Lecture Notes

Data Communication & Computer Networking

Prepared By:
SUBHAJIT PANDA, ASST.PROF., (CSE)CVRP

UNIT-1 NETWORK& PROTOCOL

1.1 INTRODUCTION TO DATA COMMUNICATION

□□ Data Communication is the exchange of data between two devices via some form of transmission medium (such as a wire cable).

□□ The purpose of data communication is to exchange information between two agents.

□□ The communicating device must be part of a communication system made up of a combination of hardware and software

1.1.1 COMPONENTS OF DATA COMMUNICATION SYSTEM-

A Communication system has following components:

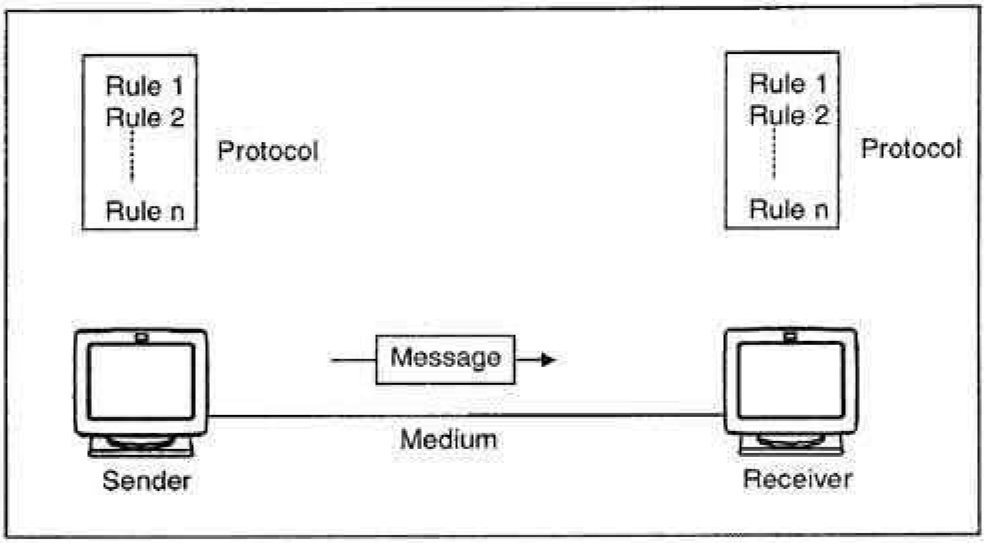
1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. **Sender**: It is the device/computer that generates and sends that message.

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.



1.1.2 THE EFFECTIVENESS DEPENDS ON FOUR FUNDAMENTAL CHARACTERISTICS OF DATA COMMUNICATIONS

1. Delivery:
The system must deliver data to the exact destination. Data must not be received by other devices than the target device.

2. Accuracy:

The system must deliver data to the destination in a way that the target device receives the data accurately. If the protocol needs to alter the while in transmission, it must alter it back to its original form before representing it to the target device. The accuracy must be maintained.

3. Timeliness:

The system must deliver data in timely manner. Data delivered late can become useless. Data must be delivered as they are produced, in the order they are produced and without any significant delay.

4. Jitter:

Jitter refers to the variation of packet arrival time. Data is sent as packets, that is, a fixed amount of the whole data is sent in each to turn. These packets get joined back in the target device to represent the complete data as it is. Each packet is sent with a predefined delay or acceptable amount delay. If packets are sent without maintaining the predefined delay then an uneven quality in the data might result.

Data Representation-

Information can be in the form of text, numbers, images, audio, and video.

Text

Text symbols are represented with a sequence of bits 0 or 1. Each sequence is called a code, and the process is called coding. Two coding standards are

- Unicode
- ASCII

Unicode

Unicode is an international coding standard where each letter, digit, or symbol is represented with the unique sequence of 32 0s and 1s. So this code can define 232 characters. It can be used in different languages.

Notation: U-XXXXXXXX

where X = hexadecimal number and ranges from 0 to F.

ASCII

American Standard Code for Information Interchange is a coding standard where each letter, number or symbol is represented with a unique sequence of 7 0s and 1s. So this code can define 27 (128) characters. It is used for the English language only.

ASCII (Basic Latin) is a subset of Unicode and occupies first 7 bits of Unicode for 128 codes and is represented in hexadecimal form as:

00000000 – 0000007F

Number

Numbers are also represented with a sequence of 0 and 1. ASCII is not used for number representation. Instead, the following numbering system is used in order to simplify the mathematical operations:

- Base 10 (decimal)
- Base 2 (binary)
- Base 8 (octal)
- Base 16 (hexadecimal)
- Base 256 (IP address)

Note: Number = 789456

Symbol = 7 8 9 4 5 6

Position = 5 4 3 2 1 0

Images

An image is also represented with a sequence of 0 and 1. A digital image is made up of small units called pixels. Each pixel is assigned a bit pattern whose size depends on the nature of the image.

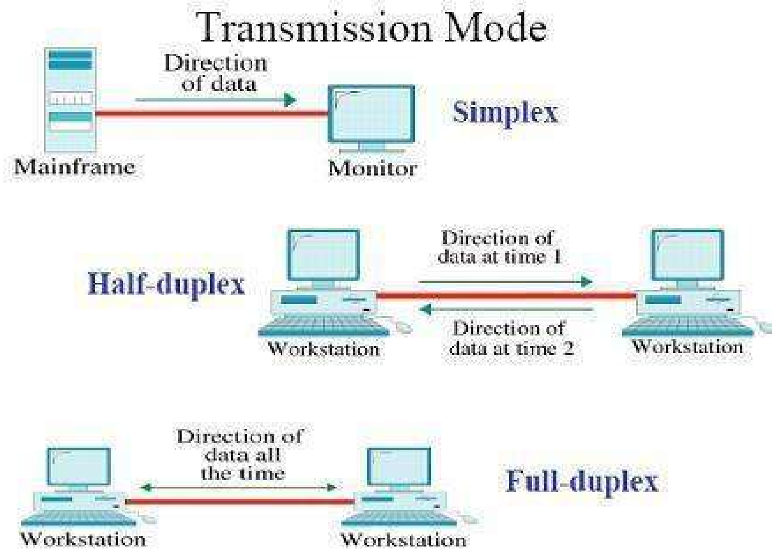
Audio

A sound which lies within the human hearing frequency range of 20 to 20000 Hertz is called audio. The sound is recorded with a microphone and then digitized to represent in the form of bit-patterns. Its transmitted form is called an audio signal.

Video

Flashing a sequence of images on the display screen which gives us a sensation of moving objects is called a video. A video is recorded with a camera and transmitted as a video signal.

Data Flow-



Data Flow in communication have the following types:

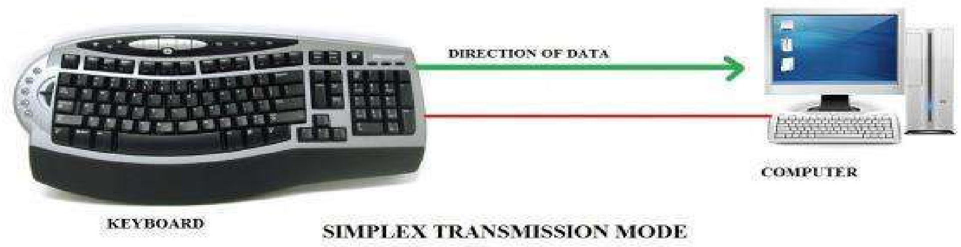
1. Simplex
2. Half duplex
3. Full duplex

1. Simplex:

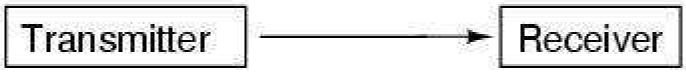
In simplex data flow only in one direction. Its mean in simplex if two devices are connected only one device will send data the other device will only receive data it can not send.

In this type channel will use all of its capacity only in sending data.

Example of this type is: Mouse (it can only input data etc)



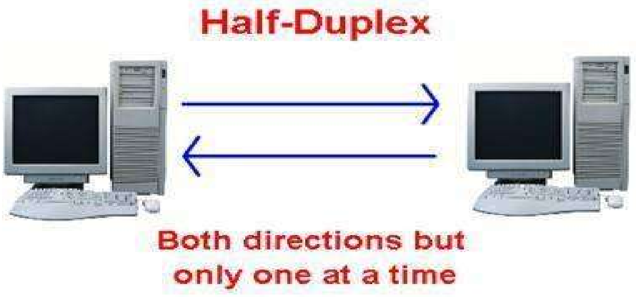
Simplex communication



2. Half duplex:

In this type of data flow, data will flow in both directions but not at the same time. For example: If two devices are connected both of them can send information to each other but not at the same time. When one device will send data the other will receive it cannot send back at the same time after receiving it can send data.

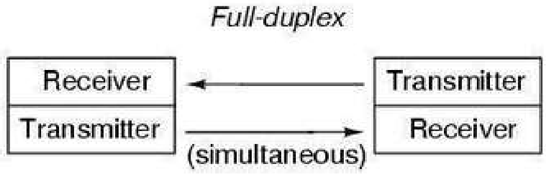
In half duplex channel will use all of its capacity for each direction. So this type will be used in the communication in which there is no need of response at the same time. Example of this type is Walkie Talkies.



3. Full Duplex:

In Full Duplex data will flow in both directions at the same time. For Example: If two devices are connected in communication both of them can send and receive data at the same time.

In Full Duplex channel will divide all of its capacity in both directions. Full Duplex is used when communication is required in both directions at the same time. Example of Full Duplex is calling on mobile phone etc.



1.2 NETWORK

A network is a set of devices connected by a media links .A node can be a computer, printer or any other device capable of sending or receiving data generated by other nodes on the network.

The three criteria necessary for an effective and efficient network

- **Performance**
- **Reliability**
- **Security**

The factors that affect the performance of a network

- **Number of users**-The design of a given network is based on an assessment of the average number of users that will be communicating at any one time.
- **Type of transmission medium**-The medium defines the speed at which the data can travel through a connection. Today’s network uses fiber-optic cable for faster and faster transmission.
- **Hardware**-The types of hardware included in a network effect both speed and capacity of transmission.
- **Software**- It used to process the data at the sender, receiver and intermediate node also.

1.2.2 TYPES OF COMMUNICATION NETWORKS

Communication Networks can be of following 5 types:

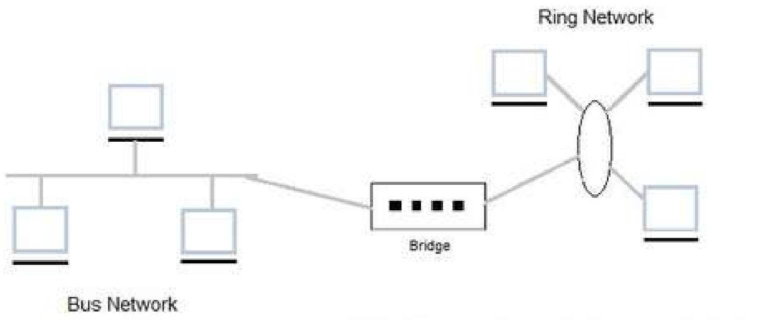
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Wireless
- Inter Network (Internet)

Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



(Different Topologies interconnected in a Local Area Network)

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages

1. Resource Sharing: Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
2. Software Applications Sharing: It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
3. Easy and Cheap Communication: Data and messages can easily be transferred over networked computers.

4. Centralized Data: The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
5. Data Security: Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
6. Internet Sharing: Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

Disadvantages

1. High Setup Cost: Although the LAN will save cost over time due to shared

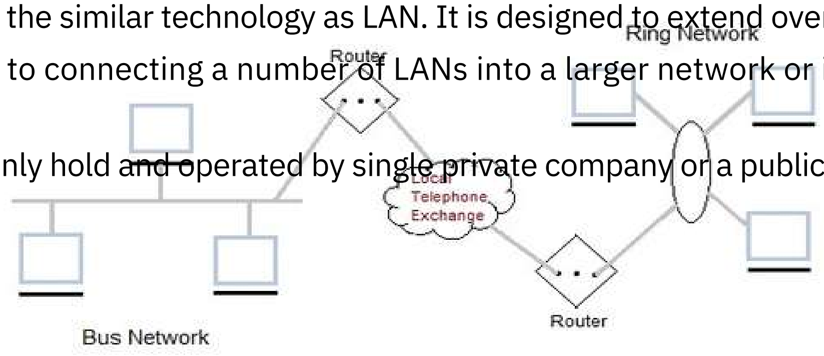
computer
resources, but the initial setup costs of installing Local Area Networks is high.
2. Privacy Violations: The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use
history of the LAN user.
3. Data Security Threat: Unauthorized users can access important data of an organization
if centralized data repository is not secured properly by the LAN administrator.
4. LAN Maintenance Job: Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances

in
Local Area Network. A LAN Administrator is needed at this full time job.
~~**5. Covers Limited Area:** Local Area~~ Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

It was developed in 1980s.It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It
can be means to connecting a number of LANs into a larger network or it can be a

single
cable. It is mainly hold and operated by single private company or a public company.



Characteristics of MAN
It generally covers towns and cities (50 km)
Communication medium used for MAN are optical fibers, cables etc. Data rates adequate for distributed computing applications.

Advantages of MAN

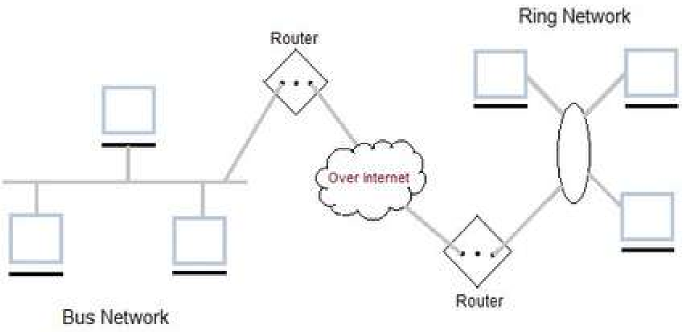
1. Extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.
2. It provides a good back bone for large network and provides greater access to WANs. The dual bus used in MAN helps the transmission of data in both directions simultaneously. 3. A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

1. More cable required for a MAN connection from one place to another.
2. It is difficult to make the system secure from hackers and industrial espionage (spying) graphical regions.

Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



Characteristics

1. It generally covers large distances (states, countries, continents).
2. Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages

1. Covers a large geographical area so long distance business can connect on the one network.
2. Shares software and resources with connecting workstations.
3. Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them (called attachments).
4. Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.

Disadvantages

1. Need a good firewall to restrict outsiders from entering and disrupting the network.
2. Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
3. Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.

4. Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better

performance,
but the basic idea is the same.
Wireless Networks can be divided into three main categories:

□ System
□ Interconnection
□ Wireless LANs
Wireless WANs

Inter Network

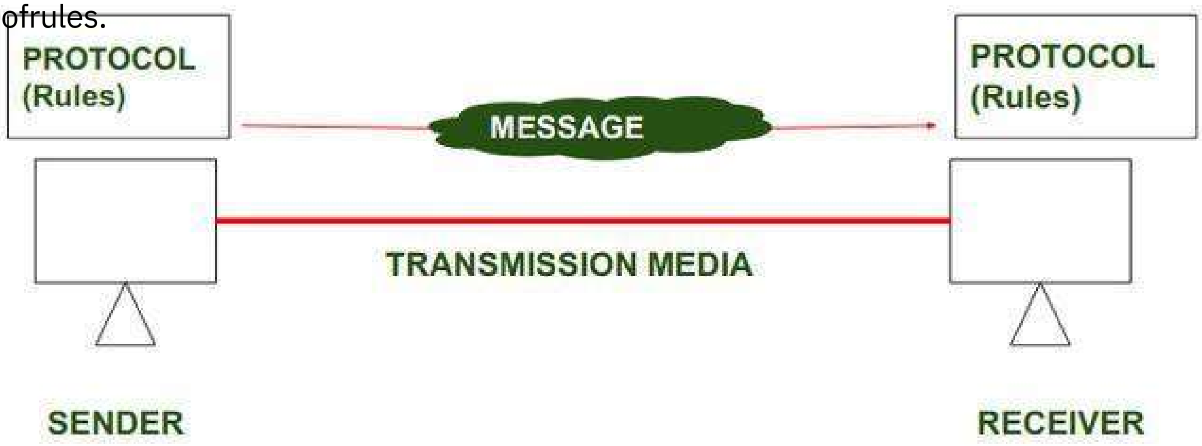
Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.

1.3 PROTOCOL&ARCHITECTURE

□

A protocol is a set of rules that governs data communication. A protocol defines what is communicated, how it is communicated and when it is communicated.

□ Layeredstructureofhardwareandsoftwarethatsupportstheexchangeofdatabetween systemsaswellasadistributedapplication(e.g.emailorfiletransfer)•Eachprotocolprov idesasetofrules.



□

□ **A protocol performs the following functions:**

□ 1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

□ 2. **Data routing**. Data routing defines the most efficient path between the source and destination.

□ 3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

□ 4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

□ 5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

□ 6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

□ 7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

□ 8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

□ **9. Log information.** Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

NEED FOR PROTOCOL ARCHITECTURE

When computers, terminals and other data processing devices exchange data, the procedures involved can be quite complex. Consider for example, the transfer of a file between two computers. There must be a data path between the two computers, either directly or via a communication network.

Typical task to be performed are as follows-

□ The source system must either activate the direct data communication path or inform the communication network of the identity of the desired destination system.

□ The source system must ascertain that the destination system is prepared to receive data.

□ The file transfer application on the source system must ascertain that the file management program on the destination system is prepared to accept and store the file for this particular user.

□ If the file formats used on the two systems are different, one or the other system must perform a format translation function.

Instead of implementing the logic for this as a single module, the task is broken up into subtasks, each of which is implemented separately. In a protocol architecture, the modules are arranged in a vertical stack. Each layer in the stack performs a related subset of the functions required to communicate with another system.

It takes two to communicate so the same set of layered functions must exist in two systems. Communication is achieved by having the corresponding, or peer, layers in two systems communicate. The peer layers communicate by means of formatted blocks of data that obey a set of rules known as a protocol.

The key features of a protocol are as follows-

□

Syntax: – Syntax refers to the structure or format of the data, meaning the order in which they are presented.

□ **Semantics: –** Semantics refer to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?

□

Timing: – Timing refers to two characteristics: when data should be sent and how fast they can be sent.

StandardizedProtocolArchitectures

□ Required for devices to communicate

□ Vendors have more marketable products

□ Customers can insist on standards based equipment

□ Two standards:–

□

OSI Reference model

□

TCP/IPprotocolsuite

OSI Reference Model

1.4.1 OSI Model

o OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

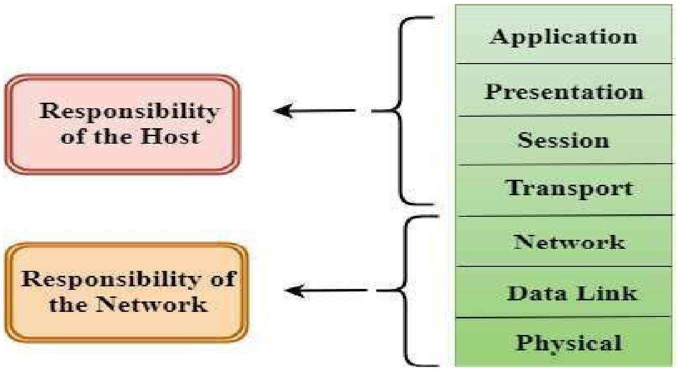
o OSI consists of seven layers, and each layer performs a particular network function.

o OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.

o OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

o Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



o The OSI model is divided into two layers: upper layers and lower layers.

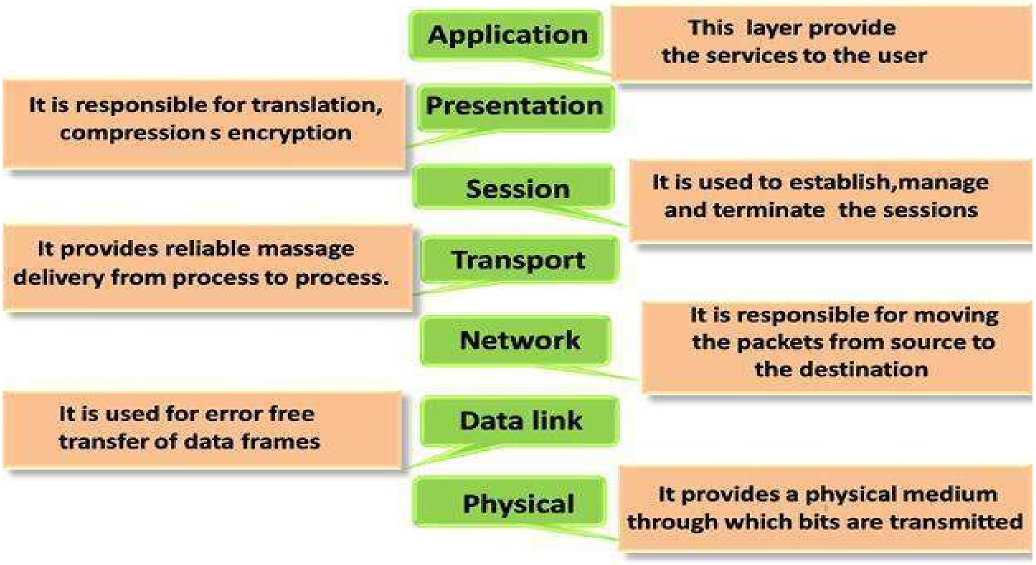
o The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

o The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

Functions of the OSI Layers

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer


Application
This layer provide the services to the user
It is responsible for translation, compression s encryption
Presentation
Session
It is used to establish,manage and terminate the sessions
It provides reliable massage delivery from process to process.
Transport
Network
It is responsible for moving the packets from source to the destination
It is used for error free transfer of data frames
Data link
Physical
It provides a physical medium through which bits are transmitted

Physical layer

o The main functionality of the physical layer is to transmit the individual bits from one node to another node.

o It is the lowest layer of the OSI model.

o It establishes, maintains and deactivates the physical connection.

o It specifies the mechanical, electrical and procedural network interface specifications.

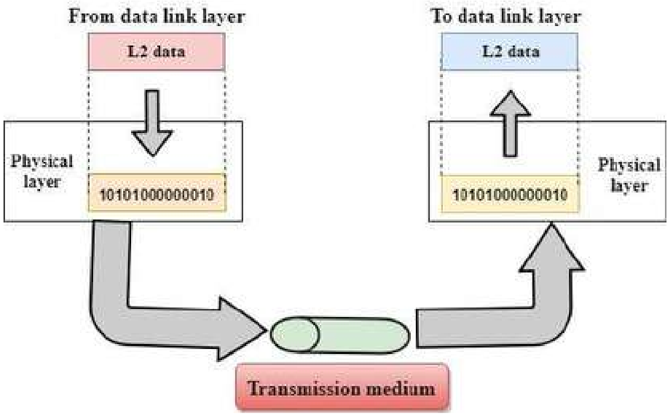
Functions of a Physical layer:

o **Line Configuration:** It defines the way how two or more devices can be connected physically.

o **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

o **Topology:** It defines the way how network devices are arranged.

o **Signals:** It determines the type of the signal used for transmitting the information.



Data-Link Layer

o This layer is responsible for the error-free transfer of data frames.

o It defines the format of the data on the network.

o It provides a reliable and efficient communication between two or more devices.

o It is mainly responsible for the unique identification of each device that resides on a local network.

o It contains two sub-layers:

o **Logical Link Control Layer**

o It is responsible for transferring the packets to the Network layer of the receiver that is receiving.

o It identifies the address of the network layer protocol from the header.

o It also provides flow control.

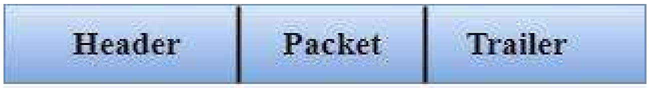
o **Media Access Control Layer**

o A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.

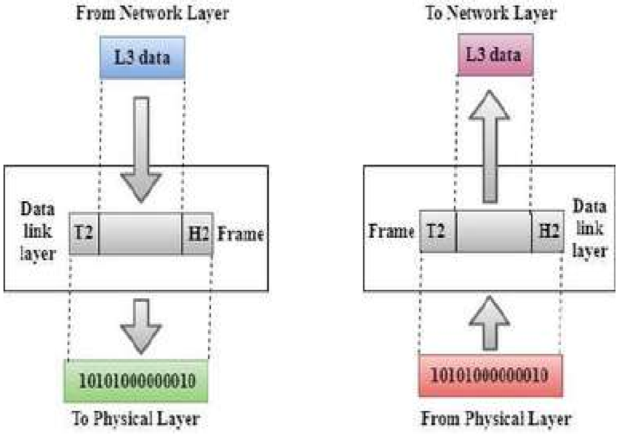
o It is used for transferring the packets over the network.

Functions of the Data-link layer

o **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.



- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.



Network Layer

o It is a layer 3 that manages device addressing, tracks the location of devices on the network.

o It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.

o The Data link layer is responsible for routing and forwarding the packets.

o Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

o The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

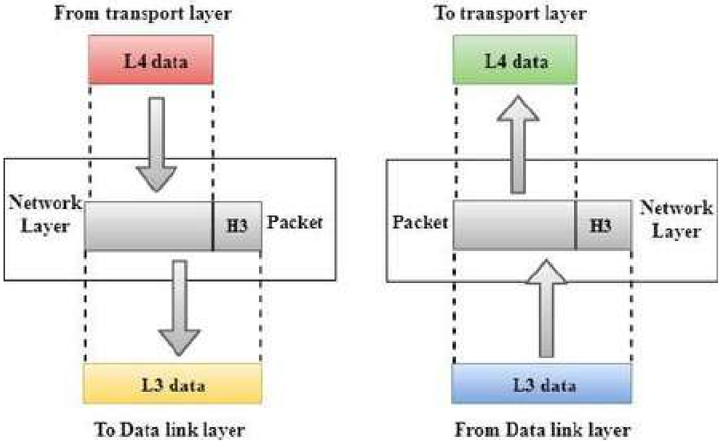
o **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.

o **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

o **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

o **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

o



Transport Layer

o The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.

o The main responsibility of the transport layer is to transfer the data completely.

The two protocols used in this layer are:

o **Transmission Control Protocol**

o It is a standard protocol that allows the systems to communicate over the internet.

o It establishes and maintains a connection between hosts.

o When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

o **User Datagram Protocol**

o User Datagram Protocol is a transport layer protocol.

o It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

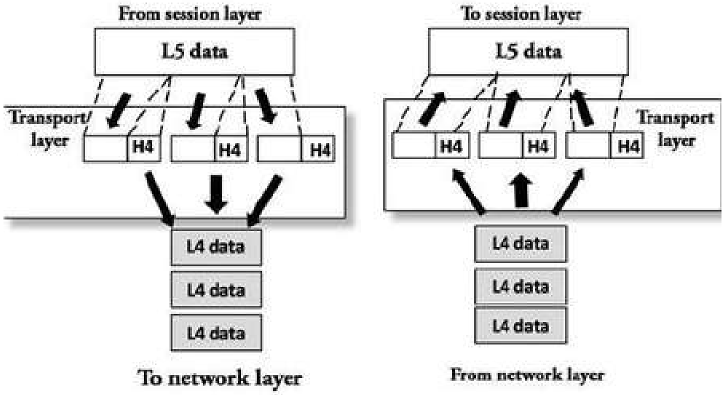
o **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

o **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

o **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

o **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

o **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.



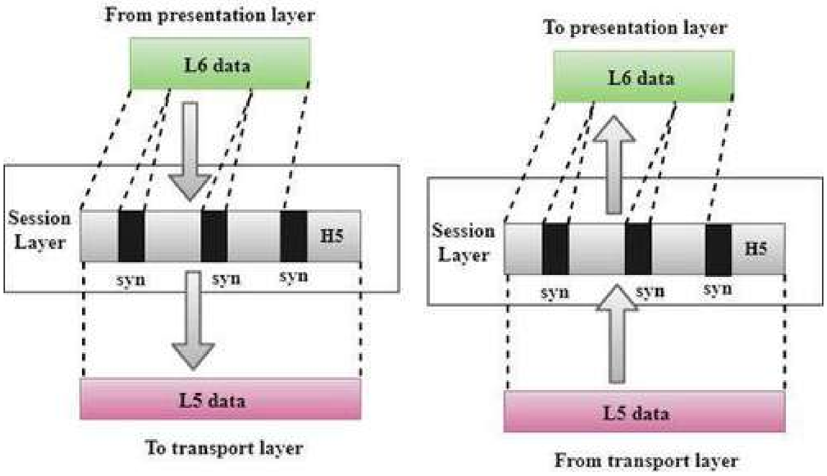
o

Session Layer

Functions of Session layer:

o **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.

o **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.



Presentation Layer

Functions of Presentation layer:

o **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

o **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.

o **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

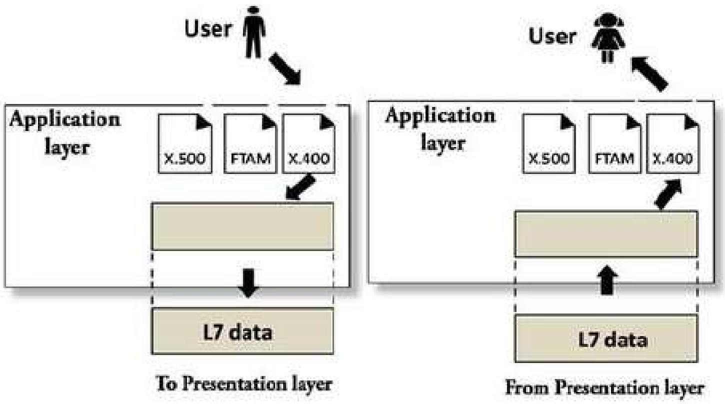
Application Layer

Functions of Application layer:

o **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.

o **Mail services:** An application layer provides the facility for email forwarding and storage.

o Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.



o

1.4.2 TCP/IP-

TCP/IP model

o The TCP/IP model was developed prior to the OSI model.

o The TCP/IP model is not exactly similar to the OSI model.

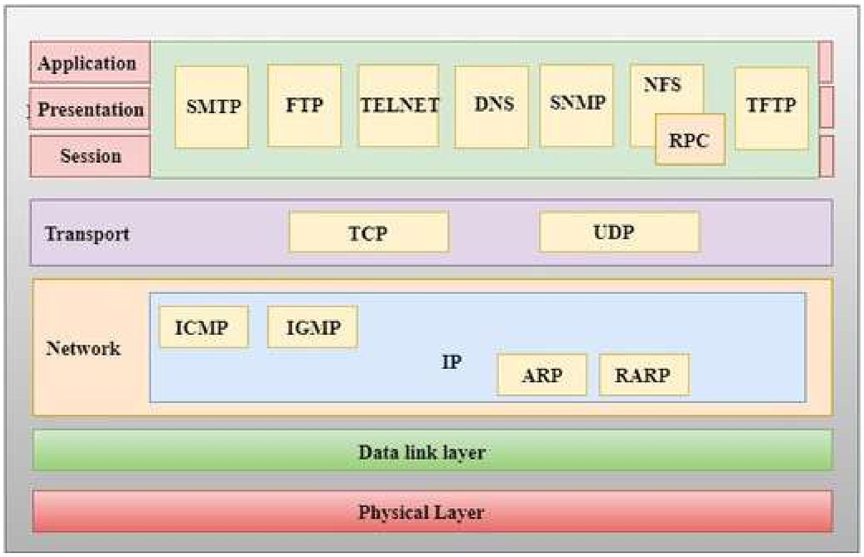
o The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.

o The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.

o TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

o A network layer is the lowest layer of the TCP/IP model.

o A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.

o It defines how the data should be sent physically through the network.

o This layer is mainly responsible for the transmission of the data between two devices on the same network.

o The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.

o The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

o An internet layer is the second layer of the TCP/IP model.

o An internet layer is also known as the network layer.

o The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

o **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.

o **Host-to-host communication:** It determines the path through which the data is to be transmitted.

o **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.

o **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

o **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

o ARP stands for **Address Resolution Protocol**.

o ARP is a network layer protocol which is used to find the physical address from the IP address.

o **The two terms are mainly associated with the ARP Protocol:**

o **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.

o **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

o **ICMP** stands for Internet Control Message Protocol.

o It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.

o A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.

o An ICMP protocol mainly uses two terms:

o **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.

o **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.

o The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.

o ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

o **User Datagram Protocol (UDP)**

o It provides connectionless service and end-to-end delivery of transmission.

o It is an unreliable protocol as it discovers the errors but not specify the error.

o User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

o **UDP consists of the following fields:**

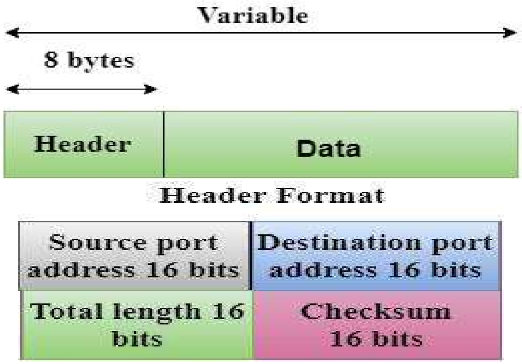
Source port address: The source port address is the address of the application program that has created the message.

Destination port address: The destination port address is the address of the application program that receives the message.

Total length: It defines the total number of bytes of the user datagram in bytes.

Checksum: The checksum is a 16-bit field used in error detection.

o UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



o **Transmission Control Protocol (TCP)**

o It provides a full transport layer services to applications.

o It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.

o TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.

o At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.

o At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

o An application layer is the topmost layer in the TCP/IP model.

o It is responsible for handling high-level protocols, issues of representation.

o This layer allows the user to interact with the application.

o When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.

o There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

DIFFERENCES BETWEEN THE OSI AND TCP/IP MODEL

- OSI has 7 layers whereas TCP/IP has 4 layers.
- The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. On the other hand, TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can be transmitted between them.
- OSI header is 5 bytes whereas TCP/IP header size is 20 bytes.
- OSI refers to Open Systems Interconnection whereas TCP/IP refers to Transmission Control Protocol.
- OSI model, the transport layer, is only connection-oriented whereas the TCP/IP model is both connection-oriented and connectionless.

- OSI model is developed by ISO (International Standard Organization), whereas TCP Model is developed by ARPANET (Advanced Research Project Agency Network).
- OSI model helps you to standardize router, switch, motherboard, and other hardware whereas TCP/IP helps you to establish a connection between different types of computers.

UNIT – 2 DATA TRANSMISSION & MEDIA

CONCEPTS AND TERMINOLOGY

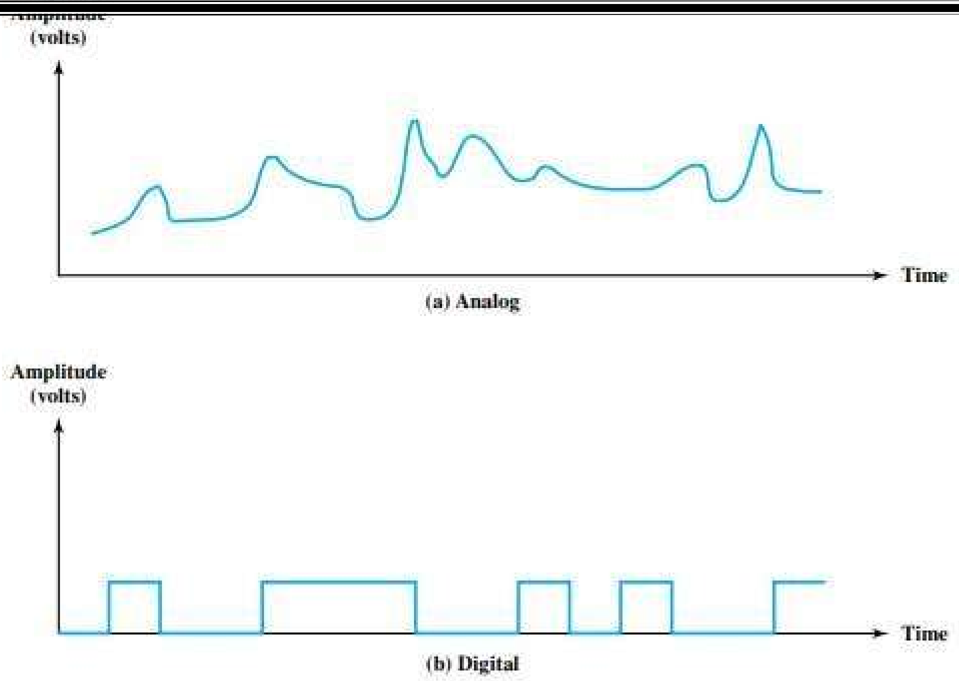
Transmission Terminology-

Guided media- In guided media, the waves are guided along a physical path, examples of guided media are twisted pair, coaxial cable and optical fiber.
Unguided media- Unguided media also called wireless, provide means for transmitting electromagnetic waves but do not guide them.
Point to Point- A guided transmission medium is point to point if it provides a direct link between two devices and those are the only two devices sharing the medium.
Multipoint- A guided transmission medium is multipoint if more than two devices share the same medium.
Simplex- In simplex transmission signals are transmitted in only one direction. One transmitter and the other is receiver.
Half duplex- In half duplex operation both station may transmit or receive, but only one at a time.
Full duplex- In full duplex operation both stations may transmit simultaneously.

Signals can be described- a) in the time domain, b) in the frequency domain

Time domain concepts-

An **analog signal** is one in which the signal intensity varies in a smooth fashion over ~~time. In other words ther~~e are no breaks or discontinuities in the signal.
A **digital signal** is one in which the signal intensity maintains a constant level for some period of time and then abruptly changes to another constant level.



(a) Analog

(b) Digital

Both analog and digital signals can take one of two forms: periodic or non periodic.

Periodic Signals are signals that repeat themselves after a certain amount of time.

Mathematically, a signal S(t) is defined to be periodic if and only if

$S(t+T)= S(t) \quad -\infty < t < +\infty$

Where the constant T is the period of the signal otherwise, a signal is **aperiodic.**

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

The completion of one full pattern is called a cycle.

Frequency domain concepts

Spectrum —range of frequencies contained in signal

Spectrum- The spectrum of a signal is the range of frequencies that it contains.

Absolute Bandwidth- The absolute bandwidth of a signal is the width of the spectrum.

Effective Bandwidth- The band of frequencies which contains most of the energy of

the
signal.

DC component- If a signal includes a component of zero frequency, that component is

a
direct current or constant component.

Relationship between data rate and bandwidth-

 Consider the case binary data is encoded into digital signal, and to be transmitted by a transmission medium.

 Digital signal contains an infinite bandwidth but a real transmission medium has a finite bandwidth, which can limit the data rate that can be carried on the transmission medium.

 Limited bandwidth creates distortions of the input signal, which makes the task of interpreting the received signal more difficult.

 The more limited bandwidth, the greater the distortion and the greater the potential for error by the receiver.

 The high the data rate of a signal, the greater is its effective bandwidth.

 The greater the bandwidth of a transmission system, the higher is the data rate that can be transmitted.

ANALOG AND DIGITAL DATA

Analog data take on continuous values in some interval. For example, voice and video are continuously varying patterns of intensity. Most data collected by sensors, such as temperature and pressure, are continuous valued.

Digital data take on discrete values; examples are text and integers. The most familiar example of analog data is audio, which, in the form of acoustic sound waves, can be perceived directly by human beings

Another common example of analog data is video. Here it is easier to characterize the data in terms of the TV screen (destination) rather than the original scene (source) recorded by the TV camera. To produce a picture on the screen, an electron beam scans across the surface of the screen from left to right and top to bottom. For black-and-white television, the amount of illumination produced (on a scale from black to white) at any point is proportional to the intensity of the beam as it passes that point. Thus at any instant in time the beam takes on an analog value of intensity to produce the desired brightness at that point on the screen.

Analog and Digital Signals

~~In a communications syste~~m, data are propagated from one point to another by means of electromagnetic signals.

An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media, depending on spectrum; examples are wire media, such as twisted pair and coaxial cable; fiber optic cable; and unguided media, such as atmosphere or space propagation.

A digital signal is a sequence of voltage pulses that may be transmitted over a wire medium; for example, a constant positive voltage level may represent binary 0 and a constant negative voltage level may represent binary 1. The principal advantages of digital signaling are that it is generally cheaper than analog signaling and is less susceptible to noise interference. The principal disadvantage is that digital signals suffer more from attenuation than do analog signals.

Data and Signals

Analog signals used to represent analog data and digital signals used to represent digital data. Generally, analog data are a function of time and occupy a limited frequency spectrum, such data can be represented by an electromagnetic signal occupying the same spectrum. Digital data can be represented by digital signals, with a different voltage level for each of the two binary digits.

Digital data can also be represented by analog signals by use of a modem (modulator/demodulator). The modem converts a series of binary (two-valued) voltage pulses into an analog signal by encoding the digital data onto a carrier frequency. The resulting signal occupies a certain spectrum of frequency centered about the carrier and may be propagated across a medium suitable for that carrier. The most common modems represent digital data in the voice spectrum and hence allow those data to be propagated over ordinary voice-grade telephone lines.

At the other end of the line, another modem demodulates the signal to recover the original data. In an operation very similar to that performed by a modem, analog data can be represented by digital signals. The device that performs this function for voice data is a codec (coder-decoder). In essence, the codec takes an analog signal that directly represents the voice data and approximates that signal by a bit stream. At the receiving end, the bit stream is used to reconstruct the analog data.

2.2 ANALOG AND DIGITAL TRANSMISSION

Both analog and digital signals may be transmitted on suitable transmission media.

Analog transmission is a means of transmitting analog signals without regard to their content; the signals may represent analog data (e.g., voice) or digital data (e.g., binary data that pass through a modem). In either case, the analog signal will become weaker (attenuate) after a certain distance. To achieve longer distances, the analog transmission system includes amplifiers that boost the energy in the signal. Unfortunately, the amplifier also boosts the noise components. With amplifiers cascaded to achieve long distances, the signal becomes more and more distorted. For analog data, such as voice, quite a bit of distortion can be tolerated and the data remain intelligible. However, for digital data, cascaded amplifiers will introduce errors.

Digital transmission, in contrast, assumes a binary content to the signal. A digital signal can be transmitted only a limited distance before attenuation, noise, and other impairments endanger the integrity of the data. To achieve greater distances, repeaters are used. A repeater receives the digital signal, recovers the pattern of 1s and 0s, and retransmits a new signal. Thus the attenuation is overcome.

TRANSMISSION IMPAIRMENT

In the data communication system, analog and digital signals go through the transmission medium. Transmission media are not ideal. There are some imperfections in transmission mediums. So, the signals sent through the transmission medium are also not perfect. This imperfection cause **signal impairment**.

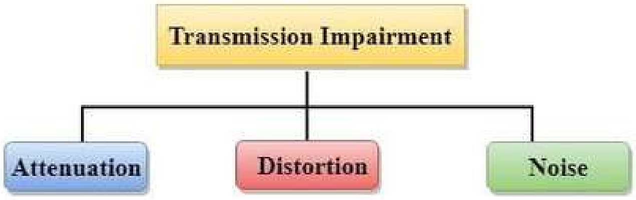
It means that signals that are transmitted at the beginning of the medium are not the same as the signals that are received at the end of the medium that is what is sent is not what is received. These impairments tend to deteriorate the quality of analog and digital signals.

Consequences

1. For a digital signal, there may occur bit errors.
2. For analog signals, these impairments degrade the quality of the signals.

Causes of impairment

There are three main causes of impairment are,



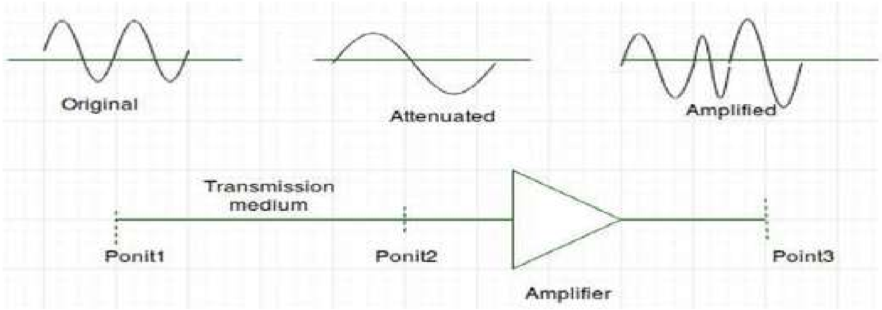
1. Attenuation
2. Distortion
3. Noise

1) Attenuation

Here attenuation Means loss of energy that is the weaker signal. Whenever a signal transmitted through a medium it loses its energy, so that it can overcome by the resistance of the medium.

 That is why a wire carrying electrical signals gets warm, if not hot, after a while. Some of the electrical energy is converted to heat in the signal.
 Amplifiers are used to amplify the signals to compensate for this loss.

This figure shows the **effect of attenuation and amplification**:



 A signal has lost or gained its strength, for this purpose engineers use the concept of decibel (dB).
 Decibel is used to measure the relative strengths of two signals or a signal at two different points.

 If a signal is attenuated then dB is negative and if a signal is amplified so the db is positive.

Attenuation (dB) = 10log10 (P2/P1)
where P2 and P1 are the power of a signal at points1 and 2.

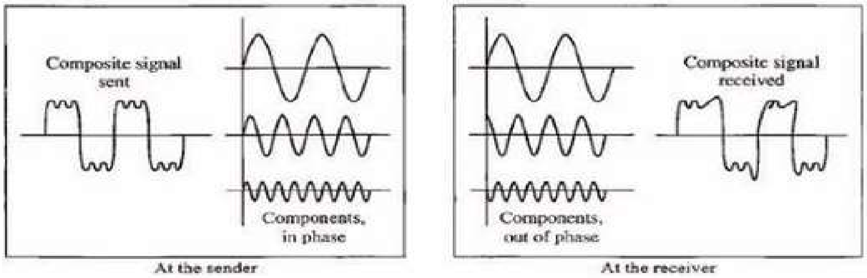
2) Distortion

If a signal changes its form or shape, it is referred to as distortion. Signals made up of different frequencies are composite signals. Distortion occurs in these composite signals.

 Each component of frequency has its propagation speed traveling through a medium and therefore, different components have different delay in arriving at the final destination.

 It means that signals have different phases at the receiver than they did at the source.

 This figure shows the effect of distortion on a composite signal:



Distortion

3) Noise

Noise is another problem. There are some random or unwanted signals mix up with the original signal is called noise. Noises can corrupt the signals in many ways along with the distortion introduced by the transmission media.

Different types of noises are:

a. Thermal noise
b. Intermodulation noise
c. Crosstalk
d. Impulse noise

a) Thermal noise

The thermal noise is random motion of electrons in a conductor that creates an extra signal not originally sent by the transmitter.

It is also known as white noise because it is distributed across the entire spectrum (as the frequency encompass over a broad range of frequencies).

b) Intermodulation noise

More than one signal share a single transmission channel, intermodulation noise is generated.

For instance, two signals S1 and S2 will generate signals of frequencies (S1 + S2) and

(s1 - S2), which may interfere with the signals of the same frequencies sent by the sender. due to If nonlinearity present in any part of the communication system, intermodulation noise is introduced.

c) Cross talk

crosstalk is any phenomenon by which a signal transmitted on one circuit or channel of a transmission system creates an undesired effect in another circuit or channel.. One wire acts as a sending antenna and the transmission medium acts as the receiving antenna.

Just like in telephone system, it is a common experience to hear conversation of other people in the background. This is known as cross talk.

d) Impulse noise

Impulse noise is irregular pulses or spikes(a signal with high energy in a very short period) generated by phenomena like that comes from power lines, lightning, spark due to loose contact in electric circuits and so on.

It is a primary source of bit-errors in digital data communication that kind of noise introduces burst errors.

2.4 CHANNEL CAPACITY-

The maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions, is referred to as the channel capacity. There are four concepts here that we are trying to relate to one another.

• **Data rate:** The rate, in bits per second (bps), at which data can be communicated.

• **Bandwidth:** The bandwidth of the transmitted signal as constrained by the transmitter and the nature of the transmission medium, expressed in cycles per second, or Hertz

• **Noise:** The average level of noise over the communications path

• **Error rate:** The rate at which errors occur, where an error is the reception of a 1 when a 0 was transmitted or the reception of a 0 when a 1 was transmitted.

The problem we are addressing is this: Communications facilities are expensive and, in general, the greater the bandwidth of a facility, the greater the cost. Furthermore, all transmission channels of any practical interest are of limited bandwidth. The limitations arise from the physical properties of the transmission medium or from deliberate limitations at the transmitter on the bandwidth to prevent interference from other sources. Accordingly, we would like to make as efficient use as possible of a given bandwidth. For digital data, this means that we would like to get as high a data rate as possible at a particular limit of error rate for a given bandwidth. The main constraint on achieving this efficiency is noise.

Nyquist Bandwidth-

Data rate governs the speed of data transmission. A very important consideration in data communication is how fast we can send data, in bits per second, over a channel. Data rate depends upon 3 factors:

□
The bandwidth available
□
Number of levels in digital signal
□
The quality of the channel – level of noise

Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

Nyquist states that if the rate of signal transmission is 2B, then a signal with frequencies no greater than B is sufficient to carry

$$C = 2B \log_2 M$$

Where M is the number of discrete signal or voltage levels.

EXAMPLE 1

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

BitRate =2 x 3000 x log2 2 =6000 bps

EXAMPLE 2

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as

BitRate =2 x 3000 X log2 4 = 12,000 bp

EXAMPLE 3

We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

265000 = 2 * 20000 * log2(L)
log2(L) = 265000/40000=6.625
L = 26.625 = 98.7 levels

Shannon Capacity Formula-

Nyquist formula indicates that doubling the bandwidth doubles the data rate. The presence of noise can corrupt one or more bits.

In reality, we cannot have a noiseless channel; the channel is always noisy. Shannon capacity is used, to determine the theoretical highest data rate for a noisy channel: The signal-to noise ratio is important in the transmission of digital data. Shannon’s result is that the maximum channel capacity in bits per second.

C= B *log*2 (1+SNR)

Where C is the capacity of the channel in bits per second and B is the bandwidth of the channel in Hertz.

SNRdb= 10*log*10 (signal power/noise power)

Examples:

Input1 : A telephone line normally has a bandwidth of 3000 Hz (300 to 3300 Hz) assigned for data communication. The SNR is usually 3162. What will be the capacity for this channel?
Output1 : C = 3000 * log2(1 + SNR) = 3000 * 11.62 = 34860 bps

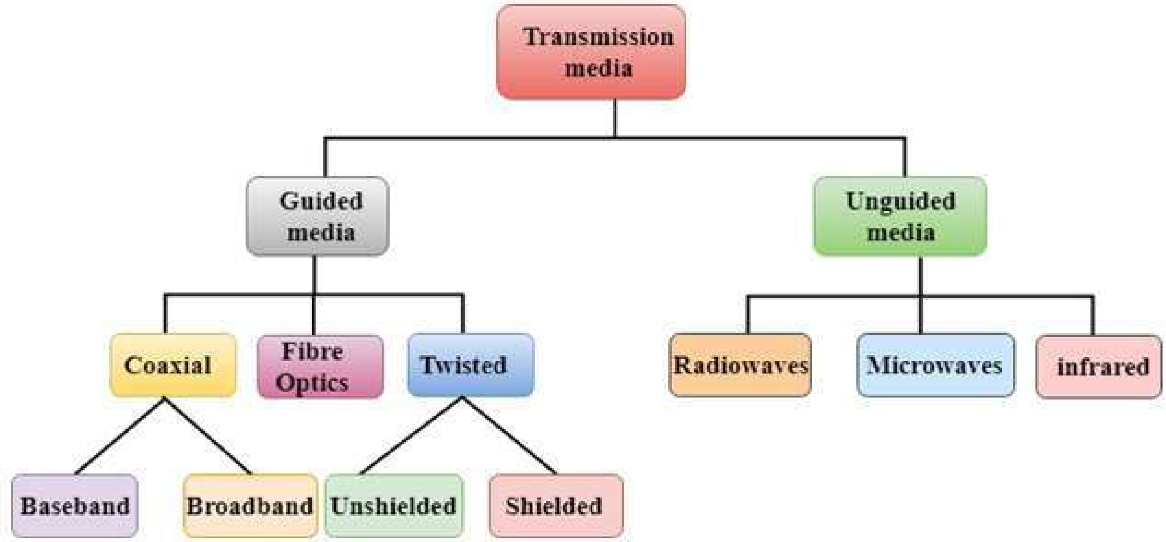
Example

, if the bandwidth of a noisy channel is 4 KHz, and the signal to noise ratio is 100, then the maximum bit rate can be computed as:

Capacity = 4000 × log2(1+100) = 26,633 bps = 26.63 kbps

2.4 Classification Of Transmission Media:

A transmission medium is one which carries a signal from one device to another.



Guided Media

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types Of Guided media:

1. Twisted pair:

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.

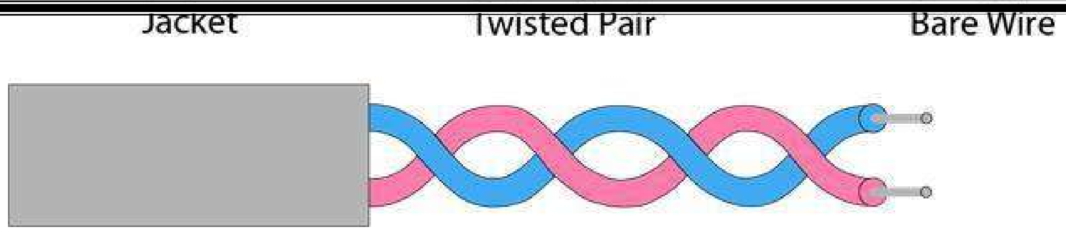
- Twisted pair is a physical media made up of a pair of cables
- twisted with
- each other.
- A twisted pair cable is cheap as compared to other transmission
-

media.

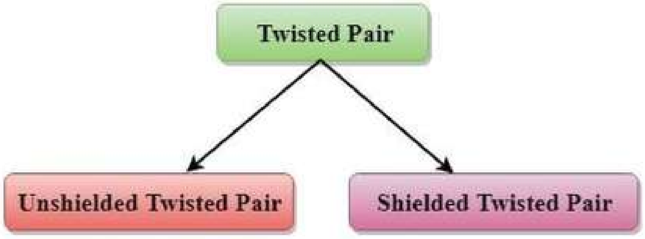
Installation of the twisted pair cable is easy, and it is a lightweight cable.

The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.



Types of Twisted pair:



Unshielded Twisted Pair:

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use

RJ-11

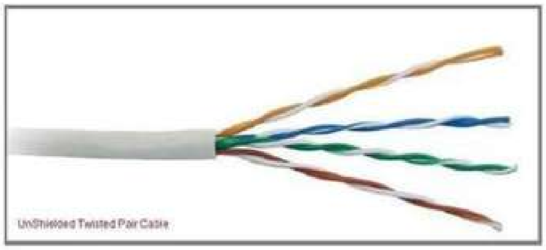
connector and 4 pair cable useRJ-45 connector.

An unshielded twisted pair is widely used in telecommunication. Following

are the

categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.



Advantages Of Unshielded Twisted Pair:

o It is cheap.

o Installation of the unshielded twisted pair is easy.

o It can be used for high-speed LAN.

Disadvantage:

o This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

o The cost of the shielded twisted pair cable is not very high and not very low.

o An installation of STP is easy.

o It has higher capacity as compared to unshielded twisted pair cable.

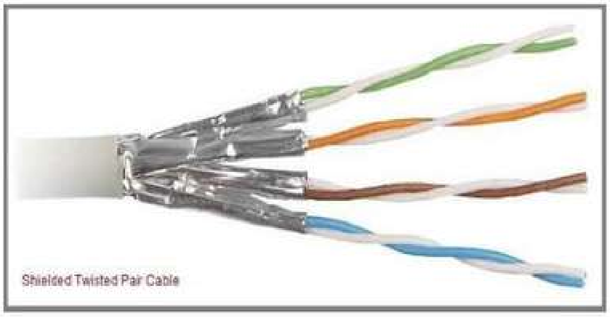
o It has a higher attenuation.

o It is shielded that provides the higher data transmission rate.

Disadvantages

o It is more expensive as compared to UTP and coaxial cable.

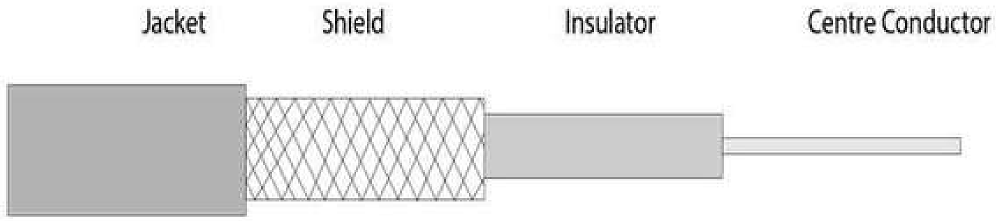
o It has a higher attenuation rate.

o 

2. Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh.
- The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

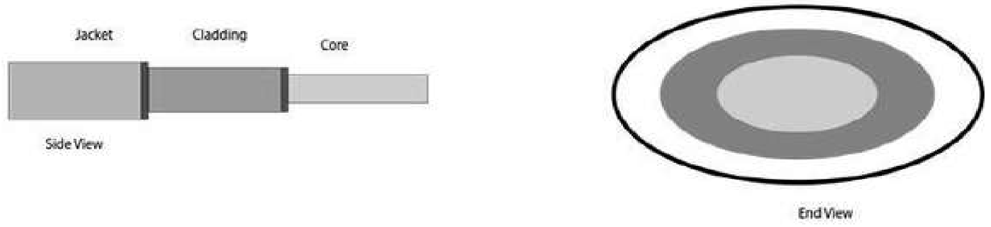
- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

3. Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.

o Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:



Basic elements of Fibre optic cable:

o **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.

o **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

o **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Advantages of fibre optic cable over copper:

o **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.

o **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.

o **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.

o **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.

o **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

Unguided transmission is broadly classified into three categories:

UNGUIDED TRANSMISSION

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.

o In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

1. Radio waves

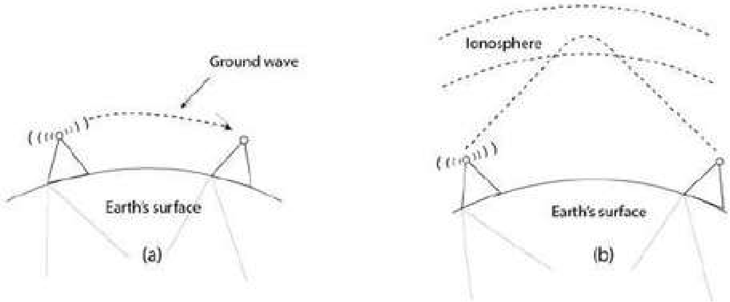
o Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.

o Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.

o The range in frequencies of radio waves is from 3 KHz to 1 kHz.

o In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.

o An example of the radio wave is **FM radio**.



Applications:

o A Radio wave is useful for multicasting when there is one sender and many receivers.
o An FM radio, television, cordless phones are examples of a radio wave.

Advantages:

o Radio transmission is mainly used for wide area networks and mobile cellular phones.
o Radio waves cover a large area, and they can penetrate the walls.
o Radio transmission provides a higher transmission rate.

2. **Microwaves-**

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

 Microwave propagation is line of sight. Since the towers with the mounted antenna need to be in direct sight of each other. Repeaters are often needed for long distance communication.

 Very high frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage of receivers that are inside buildings.

 Two types of antennas are used for microwave communications i.e, the Parabolic dish and the horn.

 Applications-

Microwaves due to their unidirectional properties are very useful when unicast communication is needed between the sender and receiver.

3. **Infrared**

o An infrared transmission is a wireless technology used for communication over short ranges.

o The frequency of the infrared in the range from 300 GHz to 400 THz.

o It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics of Infrared:

o It supports high bandwidth, and hence the data rate will be very high.

o Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.

o An infrared communication provides better security with minimum interference.

o Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

UNIT- 3: DATA ENCODING

3.1 DATA ENCODING-

Encoding is the process of converting the data or a given sequence of characters, symbols, alphabets etc. into a specified format, for the secured transmission of data.

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

- Digital data to digital signal
- Analog data to digital signal
- Digital data to analog signal
- Analog data to analog signal

Digital data to digital signal-

The simplest form of digital encoding of digital data is to assign one voltage level to binary one and another to binary zero. It is less complex and less expensive than digital to analog modulation equipment.

Analog data to digital signal-

Analog data such as voice and video, are often digitized to be able to use digital transmission facilities. The simplest technique is PCM, which involves sampling the analog data and quantizing the samples.

Digital data to analog signal-

A modem converts digital data to an analog signal so that it can be transmitted over an analog line. Some transmission media such as optical fiber and unguided media will only propagate analog signals.

Analog data to analog signal-

Analog data are modulated by a carrier frequency to produce an analog signal in a different frequency band, which can be utilized on an analog transmission system.

3.2 DIGITAL DATA TO DIGITAL SIGNAL-

To convert digital data into digital signals it can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

3.2.1 LINE CODING-

We can roughly divide line coding schemes into five categories:

1. Unipolar (eg. NRZ scheme).

2. Polar (eg. NRZ-L, NRZ-I, RZ, and Biphase – Manchester and differential Manchester).
3. Bipolar (eg. AMI and Pseudo ternary).
4. Multilevel
5. Multitransition

But, before learning difference between first three schemes we should first know the **characteristic** of these line coding techniques:

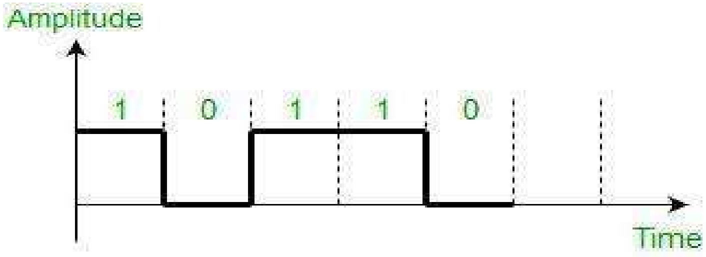
- There should be **self-synchronizing** i.e., both receiver and sender clock should be synchronized.
- There should have some error-detecting capability.
- There should be immunity to noise and interference.
- There should be less complexity.
- There should be no low frequency component (**DC-component**) as long distance transfer is not feasible for low frequency component signal.
- There should be less base line wandering.

Unipolar scheme –

In this scheme, all the signal levels are either above or below the axis.

- **Non return to zero (NRZ) –**

It is unipolar line coding scheme in which positive voltage defines bit 1 and the zero voltage defines bit 0. Signal does not return to zero at the middle of the bit thus it is called NRZ. For example: Data = 10110.



But this scheme uses more power as compared to polar scheme to send one bit per unit line resistance. Moreover for continuous set of zeros or ones there will be self-synchronization and base line wandering problem.

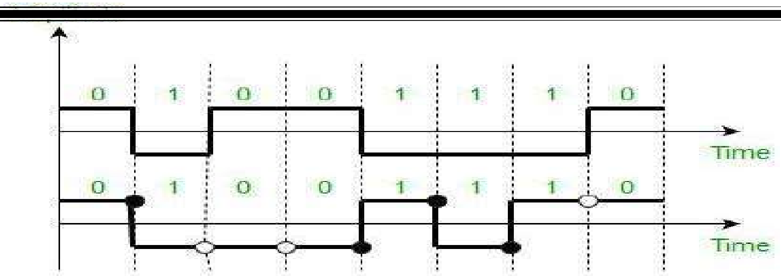
Polar schemes –

In polar schemes, the voltages are on the both sides of the axis.

- **NRZ-L and NRZ-I –**

These are somewhat similar to unipolar NRZ scheme but here we use two levels of amplitude (voltages). For **NRZ-L(NRZ-Level)**, the level of the voltage determines the value of the bit, typically binary 1 maps to logic-level high, and binary 0 maps to logic-level low, and for **NRZ-I(NRZ-Invert)**, two-level signal has a transition at a boundary if the next bit that we are going to transmit is a logical 1, and does not have a transition if the next bit that we are going to transmit is a logical 0.

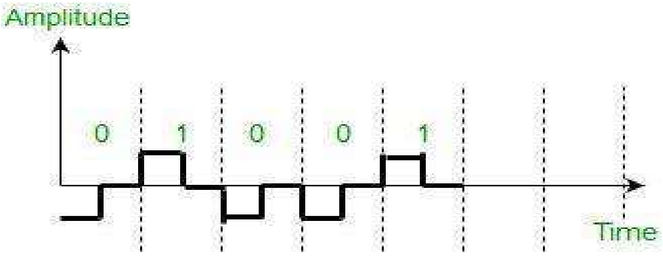
Note – For NRZ-I we are assuming in the example that previous signal before starting of data set “01001110” was positive. Therefore, there is no transition at the beginning and first bit “0” in current data set “01001110” is starting from +V. Example: Data = 01001110.



Comparison between NRZ-L and NRZ-I: Baseline wandering is a problem for both of them, but for NRZ-L it is twice as bad as compared to NRZ-I. This is because of transition at the boundary for NRZ-I (if the next bit that we are going to transmit is a logical 1). Similarly self-synchronization problem is similar in both for long sequence of 0's, but for long sequence of 1's it is more severe in NRZ-L.

- **Return to zero (RZ) –**

One solution to NRZ problem is the RZ scheme, which uses three values positive, negative and zero. In this scheme signal goes to 0 in the middle of each bit.
Note – The logic we are using here to represent data is that for bit 1 half of the signal is represented by +V and half by zero voltage and for bit 0 half of the signal is represented by -V and half by zero voltage. Example: Data = 01001.



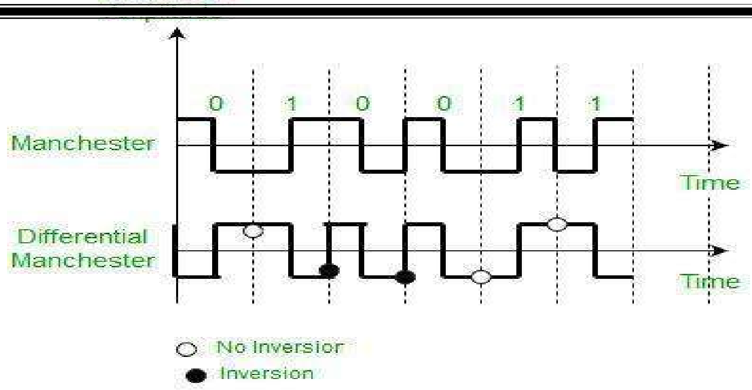
Main disadvantage of RZ encoding is that it requires greater bandwidth. Another problem is the complexity as it uses three levels of voltage. As a result of all these deficiencies, this scheme is not used today. Instead, it has been replaced by the better-performing Manchester and differential Manchester schemes.

- **Biphase (Manchester and Differential Manchester) –**

Manchester encoding is somewhat combination of the RZ (transition at the middle of the bit) and NRZ-L schemes. The duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization.

Differential Manchester is somewhat combination of the RZ and NRZ-I schemes. There is always a transition at the middle of the bit but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition, if the next bit is 1, there is no transition.

Note –
1. The logic we are using here to represent data using Manchester is that for bit 1 there is transition form -V to +V volts in the middle of the bit and for bit 0 there is transition from +V to -V volts in the middle of the bit.
2. For differential Manchester we are assuming in the example that previous signal before starting of data set "010011" was positive. Therefore there is transition at the beginning and first bit "0" in current data set "010011" is starting from -V. Example: Data = 010011.



The Manchester scheme overcomes several problems associated with NRZ-L, and differential Manchester overcomes several problems associated with NRZ-I as there is no baseline wandering and no DC component because each bit has a positive and negative voltage contribution.

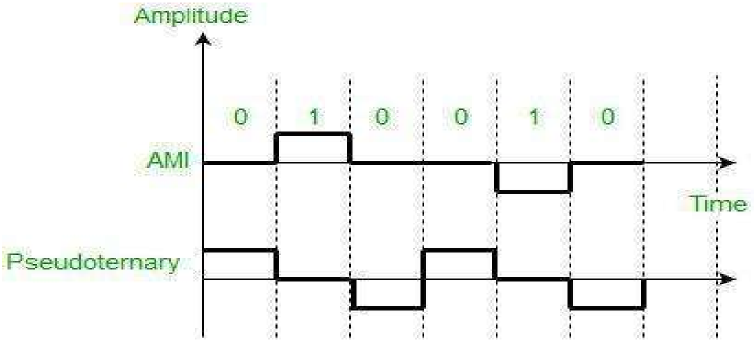
Only limitation is that the minimum bandwidth of Manchester and differential Manchester is twice that of NRZ.

Bipolar schemes –

In this scheme there are three voltage levels positive, negative, and zero. The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative.

 Alternate Mark Inversion (AMI) – A neutral zero voltage represents binary 0. Binary 1’s are represented by alternating positive and negative voltages.

 Pseudo ternary – Bit 1 is encoded as a zero voltage and the bit 0 is encoded as alternating positive and negative voltages i.e., opposite of AMI scheme. Example: Data = 010010.

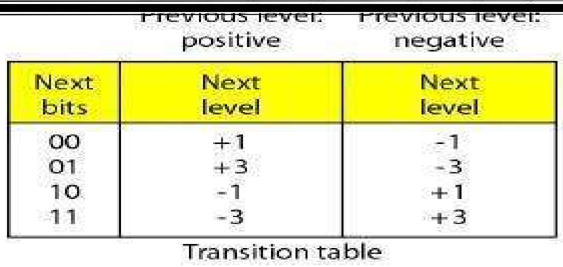


The bipolar scheme is an alternative to NRZ. This scheme has the same signal rate as NRZ, but there is no DC component as one bit is represented by voltage zero and other alternates every time.

Multilevel Scheme-

2BIQ-

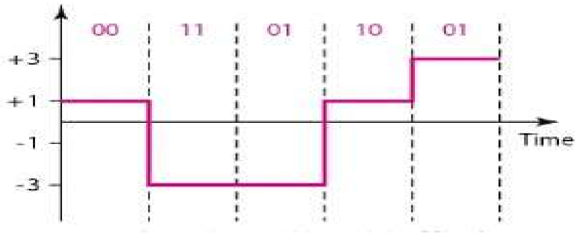
In two binary one quaternary, uses data patterns of size two and encodes the two bit patterns as one signal element belonging to a four level signal.



	Previous level: positive	Previous level: negative
Next bits	Next level	Next level
00	+1	-1
01	+3	-3
10	-1	+1
11	-3	+3

Transition table

Ex.- Data- 0011011001



8B6T- (Eight binary, six ternary)

- This code is used with 100BASE-4T cable. The idea is to encode a pattern of 8 bits as a pattern of 8 bits as a pattern of six signal elements.
- Each signal pattern has a weight of 0 or +1.
- The three possible signal levels are represented as -, 0 and +.

4D-PAM5- (Four dimensional five level pulse amplitude modulation)

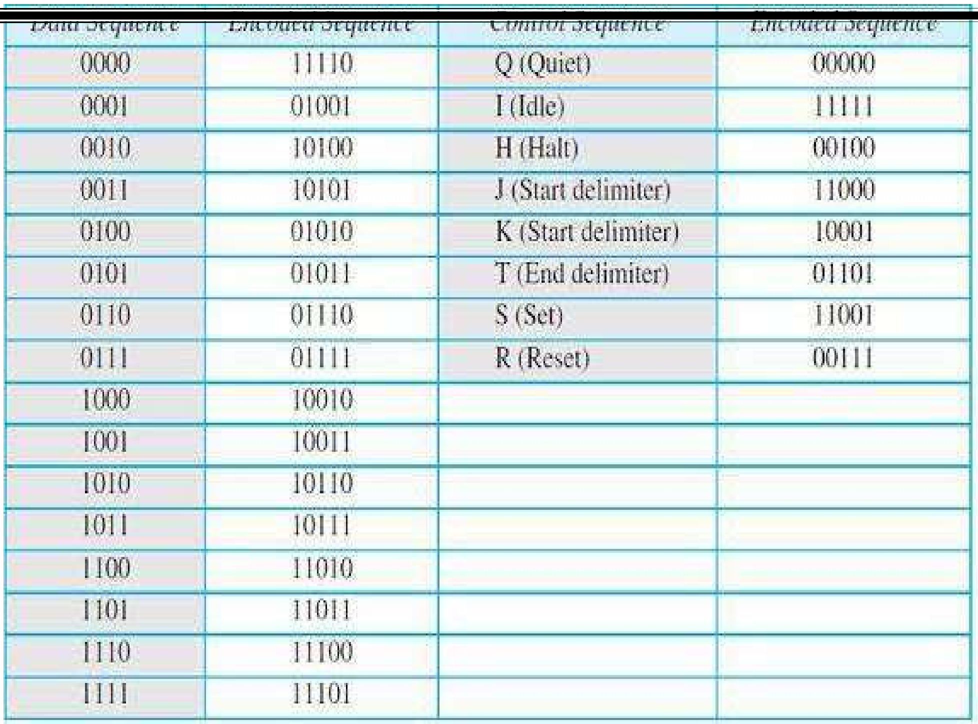
- The 4D means that data is sent over four wires at the same time.
- It uses five voltage levels, such as -2, -1, 0,1 and 2.
- However, one level, level 0 is used only for forward error detection.
- The technique is designed to send data over four channels.
- Gigabit LANs use this technique to send 1-Gbps data over four copper cables that can handle 125 Mband.

3.2.2 BLOCK CODING-

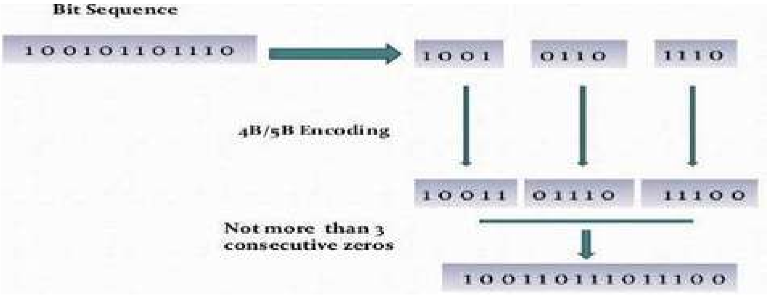
Block coding is normally referred to as mB/nB coding, it replaces each m bit group with an n bit group.

4B/5B (Four binary/ Five binary)-

- In 4B/5B, the 5 bit output that replaces the 4 bit input has no more than one leading zero and no more than two trailing zeros.0
- So, when different groups are combined to make a new sequence, there are never more than three consecutive 0s.

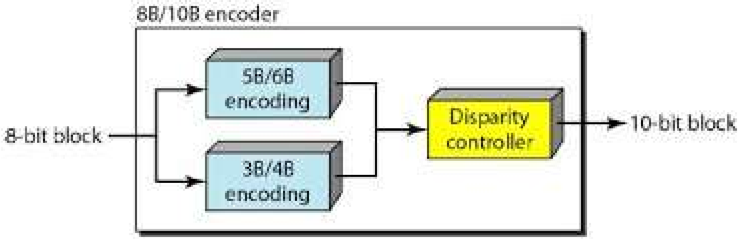


Data Sequence	Encoded Sequence	Control Sequence	Encoded Sequence
0000	11110	Q (Quiet)	00000
0001	01001	I (Idle)	11111
0010	10100	H (Halt)	00100
0011	10101	J (Start delimiter)	11000
0100	01010	K (Start delimiter)	10001
0101	01011	T (End delimiter)	01101
0110	01110	S (Set)	11001
0111	01111	R (Reset)	00111
1000	10010		
1001	10011		
1010	10110		
1011	10111		
1100	11010		
1101	11011		
1110	11100		
1111	11101		



8B/10B (Eight binary/ ten binary)-

- This is similar to 4B/5B encoding except that a group of 8 bits of data is substituted by a 10 bit code.
- It provides greater error detection capability than 4B/ 5B. the 8B/ 10B block coding is actually a combination of 5B/ 6B and 3B/ 4B encoding.



iii. SCRAMBLING-

Scrambling is a technique that does not increase the number of bits and does provide synchronization. Problem with technique like Bipolar AMI (Alternate Mark Inversion) is that continuous sequence of zero’s create synchronization problems one solution to this is Scrambling.

There are two common scrambling techniques:

1. B8ZS(Bipolar with 8-zero substitution)
2. HDB3(High-density bipolar3-zero)

B8ZS (Bipolar with 8-zero substitution) –

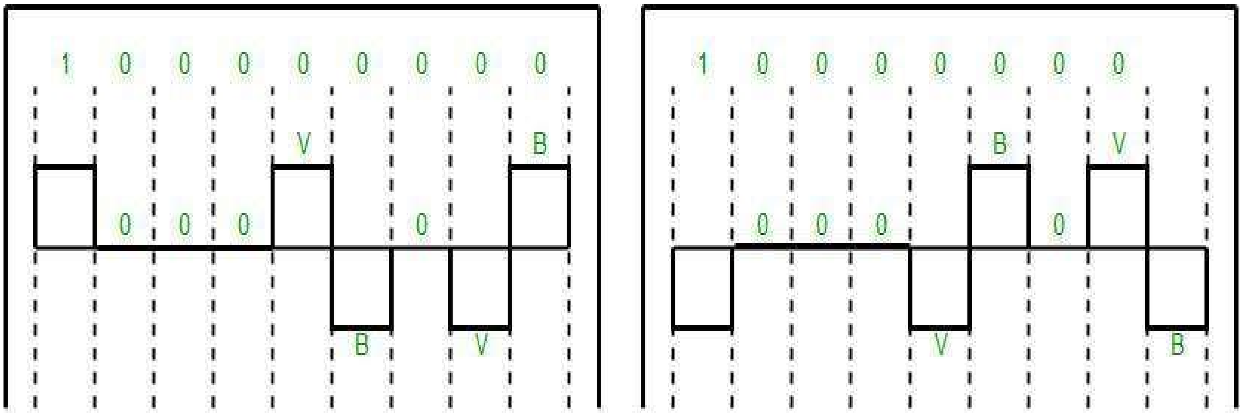
This technique is similar to Bipolar AMI except when eight consecutive zero-level voltages are encountered they are replaced by the sequence,”000VB0VB”.

Note –

 V (Violation), is a non-zero voltage which means signal have same polarity as the previous non-zero voltage. Thus it is violation of general AMI technique.

 B (Bipolar), also non-zero voltage level which is in accordance with the AMI rule (i.e., opposite polarity from the previous non-zero voltage).

Example: Data = 100000000



Note – Both figures (left and right one) are correct, depending upon last non-zero voltage signal of previous data sequence (i.e., sequence before current data sequence “100000000”).

HDB3(High-density bipolar3-zero) –

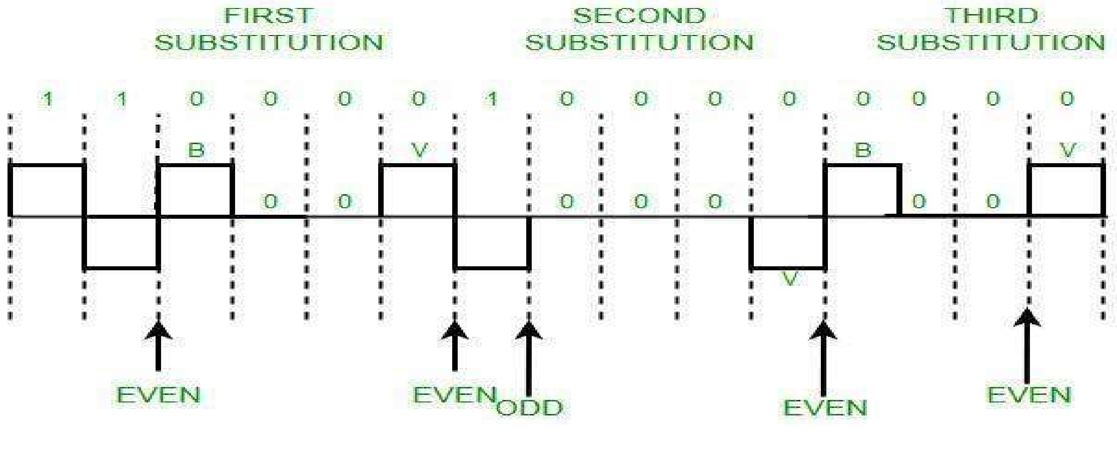
In this technique four consecutive zero-level voltages are replaced with a sequence “000V” or “B00V”.

Rules for using these sequences:

 If the number of nonzero pulses after the last substitution is odd, the substitution pattern will be “000V”, this helps maintaining total number of nonzero pulses even.

 If the number of nonzero pulses after the last substitution is even, the substitution pattern will be “B00V”. Hence even number of nonzero pulses is maintained again.

Example: Data = 1100001000000000



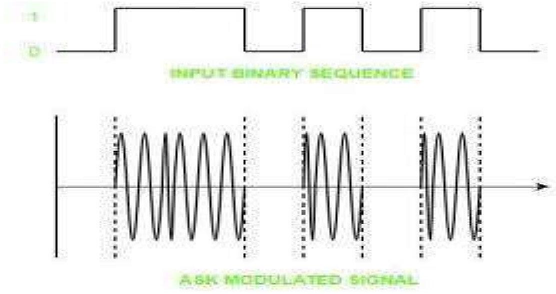
Explanation – After representing first two 1's of data we encounter four consecutive zeros. Since our last substitutions were two 1's (thus number of non-zero pulses is even).So, we substitute four zeros with "B00V".

3.3 DIGITAL DATA TO ANALOG 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 –

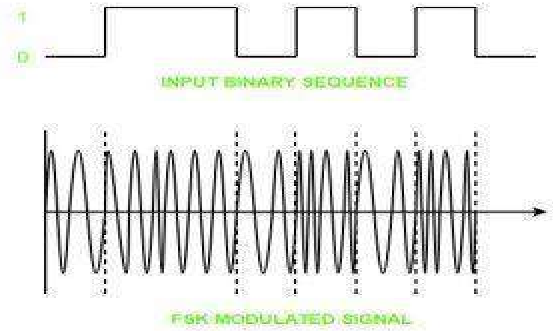
- It can be used to transmit digital data over optical fiber.
- The receiver and transmitter have a simple design which also makes it comparatively inexpensive.
- It uses lesser bandwidth as compared to FSK thus it offers high bandwidth efficiency.

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.



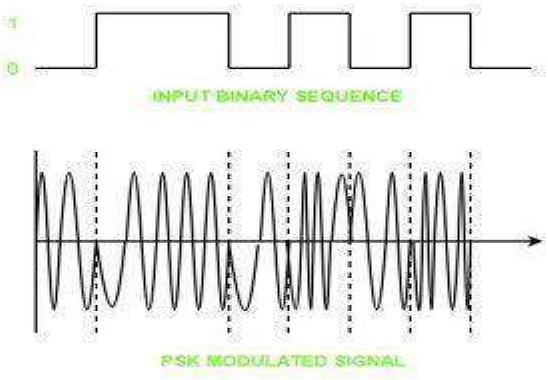
Advantages of frequency shift Keying –

 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.



It is further categorized as follows:

1. **Binary Phase Shift Keying (BPSK):**

BPSK also known as phase reversal keying or 2PSK is the simplest form of phase shift keying. The Phase of the carrier wave is changed according to the two binary inputs. In Binary Phase shift keying, difference of 180 phase shift is used between binary 1 and binary 0.

This is regarded as the most robust digital modulation technique and is used for long distance wireless communication.

2. **Quadrature phase shift keying:**

This technique is used to increase the bit rate i.e we can code two bits onto one single element. It uses four phases to encode two bits per symbol. QPSK uses phase shifts of multiples of 90 degrees.

It has double data rate carrying capacity compare to BPSK as two bits are mapped on each constellation points.

Advantages of phase shift Keying –

 It is a more power efficient modulation technique as compared to ASK and FSK.
 It has lower chances of an error.
 It allows data to be carried along a communication signal much more efficiently as compared to FSK.

Disadvantages of phase shift Keying –

- It offers low bandwidth efficiency.
- The detection and recovery algorithms of binary data is very complex.
- It is a non-coherent reference signal.

3.4 ANALOG DATA TO DIGITAL SIGNAL-

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 Analog to Digital Conversion:

a. PULSE CODE MODULATION:

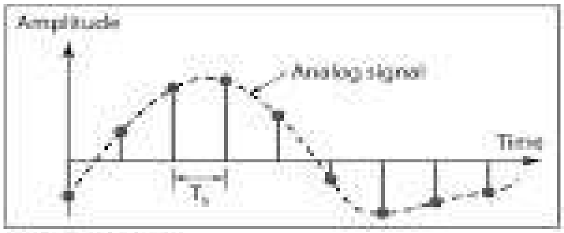
The most common technique to change an analog signal to digital data is called pulse code modulation (PCM). A PCM encoder has the following three processes:

1. Sampling
2. Quantization
3. Encoding

Low pass filter:
The low pass filter eliminates the high frequency components present in the input analog signal to ensure that the input signal to sampler is free from the unwanted frequency components. This is done to avoid aliasing of the message signal.

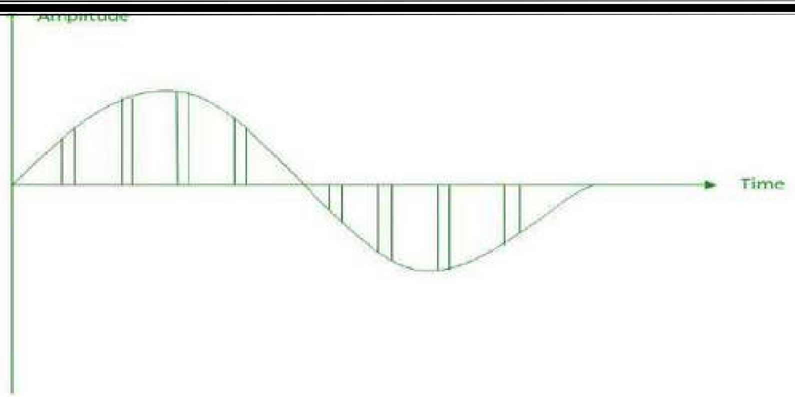
1. **Sampling –** The first step in PCM is sampling. Sampling is a process of measuring the amplitude of a continuous-time signal at discrete instants, converting the continuous signal into a discrete signal. There are three sampling methods:

(i) Ideal Sampling: In ideal sampling also known as Instantaneous sampling pulses from the analog signal are sampled. This is an ideal sampling method and cannot be easily implemented.

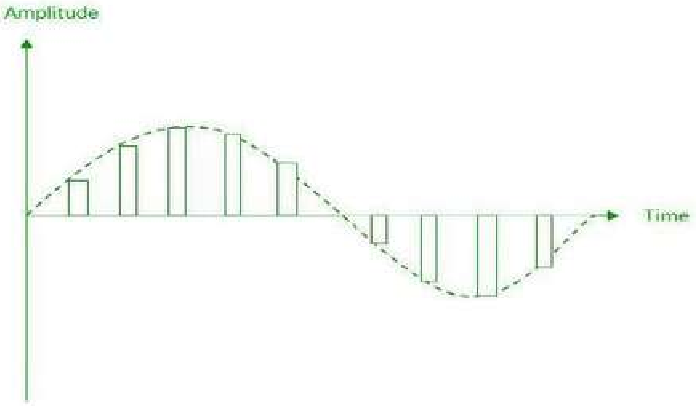


a. Ideal sampling

(ii) Natural Sampling: Natural Sampling is a practical method of sampling in which pulse have finite width equal to T.The result is a sequence of samples that retain the shape of the analog signal.



(iii) Flat top sampling: In comparison to natural sampling flat top sampling can be easily obtained. In this sampling technique, the top of the samples remains constant by using a circuit. This is the most common sampling method used.



Nyquist Theorem:

One important consideration is the sampling rate or frequency. According to the Nyquist theorem, the sampling rate must be at least 2 times the highest frequency contained in the signal. It is also known as the minimum sampling rate and given by:
Fs =2*fm

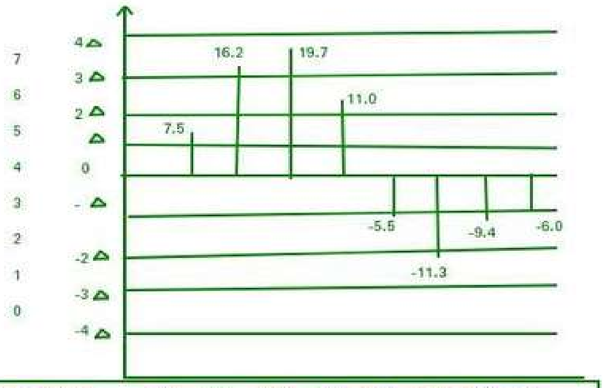
2. **Quantization –**

The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal. The set of amplitudes can be infinite with non-integral values between two limits.

The following are the steps in Quantization:

1. We assume that the signal has amplitudes between Vmax and Vmin

2. We divide it into L zones each of height d where,
d= (Vmax- Vmin)/ L



Normalised PAM value :	1.50	3.24	3.94	2.20	-1.10	2.26	-1.88	-1.20
Quantized Value :	1.50	3.50	3.50	2.50	-1.50	-2.50	-1.50	-1.50
Normalized Error :	0	0.26	-0.44	0.30	-0.40	-0.24	0.38	-0.30
Quantization Code :	5	7	7	6	2	1	2	2
Encoded Words :	101	111	111	110	010	001	010	010

3. The value at the top of each sample in the graph shows the actual amplitude.

4. The normalized pulse amplitude modulation (PAM) value is calculated using the formula amplitude/d.

5. After this we calculate the quantized value which the process selects from the middle of each zone.

6. The Quantized error is given by the difference between quantized value and normalized PAM value.

7. The Quantization code for each sample based on quantization levels at the left of the graph.

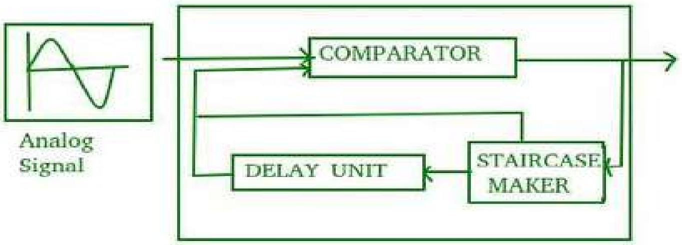
3. **Encoding–**

The digitization of the analog signal is done by the encoder. After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n bit code. Encoding also minimizes the bandwidth used.

b. DELTA MODULATION:

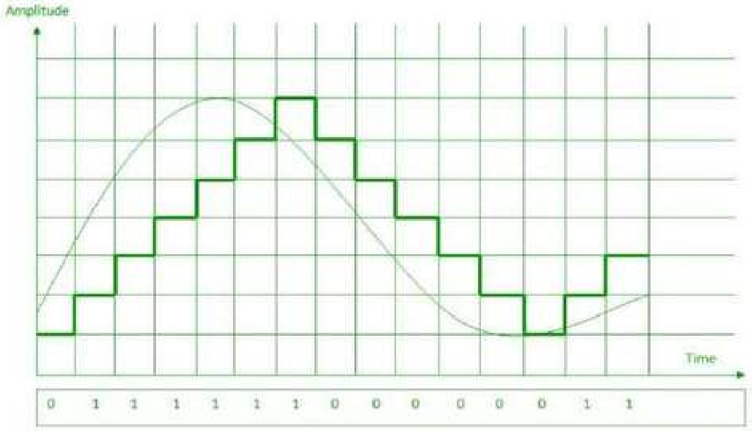
Since PCM is a very complex technique, other techniques have been developed to reduce the complexity of PCM. The simplest is delta Modulation. Delta Modulation finds the change from the previous value.

Modulator – The modulator is used at the sender site to create a stream of bits from an analog signal. The process records a small positive change called delta. If the delta is positive, the process records a 1 else the process records a 0. The modulator builds a second signal that resembles a staircase. The input signal is then compared with this gradually made staircase signal.



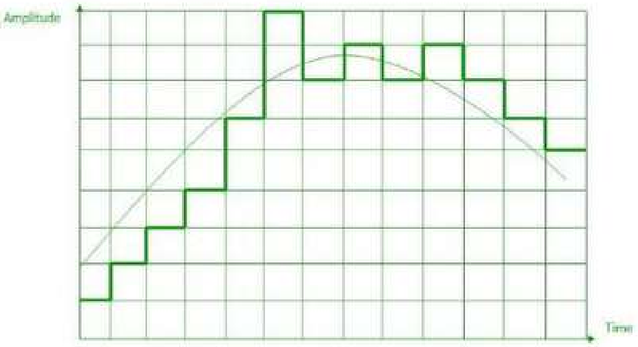
We have the following rules for output:

1. If the input analog signal is higher than the last value of the staircase signal, increase delta by 1, and the bit in the digital data is 1.
2. If the input analog signal is lower than the last value of the staircase signal, decrease delta by 1, and the bit in the digital data is 0.



c. ADAPTIVE DELTA MODULATION:

The performance of a delta modulator can be improved significantly by making the step size of the modulator assume a time-varying form. A larger step-size is needed where the message has a steep slope of modulating signal and a smaller step-size is needed where the message has a small slope. The size is adapted according to the level of the input signal. This method is known as adaptive delta modulation (ADM).



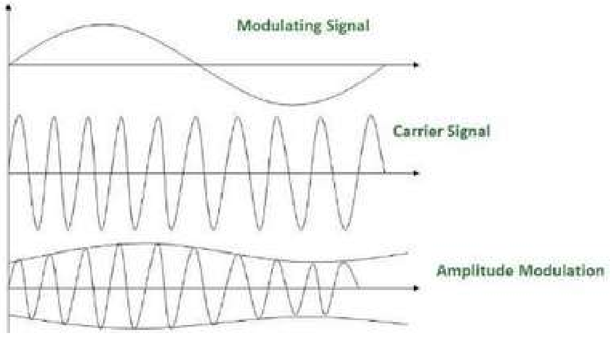
3.5 <u>ANALOG DATA TO ANALOG DATA-</u>

Analog to Analog conversion can be done in three ways:

1. Amplitude Modulation
2. Frequency Modulation
3. Phase Modulation

1. AMPLITUDE MODULATION:

The modulation in which the amplitude of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping phase and frequency as constant. The figure below shows the concept of amplitude modulation:



AM is normally implemented by using a simple multiplier because the amplitude of the carrier signal needs to be changed according to the amplitude of the modulating signal.

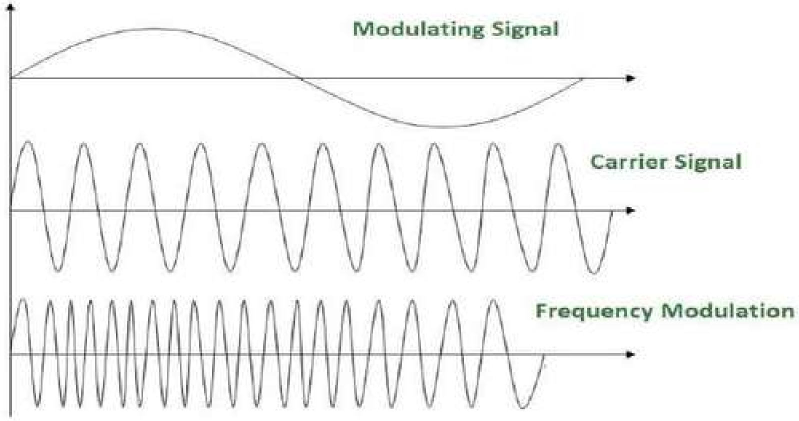
AM bandwidth:

The modulation creates a bandwidth that is twice the bandwidth of the modulating signal and covers a range centered on the carrier frequency.

Bandwidth= 2fm

2. FREQUENCY MODULATION –

The modulation in which the frequency of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping phase and amplitude as constant. The figure below shows the concept of frequency modulation:



FM is normally implemented by using a voltage-controlled oscillator as with FSK. The frequency of the oscillator changes according to the input voltage which is the amplitude of the modulating signal.

FM bandwidth:

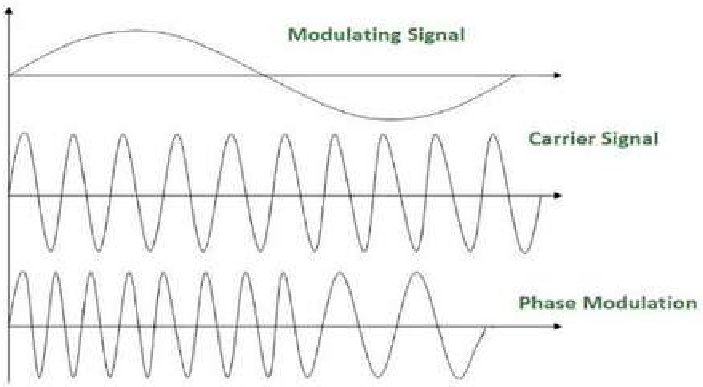
1. The bandwidth of a frequency modulated signal varies with both deviation and modulating frequency.

If modulating frequency (Mf) 0.5, wide band Fm signal.

2. For a narrow band Fm signal, bandwidth required is twice the maximum frequency of the modulation, however for a wide band Fm signal the required bandwidth can be very much larger, with detectable sidebands spreading out over large amounts of the frequency spectrum.

3. PHASE MODULATION:

The modulation in which the phase of the carrier wave is varied according to the instantaneous amplitude of the modulating signal keeping amplitude and frequency as constant. The figure below shows the concept of frequency modulation:



Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. It is normally implemented by using a voltage-controlled oscillator along with a derivative. The frequency of the oscillator changes according to the derivative of the input voltage which is the amplitude of the modulating signal.

PM bandwidth:

1. For small amplitude signals, PM is similar to amplitude modulation (AM) and exhibits its unfortunate doubling of baseband bandwidth and poor efficiency.

2. For a single large sinusoidal signal, PM is similar to FM, and its bandwidth is approximately, **2 (h+1) Fm** where h= modulation index.

Thus, Modulation allows us to send a signal over a bandpass frequency range. If every signal gets its own frequency range, then we can transmit multiple signals simultaneously over a single channel, all using different frequency ranges.

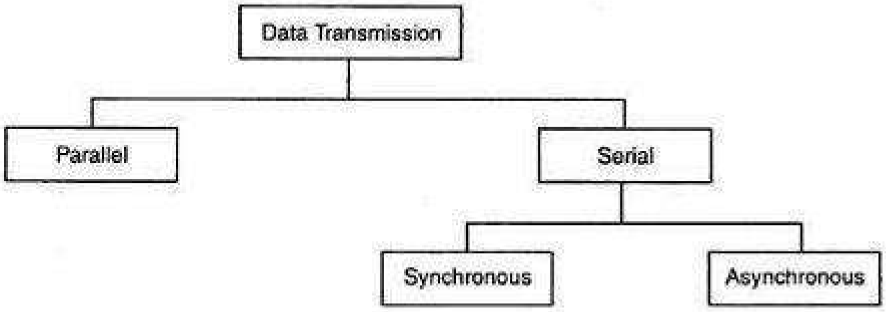
UNIT-4: DATA COMMUNICATION & DATA LINK CONTROL

4.1 DATA TRANSMISSION CONCEPT

Data transmission refers to the movement of data in form of bits between two or more digital devices.

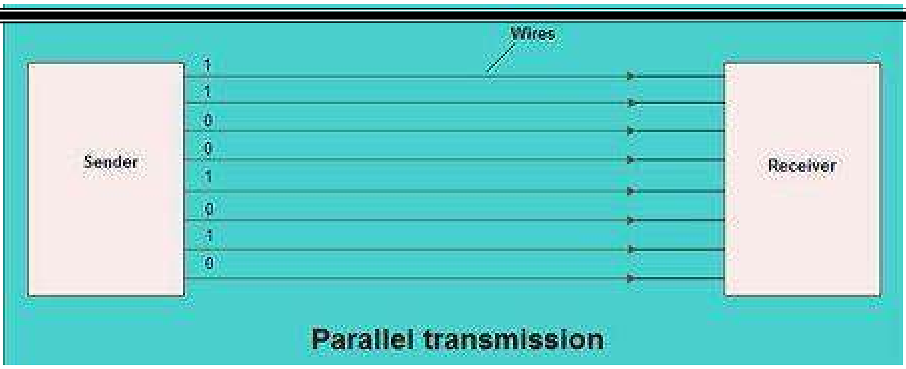
This transfer of data takes place via some form of transmission media (for example, coaxial cable, fiber optics etc.)

Types of Data Transmission



PARALLEL TRANSMISSION

- In parallel transmission, all the bits of data are transmitted simultaneously on separate communication lines.
- In order to transmit *n* bits, *n* wires or lines are used. Thus each bit has its own line.
- All n bits of one group are transmitted with each clock pulse from one device to another *i.e.*multiple bits are sent with each clock pulse.
- Parallel transmission is used for short distance communication.
- As shown in the fig, eight separate wires are used to transmit 8 bit data from sender to receiver.



Advantage of parallel transmission

It is speedy way of transmitting data as multiple bits are transmitted simultaneously with a single clock pulse.

Disadvantage of parallel transmission

It is costly method of data transmission as it requires *n* lines to transmit *n* bits at the same time.

SERIAL TRANSMISSION

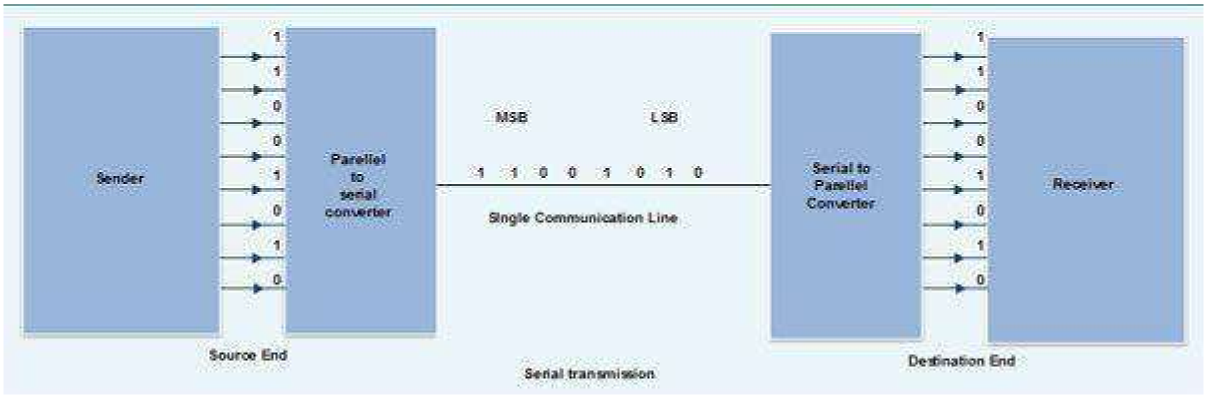
Defination: When transferring data between two physically separate devices, especially if the separation is more than a few kilometers, for reasons of cost, it is more economical to use a single pair of lines.

Data is transmitted as a single bit at a time using a fixed time interval for each bit. This mode of transmission is known as *bit-serial* transmission.

- In serial transmission, the various bits of data are transmitted serially one after the other.
- It requires only one communication line rather than *n* lines to transmit data from sender to receiver.
- Thus all the bits of data are transmitted on single line in serial fashion.
- In serial transmission, only single bit is sent with each clock pulse.
- As shown in fig., suppose an 8-bit data 11001010 is to be sent from source to destination. Then least significant bit (LSB) *i,e.*0 will be transmitted first followed by other bits. The most significant bit (MSB) *i.e.*1 will be transmitted in the end via single communication line.
- The internal circuitry of computer transmits data in parallel fashion. So in order to change this parallel data into serial data, conversion devices are used.
- These conversion devices convert the parallel data into serial data at the sender side so that it can be transmitted over single line.

- On receiver side, serial data received is again converted to parallel form so that the interval circuitry of computer can accept it

- Serial transmission is used for long distance communication.



Advantage of Serial transmission

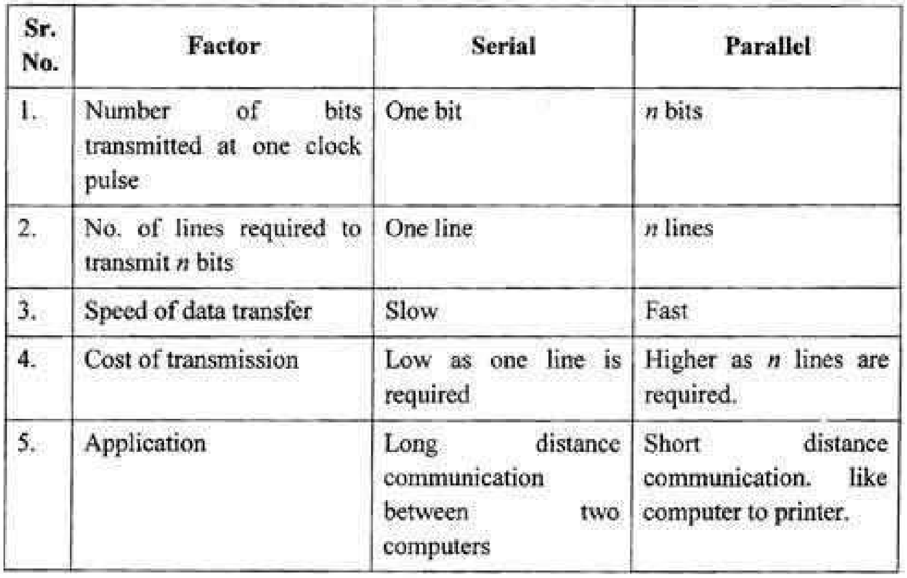
Use of single communication line reduces the transmission line cost by the factor of *n* as compared to parallel transmission.

Disadvantages of Serial transmission

1. Use of conversion devices at source and destination end may lead to increase in overall transmission cost.

2. This method is slower as compared to parallel transmission as bits are transmitted serially one after the other.

Comparison between Serial and Parallel transmission



Sr. No.	Factor	Serial	Parallel
1.	Number of bits transmitted at one clock pulse	One bit	*n* bits
2.	No. of lines required to transmit *n* bits	One line	*n* lines
3.	Speed of data transfer	Slow	Fast
4.	Cost of transmission	Low as one line is required	Higher as *n* lines are required.
5.	Application	Long distance communication between two computers	Short distance communication. like computer to printer.

TYPES OF SERIAL TRANSMISSION

There are two types of serial transmission

synchronous transmission and

asynchronous transmissions

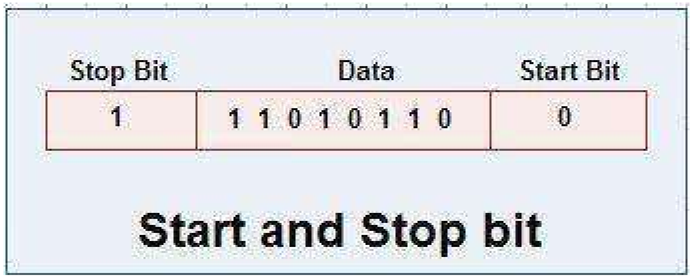
both these uses '**Bit synchronization**'.Bit Synchronization is a function that is required to determine when the beginning and end of the data transmission occurs.
Bit synchronization helps the receiving computer to know when data begin and end during a transmission. Therefore bit synchronization provides timing control.

ASYNCHRONOUS TRANSMISSION

- Asynchronous transmission sends only one character at a time where a character is either a letter of the alphabet or number or control character *i.e.*it sends one byte of data at a time.

- Bit synchronization between two devices is made possible using start bit and stop bit.

- Start bit indicates the beginning of data *i.e.*alerts the receiver to the arrival of new group of bits. A start bit usually 0 is added to the beginning of each byte.
- Stop bit indicates the end of data *i.e.*to let the receiver know that byte is finished, one or more additional bits are appended to the end of the byte. These bits, usually 1s are called stop bits.



Stop Bit	Data	Start Bit
1	1 1 0 1 0 1 1 0	0

Start and Stop bit

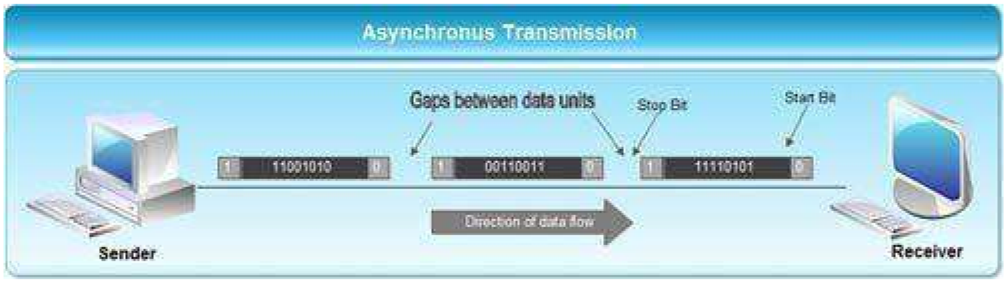
Addition of start and stop increase the number of data bits. Hence more bandwidth is consumed in asynchronous transmission.

- There is idle time between the transmissions of different data bytes. This idle time is also known as Gap
- The gap or idle time can be of varying intervals. This mechanism is called Asynchronous, because at byte level sender and receiver need not to be synchronized. But within each byte, receiver must be synchronized with the incoming bit stream.

Application of Asynchronous Transmission

1. Asynchronous transmission is well suited for keyboard type-terminals and paper tape devices. The advantage of this method is that it does not require any local storage at the terminal or the computer as transmission takes place character by character.

2. Asynchronous transmission is best suited to Internet traffic in which information is transmitted in short bursts. This type of transmission is used by modems.



Advantages of Asynchronous transmission

1. This method of data transmission is cheaper in cost as compared to synchronous *e.g.* If lines are short, asynchronous transmission is better, because line cost would be low and idle time will not be expensive.

2. In this approach each individual character is complete in itself, therefore if character is corrupted during transmission, its successor and predecessor character will not be affected.

3. It is possible to transmit signals from sources having different bit rates.

4. The transmission can start as soon as data byte to be transmitted becomes available.

5. Moreover, this mode of data transmission in easy to implement.

Disadvantages of asynchronous transmission

1. This method is less efficient and slower than synchronous transmission due to the overhead of extra bits and insertion of gaps into bit stream.

2. Successful transmission inevitably depends on the recognition of the start bits. These bits can be missed or corrupted.

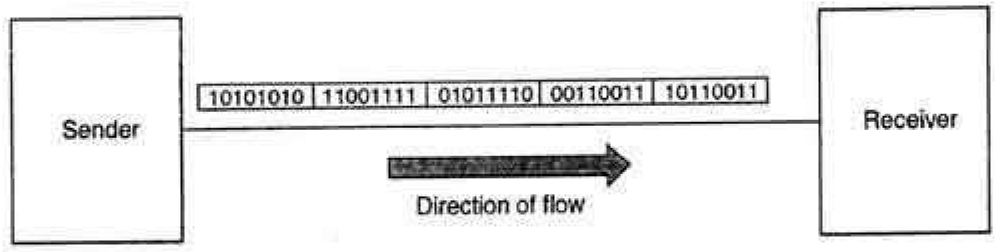
SYNCHRONOUS TRANSMISSION

Synchronous data transmission is a data transfer method in which a continuous stream of data signals is accompanied by timing signals (generated by an electronic clock) to ensure that the transmitter and the receiver are in step (synchronized) with one another. The data is sent in blocks (called frames or packets) spaced by fixed time intervals.

- Synchronous transmission does not use start and stop bits.

• In this method bit stream is combined into longer frames that may contain multiple bytes.

• There is no gap between the various bytes in the data stream.



Synchronous Transmission

• In the absence of start & stop bits, bit synchronization is established between sender & receiver by *'timing'* the transmission of each bit.

• Since the various bytes are placed on the link without any gap, it is the responsibility of receiver to separate the bit stream into bytes so as to reconstruct the original information.

• In order to receive the data error free, the receiver and sender operates at the same clock frequency.

Application of Synchronous transmission

• Synchronous transmission is used for high speed communication between computers.

Advantage of Synchronous transmission

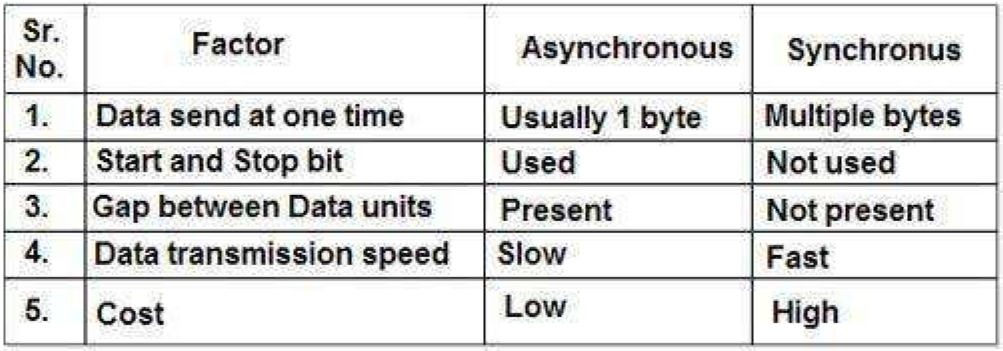
1. This method is faster as compared to asynchronous as there are no extra bits (start bit & stop bit) and also there is no gap between the individual data bytes.

Disadvantages of Synchronous transmission

1. It is costly as compared to asynchronous method. It requires local buffer storage at the two ends of line to assemble blocks and it also requires accurately synchronized clocks at both ends. This lead to increase in the cost.

2. The sender and receiver have to operate at the same clock frequency. This requires proper synchronization which makes the system complicated.

Comparison between Asynchronous and Synchronous



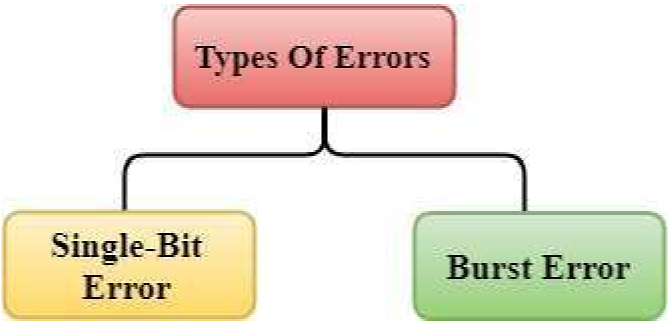
Sr. No.	Factor	Asynchronous	Synchronus
1.	Data send at one time	Usually 1 byte	Multiple bytes
2.	Start and Stop bit	Used	Not used
3.	Gap between Data units	Present	Not present
4.	Data transmission speed	Slow	Fast
5.	Cost	Low	High

4.2 ERROR

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:

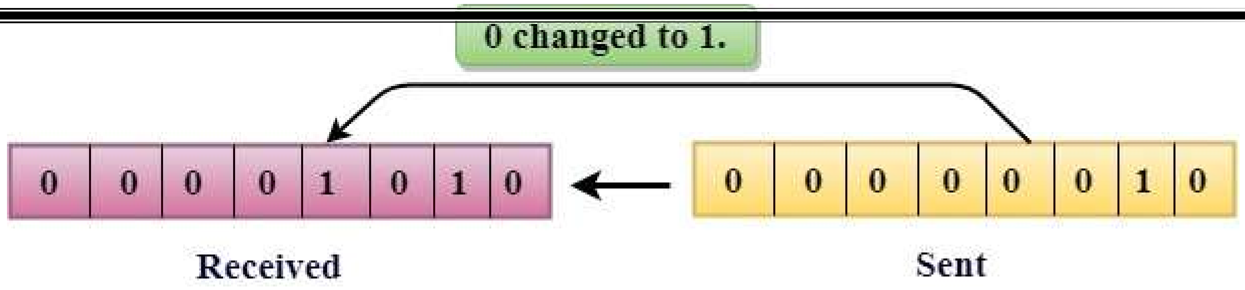
o Single-Bit Error

o Burst Error

o Single-Bit Error:

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

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

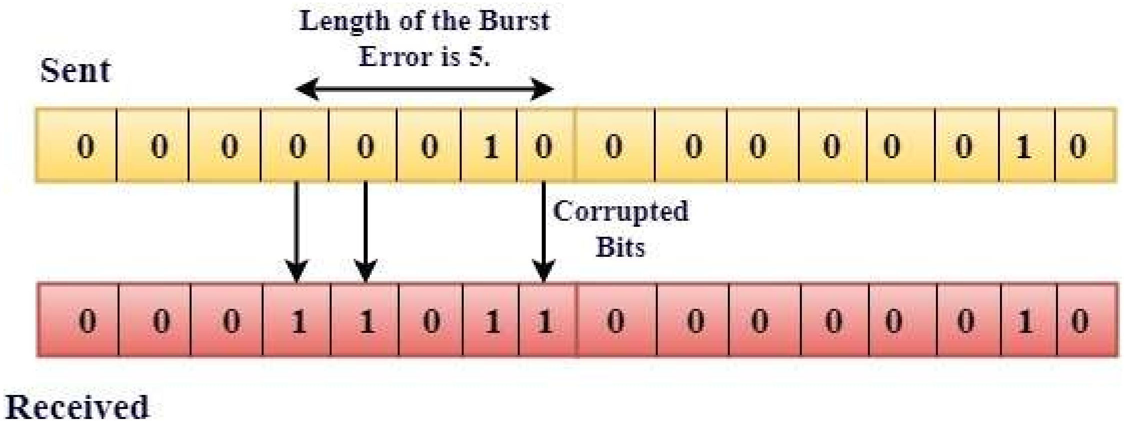


In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.

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 occur in Serial Data Transmission.

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

Error Detection Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.

Some popular techniques for error detection are:

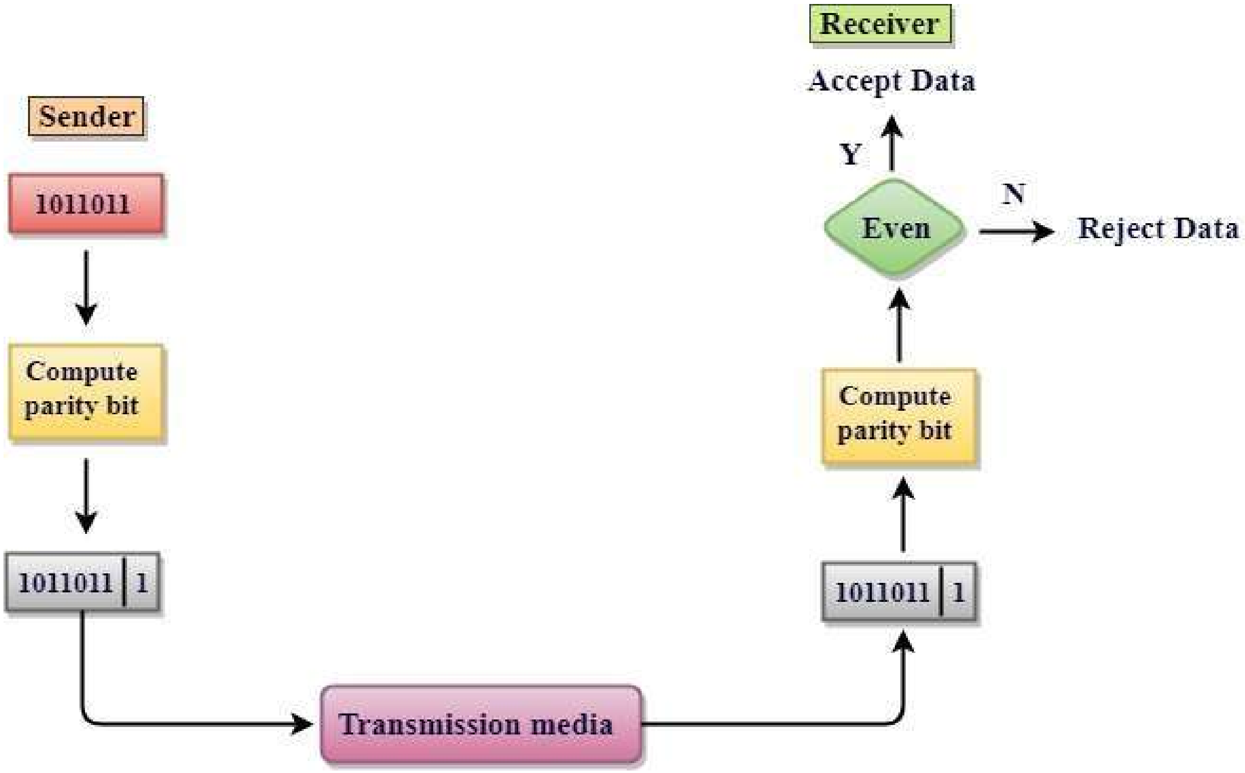
1. Simple Parity check
2. Two-dimensional Parity check

3. Checksum

4. Cyclic redundancy check

1. 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.



Example

Consider the data unit to be transmitted is 10010001 and even parity is used.

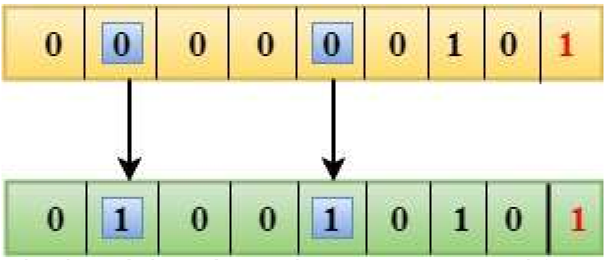
Then, code word transmitted to the receiver = 100100011

Transmitted data (unprotected): 1111000 1010101 1111111

Even parity: 11110000 10101010 11111111

Drawbacks Of Single Parity Checking

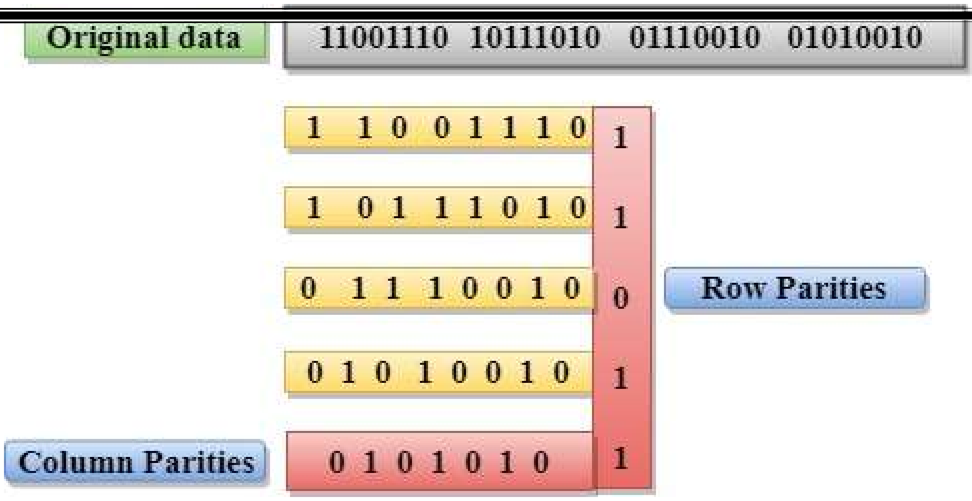
- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.



Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

2. 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

o 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.

o This technique cannot be used to detect the 4-bit errors or more in some cases.

example

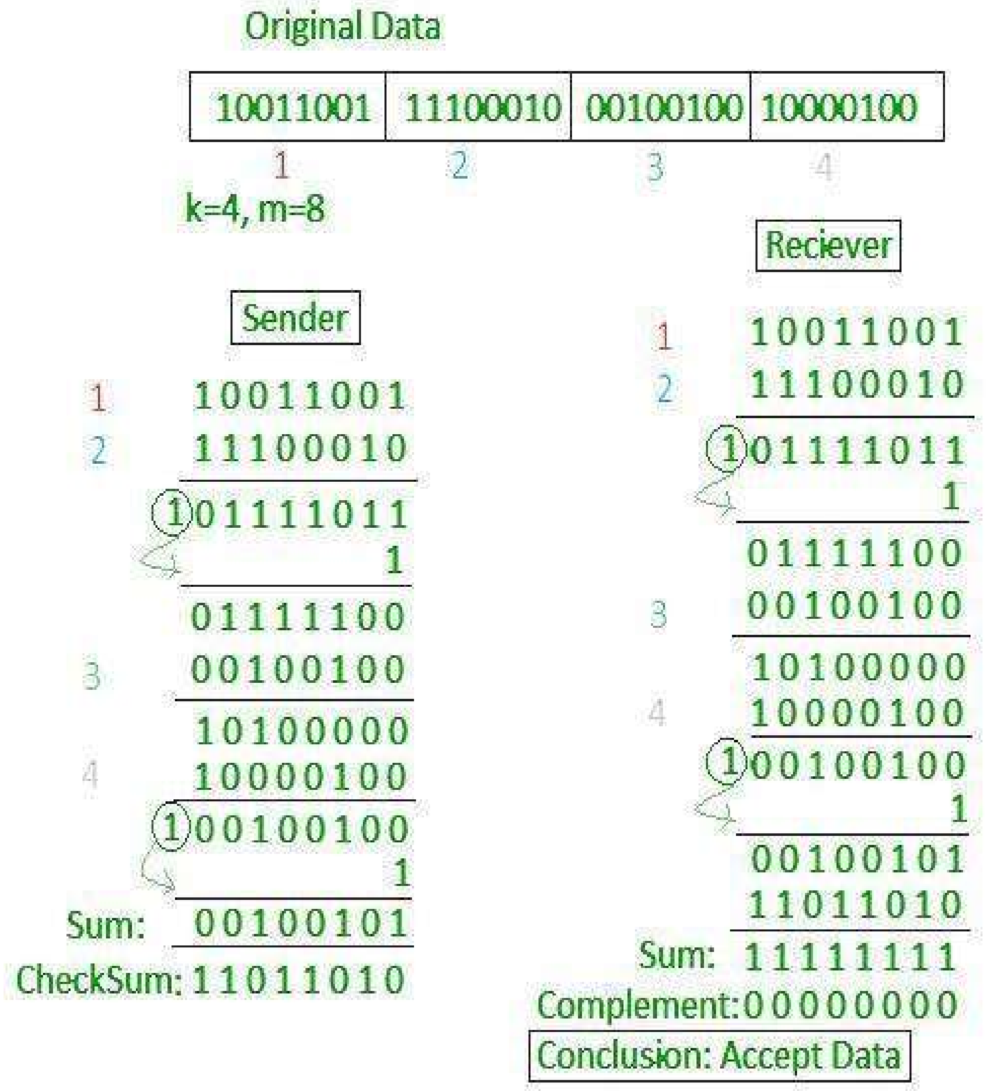
Transmitted data (unprotected): 1111000 1010101 1111111

Two dimensional (even) parity:

11110000
10101010
11111111
10100101

3. **CHECKSUM**

 In checksum error detection scheme, the data is divided into k segments each of m bits.
 In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
 The checksum segment is sent along with the data segments.
 At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
 If the result is zero, the received data is accepted; otherwise discarded.



Example

If the data unit to be transmitted is 10101001 00111001 what will be the checksum.

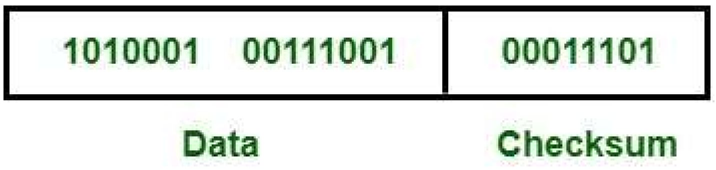
10101001 subunit 1

00111001 subunit 2

11100010 sum (using 1s complement)

00011101 checksum (complement of sum)

Data transmitted to Receiver is –



1010001 00111001	00011101
Data	Checksum

Receiver Site :

10101001 subunit 1

00111001 subunit 2

00011101 checksum

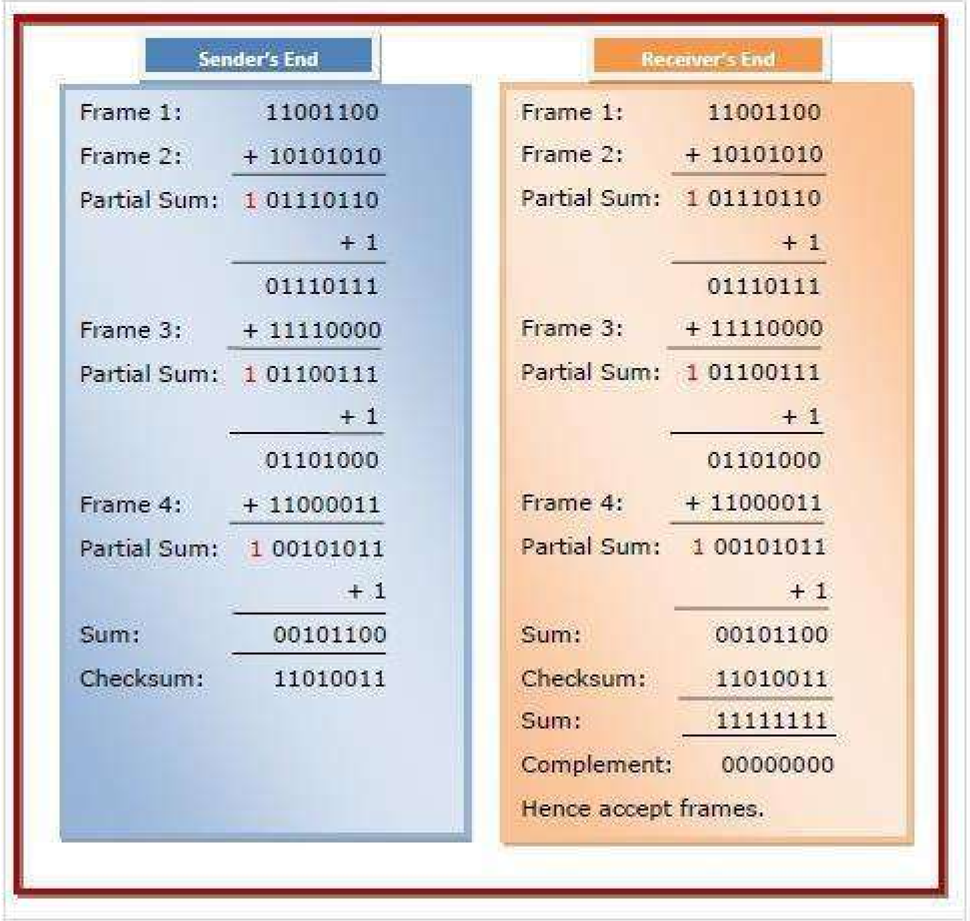
11111111 sum

00000000 sum's complement

Result is zero, it means no error.

Example

Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.



Sender's End

```
Frame 1:         11001100
Frame 2:       + 10101010
Partial Sum:   1 01110110
                      + 1
                 01110111
Frame 3:       + 11110000
Partial Sum:   1 01100111
                      + 1
                 01101000
Frame 4:       + 11000011
Partial Sum:   1 00101011
                      + 1
Sum:             00101100
Checksum:        11010011
```

Receiver's End

```
Frame 1:         11001100
Frame 2:       + 10101010
Partial Sum:   1 01110110
                      + 1
                 01110111
Frame 3:       + 11110000
Partial Sum:   1 01100111
                      + 1
                 01101000
Frame 4:       + 11000011
Partial Sum:   1 00101011
                      + 1
Sum:             00101100
Checksum:        11010011
Sum:             11111111
Complement:      00000000
Hence accept frames.
```

4. CYCLIC REDUNDANCY CHECK (CRC)

1. 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 divisior which is n+1 bits.

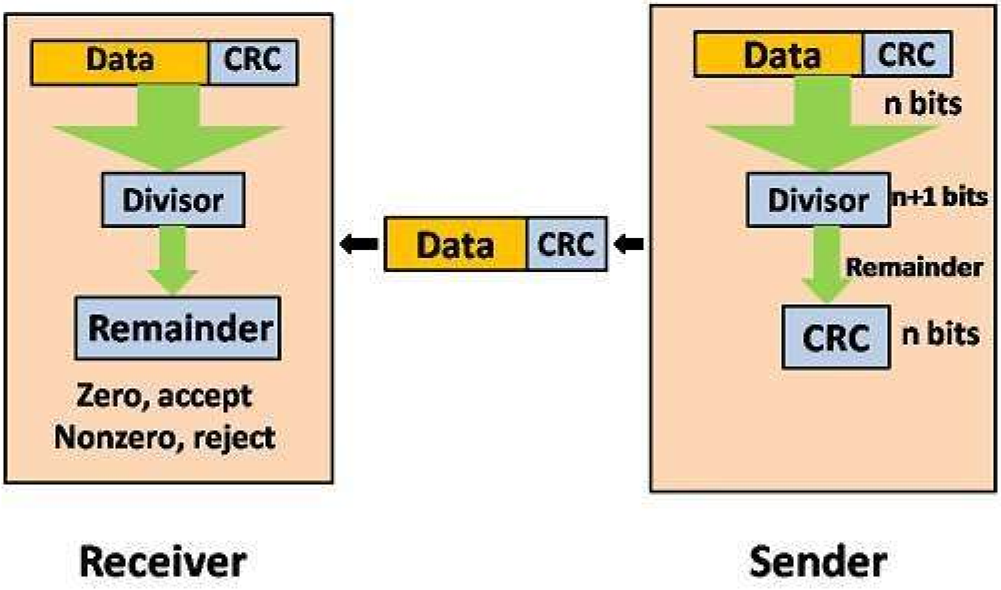
2. Secondly, the newly extended data is divided by a divisor using a process is known as binary division. The remainder generated from this division is known as CRC remainder.

3. Thirdly, the CRC remainder replaces the appended 0s at the end of the original data. This newly generated unit is sent to the receiver.

4. 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.

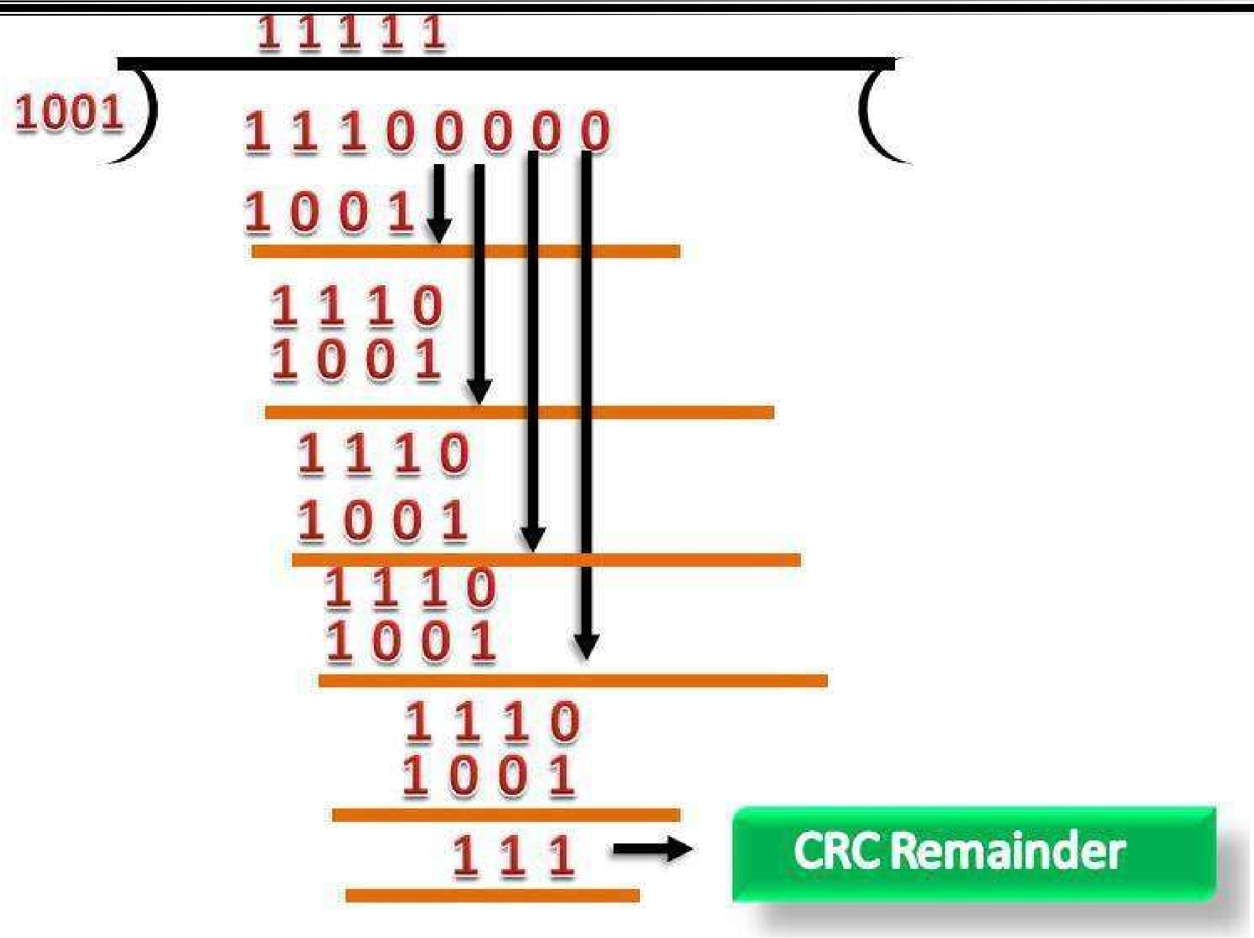


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

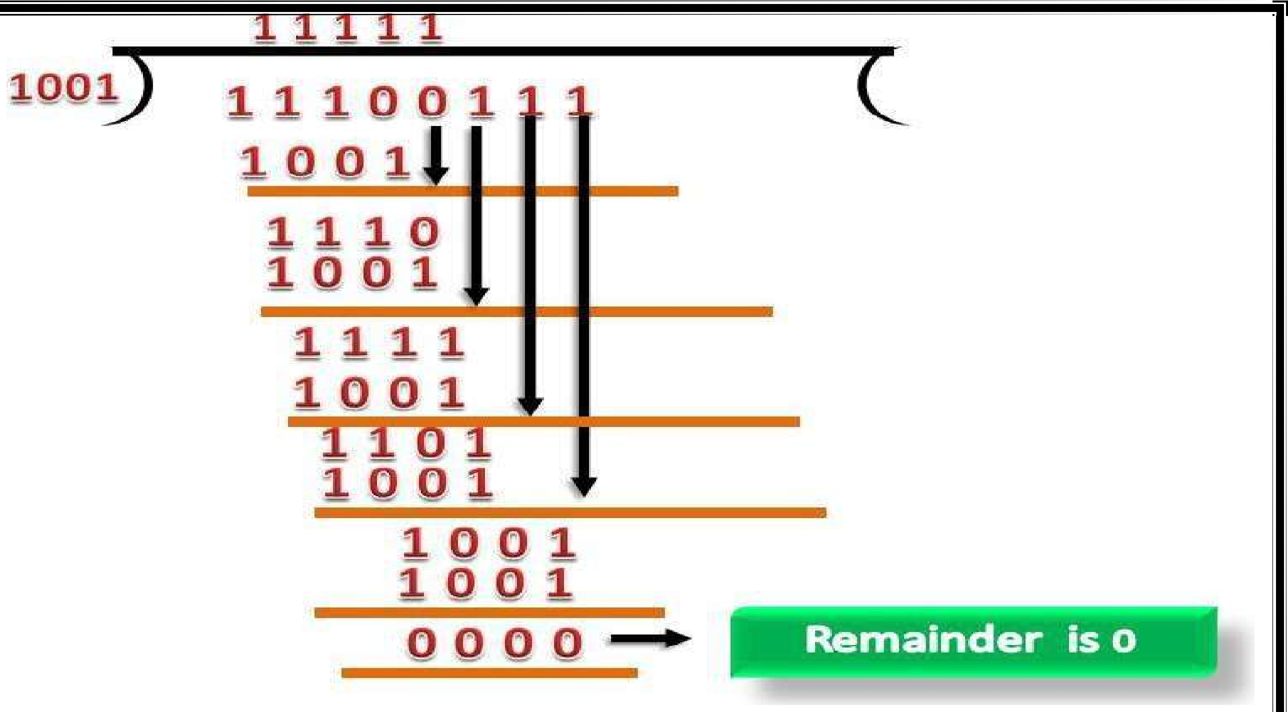
CRC Generator

- 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.

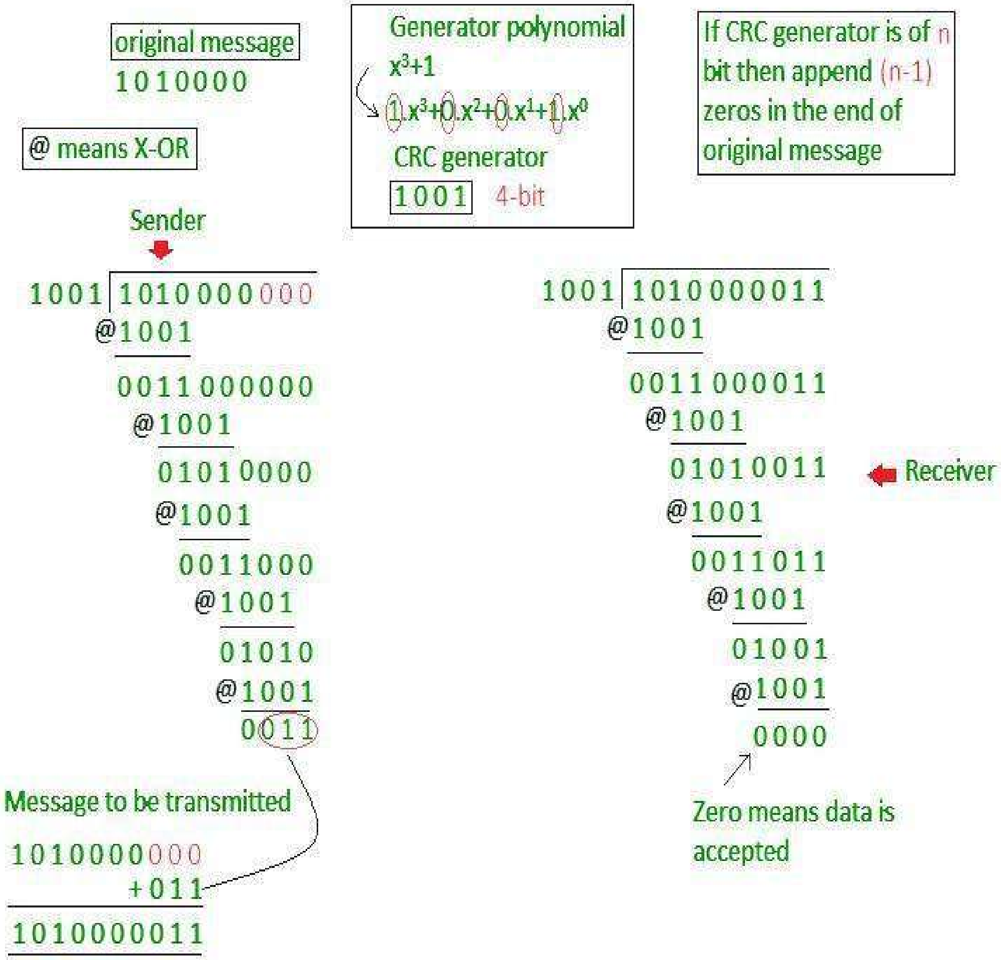


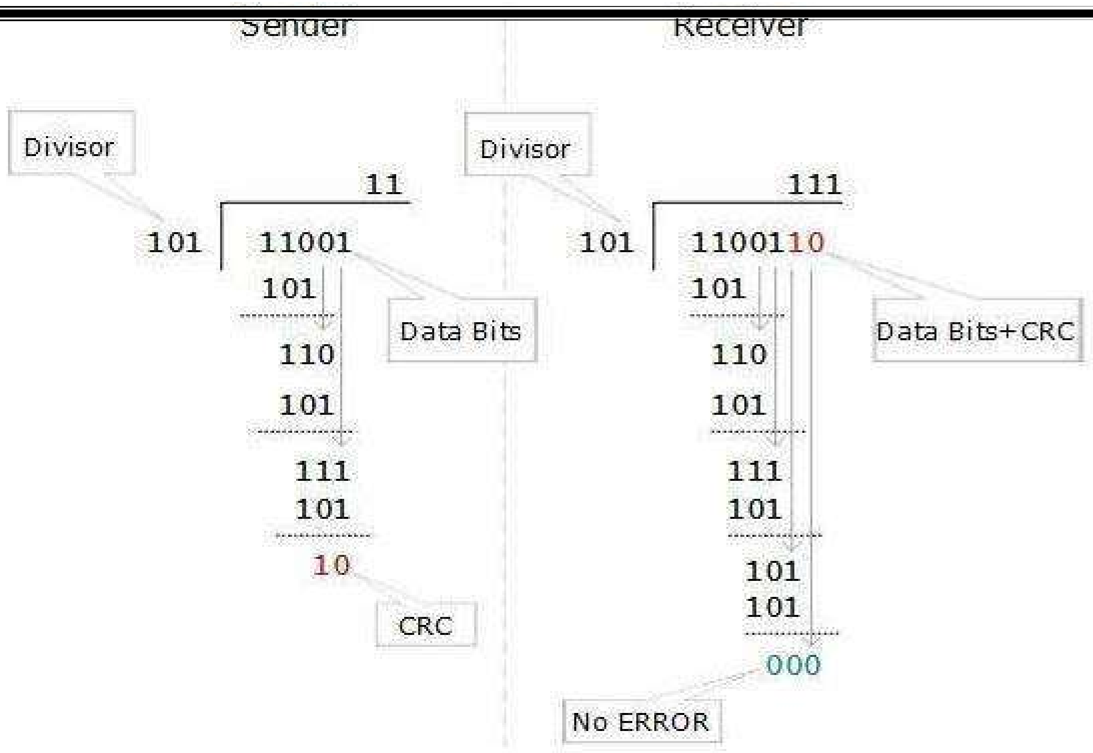
CRC Checker

- 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.


1 1 1 1 1
1001
1 1 1 0 0 1 1 1
1 0 0 1
1 1 1 0
1 0 0 1
1 1 1 1
1 0 0 1
1 1 0 1
1 0 0 1
1 0 0 1
1 0 0 1
0 0 0 0
Remainder is 0

Example :


original message
1010000
@ means X-OR
Generator polynomial
x³+1
1.x³+0.x²+0.x¹+1.x⁰
CRC generator
1001 4-bit
If CRC generator is of n bit then append (n-1) zeros in the end of original message
Sender
1001 | 1010000000
@1001
0011000000
@1001
01010000
@1001
0011000
@1001
01010
@1001
0011
Message to be transmitted
1010000000
+011
1010000011
1001 | 1010000011
@1001
0011000011
@1001
01010011
@1001
0011011
@1001
01001
@1001
0000
Receiver
Zero means data is accepted



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:

o **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.

o **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:
2r>=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:

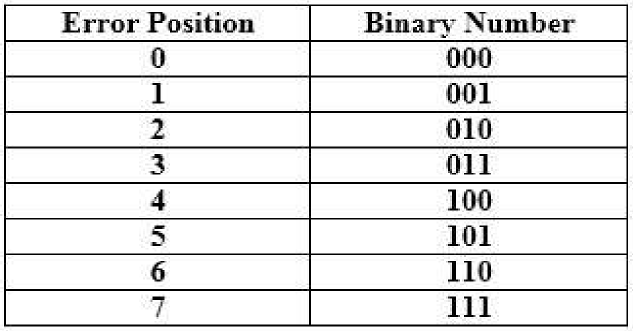
o An information of 'd' bits are added to the redundant bits 'r' to form d+r.

o The location of each of the (d+r) digits is assigned a decimal value.

The 'r' bits are placed in the positions 1,2,.....2k-1o.

o 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: 2r>= d+r+1

2r>= 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

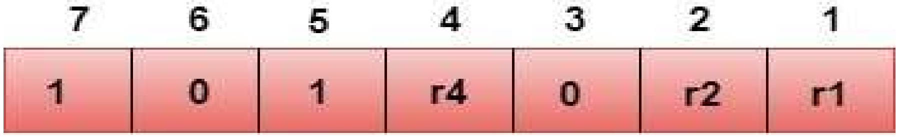
The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 21, 22**.

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:

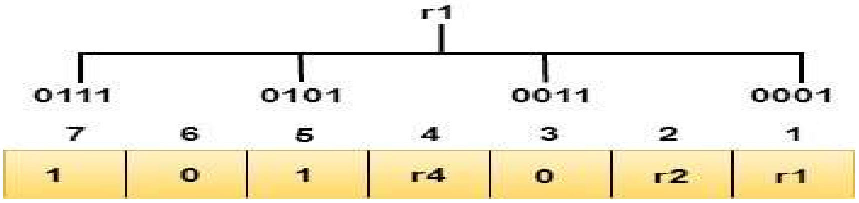


7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

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.

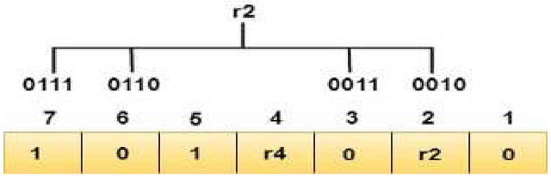


7	6	5	4	3	2	1
1	0	1	r4	0	r2	r1

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

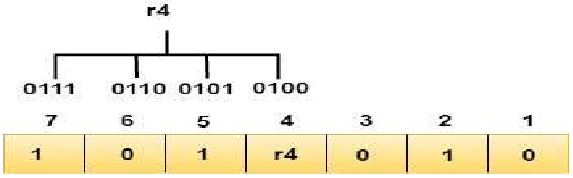
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



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**.

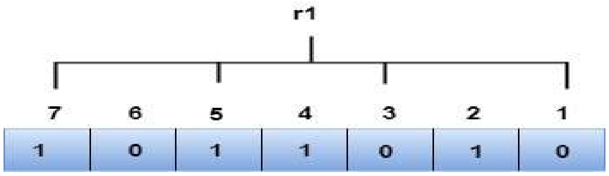
Data transferred is given below:

7	6	5	4	3	2	1
1	0	1	0	0	1	0

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

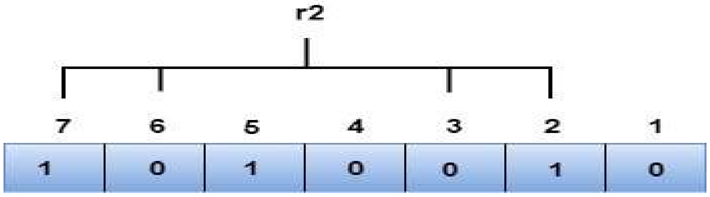


7	6	5	4	3	2	1
1	0	1	1	0	1	0

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.

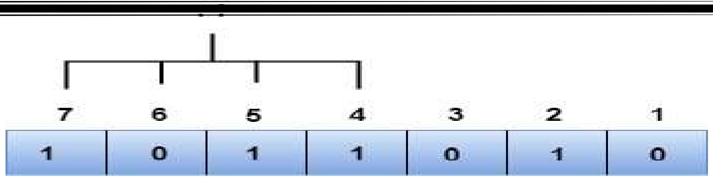


7	6	5	4	3	2	1
1	0	1	0	0	1	0

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.

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

Hamming Distance

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are different.

The Hamming distance between two strings, a and b is denoted as d(a,b).

It is used for error detection or error correction when data is transmitted over computer networks. It is also using in coding theory for comparing equal length data words.

Calculation of Hamming Distance

In order to calculate the Hamming distance between two strings, and , we perform their XOR operation, (a⊕ b), and then count the total number of 1s in the resultant string.

Example

Suppose there are two strings 1101 1001 and 1001 1101.

11011001 ⊕ 10011101 = 01000100. Since, this contains two 1s, the Hamming distance, d(11011001, 10011101) = 2.

Minimum Hamming Distance

In a set of strings of equal lengths, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of strings in that set.

Example

Suppose there are four strings 010, 011, 101 and 111.

010 ⊕ 011 = 001, d(010, 011) = 1.

010 ⊕ 101 = 111, d(010, 101) = 3.

$010 \oplus 111 = 101, d(010, 111) = 2.$

$011 \oplus 101 = 110, d(011, 101) = 2.$

$011 \oplus 111 = 100, d(011, 111) = 1.$

$101 \oplus 111 = 010, d(011, 111) = 1.$

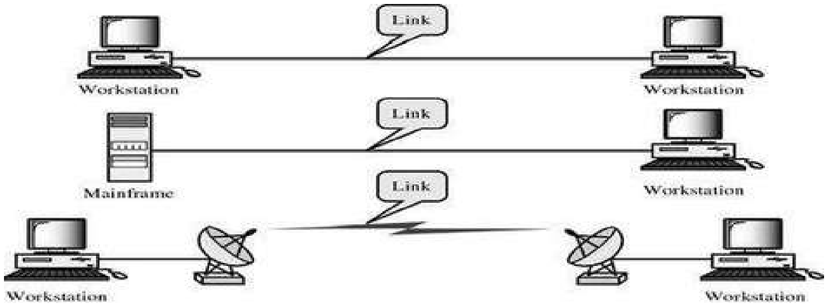
Hence, the Minimum Hamming Distance, $d_{min} = 1$.

4.2 LINE CONFIGURATION

Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A Link is the physical communication pathway that transfers data from one device to another. For communication to occur, two devices must be connected in same way to the same link at the same time.
There are two possible line configurations.
1. Point-to-Point.
2. Multipoint.

Point-to-Point

A **Point to Point Line Configuration** Provide dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control &tvs remote control.
The entire capacity of the channel is reserved for transmission between those two devices. Most point-to-point line configurations 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.
Point to point network topology is considered to be one of the easiest and most conventional network topologies. It is also the simplest to establish and understand. To visualize, one can consider point to point network topology as two phones connected end to end for a two way communication



Multipoint Configuration

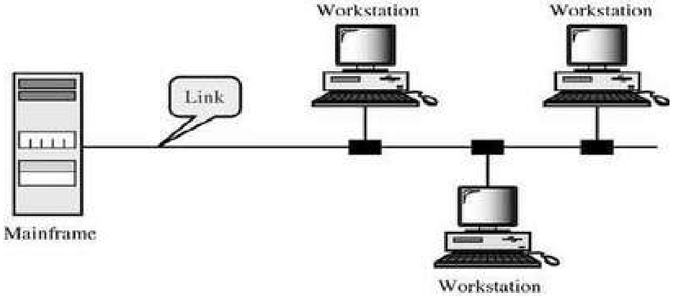
Multipoint Configuration also known as **Multidrop line configuration** one or more than two specific devices share a single link capacity of the channel is shared.

More than two devices share the Link that is the capacity of the channel is shared now.

With shared capacity, there can be two possibilities in a Multipoint Line Config:

□ **Spatial Sharing**: If several devices can share the link simultaneously, its called Spatially shared line configuration

□ **Temporal (Time) Sharing**: If users must take turns using the link , then its called Temporally shared or Time Shared Line Configuration



4.4 FLOW CONTROL-

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

Stop and wait protocol-

• In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment.

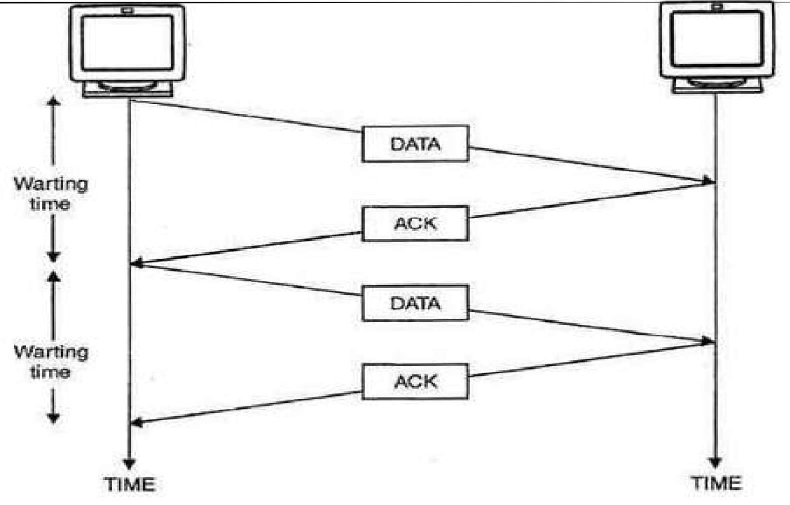
• The next frame is sent by sender only when acknowledgment of previous frame is received.

• This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send.

• To end up the transmission sender transmits end of transmission (EOT) frame.

• The main advantage of stop &wait protocols is its accuracy. Next frame is transmitted only when the first frame is acknowledged. So there is no chance of frame being lost.

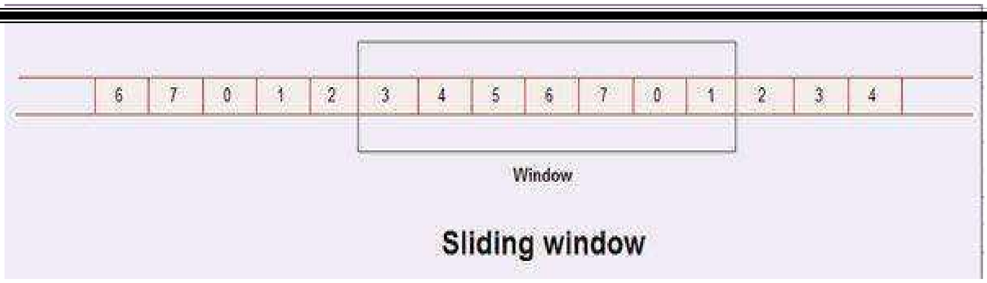
• The main disadvantage of this method is that it is inefficient. It makes the transmission process slow. In this method single frame travels from source to destination and single acknowledgment travels from destination to source. As a result each frame sent and received uses the entire time needed to traverse the link. Moreover, if two devices are distance apart, a lot of time is wasted waiting for ACKs that leads to increase in total transmission time.



Stop & Wait Method.

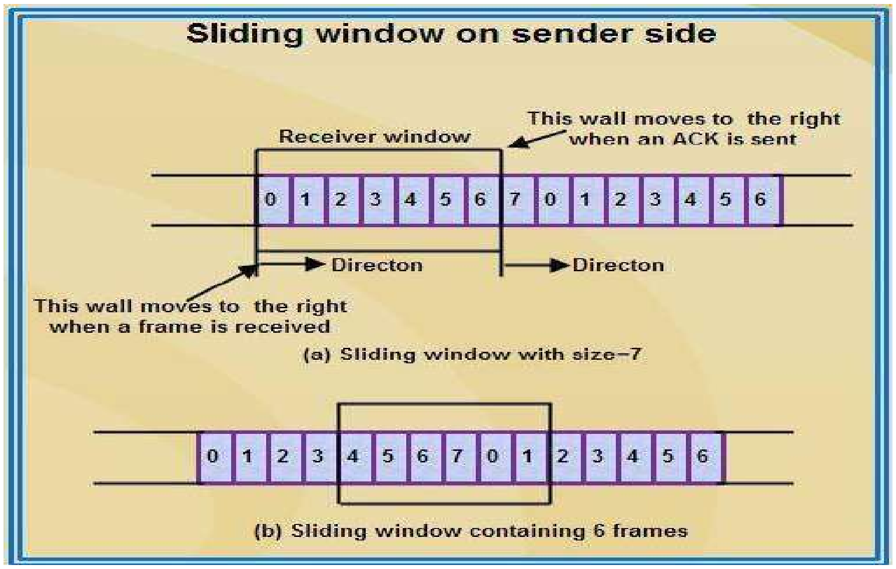
SLIDING WINDOW-

- In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgment.
- Multiple frames sent by source are acknowledged by receiver using a single ACK frame.
- Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.
- It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.
- Frames may be acknowledged by receiver at any point even when window is not full on receiver side.
- Frames may be transmitted by source even when window is not yet full on sender side.
- The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ...
- The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.
- When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.



Sliding Window on Sender Side

- At the beginning of a transmission, the sender's window contains n-l frames.
- As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.
- When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.
- For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4,5,6.
- Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.
- The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1). (See diagram (b)).


Sliding window on sender side
Receiver window
This wall moves to the right when an ACK is sent
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
Directon
Directon
This wall moves to the right when a frame is received
(a) Sliding window with size–7
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6
(b) Sliding window containing 6 frames

Sliding Window on Receiver Side

- At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.
- As the new frames come in, the size of window shrinks.
- Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.

• Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.

• As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.

• For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.

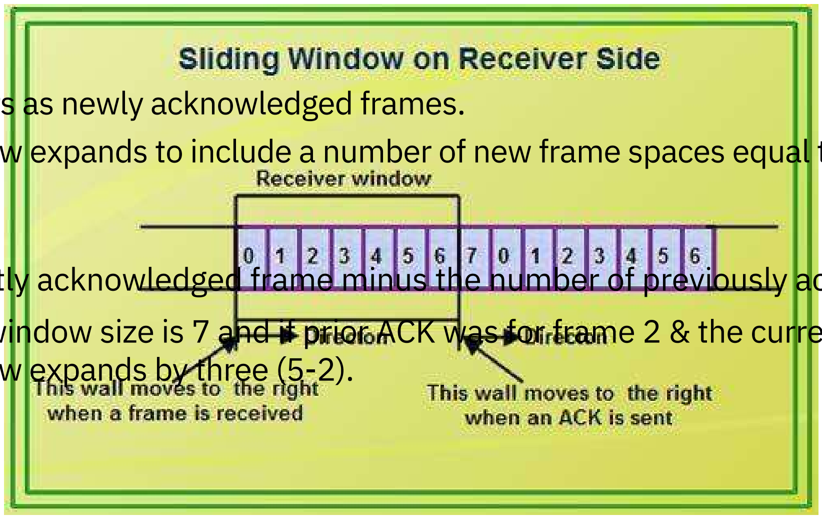
• With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.

• If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.

• As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.

• The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame.

For *e.g.,* If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three (5-2).


Sliding Window on Receiver Side
Receiver window
0
1
2
3
4
5
6
7
0
1
2
3
4
5
6
Direction
Direction
This wall moves to the right when a frame is received
This wall moves to the right when an ACK is sent

• Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.

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

4.5 ERROR CONTROL-

Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.

In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss. Data link layer follows a technique to detect transit errors and take necessary actions, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).

Phases in Error Control

The error control mechanism in data link layer involves the following phases:

 Detection of Error – Transmission error, if any, is detected by either the sender or the receiver.

 Acknowledgment – acknowledgment may be positive or negative.

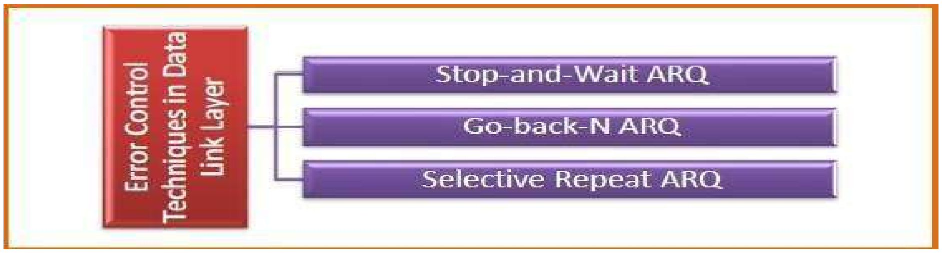
o **Positive ACK** – on receiving a correct frame, the receiver sends a positive acknowledge.

o **Negative ACK** – on receiving a damaged frame or a duplicate frame, the receiver sends a negative acknowledgment back to the sender.

 Retransmission – the sender maintains a clock and sets a timeout period. If an acknowledgment of a data-frame previously transmitted does not arrive before the timeout, or a negative acknowledgment is received, the sender retransmits the frame.

Error Control Techniques

There are three main techniques for error control:



 Stop and Wait ARQ

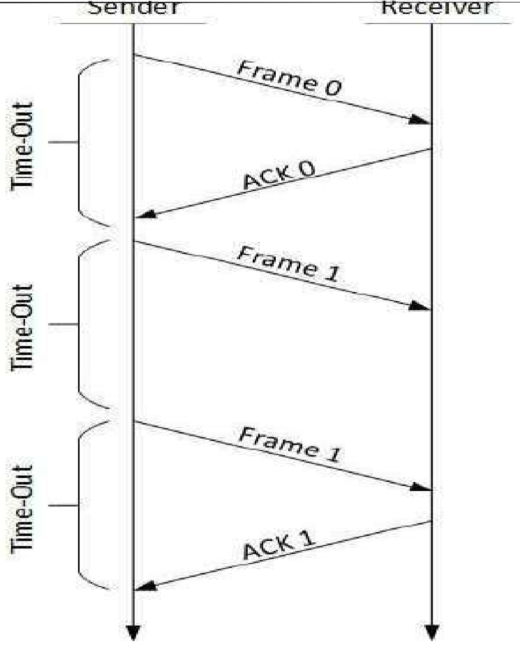
This protocol involves the following transitions:

o A timeout counter is maintained by the sender, which is started when a frame is sent.

o If the sender receives acknowledgment of the sent frame within time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.

o If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.

o If the sender receives a negative acknowledgment, the sender retransmits the frame.



- **Go-Back-N ARQ**

The working principle of this protocol is:

o The sender has buffers called sending window.

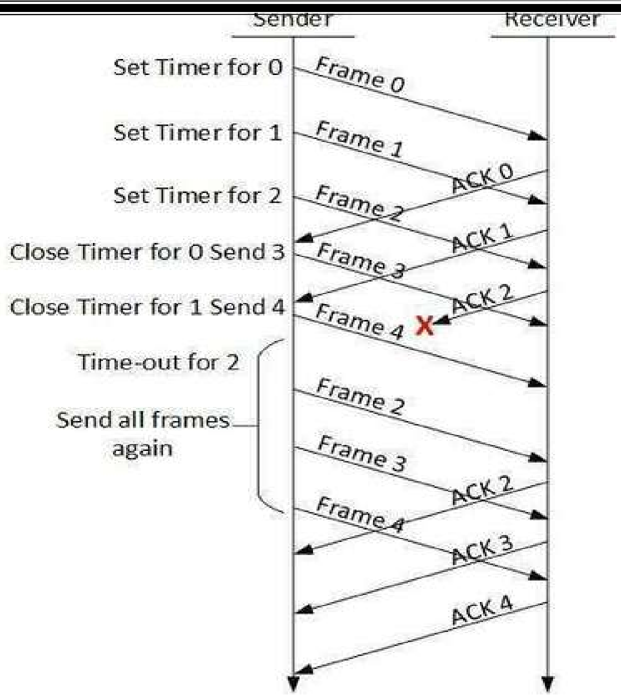
o The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.

o The receiver receives frames one by one. It keeps track of incoming frame’s sequence number and sends the corresponding acknowledgment frames.

o After the sender has sent all the frames in window, it checks up to what sequence number it has received positive acknowledgment.

o If the sender has received positive acknowledgment for all the frames, it sends next set of frames.

o If sender receives NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.



 Selective Repeat ARQ

o Both the sender and the receiver have buffers called sending window and receiving window respectively.

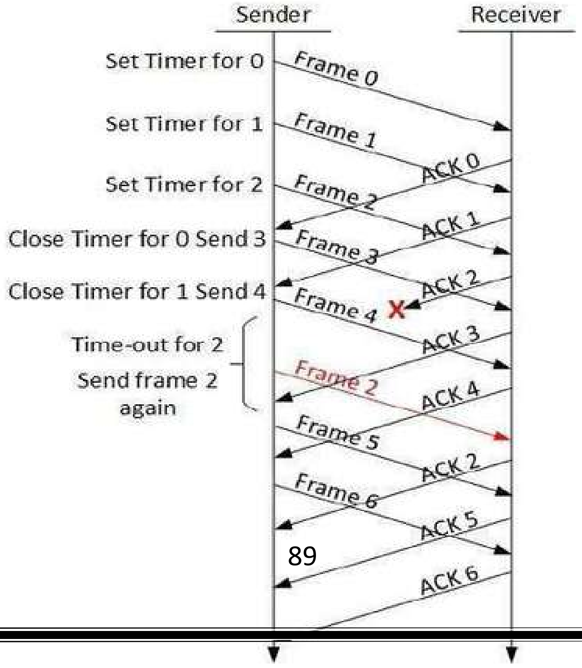
o The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.

o The receiver also receives multiple frames within the receiving window size.

o The receiver keeps track of incoming frame's sequence numbers, buffers the frames in memory.

o It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.

o The sender in this case, sends only packet for which NACK is received.



PIGGYBACKING

n reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.

Why Piggybacking?

Communications are mostly full – duplex in nature, i.e. data transmission occurs in both directions. A method to achieve full – duplex communication is to consider both the communication as a pair of simplex communication. Each link comprises a forward channel for sending data and a reverse channel for sending acknowledgments.

However, in the above arrangement, traffic load doubles for each data unit that is transmitted. Half of all data transmission comprise of transmission of acknowledgments. So, a solution that provides better utilization of bandwidth is piggybacking. Here, sending of acknowledgment is delayed until the next data frame is available for transmission. The acknowledgment is then hooked onto the outgoing data frame. The data frame consists of an *ack* field. The size of the *ack* field is only a few bits, while an acknowledgment frame comprises of several bytes. Thus, a substantial gain is obtained in reducing bandwidth requirement.

Working Principle

Suppose that there are two communication stations X and Y. The data frames transmitted have an acknowledgment field, *ack* field that is of a few bits length. Additionally, there are frames for sending acknowledgments, ACK frames. The purpose is to minimize the ACK frames.

The three principles governing piggybacking when the station X wants to communicate with station Y are –

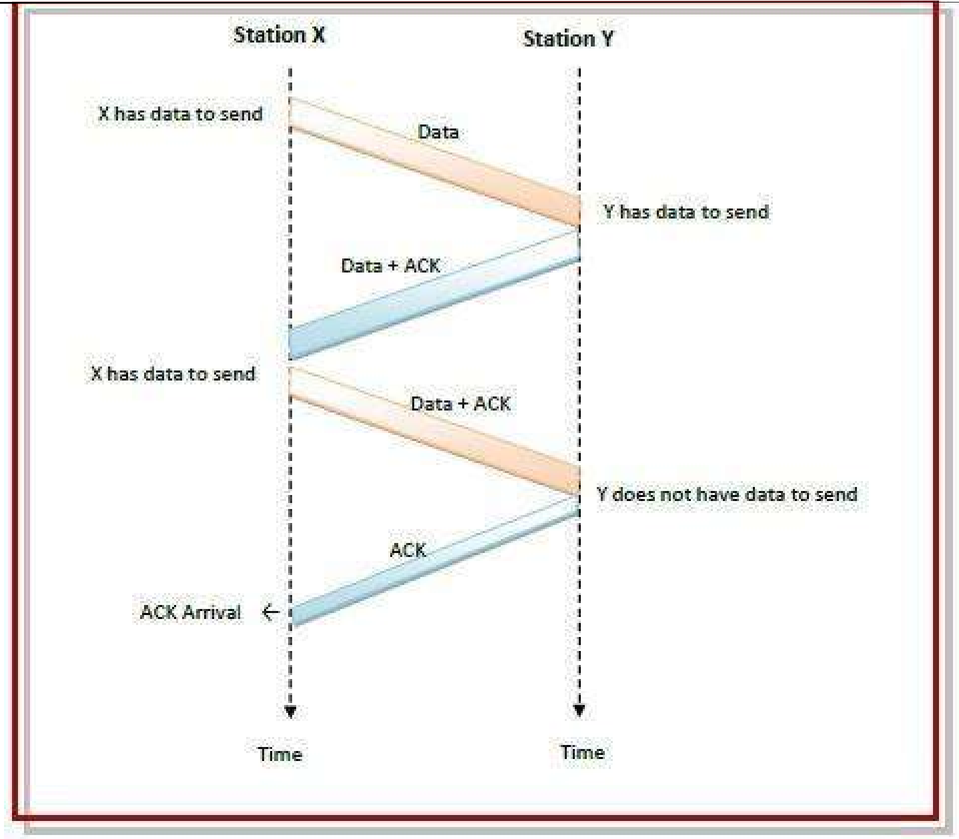
 If station X has both data and acknowledgment to send, it sends a data frame with the *ack* field containing the sequence number of the frame to be acknowledged.

 If station X has only an acknowledgment to send, it waits for a finite period of time to see whether a data frame is available to be sent. If a data frame becomes available, then it piggybacks the acknowledgment with it. Otherwise, it sends an ACK frame.

 If station X has only a data frame to send, it adds the last acknowledgment with it. The station Y discards all duplicate acknowledgments. Alternatively, station X may send the data frame with the *ack* field containing a bit combination denoting no acknowledgment.

Example

The following diagram illustrates the three scenario –



4.6 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?

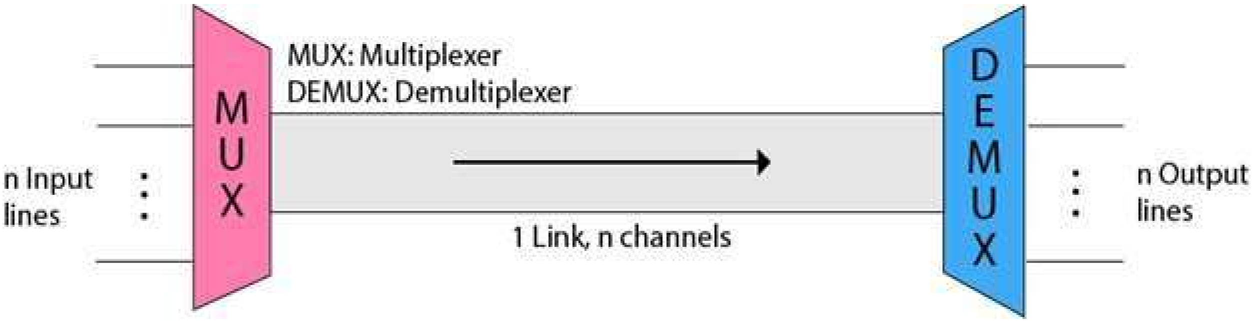
- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some

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.

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.

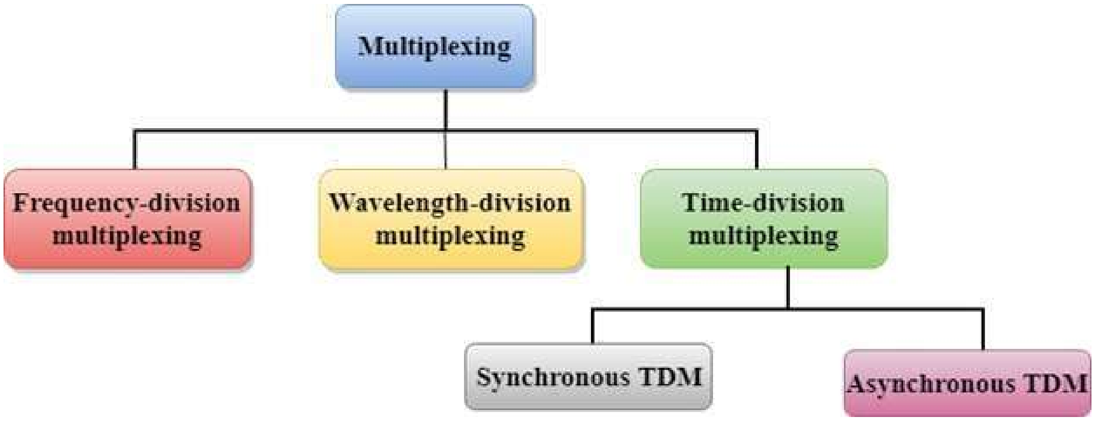
Advantages of Multiplexing:

□ More than one signal can be sent over a single medium.

□ The bandwidth of a medium can be utilized effectively.

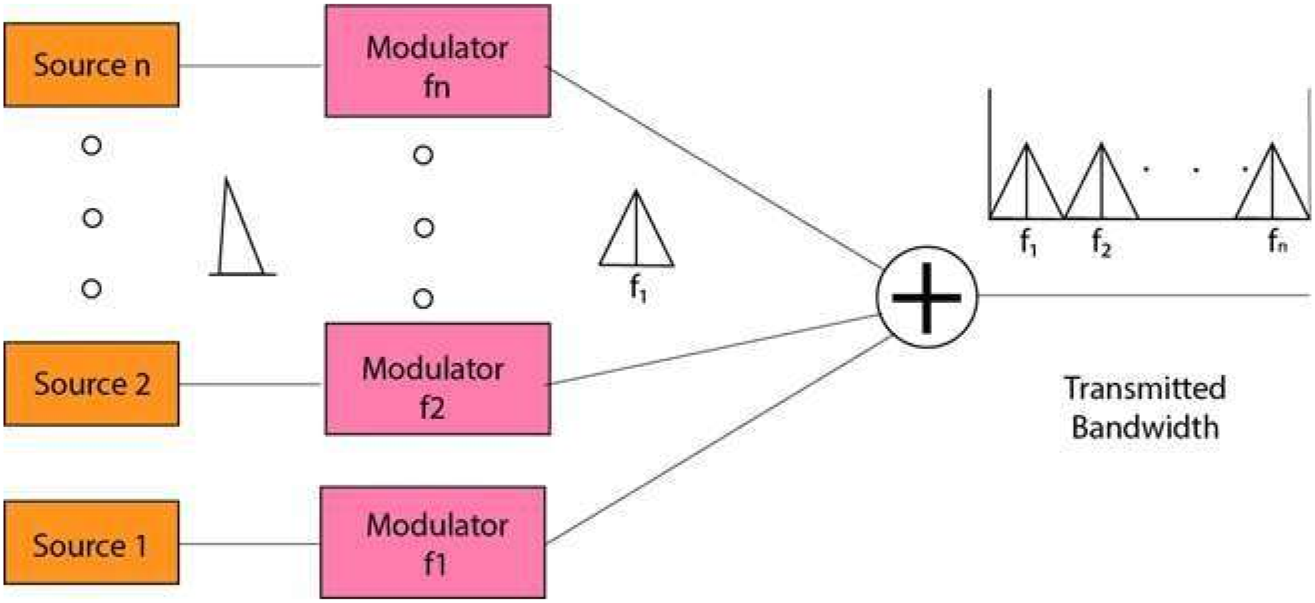
Multiplexing Techniques

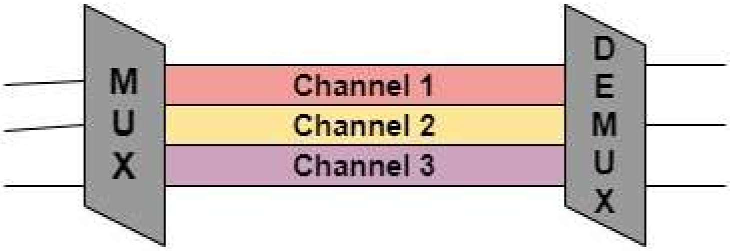
Multiplexing techniques can be classified as:


Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

Frequency-division Multiplexing (FDM)

- When the carrier is frequency, FDM is used.
- FDM is an analog technology.
- FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel.
- Each user can use the channel frequency independently and has exclusive access of it.
- All channels are divided in such a way that they do not overlap with each other.
- Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.





Frequency Division Multiplexing

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.

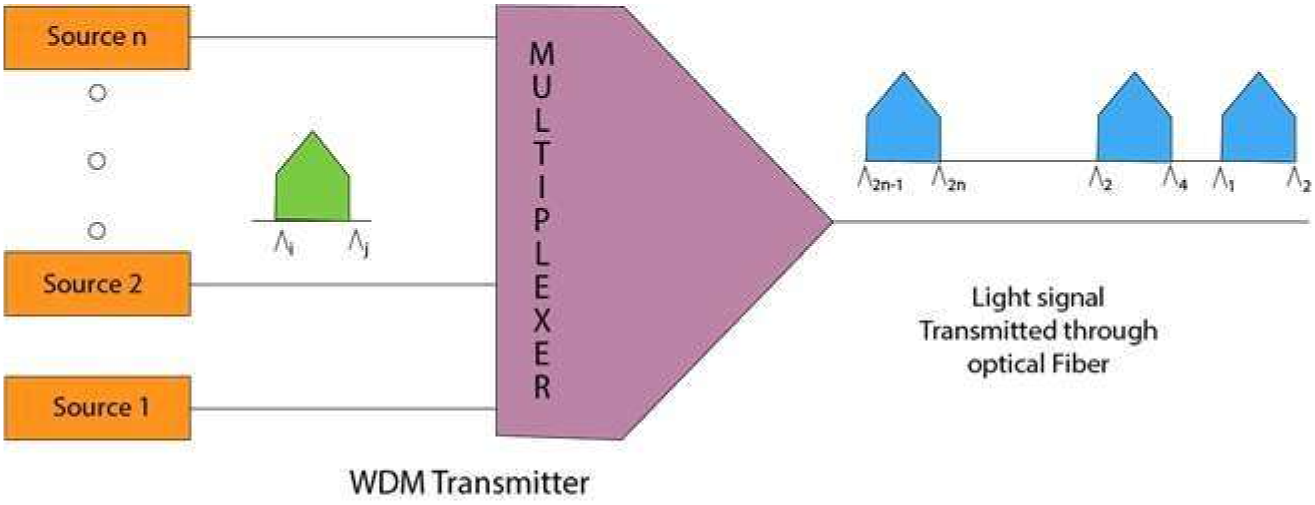
Disadvantages Of FDM:

 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:

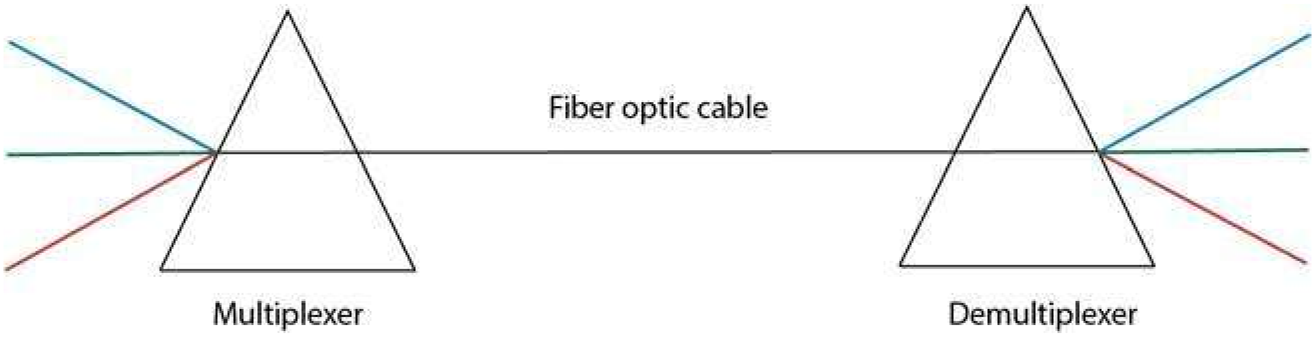
 FDM is commonly used in TV networks.
 It is used in FM and AM broadcasting. Each FM radio station has different frequencies, and they are multiplexed to form a composite signal. The multiplexed signal is transmitted in the air.

Wavelength Division Multiplexing (WDM)



Wavelength Division Multiplexing is same as FDM except that the optical signals are transmitted through the fibre optic cable.
WDM is used on fibre optics to increase the capacity of a single fibre.
It is used to utilize the high data rate capability of fibre optic cable.
It is an analog multiplexing technique.

- Optical signals from different source are combined to form a wider band of light with the help of multiplexer.
- At the receiving end, demultiplexer separates the signals to transmit them to their respective destinations.
- Multiplexing and Demultiplexing can be achieved by using a prism.
- Prism can perform a role of multiplexer by combining the various optical signals to form a composite signal, and the composite signal is transmitted through a fibre optical cable.
- Prism also performs a reverse operation, i.e., demultiplexing the signal.



Advantages of Wavelength Division Multiplexing (WDM)

1. WDM allows transmission of data in two directions simultaneously

2. Low cost

3. Greater transmission capacity

4. High security

5. Long distance communication with low signal loss

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.

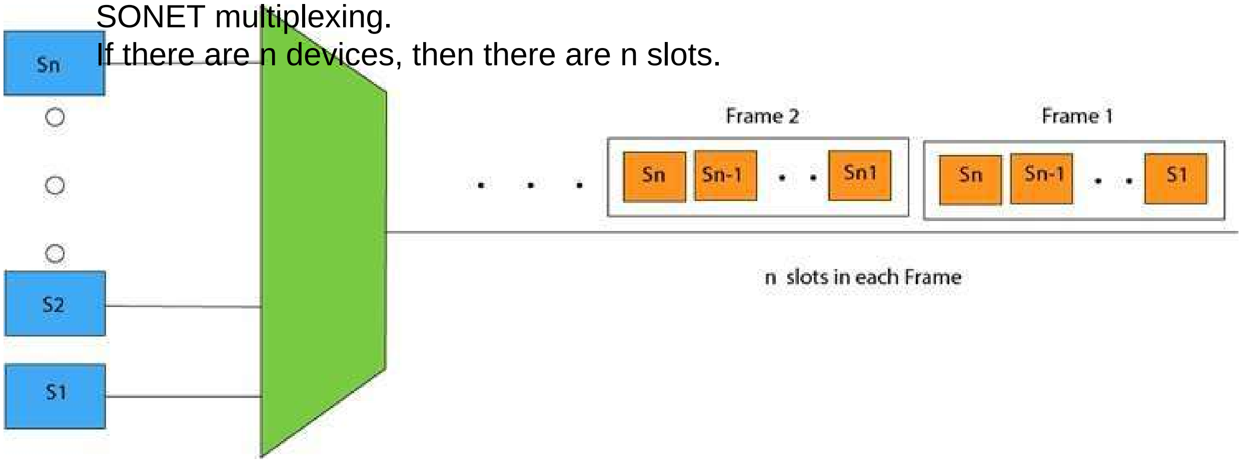
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each frame contains one or more slots dedicated to each user.
- It can be used to multiplex both digital and analog signals but mainly used to multiplex digital signals.

There are two types of TDM:

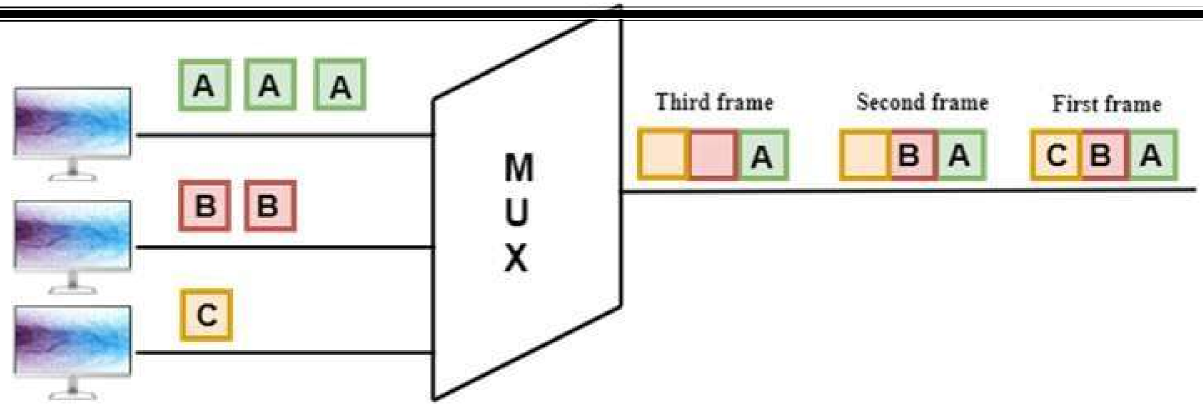
- Synchronous TDM
- Asynchronous TDM

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

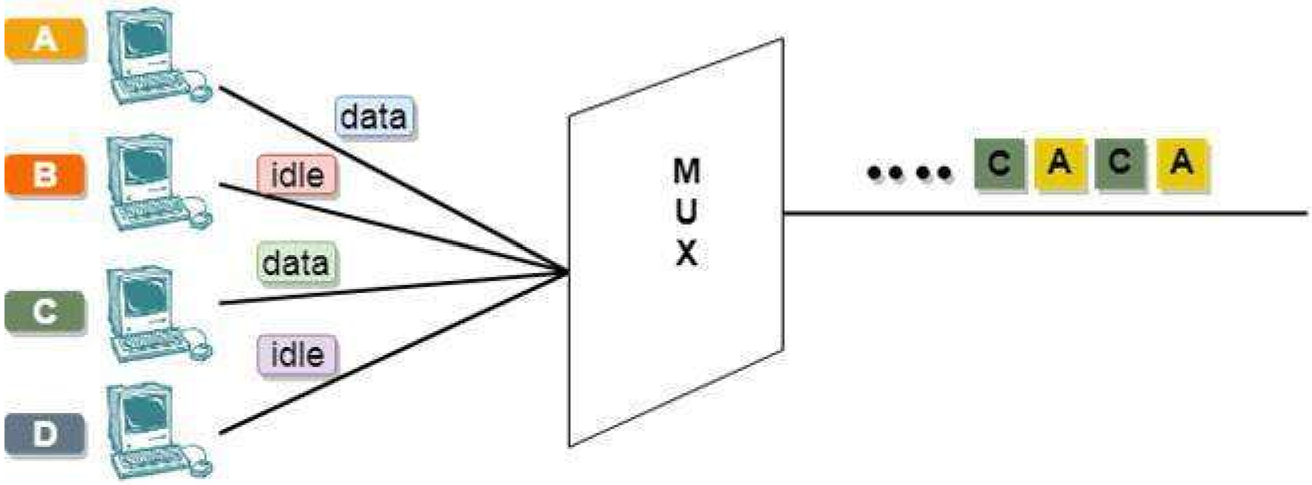
- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor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

ADDRESS
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**).

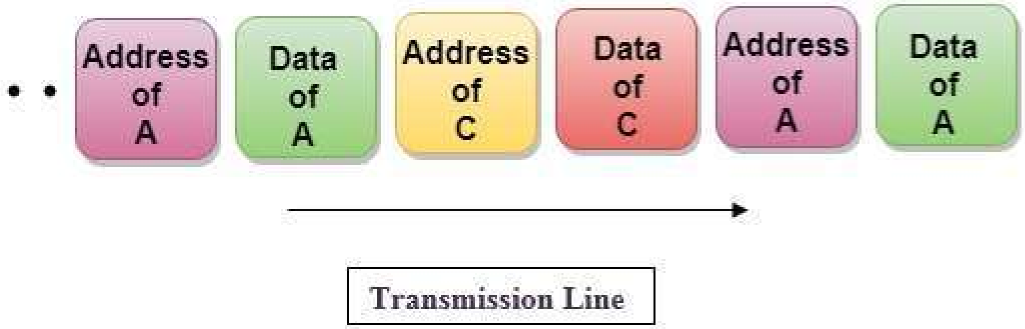
□ The number of slots in a frame depends on the statistical analysis of the number of input lines.

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.

Advantages of Time Division Multiplexing (TDM)

1. Full bandwidth is utilized by a user at a particular time.

2. The time division multiplexing technique is more flexible than frequency division multiplexing.

3. In time division multiplexing, the problem of crosstalk is very less.

Disadvantages of Time Division Multiplexing (TDM)

In time division multiplexing, synchronization is required.

4.9 DIFFERENCE BETWEEN SYNCHRONOUS TDM AND STATISTICAL TDM

Parameter	Synchronous TDM	Statistical TDM
Working	In Synchronous TDM data flow of each input connection is divided into units and each input occupies one output time slot.	In Statistical TDM slots are allotted dynamically. i.e. input line is given slots in output frame if and only if it has data to send.
No. of Slots	In Synchronous TDM no. of slots in each frame are equal to no. of input lines.	In Statistical TDM, No. of slots in each frame are less than the no. of input lines.
Buffers	Buffering is not done, frame is sent after a particular interval of time whether someone has data to send or not.	Buffering is done and only those inputs are given slots in output frame whose buffer contains data to send.
Addressing	Slots in Synchronous TDM carry data only and there is no need of addressing. Synchronization and pre assigned relationships between input and outputs that serve as an address.	Slots in Statistical TDM contain both data and address of the destination.
Synchronization	Synchronization bits are used at the beginning of each frame.	No synchronization bits are used
Capacity	Max. Bandwidth utilization if all inputs have data to send.	The capacity of link is normally is less than the sum of the capacity of each channel.
Data Separation	In Synchronous TDM de-multiplexer at receiving end decomposes each frame, discards framing bits and extracts data unit in turn. This extracted data unit from frame is then passed to destination device.	In Statistical TDM de-multiplexer at receiving end decomposes each frame by checking local address of each data unit. This extracted data unit from frame is then passed to destination device.

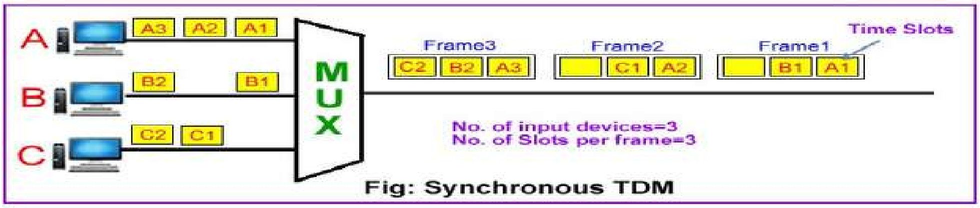


Fig: Synchronous TDM

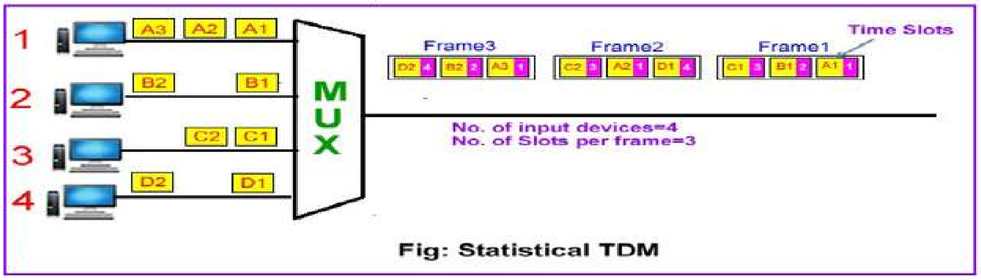


Fig: Statistical TDM

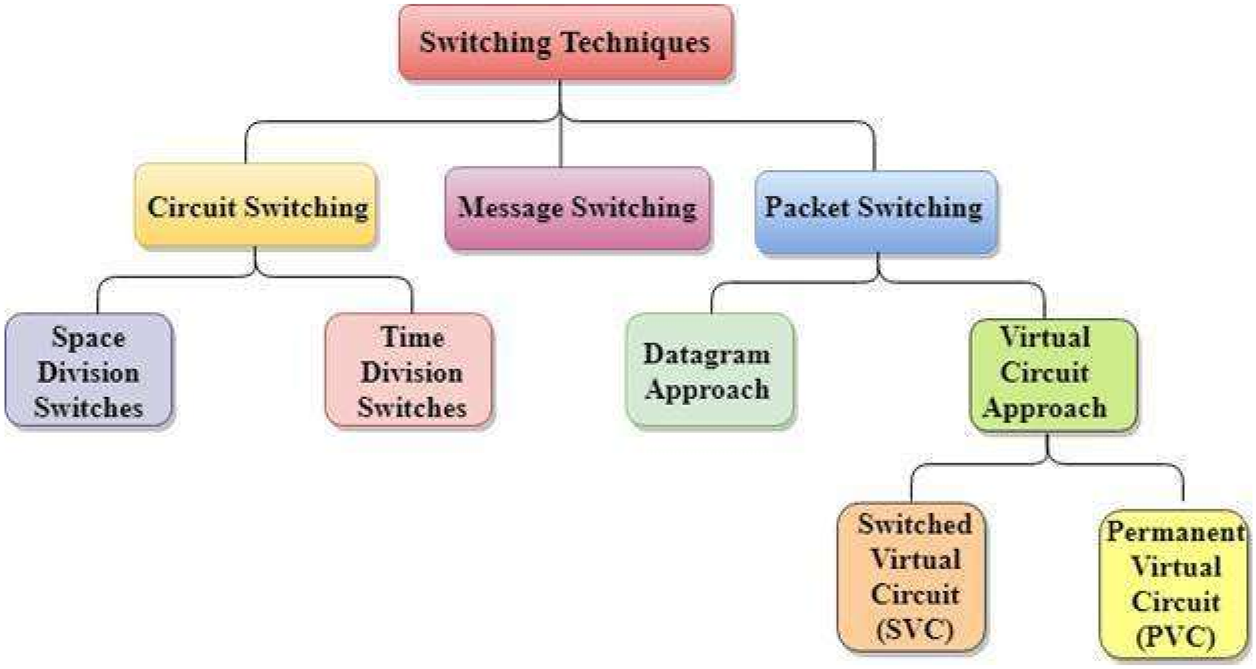
UNIT – 5 SWITCHING & ROUTING

Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

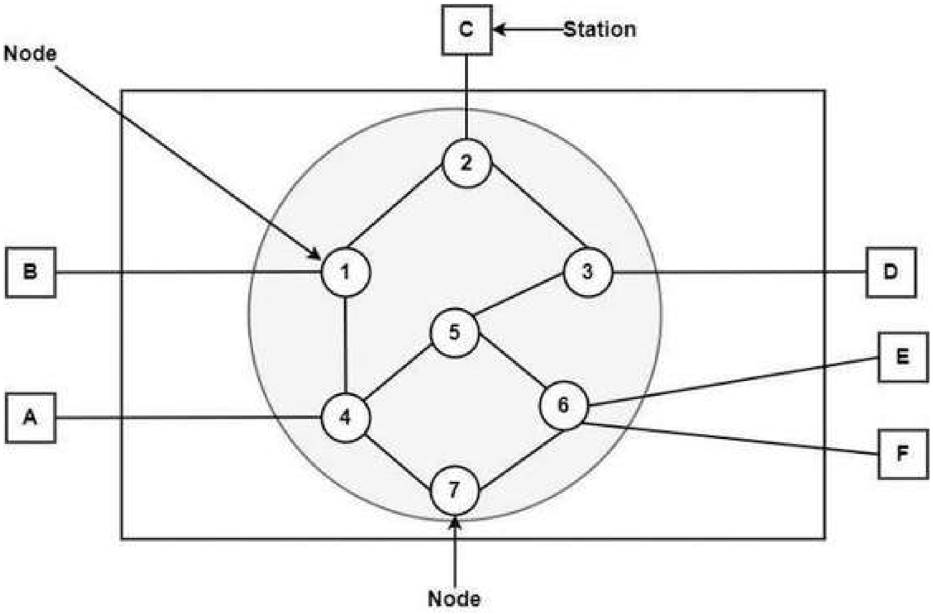
Classification Of Switching Techniques



Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.

- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.



o

Communication through circuit switching has 3 phases:

o Circuit establishment
o Data transfer
o Circuit Disconnect

Circuit Establishment

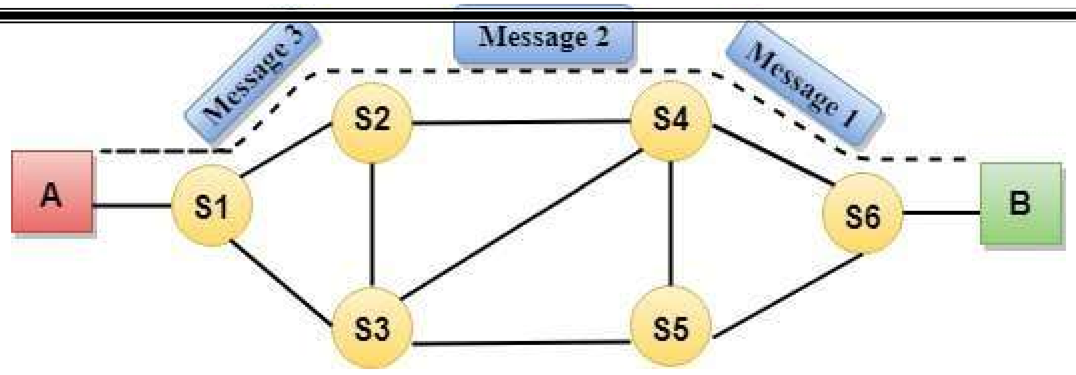
A circuit switching network is necessary to establish an end-to-end link before any signal is transmitted. For example, if the communication is between A and D, then the path from A to node 4 to node 5 to node 3 and D must be established first.

Data Transfer

Once a circuit is established between the two stations, it is exclusively used by the two parties. The information can be transferred from A to D through the network. The data can be analog or digital, relying on the features of the network.

Circuit Disconnect

After the transfer of complete data, the connection is terminated either by the sender or receiver.



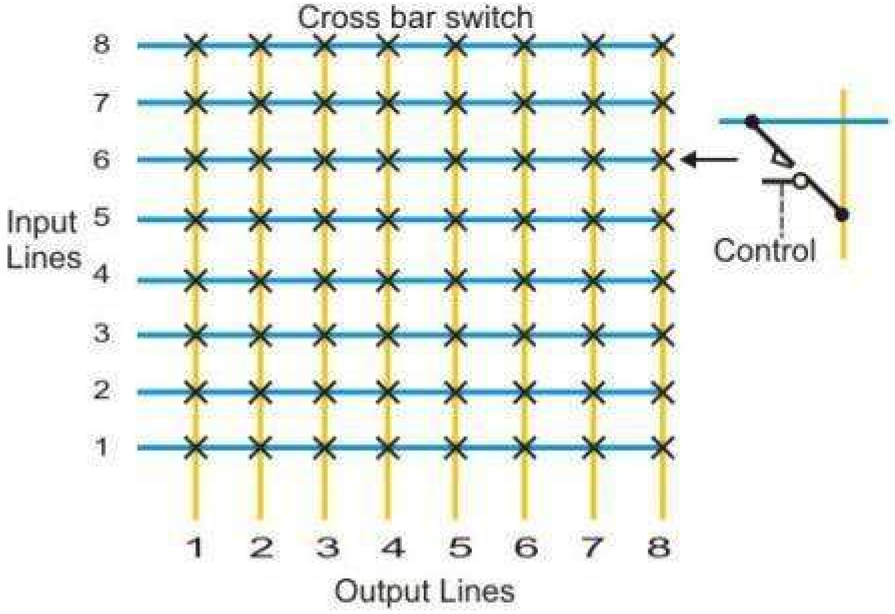
Space Division Switches:

 In space division switching, the paths in the circuit are separated with each other spatially, i.e. different ongoing connections at a same instant of time, uses different switching paths.

 This was originally developed for the analog environment and has been carried over to the digital domain. The space switches are crossbar switches and multi stage switches.

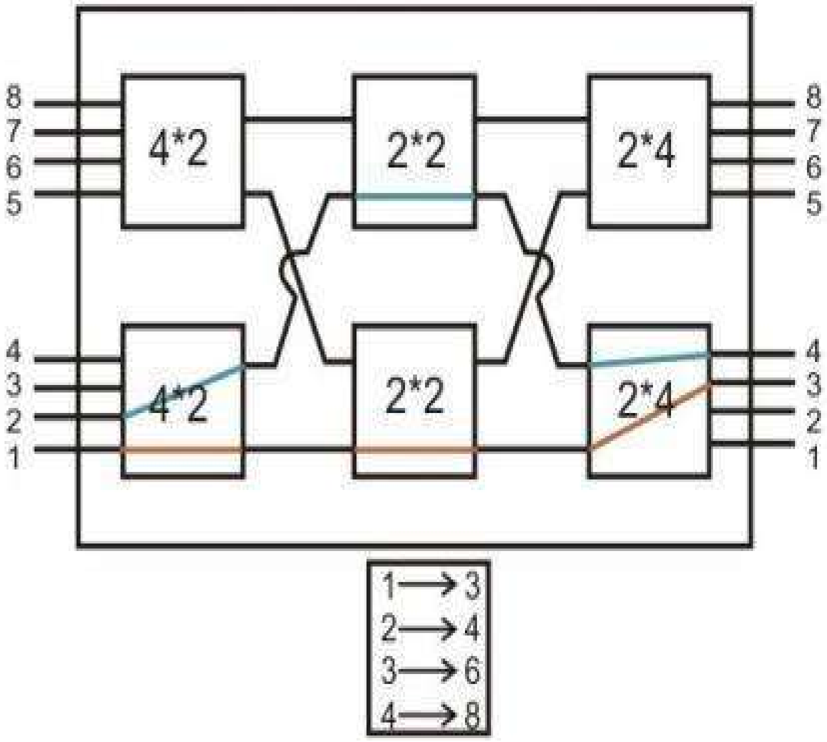
 Crossbar switch-

1. Basic building block of the switch is a metallic cross points or semiconductor gate that can be enabled or disabled by a control unit.
2. The number of cross points grows with the square of the number of attached stations.
3. Costly for a large switch.
4. The failure of a cross point prevents connection between the two devices whose lines intersect at that cross point.
5. The cross points are inefficiently utilized.
6. Only a small fraction of cross points are engaged even if all of the attached devices are active.



□Multistage space division switch-

1. Some of the problem in crossbar switch can be overcome with the help of multistage space division switches.
2. By splitting the crossbar switch into smaller units and interconnecting them it is possible to build multistage switches with fewer cross points.
3. There is more than one path through the network to connect two endpoints, thereby increasing reliability.
4. Multistage switches may lead to blocking.
5. The problem may be tackled by increasing the number or size of the intermediate switches, which also increases the cost.



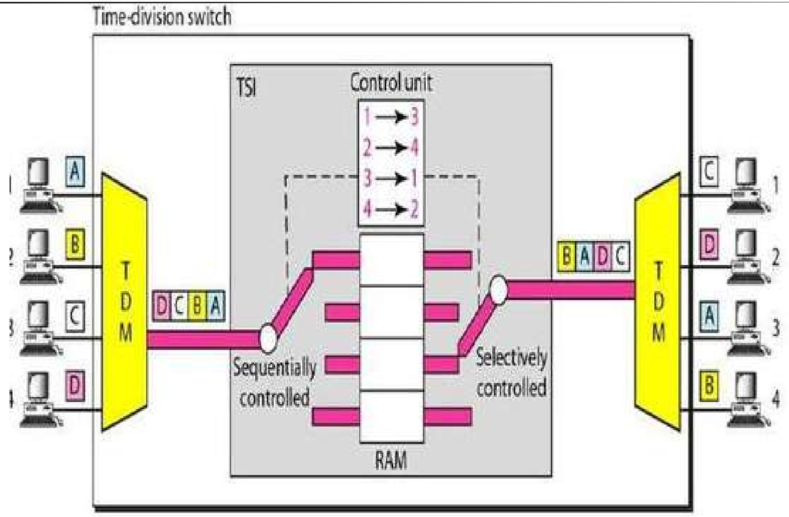
Time Division Switching

Time Division switching uses Time Division Multiplexing (TDM) inside a switch. The most popular technology is called the Time Slot Interchange (TSI).

Time-Division Switch Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the time-slot interchange (TSI).

Time-Slot Interchange shows a system connecting four input lines to four output lines. Imagine that each input line wants to send data to an output line according to the following pattern

1 ➡ 3 2 ➡ 4 3 ➡ 1 4 ➡ 2



The figure combines a TDM multiplexer, a TDM demultiplexer, and a TSI consisting of random access memory (RAM) with several memory locations. The size of each location is the same as the size of a single time slot. The RAM fills up with incoming data from time slots in the order received. Slots are then sent out in an order based on the decisions of a control unit

Advantages Of Circuit Switching:

o In the case of Circuit Switching technique, the communication channel is dedicated.
o It has fixed bandwidth.

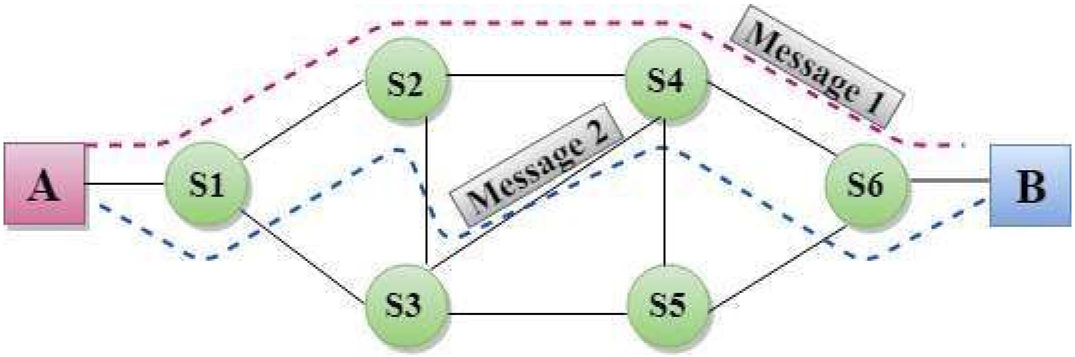
Disadvantages of Circuit Switching:

o Once the dedicated path is established, the only delay occurs in the speed of data transmission.
o It takes a long time to establish a connection approx. 10 seconds during which no data can be transmitted.
o It is more expensive than other switching techniques as a dedicated path is required for each connection.
o It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
o In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.

- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

o Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.

o Traffic congestion can be reduced because the message is temporarily stored in the nodes.

o Message priority can be used to manage the network.

o The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

o The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.

o The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

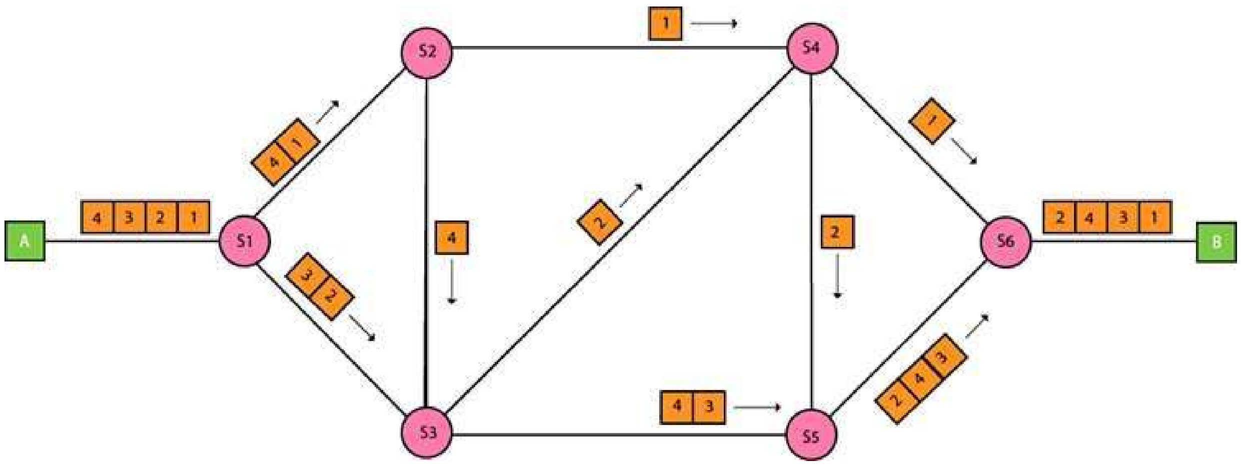
Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.

o All the packets are reassembled at the receiving end in correct order.

o If any packet is missing or corrupted, then the message will be sent to resend the message.

o If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

o It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.

o The packets are reassembled at the receiving end in correct order.

o In Datagram Packet Switching technique, the path is not fixed.

o Intermediate nodes take the routing decisions to forward the packets.

o Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

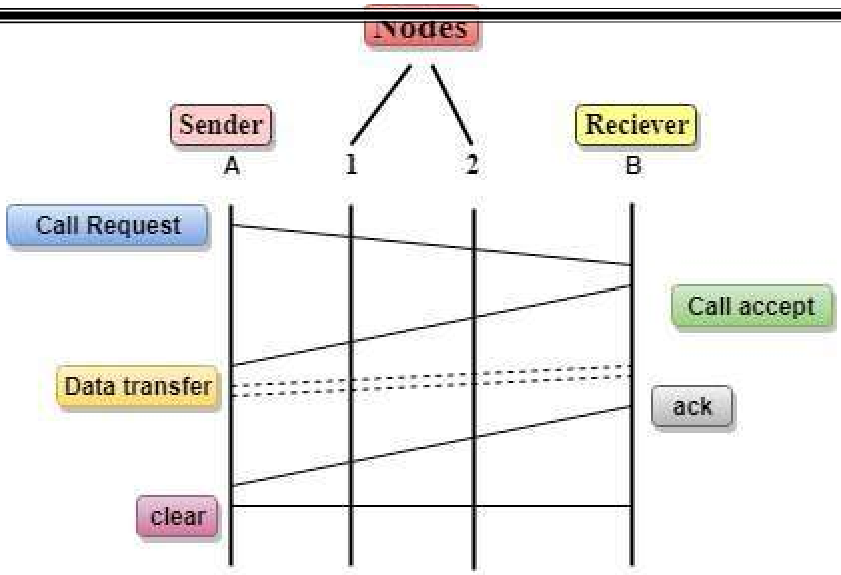
o Virtual Circuit Switching is also known as connection-oriented switching.

o In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.

o Call request and call accept packets are used to establish the connection between sender and receiver.

o In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.
- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	**Virtual Circuit approach**
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

o **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.

o **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.

o **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

o Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

o The protocols used in a packet switching technique are very complex and requires high implementation cost.

o If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.

5.2 DIFFERENCE BETWEEN CIRCUIT SWITCHING AND PACKET SWITCHING

CIRCUIT SWITCHING	PACKET SWITCHING
In circuit switching there are 3 phases i) Connection Establishment. ii) Data Transfer. iii) Connection Released.	In Packet switching directly data transfer takes place.
In circuit switching, each data unit know the entire path address which is provided by the source	In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers.
In Circuit switching, data is processed at source system only	In Packet switching, data is processed at all intermediate node including source system.
Delay between data units in circuit switching is uniform.	Delay between data units in packet switching is not uniform.

Resource reservation is the feature of circuit switching because path is fixed for data transmission.	There is no resource reservation because bandwidth is shared among users.
Circuit switching is more reliable.	Packet switching is less reliable.
Wastage of resources are more in Circuit Switching It is not a store and forward technique.	Less wastage of resources as compared to Circuit Switching It is a store and forward technique.
	Transmission of the data is done not only by the
Transmission of the data is done by the	source, but also by the intermediate routers
source Congestion can occur during connection establishment time, there might be a case will requesting for channel the channel is already occupied.	Congestion can occur during data transfer phase, large number of packets comes in no time

5.3 X.25-

X.25 was a standard suite of protocols used for packet-switched communications over a wide area network — a WAN.

A protocol is an agreed-upon set of procedures and rules.

Two devices that follow the same protocols can understand each other and exchange data.

History of X.25

X.25 was developed in the 1970s to carry voice over analog telephone lines — dial-up networks — and is one of the oldest packet-switched services.

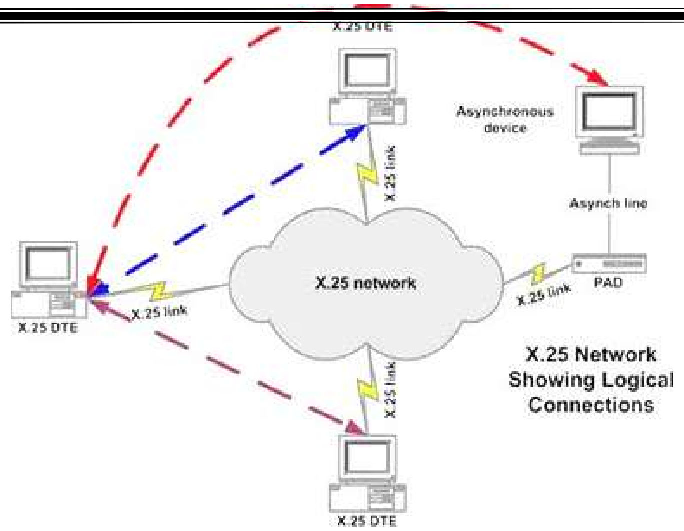
Typical applications of X.25 included automatic teller machine networks and credit card verification networks.

X.25 Structure

An **X.25 network** consists of a network of interconnected nodes to which user equipment can connect.

The user end of the network is known as **Data Terminal Equipment** (**DTE**) and the carrier's equipment is **Data Circuit-terminating Equipment** (**DCE**) .

X.25 routes packets across the network from DTE to DTE.

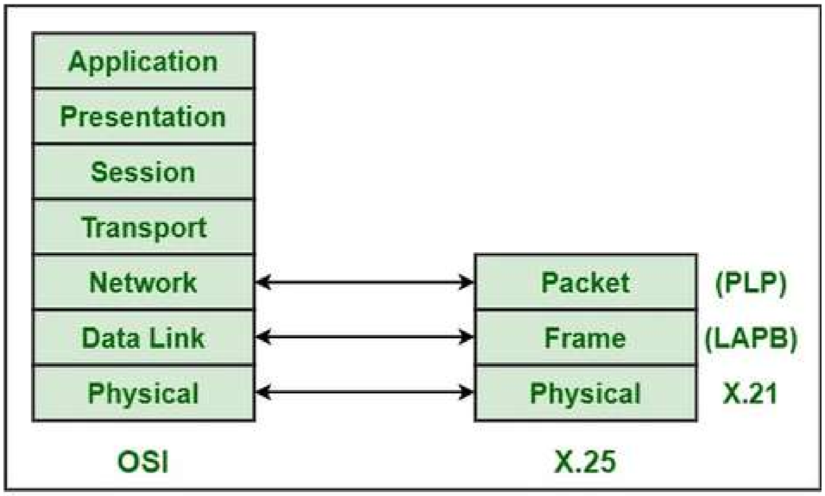


X.25 Network Showing Logical Connections

The protocol known as **X.25** was developed by the organization now known as the International Telecommunications Union (ITU) and encompasses the first three layers of the **OSI 7-layered architecture** as defined by the International Organization for Standardization (ISO) as follows:

- The functionality of X.25 is specified on three levels:

o Physical level
o Link level/frame level
o Packet level



X.25 Layer Mapping with OSI Model

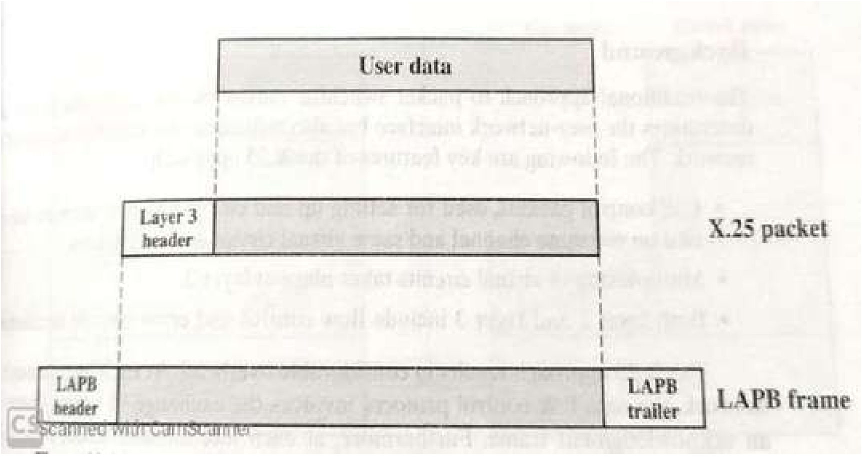
- **Layer 1: The Physical Layer** -The physical level deals with the physical interface between an attached station (computer) and the link that attaches that station to the packet switching node.
- It concerned with electrical or signaling. It includes several electrical standards including V.35 , RS232 and X.21.

- **Layer 2: The Data Link Layer**, The link level provides for the reliable transfer of data across the physical link, by transmitting the data as a sequence of frames.
- which is an implementation of the ISO HDLC standard called Link Access Procedure Balanced (LAPB) and provides an error free link between any two physically connected nodes.
- The Data Link Layer is responsible for error-free communication between any two nodes.
- Thus errors are checked and corrected for each hop all the way across the network.
- It is this feature that makes X.25 so robust, and so suitable for noisy, error-prone links.
- The downside is the latency forced on the system, because each frame has to be received in its entirety and checked before it can be forwarded to the next node.
- The larger the packet size and the lower the line speed the longer the latency period.

- **Layer 3: The Network Layer** that governs the end-to-end communication between the different DTE devices.

The packet level provides a virtual circuit service. This service enables any subscriber to the network to set up logical connections, called virtual circuits to other subscribers.

- The term virtual circuit refers to the logical connection between two stations through the network.
- Layer 3 is concerned with connection set-up and teardown and flow control between the DTE devices, as well as network routing functions and the multiplexing of simultaneous logical connections over a single physical connection.



- The above diagram shows the relationship among the levels of X.25. User data are passed down to X.25 level 3, which appends control information as a header, creating a packet.

 This control information serves several purposes including-

Identifying by number a particular virtual circuit with which this data is to be associated.

Providing sequence numbers that can be used for flow and error control.

 The entire X.25 packet is then passed down to the LAPB entity, which appends control information at the front and back of the packet forming a LAPB frame.

:

X.25 permits a DTE user on an **X.25 network** to communicate with a number of remote DTE's simultaneously. Connections occur on logical channels of two types:

Switched virtual circuits (**SVC**'s) – SVC's are very much like telephone calls; a connection is established, data are transferred and then the connection is released. Each DTE on the network is given a unique DTE address which can be used much like a telephone number.

Permanent virtual circuits (**PVC**'s) – a PVC is similar to a leased line in that the connection is always present. The logical connection is established permanently by the Packet Switched Network administration. Therefore, data may always be sent, without any call setup.

To establish a connection on an SVC, the calling DTE sends a **Call Request** Packet, which includes the address of the remote DTE to be contacted.The destination DTE decides whether or not to accept the call (the Call Request packet includes the sender's DTE address, as well as other information that the called DTE can use to decide whether or not to accept the call).A call is accepted by issuing a **Call Accepted** packet, or cleared by issuing a **Clear Request** packet.Once the originating DTE receives the Call Accepted packet, the virtual circuit is established and data transfer may take place. When either DTE wishes to terminate the call, a **Clear Request** packet is sent to the remote DTE, which responds with a **Clear Confirmation** packet.

Advantages:

1. X.25 is a protocol designed for data transfer over public telephone lines. It was first developed in the 1960s to support host-to-host data transfer over noisy lines.
2. To provide redress for the problems with noisy transmission, X.25 performs extensive error checking and error recovery.
3. In a switching network, X.25 checks packets from each switch. Packets are only forwarded when a positive acknowledgment is received. Thus the X.25 protocol achieves high reliability at the expense of low data transfer speed.

5.4 ROUTING IN PACKET SWITCHING NETWORKS-

Characteristics-

The primary function of a packet-switching network is to accept packets from a source station and deliver them to a destination station. To accomplish this, a path or route through the network must be determined; generally, more than one route is possible. Thus, a routing function must be performed. The requirements for this function include

- Correctness
- Fairness
- Simplicity
- Optimality
- Robustness
- Efficiency
- Stability

The first two items on the list, correctness and simplicity, are self-explanatory. Robustness has to do with the ability of the network to deliver packets via some route in the face of localized failures and overloads. Ideally, the network can react to such contingencies without the loss of packets or the breaking of virtual circuits.

The designer who seeks robustness must cope with the competing requirement for stability. Techniques that react to changing conditions have an unfortunate tendency to either react too slowly to events or to experience unstable swings from one extreme to another. For example, the network may react to congestion in one area by shifting most of the load to a second area.

Now the second area is overloaded and the first is underutilized, causing a second shift. During these shifts, packets may travel in loops through the network. A tradeoff also exists between fairness and optimality. Some performance criteria may give higher priority to the exchange of packets between nearby stations compared to an exchange between distant stations. This policy may maximize average throughput but will appear unfair to the station that primarily needs to communicate with distant stations. Finally, any routing technique involves some processing overhead at each node and often a transmission overhead as well, both of which impair network efficiency. The penalty of such overhead needs to be less than the benefit accrued based on some reasonable metric, such as increased robustness or fairness.

Performance Criteria

The simplest criterion is to choose the minimum-hop route (one that passes through the
□least number of nodes) through the network.
Minimum-hop criterion is least-cost routing.
□The least cost route should provide the highest throughput.
□The least cost route should minimize delay.
□

Decision Time and Place

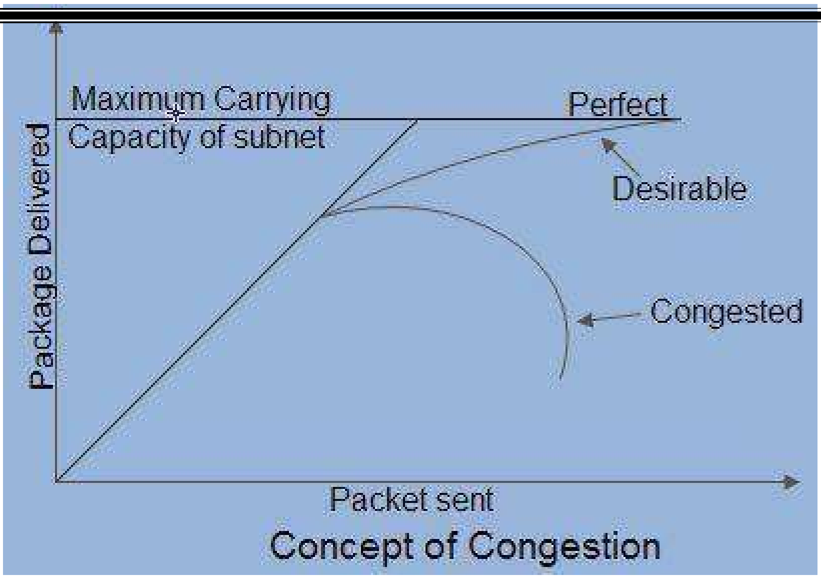
- Routing decisions are made on the basis of some performance criterion. Two key characteristics of the decision are the time and place that the decision is made.
- Decision time is determined by whether the routing decision is made on a packet or virtual circuit basis.
- The term decision place refers to which node or nodes in the network are responsible for the routing decision. Most common is distributed routing, in which each node has the responsibility of selecting an output link for routing packets as they arrive.
- For centralized routing, the decision is made by some designated node, such as a network control center.

5.5 CONGESTION

- Congestion is an important issue that can arise in packet switched network.
- Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades.
- Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.).
- Network congestion occurs in case of traffic overloading.
- In other words when too much traffic is offered, congestion sets in and performance degrades sharply

5.6 EFFECTS OF CONGESTION

- There are two buffers or queues at each port one to accept arriving packets and one to hold packets that are waiting to depart. There might be two fixed size buffers associated with each port.
- As packets arrive they are stored in the input buffer of the corresponding port. The node examines each incoming packet, makes a routing decision and then moves the packet to the appropriate output buffer.
- Packets queued for output are transmitted as rapidly as possible. If packets arrive too fast for the node to process them or faster than packets can be cleared from the outgoing buffers, then eventually packets will arrive for which no memory is available.
- When such a saturation point is reached, one of two strategies can be adopted.
- The first strategy is to discard any incoming packet for which there is no available buffer space.
- The alternative is the node that is experiencing these problems to exercise some sort of flow control over its neighbors so that the traffic flow remains manageable.
- Hence as delay increases performance decreases.

Concept of Congestion

Effects of Congestion

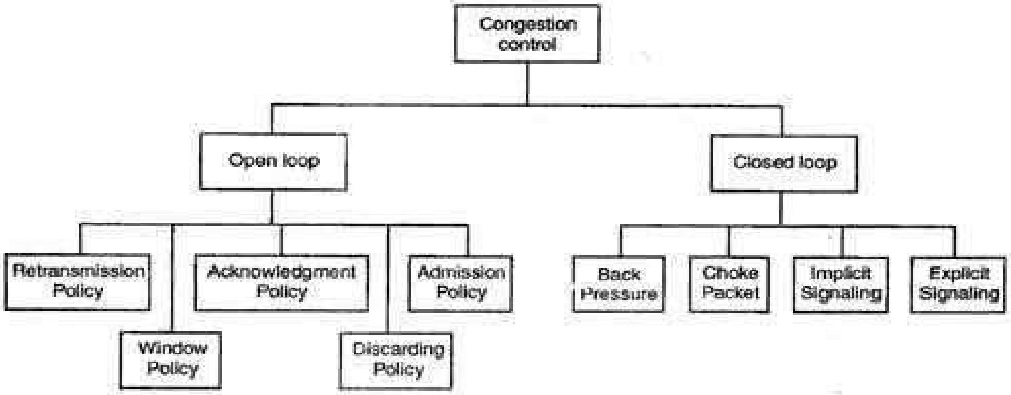
 As delay increases, performance decreases.

 If delay increases, retransmission occurs, making situation worse.

5.8 CONGESTION CONTROL

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

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



Types of Congestion Control Methods

These two categories are: 1. Open loop

2. Closed loop

1. Open Loop Congestion Control

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

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

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

□

Retransmission Policy

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

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

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

□

Window Policy

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

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

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

□

Acknowledgement Policy

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

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

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

□

Discarding Policy

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

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

□

Admission Policy

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

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

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

2. Closed Loop Congestion Control

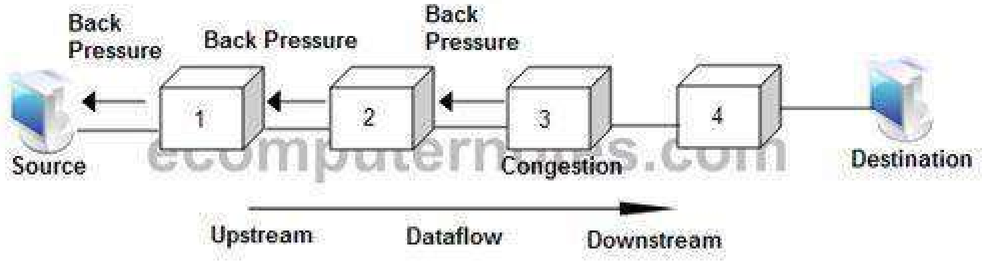
• Closed loop congestion control mechanisms try to remove the congestion after it happens.

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

□

Backpressure

• This technique produces an effect similar to backpressure in fluids flowing down a pipe. When the end of the pipe is closed, the fluid pressure backs up the pipe to the point of origin, where the flow is stopped.



Backpressure Method

• Backpressure can be selectively applied to logical connections, so that the flow from one node to the next is only restricted or halted on some connections, generally the ones with the most traffic.

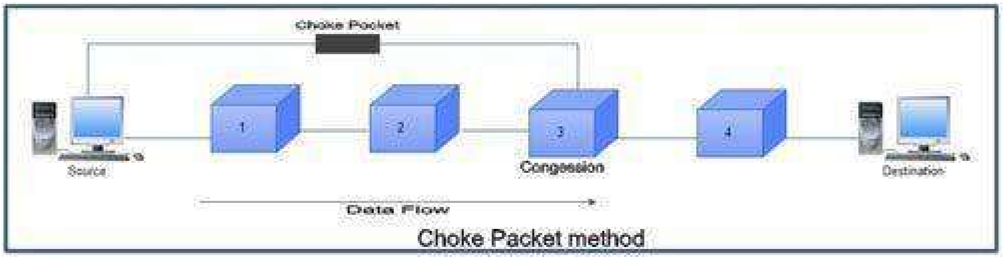
• It can be used in a connection oriented network.

Choke Packet

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

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

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



Choke Packet method

□

Implicit Signaling

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

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

• On sensing this congestion, the source slows down.

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

□

Explicit Signaling

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

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

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

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

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

5.9 TRAFFIC MANAGEMENT-

Congestion control is concerned with efficient use of a network at high load. There are a number of issues related to congestion control that might be included under the general category of traffic management.

1) Fairness

2) Quality of Service
3) Reservations

Fairness-

□ As congestion develops, flows of packets between sources and destinations will experience increased delays and, with high congestion, packet losses.

□ Simply to discard on a last-in-first-discarded basis may not be fair.

□ As an example of a technique that might promote fairness, a node can maintain a separate queue for each logical connection or for each source-destination pair.

□ If all of the queue buffers are of equal length, then the queues with the highest traffic load will suffer discards more often, allowing lower-traffic connections a fair share of the capacity.

Quality of Service-

□ Quality of Service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network.

□ Quality of Service controls and manages network resources by setting priorities for specific types of data on the network.

□ For example, a node might transmit higher-priority packets ahead of lower-priority packets in the same queue.

Reservations-

- One way to avoid congestion and also to provide assured service to applications is to use a reservation scheme. Such a scheme is an integral part of ATM networks.
- When a logical connection is established, the network and the user enter into a traffic contract, which specifies a data rate and other characteristics of the traffic flow.
- The network agrees to give a defined QoS so long as the traffic flow is within contract parameters; excess traffic is either discarded or handled on a best-effort basis, subject to discard.
- If the current outstanding reservations are such that the network resources are inadequate to meet the new reservation, then the new reservation is denied.

5.10 CONGESTION CONTROL IN PACKET SWITCHING NETWORKS-

A number of control mechanisms for congestion control in packet-switching networks have been suggested and tried. The following are examples:

1. Send a control packet from a congested node to some or all source nodes. This choke packet will have the effect of stopping or slowing the rate of transmission from sources and hence limit the total number of packets in the network. This approach requires additional traffic on the network during a period of congestion.
2. Rely on routing information. Routing algorithms, such as ARPANET’s, provide link delay information to other nodes, which influences routing decisions. This information could also be used to influence the rate at which new packets are produced. Because these delays are being influenced by the routing decision, they may vary too rapidly to be used effectively for congestion control.
3. Make use of an end-to-end probe packet. Such a packet could be timestamped to measure the delay between two particular endpoints. This has the disadvantage of adding overhead to the network.
4. Allow packet-switching nodes to add congestion information to packets as they go by. There are two possible approaches here. A node could add such information to packets going in the direction opposite of the congestion. This information quickly reaches the source node, which can reduce the flow of packets into the network. Alternatively, a node could add such information to packets going in the same direction as the congestion. The destination either asks the source to adjust the load or returns the signal back to the source in the packets (or acknowledgments) going in the reverse direction.

UNIT – 6 LAN TECHNOLOGY

6.1 TOPOLOGY AND TRANSMISSION MEDIA-

The key elements of a LAN are

- Topology
- Transmission medium
- Wiring layout
- Medium access control

These elements determine not only the cost and capacity of the LAN, but also the type of data that may be transmitted, the speed and efficiency of communications and even the kinds of applications that can be supported.

Choice of Topology

The choice of topology depends on a variety of factors, including reliability, expandability and performance.

This choice is part of the overall task of designing a LAN and thus cannot be made in isolation, independent of the choice of transmission medium. There are four alternative media that can be used for a bus LAN.

- **Twisted pair**: In the early days of LAN development, voice-grade twisted pair was used to provide an inexpensive, easily installed bus LAN.
- **Baseband coaxial cable**: A baseband coaxial cable is one that makes use of digital signaling. The original Ethernet scheme makes use of baseband coaxial cable.
- **Broadband coaxial cable**: Broadband coaxial cable is the type of cable used in cable television systems. Analog signaling is used at radio and television frequencies. This type of system is more expensive and more difficult to install and maintain than baseband coaxial cable.

- **Optical fiber**: There has been considerable research relating to this alternative over the years, but the expense of the optical fiber taps.

Thus, for a bus topology, only baseband coaxial cable has achieved widespread use, primarily for Ethernet systems. Compared to a star-topology twisted pair or optical fiber installation, the bus topology using baseband coaxial cable is difficult to work with.

Very-high-speed links over considerable distances can be used for the ring topology. Hence, the ring has the potential of providing the best throughput of any topology.

Choice of Transmission Medium

The choice of transmission medium is determined by a number of factors. It is, we shall see, constrained by the topology of the LAN. Other factors come into play, including

- Capacity: to support the expected network traffic
- Reliability: to meet requirements for availability
- Types of data supported: tailored to the application
- Environmental scope: to provide service over the range of environments required

Office buildings are wired to meet the anticipated telephone system demand plus a healthy margin; thus, there are no cable installation costs in the use of Category 3 UTP.

Category 5 UTP supports high data rates for a small number of devices, but larger installations can be supported by the use of the star topology and the interconnection of the switching elements in multiple star-topology configurations.

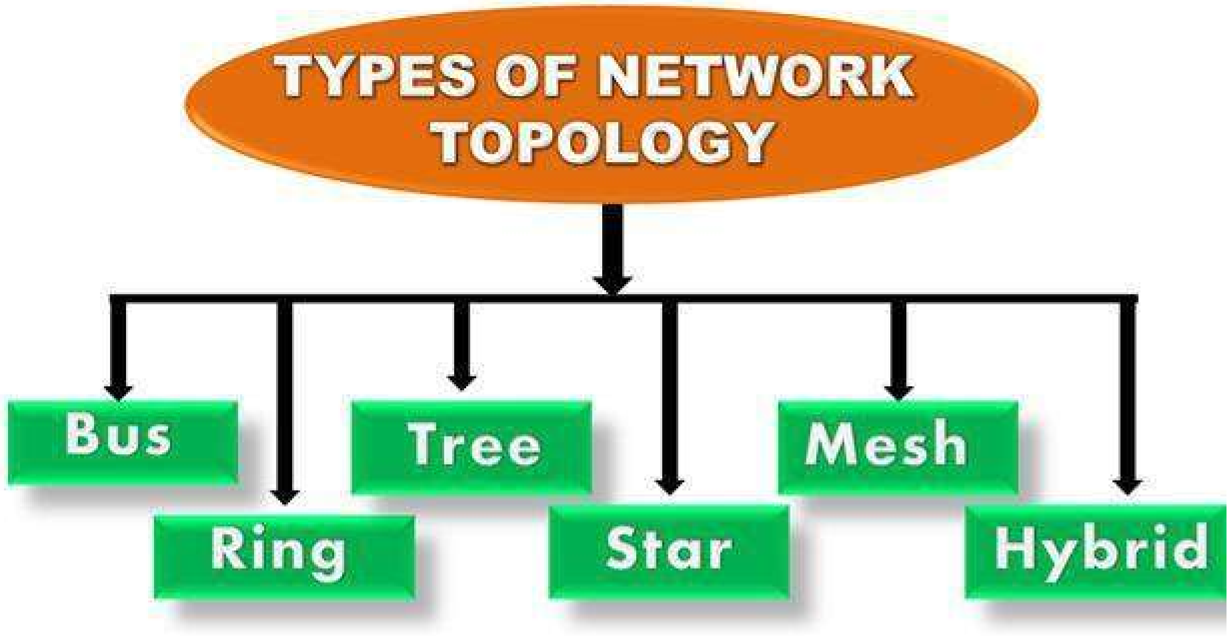
Optical fiber has a number of attractive features, such as electromagnetic isolation, high capacity, and small size, which have attracted a great deal of interest.

Topology

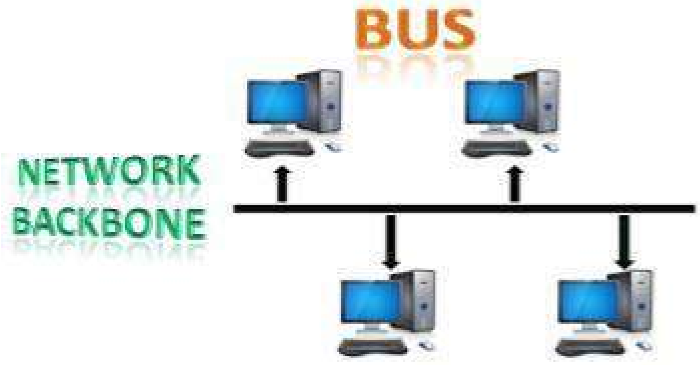
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

 The physical topology refers that, how a network is placed in a physical way and it will include the devices, installation and location.

 Logical topology refers that how a data transfers in a network as opposed to its design.



Bus Topology



- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

CSMA: It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA:CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

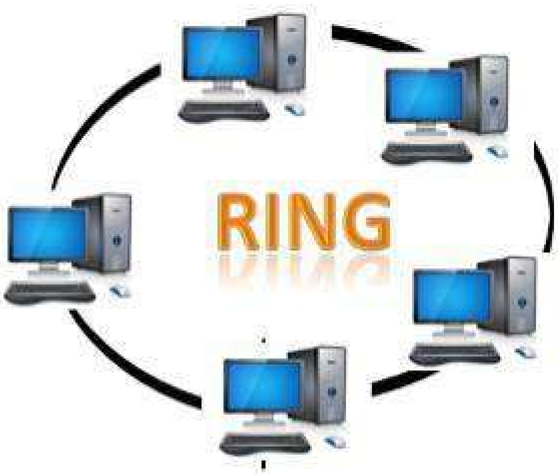
Advantages of Bus topology:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages of Bus topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology



- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The most common access method of the ring topology is **token passing**.
  o **Token passing:** It is a network access method in which token is passed from one node to another node.
  o **Token:** It is a frame that circulates around the network.

Working of Token passing

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

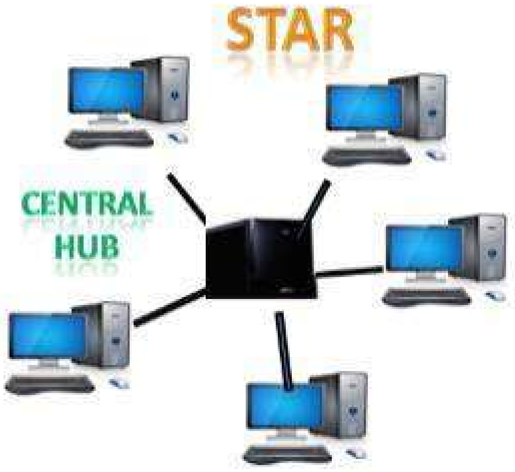
Advantages of Ring topology:

- It performs better than star topology under heavy work load
- For managing the connection between the computers, there is no need for the network server
- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology



- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

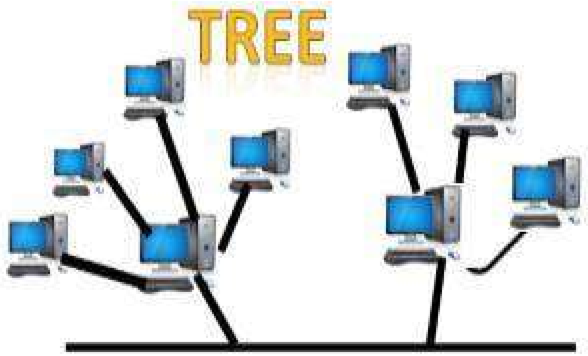
Advantages of Star topology

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star topology

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree topology



- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion..
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

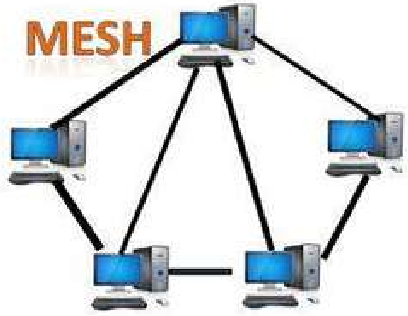
Advantages of Tree topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.

Disadvantages of Tree topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh topology



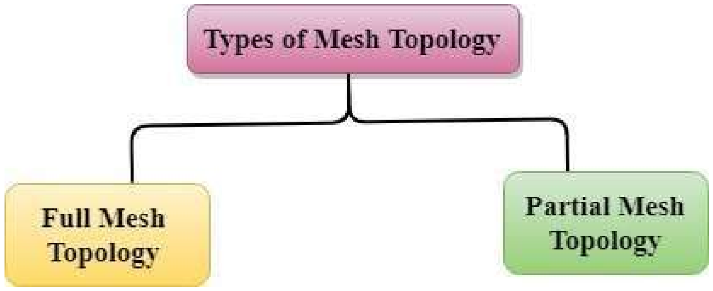
- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula:

Number of cables = (n*(n-1))/2;

Where n is the number of nodes that represents the network.

Mesh topology is divided into two categories:

- Fully connected mesh topology
- Partially connected mesh topology



- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

Advantages of Mesh topology:

Reliable: The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

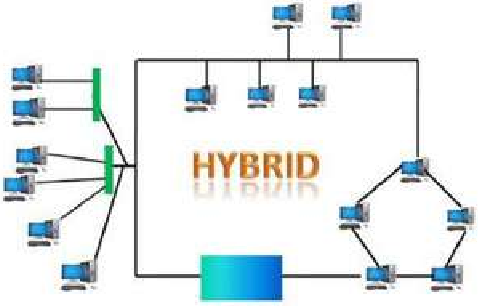
Fast Communication: Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices.

Disadvantages of Mesh topology

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology



- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

Disadvantages of Hybrid topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

6.2 LAN PROTOCOL ARCHITECTURE-

IEEE 802 Reference Model Protocols defined specifically for LAN and MAN transmission address issues relating to the transmission of blocks of data over the network. In OSI terms, higher layer protocols (layer 3 or 4 and above) are independent of network architecture and are applicable to LANs, MANs and WANs.

This architecture was developed by the IEEE 802 LAN standards committee2 and has been adopted by all organizations working on the specification of LAN standards. It is generally referred to as the IEEE 802 reference model. Working from the bottom up, the lowest layer of the IEEE 802 reference model corresponds to the physical layer of the OSI model and includes such functions as

• Encoding/decoding of signals

• Preamble generation/removal (for synchronization)

• Bit transmission/reception

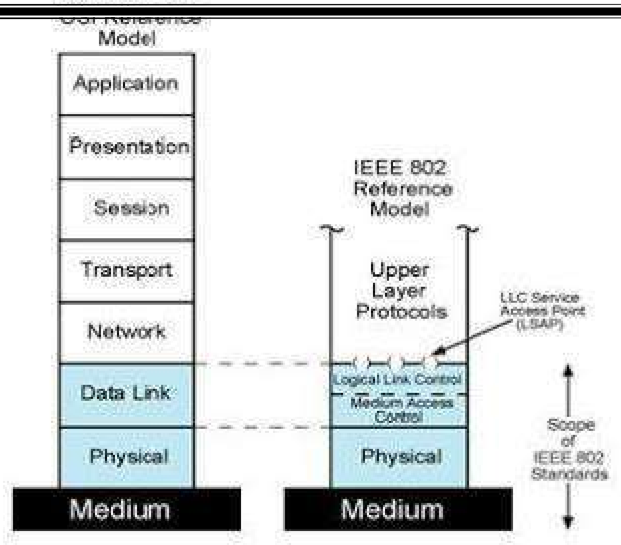
The physical layer of the 802 model includes a specification of the transmission medium and the topology. Above the physical layer are the functions associated with providing service to LAN users. These include

• On transmission, assemble data into a frame with address and error detection fields.

• On reception, disassemble frame, and perform address recognition and error detection.

• Govern access to the LAN transmission medium.

• Provide an interface to higher layers and perform flow and error control.



These are functions typically associated with OSI layer 2.The set of functions in the last bullet item are grouped into a logical link control (LLC) layer. The functions in the first three bullet items are treated as a separate layer, called medium access control (MAC).

Higher-level data are passed down to LLC, which appends control information as a header, creating an LLC protocol data unit (PDU).This control information is used in the operation of the LLC protocol. The entire LLC PDU is then passed down to the MAC layer, which appends control information at the front and back of the packet, forming a MAC frame.

Medium Access Control& Logical Link Control:

The OSI layer 2 (data link) is divided into two in LAN.

1) Medium Access Control (MAC): It performs assembling of data into frames with address and error detection field (for transmission), and disassembling of frame (on reception), MAC layer receives data from LLC layer and perform the error detection and address recognition.

2) Logical Link Control (LLC):

 LLC has two characteristics-

1) It must support the multi-access, shared medium nature of the link.

2) It is relieved of some details of link access by the MAC layer.

 LLC provide services-

1) Unacknowledged connectionless service- This service is a datagram style service. It is a very simple service that does not involve any of the flow and error control mechanisms.

2) Connection mode service- A logical connection is set up between two users exchanging data and flow control and error control are provided.

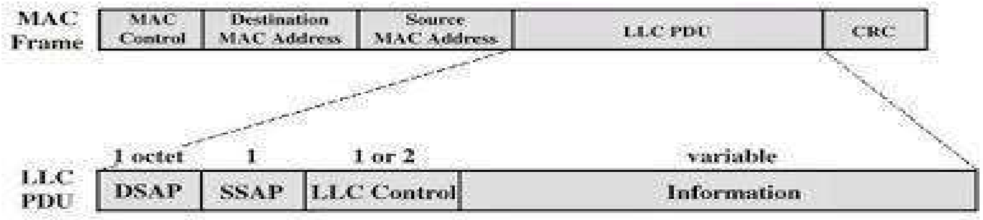
3) Acknowledged connectionless service- This is a cross between the previous two services. It provides that datagrams are to be acknowledged but no prior logical connection is set up.

 LLC Protocol-

1) LLC protocol PDU format consists of four fields. The DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) fields each contain a 7 bit address which specify the destination and source users of LLC.

2) One bit of the DSAP indicates whether the DSAP is an individual or group address.

3) One bit of the SSAP indicates whether the PDU is a command or response PDU. The rest two fields are control field and information field.



6.3 MEDIUM ACCESS CONTROL

 All LANs and MANs consist of collections of devices that must share the network’s transmission capacity. Some means of controlling access to the transmission medium is needed to provide for an orderly and efficient use of that capacity.

 This is the function of a medium access control (MAC) protocol. The key parameters in any medium access control technique are where and how. Where refers to whether control is exercised in a centralized or distributed fashion.

 In a centralized scheme, a controller is designated that has the authority to grant access to the network. A station wishing to transmit must wait until it receives permission from the controller.

 In a decentralized network, the stations collectively perform a medium access control function to determine dynamically the order in which stations transmit. A centralized scheme has certain advantages, including

1. It may afford greater control over access for providing such things as priorities, overrides and guaranteed capacity.
2. It enables the use of relatively simple access logic at each station.
3. It avoids problems of distributed coordination among peer entities.

 The principal disadvantages of centralized schemes are

1. It creates a single point of failure; that is, there is a point in the network that, if it fails, causes the entire network to fail.
2. It may act as a bottleneck, reducing performance.

□ The second parameter, **how**, is constrained by the topology and is a tradeoff among competing factors, including cost, performance, and complexity.

□ In general, we can categorize access control techniques as being either synchronous or asynchronous. With synchronous techniques, a specific capacity is dedicated to a connection. This is the same approach used in circuit switching, frequency division multiplexing (FDM), and synchronous time division multiplexing (TDM). Such techniques are generally not optimal in LANs and MANs because the needs of the stations are unpredictable.

□ It is preferable to be able to allocate capacity in an asynchronous (dynamic) fashion, more or less in response to immediate demand. The asynchronous approach can be further subdivided into three categories: round robin, reservation and contention.

1. Round Robin

□ With round robin, each station in turn is given the opportunity to transmit. During that opportunity, the station may decline to transmit

□ When many stations have data to transmit over an extended period of time, round-robin techniques can be very efficient.

□ If only a few stations have data to transmit over an extended period of time, then there is a considerable overhead in passing the turn from station to station, because most of the stations will not transmit but simply pass their turns.

2. Reservation

For stream traffic, reservation techniques are well suited. In general, for these techniques, time on the medium is divided into slots, much as with synchronous TDM.A station wishing to transmit reserves future slots for an extended or even an indefinite period. Again, reservations may be made in a centralized or distributed fashion.

3. Contention

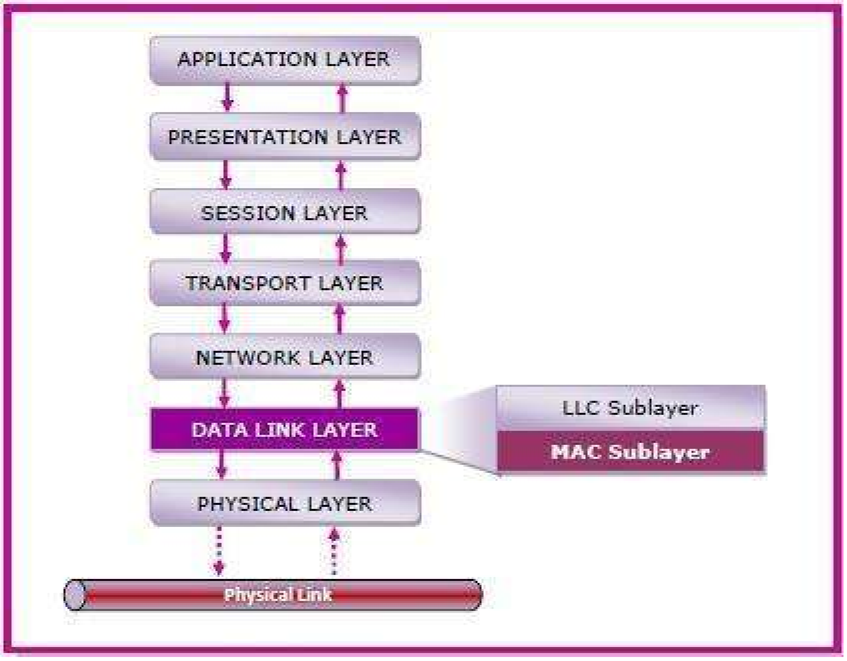
For bursty traffic, contention techniques are usually appropriate. With these techniques, no control is exercised to determine whose turn it is; all stations contend for time.

MAC Frame Format

The MAC layer receives a block of data from the LLC layer and is responsible for performing functions related to medium access and for transmitting the data. As with other protocol layers, MAC implements these functions making use of a protocol data unit at its layer. In this case, the PDU is referred to as a MAC frame.

The fields of this frame are

- **MAC Control:** This field contains any protocol control information needed for the functioning of the MAC protocol. For example, a priority level could be indicated here.
- **Destination MAC Address:** The destination physical attachment point on the LAN for this frame.
- **Source MAC Address:** The source physical attachment point on the LAN for this frame.
- **LLC**: The LLC data from the next higher layer.
- **CRC:** The Cyclic Redundancy Check field (also known as the frame check sequence, FCS, field). This is an error-detecting code.



6.4 Network Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

□ **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

□ **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

6.4 BRIDGES-

The bridge is designed for use between local area networks (LANs) that use identical protocols for the physical and link layers (e.g., all conforming to IEEE 802.3). Because the devices all use the same protocols, the amount of processing required at the bridge is minimal. More sophisticated bridges are capable of mapping from one MAC format to another (e.g., to interconnect an Ethernet and a token ring LAN). Depending on circumstance, there are several reasons for the use of multiple LANs connected by bridges:

• **Reliability:**

The danger in connecting all data processing devices in an organization to one network is that a fault on the network may disable communication for all devices. By using bridges, the network can be partitioned into self-contained units.

• **Performance:**

Performance on a LAN declines with an increase in the number of devices or the length of the wire. A number of smaller LANs will often give improved performance if devices can be clustered so that intra network traffic significantly exceeds internetwork traffic.

• **Security:**

The establishment of multiple LANs may improve security of communications. It is desirable to keep different types of traffic (e.g., accounting, personnel, strategic planning) that have different security needs on physically separate media.

• **Geography:**

Two separate LANs are needed to support devices clustered in two geographically distant locations. Even in the case of two buildings separated by a highway, it may be far easier to use a microwave bridge link than to attempt to string coaxial cable between the two buildings.

SWITCHES-

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

Two types of layer 2 switches are available as commercial products:

- **Store-and-forward switch**: The layer 2 switch accepts a frame on an input line, buffers it briefly, and then routes it to the appropriate output line.
- **Cut-through switch:** The layer 2 switch takes advantage of the fact that the destination address appears at the beginning of the MAC (medium access control) frame. The layer 2 switch begins repeating the incoming frame onto the appropriate output line as soon as the layer 2 switch recognizes the destination address.

The cut-through switch yields the highest possible throughput but at some risk of propagating bad frames, because the switch is not able to check the CRC prior to retransmission. The store-and-forward switch involves a delay between sender and receiver but boosts the overall integrity of the network. A layer 2 switch can be viewed as a full-duplex version of the hub. It can also incorporate logic that allows it to function as a multiport bridge. Lists the following differences between layer 2 switches and bridges:

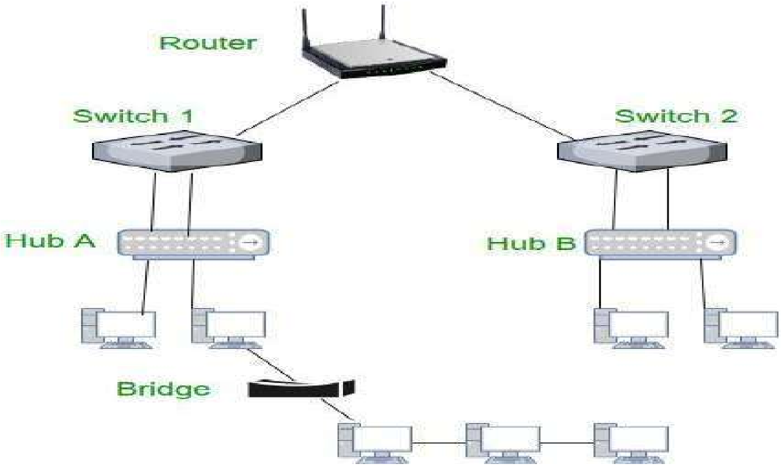
- Bridge frame handling is done in software. A layer 2 switch performs the address recognition and frame forwarding functions in hardware.
- A bridge can typically only analyze and forward one frame at a time, whereas a layer 2 switch has multiple parallel data paths and can handle multiple frames at a time.
- A bridge uses store-and-forward operation. With a layer 2 switch, it is possible to have cut-through instead of store-and-forward operation.

Because a layer 2 switch has higher performance and can incorporate the functions of a bridge, the bridge has suffered commercially. New installations typically include layer 2 switches with bridge functionality rather than bridges.

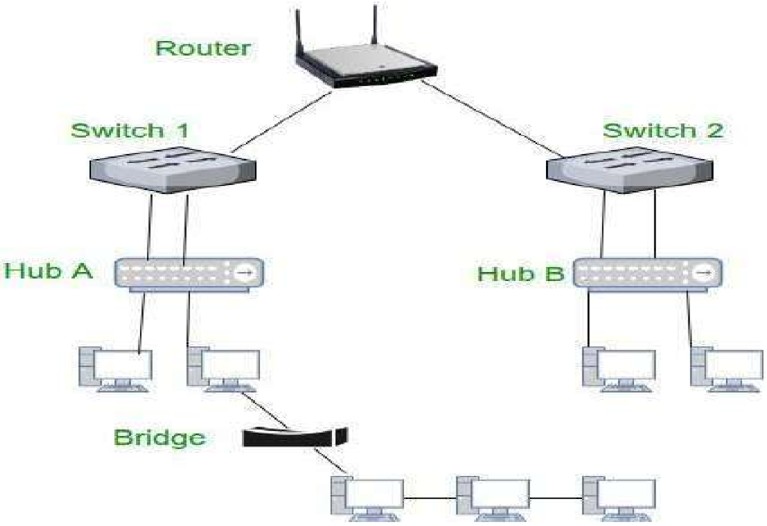
Layer 2 switches provide increased performance to meet the needs of high-volume traffic generated by personal computers, workstations and servers.

However, as the number of devices in a building or complex of buildings grows, layer 2 switches reveal some inadequacies. Two problems in particular present themselves: broadcast overload and the lack of multiple links.

To overcome these problems, it seems logical to break up a large local network into a number of subnetworks connected by routers (Layer3 Switch). A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

Ethernet :-

- □ Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- □ The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of topologies which are allowed.
- □ Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- □ For Ethernet, the protocol data unit is Frame.
- □ In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

Types of Ethernet Networks

□ There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switch Ethernet. A network is a group of two or more computer systems connected together.

1. Fast Ethernet

□

The fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps using a twisted-pair cable or a fiber-optic cable.

□

The older 10 Mbps Ethernet is still used, but such networks do not provide necessary bandwidth for some network-based video applications.

□

Fast Ethernet is based on the proven CSMA/CD Media Access Control (MAC) protocol, and uses existing 10BaseT cabling.

□

Data can move from 10 Mbps to 100 Mbps without any protocol translation or changes to the application and networking software.

2. Gigabit Ethernet

□

The Gigabit Ethernet is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps based on a twisted-pair or fiber optic cable, and it is very popular.

- The 10 Gigabit Ethernet is a latest generation Ethernet capable of transferring data at a rate of 10 Gbps using twisted-pair or fiber optic cable.

3. Switch Ethernet

- Multiple network devices in a LAN require network equipments such as a network switch or hub.
- When using a network switch, a regular network cable is used instead of a crossover cable.
- The crossover cable consists of a transmission pair at one end and a receiving pair at the other end.
- The main function of a network switch is to forward data from one device to another device on the same network.
- Thus a network switch performs this task efficiently as the data is transferred from one device to another without affecting other devices on the same network.

- .

CSMA (Carrier Sense Multiple Access)

- CSMA Protocols stands for Carrier Sense Multiple Access Protocols.
- CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- Devices attached to the network cable listen (carrier sense) before transmitting.
- If the channel is in use, devices wait before transmitting.
- MA (Multiple Access) indicates that many devices can connect to and share the same network.
- All devices have equal access to use the network when it is clear.

1-Persistant CSMA

1-persistent CSMA is an aggressive version of Carrier Sense Multiple Access (CSMA) protocol that operates in the Medium Access Control (MAC) layer. Using CSMA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

In 1-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for the end of the transmission, and transmits immediately. Since, it sends with a probability 1, the name 1 – persistent CSMA is given.

It is used in CSMA/CD (Carrier Sense Multiple Access with Collision Detection) systems including Ethernet.

Algorithm

The algorithm of 1-persistent CSMA is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits and continually checks until the channel becomes idle.
- If the channel is idle then it transmits the frame immediately, with a probability 1.
- A collision may occur if two or more channels transmit simultaneously. If collision occurs, the station waits for a random period of time and restarts the algorithm all over again.

Advantage of 1-persistent CSMA

It has better throughput than ALOHA protocols.

Disadvantages of 1-persistent CSMA

There are chances of collisions in the following situations:

- Situation 1: Suppose that a station A has transmitted a frame, which has not yet reached another station B due to propagation delay. Station B assumes that the channel is idle and transmits its frame. Thus a collision occurs.
- Situation 2: Suppose that a station A is transmitting while stations B and C are waiting for the transmission to complete. At the instance station A completes transmission, both stations B and C start transmitting simultaneously at the same time. This results is collision.

P-persistent CSMA protocol

P-persistent CSMA is an approach of Carrier Sense Multiple Access (CSMA) protocol that combines the advantages of 1-persistent CMSA and non-persistent CSMA. Using CSMA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

In p-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for the end of the transmission, and then transmits with a probability p. Since, it sends with a probability p, the name p – persistent CSMA is given.

Algorithm

The algorithm of p-persistent CMSA is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is idle then it transmits the frame immediately.
- If the channel is busy, the station waits and continually checks until the channel becomes idle.
- When the channel becomes idle, the station transmits the frame with a probability p.
- With a probability (1 – p), the channel waits for next time slot. If the next time slot is idle, it again transmits with a probability p and waits with a probability (1 – p).
- The station repeats this process until either frame has been transmitted or another station has begun transmitting.
- If another station begins transmitting, the station waits for a random amount of time and restarts the algorithm.

Advantage of p-persistent CSMA

It is the most efficient among 1-persistent CSMA, non-persistent CSMA and p-persistent CSMA. It reduces the number of collisions considerably as compared to 1-persistent CSMA. The channel utilization is much better than non-persistent CSMA.

Comparison of Throughputs

The throughput of a network system is defined as the number of successful transmissions per frame time. The through put of p-persistent CSMA depends upon the value of p. Generally speaking, lower the value of p, greater the throughput. However, with lower values of p, channel utilization also reduces.

Non-persistent CSMA protocol

Non-persistent CSMA is a non – aggressive version of Carrier Sense Multiple Access (CSMA) protocol that operates in the Medium Access Control (MAC) layer. Using CSMA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.

In non-persistent CSMA, when a transmitting station has a frame to send and it senses a busy channel, it waits for a random period of time without sensing the channel in the interim, and repeats the algorithm again.

Algorithm

The algorithm of non-persistent CMSA is

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is idle then it transmits the frame immediately.
- If the channel is busy, the station waits for a random time period during which it does not check whether the channel is idle or busy.
- At the end of the waiting time period, it again checks the status of the channel and restarts the algorithm.

Advantage of non-persistent CSMA

It rate of collisions is much reduced than 1-persistent CMSA. This is because each station waits for a random amount of time before attempting retransmission. The probability that multiple stations will wait for same amount of time is extremely low. So, collision between contending stations is greatly reduced.

Disadvantage of non-persistent CSMA

It reduces the bandwidth usage of network. This is because the channel remains idle even if there are stations who have frames to transmit. This occurs since each station wait for a random time before attempting retransmission. There may be multiple stations who are waiting while the channel is idle.

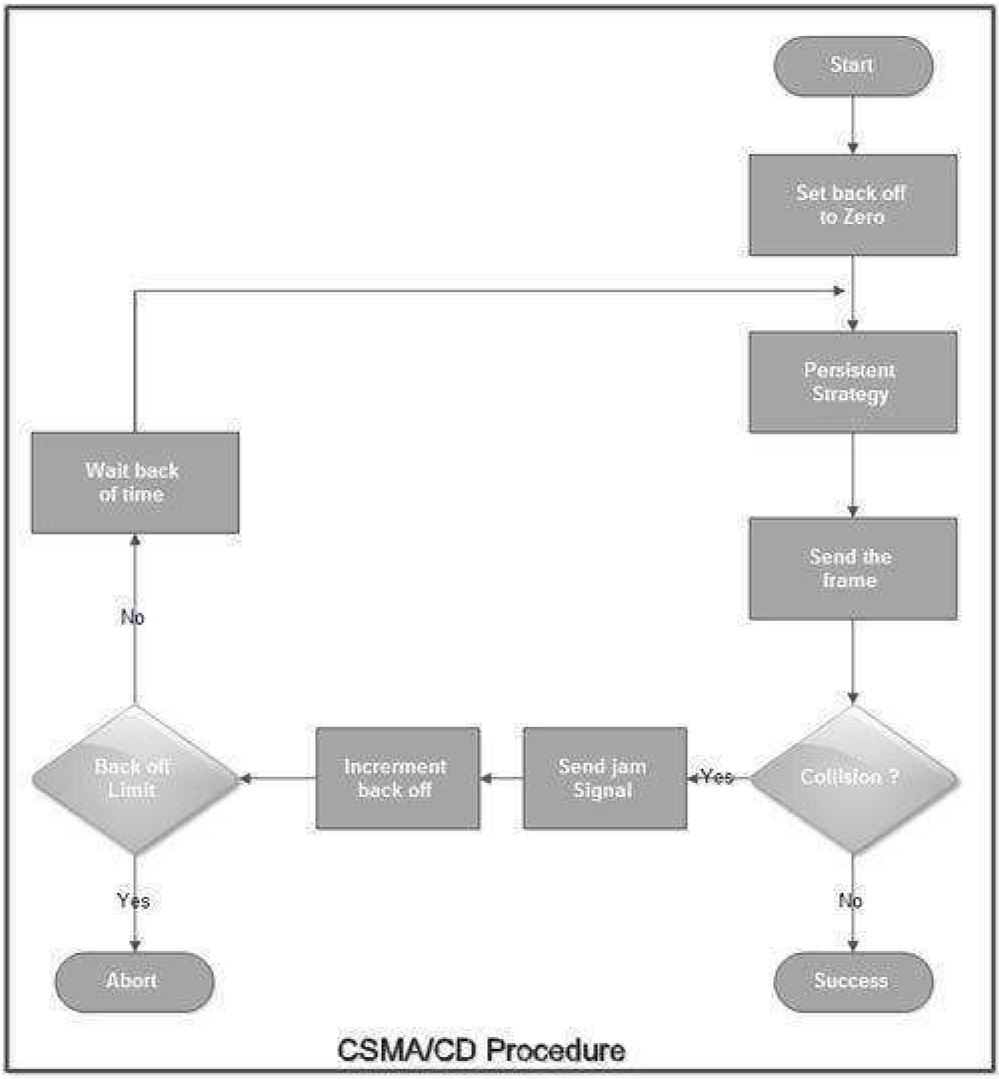
CSMA/ CD

- To reduce the impact of collisions on the network performance, Ethernet uses an algorithm called CSMA with Collision Detection (CSMA / CD).

- CSMA/CD is a protocol in which the station senses the carrier or channel before transmitting frame just as in persistent and non-persistent CSMA.
- If the channel is busy, the station waits. it listens at the same time on communication media to ensure that there is no collision with a packet sent by another station.
- In a collision, the issuer immediately cancel the sending of the package.
- This allows to limit the duration of collisions: we do not waste time to send a packet complete if it detects a collision.
- After a collision, the transmitter waits again silence and again, he continued his hold for a random number; but this time the random number is nearly double the previous one: this is called back-off exponential.
- In fact, the window collision is simply doubled (unless it has already reached a maximum).
- From a packet is transmitted successfully, the window will return to its original size.

CSMA/CD Procedure:

Fig. Shows a flow chart for the *CSMA/CD* protocol.



CSMA/CD Procedure

Explanation:

- The station that has a ready frame sets the back off parameter to zero.
- Then it senses the line using one of the persistent strategies.

- It then sends the frame. If there is no collision for a period corresponding to one complete frame, then the transmission is successful.
- Otherwise the station sends the jam signal to inform the other stations about the collision.
- The station then increments the back off time and waits for a random back off time and sends the frame again.
- If the back off has reached its limit then the station aborts the transmission.
- *CSMA/CD* is used for the traditional Ethernet.
- *CSMA/CD* is an important protocol. IEEE 802.3 (Ethernet) is an example of *CSMNCD.* It is an international standard.
- The MAC sublayer protocol does not guarantee reliable delivery. Even in absence of collision the receiver may not have copied the frame correctly.

Advantages & Disadvantages of CMSA/CD

Advantages	**Disadvantages**
It has low overhead.	Collisions degrade network performance.
Utilizes all available bandwidth when possible.	Priorities cannot be assigned to certain nodes. Performance degrades exponentially as devices are added.

CSMA/ CA

- CSMA/CA protocol is used in wireless networks because they cannot detect the collision so the only solution is collision avoidance.
- CSMA/CA avoids the collisions using three basic techniques.

  (i) Interframe space

  (ii) Contention window

  (iii) Acknowledgements

1. Interframe Space (IFS)

- Whenever the channel is found idle, the station does not transmit immediately. It waits for a period of time called interframe space (IFS).
- When channel is sensed to be idle, it may be possible that same distant station may have already started transmitting and the signal of that distant station has not yet reached other stations.
- Therefore the purpose of IFS time is to allow this transmitted signal to reach other stations.

□ If after this IFS time, the channel is still idle, the station can send, but it still needs to wait a time equal to contention time.

□ IFS variable can also be used to define the priority of a station or a frame.

2. Contention Window

□ Contention window is an amount of time divided into slots.

□ A station that is ready to send chooses a random number of slots as its wait time.

□ The number of slots in the window changes according to the binary exponential back-off strategy. It means that it is set of one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

□ This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.

□ In contention window the station needs to sense the channel after each time slot.

□ If the station finds the channel busy, it does not restart the process. It just stops the timer & restarts it when the channel is sensed as idle.

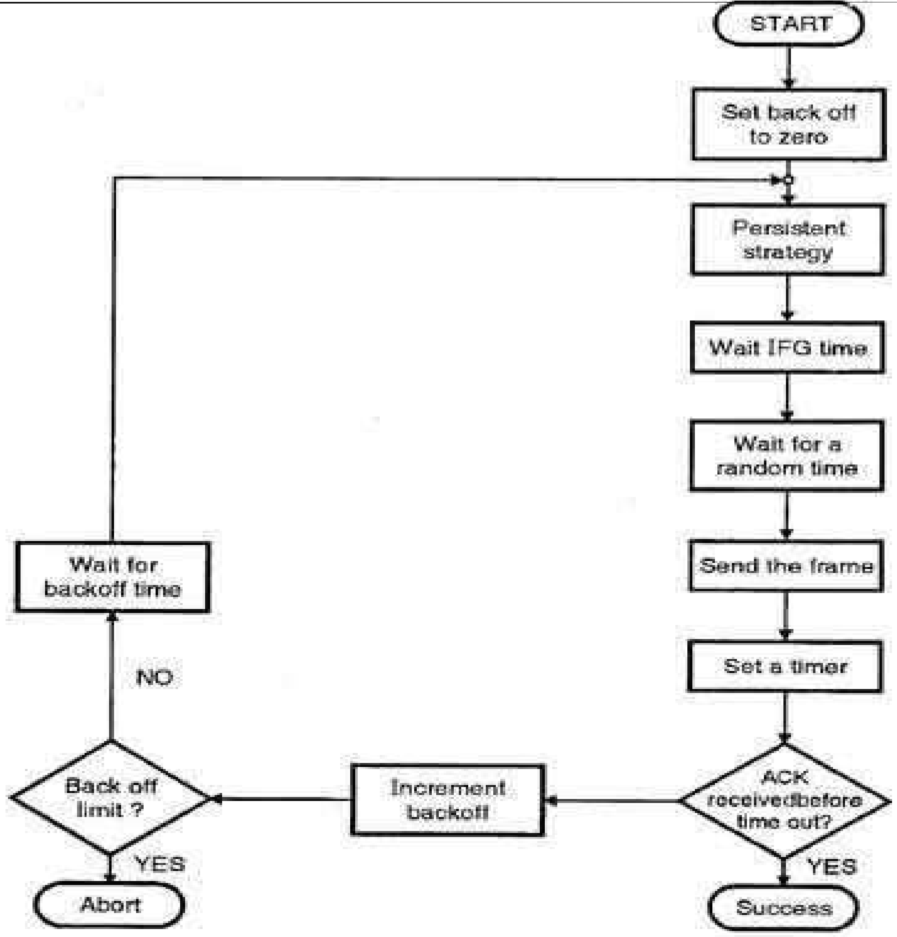
3. Acknowledgement

□ Despite all the precautions, collisions may occur and destroy the data.

□ The positive acknowledgment and the time-out timer can help guarantee that receiver has received the frame.

CSMA/CA Procedure:

Fig. Shows the flow chart explaining the principle of *CSMA/CA.*



CSMA/CA procedure

- This is the CSMA protocol with collision avoidance.
- The station ready to transmit, senses the line by using one of the persistent strategies.
- As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time.
- If then waits for some random time and sends the frame.
- After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.
- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.

Advantages and Disadvantages of CSMA/CA

Advantages	**Disadvantages**

Advantages	**Disadvantages**
Helps prevent data collisions	Longer waiting times
Thanks to feedback, no data is unnoticeably lost	Causes additional traffic
Avoids unnecessary data traffic with the RTS/CTS extension	Solves the hidden station problem only by using RTS/CTS extension
	Creates the exposed station problem through using RTS/CTS

RTS- REQUEST TO SEND

CTS- CLEAR TO SEND

6.9 FIBER CHANNEL-

- Fiber channel is a high speed networking technology primarily used for transmitting data among data centers, computer servers, switches and storage at data rates of upto 128 Gbps.
- Fiber channel suited for connecting servers to shared storage devices and interconnecting storage controllers and drives.
- Fiber channel devices can be as far as 10 Km apart if multimodal optical fiber is used as the physical medium.
- Optical fiber is not required for shorter distances. Fiber channel also works using coaxial cable and ordinary telephone twisted pair.
- The key elements of a fiber channel network are the end systems, called nodes and the network itself, which consists of one or more switching elements.
- The collection of switching elements is referred to as a fabric.
- These elements are interconnected by point to point links between ports on the individual nodes and switches.
- The fiber channel protocol architecture is organized into five levels. Each level defines a function or set of related functions. The layers are as follows-

1) FC-0 Physical Media-It includes optical fiber for long distance applications, coaxial cable for high speeds over short distances and shielded twisted pair for lower speeds over short distances.

2) FC-1 Transmission Protocol- It defines the signal encoding scheme

3) FC-2 Framing Protocol- It deals with defining topologies, frame format, flow and error control and grouping of frames into logical entities called sequences.

4) FC-3 common services- It includes multicasting.

5) FC-4 Mapping- It defines the mapping of various channel and network protocols to fiber channel.

Fiber Channel Elements

The key elements of a Fiber Channel network are the end systems, called nodes, and the network itself, which consists of one or more switching elements. The collection of switching elements is referred to as a fabric. These elements are interconnected by point-to-point links between ports on the individual nodes and switches. Communication consists of the transmission of frames across the point-to-point links.

6.10 WIRELESS LAN TECHNOLOGY-

Wireless LANs are generally categorized according to the transmission technique that is used. All current wireless LAN products fall into one of the following categories:

• Infrared (IR) LANs

• Spread spectrum LANs

Infrared LANs

 Infrared LANs use infrared signals to transmit data. This is same technology used in products like remote controls for televisions and VCRs.
 These LANs can be setup using a point to point configuration is known as Directed-Beam IR.
 An omnidirectional configuration involves a single base station that is within Line of Sight of all other stations on the LAN. This station is mounted on the ceiling. The ceiling transmitter broadcasts an omnidirectional signal that can be received by all of the other IR Tran receivers in the area. These other Trans receivers transmit a directional beam aimed at the ceiling base unit.
 In a diffused configuration, all of the IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling. IR radiation striking the ceiling is reradiated Omni directionally and picked up by all of the receivers in the area.
 Infrared equipment is inexpensive and simple.
 Many indoor environments experience rather intense infrared background radiation, from sunlight and indoor lighting.

Spread Spectrum LANs

 Spread spectrum is currently the most widely used transmission technique for wireless LANs.

 It was initially developed by the military to avoid jamming.

 This is done by spreading the signal over a range of frequencies that consist of the industrial, scientific and medical bands of the electromagnetic spectrum.

 The first type of spread spectrum developed is known as frequency hopping spread spectrum.

 The other type of spread spectrum is called direct sequence spread spectrum.

 Frequency hopping radios currently use less power than direct sequence radios and generally cost less.

While direct sequence data rate of 8

o .

UNIT – 7TCP/IP

UNIT-7: TCP/IP

7.1 TCP/IP PROTOCOL SUITE-

□ The internet protocol suit is the conceptual model and set of communications protocols used in the internet and similar computer networks. It is known as TCP/IP because the foundational protocols in the suite are the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

□ The Internet Protocol suite provides end to end data communication specifying how data should be packetized, addressed, transmitted, routed and received.

□This functionality is organized into four abstraction layers.

□From lowest to highest, the layers are the

□ link layer, containing communication methods for data that remains within a single network segment,

□ the internet layer, providing inter networking between independent networks,

□ the transport layer, handling host to host communication and

□ the application layer, providing process to process data exchange for application.

7.2 BASIC PROTOCOL FUNCTIONS IN TCP/IP

The protocol functions are grouped into the following categories:

- Encapsulation
- Fragmentation and reassembly
- Connection control
- Ordered delivery
- Flow control

- Error control

- Addressing

- Multiplexing

- Transmission services

Encapsulation-

 For virtually all protocols, data are transferred in blocks, called Protocol Data Units (PDU).

 Each PDU contains not only data but also control information. The control information falls into three categories: Address, Error detecting code, protocol control.

The addition of control information to data is referred to as encapsulation.

Fragmentation and Reassembly

 A protocol is concerned with exchanging data between two entities.

 Protocol may need to divide a block received from a higher layer into multiple blocks of some smaller bounded size. This process is called fragmentation.

The counterpart of fragmentation is reassembly. Eventually, the segmented data must be reassembled into messages appropriate to the application level. If PDUs arrive out of order, the task is complicated

Connection Control

 An entity may transmit data to another entity in such a way that each PDU is treated independently of all prior PDUs. This is known as connectionless data transfer, an example is the use of the datagram.

 Connection-oriented data transfer is preferred (even required) if stations anticipate a lengthy exchange of data.

A logical association is established between the entities using three phases.

• Connection establishment

• Data transfer

• Connection termination

Ordered Delivery

 If two communicating entities are in different hosts2connected by a network, there is a risk that PDUs will not arrive in the order in which they were sent, because they may traverse different paths through the network.

 In connection-oriented protocols, it is generally required that PDU order always be maintained.

 If each PDU is given a unique number, and numbers are assigned sequentially, then it is a logically simple task for the receiving entity to reorder received PDUs on the basis of sequence number.

Flow Control

 Flow control is a function performed by a receiving entity to limit the amount or rate of data that is sent by a transmitting entity.

 The simplest form of flow control is a stop-and-wait procedure, in which each PDU must be acknowledged before the next can be sent.

 More efficient protocols involve some form of credit provided to the transmitter, which is the amount of data that can be sent without an acknowledgment. The HDLC sliding-window technique is an example of this mechanism.

Error Control

 Error control techniques are needed to guard against loss or damage of data and control information.

 Error control is implemented as two separate functions:

1) Error detection

2) Retransmission

Addressing

The concept of addressing in a communications architecture is a complex one and covers a number of issues, including

• Addressing level

• Addressing scope

• Connection identifiers

• Addressing mode

 Addressing level refers to the level in the communications architecture at which an entity is named.

 Another issue that relates to the address of an end system or intermediate system is **addressing scope**.

 The concept of **connection identifiers** comes into play when we consider connection-oriented data transfer (e.g., virtual circuit) rather than connectionless data transfer (e.g., datagram).

 For connectionless data transfer, a global identifier is used with each data transmission.

 For connection-oriented transfer, it is sometimes desirable to use only a connection identifier during the data transfer phase.

 Another addressing concept is that of addressing mode. Most commonly, an address refers to a single system or port; in this case it is referred to as an individual or unicast address

 An address for multiple recipients may be broadcast.

Multiplexing-

One form of multiplexing is supported by means of multiple connections into a single system. For example, with frame relay, there can be multiple data link connections terminating in a single end system; we can say that these data link connections are multiplexed over the single physical interface between the end system and the network.

Transmission Services

A protocol may provide a variety of additional services to the entities that use it. We mention here three common examples:

• Priority: Certain messages, such as control messages, may need to get through to the destination entity with minimum delay. An example would be a terminate-connection request. Thus, priority could be assigned on a message basis. Additionally, priority could be assigned on a connection basis.

• Quality of service: Certain classes of data may require a minimum throughput or a maximum delay threshold.

• Security: Security mechanisms, restricting access, may be invoked.

7.3 PRINCIPLE OF INTERNETWORKING-

Internet-

A collection of communication networks interconnected by bridges and routers.

Intranet-

An internet used by a single organization that provides the key internet applications. An internet operates within the organization for internal purposes.

End System-

A device attached to one of the networks of an internet that is used to support end-user applications or services.

Intermediate System (ISs)-

A device used to connect two networks and permit communication between end systems attached to different networks. Two types of ISs are bridges and routers.

Bridges-

A bridges at layer 2 of the Open System Interconnection (OSI). An IS used to connect two LANs that use similar LAN protocols.

Routers-

A router operates at layer 3 of the OSI architecture and routes packets between potentially different networks.

Requirements

The overall requirements for an internetworking facility are as follows:

1. Provide a link between networks. At minimum, a physical and link control connection is needed.

2. Provide for the routing and delivery of data between processes on

different
networks.

3. Provide an accounting service that keeps track of the use of the various networks and routers and maintains status information.

4. Provide the services just listed in such a way as not to require

modifications
to the networking architecture. These include

- Different addressing schemes: The networks may use different endpoint names and addresses and directory maintenance schemes.

- Different maximum packet size: Packets from one network may have to

be
broken up into smaller pieces for another. This process is referred to as fragmentation.

- Different network access mechanisms: The network access mechanism between station and network may be different for stations on different networks.

- Different timeouts: Typically, a connection-oriented transport service will await an acknowledgment until a timeout expires, at which time it will retransmit its block of data. Internetwork timing procedures must allow successful transmission that avoids unnecessary retransmissions.

- Error recovery: Network procedures may provide anything from no error recovery up to reliable end-to-end (within the network) service.

- Status reporting: Different networks report status and performance differently. Yet it must be possible for the internetworking facility to provide such information on internetworking activity to interested and authorized processes.

- Routing techniques: Intra network routing may depend on fault detection and congestion control techniques. The internetworking facility must be able to coordinate these to route data adaptively between stations on different networks.

• User access control: Each network will have its own user access control technique (authorization for use of the network).

• Connection, connectionless: Individual networks may provide connection oriented (e.g., virtual circuit) or connectionless (datagram) service.

The Internet Protocol (IP) meets some of these requirements.

Connectionless Operation

Connectionless-mode operation corresponds to the datagram mechanism of

a
packet-switching network. Each network protocol data unit is treated independently and routed from source ES to destination ES through a series

of
routers and networks. The Internet Protocol (IP) meets some of these requirements.

7.4 INTERNET PROTOCOL OPERATION-

Operation of a connectionless internetworking scheme-

IP provides a connectionless, or datagram, service between end systems. There are a number of advantages to this approach:

• A connectionless internet facility is flexible.

• A connectionless internet service can be made highly robust. This is basically the same argument made for a datagram network service versus a virtual circuit service.

• A connectionless internet service is best for connectionless transport protocols, because it does not impose unnecessary overhead.

At each router, before the data can be forwarded, the router may need to fragment the datagram to accommodate a smaller maximum packet size limitation on the outgoing network.

The router may also limit the length of its queue for each network to which it attaches so as to avoid having a slow network penalize a faster one. Once the queue limit is reached, additional data units are simply dropped.

The destination end system recovers the IP datagram from its network wrapping. This service offered by IP is an unreliable one. With the Internet Protocol approach, each unit of data is passed from router to router in an attempt to get from source to destination.

Design Issues

Some design issues in greater detail:

• Routing

• Datagram lifetime

• Fragmentation and reassembly

• Error control

• Flow control

Routing-

- For the purpose of routing, each end system and router maintains a routing table that lists, for each possible destination network, the next router to which the internet datagram should be sent.
- Routing tables may also be used to support other inter-networking services, such as security and priority.
- Another routing technique is source routing.

Datagram lifetime-

 A simple way to implement lifetime is to use a hop count.

 Each time that a datagram passes through a router, the count is decremented.

 Alternatively, the life time could be a true measure of time.

Fragmentation and reassembly-

 Routers may need to fragment incoming datagrams into smaller pieces, called segments or fragments.

 To reassemble a datagram, there must be sufficient buffer space at the reassembly point.

 As fragments with the same ID arrive, their data fields are inserted in the proper position in the buffer until the entire data field is reassembled.

Error control-

 When a datagram is discarded by a router, the router should attempt to return some information to the source.

 The source Internet Protocol entity may use this information to modify its transmission strategy and may notify higher layers.

Flow control-

 Internet flow control allows routers and/or receiving stations to limit the rate at which they receive data.

For the connectionless type of service we are describing, flow control mechanisms are limited.

7.5 INTERNET PROTOCOL-

The Internet Protocol (IP) is part of the TCP/IP suite and is the most widely used internetworking protocol. As with any protocol standard, IP is specified in two parts:

- The interface with a higher layer (e.g., TCP), specifying the services that IP provides

- The actual protocol format and mechanisms

IP Services

The services to be provided across adjacent protocol layers (e.g., between IP and TCP) are expressed in terms of primitives and parameters. A primitive specifies the function to be performed, and the parameters are used to pass data and control information. The actual form of a primitive is implementation dependent. An example is a procedure call.

IP provides two service primitives at the interface to the next higher layer. The Send primitive is used to request transmission of a data unit. The Deliver primitive is used by IP to notify a user of the arrival of a data unit. The parameters associated with the two primitives are as follows:

• Source address: Internetwork address of sending IP entity.

• Destination address: Internetwork address of destination IP entity.

• Protocol: Recipient protocol entity (an IP user, such as TCP).

• Type-of-service indicators: Used to specify the treatment of the data unit in its transmission through component networks.

• Identification: Used in combination with the source and destination addresses and user protocol to identify the data unit uniquely. This parameter is needed for reassembly and error reporting.

• Don’t fragment identifier: Indicates whether IP can fragment data to accomplish delivery.

• Time to live: Measured in seconds.

• Data length: Length of data being transmitted.

• Option data: Options requested by the IP user.

• Data: User data to be transmitted.

The currently defined options are as follows:

• Security: Allows a security label to be attached to a datagram.

• Source routing: A sequenced list of router addresses that specifies the route to be followed. Routing may be strict (only identified routers may be visited) or loose (other intermediate routers may be visited).

• Route recording: A field is allocated to record the sequence of routers visited by the datagram.

• Stream identification: Names reserved resources used for stream service. This service provides special handling for volatile periodic traffic (e.g., voice).

• Timestamping: The source IP entity and some or all intermediate routers add a timestamp (precision to milliseconds) to the data unit as it goes by.

Internet Protocol

The protocol between IP entities is best described with reference to the IP datagram format. The fields are as follows:

• **Version (4 bits):** Indicates version number, to allow evolution of the protocol; the value is 4.

 Internet Header Length (IHL) (4 bits): Length of header in 32-bit words. The minimum value is five, for a minimum header length of 20 octets.

 Type of Service (8 bits): Prior to the introduction of differentiated services, this field was referred to as the Type of Service field and specified reliability, precedence, delay, and throughput parameters. This interpretation has now been superseded. The first six bits of this field are now referred to as the DS (Differentiated Services) field, the remaining 2 bits are reserved for an ECN (Explicit Congestion Notification) field, currently in the process of standardization. The ECN field provides for explicit signaling of congestion in a manner similar to that discussed for frame relay.

 Total Length (16 bits): Total datagram length,including header plus data,in octets.

 Identification (16 bits): A sequence number that, together with the source address,destinationaddress,and user protocol,is intended to identify a datagram uniquely.Thus,this number should be unique for the datagram’s source address, destination address, and user protocol for the time during which the datagram will remain in the internet.

• **Flags (3 bits):** Only two of the bits are currently defined. The More bit is used for fragmentation and reassembly, as previously explained. The Don’t Fragment bit prohibits fragmentation when set. This bit may be useful if it is known that the destination does not have the capability to reassemble fragments. However, if this bit is set, the datagram will be discarded if it exceeds the maximum size of an enroute network.

 Fragment Offset (13 bits): Indicates where in the original datagram this fragment belongs, measured in 64-bit units. This implies that fragments other than the last fragment must contain a data field that is a multiple of 64 bits in length.

• **Time to Live (8 bits):** Specifies how long, in seconds, a datagram is allowed to remain in the internet. Every router that processes a datagram must decrease the TTL by at least one, so the TTL is similar to a hop count.

• **Protocol (8 bits):** Indicates the next higher level protocol that is to receive the data field at the destination; thus, this field identifies the type of the next header in the packet after the IP header.

 Header Checksum (16 bits): An error-detecting code applied to the header only. Because some header fields may change during transit (e.g., Time to Live, fragmentation-related fields), this is reverified and recomputed at each router. The checksum is formed by taking the ones complement of the 16-bit ones complement addition of all 16-bit words in the header.

 Source Address (32 bits): Coded to allow a variable allocation of bits to specify the network and the end system attached to the specified network, as discussed subsequently.

 Destination Address (32 bits): Same characteristics as source address.

• **Options (variable):** Encodes the options requested by the sending user.

• **Padding (variable):** Used to ensure that the datagram header is a multiple of 32 bits in length.

• **Data (variable):** The data field must be an integer multiple of 8 bits in length. The maximum length of the datagram (data field plus header) is 65,535 octets.

IP Addresses

The source and destination address fields in the IP header each contain a 32-bit global internet address, generally consisting of a network identifier and a host identifier.

Network Classes

The address is coded to allow a variable allocation of bits to specify network and host. This encoding provides flexibility in assigning addresses to hosts and allows a mix of network sizes on an internet. The three principal network classes are best suited to the following conditions:

- **Class A:** Few networks, each with many hosts
- **Class B:** Medium number of networks, each with a medium number of hosts
- **Class C:** Many networks, each with a few hosts.

Internet Control Message Protocol (ICMP)- ICMP provides a means for transferring messages from routers and other hosts to a host.

ARP- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI data link layer.