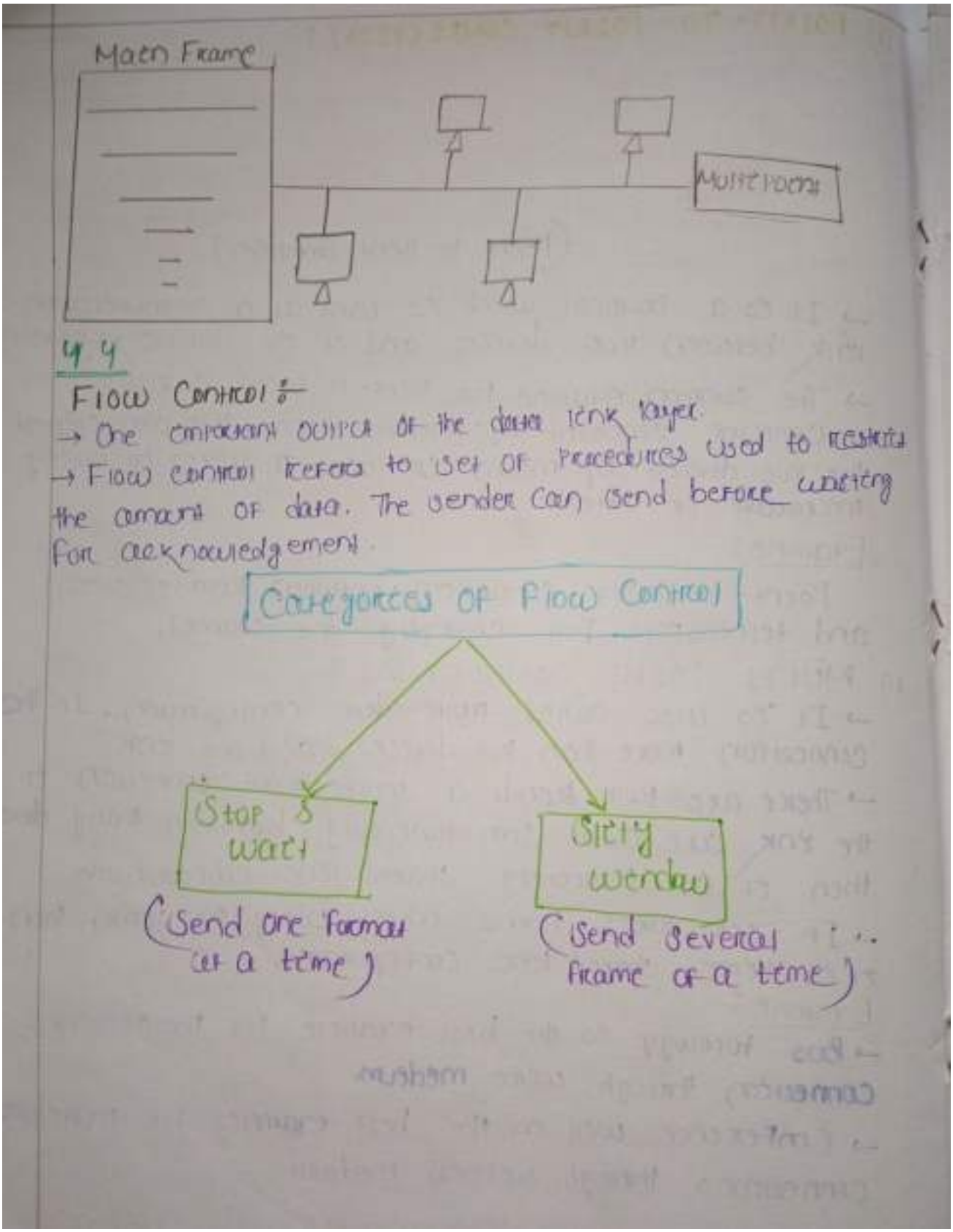
→ There are two kinds of multi-point connection if the link are used simultaneously between many devices then it is Geographically shared line configuration.

→ If user takes turns which using the link, then it is time shared line configuration.

Example :-

→ Bus topology is the best example for multipoint connection through wire medium.

→ Conference call is the best examples for multipoint connections through wireless medium.


Main Frame
Multiplexer
4 4
Flow Control :-
→ One important aspect of the data link layer.
→ Flow control refers to set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgement.
Categories of Flow Control
Stop & wait
(Send one frame at a time)
Sliding window
(Send several frame at a time)

UNIT-5 SWITCHING & ROUTING

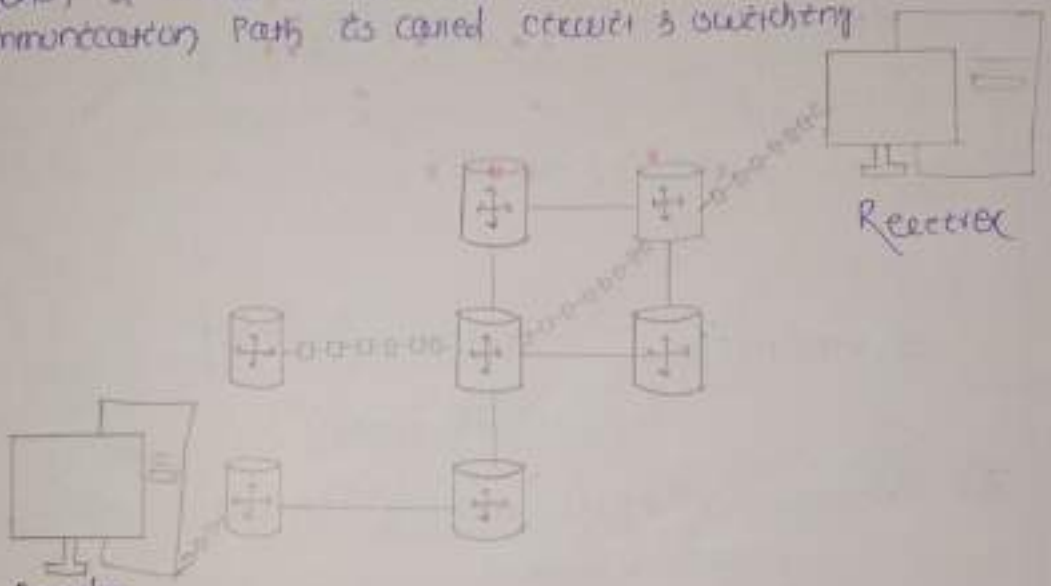
→ Switching is a method for establishing a path for point to point communication in a network.

→ Two basic methods of switching
(1) Circuit switching
(2) Packet switching

5.1

CIRCUIT SWITCHING NETWORK :-

→ When 2 nodes communicate with each other over a dedicated communication path is called circuit switching

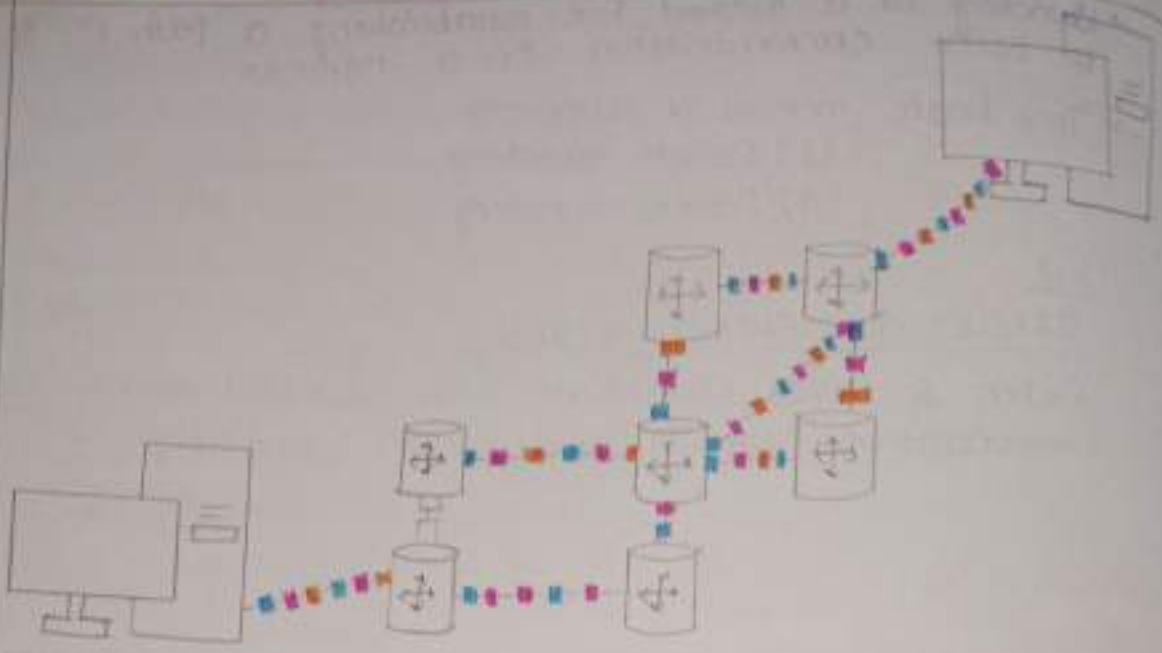


(i) Establish of circuit
(ii) Transfer of data
(iii) Disconnect the circuit

5.2

PACKET SWITCHING :-

→ In this method of switching the entire message is broken down into smaller packets. The switching information is added in the header of each packet and transmitted independently.



2 Variation
- Virtual Switching
- Data gram

Two variation of packet switching exists
(i) Virtual Switching
(ii) Data gram.

DI - 20.05.2022

(1) VIRTUAL SWITCHING

→ The virtual ckt method (also known as connection oriented) is closer to ckt switching

→ Here a complete route is worked out prior to sending data packets. The route is established by sending a connection request along the route to the intended destination.

→ This packet informs the intermediate nodes about the connection and then established route so that they will know how to route subsequent packets

→ The result is a circuit more what similar to these of circuit switching except that it uses packets as its basic unit of communication. Hence it is called a virtual ckt.

(a) DATA GRAM :-

→ The data gram method (also known as connectionless) doesn't relay on a pre-established route instead each packet treated independently. Therefore it is possible for different route its in the network to reach the same and final destination.

→ In a result packets many arrive out of order or even never arrived due to node failure. It is upto the network user to deal the with lost packets and to rearrange packets to their orginal order.

5.3

X.25 :-

→ It is a standard protocol used for packet switching across computer network.

→ X.25 defines node terminals could be interface in the network for communication in packet nodes.

→ Two key terms used as DCE and DTE in X.25.

DCE :- Data communication equipment

DTE :- Data terminal equipment

→ X.25 protocols are used in the physical layer, data link layer, network layer of OSI model.

→ X.25 contains upto less bits of data.

→ It defines how DTE communicate with networks & how packets are came over that network using DCE.

→ It is also known as subscriber network interface protocol (SNI).

5.4

Routing in Packet switching Network :-

→ Routing is a function to determination of path from any source to any destination.

→ The best path depends upon :-

(i) Minimize no of hops
(ii) Minimize end to end delay
(iii) Maximum available of bandwidth

Characteristics :-

→ **Correctness** -

Correct route and accurate delivery of packets

→ **Route** -

Adapting into change of network topology and varying traffic flow.

5.5

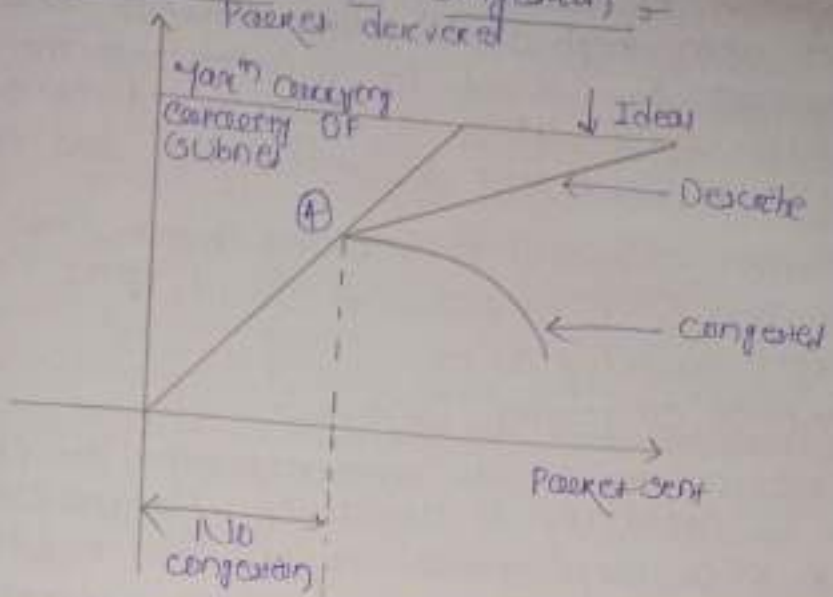
Congestion -

Definition

→ Congestion is synonymis to traffic jams in network when too many packets are present in a part of a subnet the performance degrade This situation is known as congestion.

→ Congestion in a network may occur when the load on the network i.e the number of packets sent to the network is greater than the capacity of the network.

Graphical Representation of Congestion :-



→ Upto point (A) the number of packets sent into the subnet by the host is within its carrying capacity and they all are delivered. In others words the number of packets delivered is proportional to the number of packet sent and no congestion takes place.

→ But after point (A) the traffic increases too far. The routers can't handle the increased traffic and they begin to lost packet the congestion begins here.

→ As the traffic increases further, the performance degrades more and more packets are lost. At very high traffic the performance collapses completely and almost all packets are lost. This is the worst possible congestion.

Cause of Congestion :-

(Some of the causes of congestion may be described as below).

(i) If suddenly a stream of packets start coming from 3 or 4 input lines which all needs the same output line. Then a queue will build up. If the memory capacity is not sufficient to hold all this packets some of them will be lost.

(iii) Congestion is caused by slow links the problems will be solve when high speed links becomes available.

(iv) Congestion is caused by slow processor the problems will be solved when processor speed is improved. Faster processor will transmit more data in unit time.

(v) Congestion is caused if a router doesn't have any free buffers as a result it should ignore new packets arriving as it.

Need of Congestion Control :-

→ It is not possible to completely avoid the congestion but is necessary to avoid it. Congestion will lead to a large queue length which results in loss of packets. Therefore congestion control is necessary to ensure that the user gets the negotiated QoS (Quality of service).

Principle of Congestion Control :-

Definition -

→ To solution the congestion problems can be divided into 2 categories. That is

(a) Open loop solutions
(b) Closed loop solutions

→ Congestion controls refers to the techniques and mechanisms which can either prevent congestion from ~~the~~ happening or remove. Congestion after it has taken place.

→ The open loop congestion control is based on the prevention of congestion whereas the closed loop solution are for remove the congestion.

5.6

Effects of congestion Congestion Control

In this article, let us discuss the open loop congestion control system. These systems try to avoid congestion by using the appropriate policies at different levels. Figure 18.17 depicts various policies corresponding to different layers for avoiding congestion.

(i) **Retransmission Policy :-**

The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion. The transmission policy deals with how fast a sender times out. If a sender times out early then it will transmit all the packets which can lead to congestion. Using retransmission policy, we can avoid this and prevent congestion.

(ii) **Out of order caching policy :-**

If the receiver routinely discard all the packets which are out of order, then retransmission of these packets will take place. This will increase the load and result in congestion.

(iii) **Acknowledgement Policy :-**

If each received packet is acknowledgement immediately then the acknowledgement packets will increase the traffic. If the acknowledgement is delayed (piggybacking) then there is possibility of time out and transmission. Therefore, a right flow control has to be exercised to avoid congestion.

(iv) **Window Policy :-**

The type of window at the sender may also affect congestion. The selective repeat window is better than the go back n policy.

5.7

TRAFFIC MANAGEMENT :-

Traffic shaping -

One of the important reason behind congestion is the bursty nature of the traffic. If the traffic has a uniform data rate than congestion could be less common. Traffic shaping is an open loop control. It manages the congestion by forcing the packet transmission rate to be more predictable. Thus, traffic shaping will regulate the average rate of bursiness of data transmission. Monitoring a traffic flow is called as traffic policing.

The process of monitoring and enforcing the traffic flow is called traffic policing. Penalty will be:

(i) Drop packets that violenate the description

(ii) Give low priority to them.

5.8

(i) Congestion Control in packet switching method :-

This choice at the network layer will affect the congestion because congestion control algorithms work only with virtual circuit subnets.

(ii) Packet queueing and service :-

This policy is related to whether the routers have one queue per input line and one queue per output line or both. The policy is also related to the order in which the packets are processed e.g. round robin or priority based etc.

(iii) Descard policy :-

This policy lays a rule which tells the routers about which packet is to be discarded. A good descard policy can prevent congestion and a bad one will worsen the situation.

(iii) Routing algorithms :-

The routing algorithms can spread the traffic over all the lines to avoid congestion.

(iv) Packet lifetime management :-

The policy decides the time for which a packet may live before being discarded. This time should be of adequate values so that congestion can be avoided.

UNIT-6 LAN TECHNOLOGY

6.1 Topology and transmission media

* **Topology**

Network Topology :-

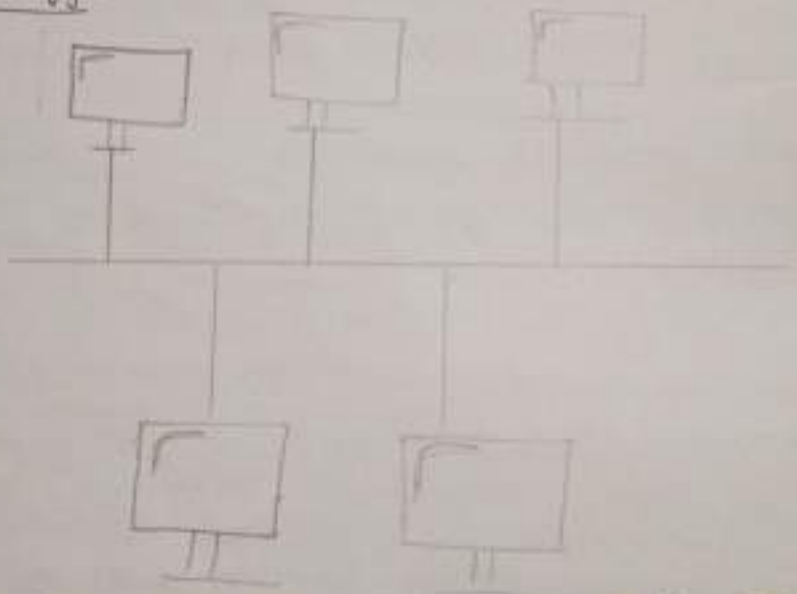
Network topology is the arrangement of the elements of a communication network. Network topology can be used to define or describe the arrangement of various types of telecommunication network.

* **Types of Network topology :-**

Basically topology is 4 types. These are :-

(i) Bus topology
(ii) Mesh topology
(iii) Star topology
(iv) Ring topology

(i) **Bus Topology :-**



→ Bus topology is a specific kind of network topology in which all of the various devices in the network are connected to a single cable or line.

Advantages :-

(i) Easy to connect a computer or peripheral to a linear bus.

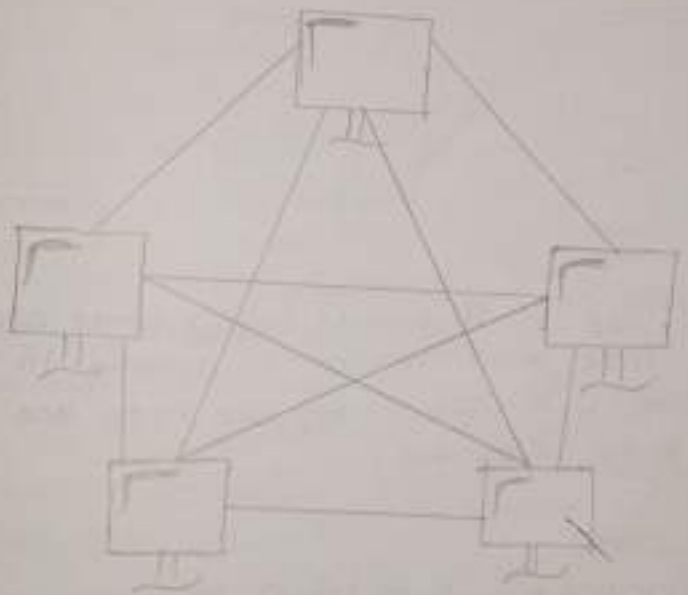
(ii) Requires less cable length than a star topology.

(iii) It is easiest network topology for connecting peripherals or computers in a linear fashion.
(iv) It is easy to connect or remove devices on this network without affecting any other devices.
(v) It is easy to understand topology

Desadvantages :-

(i) Bus topology is not great for large networks.
(ii) This networks topology is very slow as compared to other topology
(iii) Packets loss is high.

(3) Mesh Topology :-



→ Mesh topology is a type of networking where all nodes cooperate to distribute data with each other.

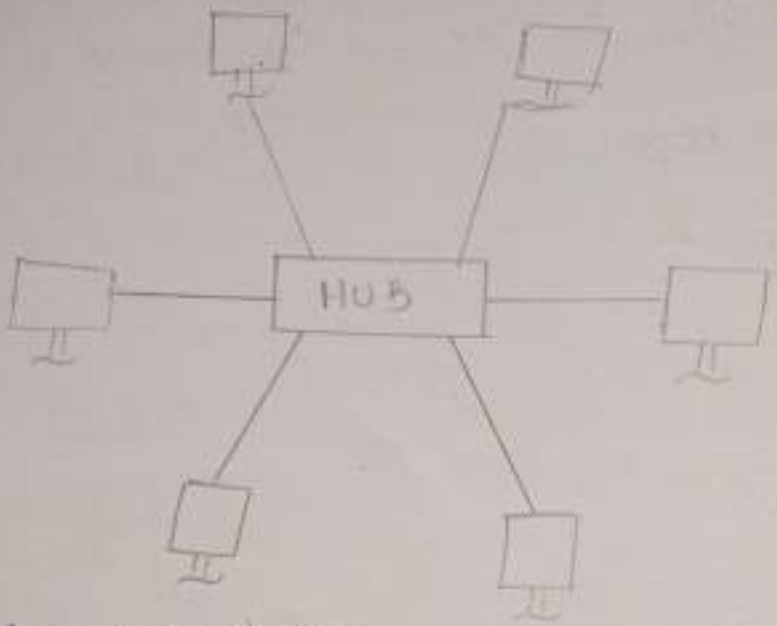
Advantages :-

(i) There is no traffic problem as there are dedicated point to point lines for each computer.
(ii) It has multiple lines so if one route is blocked then other can be accessed for data communication
(iii) It provides high privacy and security.

Desadvantages :-

(i) It requires high number of cables for the communication.
(ii) Installation is very difficult in mesh topology.
(iii) It is costly compared to the opposite network topology.

(iii) STAR ~~BUS~~ Topology :-



→ Star topology in a network topology where each individual piece of a network is attached to a central node (In star topology, the nodes are connected to the central hub).

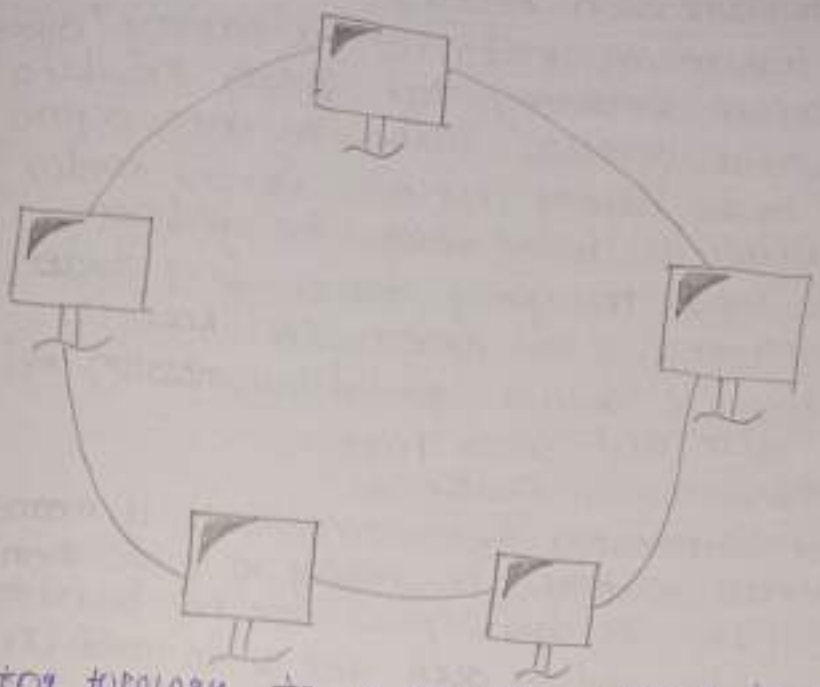
Advantages :-

→ Easy to install.
→ Easy to detect Faults & to remove parts.
→ No disruptions to the network when connecting or removing devices.

Desadvantages :-

→ The set up cost is quite high.
→ Installation is difficult.
→ If a hub or switch fails, all the devices connected to it will have no network connection.

(iv) Ring Topology :-



→ A ring topology is a network topology in which each node connects to exactly two other.

Advantages :-

(i) Easy to manage.
(ii) Equal access to the resources.
(iii) It is easy to install & expand.

Desadvantages :-

(i) It is expensive.
(ii) They were not scalable.
(iii) Total dependance on one one cable.

* Transmission Media :-

Transmission media is the physical path between transmitter and receiver in a data transmission data. transmission system. It is included in the physical layer of the OSI protocol hierarchy. The transmission medium is usually free space, metallic cable, or fibre-optic cable. The information is usually a signal that is the result of a conversion of data from another form. Transmission media can be generally

Categorized as either unguided or guided.

Guided transmission media :-

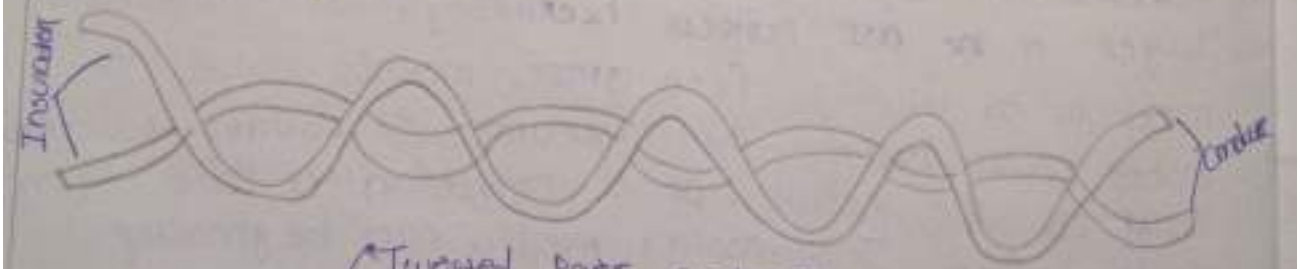
Guided transmission media uses a "cabling" system (or some sort of conductor) that guides the data signals along a specific path. The data signals are bound by the "cabling system". Guided media is also known as bound media. The conductor directs the signal propagating down it. Only devices physically connected to the medium can receive signals propagating down a guided transmission media are copper wire and optical fibre.

Unguided transmission media :-

Unguided transmission media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media and as such are often called unbound media. Unguided transmission media are wireless systems. Signals propagating down an unguided transmission medium are available to anyone who has a device capable of receiving them.

* Twisted pair transmission lines :-

A twisted pair (TP) transmission lines is formed by twisting two insulated conductors around each other. Usually a number of pairs of these wires are put together into a cable. The cable may contain more than a hundred pairs of wires for long-distance communications. Twisted pair wires are the most common media in a telephone network. These wires support both analog & digital signals and can transmit the signal at a speed of 1 Mbps over a short distance. The twisting of wires with different twisting lengths reduces the effect of cross talk & low-frequency interface.



(Twisted pair cable)

The two basic types of twisted pair transmission lines are unshielded twisted pair (UTP) & shielded twisted pair (STP).

Unshielded twisted - pair (UTP) cable :-

A UTP cable consists of two copper wires where each wire is separately encapsulated in PVC (Poly Vinyl Chloride) insulation. Bandwidth can be improved by increasing the number of twists per foot & also the manner in which multiple pairs are twisted around each other.

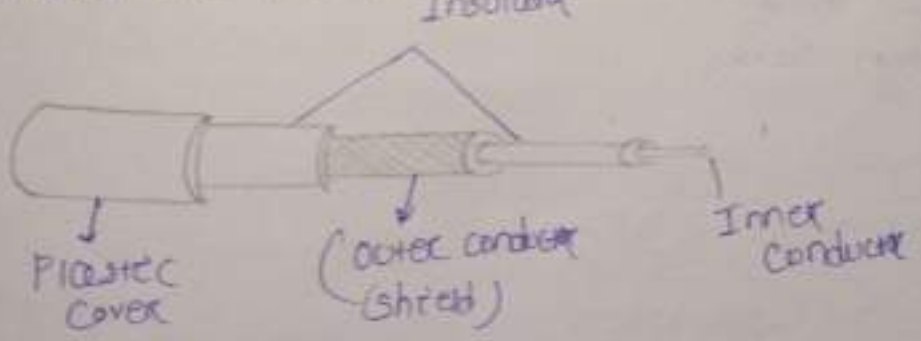
Shielded twisted pair (STP) cable :-

STP cables is a parallel two-wire transmission line consisting of two copper conductors separated by a solid dielectric material. The wires and dielectric are enclosed in a conductive material sleeve called foil. If the sleeve is woven into a mesh it is called braid.

Coaxial cable :-

Physical Description -

Coaxial cable, like twisted pair, consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor. The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield. A single coaxial cable has a diameter of from 0.4 to about 1 in. Because of its shielded, connected construction, coaxial cable is much less susceptible to interference and crosstalk than is twisted pair. Coaxial cable can be used over longer distances & supports more stations on a shared line than twisted pair.



Application
- Television distribution.
- Long-distance telephone transmission.
- Short-run computer system links.
- Local area network.

Optical Fibre :

* Physical Description -

An optical fibre is a thin (2 to 125 μm), flexible medium capable of conducting an optical ray. Various glasses & plastics can be used to make optical fibers. The lowest losses have been obtained using fibers of ultra pure fused silica. Ultra pure fibre is difficult to manufacture; higher loss multicomponent glass fibers are more economical & still provide good performance. Plastic fibre is even less costly and can be used for short-haul links, for which moderately high losses are acceptable.

An optical fibre cable has a cylindrical shape and consists of three concentric section the core, the cladding and the core is the inner most section and consists of one or more very thin strands, or fibre is surrounded by its own cabling a glass or plastic coating that has optical properties different from those of the core. The outermost layer surrounding one or a bundle of cladded fibers, is the jacket. The jacket. The jacket is composed of plastic and other materials layered to protect against moisture, abrasion, crushing and other environment dangers.

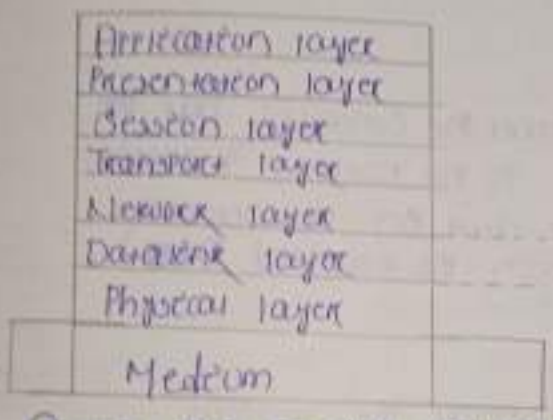
Application
- Long-haul trunks.
- Metropolitan trunks.

LAN protocol architecture :-

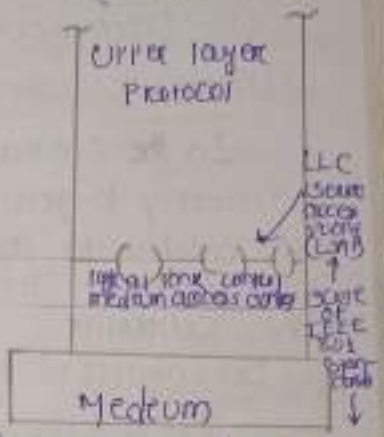
→ LAN protocol architecture :- Lan protocol architectures are created by IEEE 802 reference model - In IEEE 802 reference model, there are two separate layers corresponding to data link layer of OSI model. MAC (medium Access control) layer.

→ LLC (Logical link control) layer.

OSI Reference model



IEEE 802 Reference model



(IEEE 802 protocol layers compared to OSI model)

→ LLC layer :- Provide an interface to higher layer Flow & error control.

→ MAC layer :- Interface to Physical govern access to LAN transmission system sending / receiving frames - Frame synchronization - error detection.

→ Physical layer - Specification of the transmission medium & the topology - encoding / decoding of signals - Preamble generation / removal (for synchronization) - Bit transmission / reception.

6.9

Medium Access Control (MAC) :-

→ The MAC is a protocol which controls the access to the transmission medium for an orderly and efficient use of the transmission capacity of the network.

Such a control can be exercised in two different ways:

(i) Centralized Control

(ii) Decentralized control.

(i) Centralized control :-

In the centralized control the controller has the authority to grant access to the network. A station who wishes to transmit its data on the network has to wait till a permission is received from the controller.

(ii) Decentralized control :-

In a decentralized network the stations collectively performs the medium access control function to determine the order in which the station transmit.

Advantages of centralized control

(i) It can exercise greater control.

(ii) It can use simple access logic at each station.

(iii) It avoids the problems of distributed co-ordination.

Drawbacks of centralized control :-

(i) It creates a single point of failure. If this point fails, then it causes the entire network to fail.

(ii) It may act as a bottleneck to reduce the performance.

The synchronous techniques can be further devided into three categories as follows:

(a) Round Robin

(b) Reservation

(c) Contention

(a) Round Robin :-

With round robin, each station in LAN is given the opportunity to transmit when the turn comes, the stations may transmit or may not. After some time, the opportunity is given to the next station. The control of sequence in which the opportunity is given can be centralized or distributed. Polling is an example of centralized control.

(b) Reservation :-

This technique is suitable for the stream traffic. The total time on medium is divided into slots similar to synchronous TDM. A station that wants to transmit reserve the future slots for extended or even indefinite period.

(c) Contention :-

This techniques is useful for the bursty type traffic. No control is exercised to determine which station should transmit at the given instance of time. All the stations contend for time in a very rough and tumble manner. These techniques are necessary of distributed nature. The advantage is that these techniques are simple to implement and efficient as well.

* BRIDGE :-

A bridge is a layer-2 network connecting devices that is works on the Physical & data link layer of the OSI model. It represents data in the form of 'data Forms'. In the Physical layer, the bridge acts as a repeater which regenerates the weak signals, while in the data link layer, it checks the MAC (Media access control) address of the data forms for it transmission.

A bridge connects the devices which are present in the same network. It is mainly used to segment a network to allow a large network size. It has two type of port incoming and outgoing. It uses the the incoming port to receive the data frames and outgoing port to send the

data frames to other devices. It has two collision domain so there is still a chance of collision & traffic in the data transmission channel.

A bridge has filtering capacity. It means that it can discard the faulty data frames & will allow only the error-less data frames in the networks. Also, it can check the destination MAC address of a frame and decides the port from which the frame should be sent out.

For this, it maintains a table containing the physical (MAC) address of all the devices in the network. Whenever a data frames arrives at the incoming port of the bridge, it first checks the data frame for any kind of errors. If the frame is error-less, it directs the data frame to the specified MAC address (taking instance from the address table) using its outgoing port. It does not change the physical (mac address) of the address during transmission. In other words, a bridge is a repeater with filtering capability.

There are mainly two types of bridge, they are:

(i) Transparent bridge
(ii) Routing Bridge.

(i) Transparent bridge:-

Transparent bridge simply works as a transmission medium between 2 devices. They are actually transparent (they are present but not functionally visible to the devices) to the networking devices.

(ii) Routing bridge:-

Routing bridges have their unique identity, they can be easily identified by the network device. The source station or the sender can send the data packets through specific bridge (using the unique identity of bridges).

Advantages of using a bridge :-

(i) It is not so complex to implement
(ii) The implementation cost is moderate.
(iii) It does not require any processor system administration configuration. We can just plug & play it.
(iv) Improves security by limiting the scope of data frames.
(v) It has the filtering capability.
(vi) It can be used in a large network.

Disadvantages of using a bridge :-

(i) It can connect device of the same network only.
(ii) There is a delay in forwarding the frames due to error checking.
(iii) There is a need to maintain an address table.

* HUB :-

→ Hub is a very simple network connection device. In star / heirarchical topology, a repeater is called Hub. It is also known as multiport repeater device.

→ A hub is a layer-1 device & operates only in the physical network of the OSI model. Since it works in the physical layer, it mainly deals with the data in the form of bits or electrical signals. A Hub is mainly used to create a network & connect devices on the same network only.

→ A hub is not an intelligent device, it forwards the incoming messages to other devices without checking for any address table for connected devices. It only knows that a device is connected to one of its ports.

→ When a data packet arrives at one of the ports of a hub, it simply copies the data to every port. In other words, a hub broadcasts the incoming data packets in the network. Due to this, there are various security issues in the hub. Broadcasting also leads to unnecessary data traffic on the channel.

→ A hub uses a half-duplex mode of communication. It shares the bandwidth of its channel with the connecting devices. It has only one collision domain, so there are more chances of collision & traffic on the channel. A hub is connected in limited network size. If the network size is increased, the speed of the network size is increased, the speed of the network will slow down. Also, a hub can only connect the devices in the same network with the same data rates & format only.

There are mainly two types of hub, they are:-

(i) Active Hub
(ii) Passive Hub

(i) Active HUB :-

An active hub is also known as concentrator. It requires a power supply & can work as a repeater. Thus, it can analyze the data packets & can amplify the transmission signals, if needed.

(ii) Passive Hub :-

A passive hub does not need any power supply to operate. It only provides communication between the networking devices and does not amplify the transmission signals. In other words, it just forwards the data as it is.

Advantages of using a hub :-

(i) It is simple to implement.
(ii) The implementation cost is low.
(iii) It does not require any special administration configuration. We can just plug & play it.

Disadvantages of using a hub :-

(i) It can connect devices of the same network only.
(ii) It uses a half-duplex mode of communication.
(iii) It is less secure, as it broadcasts the data packets.
(iv) It can be used in a limited network size only.

(v) Broadcasting induces unnecessary traffic on the channel.

* SWITCH :-

A switch is a layer-2 network connecting device that is it works on the Physical & data link layer of the OSI model. It interconnects data in the form of data frame. A switch acts as a multiport bridge in the network. It provides the bridging functionality with greater efficiency.

A switch maintains a switch table which has the MAC addresses of all the devices connected to it. It is performed more over the hub, as it reduces any kind of unnecessary traffic in the transmission channel. A switch can connect the devices only in the same network. It uses the full-duplex mode of communication and saves bandwidth. The switch table keeps on updating every few seconds for better processing.

A switch is an intelligent device with filtering capabilities. It can discard the faulty data frames & will allow only the errorless data frames in the network. Also, it will forward the data frames to the specific node based on the MAC address (taken from the switch table). A switch has multiple collision domains, so it has least or no collision in the transmission channel. In fact, every port of switch has a separate collision domain.

When a data frame arrives at the switch, it first checks for any kind of error in the data frame. If the is error-free, it will search of MAC address of the destination in the switch table. If the address is available in the switch table, it will forward the data frame to the specific node, else switch will register the MAC address in the switch table. If the destination address is not specified, it will broadcast the data frame to each node in the network.

A switch can have 8/6/24/48 ports. The data transmission speed is slow in a switch around (10-100 Mbps). Also, it has only one broadcasting domain.

There are mainly four types of switches, they are :-

(i) Store and Forward switch
(ii) Cut-through switch
(iii) Fragment-Free switch
(iv) Adaptive switch

(i) STORE & FORWARD SWITCH :-

It is the most widely and commonly used switch. It does not forward the data frames unless the frames are error-less & completely received in the switch buffer. It is reliable in nature.

(ii) CUT-THROUGH SWITCH :-

Cut through switches have no error checking. Also, it starts sending the data frame to the destination node when it starts receiving it. It is unreliable in nature.

(iii) FRAGMENT SWITCH :-

It is a combination of store and forward, & cut-through switch. It checks only the starting 64 bytes (header information) of the data frame before transmitting the frame.

(iv) ADAPTIVE SWITCH :-

It is the most advanced kind of switch which automatically choose any of the above three switches as per need.

Advantages of using a switch :-

(i) The implementation cost is medium.
(ii) It doesn't require any special system administration configuration. We can just PLUG & PLAY it.
(iii) Improves security by limiting the scope of data frames.
(iv) It has the filtering capability.
(v) It can be used in a large network.
(vi) It uses Full-duplex mode of communication.
(vii) It has multiple collision domains, so there are least or no collision in the channel.

Disadvantages of using a switch :

(i) It can connect devices of the same network only.

(ii) There is a delay in forwarding the frames due to error checking.

(iii) There is a need to maintain a switch table.

UNIT-7 TCP/IP PROTOCOL SUITE

7.1

PROTOCOL SUITE -

- What is protocol?

→ A protocol is set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

- What is a protocol suite?

→ A protocol suite is collection of protocols that are designed to work together.

Protocol stacks :-

It is possible to write a single protocol that takes data from one computer application and sends it to an application on another computer. A single stack protocol.

The problem with this approach is that it very inflexible, as any changes requires changing the entire application and protocol software.

The approach used in networking is to create layered protocol stacks.

Each level of the stack performs a particular function and communicates with the levels above and below it.

This layered arrangement is not confined to networking, and how it works is probably best understood if you compare it to real life example.

Lets take an example of a parcel service between two offices.

The task is simple - Send parcels between people in each office.

We will divide the task into two distinct processes as follows:

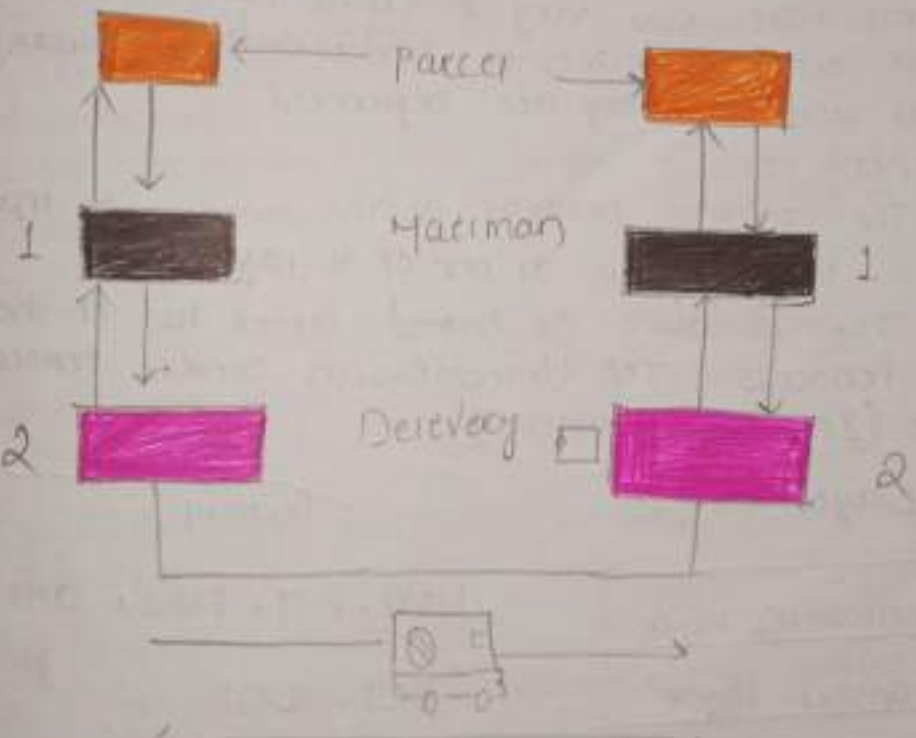
1. Take a package, wrap it and address it.
2. Send it to the destination. At the receiving end

1. Receive the package.
2. Deliver it to the recipient.

Typically you would have an internal mail man that:
1. Collects the parcels from the senders and taken them to a mail dispatch room.
2. The parcels are placed in a van by the dispatcher and then driven to the remote office.

At the remove office

1. The parcels are received by the dispatcher and placed into a tray for the mail man
2. The mail man collects the parcels and delivers them to the recipients, Here is a simple diagram to illustrate the process.



Layered System Example

The question really is what is the advantage of splitting the task into different layers / tasks?

The answer is that any of the layers / tasks can be changed without affecting the other layers.

So, if for example, if we decide to use a train instead of a van to transport the message between the offices we could do so without affecting the mail man.

In fact the mail man doesn't know, and doesn't care, how the parcels are transported between the offices, as all he does is collect them, and pass them to the delivery man.

Although this appears very simple, and maybe trivial, it does illustrate some very important points that are crucial when it comes to understanding networking protocols and how they are organized

The TCP/IP protocol suite

The TCP/IP protocol suite consists of many protocols that operate at one of 4 layers.

The protocol suite is named after two of the most common protocols - TCP (transmission control protocol) and IP (Internet Protocol).

Layer Names	Protocol
Application layer	HTTP, FTP, POP3, SMTP, SNMP
Transport layer	TCP, UDP
Networking layer	IP, ICMP
Datalink layer	Ethernet, ARP

(TCP/IP Networking Model)

TCP/IP was designed to be independent of network hardware and should run across any connection media the earliest use, and the most common uses is over ethernet networks.

Ethernet is a 2 layer protocol / standard covering the physical and data link layer, shown in the diagram above.

IMPORTANT Notes:

HTTP (hypertext transfer protocol) - This is the work-horse of the web.

SMTP, POP3, IMAP4 - These are email protocols.

TCP (transmission control protocol) is a connection oriented protocol and is used to provides a reliable end to end connection.

UDP (User datagram protocol) is connection less protocol and doesn't guarantee delivery. See UDP Vs TCP - what is the difference?

Application will choose which transmission protocol to use based on their function. HTTP, POP3, IMAP4, SMTP and many more use TCP.

UDP is used more on utility applications like DNS, RIP (Routing information protocol), DHCP.

IP (Internet protocol) - This is the main networking protocol. There are two version of IP (IPV4 and IPV6).

ARP (address resolution protocol) - Translates an IP address to a MAC or physical address. (IP4 networks)

Basic Protocol Functions

TCP and UDP Protocols

TCP stands for transmission control protocol. UDP stands for user datagram protocol. Both protocols allow network applications to exchange data between nodes. The main difference between both is that TCP is a connection-oriented protocol while UDP is a connectionless protocol.

When the TCP protocol is used, a stream connection is opened or between two network device, and the channel remains open to transmit data until it is closed. On the other hand, a UDP transmission does not make a proper connection and merely broadcasts its data to the specified network address without any verification or receipt.

IP Control

IP stands for internet protocol. This protocol works with TCP and UDP protocols. It provides a unique identity to each node on the computer network. This identity is known as and IP address. An IP address is a software address of the node on a computer network. There are two versions of IP protocol: IPV4 and IPV6. IPV4 users 32 bits to create an IP address while IPV6 uses 128 bits to create and IP address

DNS

DNS stands for domain name service. This service allows us to access a node by its name. By default, nodes use IP address to identify each other on the network. DNS service allows us to map a name to an IP address. When we access a node by its name, the DNS service translates the name into the IP address.

NAT

NAT stands for network address translation. The protocol translates one IP address to another, this can be a source address or a destination address. Two basic implementations of NAT can be used: static and dynamic. In the static NAT, a manual translation is performed. In the dynamic NAT, an automatic address translation is performed by an address translation device.

SNMP (Simple Network Management Protocol)

Simple network management protocol is a TCP/IP protocol for monitoring networks and network components. SNMP uses small utility programs called agents to monitor behaviour and traffic on the network. These agents can be loaded onto managed devices such as hubs, NIC's, servers, routers and bridges.

SMB (Server Message Block)

SMB is a file-sharing protocol. It allows networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. It is mainly used by microsoft windows-equipped computers. SMB works through a client-server approach, where a client makes specific requests and the server responds accordingly.

FTP (File transfer Protocol)

One of the earliest uses on the internet, long before web browsing came along, was transferring files between computers. The file transfer protocol (FTP) is used to connect to remote computers list shared files and either upload or download files between local and remote computers.

TFTP (Trivial File transfer Protocol)

TFTP is used when a file transfer doesn't require an acknowledgement packet during file transfer, TFTP is used often in the router configuration. TFTP is same service in operation to FTP. TFTP is also known a command-line-based utility

SMTP (Simple mail transfer Protocol)

SMTP is a standard electronic-mail protocol that handles the sending of mail from one SMTP to another SMTP server. To accomplish the transfer, the SMTP server has its MX (mail exchanger) record in the DNS database that corresponds to the domain for which it is configured to receive mail.

HTTP (Hypertext transfer Protocol)

HTTP is often called the protocol of the internet. HTTP received this designation because most internet traffic is based on HTTP. When a user requests a web resource, it is requested using HTTP. The following is a web request.

HTTPS (Hypertext transfer Protocol Secure)

→ HTTPS is for web sites using additional security features such as certificate. HTTPS is used when web transactions are required to be secure. HTTPS uses a certificate based technology such as Verisign