Components of Data Communication System

Data Communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

Data Communication System Components :

There are mainly five components of a data communication system:

1. Message
2. Sender
3. Receiver
4. Transmission Medium
5. Set of rules (Protocol)

All above mentioned elements are described below:

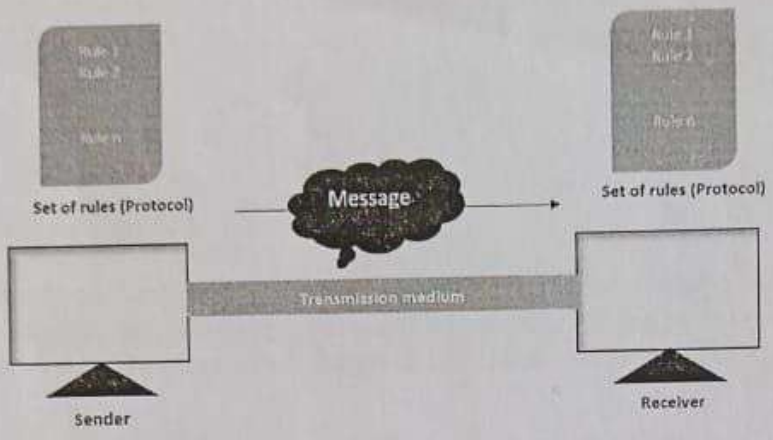


Figure – Components of Data Communication System

1. **Message :**
   This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.

2. **Sender :**
   To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.

3. **Receiver :**
   It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.

4. Transmission Medium :
   In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message

travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.

5. **Set of rules (Protocol) :**
   To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

A typical example of a data communication system is sending an e-mail. The user which send email act as sender, message is data which user wants to send, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send and receive email.

What is a Signal?

Gestures, actions, sounds, expressions tell us some information, and these are the ways of communicating one to other. Similarly **signal** is a way of communicating by sending information from one system to other system. In other words signal is a function that represents information or data.

Signal is an electromagnetic wave that carries information through physical medium. Here the data is converted into electromagnetic signal either as analog or digital and sent from sender to receiver.

For communicating between two systems, a message signal is passed through encoder and modulator to transmit through a medium while it is passed through decoder and demodulator to receive the message signal at the other end.

Signals are divided into two categories based on their nature.

Signals which are

1. Signal which are Continuous as time varying in nature are **analog signals**
2. Signal which are discrete are called **digital signals**.

Network Standards

Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are –

- **Application layer** – HTTP, HTML, POP, H.323, IMAP
- **Transport layer** – TCP, SPX
- **Network layer** –IP, IPX
- **Data link layer** – Ethernet IEEE 802.3, X.25, Frame Relay
- **Physical layer** –RS-232C (cable), V.92 (modem)

Types of Standards

Standards are of two types

- **De facto** – These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.
- **De jure** – These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

Standards Organizations

Some of the noted standards organizations are

- International Standards Organization (ISO)
- International Telecommunication Union (ITU)
- Institute of Electronics and Electrical Engineers (IEEE)
- American National Standards Institute (ANSI)
- Internet Research Task Force (IETF)
- Electronic Industries Association (EIA)

1. Bandwidth :
Bandwidth is defined as the potential of the data that is to be transferred in a specific period of time. It is the data carrying capacity of the network or transmission medium. In simple words, it is the maximum amount of data that can be transferred per second on a link. It is generally measured in bits per second(bps), Mega bits per second(Mbps) or Giga bits per second(Gbps).
For example, if bandwidth is 100 Mbps, it means maximum 100 Mb data can be transferred per second on that channel.

2. Data Rate :
Data Rate is defined as the amount of data transmitted during a specified time period over a network. It is the speed at which data is transferred from one device to another or between a peripheral device and the computer. It is generally measured in Mega bits per second(Mbps) or Mega bytes per second(MBps).
For example, if bandwidth is 100 Mbps but data rate is 50 Mbps, it means maximum 100 Mb data can be transferred but channel is transmitting only 50 Mb data per second.

Bandwidth	Data Rate
It is the potential of the data that is to be transferred in a specific period of time.	It is the amount of data transmitted during a specified time period over a network.

5.	Bit rate is not used to decide the requirement of bandwidth for transmission of signal.	While baud rate is used to decide the requirement of bandwidth for transmission of signal.

Transmission modes

- The way in which data is transmitted from one device to another device is known as **transmission mode**.
- The transmission mode is also known as the communication mode.
- Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:

- Simplex mode
- Half-duplex mode
- Full-duplex mode

Simplex mode

- In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
- A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
- This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.
- The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
- Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
- The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

Advantage of Simplex mode:

- In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data c be transmitted at a time.

speed, and it has no overhead of

Difference between Bit Rate and Baud Rate

Both Bit rate and Baud rate are generally used in data communication.

Bit rate is the transmission of number of bits per second. On the other hand, Baud rate is defined as the number of signal units per second. The formula which relates both bit rate and baud rate is given below:

Bit rate = Baud rate x the number of bit per baud.

Let's see the difference between Bit Rate and Baud Rate:

S.NO	Bit Rate	Baud Rate
1.	Bit rate is defined as the transmission of number of bits per second.	Baud rate is defined as the number of signal units per second.
2.	Bit rate is also defined as per second travel number of bits.	Baud rate is also defined as per second number of changes in signal.
3.	Bit rate emphasized on computer efficiency.	While baud rate emphasized on data transmission.
4.	The formula of **Bit Rate** is: = baud rate x the number of bit per baud	The formula of **Baud Rate** is: = bit rate / the number of bit per baud

Direction of communication	In simplex mode, the communication is unidirectional.	In half-duplex mode, the communication is bidirectional, but one at a time.	In full-duplex mode, the communication is bidirectional.
Send/Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Performance	The performance of half-duplex mode is better than the simplex mode.	The performance of full-duplex mode is better than the half-duplex mode.	The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel.
Example	Examples of Simplex mode are radio, keyboard, and monitor.	Example of half-duplex is Walkie-Talkies.	Example of the Full-duplex mode is a telephone network.

Disadvantage of Simplex mode:

- Communication is unidirectional, so it has no inter-communication between devices.

Half-Duplex mode

- In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
- Messages flow in both the directions, but not at the same time.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
- A **Walkie-talkie** is an example of the Half-duplex mode. In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

Advantage of Half-duplex mode:

- In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

Disadvantage of Half-Duplex mode:

- In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

Full-duplex mode

- In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the fastest mode of communication between devices.
- The most common example of the full-duplex mode is a telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

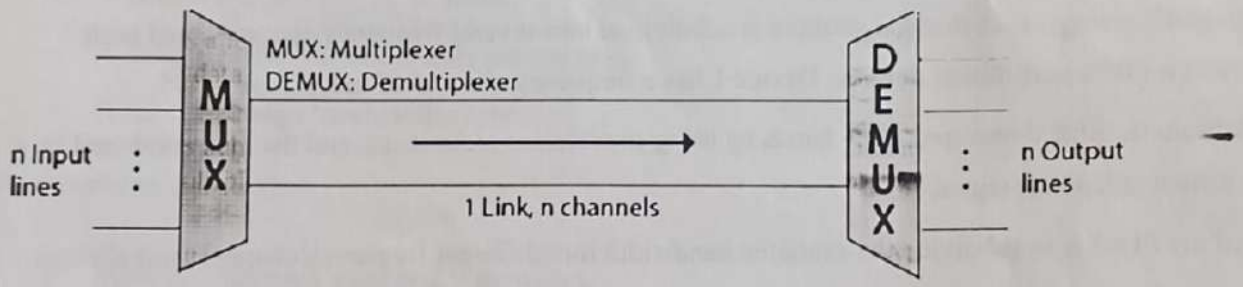
What is Multiplexing?

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.

Concept of Multiplexing



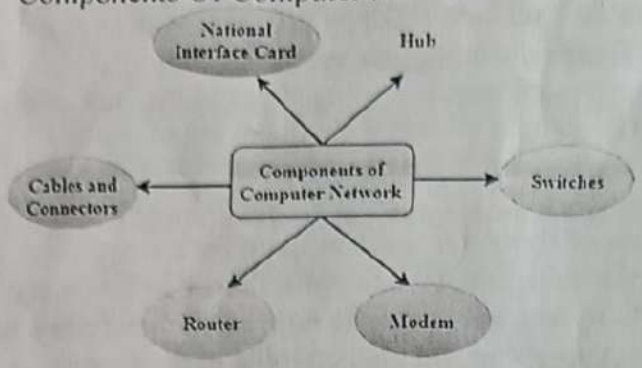
- The 'n' input lines are transmitted through a multiplexer and multiplexer combines the signals to form a composite signal.
- The composite signal is passed through a Demultiplexer and demultiplexer separates a signal to component signals and transfers them to their respective destinations.

- Multiplexing Techniques
- Multiplexing techniques can be classified as:

What is a Computer Network?

- **Computer Network** is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.
- The aim of the computer network is the sharing of resources among various devices.
- In the case of computer network technology, there are several types of networks that vary from simple to complex level.

Components Of Computer Network:



Uses Of Computer Network

- **Resource sharing:** Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.
- **Server-Client model:** Computer networking is used in the **server-client model**. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.
- **Communication medium:** Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.
- **E-commerce:** Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

File sharing is simply the act of sharing one or more files. A file can exist on your computer for you to use it, but you can also send the file to someone else in the same house, within your company, or literally anywhere else in the world.Sharing files over a computer network means that you're using a network connection to send the files. This could be a local network like in an office or at home where you share files with other local users, or you can share files over the internet.You might share files for work or entertainment, or so that you can access your files from anywhere. Below are several file sharing methods that you can use for any reason.

Types of File Sharing

Categories of network

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

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

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

LAN (Local Area Network)

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

- Local Area Network provides higher security.

MAN(Metropolitan Area Network)

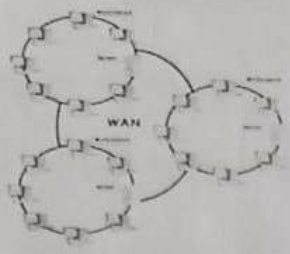
- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

Uses Of Metropolitan Area Network:

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

WAN(Wide Area Network)

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



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.
- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

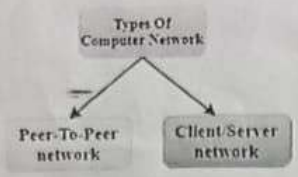
The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Categories of network based on connection

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

The two types of network architectures are used:



- Peer-To-Peer network
- Client/Server network

Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

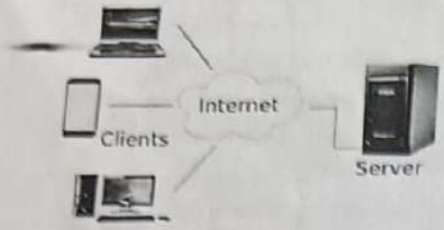
Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system . Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients.**
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.

- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources

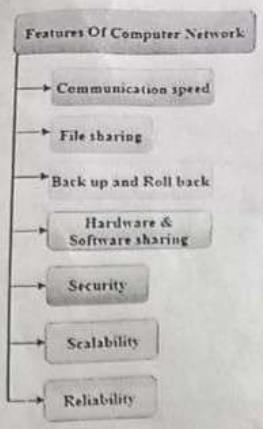
Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Centralized and Distributed computer network

- In Centralized computer network model, the network resources are placed and managed from a main location. Centralized network model allows administrators to manage the resources centrally (typically in Head Office). The network servers and other critical network resources are located in a central location in a secure and dedicated server room.
- Centralized network model provides following advantages to Network and System Administrators.
- Centralized network model provides Network and System Administrators better access to network devices
- In Centralized network model, Network Resources can be managed more easily
- Centralized network model provides better Network Security.
- The main disadvantage is more work load of Network and System Administrators and increased risk of communication failure due to a catastrophe in the central location.
- In Distributed network model, the network resources are placed and managed from different geographical locations. Designated network and system administrators manage the network resources in different locations. These days most of the Enterprise network models are distributed.

Features Of Computer network



A list Of Computer network features is given below.

Communication speed

- File sharing
- Back up and Roll back is easy
- Software and Hardware sharing
- Security
- Scalability
- Reliability

Communication speed

Network provides us to communicate over the network in a fast and efficient manner. For example, we can do video conferencing, email messaging, etc. over the internet. Therefore, the computer network is a great way to share our knowledge and ideas.

File sharing

File sharing is one of the major advantage of the computer network. Computer network provides us to share the files with each other.

Back up and Roll back is easy

Since the files are stored in the main server which is centrally located. Therefore, it is easy to take the back up from the main server.

Software and Hardware sharing

We can install the applications on the main server, therefore, the user can access the applications centrally. So, we do not need to install the software on every machine. Similarly, hardware can also be shared.

Security

Network allows the security by ensuring that the user has the right to access the certain files and applications.

Circuit Switching

Circuit Switching is a connection-oriented service. It provides a dedicated path from the sender to the receiver. In-circuit switching, a connection setup is required to send and receive data. It has very little chance of data loss and error due to the dedicated circuit, but a lot of bandwidth is wasted because the same path cannot be used by other senders during a congestion. Circuit switching is completely transparent; the sender and receiver can use any bit rate format or framing method.

Advantages of Circuit Switching

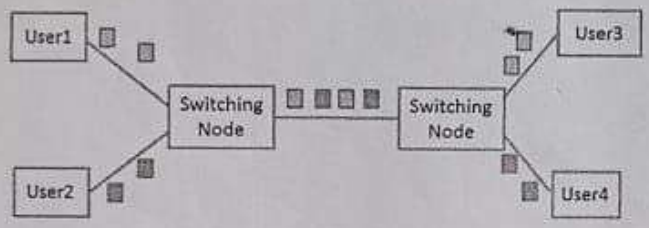
- It uses a fixed bandwidth.
- A dedicated communication channel increases the quality of communication.
- Data is transmitted with a fixed data rate.
- No waiting time at switches.
- Suitable for long continuous communication.

Disadvantages of circuit switching

- A dedicated connection makes it impossible to transmit other data even if the channel is free.
- Resources are not utilized fully.
- The time required to establish the physical link between the two stations is too long.
- A dedicated path has to be established for each connection.
- Circuit switching is more expensive.
- Even if there is no transfer of data, the link is still maintained until it is terminated by users.
- Dedicated channels require more bandwidth.

Packet Switching

Packet switching is a connectionless service. It does not require any dedicated path between the sender and receiver. It places an upper limit on block size. In packet switching bandwidth is freely utilized as unrelated sources can be used in any path. It has more chance of data loss and error; the packets may arrive in the wrong order.



Packet Switching

Advantages of Packet switching

- It reduces access delay.
- Costs are minimized to great extent. Hence packet switching is a very cost-effective technique.
- Packets are rerouted in case of any problems. This ensures reliable communication.
- It is more efficient for data transmission because no need to establish the path.
- Several users can share the same channel simultaneously. Therefore packet switching makes use of available bandwidth efficiently.

Disadvantages of Packet switching

- In packet switching, the network can not be used in applications requiring very little delay and higher quality of service.

- Protocols used in the packet switching are complex.
- If the network becomes overloaded, packets are delayed or discarded, or dropped. This leads to the retransmission of lost packets by the sender.
- It is not secured if security protocols are not used during packet transmission.

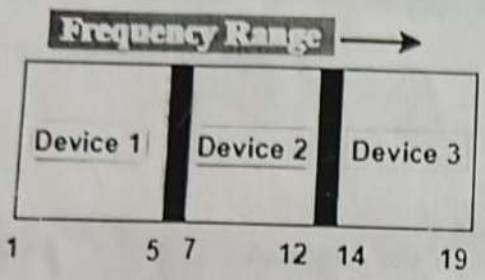
Difference between circuit switching and packet switching

The following table highlights the major differences between circuit switching and packet switching –

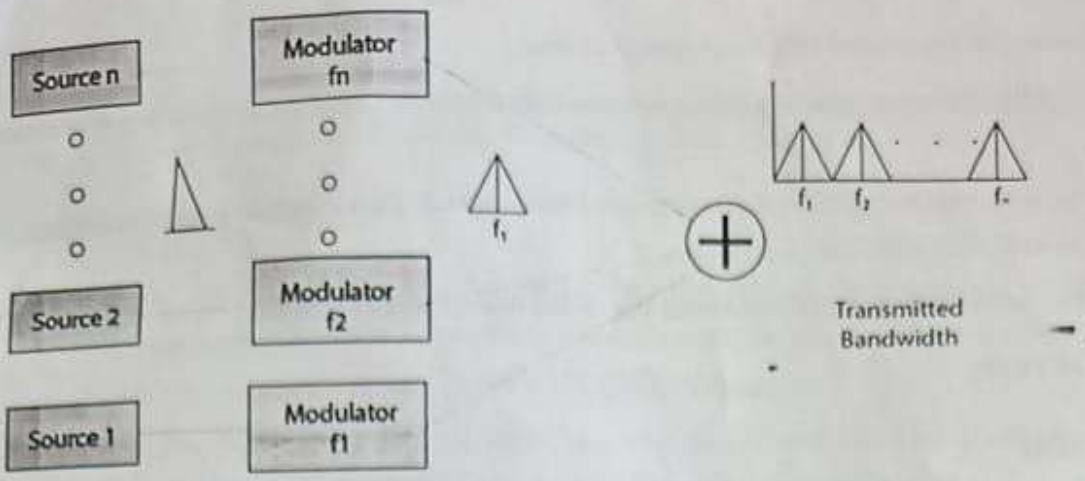
Circuit Switching	Packet Switching
Circuit switching requires a dedicated path before sending data from source to destination.	Packet switching does not require any dedicated path to send data from source to destination.
It reserves the entire bandwidth in advance.	It does not reserve bandwidth in advance
No store and forward transmission	It supports store and forward transmission
Each packet follows the same route	A packet can follow any route
Call setup is required	No call setup is required
Bandwidth wastage	No bandwidth wastage

Frequency-division Multiplexing (FDM)

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



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



Advantages Of FDM:

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

Disadvantages Of FDM:

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

Applications Of FDM:

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

Time Division Multiplexing

- It is a digital technique.
- In Frequency Division Multiplexing Technique, all signals operate at the same time with different frequency, but in case of Time Division Multiplexing technique, all signals operate at the same frequency with different time.
- In **Time Division Multiplexing technique**, the total time available in the channel is distributed among different users. Therefore, each user is allocated with different time interval known as a Time slot at which data is to be transmitted by the sender.

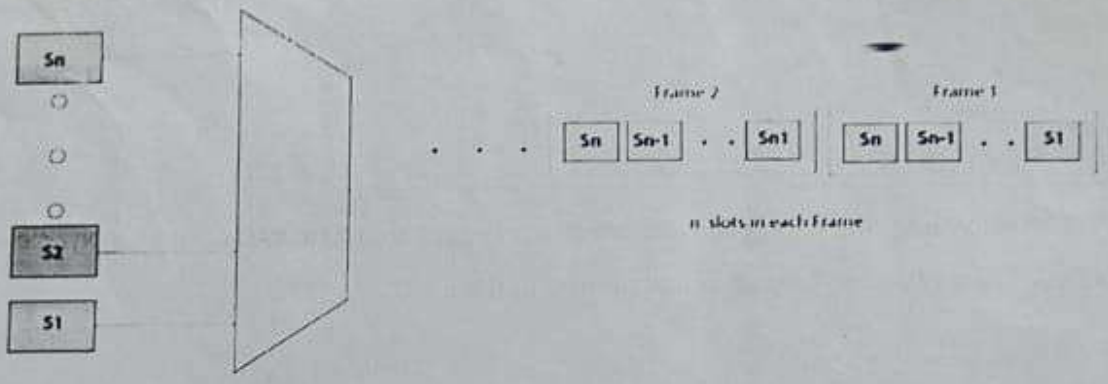
- A user takes control of the channel for a fixed amount of time.
- In Time Division Multiplexing technique, data is not transmitted simultaneously rather the data is transmitted one-by-one.
- In TDM, the signal is transmitted in the form of frames. Frames contain a cycle of time slots in which each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

There are two types of TDM:

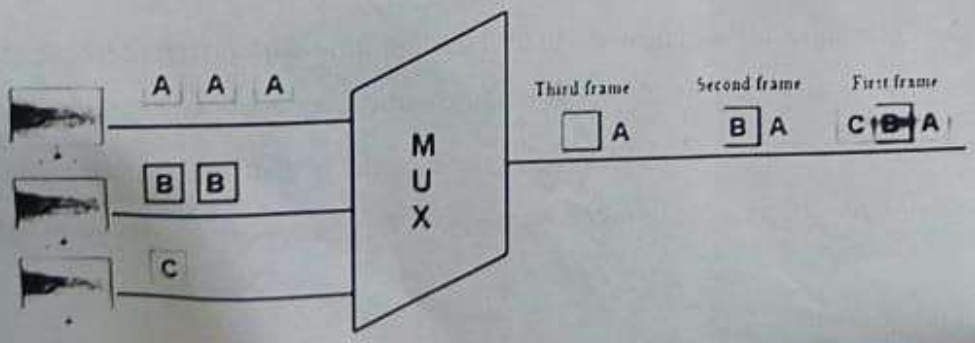
- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

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



Concept Of Synchronous TDM



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

Disadvantages Of Synchronous TDM:

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

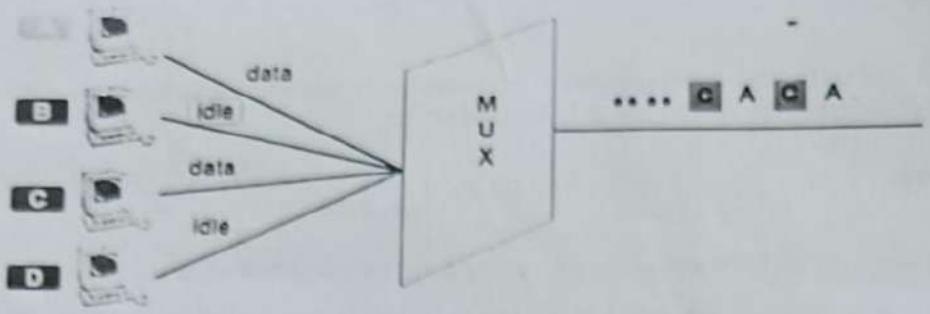
Asynchronous TDM

- An asynchronous TDM is also known as Statistical TDM.
- An asynchronous TDM is a technique in which time slots are not fixed as in the case of Synchronous TDM. Time slots are allocated to only those devices which have the data to send. Therefore, we can say that Asynchronous Time Division multiplexor transmits only the data from active workstations.
- An asynchronous TDM technique dynamically allocates the time slots to the devices.
- In Asynchronous TDM, total speed of the input lines can be greater than the capacity of the channel.
- Asynchronous Time Division multiplexor accepts the incoming data streams and creates a frame that contains only data with no empty slots.
- In Asynchronous TDM, each slot contains an address part that identifies the source of the data.

ADDRESS	DATA

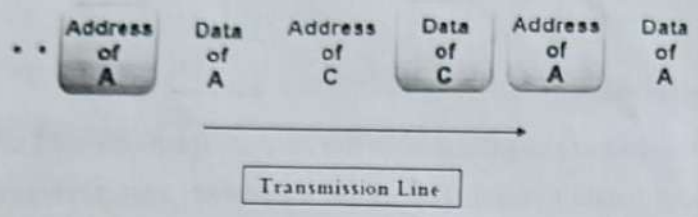
- The difference between Asynchronous TDM and Synchronous TDM is that many slots in Synchronous TDM are unutilized, but in Asynchronous TDM, slots are fully utilized. This leads to the smaller transmission time and efficient utilization of the capacity of the channel.
- In Synchronous TDM, if there are 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:

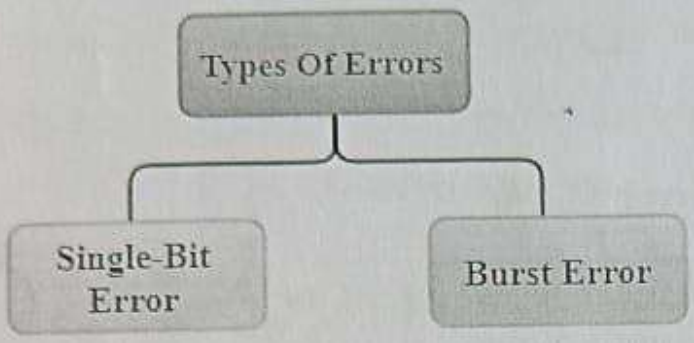


The above figure shows that the data part contains the address to determine the source of the data.

Error Detection

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

Types Of Errors

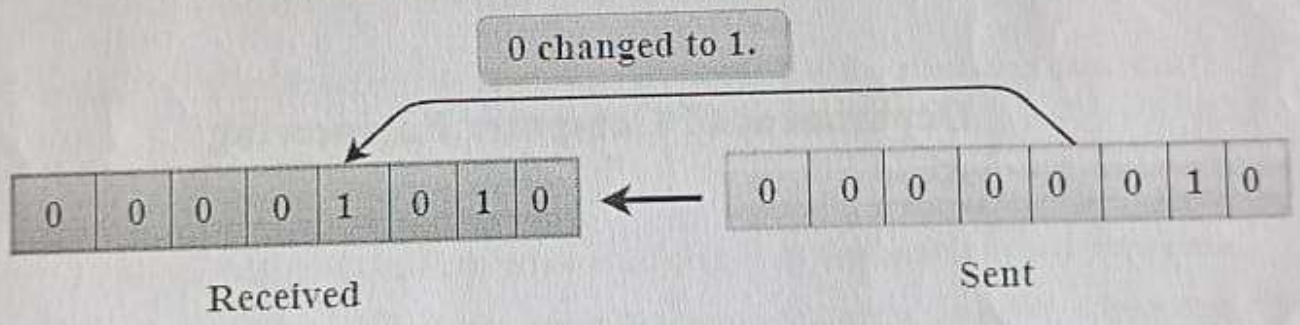


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

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



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

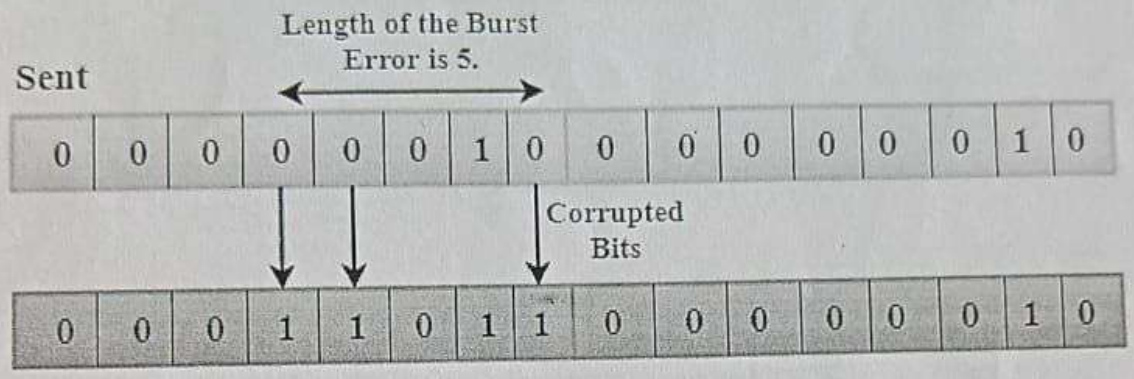
Single-Bit Error does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.

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

Burst Error:

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

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



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

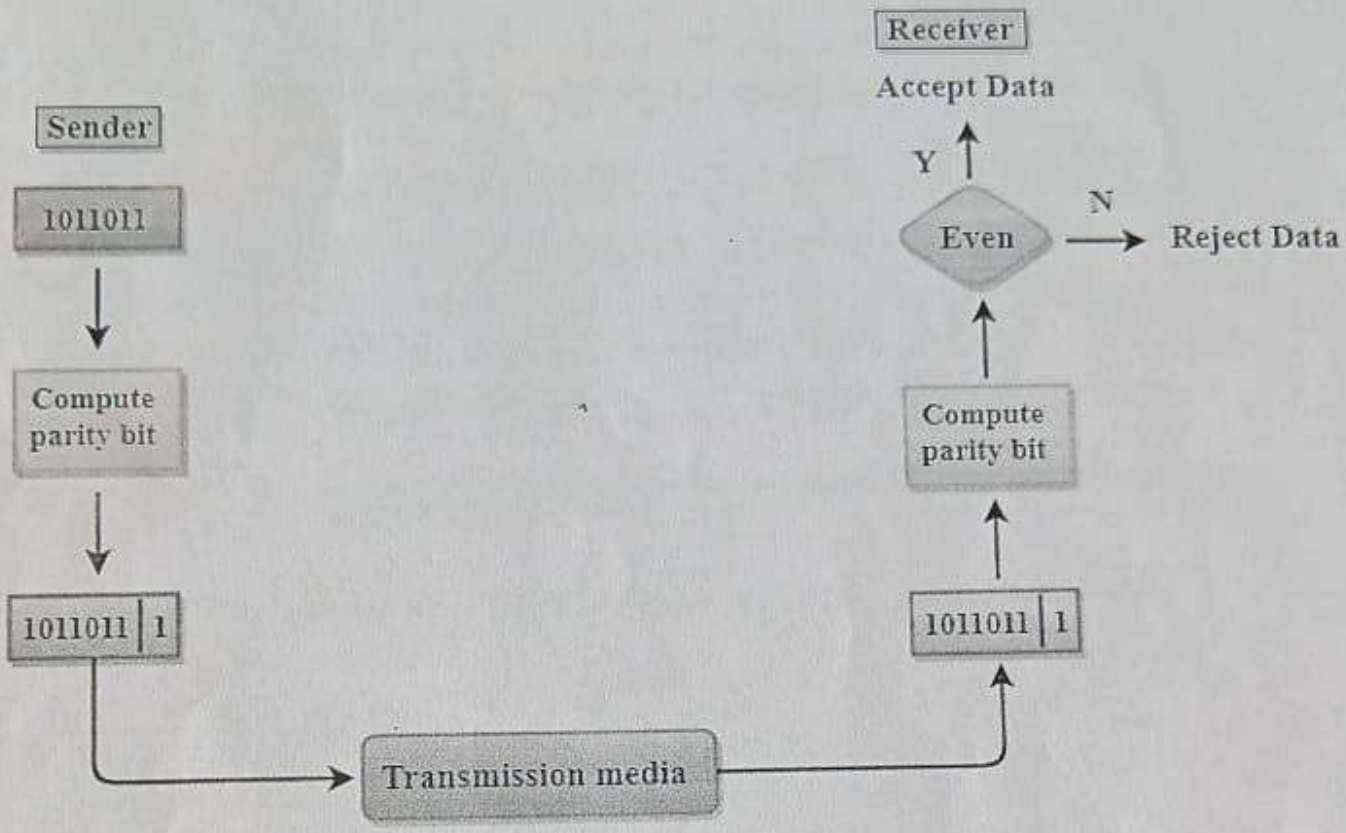
Burst Errors are most likely to occurr in Serial Data Transmission.

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

Single Parity Check

- Single Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

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



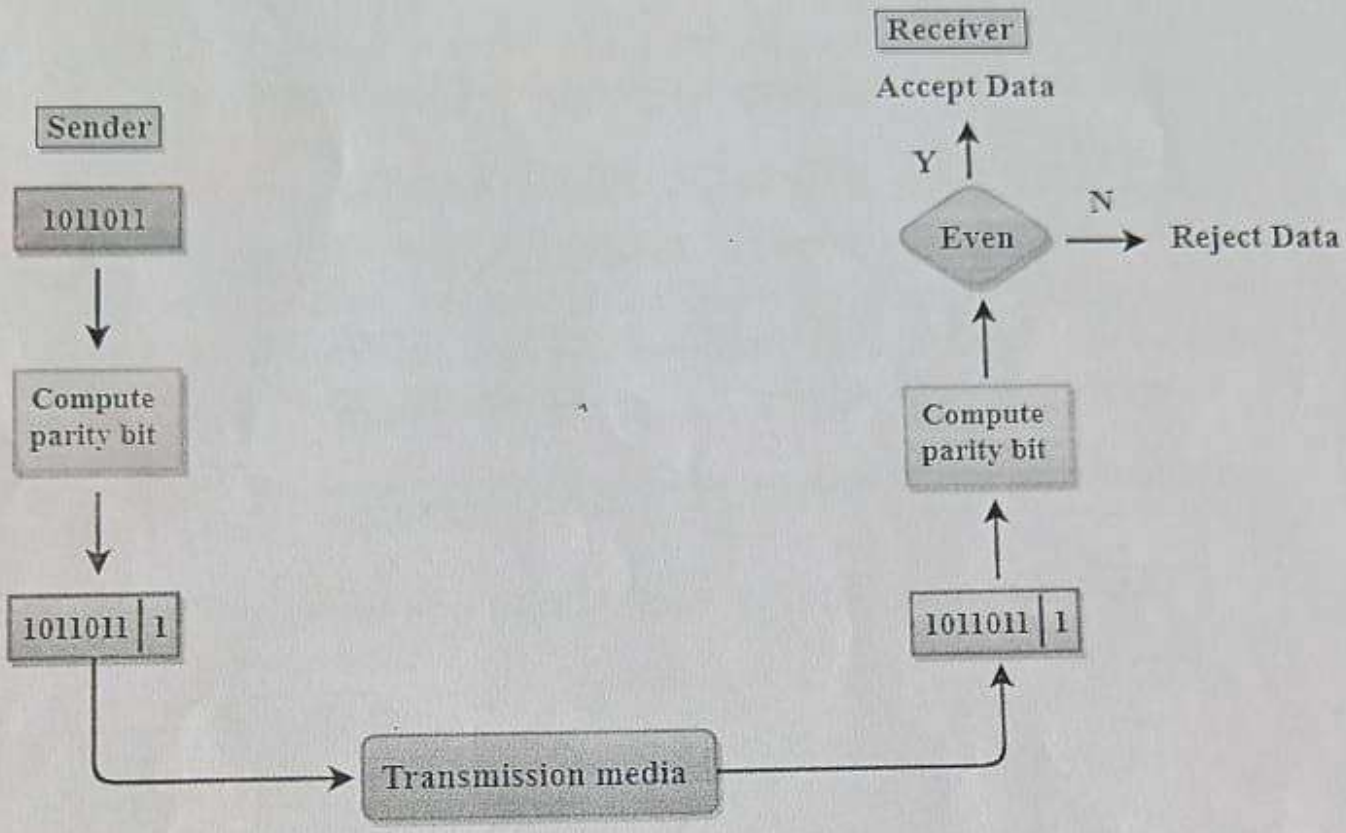
Drawbacks Of Single Parity Checking

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

Cyclic Redundancy Check (CRC)

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

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



Drawbacks Of Single Parity Checking

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

Cyclic Redundancy Check (CRC)

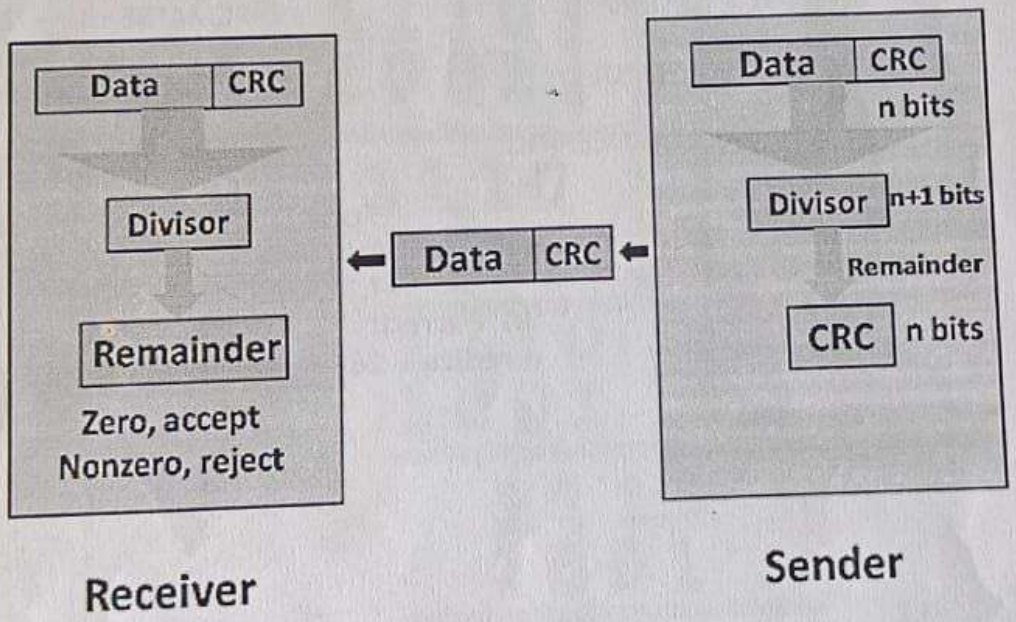
CRC is a redundancy error technique used to determine the error.

Following are the steps used in CRC for error detection:

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

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

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

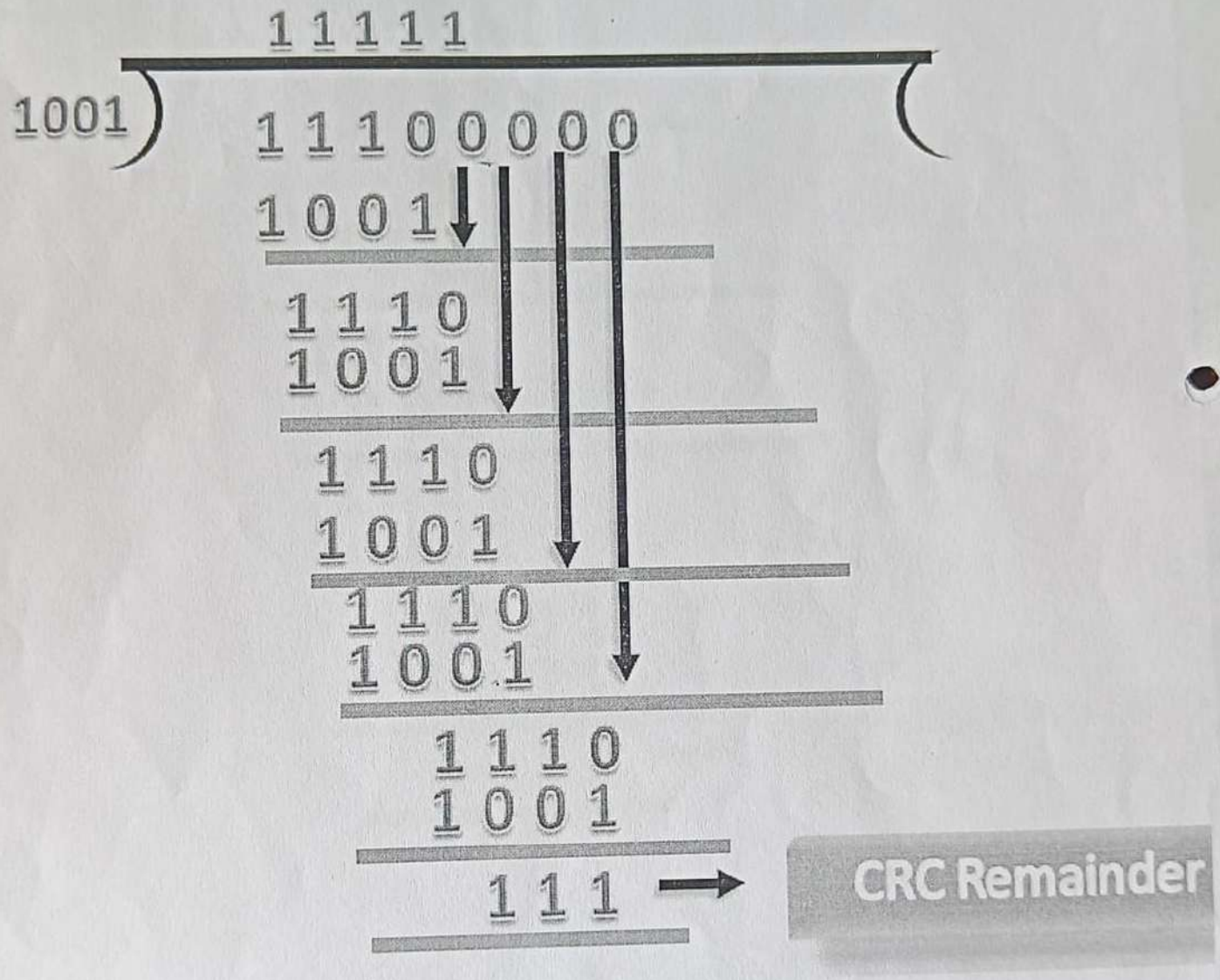


Let's understand this concept through an example:

Suppose the original data is 11100 and divisor is 1001.

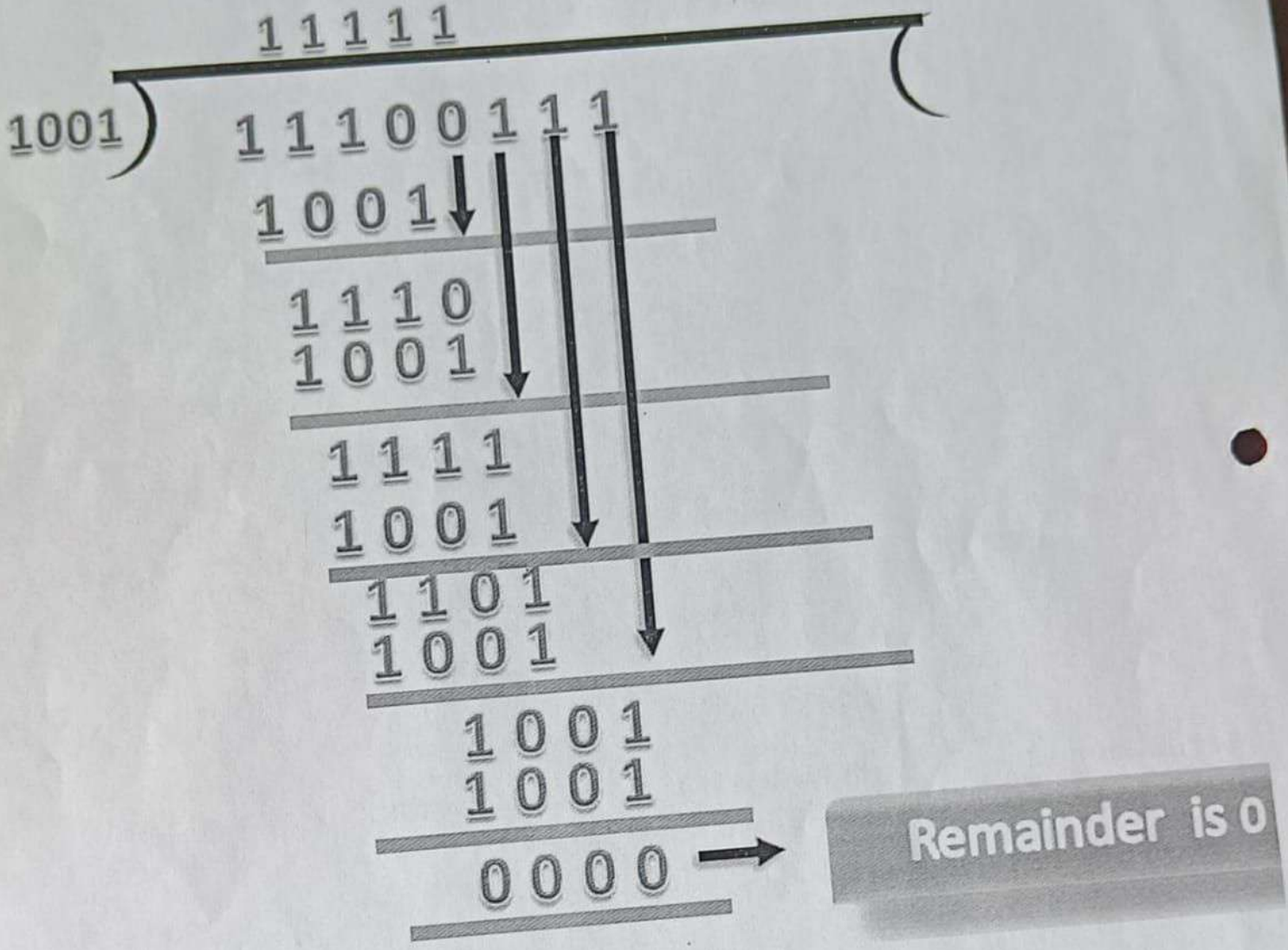
CRC Generator

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



CRC Checker

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



Longitudinal Redundancy Check (LRC)/2-D Parity Check

Longitudinal Redundancy Check is also known as 2-D parity check. In this method, data which the user want to send is organized into tables of rows and columns. A block of bit is divided into table or matrix of rows and columns. In order to detect an error, a redundant bit is added to the whole block and this block is transmitted to receiver. The receiver uses this redundant row to detect error. After checking the data for errors, receiver accepts the data and discards the redundant row of bits.

Example :

If a block of 32 bits is to be transmitted, it is divided into matrix of four rows and eight columns which as shown in the following figure :

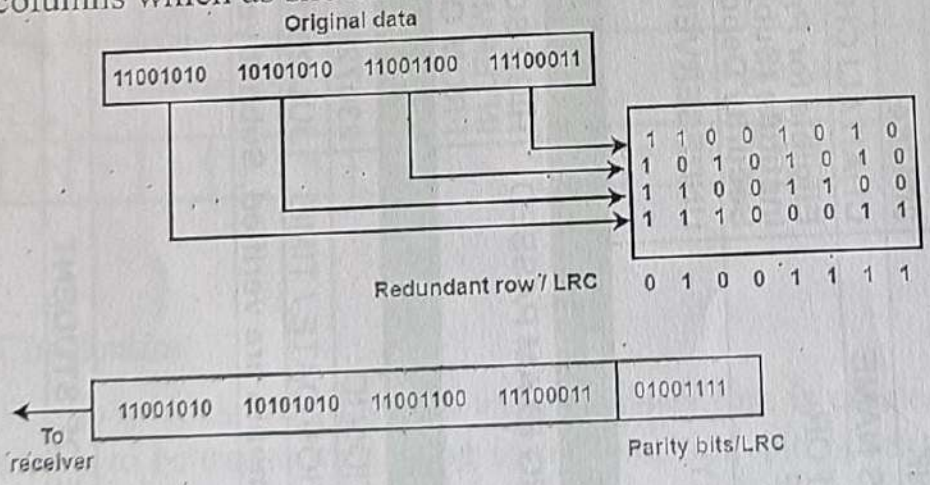
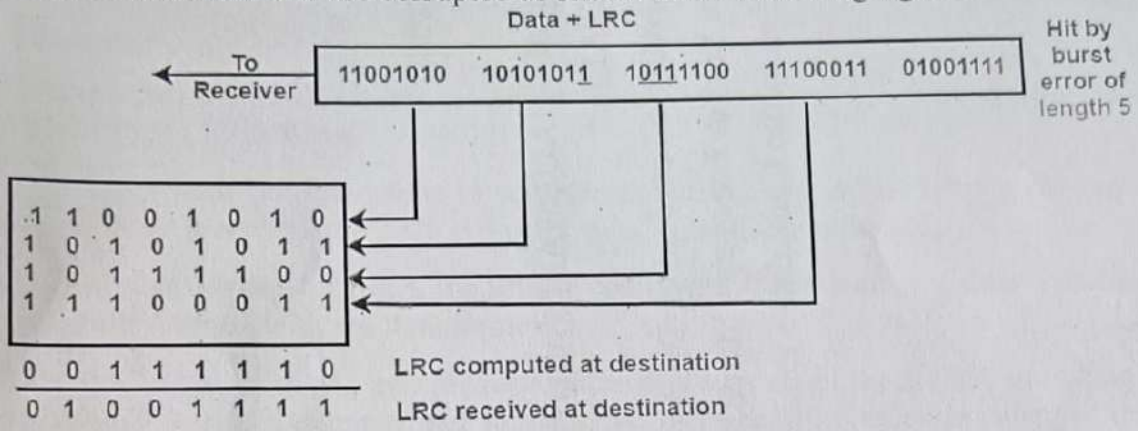


Figure: LRC

In this matrix of bits, a parity bit (odd or even) is calculated for each column. It means 32 bits data plus 8 redundant bits are transmitted to receiver. Whenever data reaches at the destination, receiver uses LRC to detect error in data.

Advantage :
LRC is used to detect burst errors.

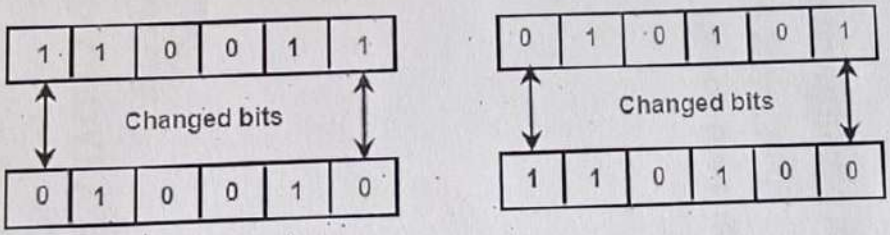
Example : Suppose 32 bit data plus LRC that was being transmitted is hit by a burst error of length 5 and some bits are corrupted as shown in the following figure :



The LRC received by the destination does not match with newly corrupted LRC. The destination comes to know that the data is erroneous, so it discards the data.

Disadvantage :
The main problem with LRC is that, it is not able to detect error if two bits in a data unit are damaged and two bits in exactly the same position in other data unit are also damaged.

Example : If data 110011 010101 is changed to 010010110100.



Checksums

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data. When the receiver gets

is data, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error.

Error Detection by Checksums

For error detection by checksums, data is divided into fixed sized frames or segments.

- **Sender's End** – The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- **Receiver's End** – The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

If the result is zero, the received frames are accepted; otherwise they are discarded.

Example

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

The sender adds the bits using 1s complement arithmetic. While adding two numbers using 1s complement arithmetic, if there is a carry over, it is added to the sum.

After adding all the 4 frames, the sender complements the sum to get the checksum, 11010011, and sends it along with the data frames.

The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.

This method makes the use of checksum generator on sender side and checksum checker on receiver side

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.