KIIT POLYTECHNIC

LECTURE NOTES

ON

Data Communication & Computer Network

Compiled by

Laxmipriya Samantaray

(Lecturer, Computer Science & Engineering, KIIT Polytechnic, BBSR)

Email: laxmipriyasamantarayfcs@kp.kiit.ac.in

CONTENTS

CHAPTER -1
NETWORK & PROTOCOL

Data communication

- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.
- It includes the transfer of data, the method of transfer and the preservation of data during transfer process.
- To initiate data communication the devices should be collection of both physical equipment's(hardware) and programs(software).

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness.

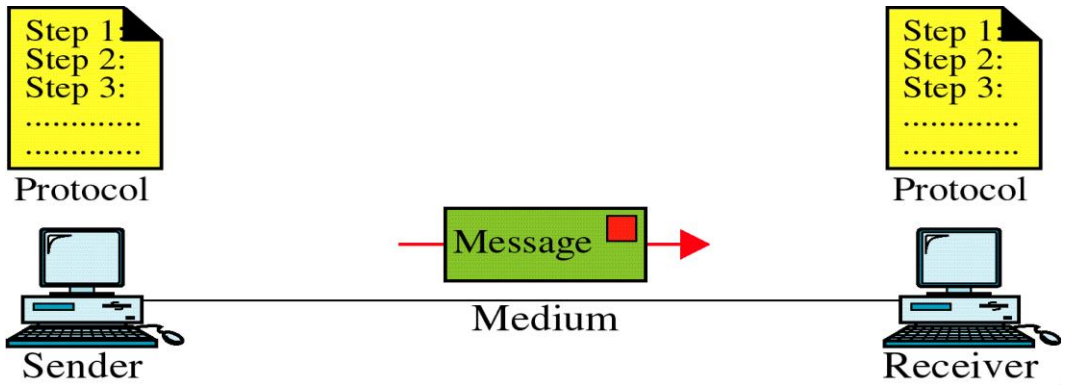
1. Delivery: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

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

3. Timeliness: The system must deliver data in a timely manner. Data delivered late are Useless.

Data Communication System Components

A data communications system has five components.



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

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

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

4.*Transmission medium.* The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

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

Note: The devices generally called as nodes in networking concept.

COMPUTER NETWORKS

A computer 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.

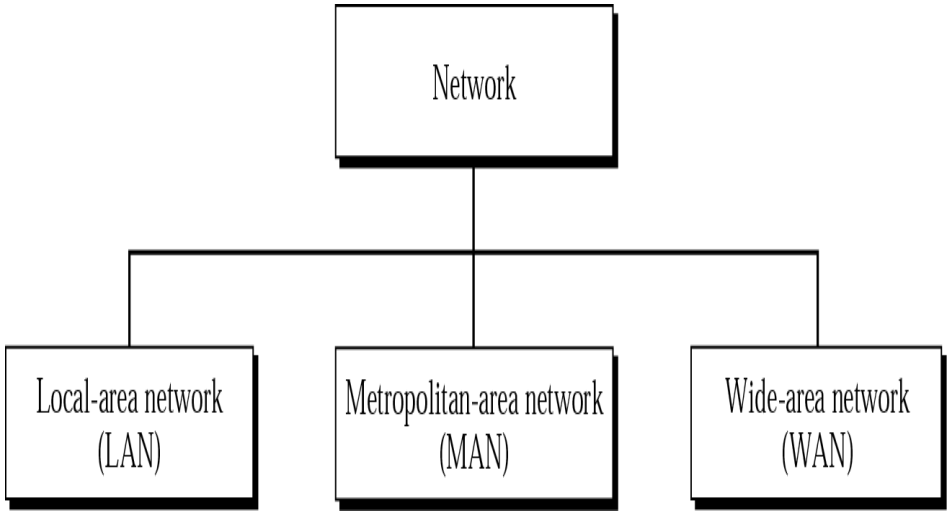
NETWORK CRITERIA

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

1. **Performance:** Performance can be measured in many ways, including Transit and response time.
   - Transit time is the amount of time required for a message to travel from one device to another.
   - Response time is the elapsed time between an inquiry and a response.
   - The performance of a network depends upon number of users, type of transmission medium, capabilities of hardware, efficiency of software.
2. **Reliability:** 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 catastrophe.
3. **Security:** Network security issues include protecting data from unauthorized access, protecting data from damage.

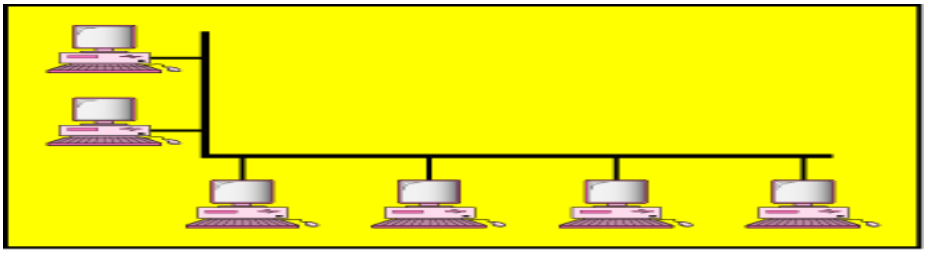
CATEGORIES OF NETWORKS

Network divided in to three primary categories: LAN, MAN, WAN. In to which category a network falls is determined by its Size, Ownership, Distance it covers, and Physical architecture.

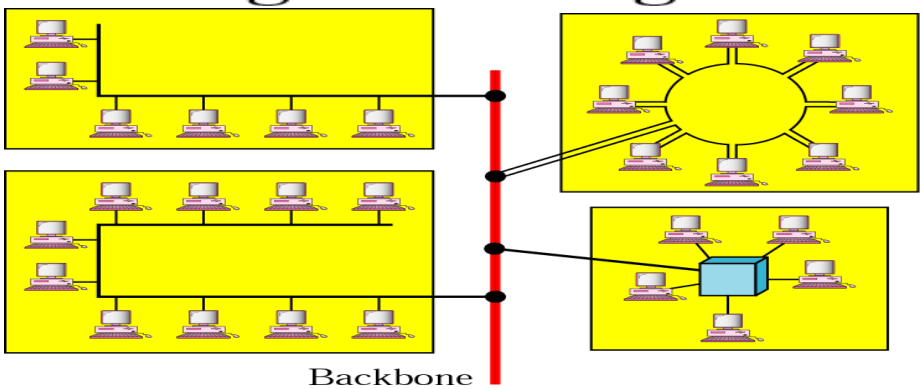


1. LOCAL-AREA NETWORK(LAN) :

- LAN is usually Privately owned and Links devices in single office, building or campus.
- LAN size is Limited to few kilometres.
- LANs are designed to allow resources (i.e. hardware or software) to be shared between PCs and workstations.
- LAN will use a single transmission media.
- The most common LAN Topologies are Ring, bus, star.

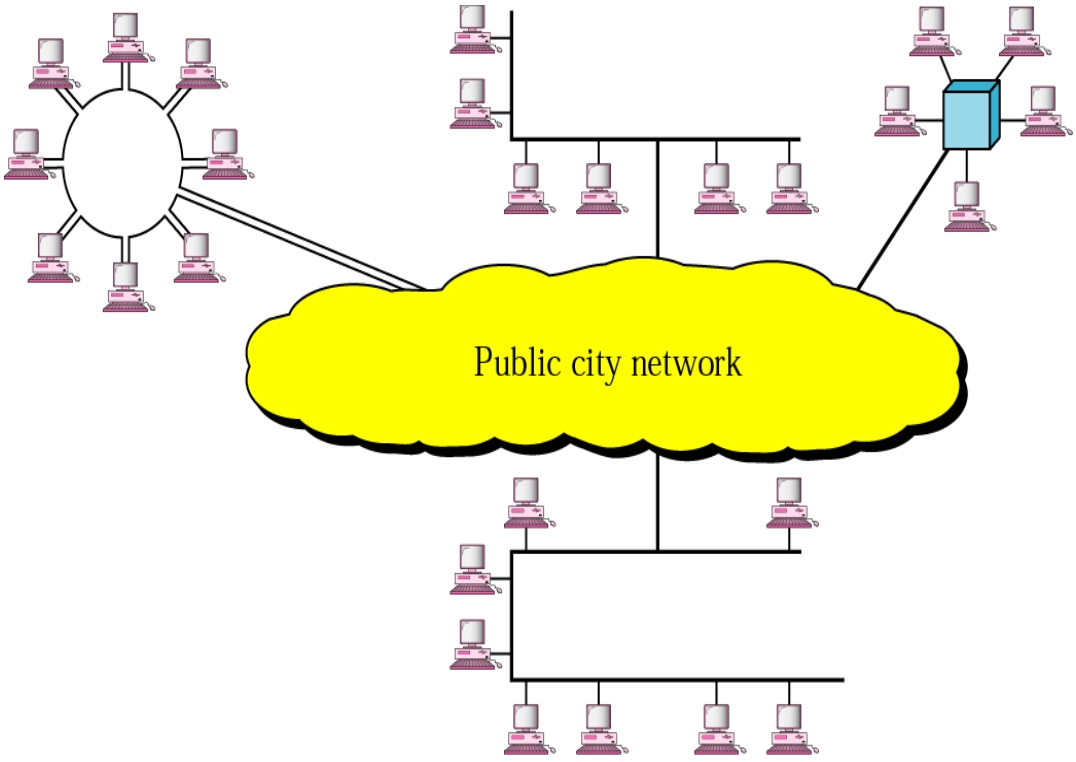


a. Single-building LAN



b. Multiple-building LAN

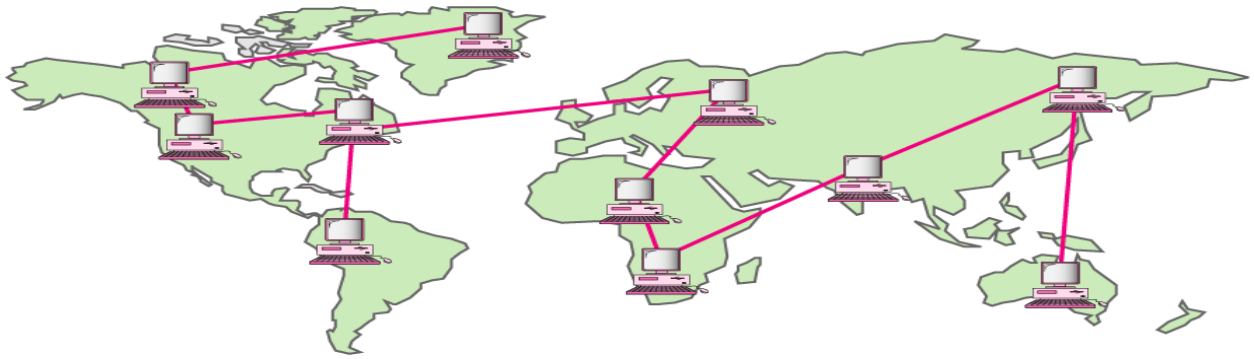
2.METROPOLITAN-AREA NETWORK (MAN):



- A MAN is designed to extend over an entire city.
- It may be single network such as cable television network, or it may be a means of connecting number of LANs in to a larger network.
- A MAN be wholly Owned and operated by a private company, or it may be a Service provider by public company such as a local telephone company.

3.WIDE-AREA NETWORK(WAN):

WAN provides long-transmission of data, voice, image and video information over large geographic areas that may comprise a country, a continent or even the whole world.



WAN that is wholly owned and used by a single company is often referred to as an enterprise network.

Computer Network & Administration: The managing and administrating of group of networks is called CNA

Intranet: A network within itself is called intranet.

Internet:

- Interconnection of two or more networks is called internetworks, or internet.
- Network of networks is also called internet.
- Internet is different from internet (i.e., Internet is the name of a specific worldwide network & internet is the interconnection networks).

Protocol

A network protocol defines rules and conventions for communication between network devices. It defines

- What is communicated
- How it is communicated
- When it is communicated

Key element of Protocol

- Syntax
- Semantics
- Timing

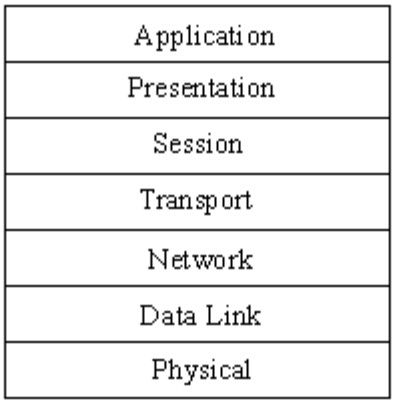
THE OSI MODEL

- An ISO (International Standard Organization) standard that covers all aspects of network communications is the **Open Systems Interconnection model.**
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software standards.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network

- An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

Layered Architecture:

It mainly consists of seven layers: **Physical** (layer 1), **Data link** (layer 2), **Network** (layer 3), **Transport** (layer 4), **Session** (layer 5), **Presentation** (layer 6), and **Application** (layer 7).



The OSI 7-layer Reference Model

LAYERS IN THE OSI MODEL:

1.Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.
- The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- The transmission rate-the number of bits sent each second is also defined by the physical layer.
- The physical layer is concerned with the connection of devices to the media.
- In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

2.Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer.

- **Framing**. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.
- **Error control**. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.
- **Access control**. When two or more devices are connected to the same link, datalink layer protocols are necessary to determine which device has control over the link at any given time.

3.Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

- **Logical addressing.** The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing.** When independent networks or links are connected to create *internet works*(network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

4.Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.

- **Service-point addressing** .The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly**. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **Flow control**. Like the data link layer, the transport layer is responsible for flow control.
- **Error control**. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link.

5.Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller.*

It establishes, maintains, and synchronizes the interaction among communicating systems.

- **Dialog control**. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization**. The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

6. Presentation Layer

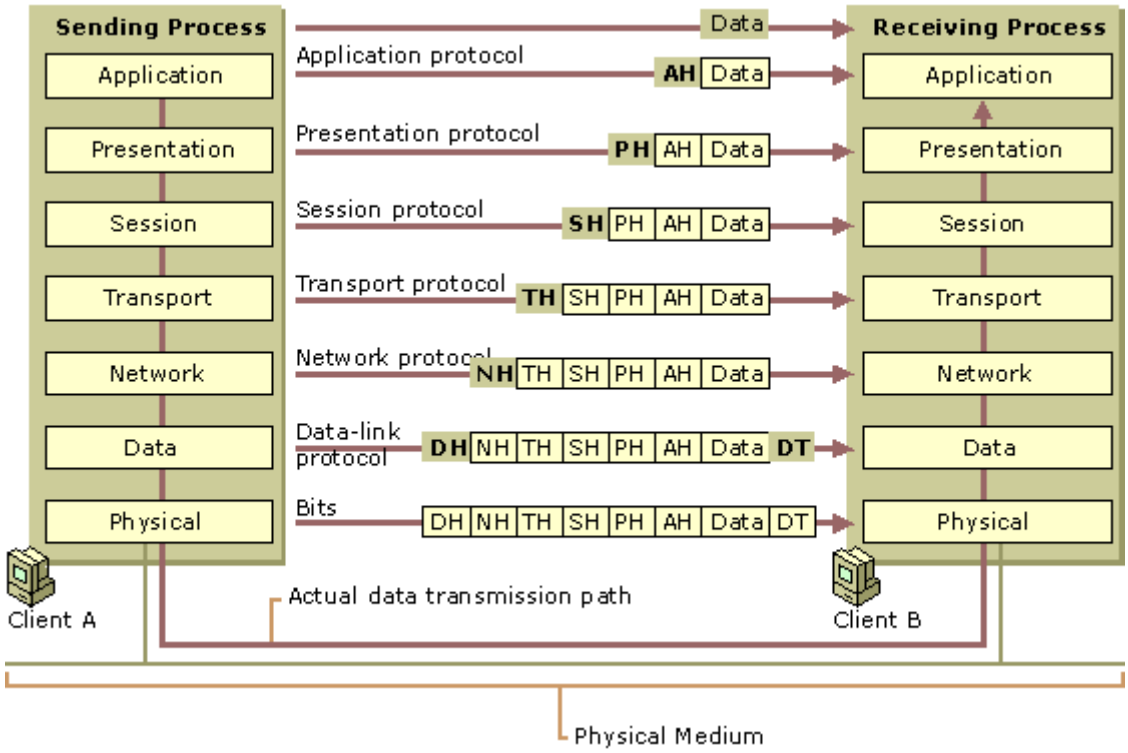
The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

- **Translation:** The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption**. To carry sensitive information, a system must be able to ensureprivacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression**. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

7. Application Layer

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

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



Advantages of Layering :

Standards interfaces between layers allow internal development within a particular layer to evolve.

1. Alternative services may be offers at a given layer by having different option of routes through the layer.
2. Internal mechanism of layers is invisible to other layers.
3. Layers may be completely removed if not required, or simplified version can be used as a substitute where appropriate.
4. It is flexible and robust
5. This allows any two different system to communicate regard less of their underlying architecture.

Interfaces between layers

The processing of data and networks information down through the layers of receiving machines made possible by an interface between each pair of adjacent layers. Each interface defines what information and services a layer must provide for the layer above it.

Peer to Peer Process

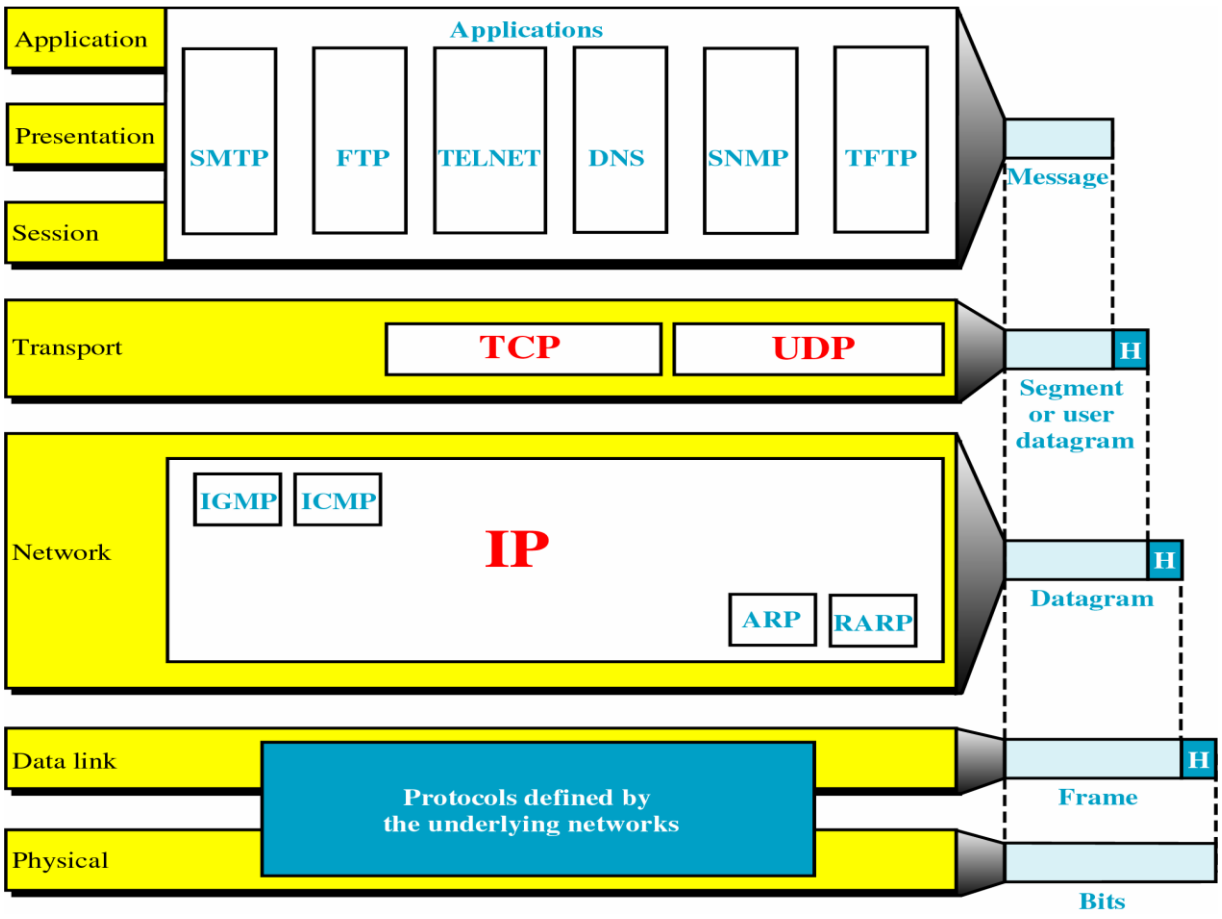
A layer uses the service provided by its upper layer & provides service to the layer to its below. Between machines, the layer x on one machine communicates to layer x on other machine. This communication is possible by protocols. So, the communication process on each machine that communicate at a given layer is called as peer to peer process.

TCP/IP PROTOCOL SUITE

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- It is a set of protocols or a protocol suite that defines how all transmission are exchanged across the internet.
- TCP/IP protocol suite is made of five layers:

1. **Physical**
2. **Datalink**
3. **Network**
4. **Transport**
5. **Application**

- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.
- It is hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- However, the modules are not necessarily interdependent.



DESCRIPTION ABOUT LAYERS:

1.Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2. Network Layer

At the network layer (or, more accurately, the internetwork layer),TCP/IP supports the **Internetworking Protocol, IP**. Also it uses four supporting protocols:

ARP, RARP, ICMP, and IGMP

Internetworking Protocol (IP)

- It is the transmission mechanism used by TCP/IP protocol.
- It is an unreliable and connectionless protocol.
- IP transports data in packets called datagrams.
- Each packet transport separately.

Address Resolution Protocol(ARP)

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.

Reverse Address Resolution Protocol (RARP)

It allows a host to find its internet address when it knows only physical address. It is used when computer connected to n/w first time.

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

Internet Group Message Protocol (IGMP)

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. Transport Layer

- Traditionally the transport layer was represented in *TCP/IP* by two protocols**: TCP and UDP.**
- IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.
- But **UDP and TCP** are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- A new transport layer protocol, **SCTP**, has been devised to meet the needs of some newer applications.

User Datagram Protocol (UDP)

- It is a process-to-process protocol That adds only port addresses, checksum error control and length information to the data from the upper layer.
- It is simple & fast but a unreliable connectionless delivery service.

Transmission Control Protocol (TCP)

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

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet.

4.Application Layer

The *application layer* in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model Many protocols are defined at this layer. They are SMTP, FTP, HTTP, DNS, SNMP, TELNET etc.

SMTP (Simple Mail Transfer Protocol)

It is used to send email from one system to another.

FTP (File Transfer Protocol)

It is used to send an application program(file) to another system. i.e files are transferred from server to client.

HTTP (Hypertext Transfer protocol)

- Used mainly to access data on WWW.
- Used to transfer data in the form of plain text, hypertext, audio, video and so on.

DNS (Domain Name Server or System)

- Provides the protocol that allows clients and server to communicate with each other.
- It allows computer to have names like kp.kiit.edu rather than just IP address like 144.162.120.233.

SNMP (Simple N/W Management Protocol)

It provides a systematic way of monitoring and managing or maintaining an internet or computer n/w.

TELNET (Terminal Network)

- It is a client-server application program.
- Responsible for establishment of a connection to a remote system so that the terminal appears as a local terminal at the remote system.

CHAPTER -2
DATA TRANSMISSION & MEDIA

Data Transmission

The way in which data is transmitted from one place to another is called *data transmission mode*. It is also called the *data communication mode*. It is indicating the direction of flow of information. Sometimes, data transmission modes are also called *directional modes*.

Data transmission can either be analog or digital.

Analog transmission :-

Analog transmission consists of sending information over a physical transmission medium in the form of wave .

Terminology used related to Data Transmission

1. Bit rate:-The bit rate is the number of bits transmitted in one second. it is expressed in the terms of bps.
2. Baud rate:-The number of signals transmitted in 1 second is defined as baud rate/signal rate or pulse rate.

Data rate/bit rate VS **signal rate/baud rate**: -

S = N *1/R baud

were,

N=data rate

S=signal rate

R=$\log_2 L$

L=no of level used in a signal

3. Carrier signal: - In analog transmission the sending device produces a high frequency signal that act as a base for the information signal. The base signal is called as carrier signal/carrier frequency.

4. Bandwidth:- The bandwidth of a signal is the difference between the highest to lowest frequency content in the signal.
5. Dc component:- When the voltage level in a digital signal is constant for a while the spectrum creates a very low frequency (around 0) called as DC component which creates some problem during transmission.
6. Throughput is the measure of how fast the data is being sent through a network. It is normally expressed in bps.
7. Latency:-

Latency=propagation time + transmission time + queuing time + process delay.

Propagation time= distance/propagation speed

Transmission time=message size/bandwidth

Queuing time:-this time needed for each intermediate device to hold the message before it can be processed.

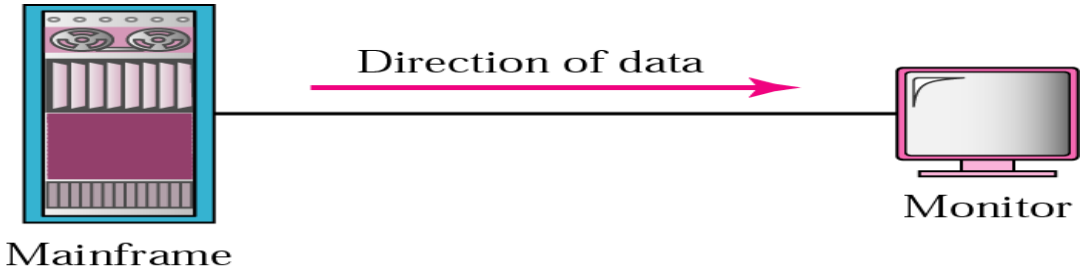
Processing delay:-processing delay or bandwidth delay .it defines the number of bits can fill the link.

Base band transmission	Broad band transmission
• The digital signal is sent over a channel without converting it into an analog signal is called as base band transmission. • The entire bandwidth of a link is consumed by a single channel. • It requires a low pass channel whose bandwidth starts from 0. • For transmission modulation is not required . • Transmission is bidirectional. • For encoding Manchester and differential Manchester encoding is used.	• The digital signal is first converted to analog and then the transmission takes place over the channel is known as broad band transmission. • Signals having multiple number of frequencies are allowed to travel in a single link simultaneously. • It requires a band pass channel whose bandwidth does not start from 0. • Before transmission modulation takes place. • Transmission is unidirectional. • For encoding binary PSK encoding is used.

Transmission

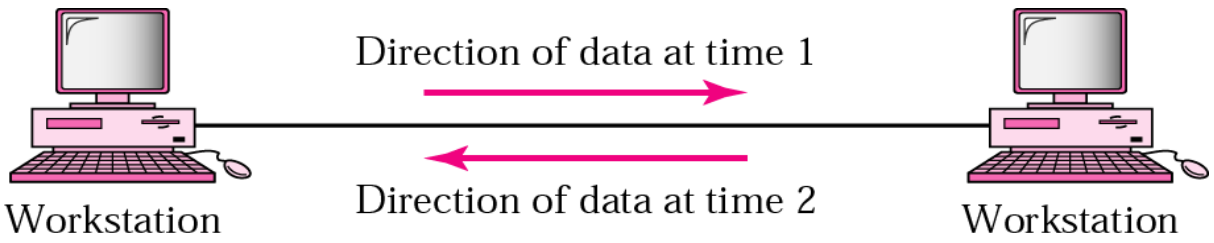
Communication between two devices can be simplex, half-duplex, or full-duplex.

1.Simplex



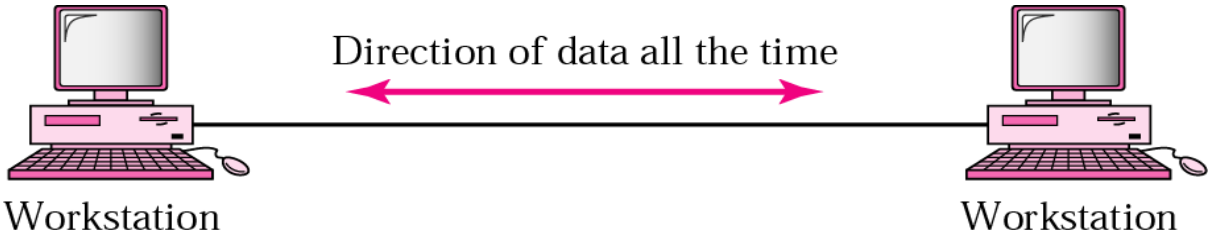
- In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Keyboards and monitors are traditional examples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

2.Half-Duplex



- In half-duplex mode, each station can both transmit and receive, but not at the same time When one device is sending, the other can only receive, and vice versa.
- The half-duplex mode is like a one-lane road with traffic allowed in both directions. half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are example of half-duplex systems.

3.Full- Duplex



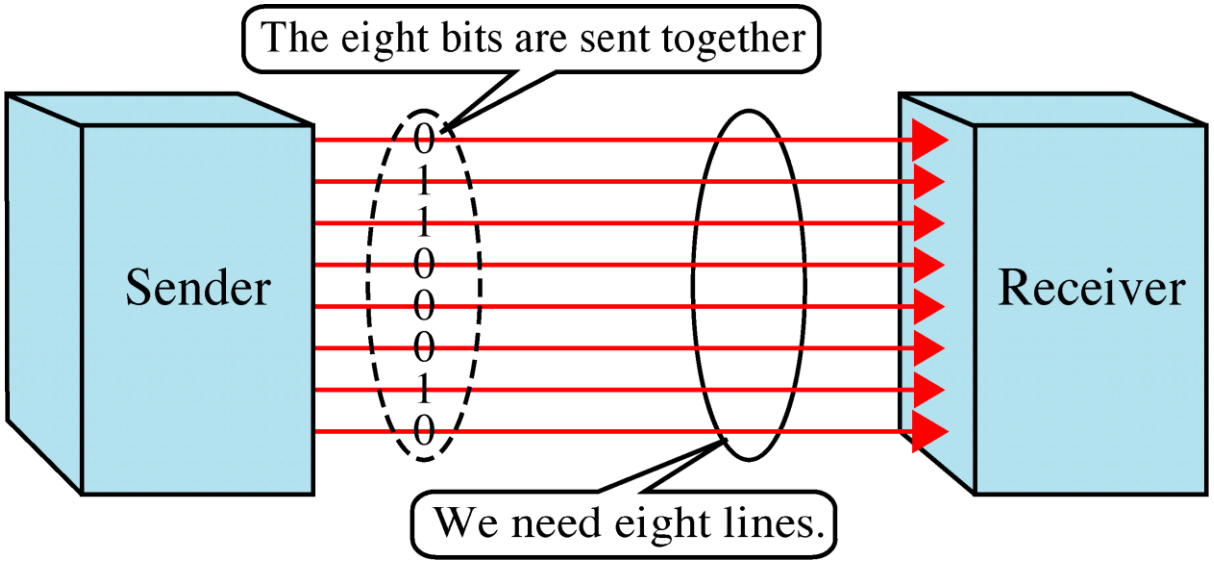
- In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously.
- The full-duplex mode is like a two way street with traffic flowing in both directions at the same time.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.
- One common example of full-duplex communication is the telephone network.
- When two people are communicating by a telephone line, both can talk and listen at the same time.
  Information generated by a source need to be encoded into a suitable format for transmission. To transmit the encoded signals generated by the Information-processing equipment over a communication link, assistance is needed.

TRANSMISSION TYPES

The transmission of binary data across a link can be accomplished in either parallel or serial mode.

Parallel Transmission

- Binary data, consisting of 1s and 0s, may be organised into groups of n bits each, By grouping, we can send data n bits at a time instead of one. This is called parallel transmission.
- We use n wires to send n bits at one time. That way each bit has its own wire, and all n bits of one group can be transmitted with each clock pulse from one device to another.
- The Figure below shows how parallel transmission works for n = 8. Typically, the eight wires are bundled in a cable with a connector at each end.



Advantage

- The advantage of parallel transmission is speed.

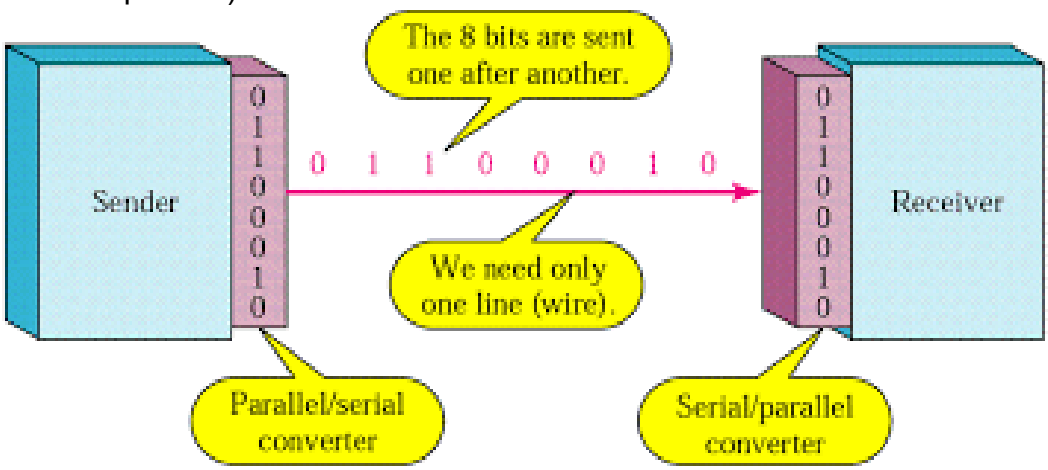
- All else being equal, parallel transmission can increase the transfer speed by a factor of n over serial transmission.

Disadvantage

- A significant disadvantage of parallel transmission is cost.
- Parallel transmission requires n communication lines (wires in the example) just to transmit the data stream.
- As this is expensive, parallel transmission is usually limited to short distances.

Serial transmission

- In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices.
- The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of n.
- Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel).



Serial transmission occurred in two ways

Asynchronous transmission

✓ Asynchronous transmission is so named because the timing of a signal is unimportant. Instead, information is received and translated by agreed-upon patterns.

✓ Patterns are based on grouping the bit stream into bytes.

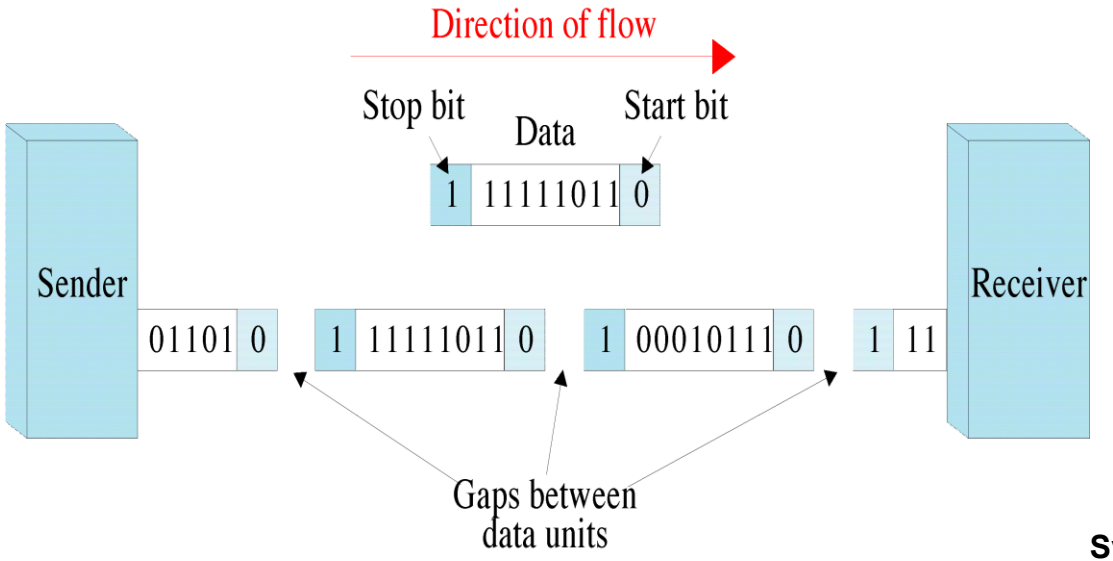
✓ Each group, usually eight bits, is sent along the link as a unit.

✓ To alert the receiver to the arrival of a new group, an extra bit is added to the beginning of each byte. This bit, usually a 0, is called the start bit.

✓ To let the receiver know that the byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s, are called stop bits.

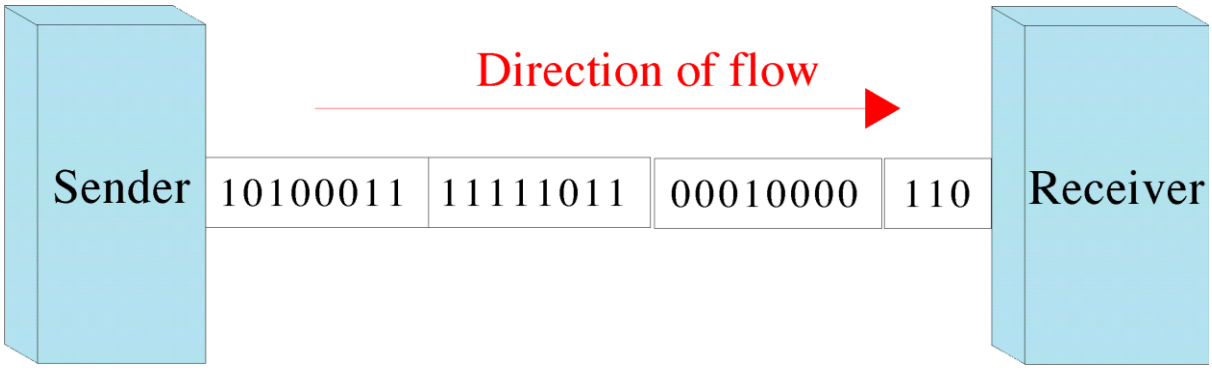
✓ In addition, the transmission of each byte may then be followed by a gap of varying duration. This gap can be represented either by an idle channel or by a stream of additional stop bits.

✓ This mechanism is called asynchronous because, at the byte level, sender and receiver do not have to be synchronise



Synchronous Transmission

- ✓ In synchronous transmission, the bit stream is combined into longer "frames," which may contain multiple bytes.
- ✓ Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes.
- ✓ In other words, data are transmitted as an unbroken string of 1s and 0s, and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.
- ✓ In synchronous transmission, we send bits one after another without start/stop bits or gaps. It is the responsibility of the receiver to group the bits.
- ✓ The advantage of synchronous transmission is speed. With no extra bits or gaps to introduce at the sending end and remove at the receiving end and, by extension, with fewer bits to move across the link, synchronous transmission is faster than asynchronous transmission. For this reason, it is more useful for high-speed applications like the transmission of data from one computer to another.



Transmission Impairments

- When a signal is transmitted over a communication channel, it is subjected to different types of impairments because of imperfect characteristics of the channel. As a consequence, the received and the transmitted signals are not the same.
- Outcome of the impairments are manifested in two different ways in analog and digital signals. These impairments introduce random modifications in analog signals leading to distortion. On the other hand, in case of digital signals, the impairments lead to error in the bit values. The impairment can be broadly categorised into the following three types:

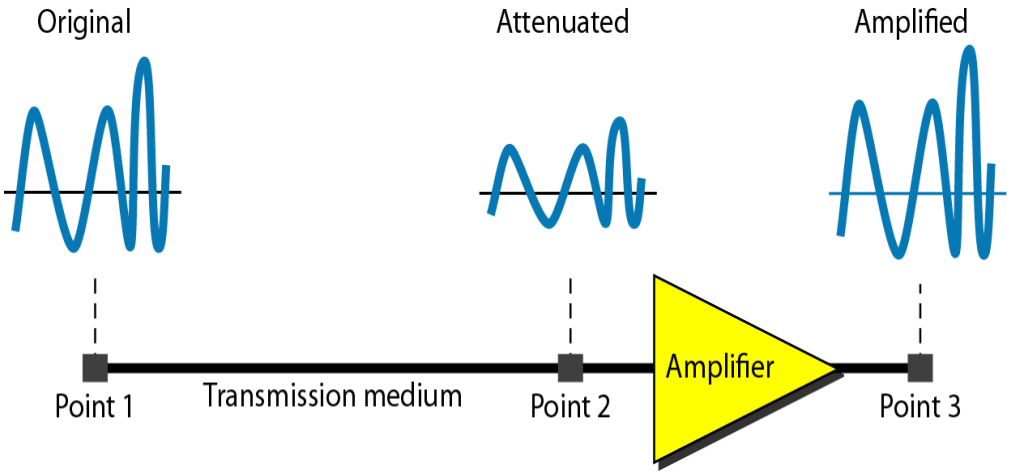
- ✓ Attenuation
- ✓ distortion
- ✓ Noise

Attenuation

- When a signal travels through a medium it loses energy overcoming the resistance of the medium.
- This is known as attenuation.
- Amplifiers are used to compensate for this loss of energy by amplifying the signal.
- To show the loss or gain of energy the unit “decibel” is used.
- $dB = 10\log_{10}P_2/P_1$

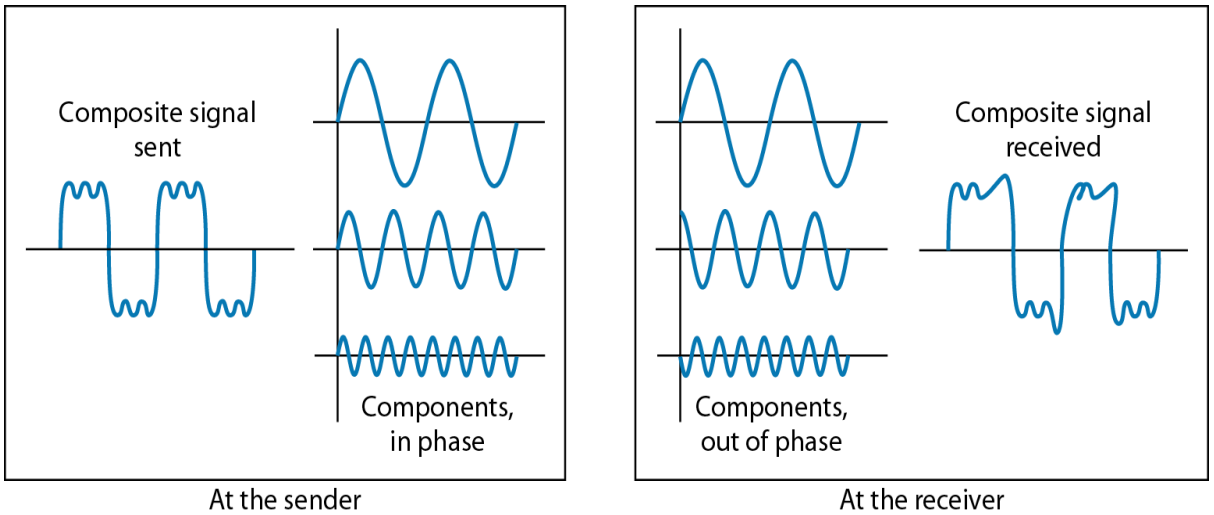
  P_1 - input signal

  P_2 - output signal



Distortion

- It means that the signal changes its form or shape.
- Distortion occurs in composite signals

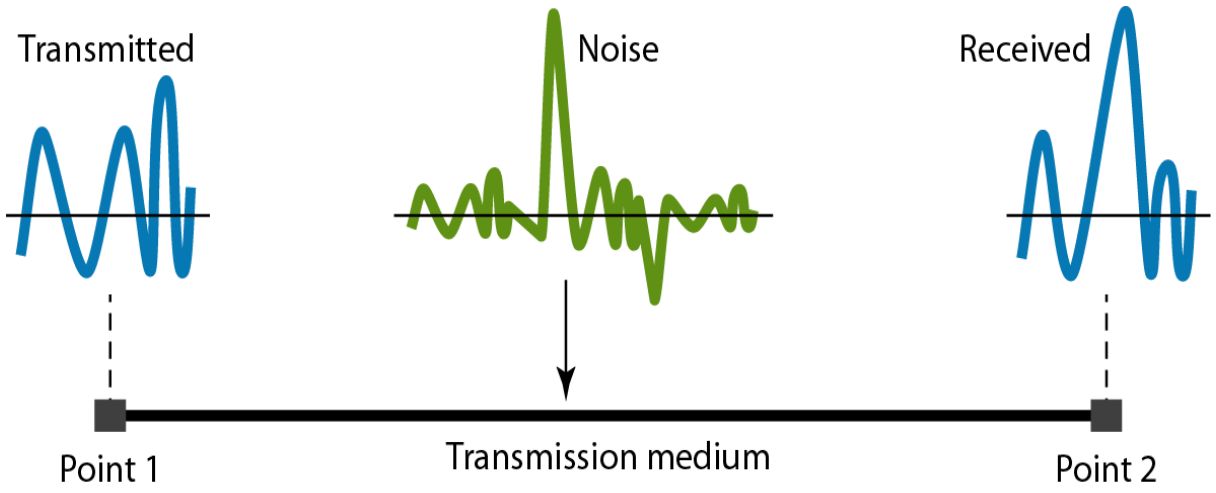


Noise

While transmission additional signal is inserted between transmitter and receiver, called as noise.

- There are different types of noise
- **Thermal** - random noise of electrons in the wire creates an extra signal

- **Induced** - from motors and appliances, devices act is transmitter antenna and medium as receiving antenna.
- **Crosstalk** - same as above but between two wires.
- **Impulse** - Spikes that result from power lines, lighning, etc.



Signal to Noise Ratio (SNR)

- To measure the quality of a system the SNR is often used. It indicates the strength of the signal with respect to the noise power in the system.
- It is the ratio between two powers.
- It is usually given in dB and referred to as SNR_{dB}.
- SNR=Average signal Power/Average Noise Power

Channel Capacity

- It is defined as the data elements (bits) sent in 1 sec.
- The unit is bits per second(bps).

DATA RATE LIMITS:

A very important consideration in data communications is how fast we can send data, in bits per second. over a channel. Data rate depends on three factors:

1. The bandwidth available.
2. The level of the signals we use.
3. The quality of the channel (the level of noise).

Two theoretical formulas were developed to calculate the data rate:

1.Nyquist for a noiseless channel.
2.Shannon for a noisy channel.

Noiseless Channel: Nyquist Bit Rate:

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

Bitrate = 2 x bandwidth x 10g2 *L*

bandwidth is the bandwidth of the channel,
L= is the number of signal levels used to represent data, and
Bitrate is the bit rate in bits per second.

EXAMPLE:
Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as
Bitrate =2 x 3000 x $\log_2$ 2 =6000 bps

EXAMPLE:
We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?
Solution
We can use the Nyquist formula as shown:
265,000 =2 X 20,000 X $\log_2$ *L*
$\log_2$ *L* =6.625 *L* =26.625 = 98.7 level

Noisy Channel: Shannon Capacity
In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the **Shannon capacity**, to determine the Theoretical highest data rate for a noisy channel:

Capacity =bandwidth X $\log_2$ (1 +SNR)

bandwidth is the bandwidth of the channel,
SNR is the signal-to noise ratio, and
capacity is the capacity of the channel in bits per second.

Example
Consider an extremely noisy channel in which the value of the signal-to-noise ratio is almost zero. In other words, the noise is so strong that the signal is faint. For this channel the capacity C
is calculated as

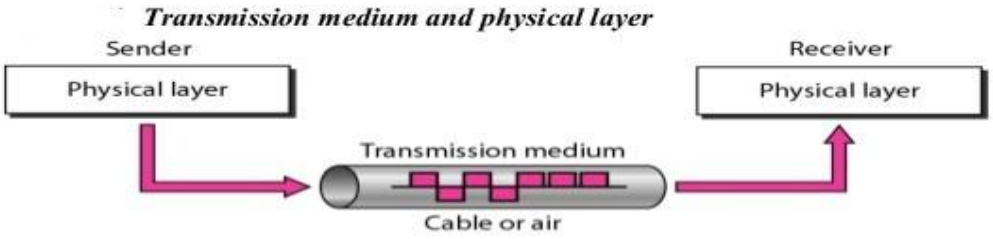
C=*B* $\log_2$ (1 + SNR)
=*B* 10g_2 (I + 0)
=*B* $\log_2$ 1 =*B* x 0 = 0

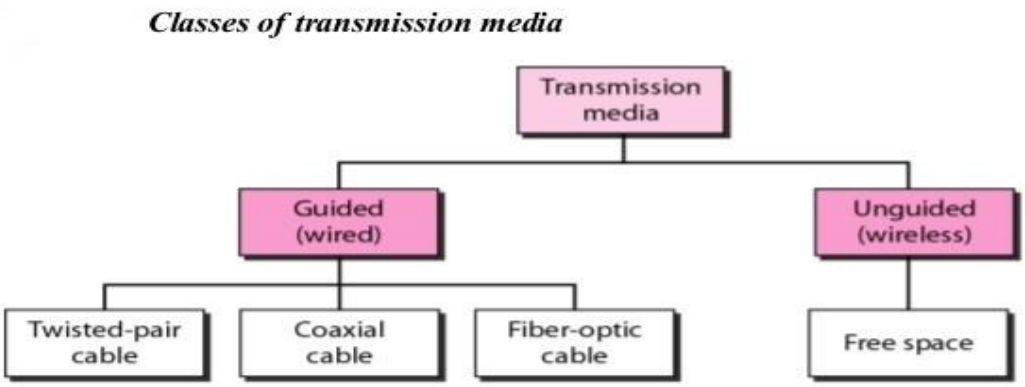
This means that the capacity of this channel is zero regardless of the bandwidth. In other words, we cannot receive any data through this channel.

Transmission Media

1`.A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
2 .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.

CATEGORIES:
In telecommunications, transmission media can be divided into two broad categories:
1.guided
2. unguided



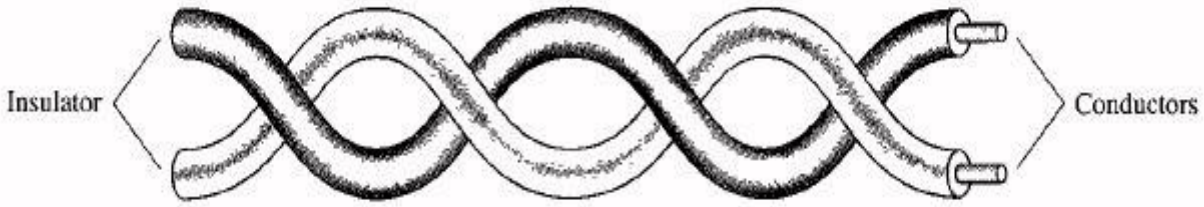


GUIDED MEDIA:

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

1. A signal traveling along any of these media is directed and contained by the physical limits of the medium.
2. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
3. Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable

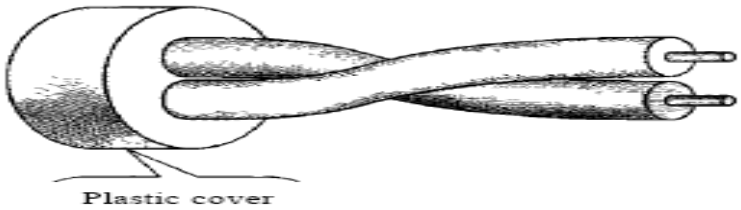


1. A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.
2. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

CATEGORIES/TYPES/KINDS:

1. Unshielded twisted Pair Cable (UTP)
2. Shielded Twisted-Pair Cable (STP)

1.Unshielded twisted Pair Cable (UTP):



1. The most common twisted-pair cable used in communications is referred to as Unshielded twisted-pair (UTP).
2. It consists of two conductors usually copper which is covered by plastic insulator.
3. Two wires are twisted one over the other at regular interval to decrease the noise and disturbances. So that at the receiving end the receiver will get the desired information.

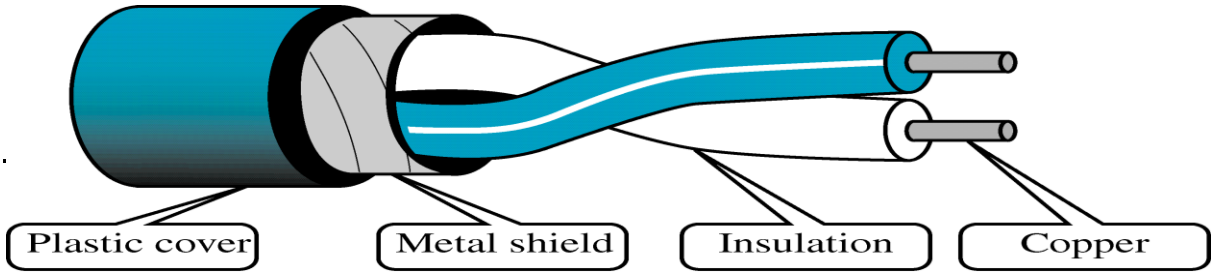
ADVANTAGES:

1. It is easy to use and flexible.
2. It is cheap.
3. It is easy to install.

APPLICATIONS:

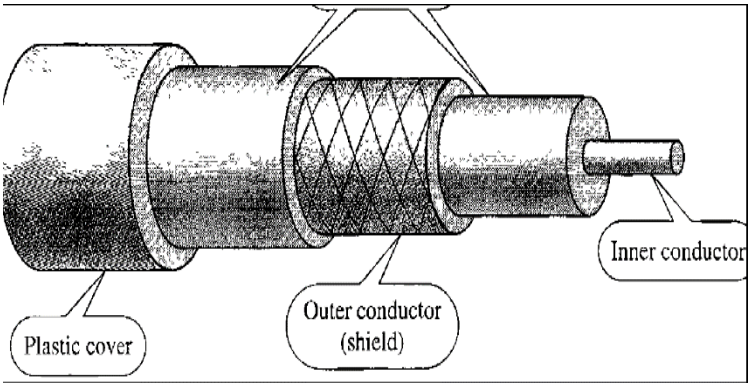
1. Is used in telephone lines to provide voice and data channels.
2. The most commonly used connecter is RJ 45 (Register jack).

2.Shielded Twisted-Pair Cable (STP):



1. STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
2. It eliminates crosstalk.
3. Here the metal foil is connected to the ground and other connection are same as UTP.

Coaxial Cable:



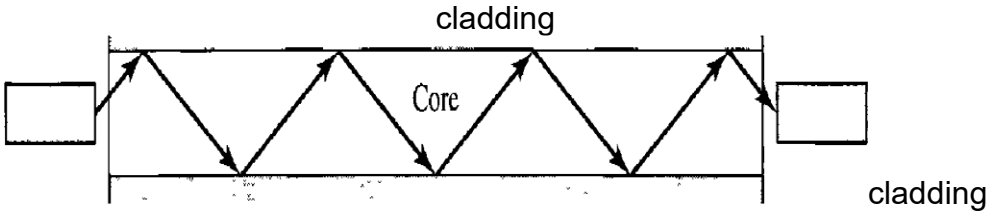
1. Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.
2. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
3. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
4. This outer conductor is also enclosed in an insulating sheath, and the whole cable is Protected by a plastic cover.
5. Coax carries signals of higher frequency ranges (i.e. 100 KHz – 500MHz) than those in twisted pair cable, in part because the two media are constructed quite differently.
6. Coaxial cables categorized by their radio government (RG) ratings.

APPLICATION:

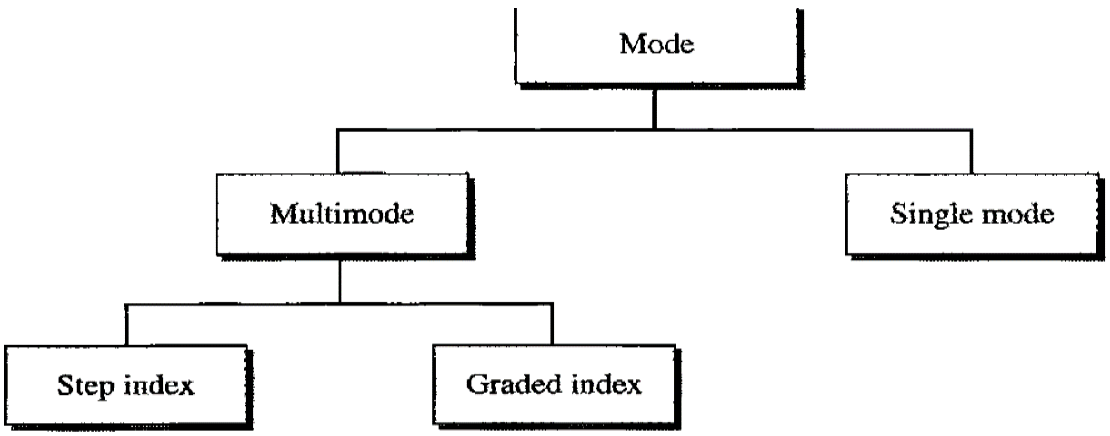
1. Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
   Cable TV networks also use coaxial cables.
2. Another common application of coaxial cable is in traditional Ethernet LANs.
3. Connectors used: Barrel connector, T-connector, Terminator

FIBER OPTICS CABLE:

1. A fibre-optic cable is made of glass or plastic and transmits signals in the form of light.
2. Optical fibres use reflection to guide light through a channel.
3. A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
4. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



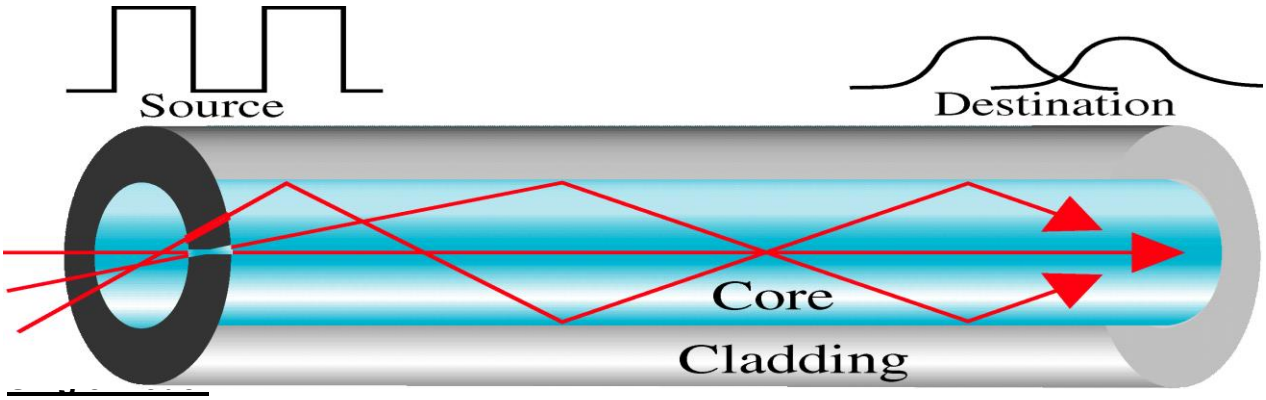
Propagation Modes:



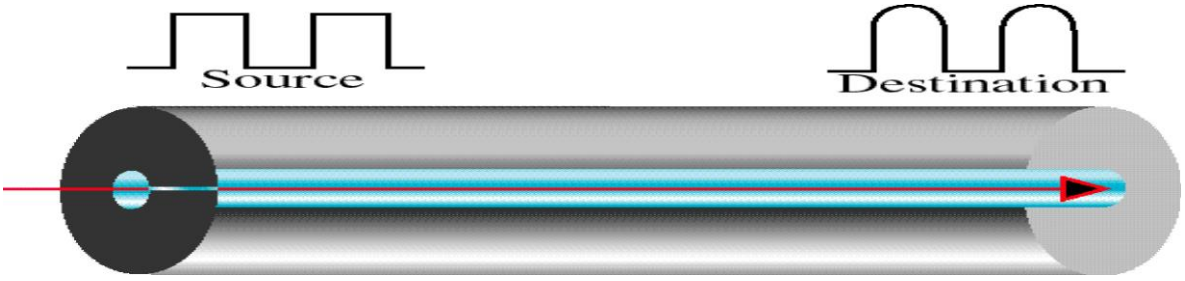
1. Current technology supports two modes -multimode and single mode for propagating light along optical channels, each requiring fiber with different physical characteristics.
2. Multimode can be implemented in two forms:
   step-index or graded-index.

Multimode:

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.



1. Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
2. The single mode fibre itself is manufactured with a much smaller diameter than that of multimode fibre, and with substantially lower density (index of refraction).
3. The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible.
4. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.



Applications:

1.Fiber-optic cable is often found in backbone networks because its wide bandwidth is Cost-effective.
2. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages: Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

1. Higher bandwidth.
2. Less signal attenuation.

3. Noise resistance
4. Light weight.

Disadvantages: There are some disadvantages in the use of optical fiber.

1. Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
2. Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
3. Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.
4. Fragility: Glass fiber is more easily broken than wire which makes it less useful, where hardware portability is required.

Wireless transmission / unguided transmission:-

- Unguided transmission involves the mode of communication by means of electro-magnetic waves without using physical conductor.
- Signals are normally broadcast through free space and the receiver are allowed to capture the signals by using an antenna.

There are three modes of wireless transmission: -

1. Earth propagation/ground propagation
2. Sky propagation (high frequency)
3. Line of sight propagation (very high frequency).

Types of wireless transmission: -

1. Radio wave
2. Micro wave
3. Infra-red

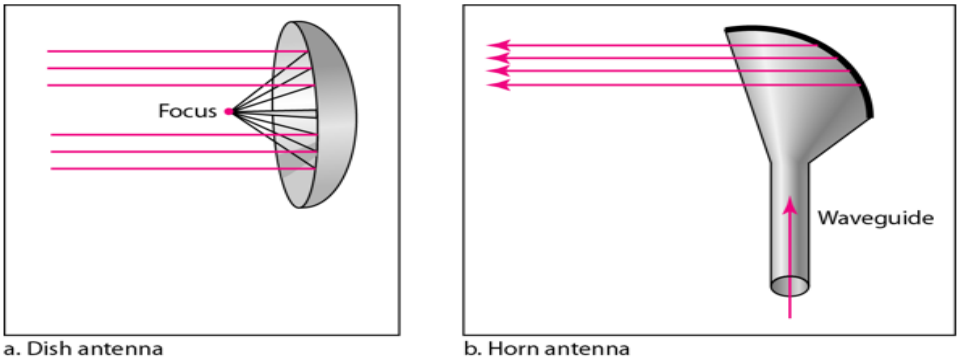
Radio waves: -

- The radio waves are omni-directional.
- When the antenna transmits radio waves they are propagated in all direction.
- It follows sky propagation mode.
- The frequencies it transmits can penetrate the wall.
- It transmits in two ways i.e Amplitude modulation (AM) and frequency modulation(FM).
- The bandwidth of the radio waves is relatively narrow i.e under 1GHz.
- Radio waves are used for multi-cost communication such as radio, television and live streaming.

Micro waves: -

- The electromagnetic waves having frequencies 1-30GHz are known as microwaves.
- These waves are unidirectional.
- When an antenna transmits microwaves, they can be narrowly focused.
- This means that sending and receiving antenna need to be aligned.
- Microwaves propagation follows line-of-sight propagation mode.
- It transmits very high frequency range.
- The bandwidth of this propagation is relatively wide. So, sub-bands can be assigned in between them.
- Two types of antennae are used:- a-parabolic dish antenna b-horn antenna.

a:-parabolic dish antenna



a. Dish antenna b. Horn antenna

- These are used in cellular network and satellite network and also in case of wireless LAN.

Infra-red:-

- Infra-red frequency ranges from (300 GH_z-400THz).
- It is used for short range communication.
- These frequencies cannot penetrate any type of obstacles.
- It also works in the mode of line-of-sight propagation.

For example:- the communication between remote to a device.

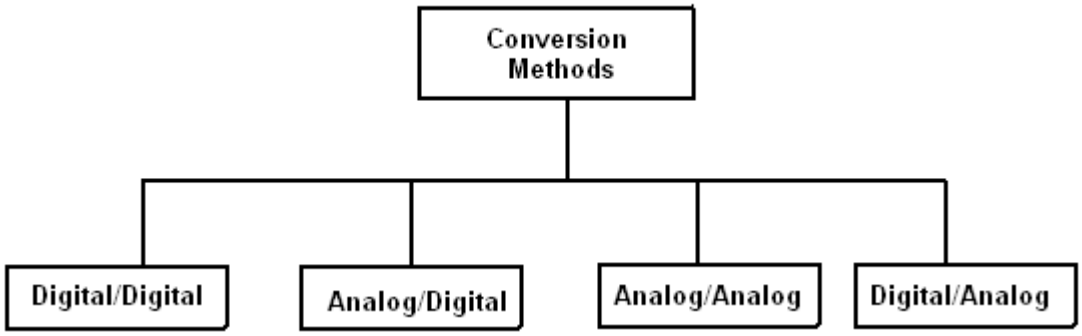
CHAPTER -3
DATA ENCODING

Data Encoding

In the process of data communication, the data must be transformed into signals to send them from one place to another. Data stored in a computer is in the form of 0s and 1s.To transform this data from one place to another place , it must be converted into digital signals. This is called Encoding digital data into digital signal or digital to digital conversion. The process of converting analog signal into digital signal is called analog to digital conversion or digitizing an analog signal.

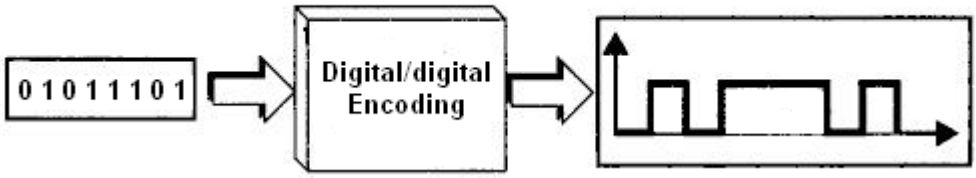
The process of converting the digital signal into analog signal is called digital to analog conversion or modulating a digital signal.

The process of sending an analog signal over long distances using a high frequency carrier signal is called analog to analog conversion or modulating an analog signal.



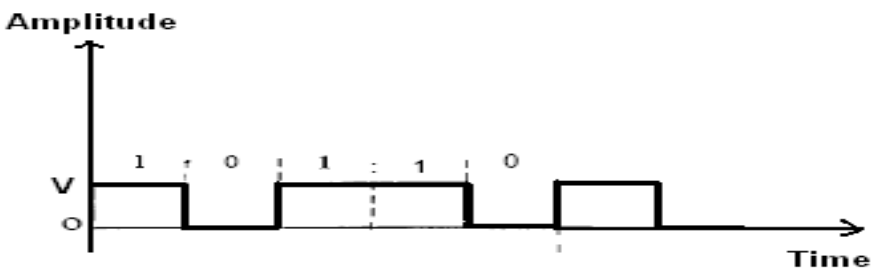
Digital data digital signals

It is the representation of a digital information by a digital signal. In this process of encoding the binary 1s and 0s generated by a computer are translated into a sequence of voltage pulses that can be transmitted over a cable or wire.



There are three types of digital encodings. Unipolar, Polar and Bi-polar.

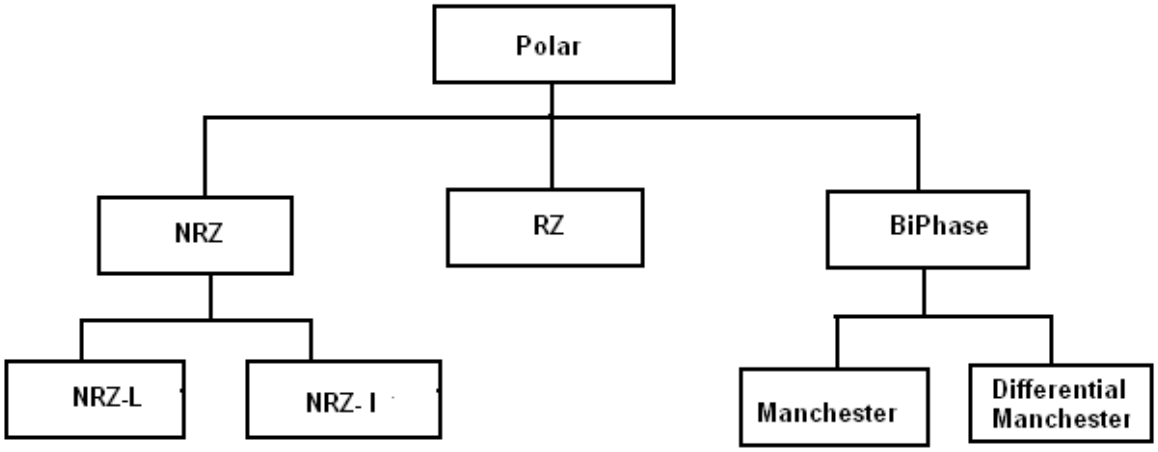
Uni-polar: Unipolar encoding uses only one level of value. i.e in a uni-polar scheme, all the signal levels are on one side of the time axis, either above or below.



The uni-polar encoding has two problems. One is DC component and the other is synchronization. Due to these limitations, this encoding is not widely used.

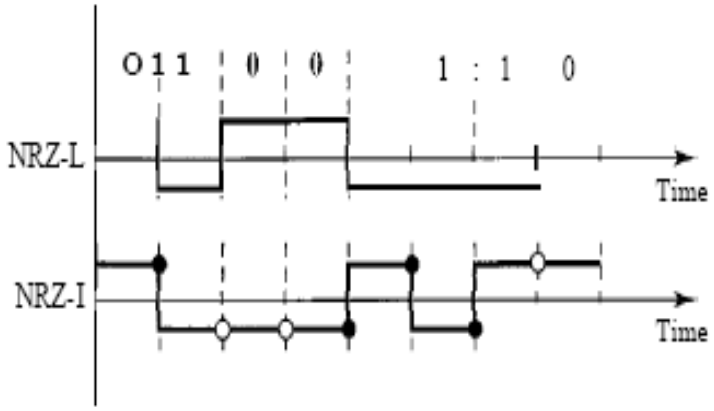
Polar Schemes:

- In polar schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.
- The popular Polar encoding techniques are non-return zero(NRZ),Return to Zero(RZ) and bi-phase.
- The bi-phase refers to two methods. One is Manchester used in Ethernet LAN and the second is Differential Manchester used by token rings LANs.



Non-Return-to-Zero (NRZ):

- In polar NRZ encoding, two levels of voltage amplitude are used.
- There are two versions of polar NRZ: NRZ-Land NRZ-I.
- In the first variation, NRZ-L (NRZ-Level), the level of the voltage determines the value of the bit. In the second variation, NRZ-I (NRZ-Invert), the change or lack of change in the level of the voltage determines the value of the bit.
- If there is no change, the bit is 0; if there is a change, the bit is 1. NRZ-L and NRZ-J both have a DC component problem.

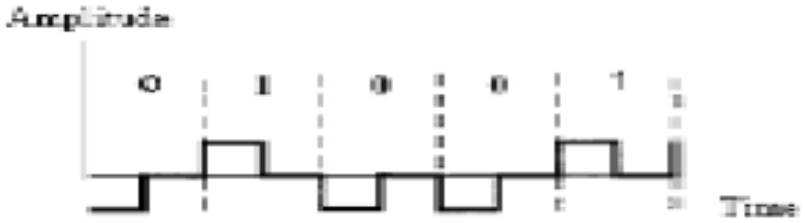


The synchronization problem (sender and receiver clocks are not synchronized) also exists in both the schemes. This problem is more serious in NRZ-L than in NRZ-I.

Return to Zero (RZ)

- The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. Hence the Return-to-zero (RZ) scheme is used.
- This scheme uses three values: positive, negative, and zero.
- In RZ, the signal changes not between bits but during the bit.

- The main disadvantage of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth.
- This scheme has no DC component problem, but the problem is the complexity . RZ uses three levels of voltage, which is more complex to create .
- As a result of all these deficiencies, the scheme is not used today. Instead, the better-performing schemes like Manchester and differential Manchester schemes are used.



Bi phase:

The best solution for the problem of synchronization is the Bi-phase encoding. This bi-phase encoding consists of two important encodings namely Manchester and Differential **Manchester encodings.**

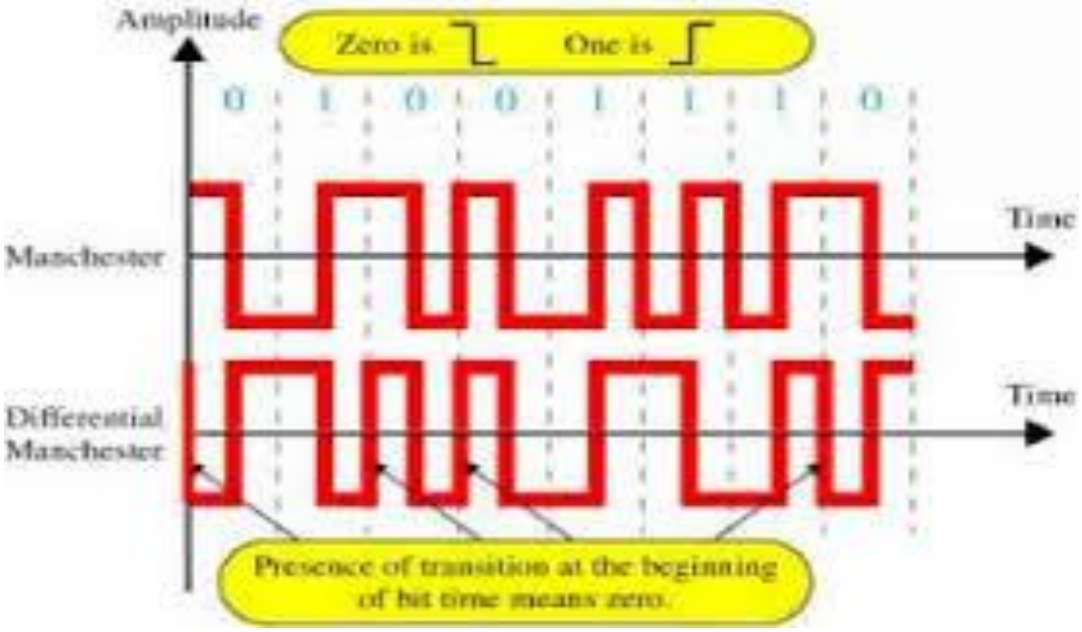
Manchester scheme is the resultant of the idea of RZ (transition at the middle of the bit) and the idea of NRZ-L .

In Manchester encoding, the duration of the bit is divided into two halves, the voltage remains at one level during the first half and moves to the other level in the second half.

The transition at the middle of the bit provides synchronization.

Differential Manchester

Differential Manchester, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none. Figure below shows both Manchester and differential Manchester encodings.



In Manchester and differential Manchester encoding, the transition at the middle of the bit is used for synchronization. The Manchester scheme overcomes several problems associated with NRZ-L, and differential Manchester overcomes several problems associated with NRZ-I.

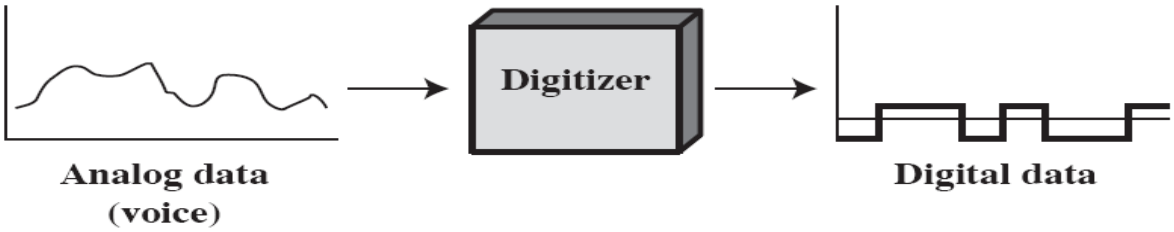
Analog data digital signals

Analog data such as voice, video and music can be converted into digital signal communication through transmission media. This allows the use of modern digital transmission and switching equipment's. The device used for conversion of analog data to digital signal and vice versa is called a coder (coder-decoder). There are two basic approaches: - Pulse Code Modulation (PCM) - Delta Modulation (DM)

Pulse Code modulation

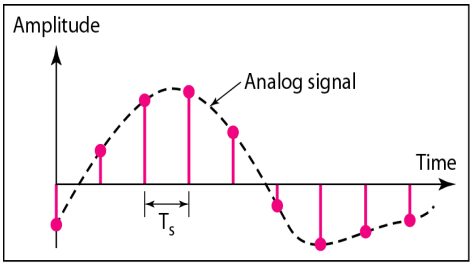
Pulse Code Modulation involves the following three basic steps

- Sampling – PAM
- Quantization
- Line coding

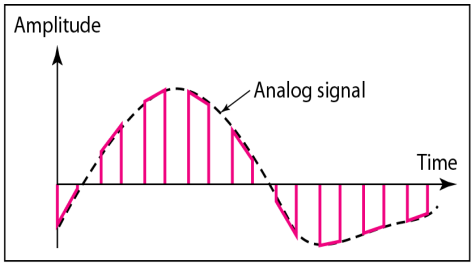


Sampling:

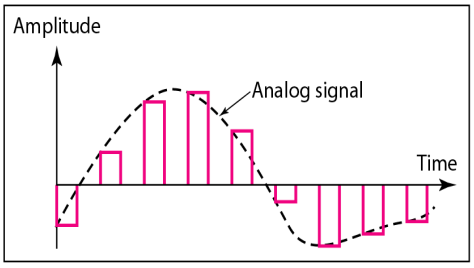
- This process is based on Shannon's sampling theorem. Numbers of samples of the signal are taken at regular intervals, at a rate higher than twice the highest significant signal frequency. This basic step is known as Pulse Amplitude Modulation.
- For example, during the sampling of voice data, in the frequency range 300 to 4000 Hz, 8000 samples per second are sufficient for the coding.
- There are different types of sampling technique are there:
  - Ideal sampling
  - Natural sampling
  - flattop sampling



a. Ideal sampling



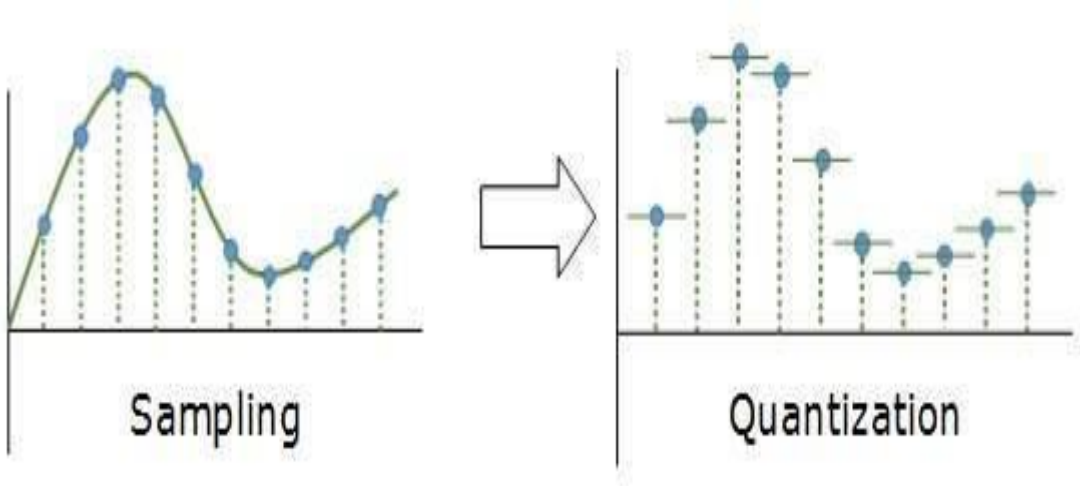
b. Natural sampling



c. Flat-top sampling

Quantization

- Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.
- The PAM samples are quantized and approximated to n-bit integer by using analog-to-digital converter.
- For example, if n = 4, then there are 16 (=24) levels available for approximating the PAM signals. This process introduces an error are known as quantization error.



Line Coding

- The last step in PCM is encoding, after each sample is quantized and the number of bits per sample is decided, each sample can be changed to an nb code word.
- Number of bits for each sample is determined from the no of quantization level. For ex. L =8,no of bit is nb=log2L.=3(A quantization code of 2 is encoded as 010,5 as 101) .
- The digital data thus obtained can be encoded into one of digital signals.

DIGITAL-TO-ANALOG CONVERSION

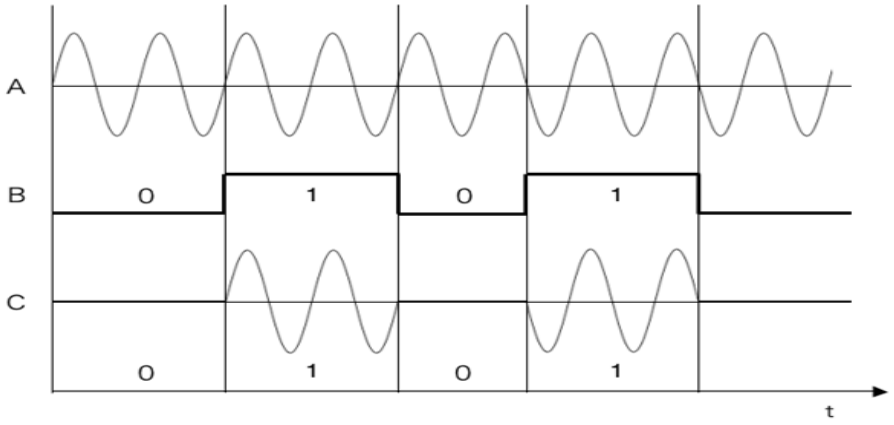
- **Digital-to-analog conversion** is the process of changing one of the characteristics of an analog signal based on the information in digital data.
- It is also called as Modulation of digital signal.
- Depending on whether the amplitude, frequency, and phase of the carrier signals modified there are three mechanisms for modulating digital data into an analog signal such as amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK).

1. Amplitude Shift Keying (ASK)

- In amplitude shift keying, the amplitude of the carrier signal is varied without changing its frequency and phase.
- The amplitude of a carrier signal is multiplied by binary 0 or 1. ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or on-off keying (OOK).
- The bandwidth B is directly proportional to signal rate as shown below.

$$B$$

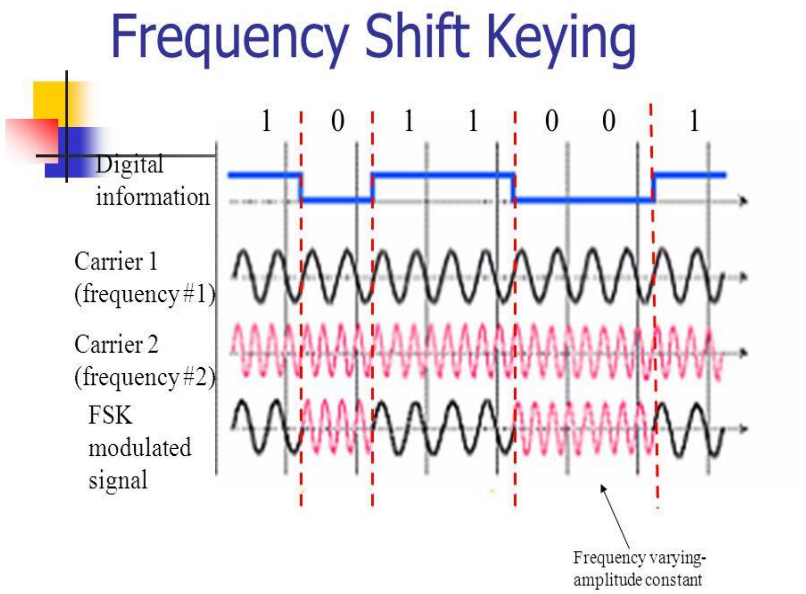
Where fc is a factor lies between 0 & 1.



2. Frequency Shift Keying (FSK)

- In frequency shift keying, the frequency of the carrier signal is changed without changing its amplitude and phase.
- The simplest form of FSK is binary FSK in which two carrier frequencies are taken to represent two binary values.in digital data.
- The bandwidth for BFSK can be calculated as :

$$B = $$

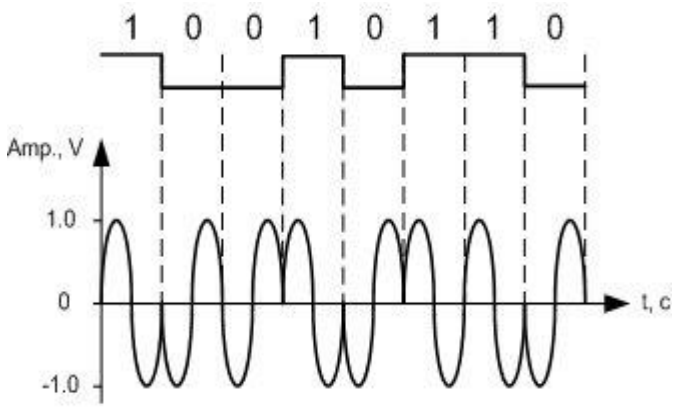


23

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

In phase shift keying, the phase of the carrier is varied by keeping both peak amplitude and frequency remain constant .

The simplest PSK is binary PSK, in which we have only two signal elements, one with a phase of 0°, and the other with a phase of 180°.



Phase shift keying (PSK)

ANALOG-TO-ANALOG CONVERSION

- The process of representing analog data by analog signal is known as analog –to-analog conversion or Analog Modulation.
- Modulation is categorised into following types:

Amplitude Modulation –

In Amplitude Modulation transmission, the amplitude of the carrier wave is varied in accordance with the characteristics of the modulating signal . The frequency and phase of the carrier remains the same only the amplitude changes to follow the variation in information.

The bandwidth of the amplitude modulated signal is twice of that of modulating signal.

Bm=2B.

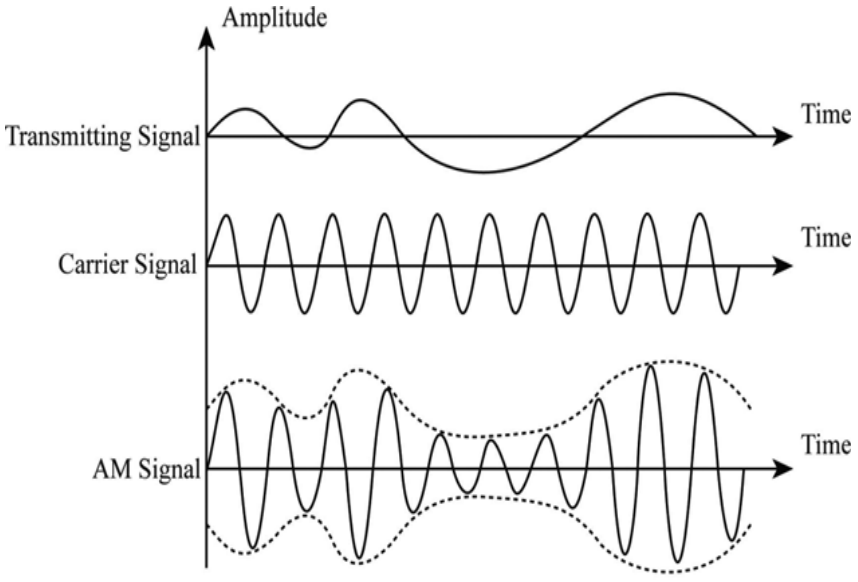


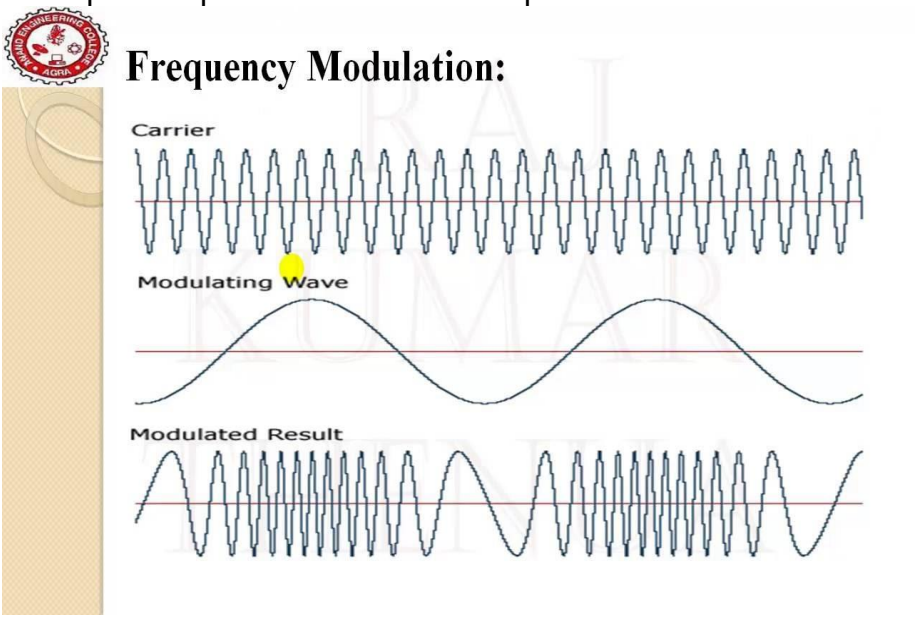
Figure 1

Frequency Modulation –

In Frequency Modulation transmission, the frequency of carrier signal is modulated to follow the changing voltage level of modulating signal. The peak amplitude and phase of carrier signal remains constant but as the amplitude of information system changes, the frequency of carrier changes corresponding. The actual bandwidth is difficult to determine exactly but it can be solved shown that it is several lines that of analog signal. B

FM= 2(1 + β)B

Here β is a factor depends upon modulation technique

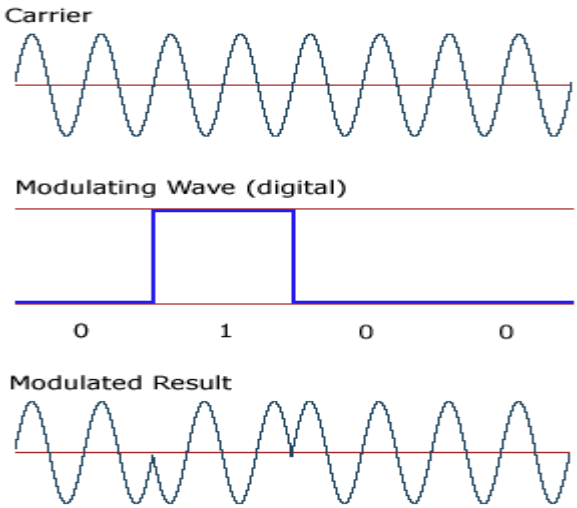


Phase Modulation –

In phase modulation transmission the phase of carrier signal is modulated to follow the changing voltage level of modulating signal. The peak of amplitude and frequency of carrier signal remains constant but the amplitude of information signal changes the phase of carrier signal. The total bandwidth that is needed by a PM signal can be calculated as

Bpm= 2(1 + β)B

Where β is a factor whose value is lower in PM than FM.



Analog data digital signals

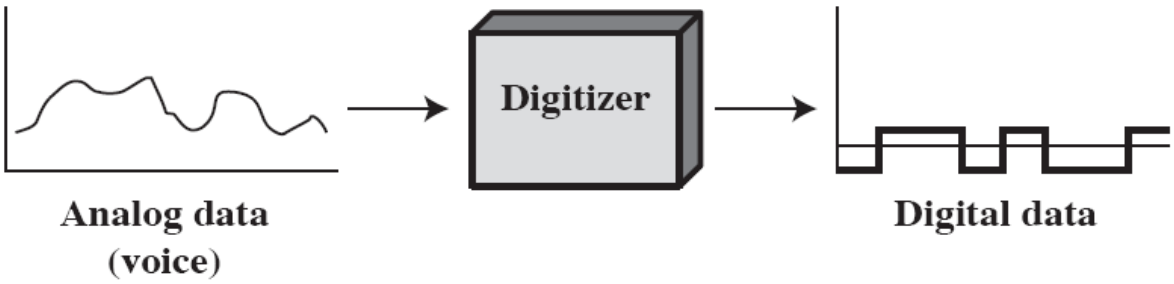
Analog data such as voice, video and music can be converted into digital signal communication through transmission media. This allows the use of modern digital transmission and switching equipment's. The device used for conversion of analog data to digital signal and vice versa is called a coder (coder-decoder). There are two basic approaches: - Pulse Code Modulation (PCM)

- Delta Modulation (DM)

Pulse Code modulation

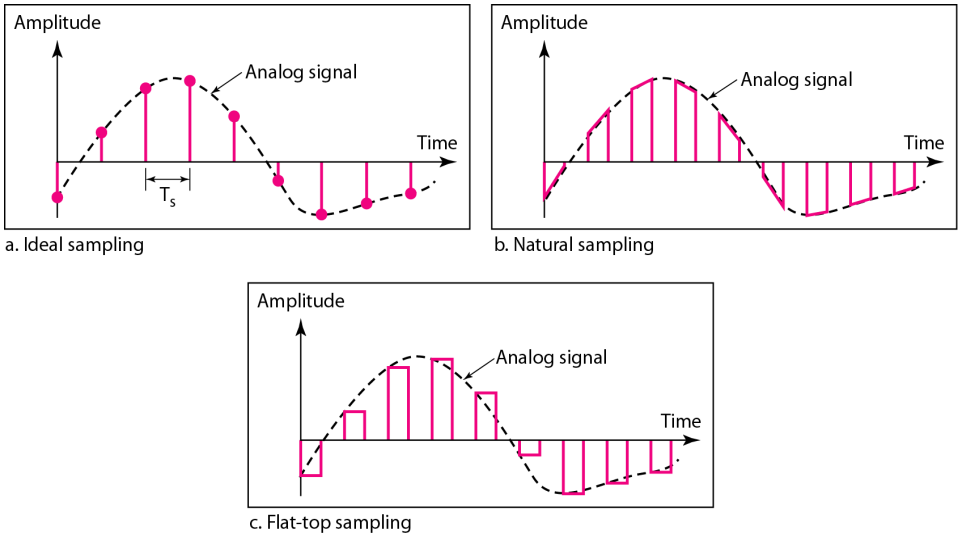
Pulse Code Modulation involves the following three basic steps

- Sampling – PAM
- Quantization
- Line coding



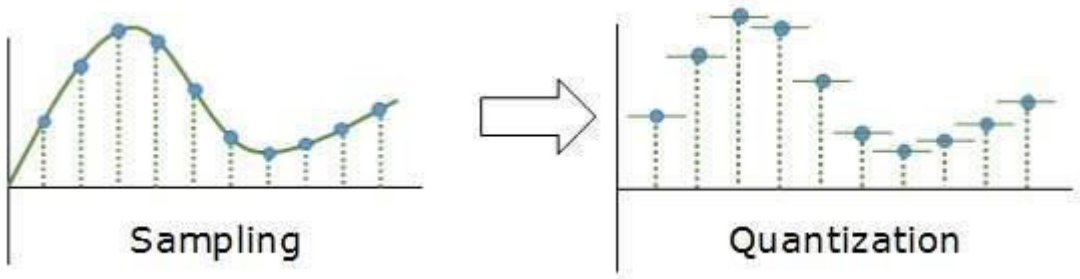
Sampling:

- This process is based on Shannon's sampling theorem. Numbers of samples of the signal are taken at regular intervals, at a rate higher than twice the highest significant signal frequency. This basic step is known as Pulse Amplitude Modulation.
- For example, during the sampling of voice data, in the frequency range 300 to 4000 Hz, 8000 samples per second are sufficient for the coding.
- There are different types of sampling technique are there:
  - Ideal sampling
  - Natural sampling
  - Fltptop sampling



Quantization

- Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.
- The PAM samples are quantized and approximated to n-bit integer by using analog-to-digital converter.
- For example, if n = 4, then there are 16 (=24) levels available for approximating the PAM signals. This process introduces an error are known as quantization error.



Line Coding

- The last step in PCM is encoding, after each sample is quantized and the number of bits per sample is decided,each sample can be changed to an nb code word.
- Number of bits for each sample is determined from the no of quantization level. For ex. L =8,no of bit is nb=log2L.=3(A quantization code of 2 is encoded as 010,5 as 101) .
- The digital data thus obtained can be encoded into one of digital signals.

CHAPTER -4
DATA COMMUNICATION & DATA LINK CONTROL

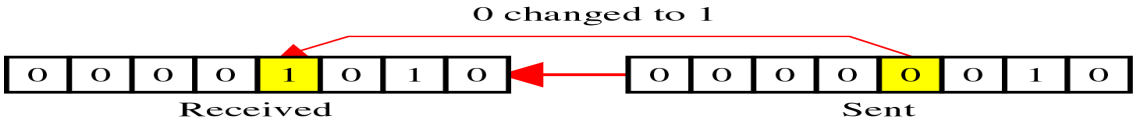
.

Error Detection

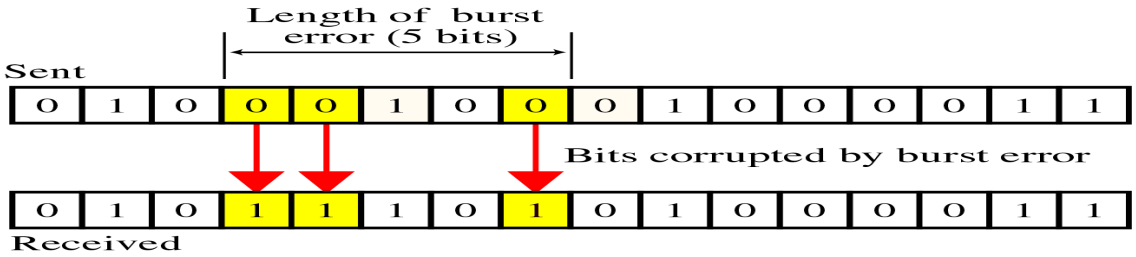
Data can be corrupted during transmission. Some applications require that errors be detected and corrected.

Types of Errors:

1.Single-Bit Error: *single-bit error* means that only 1 bit of a given data unit is changed from 1 to 0 or from 0 to 1



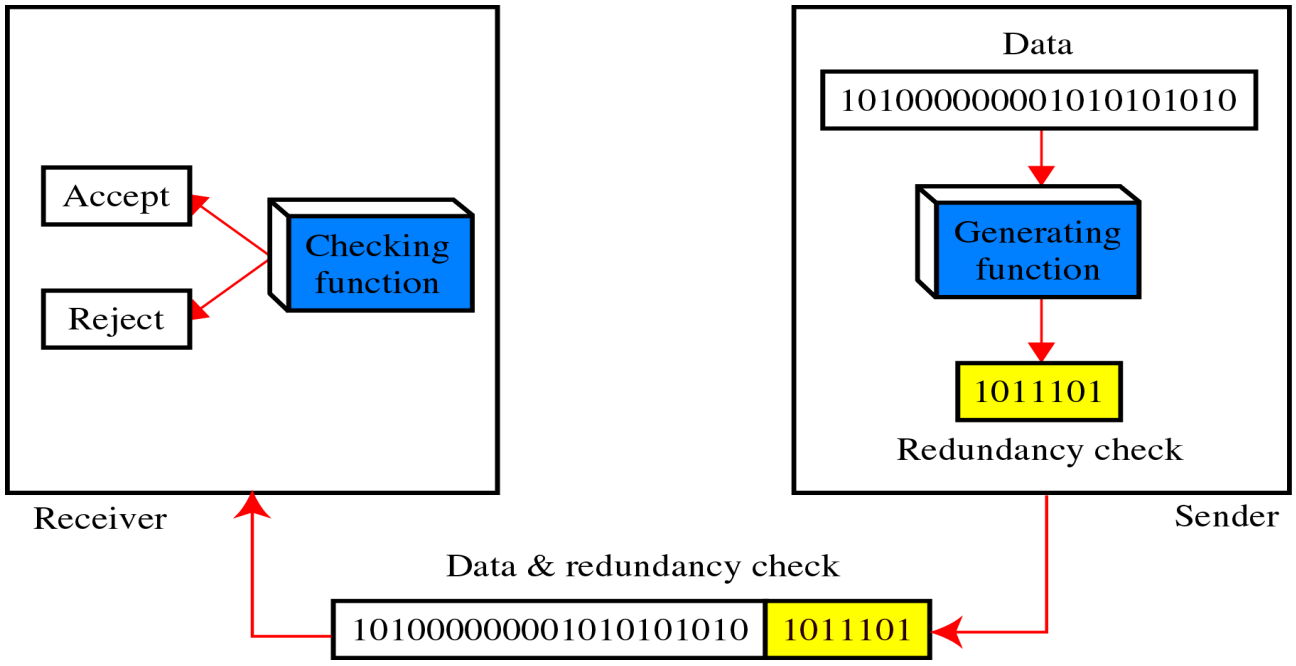
2. Burst Error: *Burst error* means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



A burst error does not necessarily mean that the errors occur in consecutive bits. The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

Redundancy :

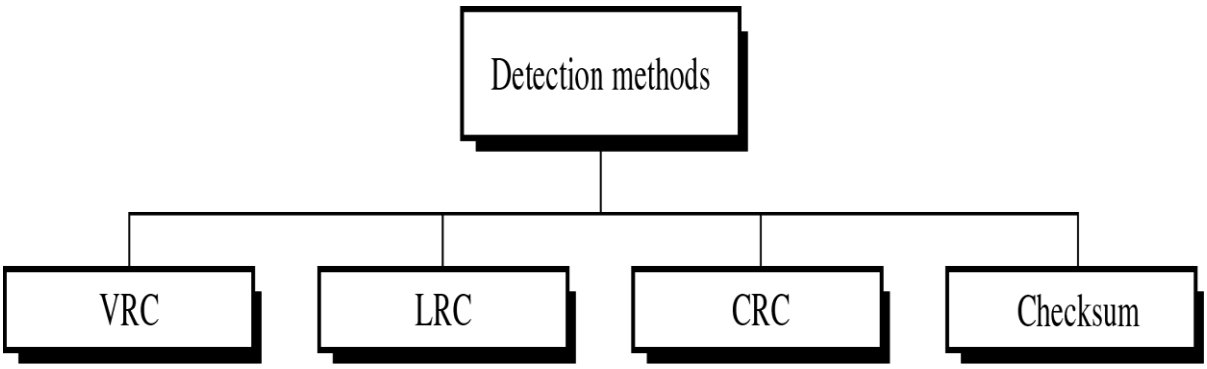
To detect or correct errors, we need to send some extra bits(called redundant bits) with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.



Detection Versus Correction :

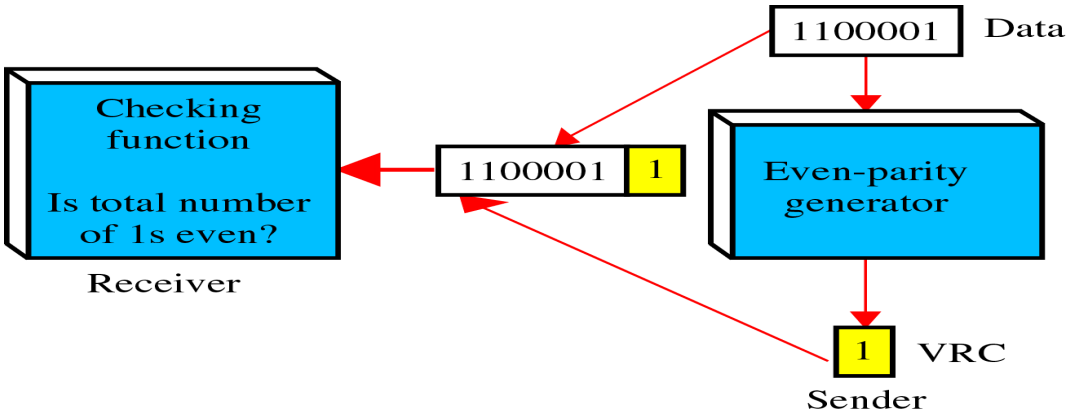
In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. But in error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.

Different error detection methods:



1. Vertical Redundancy Check (VRC):

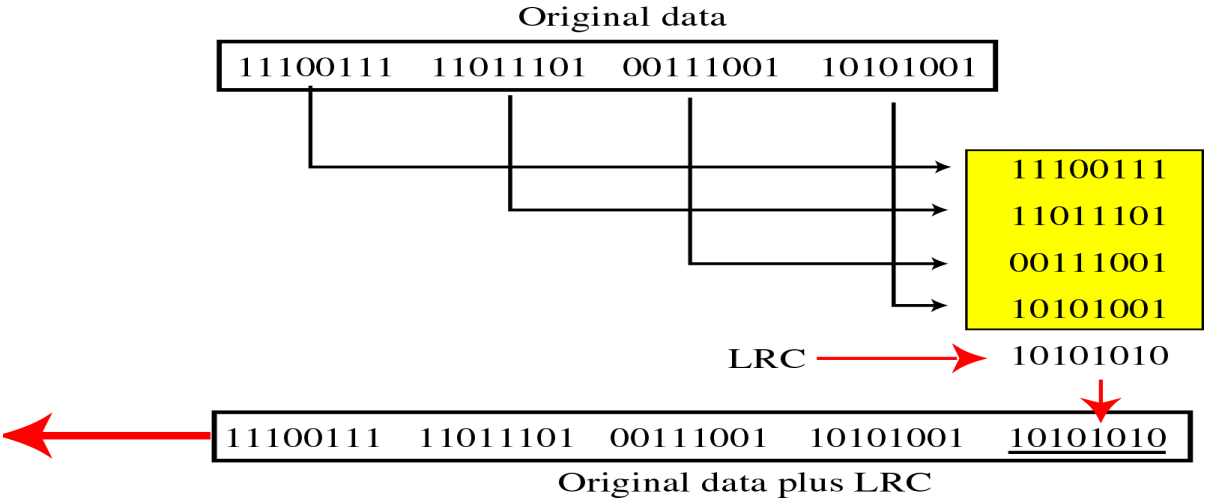
- It is most commonly and least expensive mechanism for error detection, often called as parity check.
- In this technique, a redundant bit called parity bit is appended to every data unit so that total no. of 1s in the unit becomes even.
- Before transmitting we pass the data unit through generator and it counts the 1s and appends the parity bit to end so that the total number of 1s is even.



- When it reaches the destination, the receiver puts all 8 bits through an even- parity checking function and it counts the no. of 1s, if it is even then the data is correct otherwise there is an error on data so it is rejected
- VRC can detect all single-bit errors. It can detect brust errors only if the total number of errors in each data unit is odd.

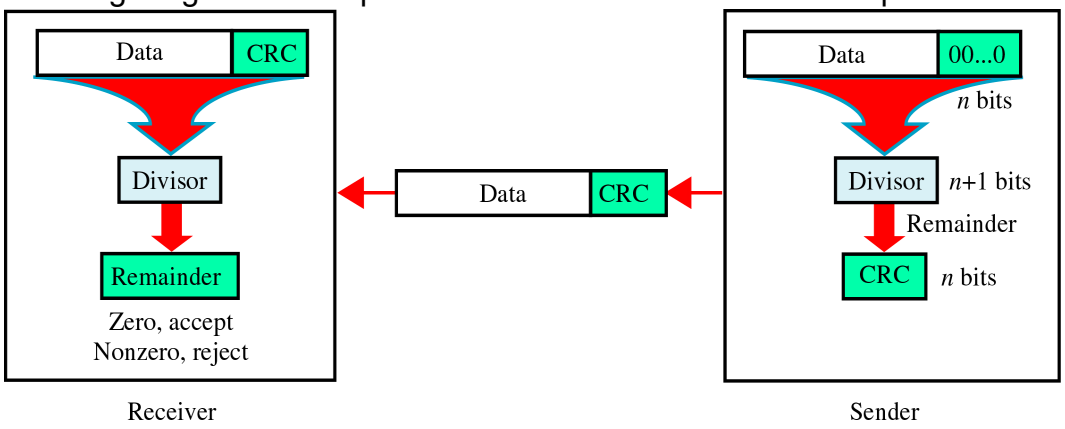
2. Longitudinal Redundancy Check (LRC)

- In LRC, a block is organized in a table (block is divided in to rows and a redundant row of bits is added to whole block).
- For an example, instead of sending a block of 32 bits , we organize them in a table made of 4 rows and eight columns as shown in below figure.
- We then calculate the parity bit for each column and create a new row of 8 bits , which are the parity bits of whole block
- Note that the first parity bit in the 5^{th} row is calculated based on the all 1^{st} bits and so on.
- We then attach the 8 parity bits to original data and send them to the receiver.



3. **Cyclic Redundancy Check (CRC) :**

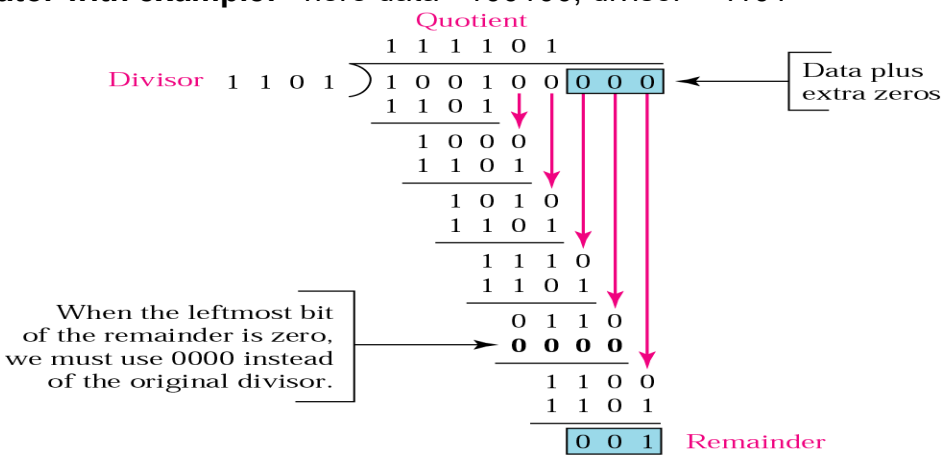
The and most powerful of the redundancy checking is CRC, it is based on modulo-2 binary division. the figure given below provides an outline of three basic steps.



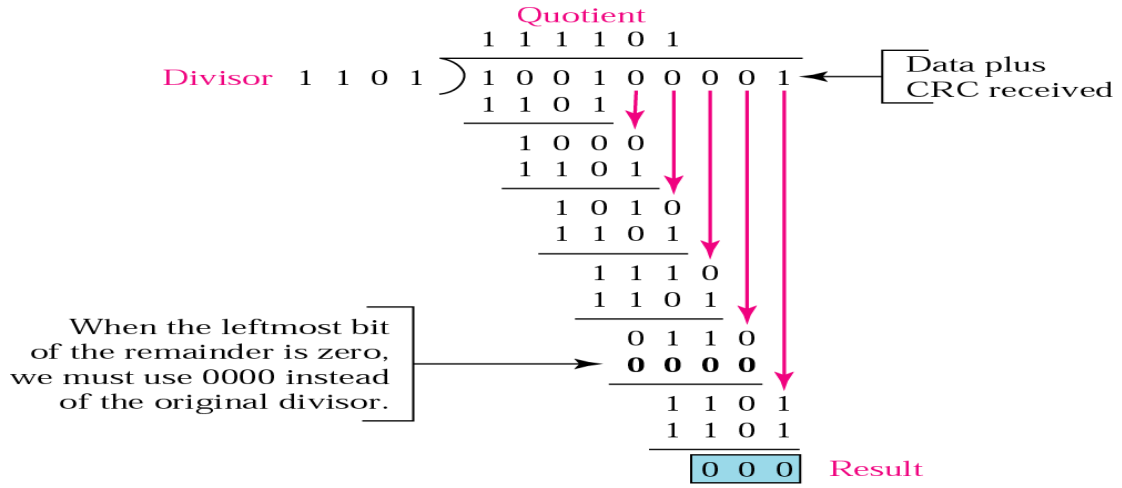
- First, a string of *n* 0s is appended to the data unit. The number *n* is one less than the number of bits in the predetermined divisor, which is *n+1* bits.
- Second, the newly elongated data unit is divided by the divisor using a process called binary division. The remainder resulting from this division is CRC.
- Third, the CRC of *n* bits derived from in step 2 replaces the appended 0s at the end of the data unit. Note that the CRC may consist of all 0s.

The data units arrives at the receiver data first, followed by CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder. If CRC = zero the accept otherwise reject

CRC generator with example: here data= 100100, divisor = 1101



CRC checker with example: here data= 100100, divisor = 1101



As reminder is 000 so there is no error otherwise the data is erroneous.

4. Checksum:

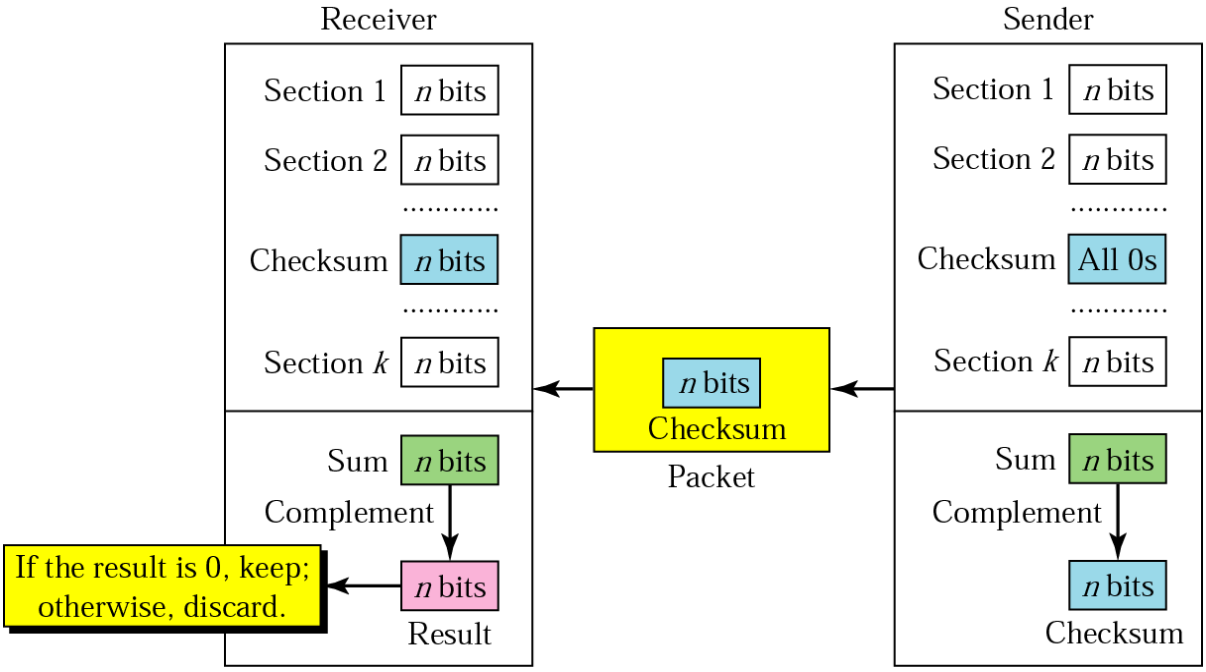
The error detection method used by the higher-layer protocols is called checksum.

The sender (or checksum generator) follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using one's complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

The receiver (or checksum checker) follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using one's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, rejected.



Example

Suppose the following block of 16 bits is to be sent using a checksum of 8 bits.

10101001 00111001

The numbers are added using one's complement

```
                10101001
                00111001
                ----------
Sum             11100010
Checksum        00011101
```

The pattern sent is 10101001 00111001 **00011101**

Example

Now suppose the receiver receives the pattern sent in above Example and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

```
                10101001
                00111001
                00011101
Sum             11111111
```

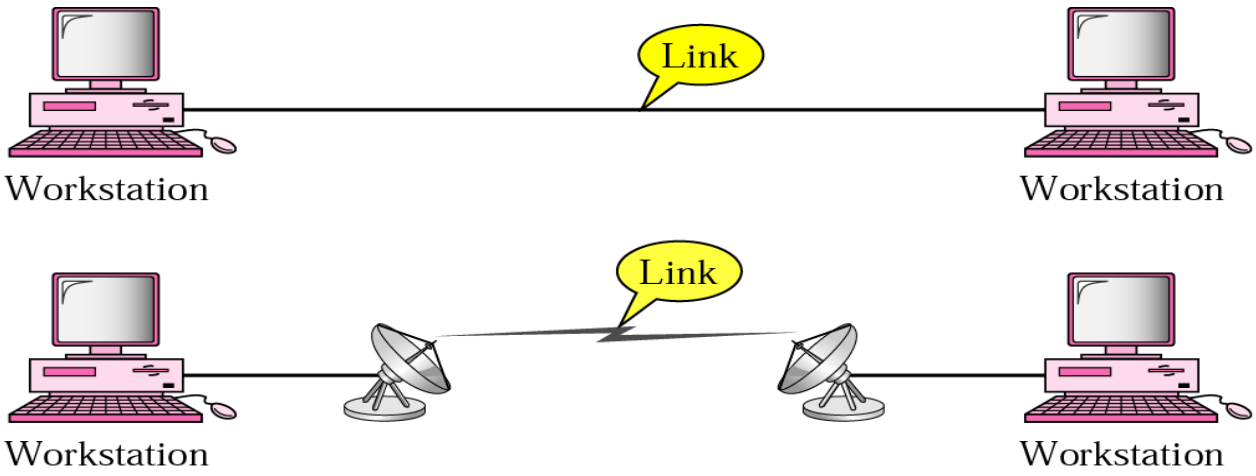
Complement **00000000** means that the pattern is OK

LINE CONFIGURATION

Line configuration refers to the way two or more communication devices attached to a link. There are two possible line configuration or physical connection: point-to-point and multipoint connection.

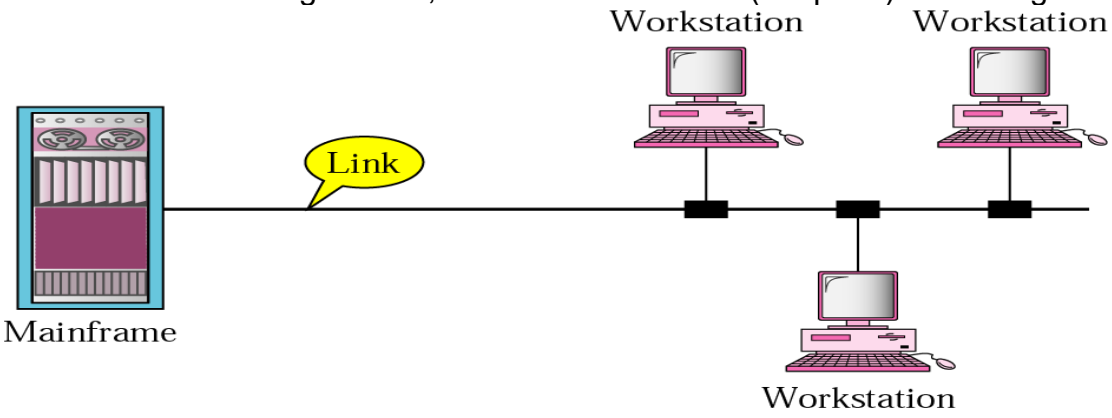
1. **Point-to-point connection:**

- A Point-to-point connection Provides a dedicated link between two devices.
- Entire capacity of the link is reserved for those two devices.
- Connection between infrared remote control and Television set is an example of Point-to-point connection.



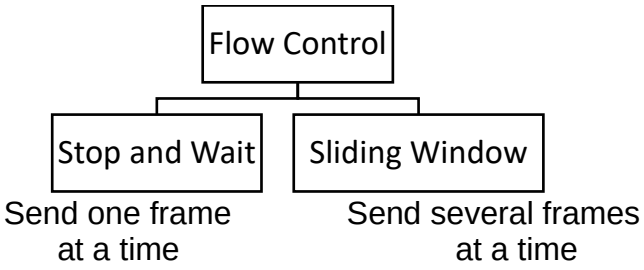
2. Multipoint connection/ multidrop:

- Multipoint connection is More than two specific devices share a single link.
- Capacity of channel is shared, either spatially or temporally.
- It is also called Multidrop configuration.
- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration



FLOW CONTROL

- Flow Control is a mechanism or a set of procedures to tell the sender that how much data it can transmit before waiting for acknowledgment.
- The data link layer is responsible for flow control.
- There are 2 methods for controlling the flow of data.



Stop and Wait

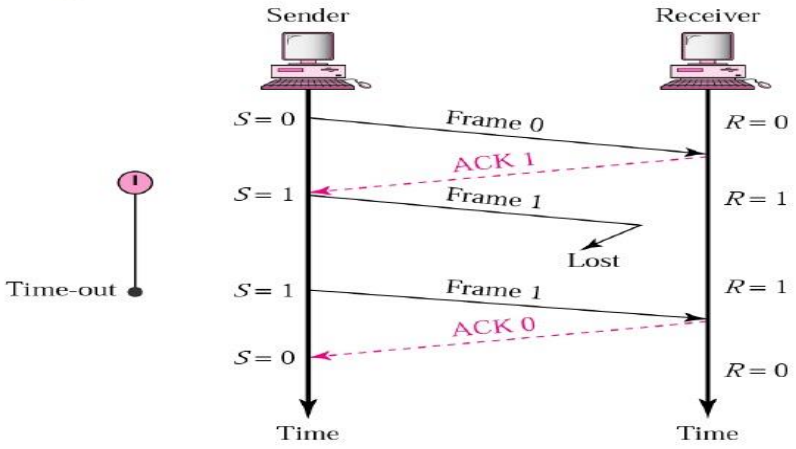
- In Stop and Wait flow control method the sender waits for the acknowledgment after every frame it sends.
- When it receives an acknowledge it transmit the next frame.
- If a frame is not received by the receiver, an acknowledgement cannot be given. So the next cannot be sent.
- So the sender uses the timer to send the data.
- After a particular time if the sender does not receiver the acknowledgement the data is again retransmitted.

Advantage

- It is simple to implement.

Disadvantage

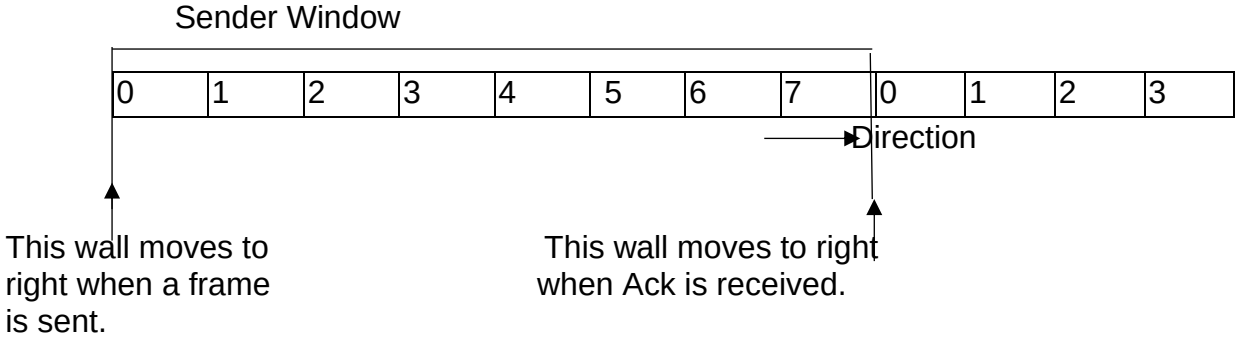
The disadvantage is inefficiency i.e. it is very slow.



Sliding Window

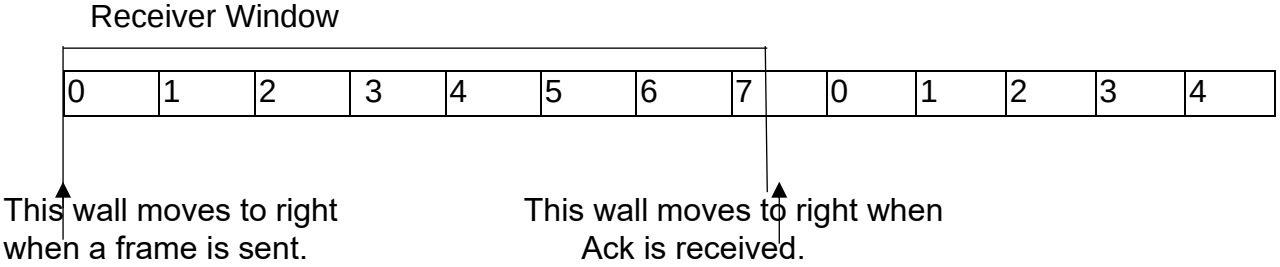
- In sliding window method of flow control the sender can transmit several frames before getting an acknowledgement.
- This is a major advantage over stop and wait concept of flow control.
- Here several frames are combined to form a window.
- It uses modulo. n formula for numbering a window that means if the size of the window is n then the frames are numbered from 0 to n-1.
- Here the acknowledgement number is the next frame it expects to receive next.
- The sliding window of the sender shrinks from the left when frames of data are sent and expands to right when acknowledgement is received.

Sender Sliding Window



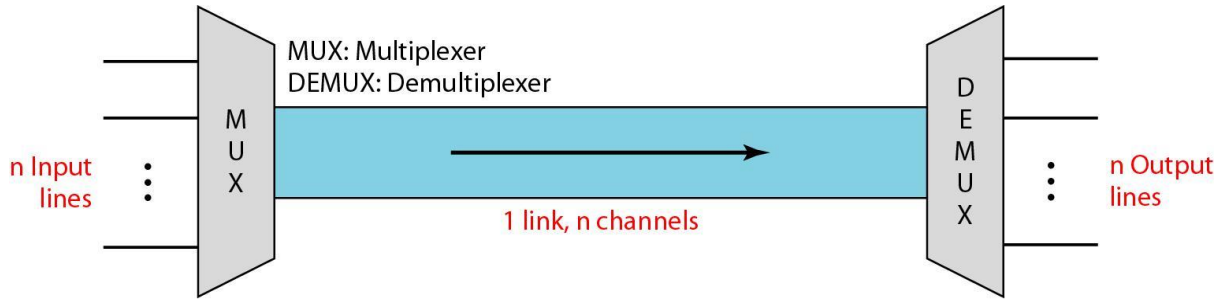
The sliding window of the receiver shrinks from the left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgment are sent.

Receiver Sliding Window



MULTIPLEXING

- Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.
- It the transmission capacity of a link is greater than the transmission needs of the devices connected to it, then the excess capacity is wasted. At that case multiplexing is used.
- In a multiplexed system, n no. of devices share the capacity of one link.



- The lines on the left direct their transmissions stream to a multiplexer, which combines them into a single stream.
- At the receiving end, that stream is fed into a demultiplexer, which separates the stream back into its component transmission(one to many) and directs them to their intended receiving devices.

CATAGORIES OF MULTIPLEXING TECHNIQUES:-

There are three basic multiplexing techniques

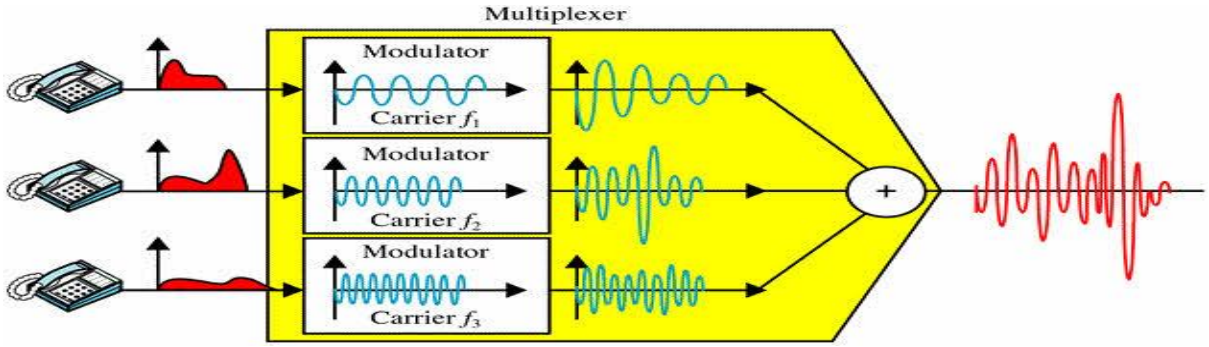
1. Frequency-division-multiplexing(FDM)
2. Wave-division-multiplexing(WDM)
3. Time-division-multiplexing

FREQUENCY-DIVISION-MULTIPLEXING(FDM):-

- FDM is an analog technique that can be applied when the bandwidth of a link as greater than the combined bandwidth of the signals to be transmitted.
- In this technique the signals generated by each sending device modulate different carrier frequencies.
- These modulated signals are then combined into a single composite single that can be transmitted by the link.
- Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal.
- FDM as not only used for analog signals but also for digital signal.But for this digital signals must be converted to analog signal before multiplexing.

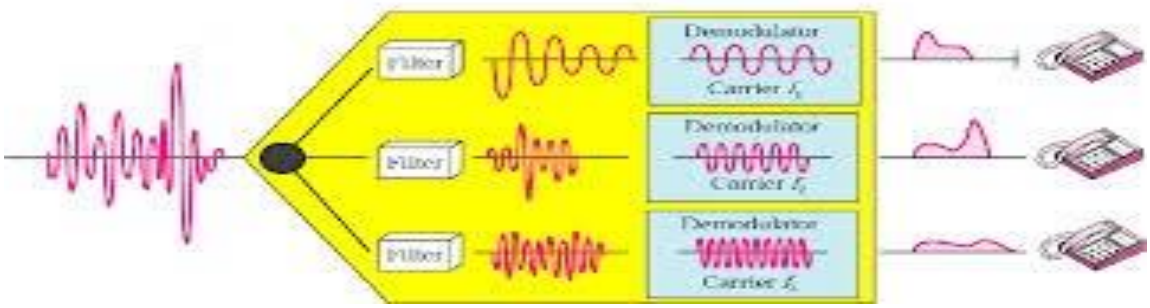
Multiplexing process:-

- Each source generate a signal of same frequency range. Inside the mux, these similar signals modulate different carrier frequencies.
- The resulting modulate signals are combined into a single composite signal that is transmitted over a link which has enough bandwidth to accommodate it.



Demultiplexing process: -

- The DEMUX uses a series of filters to decompose the multiplexed signals into its constituent component signals.
- The individual signals are then passed to a demodulator that separates them from their carrier and passes them to the output lines.

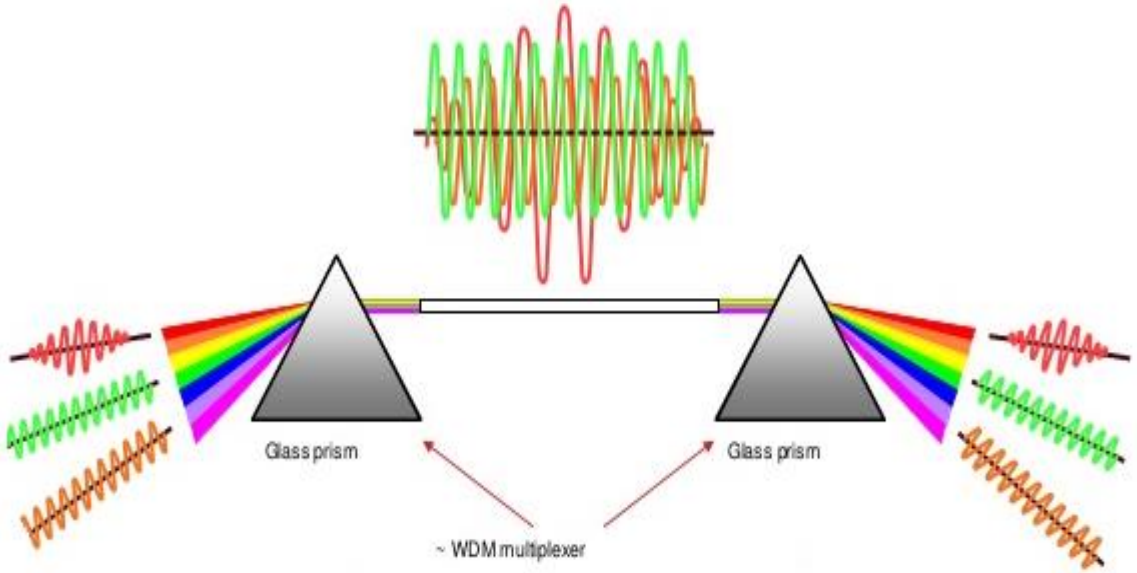


Application of FDM:-

A very common application of FDM is radio broadcasting and also FDM is used for television broadcasting.

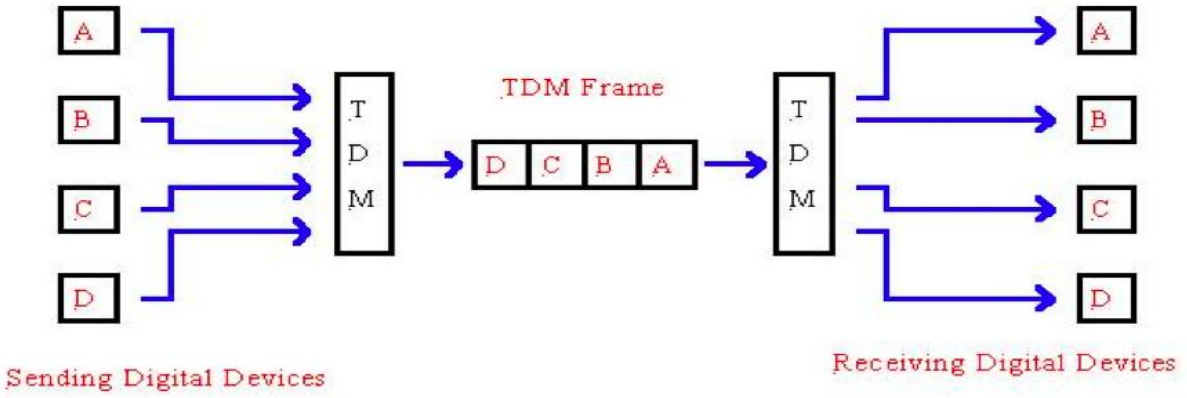
WAVE-DIVISION-MULTIPLEXING(WDM):-

- WDM is designed to use the high data rate capability of fibral-optic cable.
- The optical fibra data rate is higher than the data rate of metallic transmission cable. Using fibra optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.
- Conceptually WDM is same as FDM but the multiplexing and demultiplexing technique involve optical/light signals transmitted through fibra optic cables.
- In WDM technique we want to combine multiple light source into one single light at the MUX and so the reverse at DEMUX.
- The combining and splitting of light sources are handled by prism.
- Using WDM technique, a MUX can be made to combine several input beams of light, each containing a narrow band frequencies into one output beam of wider band frequencies . A DEMUX can also be made to reverse the process.



TIME-DIVISION-MULTIPLEXING:-

- Time division multiplexing is a digital process that allows several connection to share the bandwidth of a link.
- In FDM a portion of bandwidth is shared but in TDM time is shared.
- Each connection occupies a portion of the time in link.
- TDM is a digital multiplexing techniques. Digital data from different sources are combined into one time shared link.

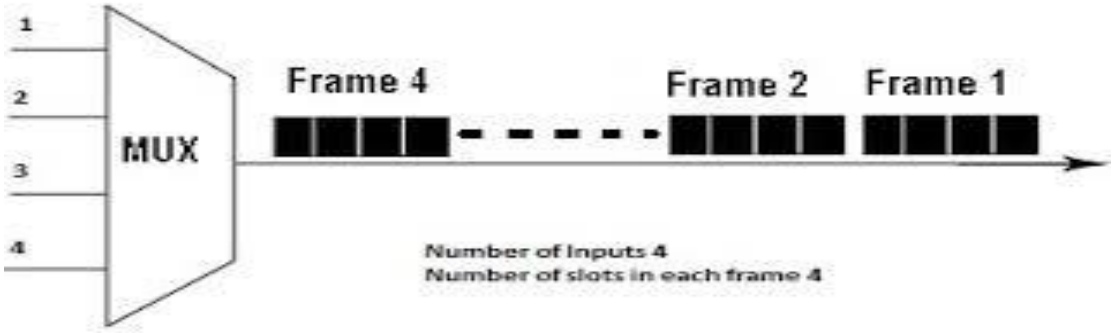


interleaving:-

- TDM can be visualized as to fast rotating switches, one on the multiplexing side and other on the demultiplexing side.
- The switches are synchronized and rotate at the same speed, but in opposite direction.
- When the switch opens in front of a device, that device has the opportunity to send data into the path.
- The switch moves from device to device at a constant rate and in a fixed order. This process is called as interleaving.
- TDM can be divided into two types:-
  1.Synchronous Time-division-multiplexing
  2.Asynchronous Time-division-multiplexing

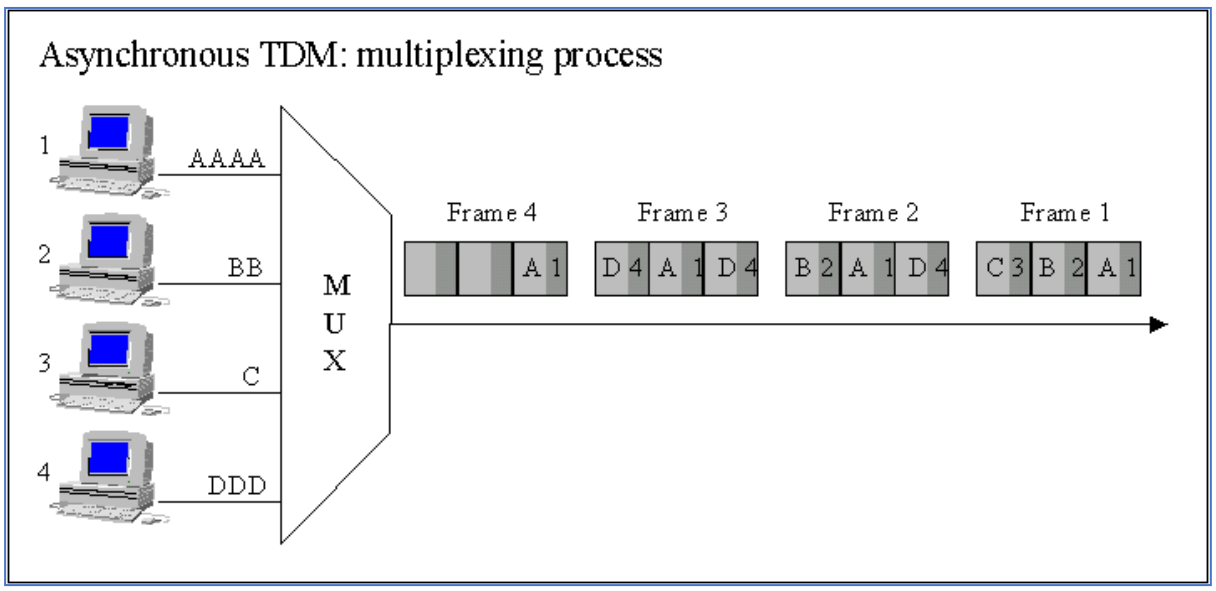
SYNCHRONOUS TDM :-

- In synchronous TDM the multiplexer allocates exactly the same slot to each device at all times even if a device has not anything to transmit.
- The time slots are grouped into frames.
- It we have n connection the frame is divided into n time slots and one slot is allocated for each unit, for each input line.
- In a system with n input lines, each frame has n slots, with each slot is allocated to carrying data from a specific input line.



ASYNCHRONOUS / STATISTICAL TDM:-

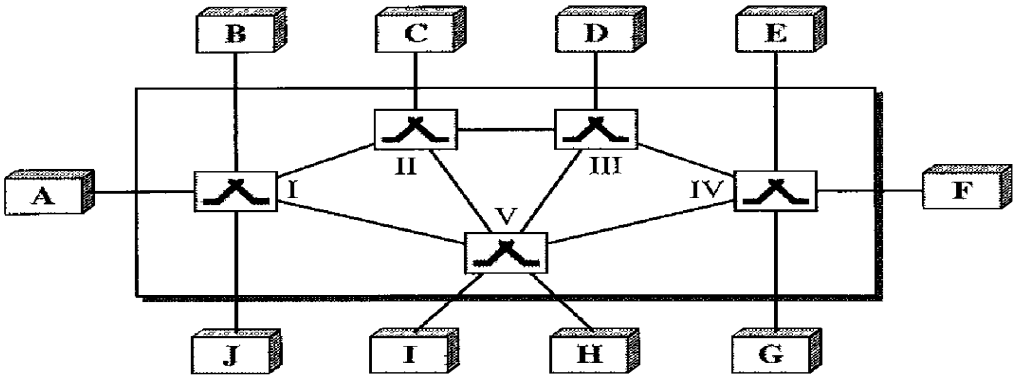
- Asynchronous TDM/ Statistical TDM is designed to avoid the waste in synchronous TDM.
- In synchronous TDM there may be a device attached which may not sending data. So the slot for that device remains empty., So the maximum utilization of link is not used efficiently.
- In asynchronous TDM, the number of slots in each frame is less than the number of input lines.
- The MUX checks each input line in round robin manner that means it allocated a slot for an input line if the line has data to send.
- Otherwise, it skips the line and checks for the next lines.



CHAPTER -5
SWITCHING & ROUTING

SWITCHING:

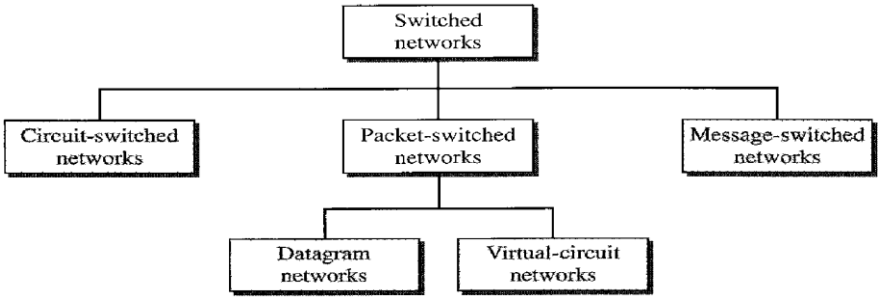
- A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- The process by which data are transmitted from one node to the other via a switched network is called switching.



The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

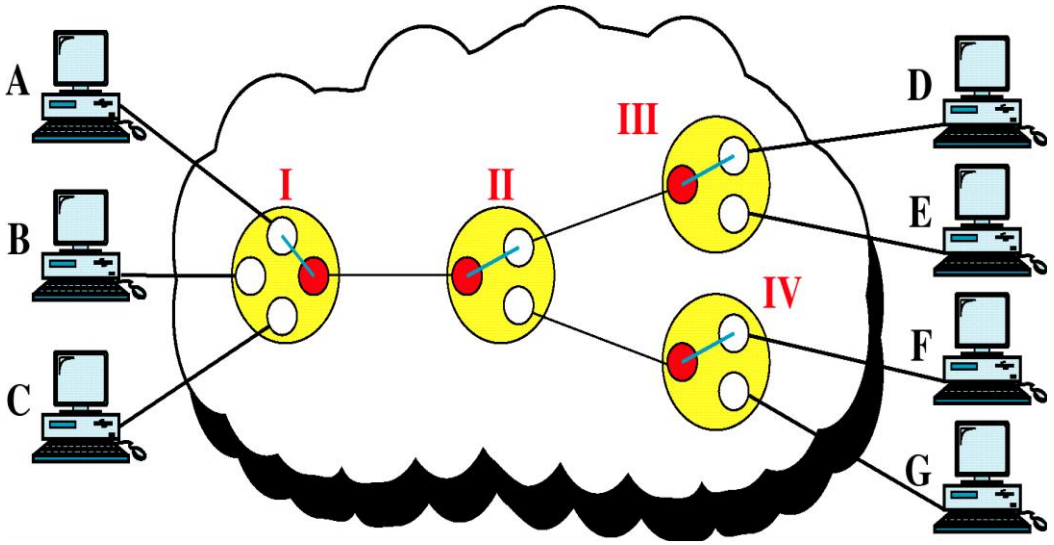
TYPES:

1.Circuit switching
2.Packet switching
3.Message switching.



CIRCUIT-SWITCHED NETWORKS

- **A** circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- However, each connection uses only one dedicated channel on each link. Each link is normally divided into *n* channels by using FDM or TDM.
- Circuit switching takes place at the physical layer.
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and receive by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used .



Three Phases

The actual communication in a circuit-switched network requires three phases: connection **setup, data transfer, connection teardown.**

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

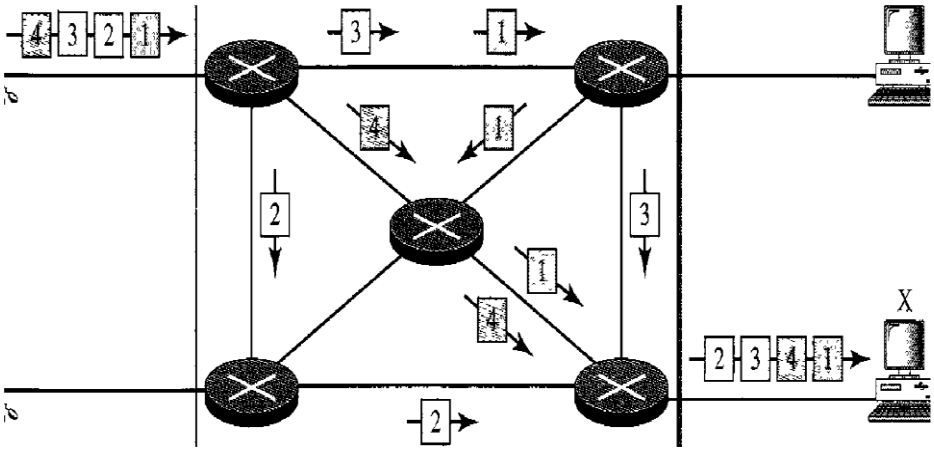
PACKET SWITCHED NETWORK

- In this switching network data are transmitted in discrete units called as packets.
- The problems associated with circuit switching like non voice and data transmission problem was successfully overcome in packet switching.
- In packet switching there is no resource allocation for the packets. The allocation is done on first come first serve basis.
- There are two popular approaches for packet switching.
    1) **Datagram approach**
    2) **Virtual circuit approach**

DATAGRAM NETWORKS

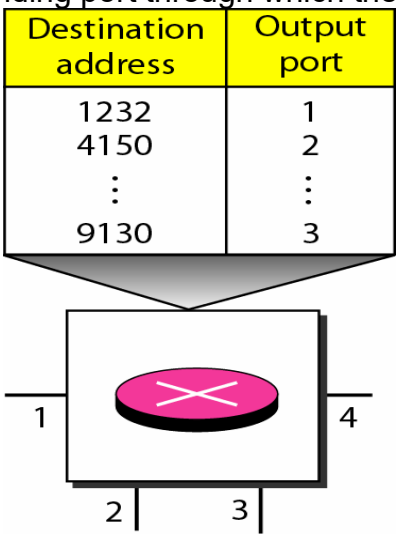
- In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as data grams.

- Datagram switching is normally done at the network layer.
- The switches in a datagram network are traditionally referred to as routers.
- The datagram networks are sometimes referred to as connectionless networks. The term *connectionless* here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.



Routing Table

- Each packet switch has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.
- The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.
- When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.



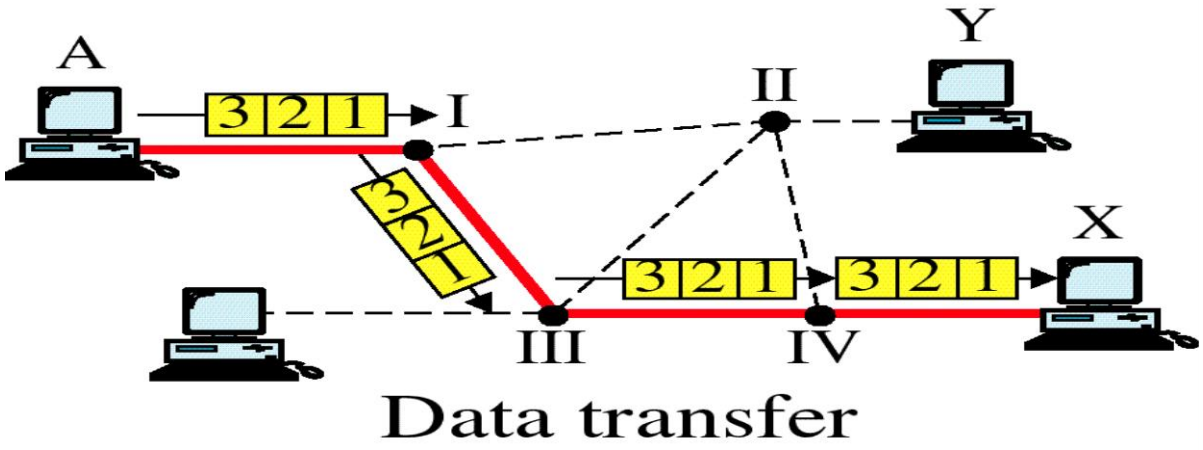
Efficiency

- Better than that of a circuit-switched network.
- Resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.
- Switching in the Internet is done by using the datagram approach to packet switching at the network layer

VIRTUAL-CIRCUIT NETWORKS

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a circuit-switched network, all packets follow the same path established during the connection.

- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.



Data transfer

Addressing In a virtual-circuit network,

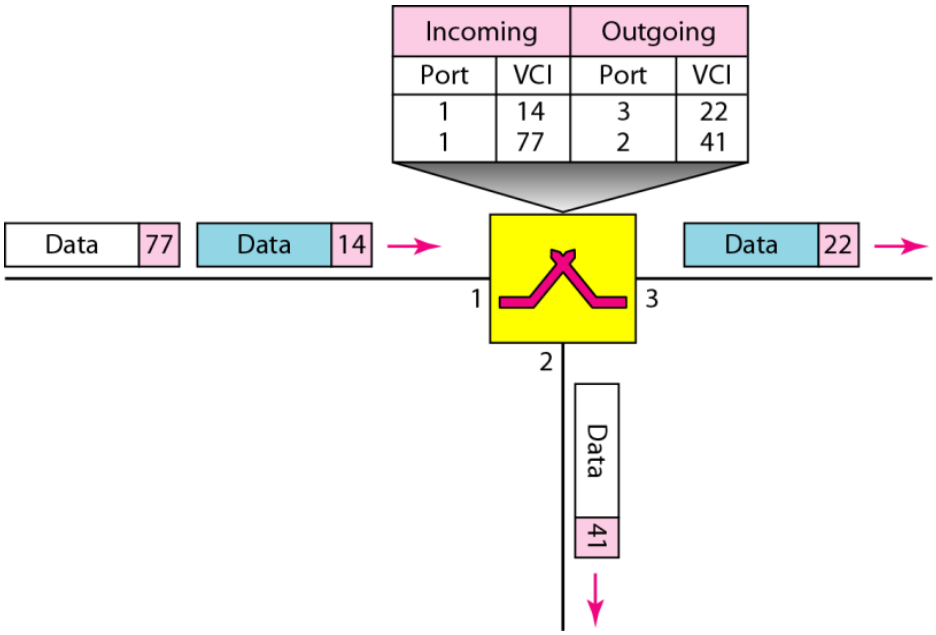
It has two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing:

A source or a destination needs to have a global address, an address that can be unique in the scope of the network or internationally if the network is part of an international network.

Virtual-Circuit Identifier:

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves it has a different VCI.



Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

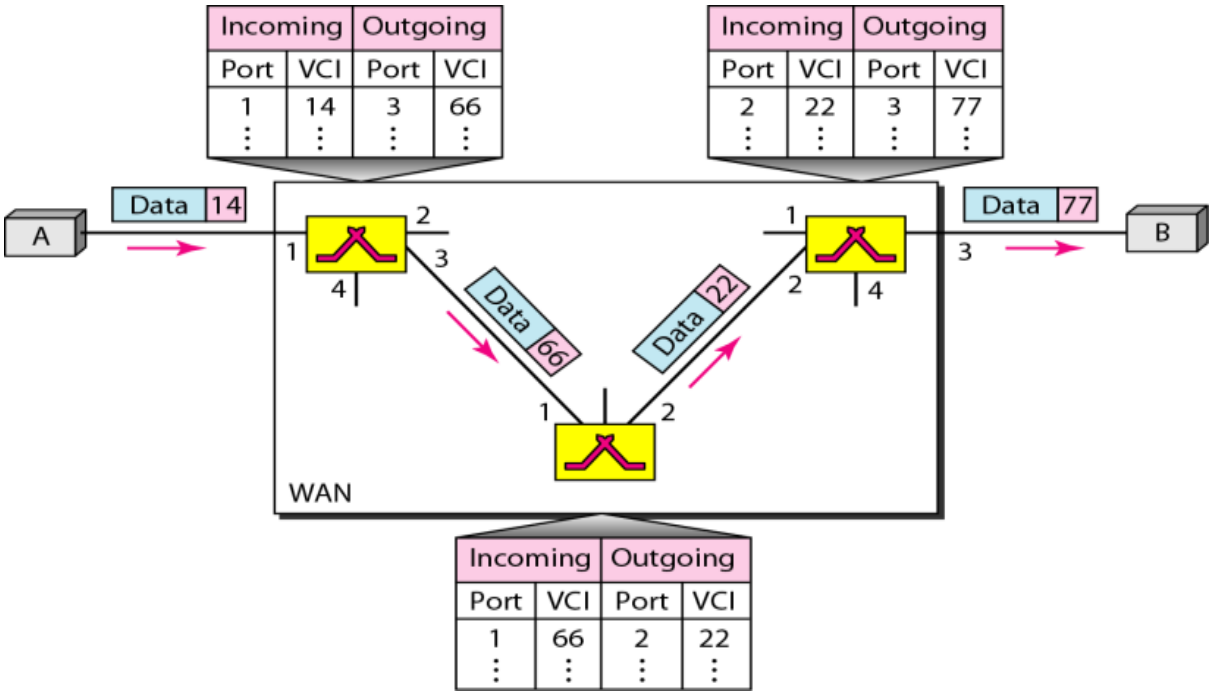
Setup phase

In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

Data Transfer Phase and teardown phase

- To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit.

- The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up.
- The data transfer phase is active until the source sends all its frames to the destination. The process creates a virtual circuit, not a real circuit, between the source and destination.
- After sending all frames, a special frame is send to end the connection
- Destination B responds with a teardown confirmation frame



Differences between Circuit switching and Packet switching

CIRCUIT SWITCHING	***PACKET SWITCHING***
1. In circuit switching a message path or data communication path or channel or circuit is dedicated to an entire message .	1. In this switching network data are transmitted in discrete units called as packets.
2. Circuit-switching is more reliable than packet-switching	2. Packet-switching is less reliable than circuit-switching
3.circuit switching statically reserves the required bandwidth	3.packet switching acquires & releases it as it is needed
4. In circuit switching, path is dedicated for the transmission.	4. In packet switching, route can be shared for different transmission.
5. With circuit switching any unused bandwidth on a allocated circuit is just wasted.	5. with packet switching any unused bandwidth may be utilized by other packets
6. Circuit switching is old and expensive.	6. Packet switching is more modern.

Difference between datagram and virtual circuit approach

Datagram	Virtual circuit
Connection setup is not required	Connection setup is initially required prior to sending data
Packet contains full source and destination address	Packet contains short virtual circuit number identifier.
None other than router table containing destination network	Each virtual circuit number entered to table on setup, used for routing.
Packets routed independently	Route established at setup, all packets follow same route.
It does not affect if any router Fails except those packets lost during crash.	All virtual circuits passing through failed router terminated.
Difficult since all packets routed independently router resource requirements can vary.	Simple by pre-allocating enough buffers to each virtual circuit at setup, since maximum number of circuits fixed.

X.25

X.25 is a protocol suite defined by ITU-T for packet switched communications over WAN (Wide Area Network). It was originally designed for use in the 1970s and became very popular in 1980s. Presently, it is used for networks for ATMs and credit card verification. It allows multiple logical channels to use the same physical line. It also permits data exchange between terminals with different communication speeds.

X.25 has three protocol layers

Physical Layer: It lays out the physical, electrical and functional characteristics that interface between the computer terminal and the link to the packet switched node. X.21 physical implementer is commonly used for the linking.

Data Link Layer: It comprises the link access procedures for exchanging data over the link.

Packet Layer: This layer defines the format of data packets and the procedures for control and transmission of the data packets. It provides external virtual circuit service.

Equipment used

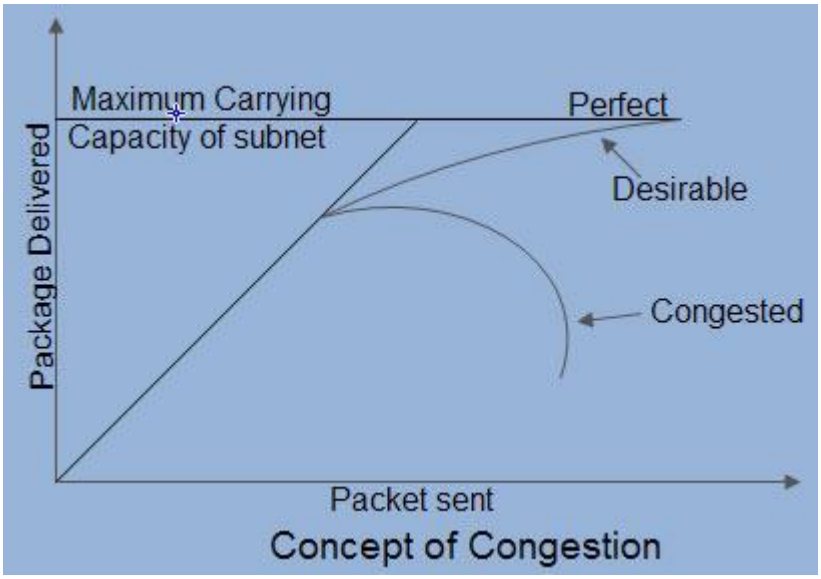
X.21 implementer

DTE − Data Terminal Equipmen

DCTE − Data Circuit Terminating Equipment

Congestion

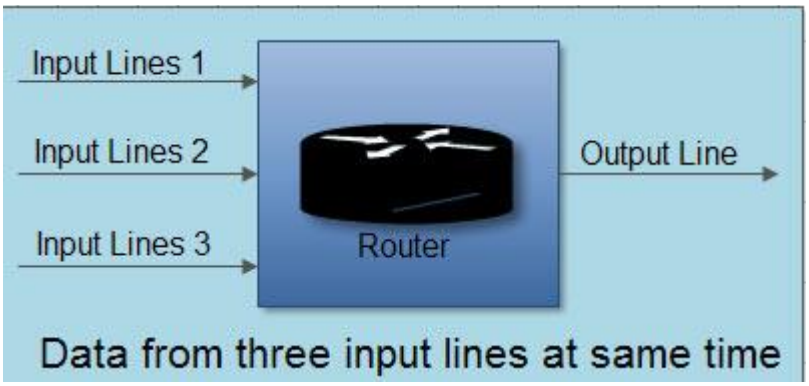
Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network*(i.e.* the number of packets sent to the network) is greater than the capacity of the >] network *(i.e.* the number of packets a network can handle.)



Causing of Congestion:

The various causes of congestion in a subnet are

- The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packet starts arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the problem.

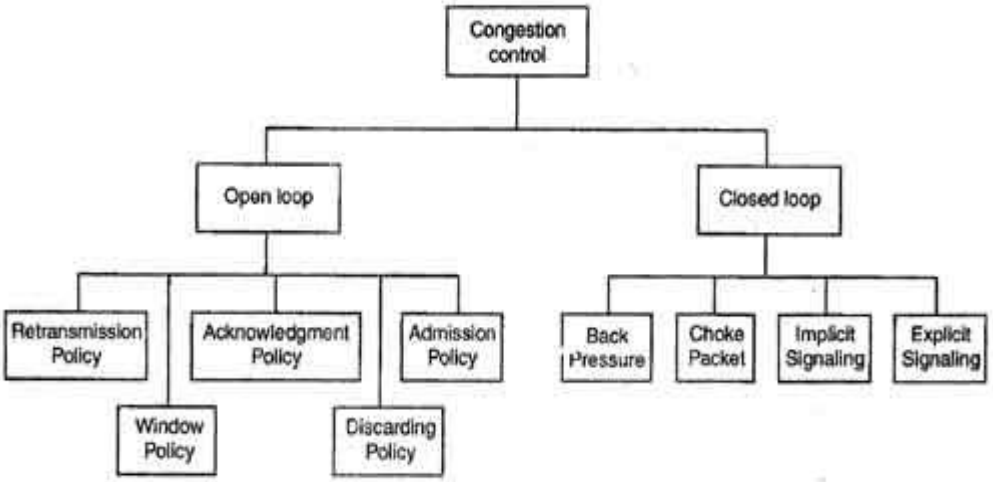


- The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).
- The routers' buffer is too limited.
- Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.
- Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced. Congestion can make itself worse.

Congestion Control Technique

Congestion Control refers to techniques and mechanisms that can either prevent a congestion, before it happens, or remove congestion, after it has happened.

Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Types of Congestion Control Methods

These two categories are:
1. Open loop
2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion control are:

1. Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

• However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

• The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

2. Window Policy

• To implement window policy, selective reject window method is used for congestion control.

• Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.

• Selective reject method sends only the specific lost or damaged packets.

3. Acknowledgement Policy

• The acknowledgement policy imposed by the receiver may also affect congestion.

• If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.

• Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgements we can reduce load on the network.

• To implement it, several approaches can be used:

- A receiver may send an acknowledgement only if it has a packet to be sent.
- A receiver may send an acknowledgement when a timer expires.
- A receiver may also decide to acknowledge only *N* packets at a time.

4. Discarding Policy

• A router may discard less sensitive packets when congestion is likely to happen.

• Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

5. Admission Policy

• An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.

• Switches in a flow first check the resource requirement of a flow before admitting it to the network.

• A router can deny establishing a virtual circuit connection if there is congestion in the "network or if there is a possibility of future congestion.

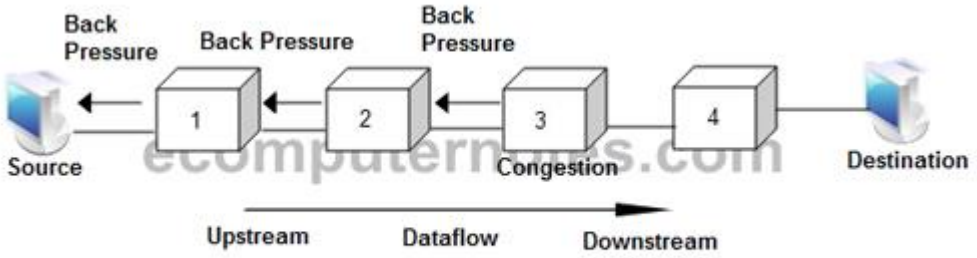
Closed Loop Congestion Control

• Closed loop congestion control mechanisms try to remove the congestion after it happens.

• The various methods used for closed loop congestion control are:

1. Backpressure

• Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.



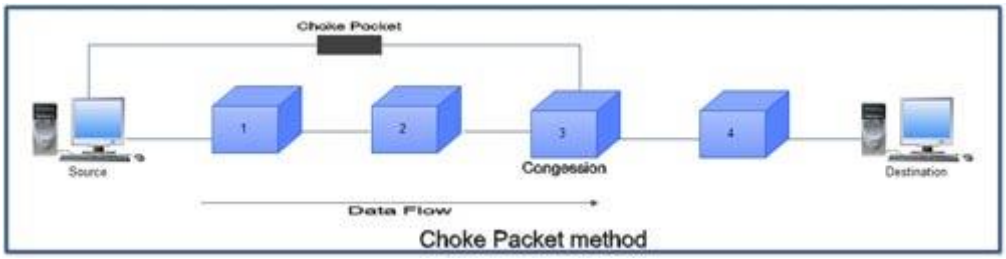
Backpressure Method

2.Choke Packet

• In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.

• Here, congested node does not inform its upstream node about the congestion as in backpressure method.

• In choke packet method, congested node sends a warning directly to the source station *i.e.* the intermediate nodes through which the packet has travelled are not warned.



3. Implicit Signalling

• In implicit signalling, there is no communication between the congested node or nodes and the source.

• The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.

• On sensing this congestion, the source slows down.

• This type of congestion control policy is used by TCP.

4. Explicit Signalling

• In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

• Explicit signalling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signalling method, the signal is included in the packets that carry data .

• Explicit signalling can occur in either the forward direction or the backward direction.

• In backward signalling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slow down.

• In forward signalling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.

REFERENCES

LINKS

https://www.tutorialspoint.com/data_communication_computer_network/physical_layer_switching.htm
https://www.javatpoint.com/computer-network-switching-techniques
https://www.tutorialspoint.com/X-25-and-Frame-Relay

BOOKS

Data Communications and Networking By Behrouz A.Forouzan 4th Edition , TMH
EXPRESS LEARNING Data Communication and Computer Network, ITL Education Solutions limited.

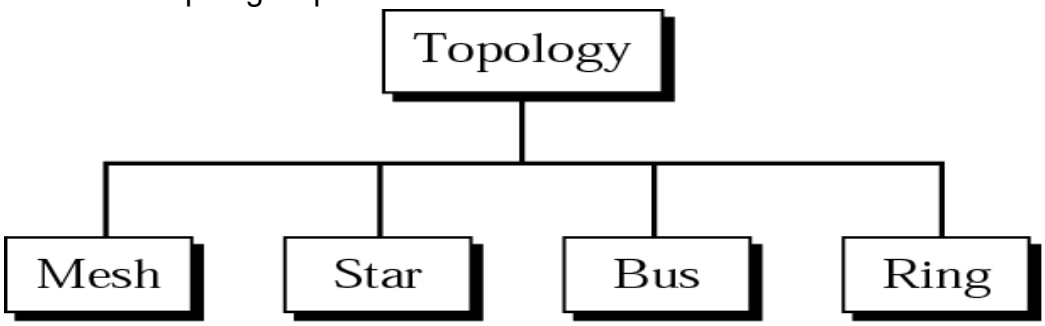
CHAPTER -6
LAN TECHNOLOGY

TOPOLOGY:

- Topology refers to the way in which a network is laid out physically.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Categories of topology:

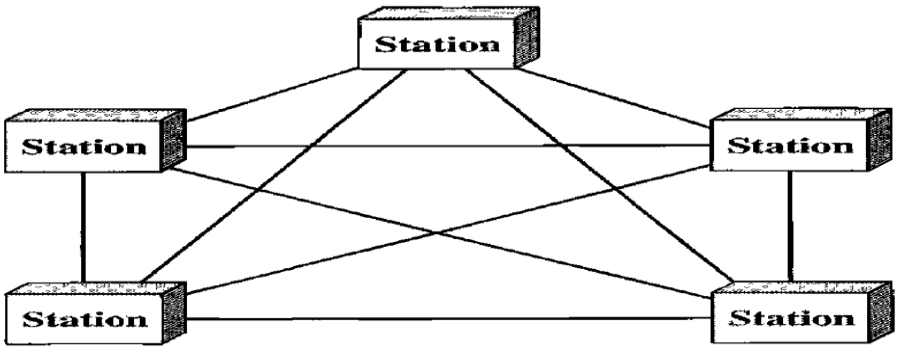
There are four basic topologies possible.



There are two derived topologies: Tree, Hybrid.

1.Mesh topology:

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- A fully connected mesh network therefore has n(n -1) /2 physical channels link n devices.
- To accommodate that many links, every device on the network must have n – 1 input/output (I/O) ports to be connected to the other n - 1 stations.



ADVANTAGES:

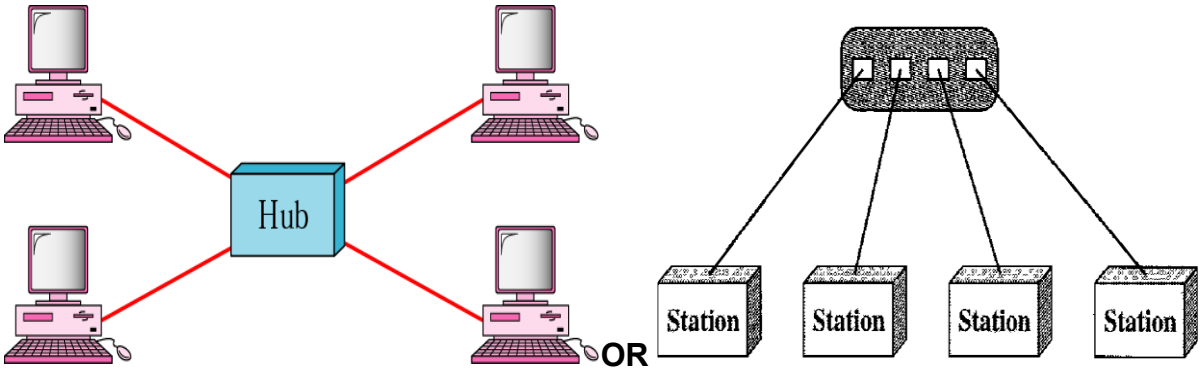
- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.
- A mesh topology is robust. If one link becomes unusable, it does not hamper the entire system.
- There is the advantage of privacy or security.
- Finally, point-to-point links make fault identification and fault isolation easy.

DISADVANTAGES:

- Every device must be connected to every other device, so installation and reconnection are difficult.
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

2.Star Topology:

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



ADVANTAGES:

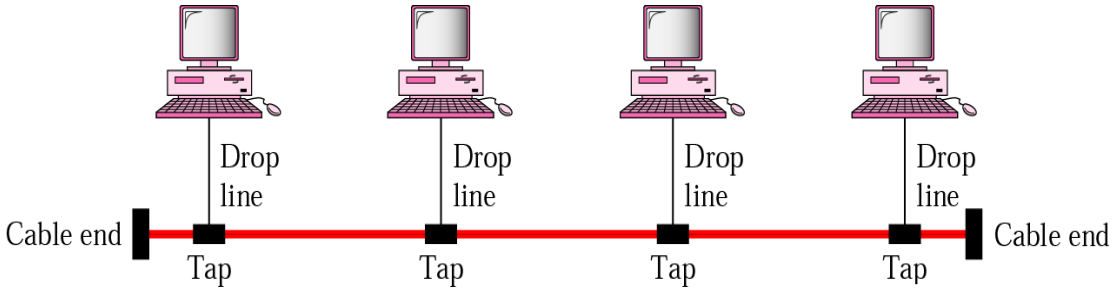
- A star topology is less expensive than a mesh topology.
- It is easy to install and reconfigure.
- Other advantages include robustness
- Easy fault identification and fault isolation.

DISADVANTAGE:

The dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

3.Bus Topology:

- A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



ADVANTAGES

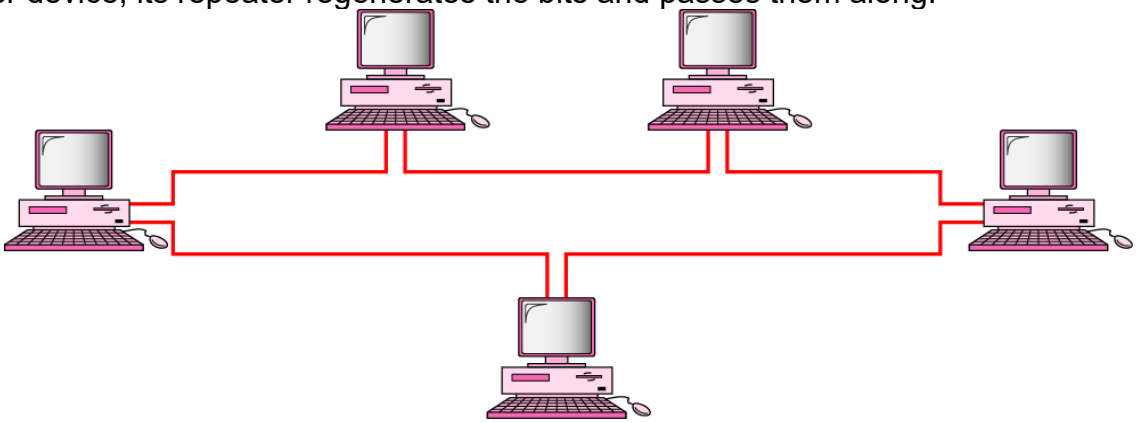
- Advantages of a bus topology include ease of installation
- Bus uses less cabling.

DISADVANTAGES:

- Difficult reconnection and fault isolation is also difficult.
- Signal reflection at the taps can cause degradation in quality.

4.Ring topology:

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



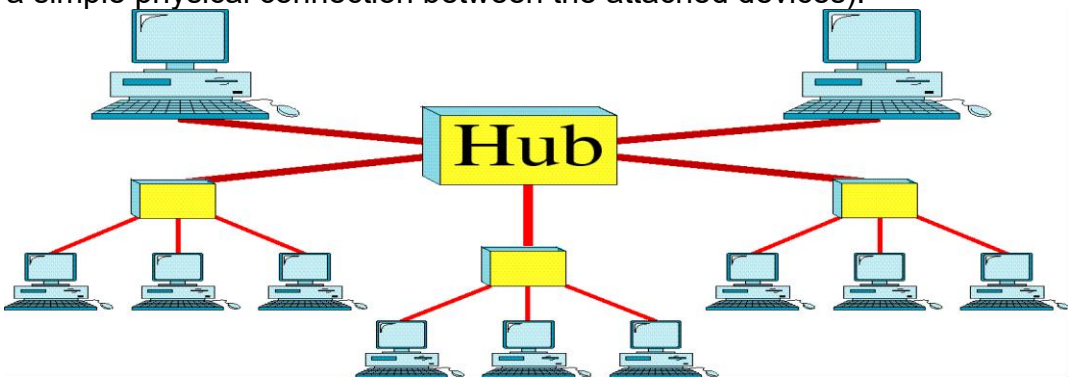
ADVANTAGE:

- A ring is relatively easy to install and reconfigure.
- Fault isolation is simplified.

DISADVANTAGE: Unidirectional traffic can be a disadvantage.

Tree topology:

- A tree topology is a variation of star topology.
- In star, nodes in a tree are linked to a central hub that controls the traffic to the network. However, not every device plugs directly into the central hub.
- The majority of devices connect to a secondary hub that in turn connected to the central hub.
- The central hub in the tree is an active hub (i.e. an active hub contains an repeater which regenerates signal.).the secondary hubs may be active or passive hub(i.e. the passive hub provides a simple physical connection between the attached devices).



Advantage

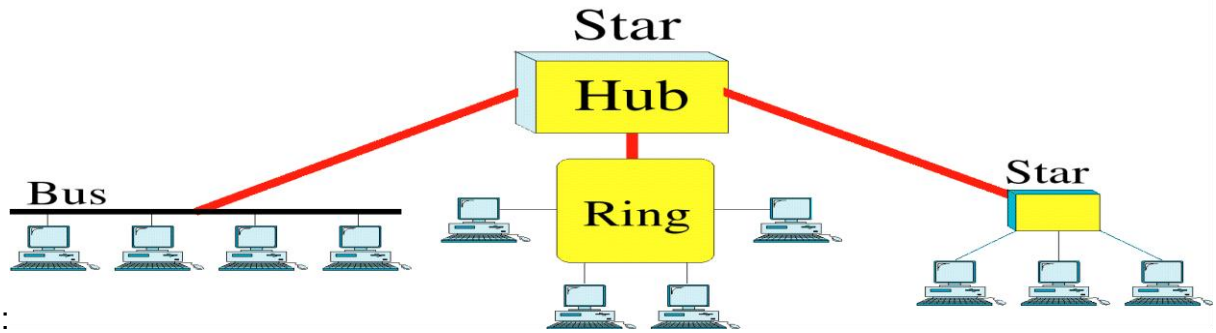
- It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
- It allows the network to isolate and prioritize communication from different computers.

Disadvantage

The dependency of the whole topology on one single point, the central hub. If the central hub goes down, the whole system is dead.

5.Hybrid topology:

Often a network combines a several topologies as subnet works linked together in a larger topology. For example ,one department of a business may have decided to use a bus topology while another department has a ring . The two can be connected to each other via a central controller in a star topology.



:

Transmission Media

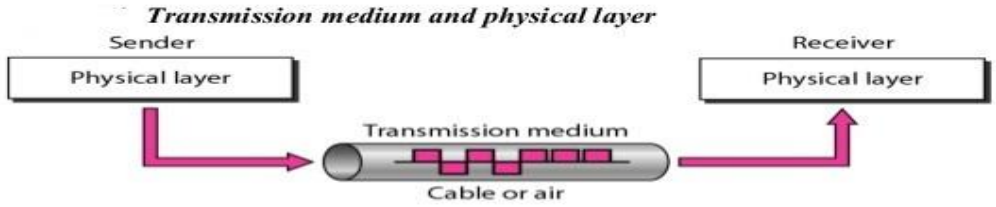
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable or fibre-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

CATEGORIES:

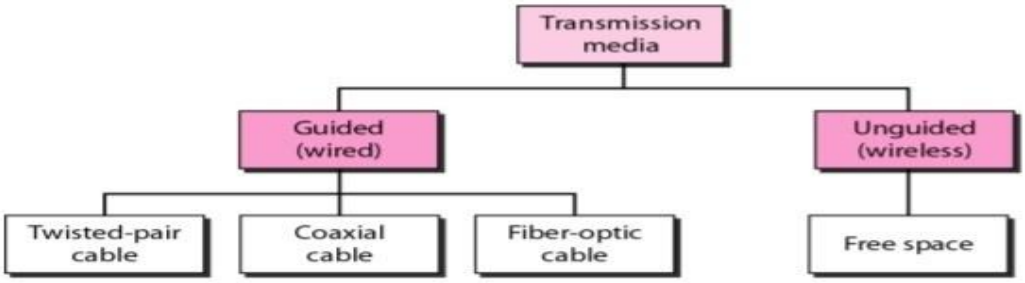
In telecommunications, transmission media can be divided into two broad categories:

1.guided

2. unguided.



Classes of transmission media

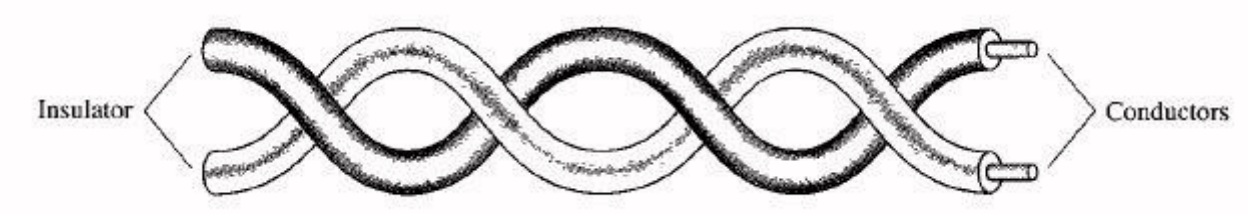


GUIDED MEDIA:

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fibre-optic cable.

- A signal traveling along any of these media is directed and contained by the physical limits of the medium.
- Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current.
- Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable



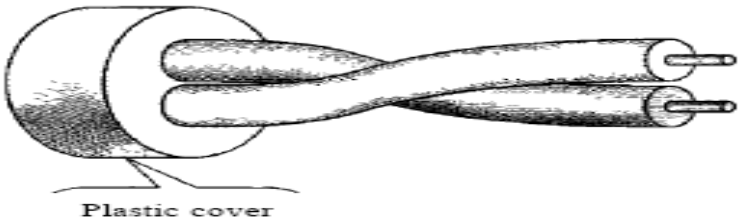
A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

CATEGORIES/TYPES/KINDS:

3. Unshielded twisted Pair Cable (UTP)
4. Shielded Twisted-Pair Cable (STP)

1.Unshielded twisted Pair Cable (UTP):



- The most common twisted-pair cable used in communications is referred to as Unshielded twisted-pair (UTP).
- It consists of two conductors usually copper which is covered by plastic insulator.
- Two wires are twisted one over the other at regular interval to decrease the noise and disturbances. So that at the receiving end the receiver will get the desired information.

ADVANTAGES:

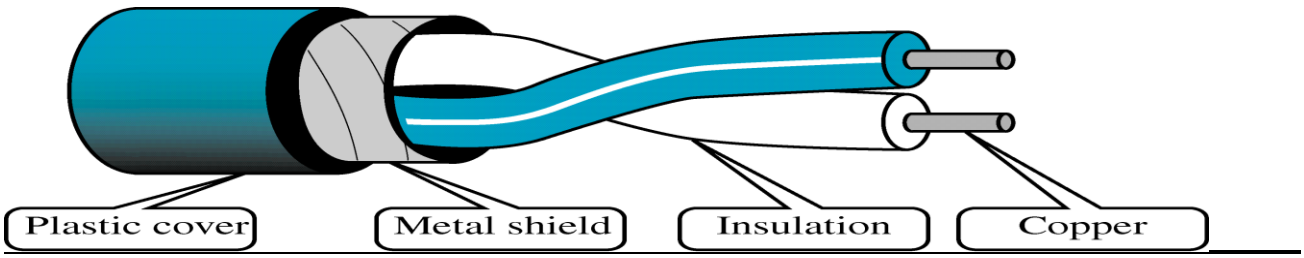
- It is easy to use and flexible.
- It is cheap.
- It is easy to install.

APPLICATIONS:

Is used in telephone lines to provide voice and data channels.

The most commonly used connecter is RJ 45 (Register jack).

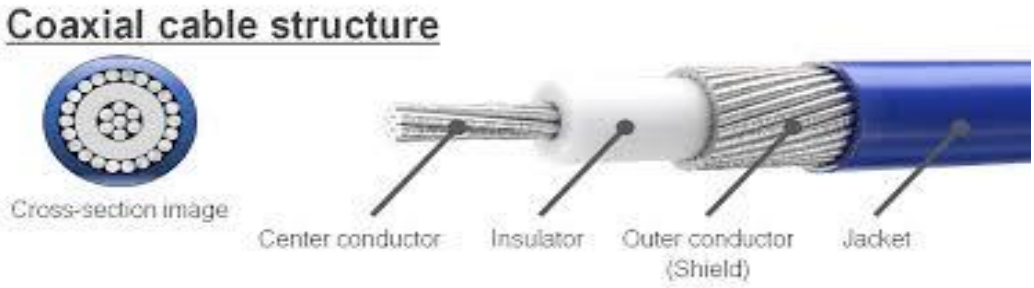
2.Shielded Twisted-Pair Cable (STP):



- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- It eliminates crosstalk.
- Here the metal foil is connected to the ground and other connection are same as UTP.

Coaxial Cable:

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is
- Protected by a plastic cover.
- Coax carries signals of higher frequency ranges (i.e. 100 KHz – 500MHz) than those in twisted pair cable, in part because the two media are constructed quite differently.
- Coaxial cables categorized by their radio government (RG) ratings.

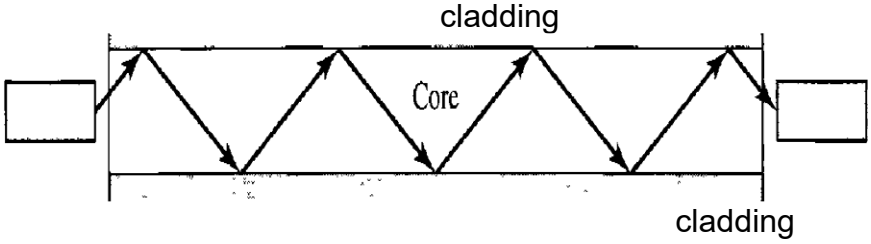


APPLICATION:

- Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
- Cable TV networks also use coaxial cables.
- Another common application of coaxial cable is in traditional Ethernet LANs.
- Connectors used: Barrel connector, T-connector, Terminator

FIBER OPTICS CABLE:

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

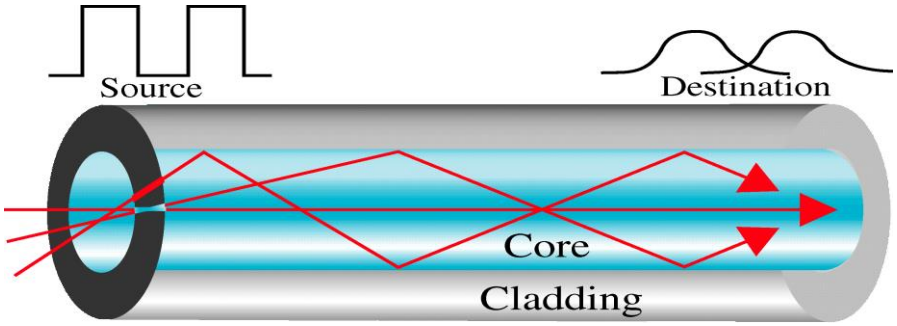


Propagation Modes:

- Current technology supports two modes -multimode and single mode for propagating light along optical channels, each requiring fiber with different physical characteristics.
- Multimode can be implemented in two forms:
  - step-index
  - graded-index.

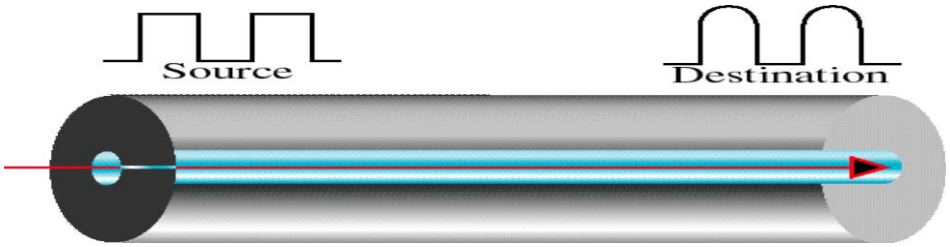
Multimode:

Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core.



Single-Mode:

- Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.
- The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction).
- The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible.
- All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.



Applications:

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is Cost-effective.
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

  Advantages : Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).
- Higher bandwidth.
- Less signal attenuation.
- Noise resistance
- Light weight.

Disadvantages: There are some disadvantages in the use of optical fiber.

- Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- Cost. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.
- Fragility: Glass fiber is more easily broken than wire which makes it less useful, where hardware portability is required.

WIRELESS TRANSMISSION / UNGUIDED TRANSMISSION:-

- Unguided transmission involves the mode of communication by means of electro-magnetic waves without using physical conductor.
- Signals are normally broadcast through free space and the receiver are allowed to capture the signals by using an antenna.

There are three modes of wireless transmission:-

- Earth propagation/ground propagation
- Sky propagation (high frequency)
- Line of sight propagation (very high frequency).

Types of wireless transmission:-

- Radio wave
- Micro wave
- Infra-red

Radio waves:-

- The radio waves are omni-directional.
- When the antenna transmits radio waves they are propagated in all direction.
- It follows sky propagation mode.
- The frequencies it transmits can penetrate the wall.
- It transmits in two ways i.e Amplitude modulation (AM) and frequency modulation(FM).
- The bandwidth of the radio waves is relatively narrow i.e under 1GHz.
- Radio waves are used for multi-cost communication such as radio, television and live streaming.

Micro waves:-

- The electromagnetic waves having frequencies 1-30GHz are known as microwaves.
- These waves are unidirectional.
- When an antenna transmits microwaves they can be narrowly focused.
- This means that sending and receiving antenna need to be aligned.
- Microwaves propagation follows line-of-sight propagation mode.
- It transmits very high frequency range.
- The bandwidth of this propagation is relatively wide. So, sub-bands can be assigned in between them.
- Two types of antenna are used:- a-parabolic dish antenna b-horn antenna.

a:-parabolic dish antenna

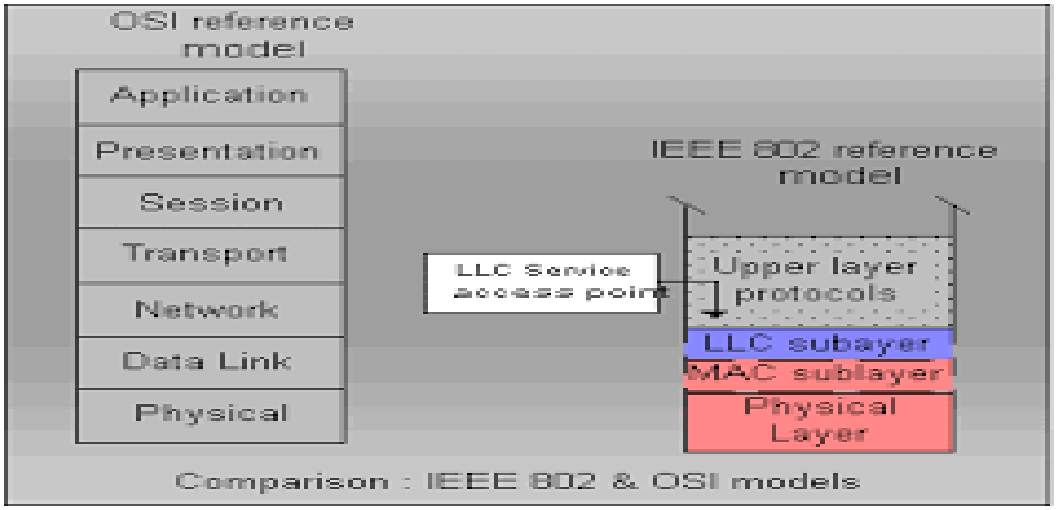
These are used in cellular network and satellite network and also in case of wireless LAN.

Infra-red:-

- Infra-red frequency ranges from (300 GHz-400THz).
- It is used for short range communication.
- These frequencies cannot penetrate any type of obstacles.
- It also works in the mode of line-of-sight propagation.
- For example:- the communication between remote to a device.

LAN protocol Architecture

- In 1985 the computer society of the IEEE started a project 802 ,to set the standards to enable intercommunication.
- It is a way of specifying functions of the physical layer and datalink layer of major LAN protocol.
- The LAN architecture consists of three layers: Physical, MAC (Medium Access Control) and LLC (Logical Link Control).
- LLC provides connection management, if needed. (For most applications, it is not needed.)
- MAC is a protocol for accessing high speed physical links and for transferring data frames from one station to another.
- Physical layer deals mainly with actual transmission and reception of bits over the transmission medium. Its specification depends on the specific physical medium and MAC protocols it interfaces with.



Physical Layer

The physical layer is dependent on the implementation and type of physical media used. This layer has following functions.

- Encoding and decoding of signals
- Preamble generation and removal (for synchronization)
- Bit transmission and reception

Data link layer

- Assemble data into a frame with address and error-detection fields
- Disassemble frame and perform address recognition and error detection
- Govern access to the LAN transmission medium
- Interface to higher levels and performs flow and error control.
- The datalink layer in the IEEE standard is divided into two sublayers: LLC and MAC.
- LLC
- LLC is concerned with transmission of link-level PDU (protocol data unit) between two stations
- LLC is meant for error control, flow control and part of the framing duties message sequencing and message acknowledgement.

MAC

The MAC (Media Access Control) 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:

- ✓ Centralized control
- ✓ Decentralized control

MAC frame format

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

Preamble (7 bytes)	Start of Frame Delimiter (1 byte)	Dest. Address (6 bytes)	Source Address (6 bytes)	Length (2 bytes)	Header+Data	Frame Checksum (4 bytes)

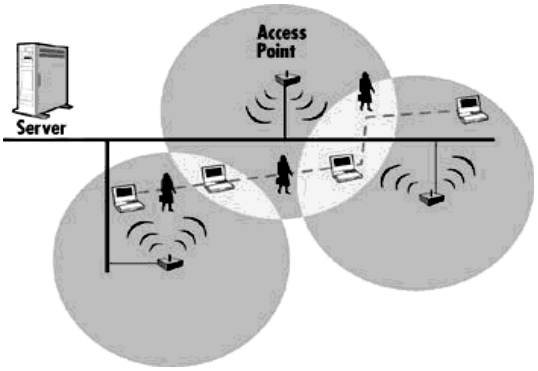
- **Preamble: Each** frame starts with a preamble of 7 bytes, each byte containing the bit pattern 10101010. Manchester encoding is employed here and this enables the receiver's clock to synchronize with the sender's and initialise itself.
- **Start of Frame Delimiter: This** field containing a byte sequence 10101011 denotes the start of the frame itself.
- **Dest. Address: The** destination address field is 6-byte addresses and contains the physical address of the destination station.
- **Source Address:** The SA field is also 6 bytes and contains the physical address of the sender of the frame.

- **Length:** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field
- **Data: This** field carries data encapsulated from the upper layer protocol.it is a minimum of 46 and a maximum of 500 bytes.
- **Frame Checksum:** It is a 32-bit hash code of the data. If some bits are erroneously received by the destination (due to noise on the cable), the checksum computed by the destination wouldn't match with the checksum sent and therefore the error will be detected. The checksum algorithm is a cyclic redundancy checksum (CRC) kind. The checksum includes the packet from Dest. Address to Data field.

Wireless LAN

- A wireless LAN (WLAN) is a flexible data communication system implemented as either extension or alternative of a wired LAN within a building or campus. So it combines data connectivity with user mobility.
- A WLAN is a local area network that doesn't rely on wired Ethernet connections. It uses electromagnetic waves for data transmission. It has data transfer speeds of up to 54Mbps.
- A WLAN signal can be broadcast to cover an area ranging in size from a small office to a large campus. Commonly, a WLAN access point provides access within a radius of 65 to 300 feet.

How WLANs Work



- In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard Ethernet cable.
- Each access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure.
- A single access point can support a small group of users and can function within a range of several hundred feet.
- The client computer or USER access the WLAN through wireless LAN adapters, which are installed in the PC or LAPTOP.
- The WLAN adapter acts as an interface between the computer and the AP.

WLAN standards

Several standards for WLAN hardware exist:

WLAN standard	Pros	Cons
802.11a	• Faster data transfer rates (up to 54Mbps) • Supports more simultaneous connections • Less susceptible to interference	• Short range (60-100 feet) • Less able to penetrate physical barriers
802.11b	• Better at penetrating physical barriers • Longest range (70-150 feet) • Hardware is usually less expensive	• Slower data transfer rates (up to 11Mbps) • Doesn't support as many simultaneous connections • More susceptible to interference

802.11g	• Faster data transfer rates (up to 54Mbps) • Better range than 802.11b (65-120 feet)	• More susceptible to interference
802.11n	• The 802.11n standard is recently certified by the Institute of Electrical and Electronics Engineers (IEEE), as compared to the previous three standards. Though specifications may change, it is expected to allow data transfer rates up to 600Mbps, and may offer larger ranges.	

Fibre Channel

- A high-speed transmission technology used as a peripheral channel or network backbone.
- Fibre Channel transfers digital data between sources and users of information.
- This digital data represents different types of information like programs, files,graphics,videos and sound.
- Each having its own structure, protocol, connectivity, measures of performance and reliability requirements.
- Fibre Channel is a switched medium that works similar to a telephone network: any user will have a temporary, direct connection that provides the option of the full bandwidth of the Fibre Channel as long as the connection is established.
- Fibre Channel's acknowledgment and flow control supports connection-less traffic by using time division multiplexing.
- Fibre Channel is designed to transport many protocols, such as FDDI, serial HIPPI , SCSI , IPI, and many more that will be listed in the section describing the FC-4 layer.
- The transfer rates of Fibre Channel are currently (133 Mbps,266 Mbps,530 Mbps, and 1 Gbps). However, data rates of 2 to 4 Gbps should be available soon.
- Fibre Channel will allow simultaneous transmission of different protocols over a single optical-fiber pair and it can allow a number of existing services, such as network, point-to-point, and peripheral interfaces, to be accessed over a single medium using the same hardware connection.
- Fibre Channel also provides control and complete error checking.
- The Fibre Channel structure is defined as a multi-layered stack of functional levels, not unlike those used to represent network protocols, although not mapping directly to OSI layers.
- The layers of the Fibre channel standard define the physical media and transmission rates, encoding scheme, framing protocol and flow control, common service, and the upper-level applications interfaces. The five layers are: FC-0,FC-1,FC-2,FC-3,FC-4

Hub

- A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability.
- A Hub basically take the input data from one of the ports and broadcast the information to all the ports connected to the network.
- It used in traditional 10-Mbps Ethernet networks to connect network computers to form a local area network (LAN).

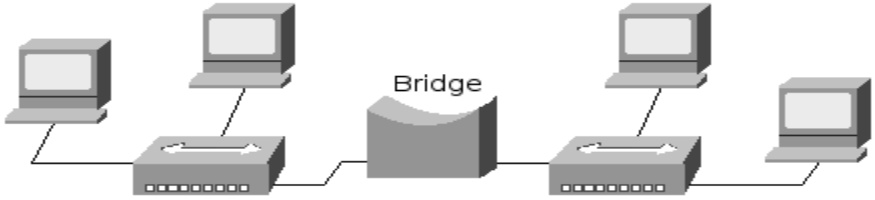
Switch

- A switch is an intelligent device that works in the data link layer.
- The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.
- When a signal enters a port of the switch, the switch looks at the destination address of the frame and internally establishes a logical connection with the port connected to the destination node.
- It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.

Switch

Bridge

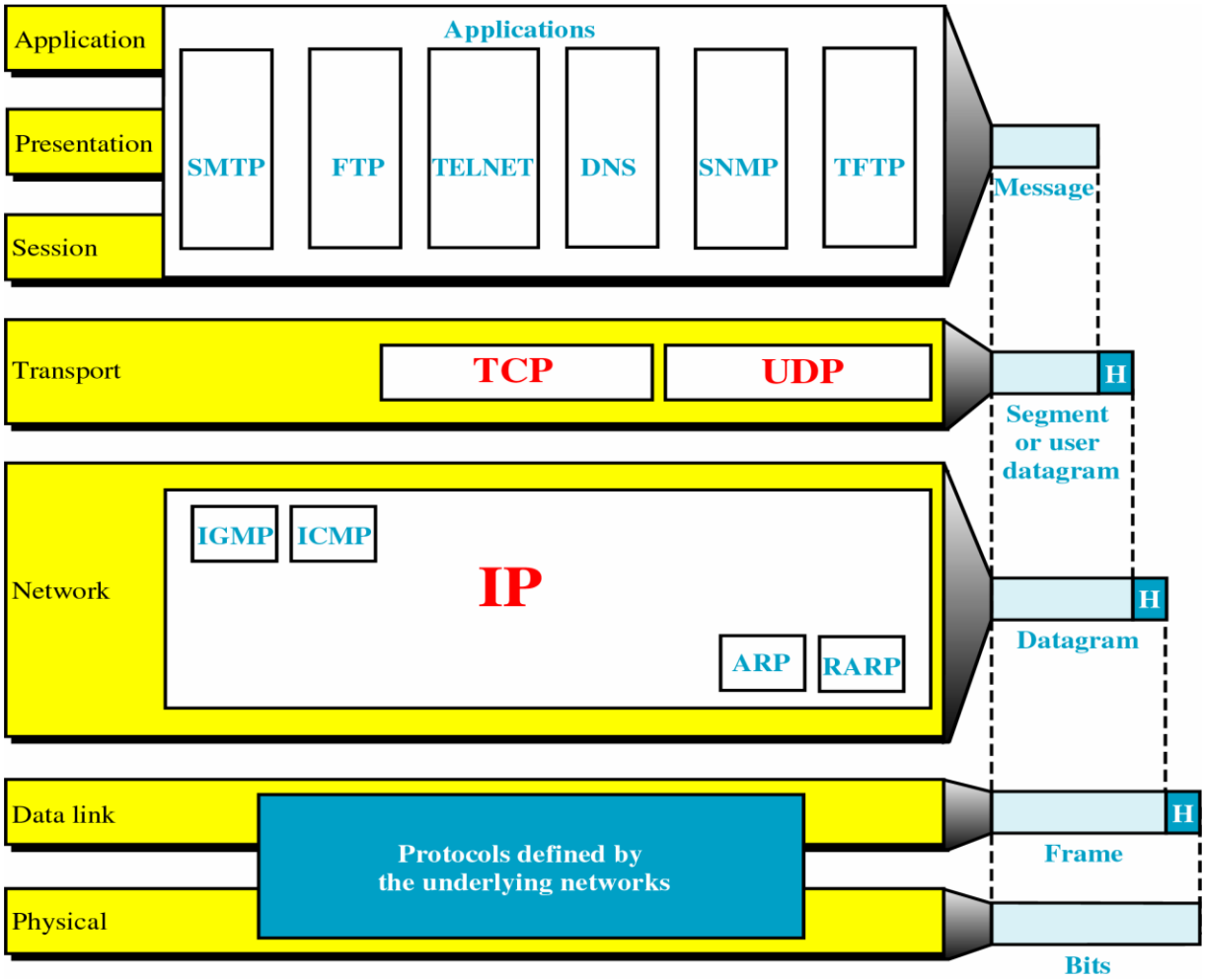
- Bridge operates in both the physical and data link layer of the OSI model.
- Bridges can divide a large network into smaller segments.
- Bridges utilizes the addressing protocol and can affect the flow control of a single LAN.
- This mechanism helps to filter the traffic which leads to control the congestion problem and isolating problem.
- Bridges also provide security through this partitioning of traffic.
- When a frame enters a bridge the bridge not only regenerates the signal but checks the address of the destination and forwards the new copy only to the segment to which the address belongs.
- There are different types of bridge such as –Simple ,multiport and transparent.



CHAPTER -7
TCP/IP

TCP/IP PROTOCOL SUITE

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- It is a set of protocols or a protocol suite that defines how all transmission are exchanged across the internet.
- TCP/IP protocol suite is made of five layers:
  Physical
  Datalink
  Network
  Transport
  Application
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model.
- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.
- It is hierarchical protocol made up of interactive modules, each of which provides a specific functionality.
- However the modules are not necessarily interdependent.



***DESCRIPTION ABOUT LAYERS*:**

1.Physical and Data Link Layers

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

2. Network Layer

At the network layer (or, more accurately, the internetwork layer),TCP/IP supports the Internetworking Protocol, IP. Also it uses four supporting protocols:

ARP, RARP, ICMP, and IGMP

Internetworking Protocol (IP)

- It is the transmission mechanism used by TCP/IP protocol.
- It is an unreliable and connectionless protocol.
- IP transports data in packets called datagrams.
- Each packet transport separately.

Address Resolution Protocol(ARP)

The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address.

Reverse Address Resolution Protocol(RARP)

It allows a host to find its internet address when it know only physical address. It is used when computer connected to n/w first time.

Internet Control Message Protocol(ICMP)

The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.

Internet Group Message Protocol(IGMP)

The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

3. Transport Layer

- Traditionally the transport layer was represented in *TCP/IP* by two protocols**: TCP and UDP.**
- IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.
- But **UDP and TCP** are transport level protocols responsible for delivery of a message from a process (running program) to another process.
- A new transport layer protocol, **SCTP**, has been devised to meet the needs of some newer applications.

User Datagram Protocol(UDP)

- It is a process-to-process protocol That adds only port addresses, checksum error control and length information to the data from the upper layer.
- It is simple & fast but a unreliable connectionless delivery service.

Transmission Control Protocol(TCP)

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

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet.

4.Application Layer

The *application layer* in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model Many protocols are defined at this layer.
They are SMTP,FTP,HTTP,DNS,SNMP,TELNET etc.

SMTP(Simple Mail Transfer Protocol)

It is used to send email from one system to another.

FTP(File Transfer Protocol)

It is used to send an application program(file) to another system. i.e files are transferred from server to client.

HTTP(Hypertext Transfer protocol)

- Used mainly to access data on WWW.
- Used to transfer data in the form of plain text, hypertext, audio, video and so on.

DNS(Domain Name Server or System)

- Provides the protocol that allows clients and server to communicate with each other.
- It allows computer to have names like kp.kiit.edu rather than just IP address like 144.162.120.233.

SNMP(Simple N/W Management Protocol)

It provides a systematic way of monitoring and managing or maintaining an internet or computer n/w.

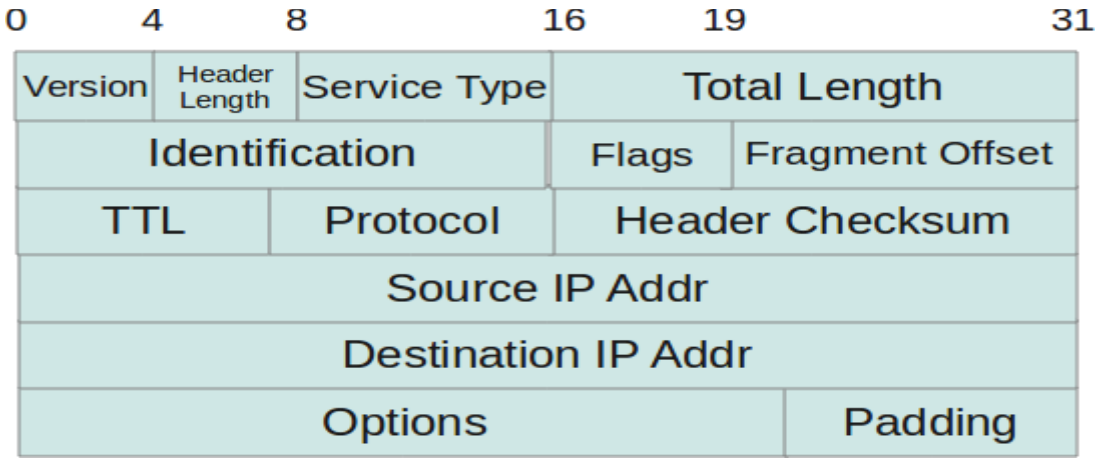
TELNET(Terminal Network)

- It is a client-server application program.
- Responsible for establishment of a connection to a remote system so that the terminal appears as a local terminal at the remote system.

Internet Protocol

- IP protocol is one of the main protocols in the TCP/IP stack.
- It is in the form of IP datagrams that all the TCP, UDP, ICMP and IGMP data travels over the network.
- IP is connection less and unreliable protocol. It is connection less in the sense that no state related to IP datagrams is maintained either on source or destination side and it is unreliable in the sense that it not guaranteed that an IP data gram will get delivered to the destination or not.
- If an IP datagram encounters some error at the destination or at some intermediate host (while traveling from source to destination) then the IP datagram is generally discarded and an ICMP error message is sent back to the source.
- The IP protocol sits at the layer-2 of TCP/IP protocol suite i.e. the Internet layer .

IP Header Format



- ***Protocol Version(4 bits)*** : This is the first field in the protocol header. This field occupies 4 bits. This signifies the current IP protocol version being used. Most common version of IP protocol being used is version 4 while version 6 is out in market and fast gaining popularity.
- ***Header Length(4 bits)*** *:* This field provides the length of the IP header. The length of the header is represented in 32 bit words. This length also includes IP options (if any). Since this field is of 4 bits so the maximum header length allowed is 60 bytes
- ***Type of service(8 bits)*** : The first three bits of this field are known as precedence bits and are ignored as of today. The next 4 bits represent type of service and the last bit is left unused. The 4 bits that represent TOS are : minimize delay, maximize throughput, maximize reliability and minimize monetary cost.
- ***Total length(16 bits)***: This represents the total IP datagram length in bytes. Since the header length (described above) gives the length of header and this field gives total length so the length of data and its starting point can easily be calculated using these two fields. Since this is a 16 bit field and it represents length of IP datagram so the maximum size of IP datagram can be 65535 bytes.
- ***Identification(16 bits)***: This field is used for uniquely identifying the IP datagrams. This value is incremented every-time an IP datagram is sent from source to the destination. This field comes in handy while reassembly of fragmented IP data grams.
- ***Flags(3 bits)***: This 3 bit field contains information that controls fragmentation. An application may choose whether to do fragment to datagram or not.
- ***Fragment offset (13 bits)***: In case of fragmented IP data grams, this field contains the offset(in terms of 8 bytes units) from the start of IP datagram. So again, this field is used in reassembly of fragmented IP datagrams.
- **Time to live (8 bits)** : This value represents number of hops that the IP datagram will go through before being discarded. The value of this field in the beginning is set to be around 32

or 64 (lets say) but at every hop over the network this field is decremented by one. When this field becomes zero, the data gram is discarded. So, we see that this field literally means the effective lifetime for a datagram on network.

- **Protocol (8 bits)** : This field represents the transport layer protocol that handed over data to IP layer. This field comes in handy when the data is demultiplex-ed at the destination as in that case IP would need to know which protocol to hand over the data to.
- **Header Checksum (16 bits)** : This 16 bit field ensure the integrity of header value A checksum on the header only. Since some header fields change (e.g., time to live), this is recomputed and verified at each point that the internet header is processed.
- **Source and destination IP(32 bits each)** : These fields store the source and destination address respectively. Since size of these fields is 32 bits each so an IP address os maximum length of 32 bits can be used. So we see that this limits the number of IP addresses that can be used. To counter this problem, IP V6 has been introduced which increases this capacity.
- **Options(Variable length)** : The options may appear or not in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation. In some environments the security option may be required in all datagrams. The option field is variable in length. There may be zero or more options.

Difference between IPv4 and IPv6

IPv4	IPv6
The size of an address in IPv4 is 32 bits	The size of an address in IPv6 is 128 bits
Address Shortages: IPv4 supports 4.3×10^9 (4.3 billion) addresses, which is inadequate to give one (or more if they possess more than one device) to every living person.	Larger address space: IPv6 supports 3.4×10^{38} addresses, or 5×10^{28}(50 octillion) for each of the roughly 6.5 billion people alive today.[33(*)]
IPv4 header has 20 bytes	IPv6 header is the double, it has 40 bytes
IPv4 is subdivided into classes <A-E>.	IPv6 is classless.
IPv4 address uses a subnet mask.	IPv6 uses a prefix length.
IPv4 has lack of security.	IPv6 has a built-in strong security
ISP(Internet service provider) have IPv4 connectivity or have both IPv4 and IPv6	Many ISP don't have IPv6 connectivity