CHAPTER 1

FUNDAMENTALS OF DATA COMMUNICATION

A computer network is a set of devices connected through links. A node can be computer, printer,or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels.

TOPIC 1:FUNDAMENTALS OF DATA COMMUNICATION

Data communications are the exchange of data between two devices via some form of transmissionmedium such as a wire cable.

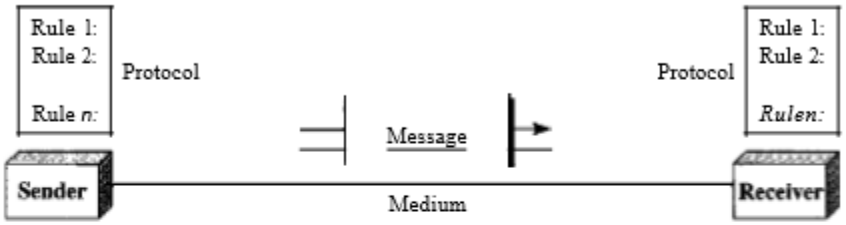
For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

- 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.
- Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- Timeliness. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind ofdelivery is called real-time transmission.
- Jitter. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery ofaudio or video packets. For example, let us assume that video packets are sent every 3D ms. Ifsome ofthe packets arrive with 3D-ms delay and others with 4D-ms delay,an uneven quality in the video is the result.

TOPIC : COMPONENTS OF DATA COMMUNICATION

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

Figure 1.1 *Five components of data communication*

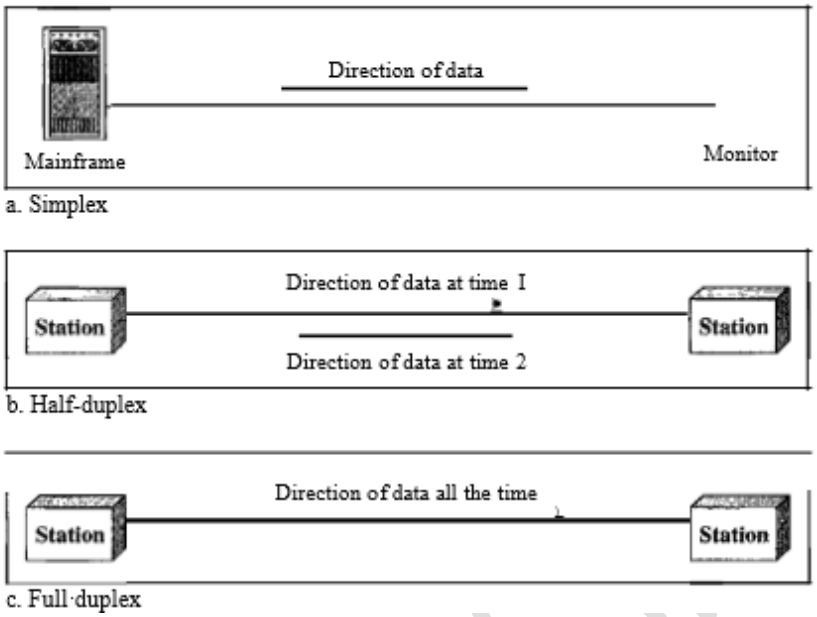


1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver.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

TOPIC 3: DATA FLOW

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

Figure 1.2 *Dataflow (simplex, half-duplex, andfull-duplex)*



❖ **Simplex**

In simplex mode, the communication is unidirectional, as on a one-way street. Only one ofthetwo devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards andtraditional monitors are examples of simplex devices. The keyboard can only introduce input;the monitor can only accept output. The simplex mode can use the entire capacity ofthe channelto send data in one direction.

❖ **Half-Duplex**

In half-duplex mode, each station can both transmit and receive, but not at the same time. : When one device is sending, the other can only receive, and vice versa (see Figure 1.2b).

The half-duplex mode is like a one-lane road with traffic allowed in both directions. When carsare traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices istransmitting at the time. Walkie-talkies and CB (citizens band) radios are

both half-duplex systems.

- **Full-Duplex**

In full-duplex (alsO called duplex), both stations can transmit and receive simultaneously(see Figure 1.2c). The full-duplex mode is like a tWo way street with traffic flowing in both directions at the same time.

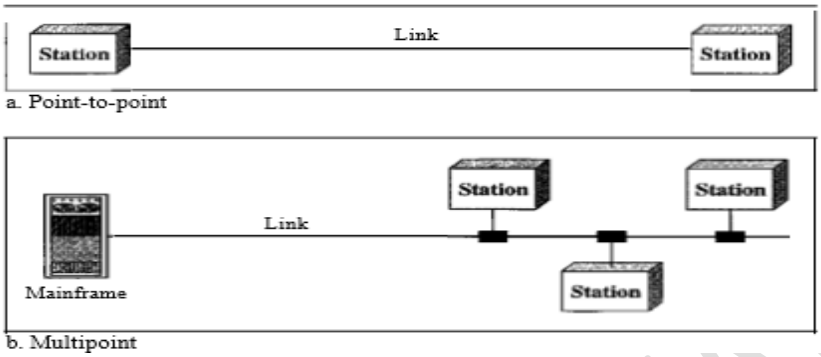
One common example of full-duplex communication is the telephone network. When twopeople are communicating by a telephone line, both can talk and listen at the same time.

TOPIC: TYPE OF CONNECTION

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. Thereare two possible types of connections: point-to-point and multipoint.

- **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (seeFigure 1.3a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.
- **Multipoint:** A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure 1.3b).

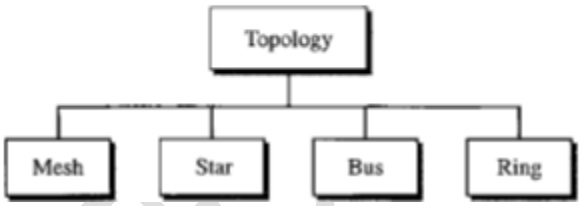
Figure 1.3 *Types ofconnections: point-to-point and multipoint*



TOPIC: PHYSICAL TOPOLOGY

The term physical topology refers to the way in which a network is laid out physically.: Two ormore devices connect to a link; two or more links form a topology.

Figure 1.4 *Categories oftopology*



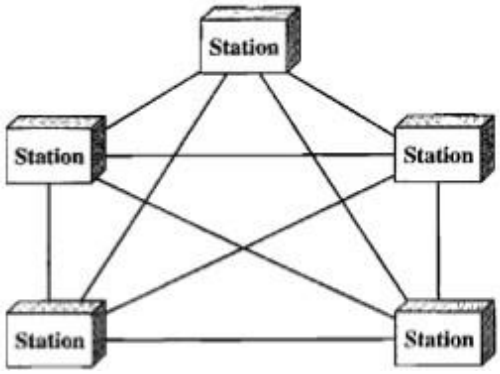
❖ **Mesh**

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problemsthat can occur when links must be shared by multiple devices. Second, a mesh topology is robust.Ifone link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage ofprivacy or security. When every message travels along a dedicated line, only the intended recipient sees

it.

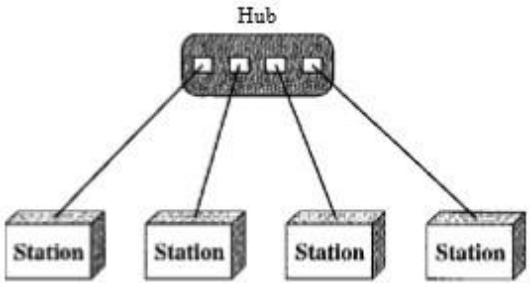
Figure 1.5 *A fully connected mesh topology (five devices)*



❖ **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. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: Ifone device wants to send data to another, it sends the data to the controller, which then relays thedata to the other connected device (see Figure 1.6) . A star topology is less expensive than a meshtopology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device andthe hub. Other advantages include robustness. Ifone link fails, only that link is affected. All otherlinks remain active.

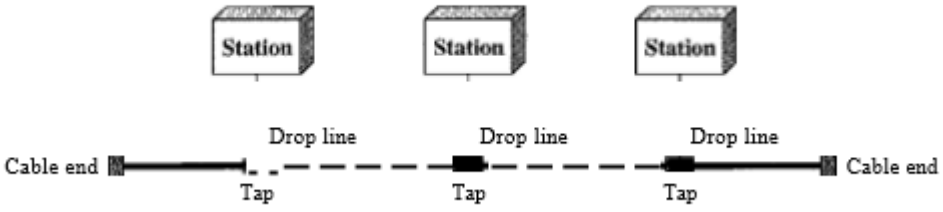
Figure 1.6 *A star topology connecting four stations*



❖ **Bus Topology**

A bus topology, on the otherhand, is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7).

Figure 1.7 *A bus topology connecting three stations*

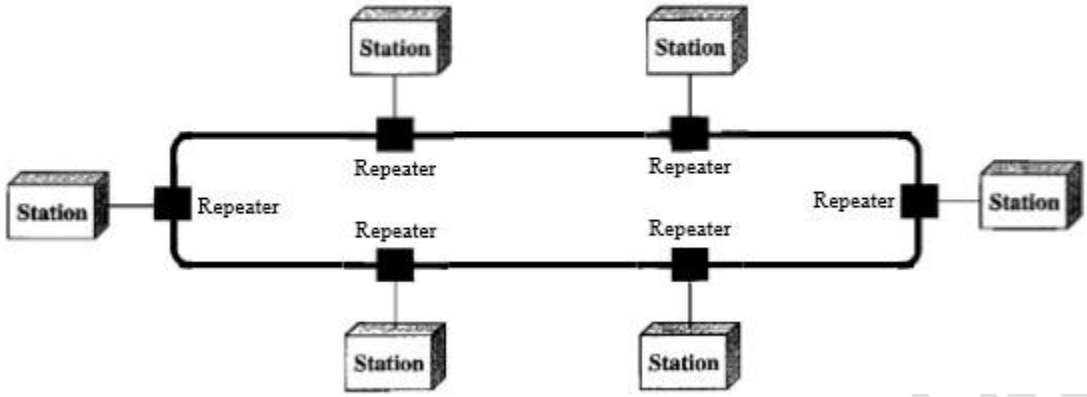


Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable.

❖ **Ring Topology**

In a ring topology, each device has a dedicated point-to-point connection with only the two deviceson 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 (see Figure 1.8).

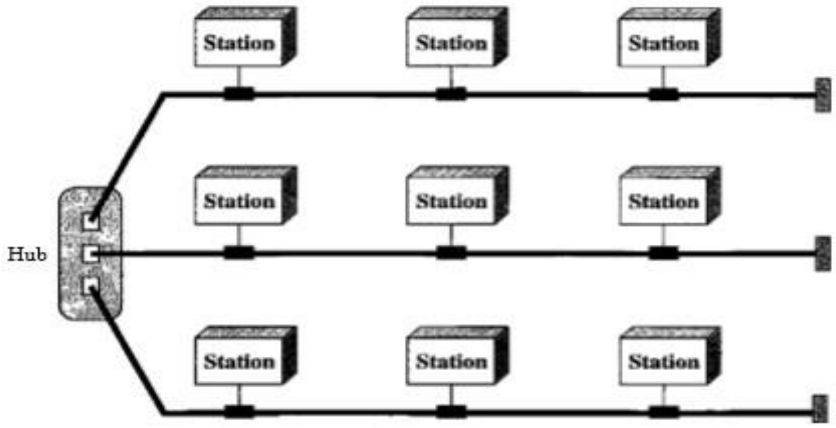
Figure 1.8 *A ring topology connecting six stations*



❖ **Hybrid Topology**

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

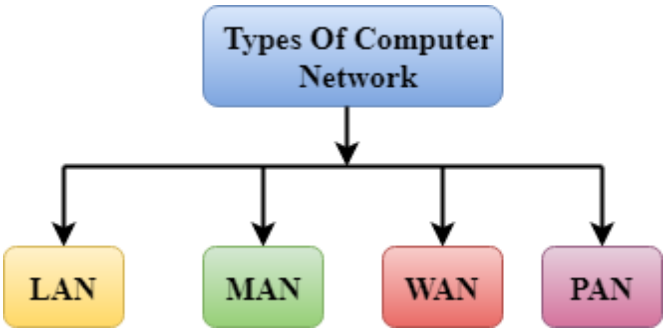
Figure 1.9 A *hybrid topology: a star backbone with three bus networks*



TOPIC 6: TYPES OF NETWORK

A computer network is a group of computers linked to each other that enables the computer tocommunicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **fourtypes**:



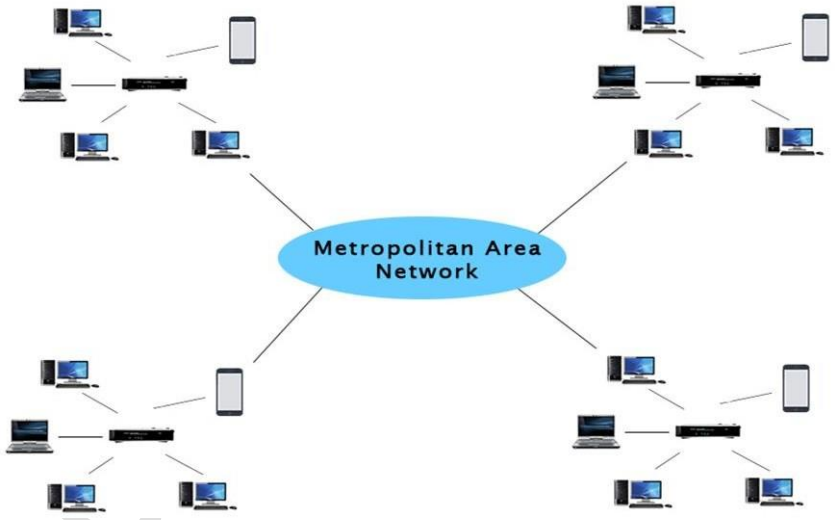
- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area suchas building, office.
- LAN is used for connecting two or more personal computers through a communicationmedium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, andethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area byinterconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).

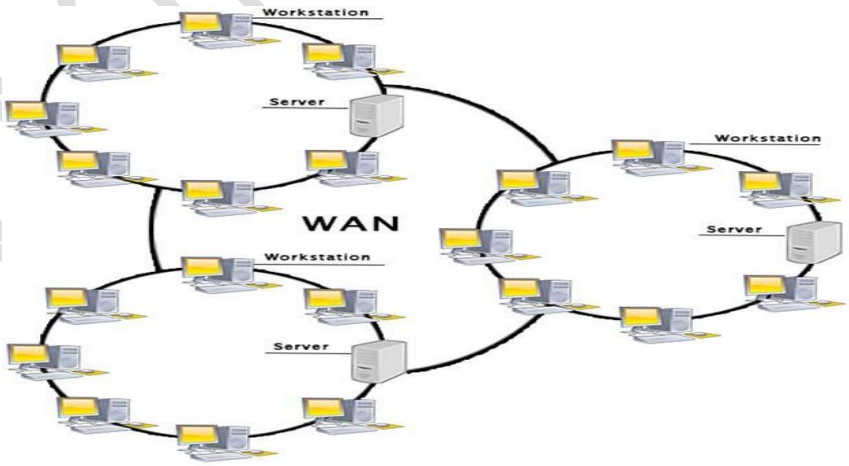


Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such asstates or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a largegeographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Private network:** A bank provides a private network that connects the 44 offices. Thisnetwork is made by using the telephone leased line provided by the telecom company.

TOPIC 2 :INTERNET

The **Internet** (or **internet**)[a] is the global system of interconnected computer networks that usesthe Internet protocol suite (TCP/IP) to communicate between networks and devices.

The basic distinction between network and net is that the **Network** consists of pcs that area unit physically connected and may be used as a private computer yet on share data with one another. Conversely, the **Internet** could be a technology that links these little and huge networks withone another and builds a additional in depth network.

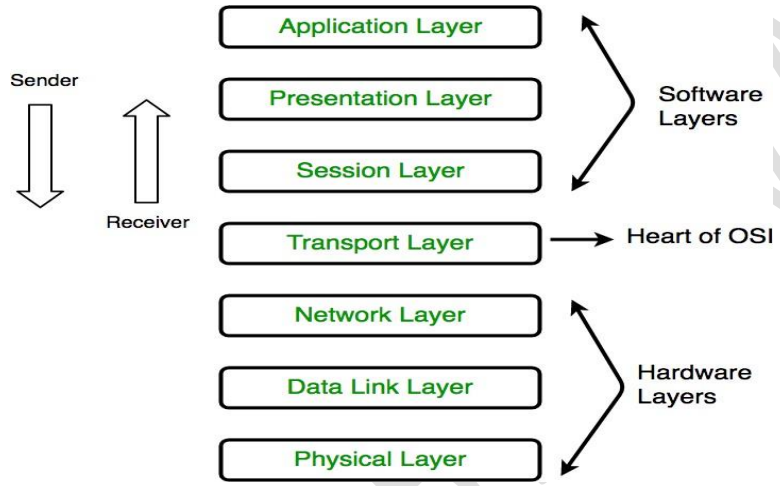
PROTOCOLS AND STANDARDS

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set ofrules that govern data communications. A protocol defines what is communicated, how it is communicated, and when itis communicated.

OSI MODEL (MOST IMPORTANT)

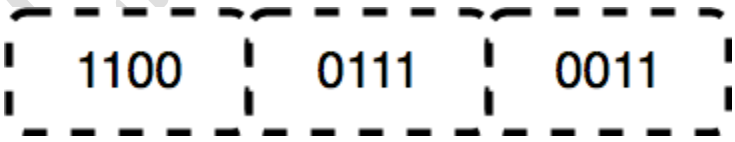
OSI stands for **Open Systems Interconnection**. It has been developed by ISO –

'**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the formof **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits

by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half- duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, overthe physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MACaddress in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution

Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the Data Link layer are :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

* *Packet in Data Link layer is referred to as **Frame**.*

*** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines. **** Switch & Bridge are Data Link Layer devices.*

3. Network Layer (Layer 3) :

The network layer works for the transmission of data from one host to the other located indifferent networks. It also takes care of packet routing i.e. selection of the shortest path totransmit the packet, from the number of routes available. The sender & receiver's IP addressesare placed in the header by the network layer. The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

* *Segment* in Network layer is referred to as **Packet**.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the networklayer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgementof the successful data transmission and re-transmits the data if an error is found.

- **At sender's side:** Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Note: The sender needs to know the port number associated with the receiver's application. Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

- At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, breaks the message into smaller units. Each of the segments produced has a header associatedwith it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to the correct process, thetransport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. **Connection-Oriented Service:** It is a three-phase process that includes

Connection Establishment, Data Transfer, Termination/disconnection In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packets is received. This type of transmission is reliable and

secure.

2. **Connectionless service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

* *Data in the Transport Layer is called as **Segments**.*

*** Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls. Transport Layer is called as **Heart of OSI** model.*

5. Session Layer (Layer 5) :

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security. The functions of the session layer are :

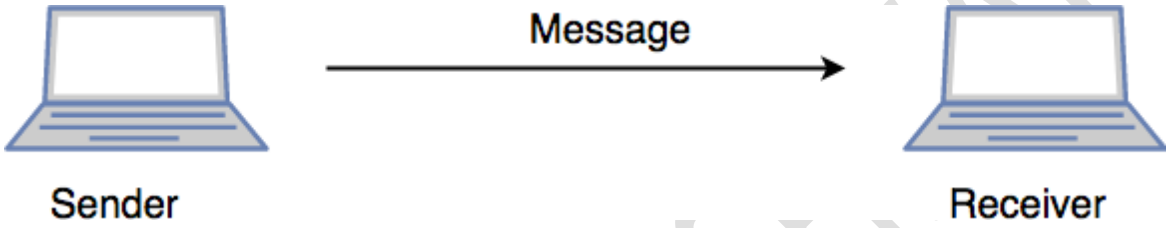
1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the errorso that the data is re-synchronized properly, and ends of the messages are not cut prematurelyand data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as "Application Layer".*

***Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers** or **Software Layers**.*

SCENARIO:

Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

The presentation layer is also called the **Translation layer**. The data from the application layeris extracted here and manipulated as per the required format to transmit over the network. The functions of the presentation layer are :

1. **Translation:** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has tobe transferred over the network. This layer also serves as a window for the application servicesto access the network and

for displaying the received information to the user. Ex: Application – Browsers, Skype Messenger, etc.

***Application Layer is also called Desktop Layer.*

The functions of the Application layer are :

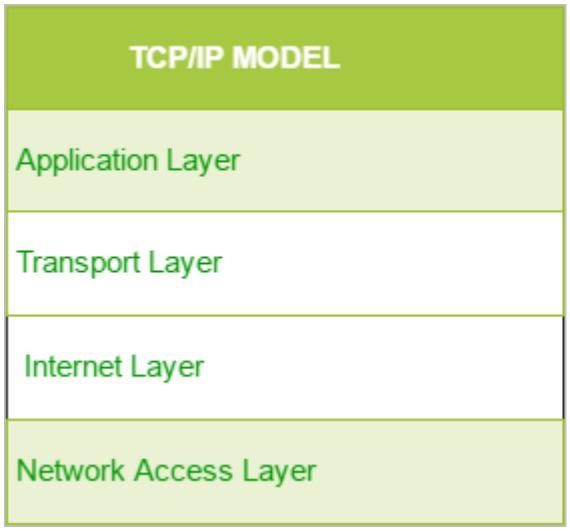
1. Network Virtual TerminalIU
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

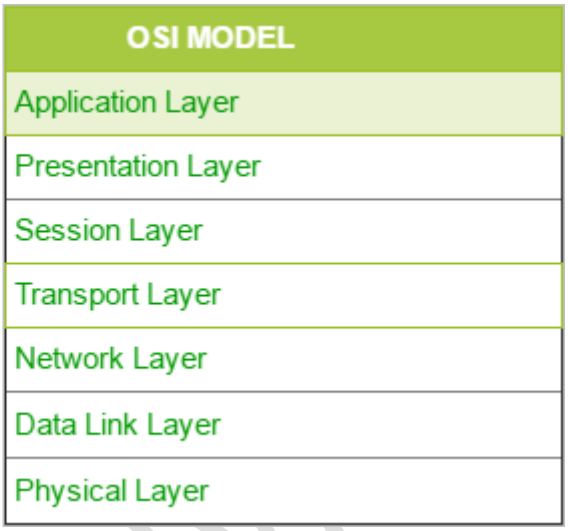
TOPIC 3 : TCP/IP MODEL

The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike sevenlayers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :





Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:

   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **IGMP**

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

4. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.
5. **RARP**

   The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when itknows only its physical address. It is used when a computer is connected toa network for the first time orwhen a diskless computer is booted

3. Transport Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. Itis the go-to protocol if your application does not require reliable transport as it is very cost- effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.
3. **SCTP**

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

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window,
LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPSstands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

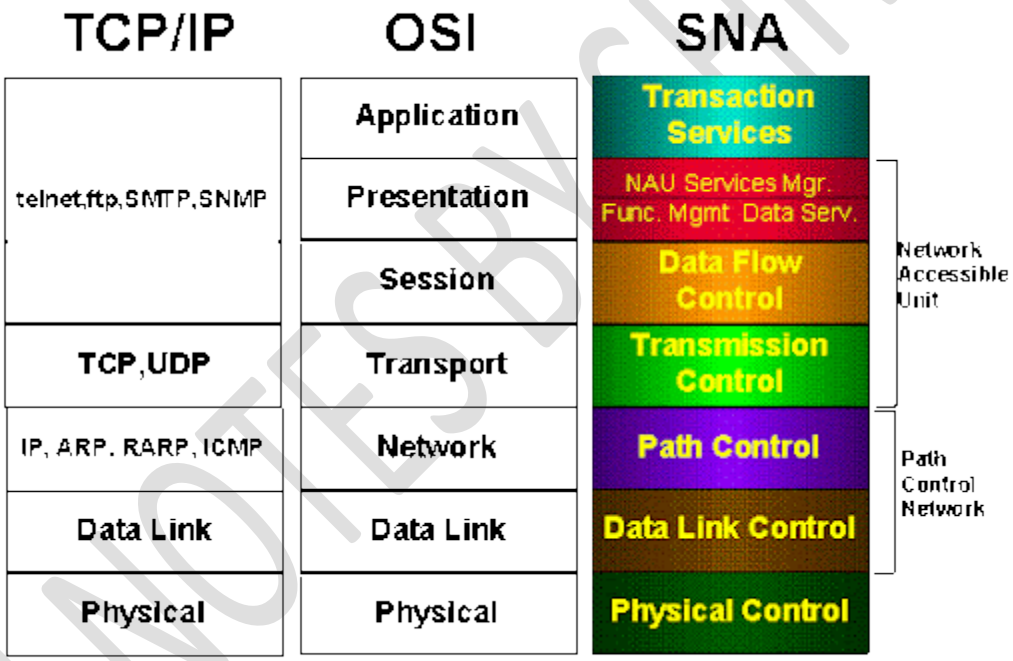
TOPIC 4: SNA, Appletalk, Netware

SNA PROTOCOL

Systems Network Architecture (SNA) is a data communication architecture established by IBM to specify common conventions for communication among the wide array of IBM hardware and software data communication products and other platforms.

The **Systems Network Architecture** (**SNA**) from IBM uses a 7 layer architecture similar to the OSI model.

SNA is designed to provide networking facilities for IBM systems only. Because of this, it is used by only a limited set of users. SNA, as a proprietary networking architecture, describes the general characteristics of computer hardware and software required for interconnection. The OSI reference model was developed a decade after the development of SNA. It has used SNA as a model. SNA was first released during 1974. The main idea was to connect many different hardware and software via links. A link consists Of a link connection and one or more link stations. The transmission media can be telephone cables, microwave links, optical fibers, and coaxial cables, etc. SNA supports distributed processing, internetworking, network management, and many advanced features.



Layers of SNA

The SNA layers are briefly discussed below.

1. ***Physical control*** Similar to the OSI physical layer, this layer is concerned with electrical, mechanical, and procedural characteristics of the transmission media and

the methods used for interfacing. No specific protocols are defined for this layer. This layer can be implemented using anyone of the international standards.

2. ***Data link control*** This layer is similar to the data link layer of the OSI. SNA defines SDLC protocol for message transfer across a communication link. It also supports *X.25* and Token ring protocols. It allows primary stations to communicate with secondary and token ring networks communicate with the peer network, using this protocol.
3. ***Path control*** Path control layer of the SNA includes many functions of the OSI network layer. It performs packet formation, path selection, routing, packet reassembling, controlling virtual routes and a few functions of OSI data link layer also.
4. ***Transmission control*** The functions of this layer are similar to OSI transport layer. The main functions are verification of sequence number when the packet is received, managing the rate at which requests are sent and received between logical units. This layer also performs few of the functions performed by the OSI presentation layer such as data encryption and decryption.
5. ***Data flow control*** The role of this layer is to arrange sessions between the source and destination stations. It also assigns data flow sequence number, receives chains of requests and responses from calling and called stations and forms brackets by grouping related chains. It roughly matches the functions of OSI session layer.
6. ***Presentation services*** The primary role of this layer is to run data transmission algorithms in accordance with a well-defined conversation (communication) protocol, by using conversation verbs. Coordinating the resource sharing and synchronization are the other functions of this layer. This layer has resemblance with OSI presentation layer.
7. ***Transaction services*** This layer is on the top of SNA architecture. It performs distributed processing and management.

Topic: AppleTalk

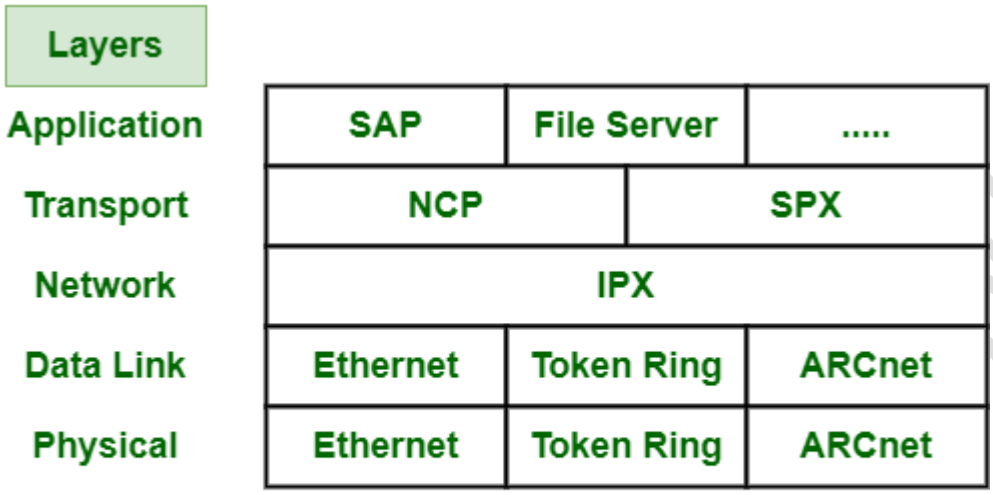
AppleTalk is a set of proprietary networking protocols developed by Apple for their computer systems. AppleTalk was included in the original Macintosh released in 1984. In 2009, it became unsupported with the release of Mac OS X v10.6 and was dropped in favor of TCP/IP networking, allowing Apple computers to use the same standard to communicate with other computers.

The design of AppleTalk followed the OSI Model of protocol layering with two protocols aimed at making the system completely self-configuring:

- AppleTalk Address Resolution Protocol (AARP): Allowed hosts to automaticall generate their own network addresses
- Name Binding Protocol (NBP): A dynamic system that maps network addresses to user-readable names.

Topic: Netware

Novell NetWare is type of Network Operating System. It provides wide networking services ranging from easy and simple file to network user, data, security, and even resource management. It is generally designed for networks or Local Area Network (LAN) operating system. **Novell NetWare** is most popular and widely used network system in PC world. Novell NetWare is simply designed to get used by various companies downsizing from mainframe to network of PCs. It only needs low hardware requirements and has memory protection. It keeps safe and protects single processes from each other. It generally uses proprietary protocol stack as shown in below diagram. Novell NetWare 6.5 is one of Novell's most current network operating system used nowdays.

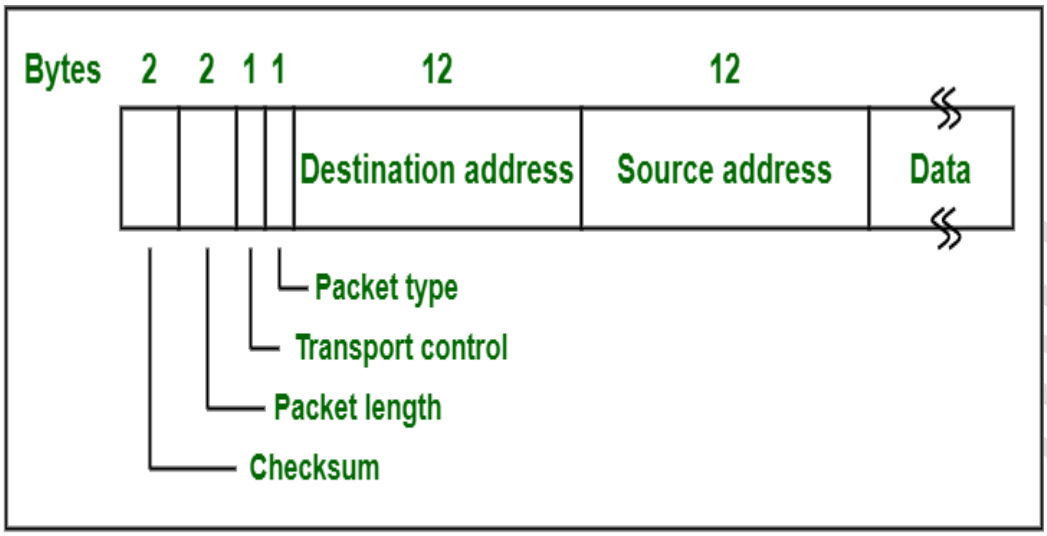


The Novell NetWare Reference Model

Protocols in Novell Netware :

- **Internet Package Exchange (IPX) –** Network layer generally runs unreliable connectionless internetwork protocol. It is called Internet Package Exchange (IPX) protocol. This protocol is simply used for routing and showing path to packets to move from one network node to another network throughout internetwork. Format

of IPX is shown below:



A Novell NetWare IPX Packet

- **NetWare Core Protocol (NCP) –** NCP is type of network protocol that is used in many products from Novell, Inc. It is actually Novell client-server protocol used for mainly Local Area Network (LAN). It is generally connected to NetWare Operating systems (OS). It also works with alternating operating systems along with UNIX, Linux, and Windows NT.
- **Sequenced Packet Exchange (SPX) –** SPX is also type of network protocol that is used by Novell Netware. SPX is also supported by other operating systems. It is nowadays considered legacy protocol as it has largely been replaced by TCP/IP. This protocol is simply used for handling packet sequencing in Novell Netware network.

Features of Novell Netware : Most important features of Netware are following:

- **User Interface –** It contains simple user interface by which user and computer system can interact in easy way.
- **Hardware requirements –** This network operating system does not require or needs many hardware devices. It needs very minimal hardware devices.

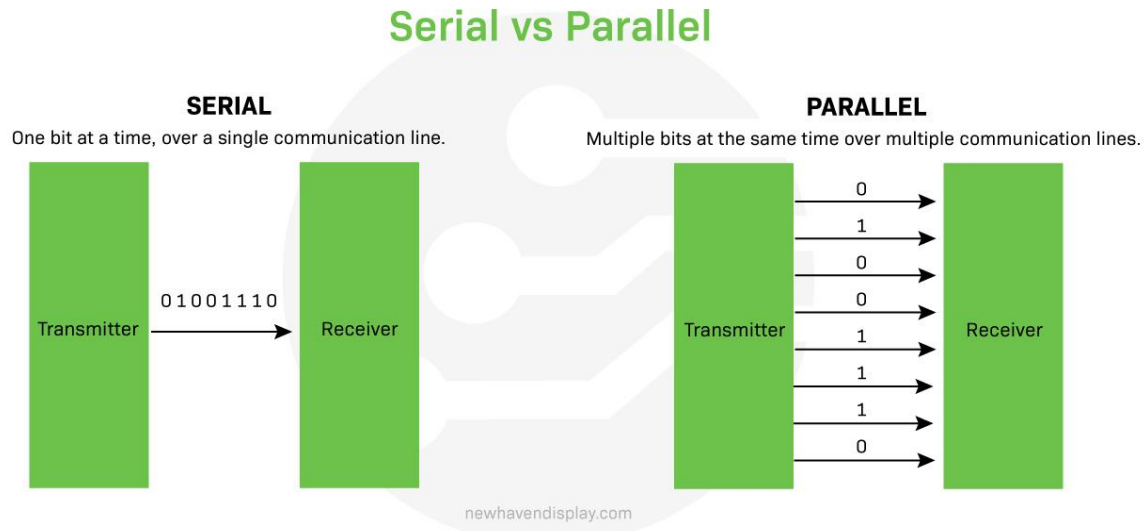
- **Interoperability** – Using this networking operating system, ability of computer systems or software to simply exchange and make use of information with many types of computer systems is increased.

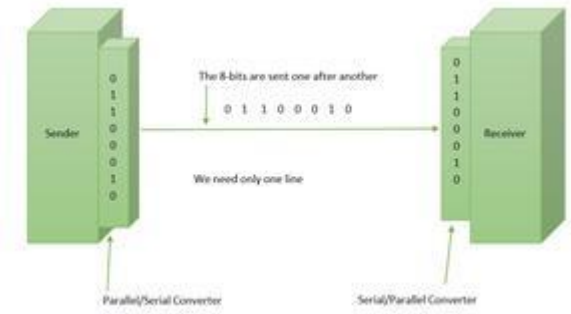
TOPIC 6 : Physical Layer

DATA TRANSMISSION

The process of sending data between two or more digital devices is known as *data transmission*. Data is transmitted between digital devices using one of the two methods − *serial transmission* or *parallel transmission*.

In serial transmission, data bits are sent one after the other across a single channel. Parallel data transmission distributes numerous data bits through various channels at the same time.

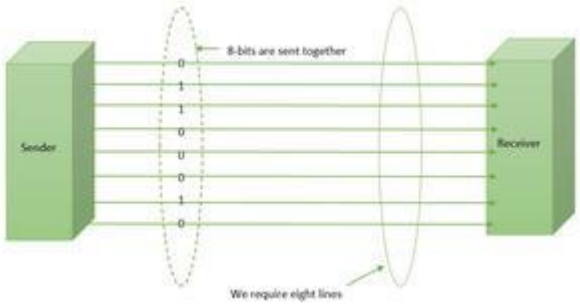




Serial Transmission

Parallel_Transmission:

In Parallel Transmission, many bits are flow together simultaneously from one computer to another computer. Parallel Transmission is faster than serial transmission to transmit the bits. Parallel transmission is used for short distance.



Parallel Transmission

Difference between Serial and Parallel Transmission:

S.NO	Serial Transmission	Parallel Transmission
1.	In this type, a single communication link is used to transfer data from one end to another	In this type, multiple parallels links used to transmit the data

S.NO	Serial Transmission	Parallel Transmission
2.	In serial transmission, data(bit) flows in bi-direction.	In Parallel Transmission, data flows in multiple lines.
3.	Serial Transmission is cost-efficient.	Parallel Transmission is not cost-efficient.
4.	In serial transmission, one bit transferred at one clock pulse.	In Parallel Transmission, eight bits transferred at one clock pulse.
5.	Serial Transmission is slow in comparison of Parallel Transmission.	Parallel Transmission is fast in comparison of Serial Transmission.
6.	Generally, Serial Transmission is used for long-distance.	Generally, Parallel Transmission is used for short distance.
7.	The circuit used in Serial Transmission is simple.	The circuit used in Parallel Transmission is relatively complex.
8.	Serial Transmission is full duplex as sender can send as well as receive the data	Parallel Transmission is half-duplex since the data is either send or receive
9.	Converters are required in a serial transmission to convert the data between internal and parallel form	No converters are required in Parallel Transmission
10.	Serial transmission is reliable and straightforward.	Parallel transmission is unreliable and complicated.

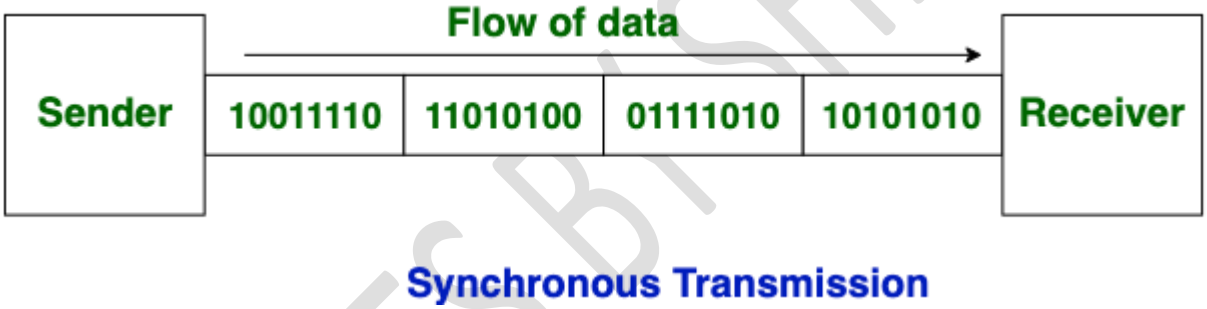
TOPIC : TYPES OF SERIAL TRANSMISSION

Synchronous Transmission: In Synchronous Transmission, data is sent in form of blocks

or frames. This transmission is the full-duplex type. Between sender and receiver, synchronization is compulsory. In Synchronous transmission, There is no time-gap present between data. It is more efficient and more reliable than asynchronous transmission to transfer a large amount of data.

Example:

- Chat Rooms
- Telephonic Conversations
- Video Conferencing



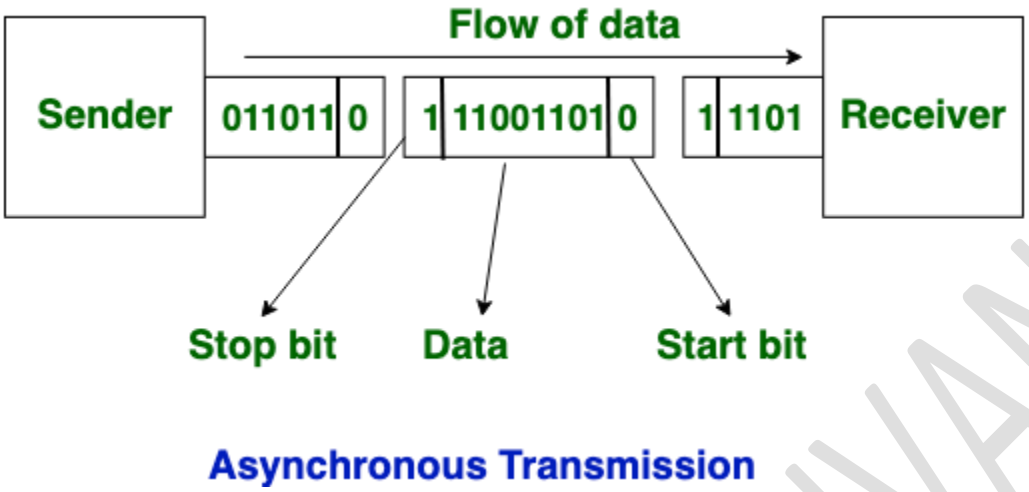
Synchronous Transmission

Asynchronous Transmission: In Asynchronous Transmission, data is sent in form of byte or character. This transmission is the half-duplex type transmission. In this transmission start bits and stop bits are added with data. It does not require synchronization.

Example:

- Email
- Forums

- Letters



Asynchronous Transmission

Now, let's see the difference between Synchronous Transmission and Asynchronous Transmission:

S. No.	Synchronous Transmission	Asynchronous Transmission
1.	In Synchronous transmission, data is sent in form of blocks or frames.	In Asynchronous transmission, data is sent in form of bytes or characters.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.
3.	Synchronous transmission is costly.	Asynchronous transmission is economical.
4.	In Synchronous transmission, the time interval of transmission is constant.	In Asynchronous transmission, the time interval of transmission is not constant, it is random.
5.	In this transmission, users have to wait till the transmission is complete before getting a response back from	Here, users do not have to wait for the completion of transmission in order to get a

S. No.	Synchronous Transmission	Asynchronous Transmission
	the server.	response from the server.
6.	In Synchronous transmission, there is no gap present between data.	In Asynchronous transmission, there is a gap present between data.
7.	Efficient use of transmission lines is done in synchronous transmission.	While in Asynchronous transmission, the transmission line remains empty during a gap in character transmission.
8.	The start and stop bits are not used in transmitting data.	The start and stop bits are used in transmitting data that imposes extra overhead.
9.	Synchronous transmission needs precisely synchronized clocks for the information of new bytes.	Asynchronous transmission does not need synchronized clocks as parity bit is used in this transmission for information of new bytes.
10.	Errors are detected and corrected in real time.	Errors are detected and corrected when the data is received.
11.	Low latency due to real-time communication.	High latency due to processing time and waiting for data to become available.
12.	Examples: Telephonic conversations, Video conferencing, Online gaming.	Examples: Email, File transfer,Online forms.

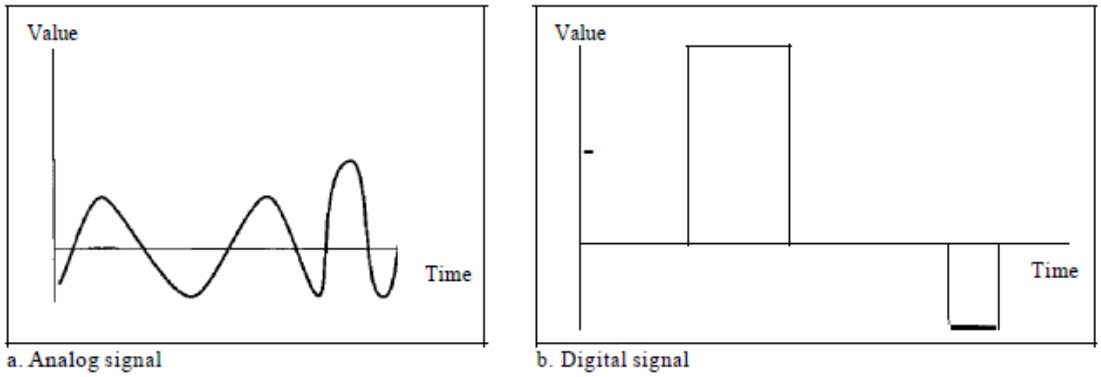
Topic: **DATA TRANSMISSION CONCEPTS**

A signal is an electrical or electromagnetic quantity that transports data or information from one system to another. For data transmission, two types of signals are used: Analog signals and digital signals.

Data can be analog or digital. The term **analog data** refers to information that is continuous; **digital data** refers to information that has discrete states. For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

Analog data, such as the sounds made by a human voice, take on continuous values. When someone speaks, an analog wave is created in the air. This can be captured by a microphone and converted to an analog signal or sampled and converted to a digital signal. Digital data take on discrete values. For example, data are stored in computer memory in the form of Os and 1s. They can be converted to a digital signal or modulated into an analog signal for transmission across a medium.

Figure 3.1 *Comparison of analog and digital signals*



a. Analog signal

b. Digital signal

Difference between Analog and Digital Signals

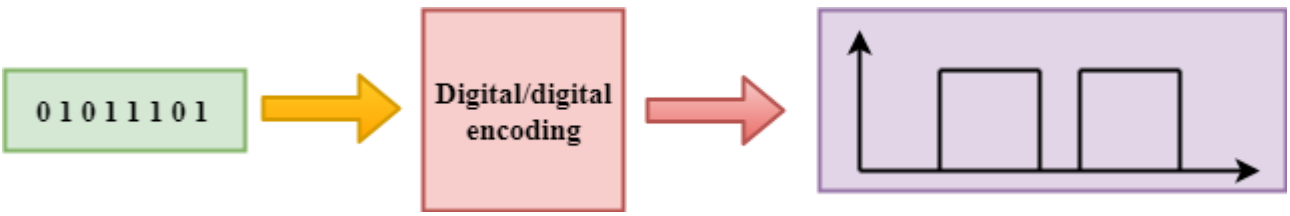
To summarise, we have given the various differences between analog signal and digital signal in a tabular form below. Both these signals are used in electronic communication system to transfer information from one place to another.

Difference between Analog and Digital Signal

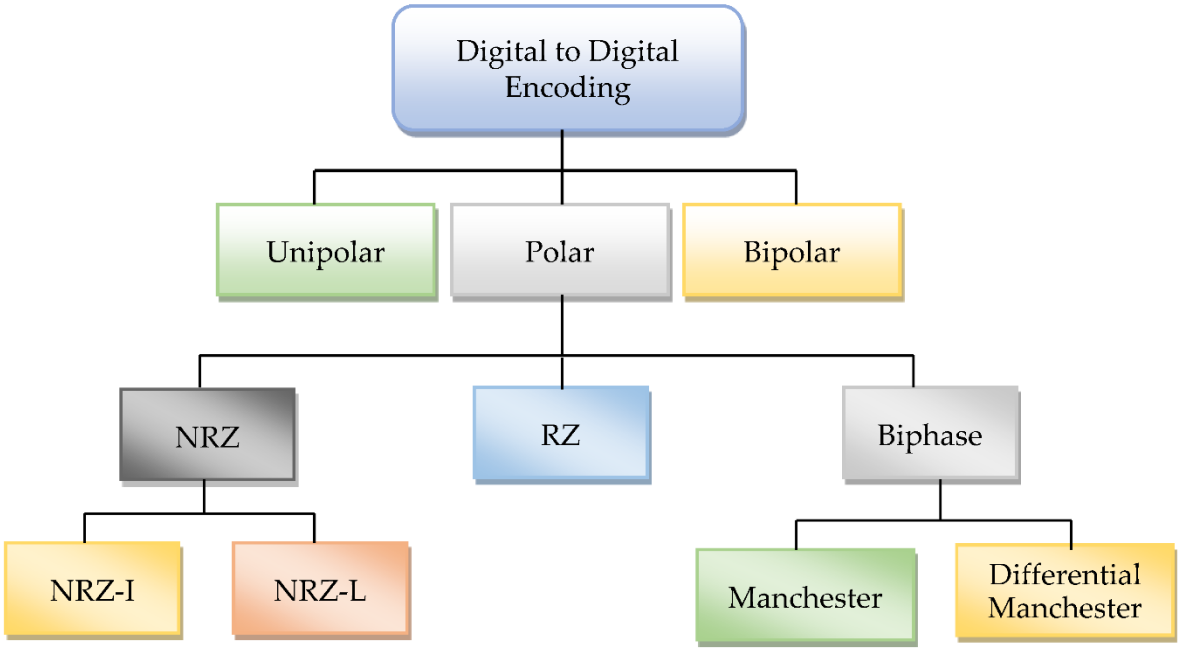
Analog Signals	Digital Signals
Continuous signals	Discrete signals
Represented by sine waves	Represented by square waves
Human voice, natural sound, analog electronic devices are a few examples	Computers, optical drives, and other electronic devices
Continuous range of values	Discontinuous values
Records sound waves as they are	Converts into a binary waveform
Only used in analog devices	Suited for digital electronics like computers, mobiles and more

TOPIC: DIGITAL-TO-DIGITAL CONVERSION

Digital-to-digital encoding is the representation of digital information by a digital signal. When binary 1s and 0s generated by the computer are translated into a sequence of voltage pulses that can be propagated over a wire, this process is known as digital-to-digital encoding.

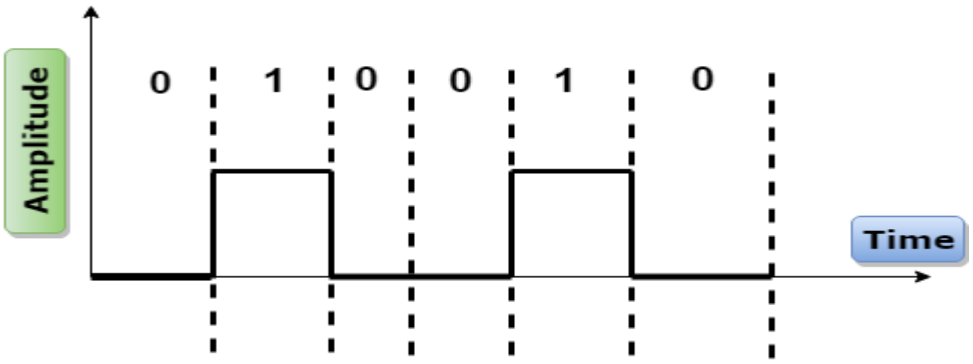


Digital-to-digital encoding is divided into three categories:



Unipolar

- Digital transmission system sends the voltage pulses over the medium link such as wire or cable.
- In most types of encoding, one voltage level represents 0, and another voltage level represents 1.
- The polarity of each pulse determines whether it is positive or negative.
- This type of encoding is known as Unipolar encoding as it uses only one polarity.
- In Unipolar encoding, the polarity is assigned to the 1 binary state.
- In this, 1s are represented as a positive value and 0s are represented as a zero value.
- In Unipolar Encoding, '1' is considered as a high voltage and '0' is considered as a zero voltage.
- Unipolar encoding is simpler and inexpensive to implement.



Polar

- Polar encoding is an encoding scheme that uses two voltage levels: one is positive, and another is negative.

NRZ

- NRZ stands for Non-return zero.
- In NRZ encoding, the level of the signal can be represented either positive or negative.

The two most common methods used in NRZ are:

NRZ-L: In NRZ-L encoding, the level of the signal depends on the type of the bit that it represents. If a bit is 0 or 1, then their voltages will be positive and negative respectively. Therefore, we can say that the level of the signal is dependent on the state of the bit.

TRICK: IF BIT IS 0, MAKE LINE ABOVE X AXIS.

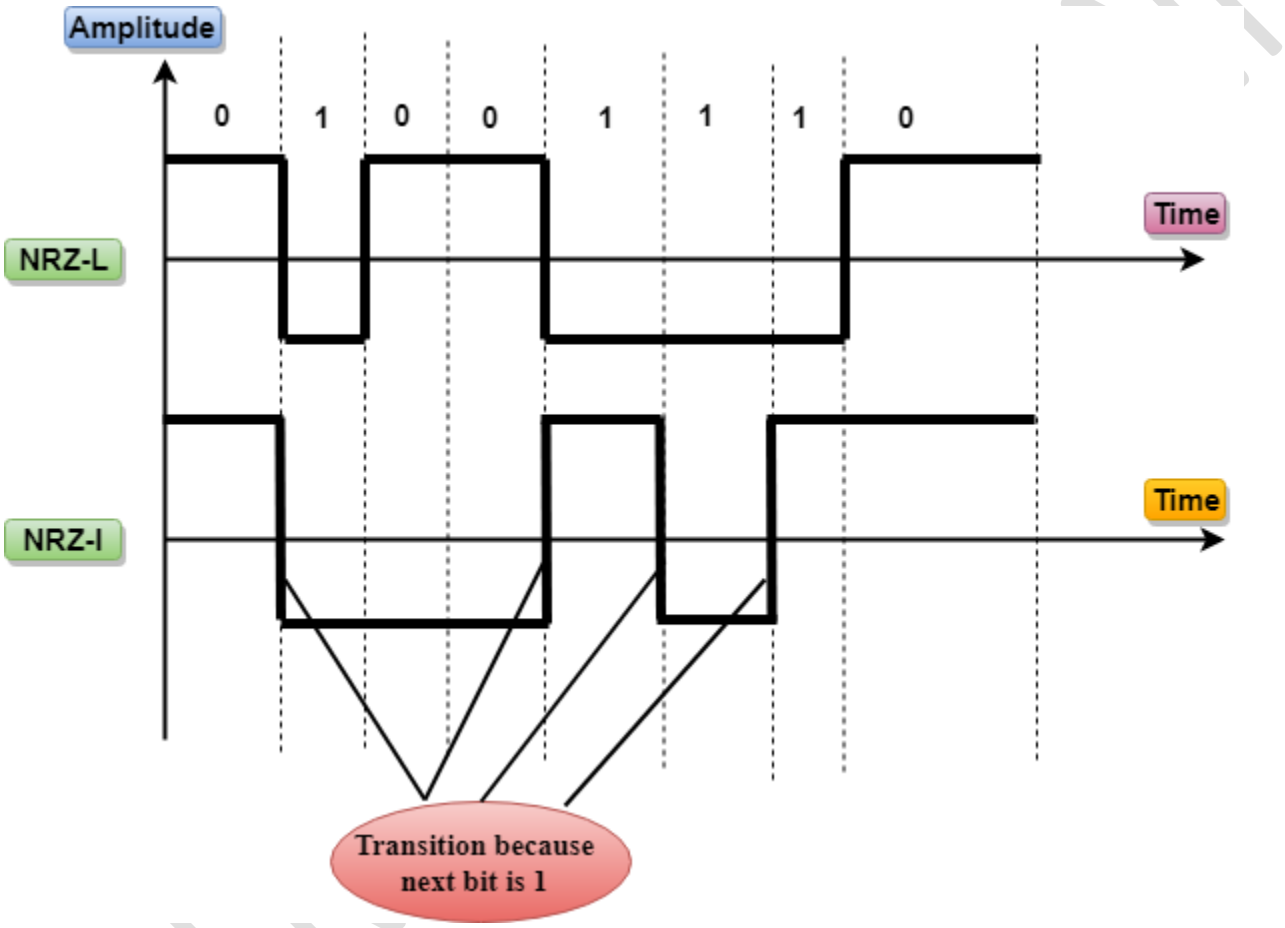
IF BIT IS 1, MAKE LINE BELOW X AXIS

NRZ-I: NRZ-I is an inversion of the voltage level that represents 1 bit. In the NRZ-I encoding scheme, a transition occurs between the positive and negative voltage that

represents 1 bit. In this scheme, 0 bit represents no change and 1 bit represents a change in voltage level.

TRICK: IF BIT IS ZERO, NO TRANSITION

IF BIT IS ONE, MAKE TRANSITION



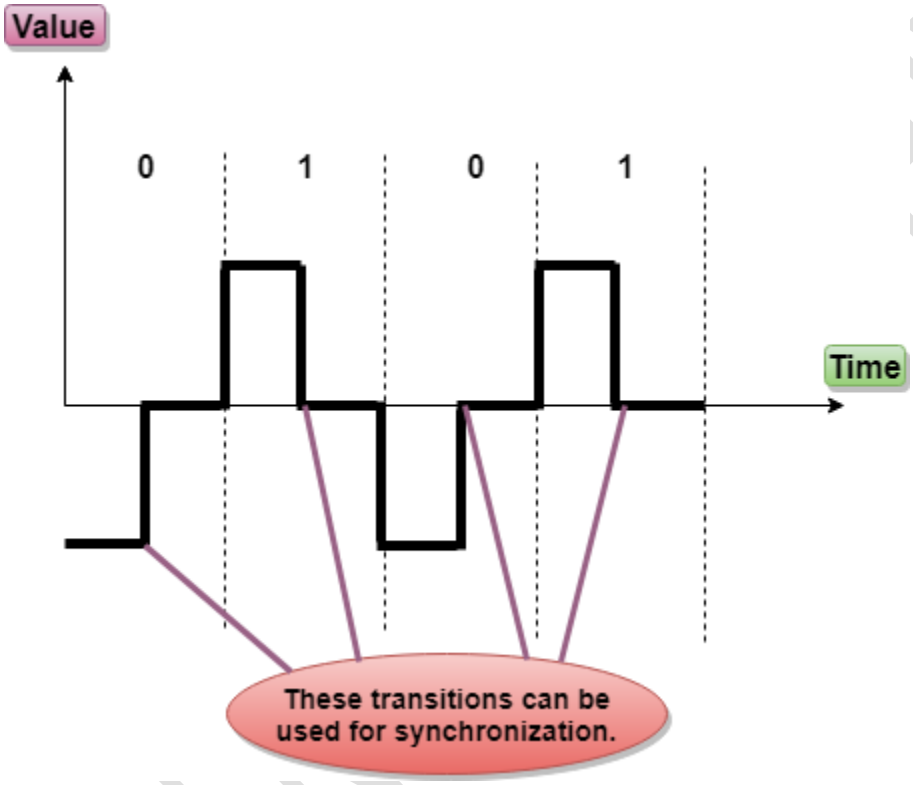
RZ

- RZ stands for Return to zero.
- There must be a signal change for each bit to achieve synchronization. However, to change with every bit, we need to have three values: positive, negative and zero.
- RZ is an encoding scheme that provides three values, positive voltage represents 1, the negative voltage represents 0, and zero voltage represents none.

- In the RZ scheme, halfway through each interval, the signal returns to zero.
- In RZ scheme, 1 bit is represented by positive-to-zero and 0 bit is represented by negative-to-zero.

TRICK: IF BIT IS 1, MAKE Z ABOVE X AXIS

IF BIT IS ZERO, MAKE INVERTED Z BELOW X AXIS

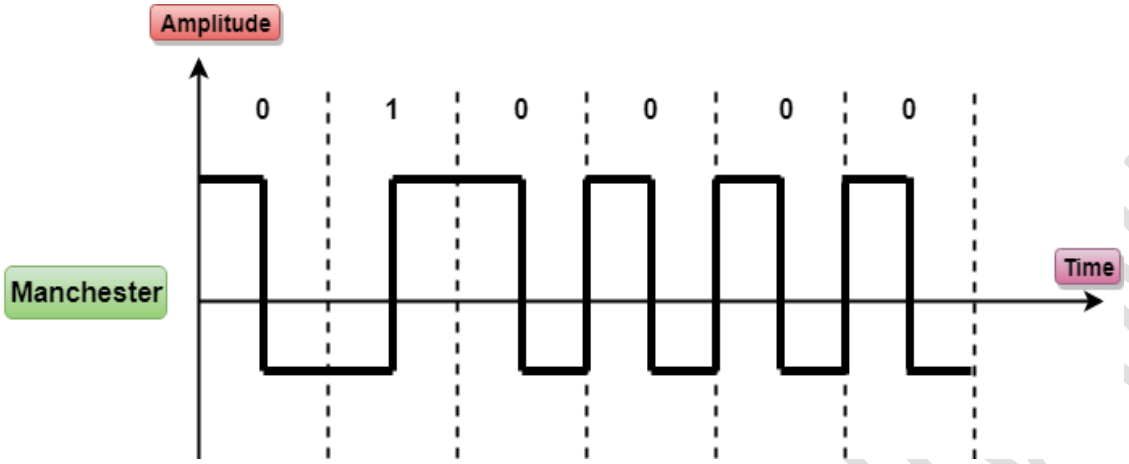


Manchester

- It changes the signal at the middle of the bit interval but does not return to zero for synchronization.
- In Manchester encoding, a negative-to-positive transition represents binary 1, and positive-to-negative transition represents 0.

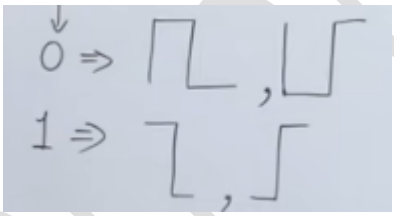
TRICK: IF BIT IS 1, TRANSITION FROM –VE TO POSITIVE

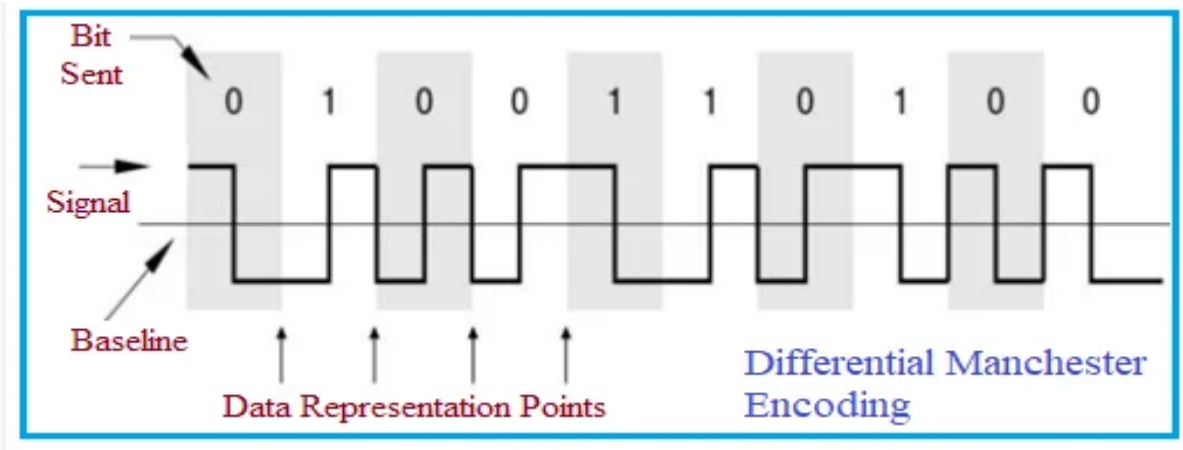
IF BIT IS 0, TRANSITION FROM +VE TO NEGATIVE



Differential Manchester

- It changes the signal at the middle of the bit interval for synchronization, but the presence or absence of the transition at the beginning of the interval determines the bit. A transition means binary 0 and no transition means binary 1.
- In Manchester Encoding scheme, two signal changes represent 0 and one signal change represent 1.

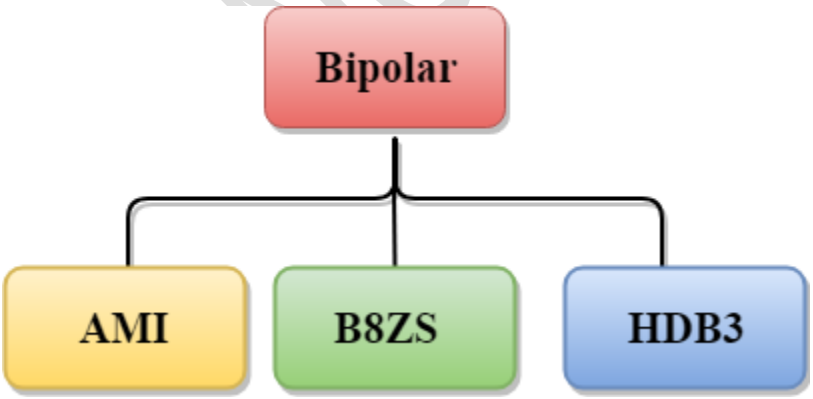
TRICK 



Bipolar

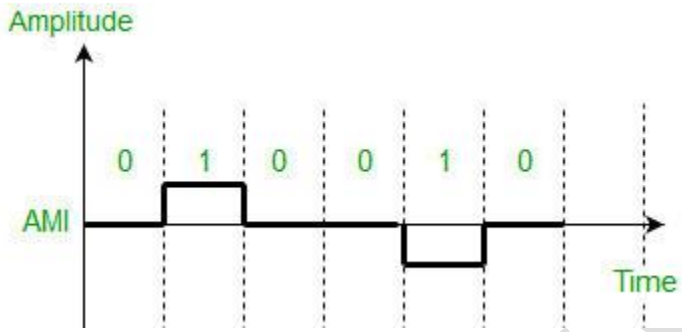
- Bipolar encoding scheme represents three voltage levels: positive, negative, and zero.
- In Bipolar encoding scheme, zero level represents binary 0, and binary 1 is represented by alternating positive and negative voltages.
- If the first 1 bit is represented by positive amplitude, then the second 1 bit is represented by negative voltage, third 1 bit is represented by the positive amplitude and so on. This alternation can also occur even when the 1bits are not consecutive.

Bipolar can be classified as:



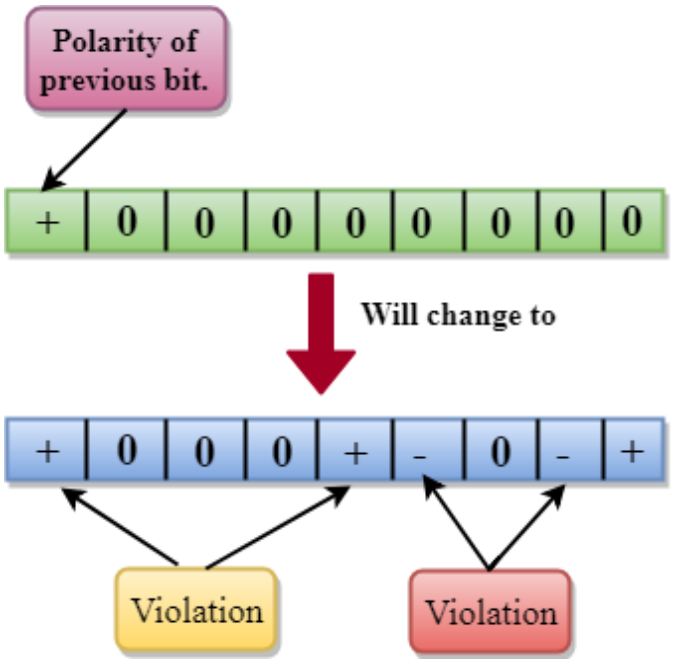
AMI

- AMI stands for ***alternate mark inversion*** where mark work comes from telegraphy which means 1. So, it can be redefined as **alternate 1 inversion**.
- In Bipolar AMI encoding scheme, 0 bit is represented by zero level and 1 bit is represented by alternating positive and negative voltages.



B8ZS

- B8ZS stands for **Bipolar 8-Zero Substitution**.
- This technique is adopted in North America to provide synchronization of a long sequence of 0s bits.
- In most of the cases, the functionality of B8ZS is similar to the bipolar AMI, but the only difference is that it provides the synchronization when a long sequence of 0s bits occur.
- B8ZS ensures synchronization of a long string of 0s by providing force artificial signal changes called violations, within 0 string pattern.
- When eight 0 occurs, then B8ZS implements some changes in 0s string pattern based on the polarity of the previous 1 bit.
- If the polarity of the previous 1 bit is positive, the eight 0s will be encoded as zero, zero, zero, positive, negative, zero, negative, positive.

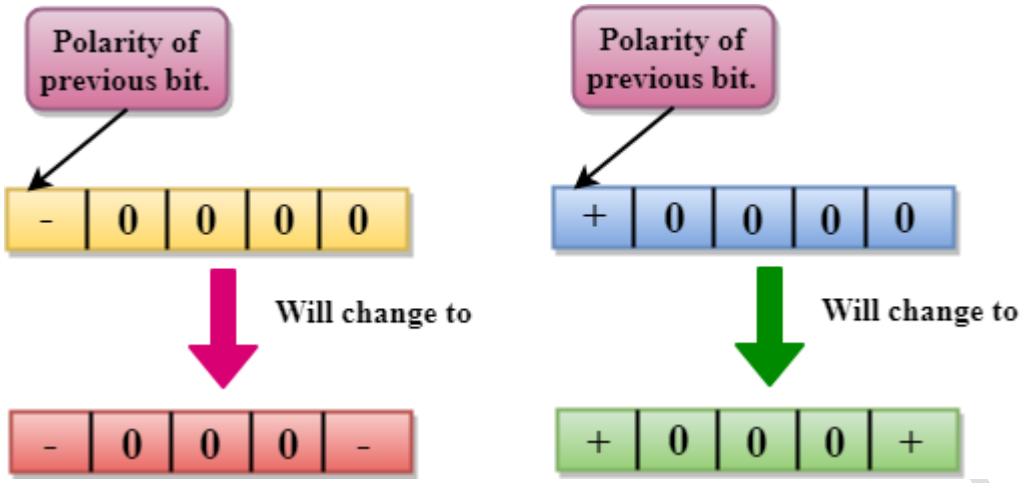


- If the polarity of previous 1 bit is negative, then the eight 0s will be encoded as zero, zero, zero, negative, positive, zero, positive, negative.

HDB3

- HDB3 stands for **High-Density Bipolar 3**.
- HDB3 technique was first adopted in Europe and Japan.
- HDB3 technique is designed to provide the synchronization of a long sequence of 0s bits.
- In the HDB3 technique, the pattern of violation is based on the polarity of the previous bit.
- When four 0s occur, HDB3 looks at the number of 1s bits occurred since the last substitution.
- If the number of 1s bits is odd, then the violation is made on the fourth consecutive of 0. If the polarity of the previous bit is positive, then the violation is positive. If the polarity of the previous bit is negative, then the violation is negative.

If the number of 1s bits since the last substitution is odd.

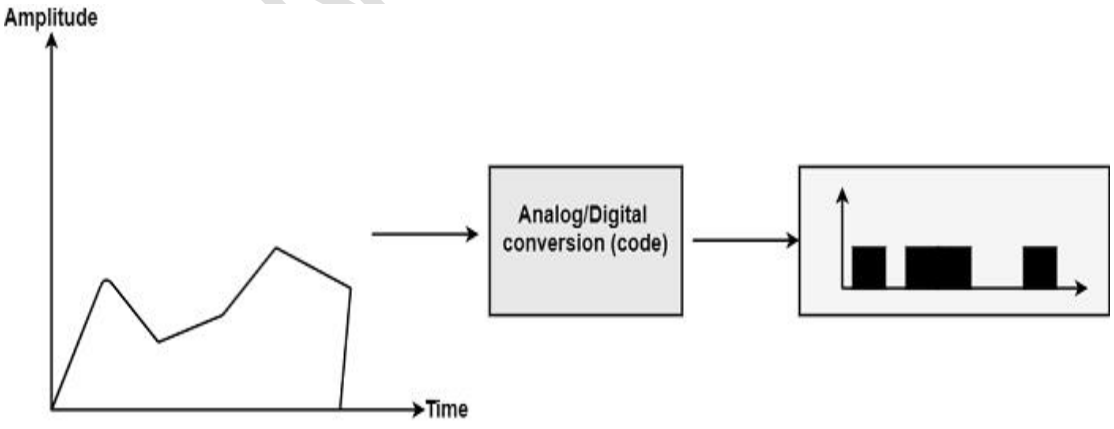


If the number of 1s bits is even, then the violation is made on the place of the first and fourth consecutive 0s. If the polarity of the previous bit is positive, then violations are negative, and if the polarity of the previous bit is negative, then violations are positive.

Analog to Digital Transmission

When an analog signal is digitalized, that is known as analog-to-digital conversion.

Consider a human address a voice in the structure of an analog signal. We require to digitalize the analog signal that is smaller inclined to noise. It needed a decrease in the several values in an analog message defined in the digital flow.



Analog to Digital Conversion

In analog-to-digital conversion, the data involved in a constant waveform is modified into digital pulses.

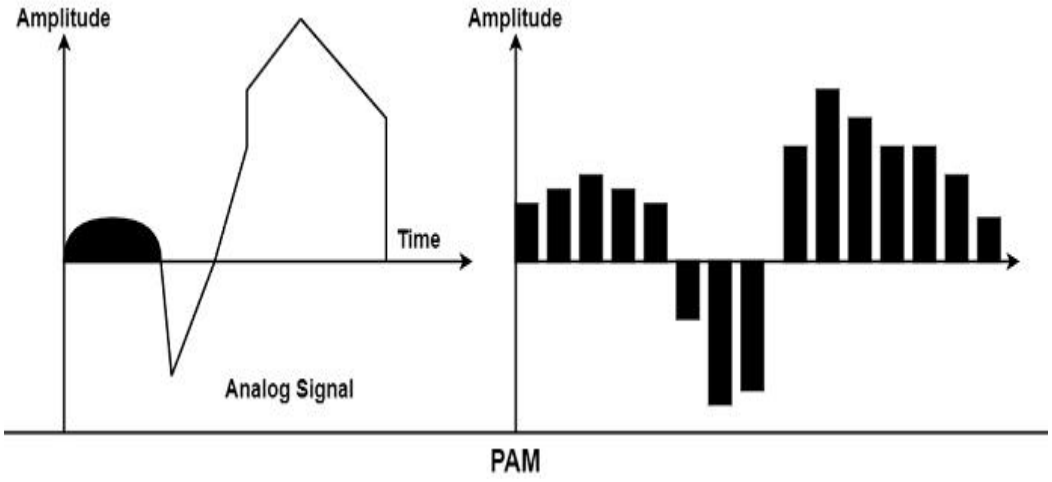
Methods for Analog-To-Digital Conversion

The various methods for Analog-to-Digital conversion are as follows −

PAM

The first phase in analog to digital conversion is known as PAM. PAM represents **pulse amplitude modulation**. This method creates an analog signal, samples it, and creates digital pulses sequences based on sampling. The sampling method used in PAM is more helpful to other manufacturing fields than data communication. PAM is the infrastructure of an essential analog-to-digital conversion method known as **pulse code modulation (PCM)**.

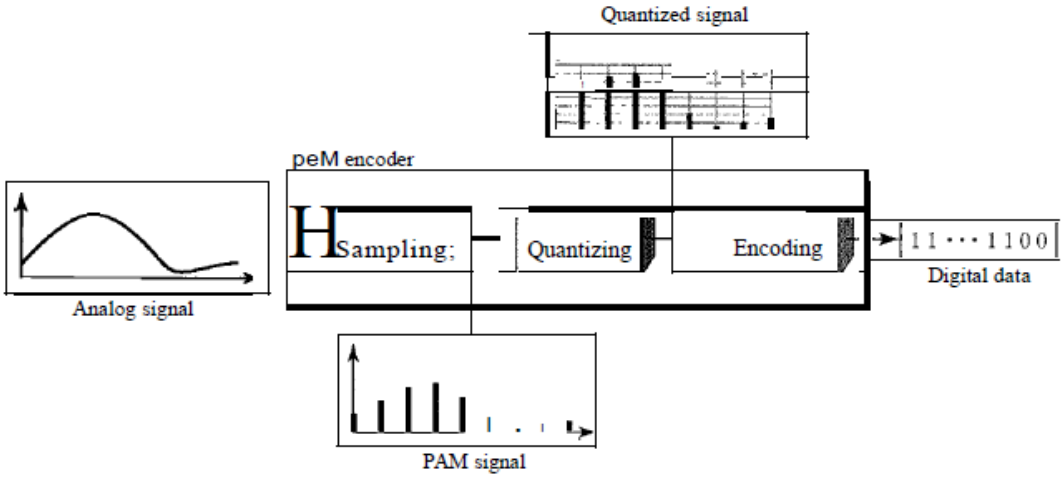
In PAM, the initial signal is sampled at the same intervals, as display in the figure. PAM uses a method known as a sample and hold.



PCM

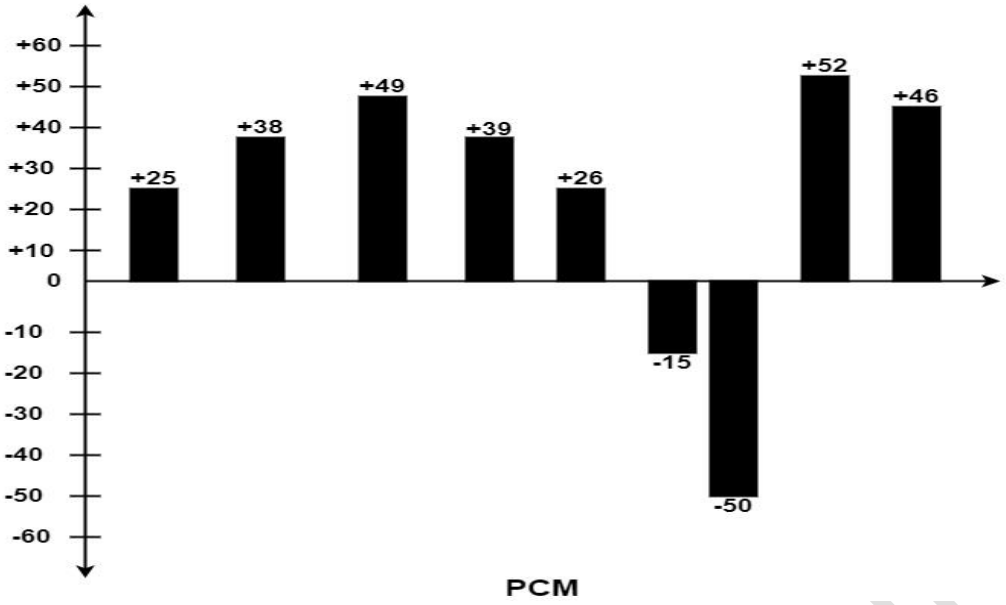
PCM represents **Pulse Code Modulation**. PCM method can change the pulses generated by PAM to develop a completely digital signal.

Figure 4.21 *Components of PCM encoder*



1. The analog signal is sampled.
2. The sampled signal is quantized.
3. The quantized values are encoded as streams of bits.

To manage this, PCM first measures the PAM pulses. Quantization is a technique of authorizing integral values in a particular area to sampled instances. The outcome of quantization is shown in the figure.



The figure displays a simple method of creating sign and magnitude costs to quantized samples. Each cost is interpreted into a six-bit binary proportionate. The seventh bit denoted the sign.

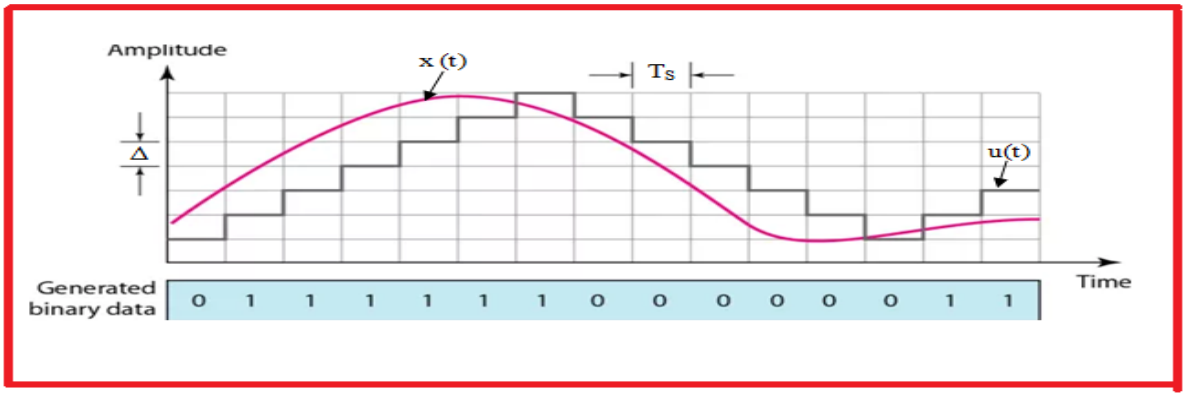
Quantizing using sign and magnitude.

+25 0011001 +39 0100111 -50 1110010
+38 0100110 +26 0011010 +52 0110100
+49 0110001 -15 1001111 +46 0101110

Where sign bit for + is 0 and for – is 1.

Delta Modulation

Delta modulation is a process mainly used in the transmission of voice information. It is a technique where analog-to-digital and digital-to-analog signal conversion are seen. In this technique, the difference between consecutive signal samples is encoded into n-bit data streams. In DM, the data which is to be transmitted is minimized to a 1-bit data stream



Analog to Analog Encoding

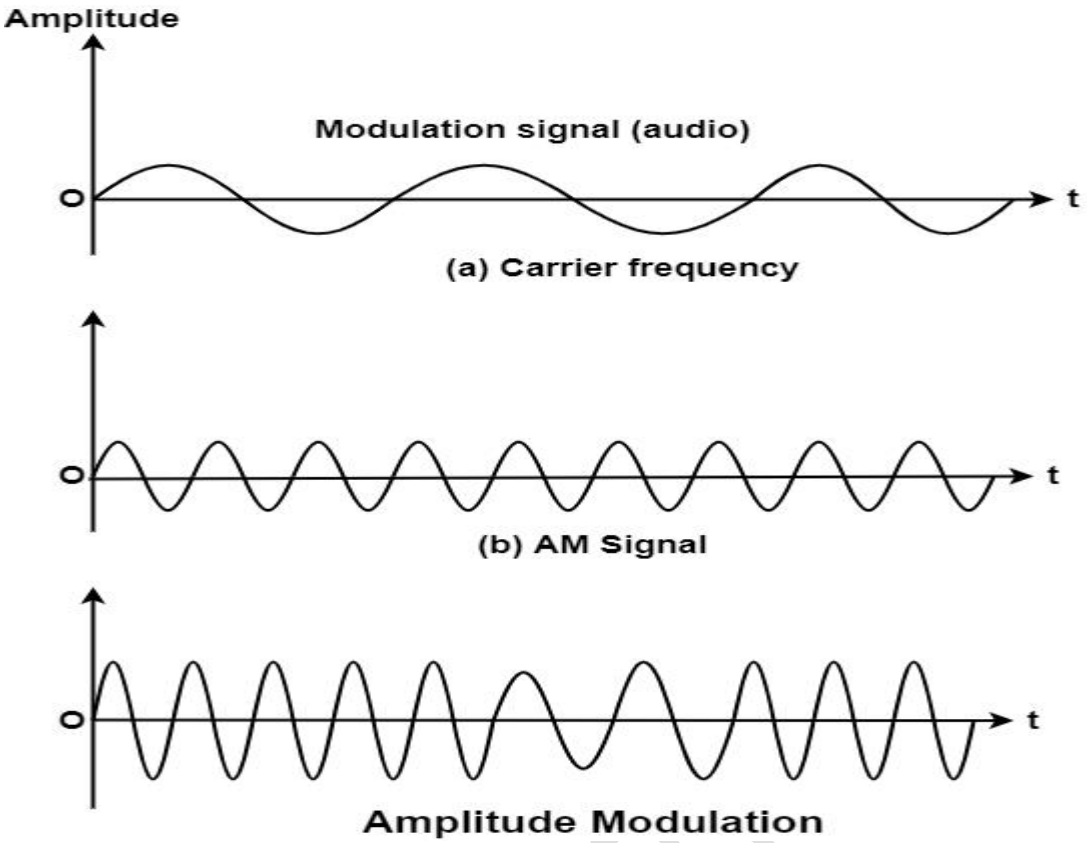
It is the description of analog data by an analog signal. Modulation of analog signals means converting analog signals to an analog signal. It is required because the sender's signal is of low pass and can be of the same range. For example, each radio station has a low pass signal, which may be of the same range. Different stations signal to avoid intermixing; each low pass signal must be shifted to a diverse range on the frequency band.

The diagram shows the relationship between the analog information, the analog-to-analog conversion hardware, and the resultant analog signal.

Analog-to-Analog modulation can be achieved in three ways as under −

Amplitude Modulation

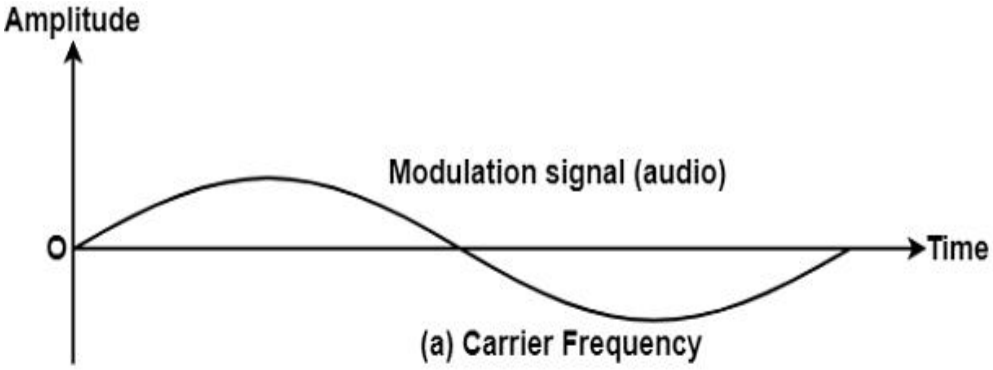
In AM transmission, the carrier signal modulates to vary with the modulation signal's amplitude.



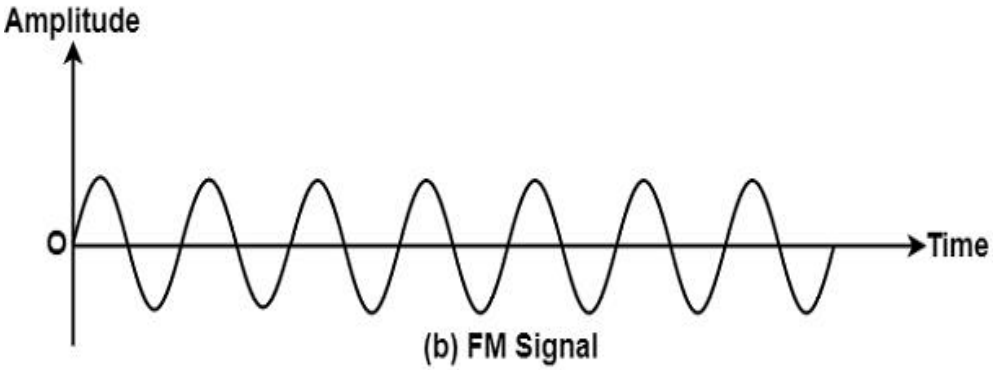
It can be noted that in amplitude modulation, the frequency and phase of the carrier remain constant. The amplitude modifies to follow variations in the data or message signal. The figure shows the concept of the amplitude modulation process. It can be observed that here the modulation signal turn into an envelope to the carrier.

Frequency Modulation

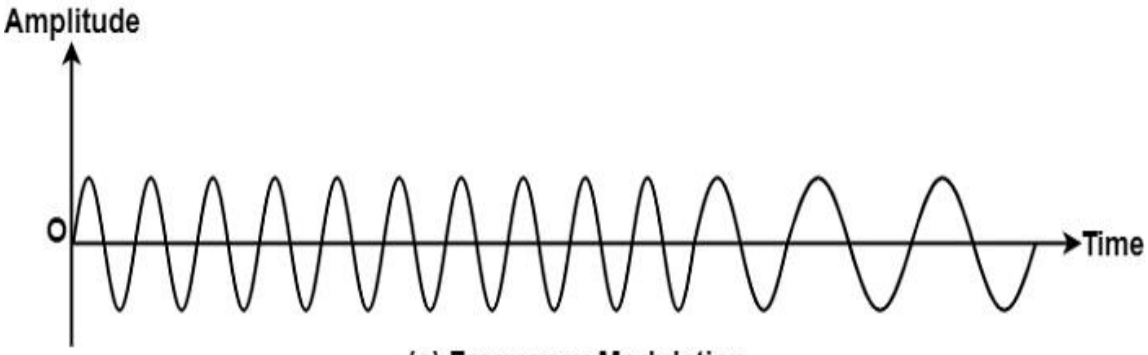
In FM transmission, the carrier signal frequency is modulated (i.e., varied) according to the voltage level variations (i.e., amplitude) of the modulation signal.



(a) Carrier Frequency



(b) FM Signal



(c) Frequency Modulation

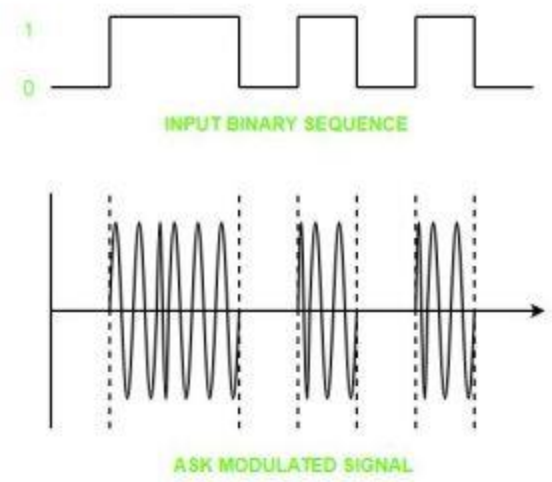
The carrier signal's peak amplitude and phase remain constant, but as the signal amplitude changes, the carrier's frequency changes correspondingly. The figure displays the modulation signal's relationships, the carrier signal, and the resultant FM signal.

Digital to Analog Encoding

Digital Signal – A digital signal is a signal that represents data as a sequence of discrete values; at any given time it can only take on one of a finite number of values. **Analog Signal –** An analog signal is any continuous signal for which the time varying feature of the signal

is a representation of some other time varying quantity i.e., analogous to another time varying signal. The following techniques can be used for Digital to Analog Conversion:

1. Amplitude Shift keying – Amplitude Shift Keying is a technique in which carrier signal is analog and data to be modulated is digital. The amplitude of analog carrier signal is modified to reflect binary data. The binary signal when modulated gives a zero value when the binary data represents 0 while gives the carrier output when data is 1. The frequency



and phase of the carrier signal remain constant.

Advantages of amplitude shift Keying –

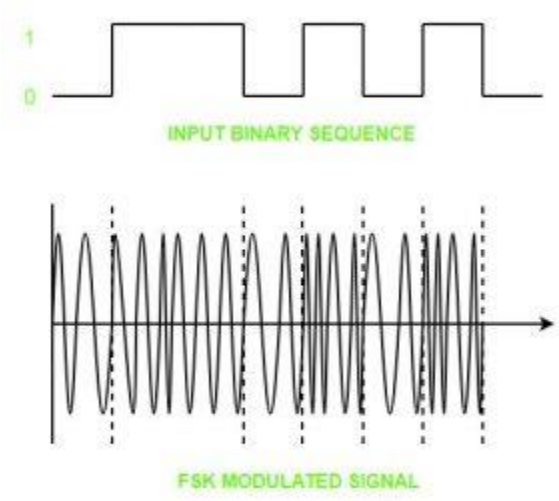
- It can be used to transmit digital data over optical fiber.
- The receiver and transmitter have a simple design which also makes it comparatively inexpensive.

Disadvantages of amplitude shift Keying –

- It is susceptible to noise interference and entire transmissions could be lost due to this.
- It has lower power efficiency.

2. Frequency Shift keying – In this modulation the frequency of analog carrier signal is

modified to reflect binary data. The output of a frequency shift keying modulated wave is high in frequency for a binary high input and is low in frequency for a binary low input. The amplitude and phase of the carrier signal remain constant.



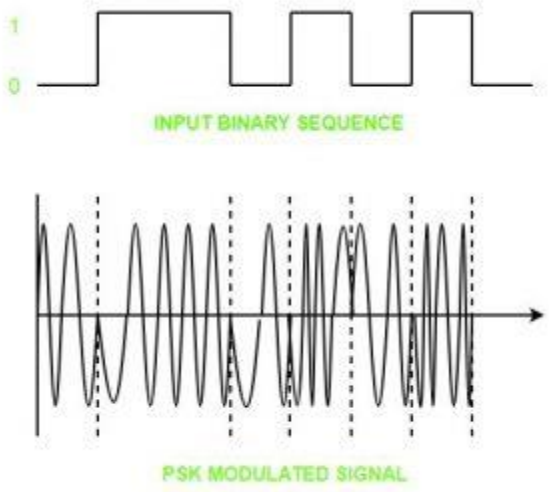
Advantages of frequency shift Keying –

- Frequency shift keying modulated signal can help avoid the noise problems beset by ASK.
- It has lower chances of an error.
- It provides high signal to noise ratio.
- The transmitter and receiver implementations are simple for low data rate application.

Disadvantages of frequency shift Keying –

- It uses larger bandwidth as compared to ASK thus it offers less bandwidth efficiency.
- It has lower power efficiency.

3. Phase Shift keying – In this modulation the phase of the analog carrier signal is modified to reflect binary data.The amplitude and frequency of the carrier signal remains constant.

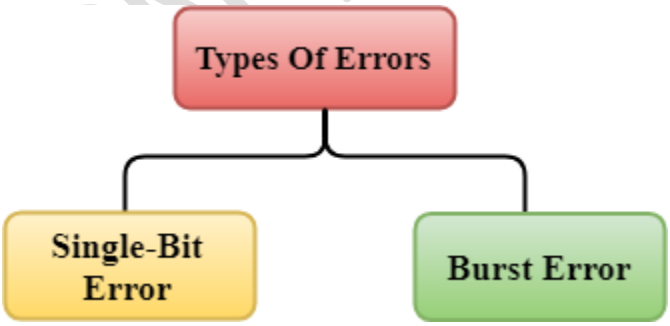


Topic: ERROR DETECTION

Error Detection

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types Of Errors

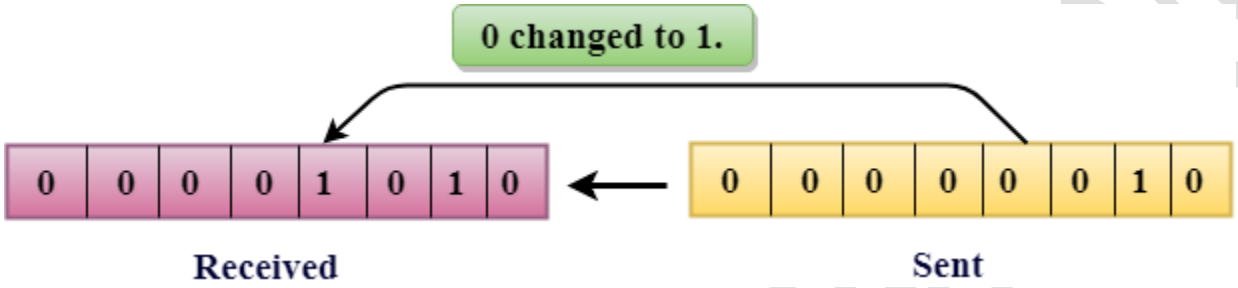


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

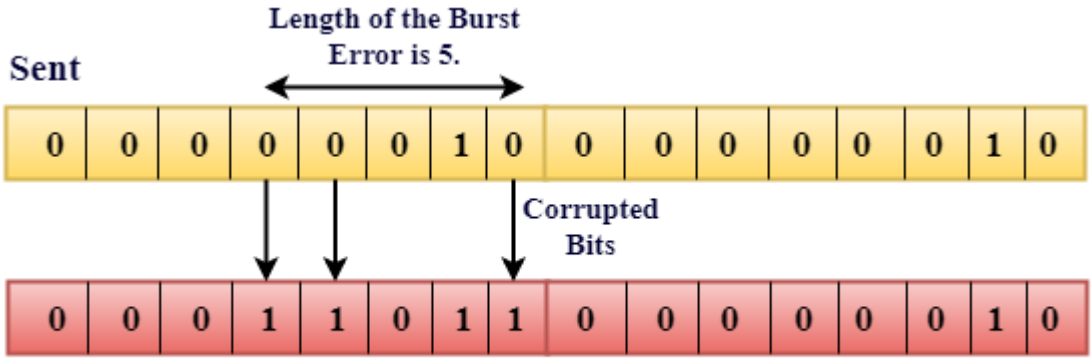
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error:

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

The Burst Error is determined from the first corrupted bit to the last corrupted bit.



The duration of noise in Burst Error is more than the duration of noise in Single-Bit.

Burst Errors are most likely to occurr in Serial Data Transmission.

The number of affected bits depends on the duration of the noise and data rate.

Error Detecting Techniques:

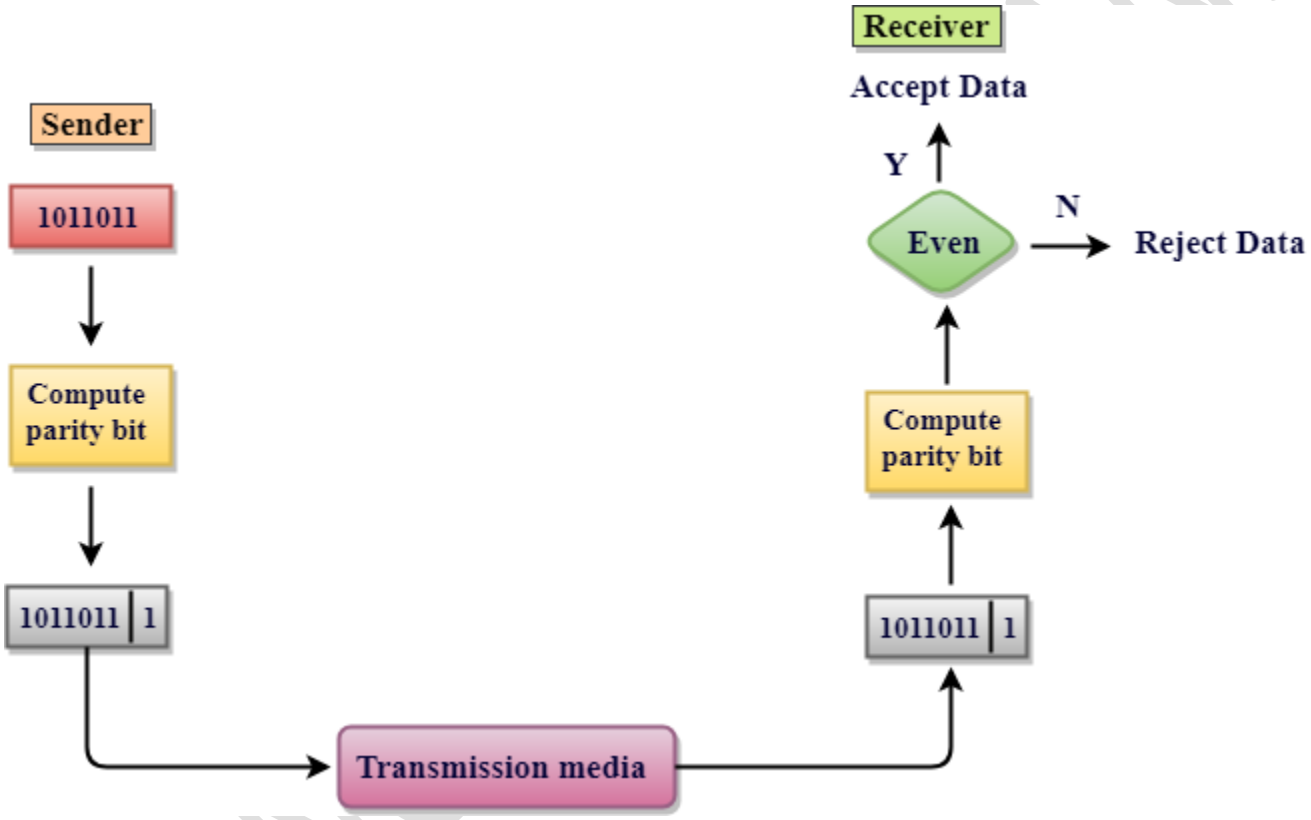
The most popular Error Detecting Techniques are:

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Single Parity Check

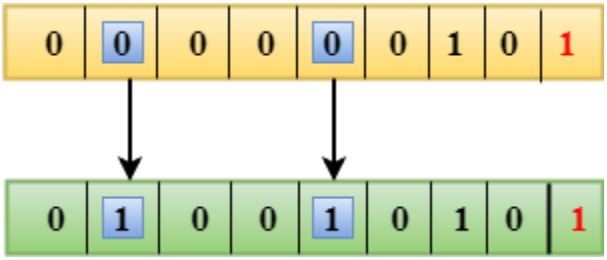
- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.

- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.
- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



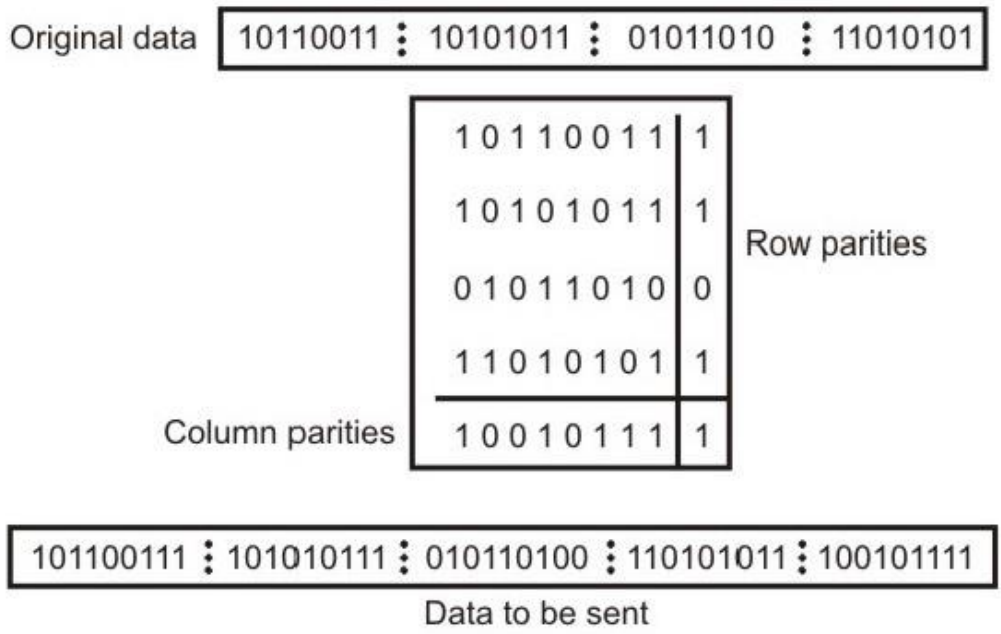
Drawbacks Of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Two-Dimensional Parity Check

- Performance can be improved by using **Two-Dimensional Parity Check** which organizes the data in the form of a table.
- Parity check bits are computed for each row, which is equivalent to the single-parity check.
- In Two-Dimensional Parity check, a block of bits is divided into rows, and the redundant row of bits is added to the whole block.
- At the receiving end, the parity bits are compared with the parity bits computed from the received data.



Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

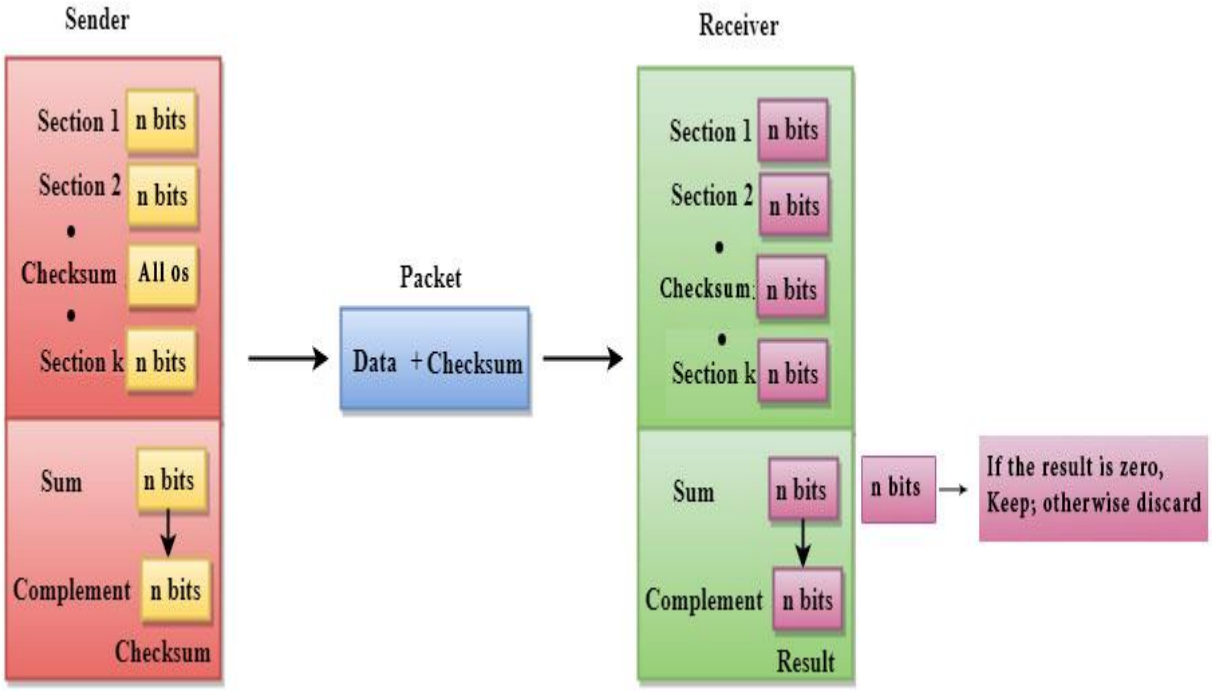
A Checksum is an error detection technique based on the concept of redundancy.

It is divided into two parts:

Checksum Generator

A Checksum is generated at the sending side. Checksum generator subdivides the data into equal segments of n bits each, and all these segments are added together by using one's complement arithmetic. The sum is complemented and appended to the original data, known as checksum field. The extended data is transmitted across the network.

Suppose L is the total sum of the data segments, then the checksum would be ?L



1. The Sender follows the given steps:
2. The block unit is divided into k sections, and each of n bits.
3. All the k sections are added together by using one's complement to get the sum.
4. The sum is complemented and it becomes the checksum field.
5. The original data and checksum field are sent across the network.

NUMERICAL

If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

Sender Site :

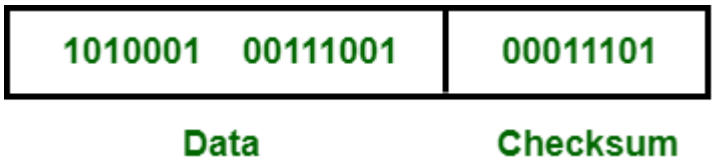
10101001 subunit 1

00111001 subunit 2

11100010 sum (using 1s complement)

00011101 checksum (complement of sum)

Data transmitted to Receiver is –



Checksum Checker

A Checksum is verified at the receiving side. The receiver subdivides the incoming data into equal segments of n bits each, and all these segments are added together, and then this sum is complemented. If the complement of the sum is zero, then the data is accepted otherwise data is rejected.

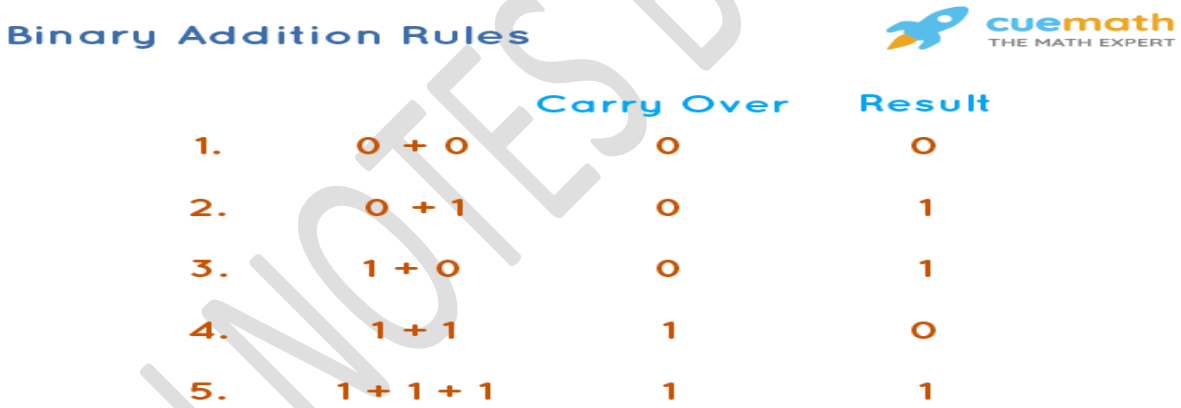
1. The Receiver follows the given steps:
2. The block unit is divided into k sections and each of n bits.
3. All the k sections are added together by using one's complement algorithm to get t he sum.
4. The sum is complemented.
5. If the result of the sum is zero, then the data is accepted otherwise the data is disca rded.

Receiver Site :

10101001	subunit 1
00111001	subunit 2
00011101	checksum
11111111	sum
00000000	sum's complement

Result is zero, it means no error.

NOTE: BINARY ADDER RULES



Cyclic Redundancy Check (CRC)

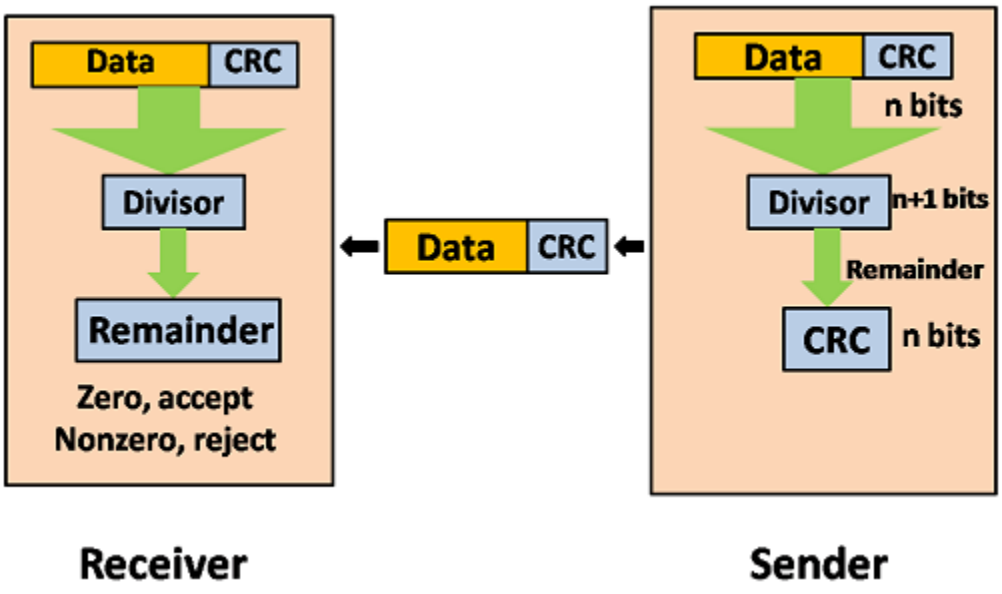
CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

- In CRC technique, a string of n 0s is appended to the data unit, and this n number is less than the number of bits in a predetermined number, known as division which is n+1 bits.
- Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.
- Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.
- The receiver receives the data followed by the CRC remainder. The receiver will treat this whole unit as a single unit, and it is divided by the same divisor that was used to find the CRC remainder.

If the resultant of this division is zero which means that it has no error, and the data is accepted.

If the resultant of this division is not zero which means that the data consists of an error. Therefore, the data is discarded.

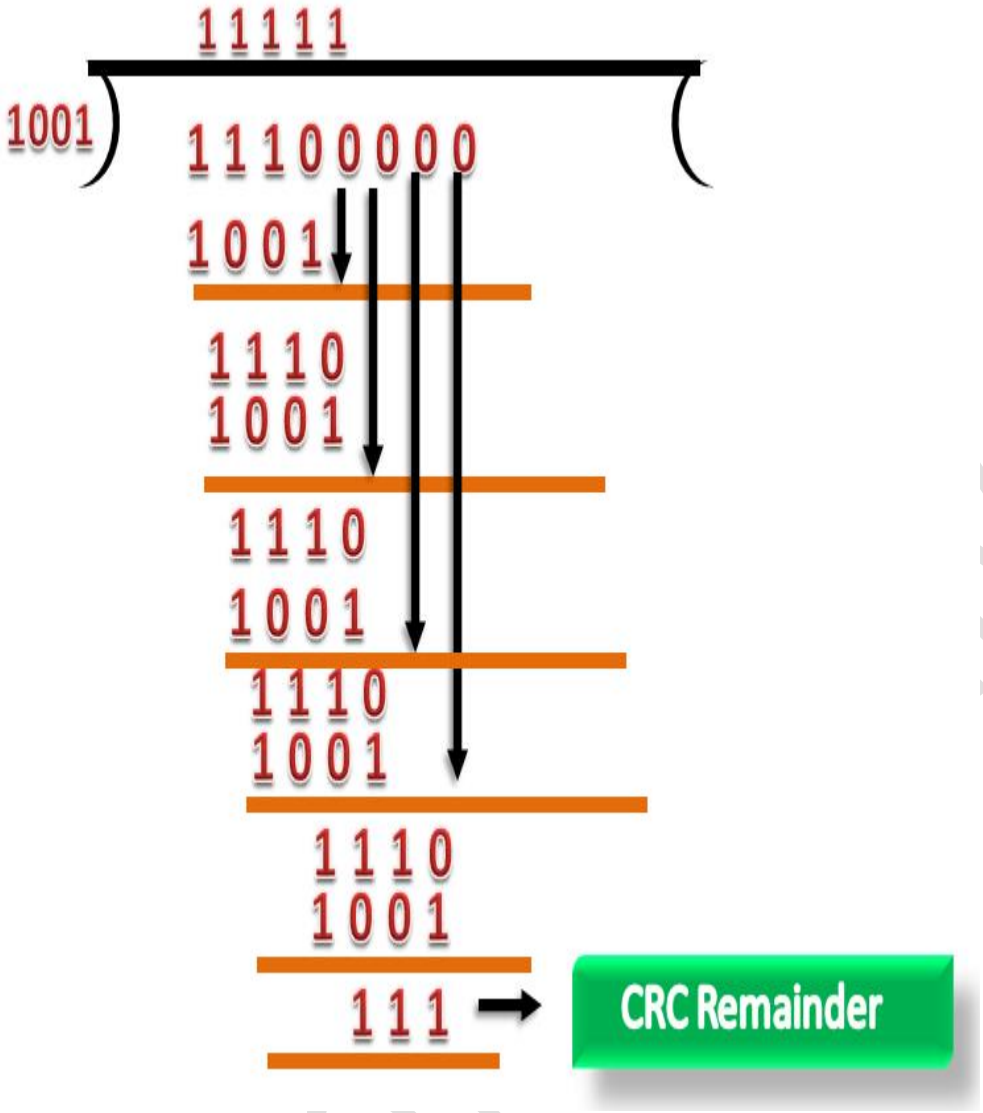


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

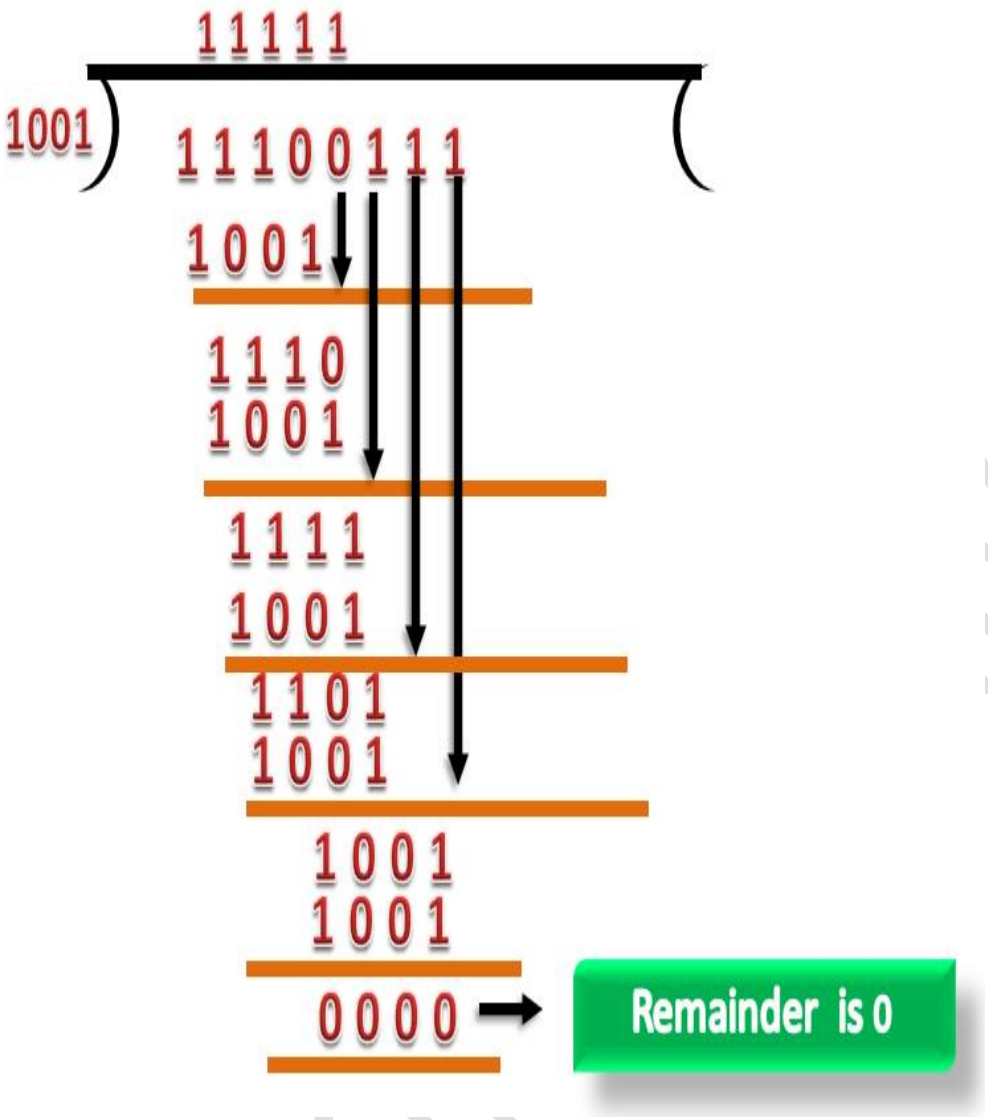
CRC Generator

- A CRC generator uses a modulo-2 division. Firstly, three zeroes are appended at the end of the data as the length of the divisor is 4 and we know that the length of the string 0s to be appended is always one less than the length of the divisor.
- Now, the string becomes 11100000, and the resultant string is divided by the divisor 1001.
- The remainder generated from the binary division is known as CRC remainder. The generated value of the CRC remainder is 111.
- CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string would be 11100111 which is sent across the network.



CRC Checker

- The functionality of the CRC checker is similar to the CRC generator.
- When the string 11100111 is received at the receiving end, then CRC checker performs the modulo-2 division.
- A string is divided by the same divisor, i.e., 1001.
- In this case, CRC checker generates the remainder of zero. Therefore, the data is accepted.



ERROR CORRECTION

Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose r is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$2^r >= d+r+1$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity

bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 1,2,.....2^{k-1}.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Relationship b/w Error position & binary number.

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:

Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

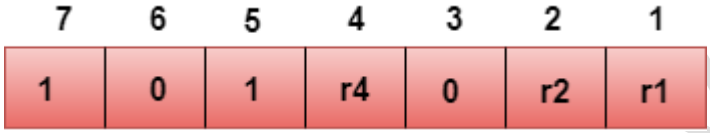
Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

1. The position of r1 = 1
2. The position of r2 = 2
3. The position of r4 = 4

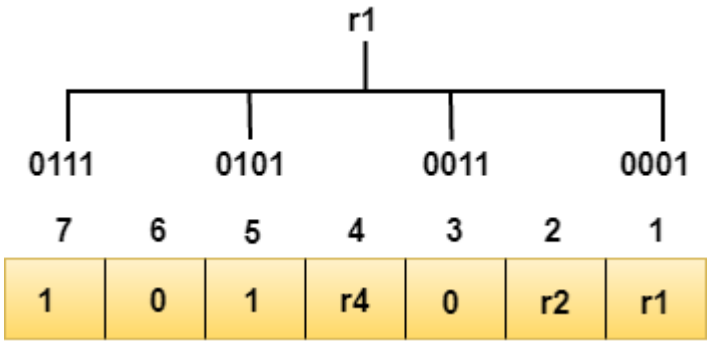
Representation of Data on the addition of parity bits:



Determining the Parity bits

Determining the r1 bit

The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.

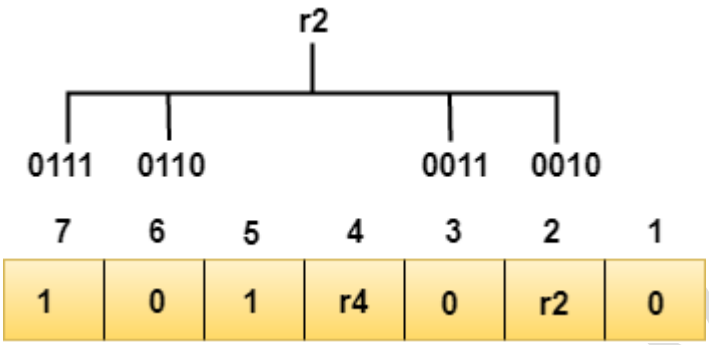


We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total

number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

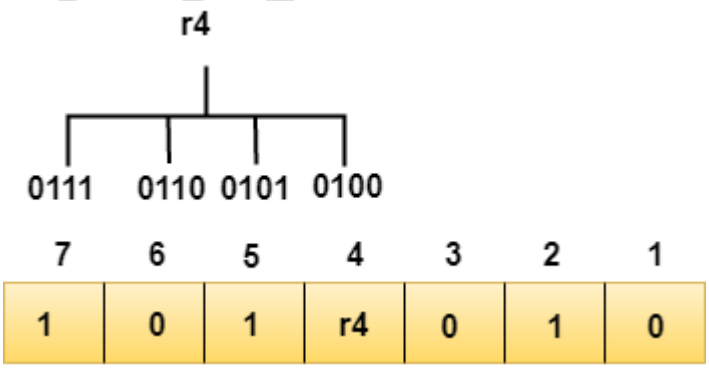
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

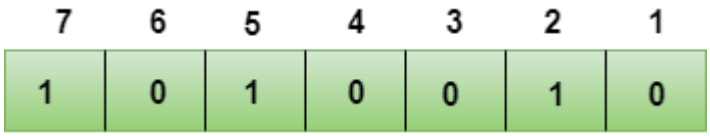
Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

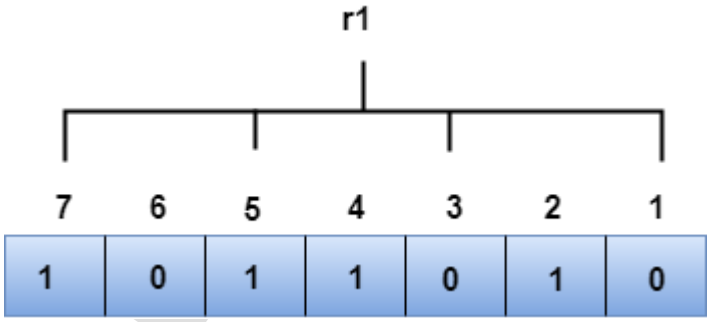
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

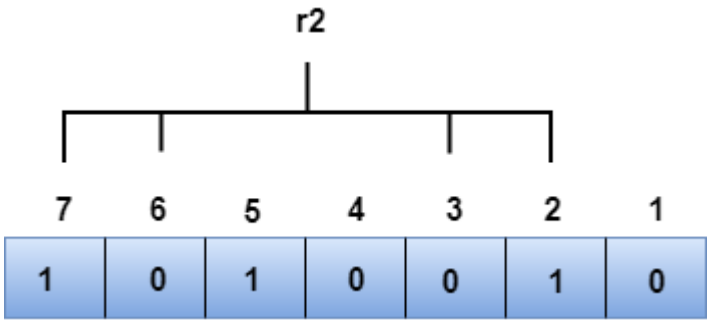
The bit positions of the r1 bit are 1,3,5,7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

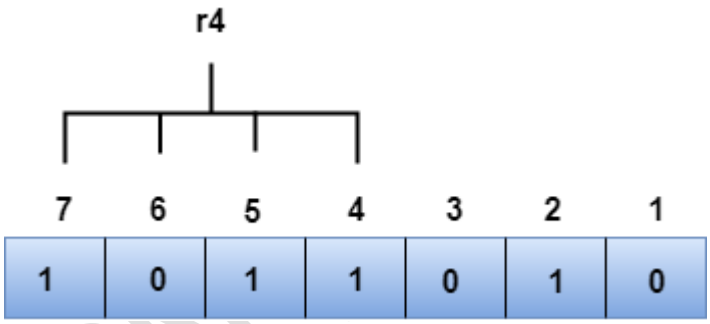
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1.

- *The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4^{th} bit position. The bit value must be changed from 1 to 0 to correct the error.*

TOPIC: MULTIPLEXING

Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (**MUX**) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

Demultiplexing is achieved by using a device called Demultiplexer (**DEMUX**) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach.

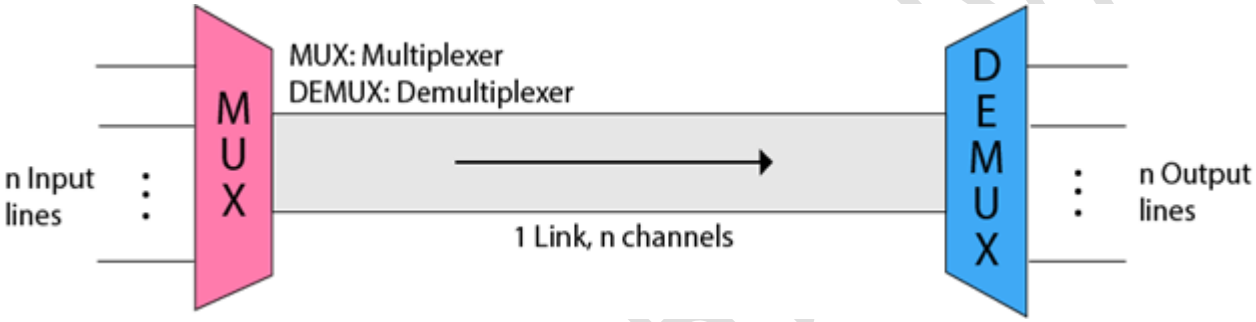
Why Multiplexing?

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.

History of Multiplexing

- Multiplexing technique is widely used in telecommunications in which several telephone calls are carried through a single wire.
- Multiplexing originated in telegraphy in the early 1870s and is now widely used in communication.
- George Owen Squier developed the **telephone carrier multiplexing** in 1910.

Concept of Multiplexing



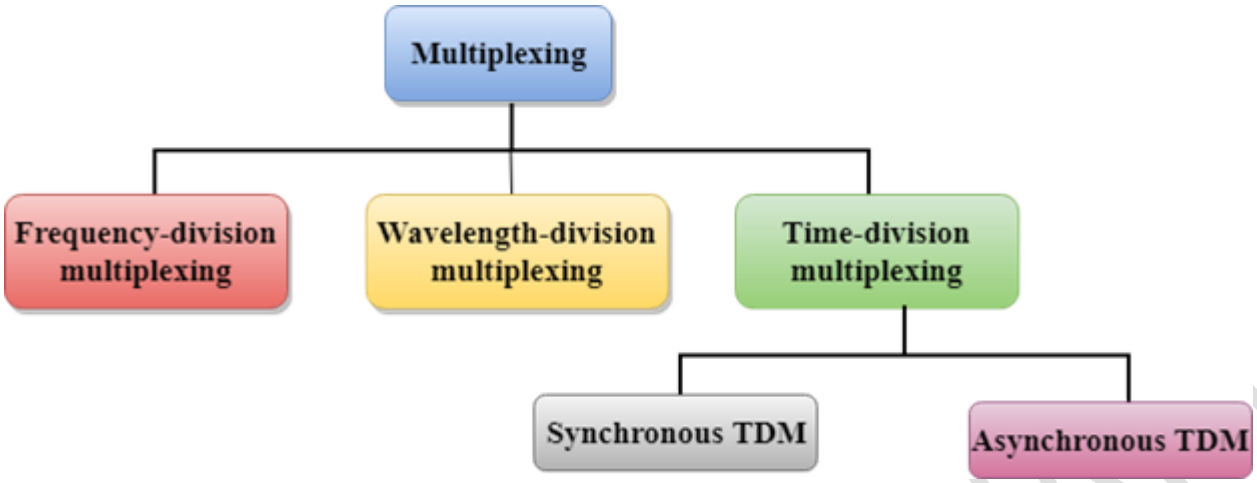
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

Advantages of Multiplexing:

- More than one signal can be sent over a single medium.
- The bandwidth of a medium can be utilized effectively.

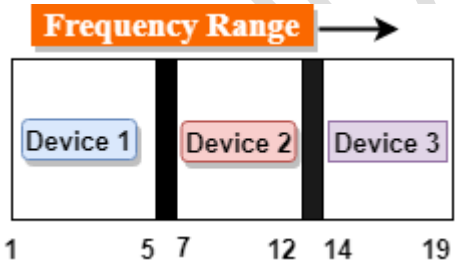
Multiplexing Techniques

Multiplexing techniques can be classified as:

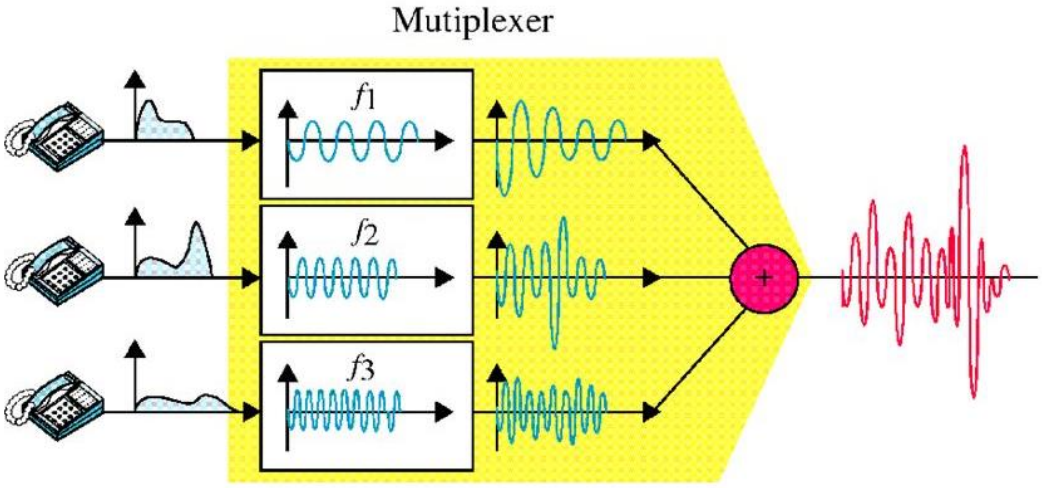


Frequency-division Multiplexing (FDM)

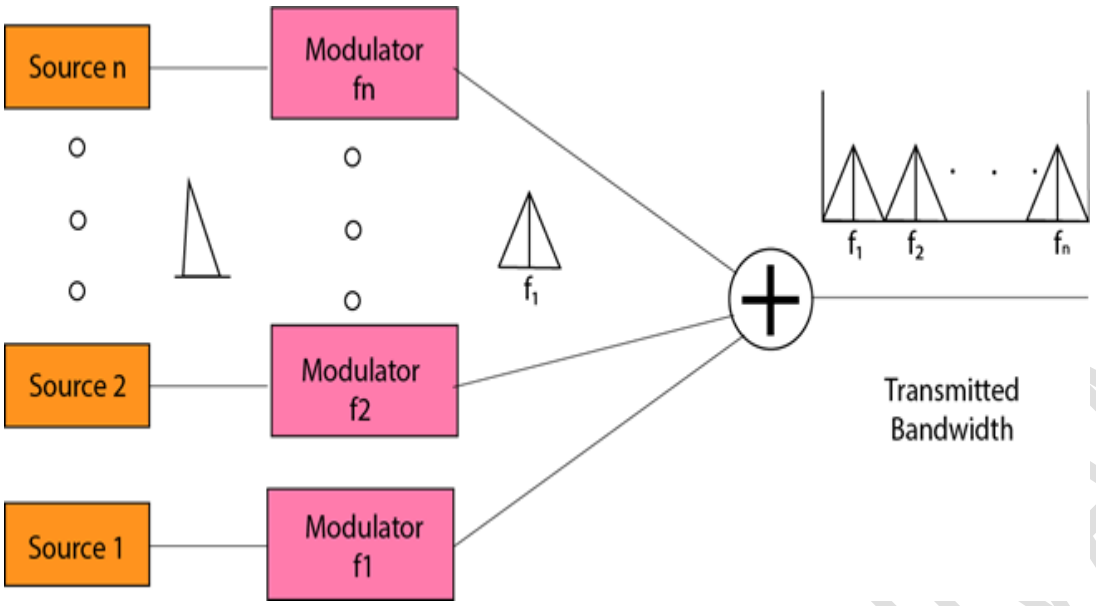
- It is an analog technique.
- **Frequency Division Multiplexing** is a technique in which the available bandwidth of a single transmission medium is subdivided into several channels.



■ FDM multiplexing process, time-domain



- In the above diagram, a single transmission medium is subdivided into several frequency channels, and each frequency channel is given to different devices. Device 1 has a frequency channel of range from 1 to 5.
- The input signals are translated into frequency bands by using modulation techniques, and they are combined by a multiplexer to form a composite signal.
- The main aim of the FDM is to subdivide the available bandwidth into different frequency channels and allocate them to different devices.
- Using the modulation technique, the input signals are transmitted into frequency bands and then combined to form a composite signal.
- The carriers which are used for modulating the signals are known as **sub-carriers**. They are represented as f1,f2..fn.
- **FDM** is mainly used in radio broadcasts and TV networks.



Advantages Of FDM:

- FDM is used for analog signals.
- FDM process is very simple and easy modulation.
- A Large number of signals can be sent through an FDM simultaneously.
- It does not require any synchronization between sender and receiver.

Disadvantages Of FDM:

- FDM technique is used only when low-speed channels are required.
- It suffers the problem of crosstalk.
- A Large number of modulators are required.
- It requires a high bandwidth channel.

Applications Of FDM:

- FDM is commonly used in TV networks.

- It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Time Division Multiplexing

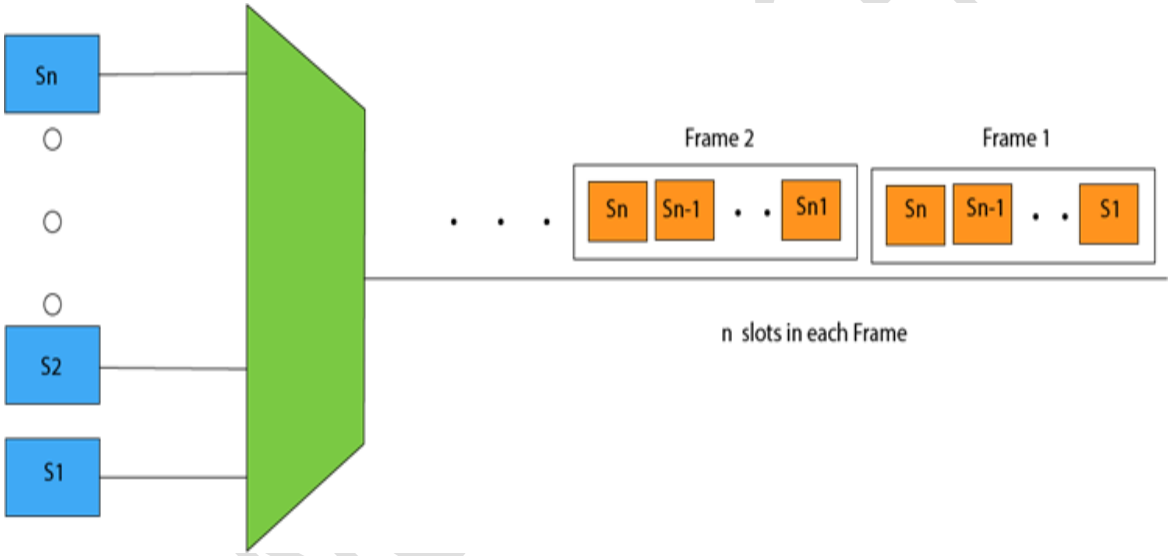
- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

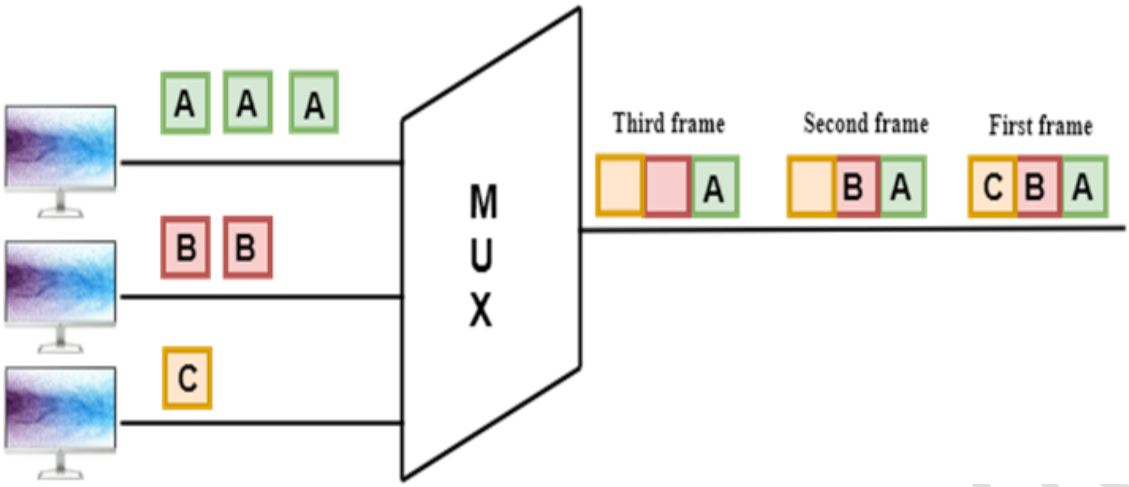
- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- A Synchronous TDM is a technique in which time slot is preassigned to every device.
- In Synchronous TDM, each device is given some time slot irrespective of the fact that the device contains the data or not.
- If the device does not have any data, then the slot will remain empty.
- In Synchronous TDM, signals are sent in the form of frames. Time slots are organized in the form of frames. If a device does not have data for a particular time slot, then the empty slot will be transmitted.
- The most popular Synchronous TDM are T-1 multiplexing, ISDN multiplexing, and SONET multiplexing.
- If there are n devices, then there are n slots.



Concept Of Synchronous TDM



In the above figure, the Synchronous TDM technique is implemented. Each device is allocated with some time slot. The time slots are transmitted irrespective of whether the sender has data to send or not.

Disadvantages Of Synchronous TDM:

- The capacity of the channel is not fully utilized as the empty slots are also transmitted which is having no data. In the above figure, the first frame is completely filled, but in the last two frames, some slots are empty. Therefore, we can say that the capacity of the channel is not utilized efficiently.
- The speed of the transmission medium should be greater than the total speed of the input lines. An alternative approach to the Synchronous TDM is Asynchronous Time Division Multiplexing.

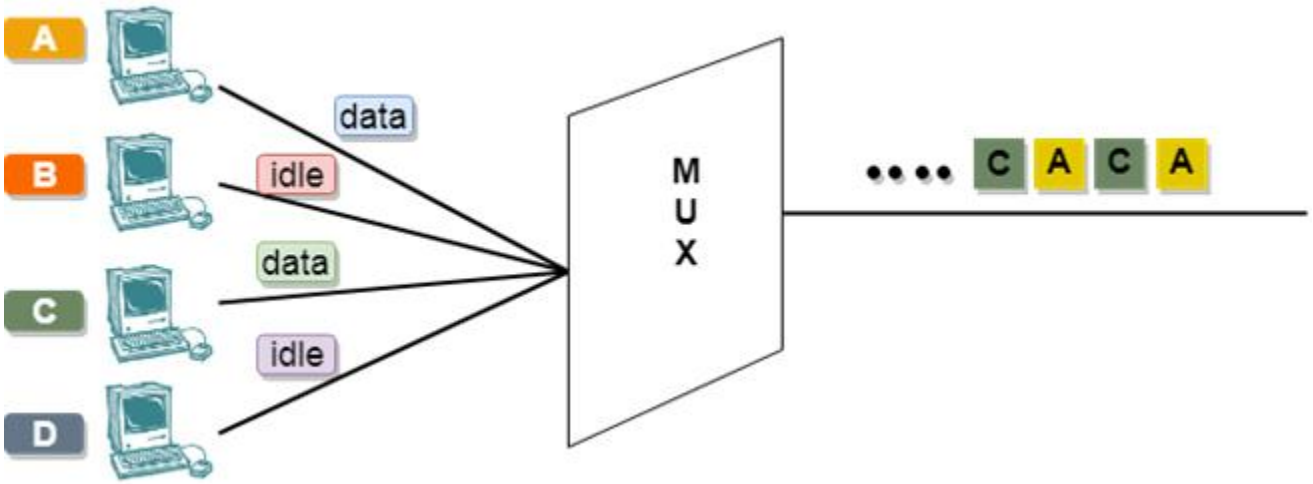
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.

- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

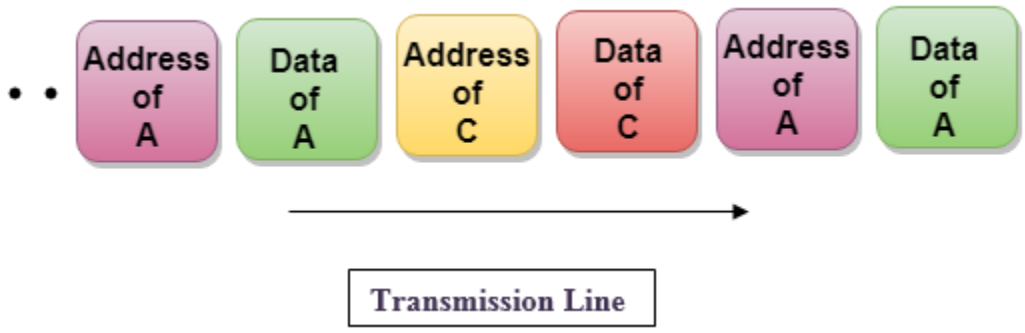
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are n sending devices, then there are n time slots. In Asynchronous TDM, if there are n sending devices, then there are m time slots where m is less than n (**m<n**).
- The number of slots in a frame depends on the statistical analysis of the number of input lines.

Concept Of Asynchronous TDM



In the above diagram, there are 4 devices, but only two devices are sending the data, i.e., A and C. Therefore, the data of A and C are only transmitted through the transmission line.

Frame of above diagram can be represented as:



The above figure shows that the data part contains the address to determine the source of the data.

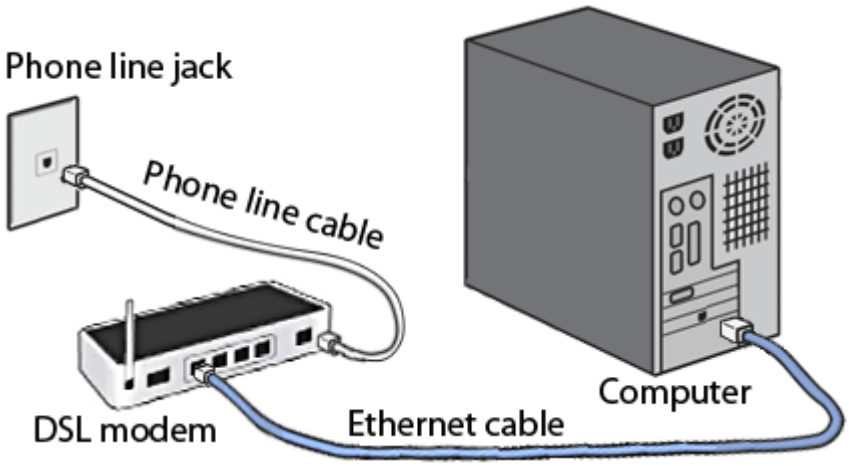
Topic: DSL

The Digital Subscriber Line (DSL), *originally*, a **digital subscriber loop** is a communication medium, which is used to transfer the internet through copper wire telecommunication lines. Along with cable internet, DSL is one of the most popular ways

ISPs provide broadband internet access.

Properties of DSL

- Its aim is to maintain the high speed of the data being transferred.
- If we ask how we going to achieve such a thing i.e., both telephone and internet facilities, then the answer is by using *splitters or DSL filters*(shown in the below diagram). Basically, the *splitter* is used to split the frequency and make sure that it can't get interrupted.



Types of DSL

- **SDSL:** Symmetric DSL provides equal bandwidth for both uploading and downloading and is mostly preferred by small organizations.
- **ADSL:** Asymmetric DSL. Most users download more data than they upload; for this, they use ADL. In this, downstream speed is much more than upstream. The uploading capacity may not work as well as downloading capacity. Users who do not upload that much in comparison to downloading can use ASDL. It may offer as high as 20 Mbps speed for downloading while uploading 1.5 Mbps.

Features

- It is widely available.
- It is less costly and offers more security.
- It is much more reliable than other broadband services.
- It offers less speed than broadband service.
- It provides a limited range due to which internet quality is affected due to the larger distance between the main hub DSL provider and the receiver.