Data Communications:

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

The effectiveness of a data communications system depends on four fundamental characteristics:

1. **Delivery** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. **Accuracy** The system must deliver the data accurately. Data should not be altered. If the data is altered in transmission and left uncorrected are unusable.
3. **Timeliness** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced and without significant delay. This kind of delivery is called *real-time* transmission.
4. **Jitter** It refers to the variation in the packet arrival time. Jitter is the uneven delay in the delivery of audio or video packets.
   Example: Let us assume that video packets are sent every 3ms. If some of the packets arrive with 3ms delay and others with 4ms delay, an uneven quality in the video is the result.

Components:

A data communications system has five components:

1. Message: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. Protocol: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a

person speaking French cannot be understood by a person who speaks only Japanese.
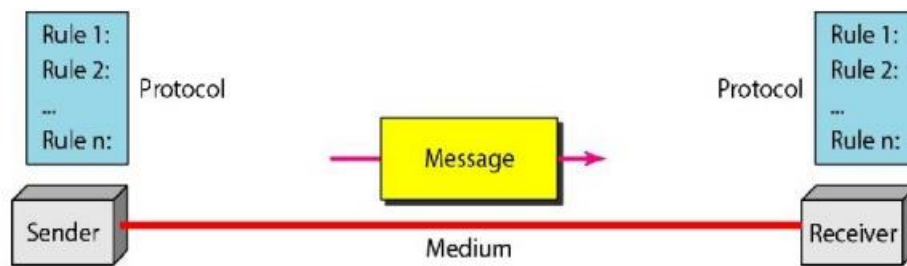

Fig 1: Components of Data Communication.

Direction of Data flow:

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

Simplex: The communication is unidirectional, as on a one-way street.

Only one of the two devices on a link can transmit; the other can only receive.

Keyboards and traditional monitors are examples of simplex devices.

The simplex mode can use the entire capacity of the channel to send data in one direction as shown in **Fig 2.a**

Half-Duplex: Each station can both transmit and receive, but not at the same time.

The half-duplex mode is like a one-lane road with traffic allowed in both directions.

The entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time as shown in **Fig 2.b**
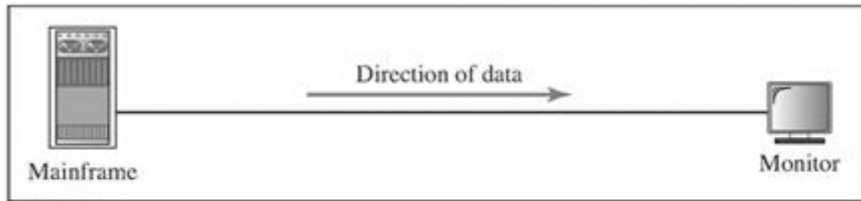
Walkie-talkies and CB (citizens band) radios are both half-duplex systems.
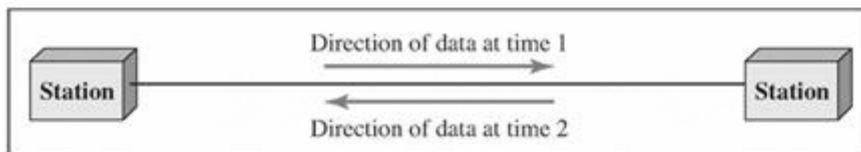
Full-Duplex:

Both stations can transmit and receive simultaneously.

Signals going in one direction share the capacity of the link with signals going in the other direction as shown in **Fig 2.c.**
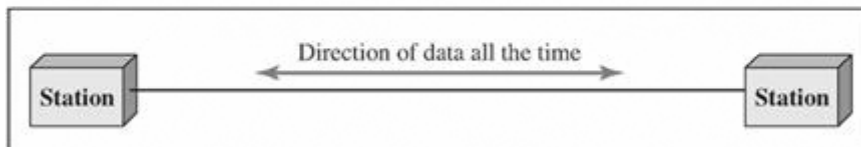
One common example of full-duplex communication is the telephone network.

Direction of data

Mainframe   Monitor

a. Simplex

Direction of data at time 1

Station   Station

Direction of data at time 2

b. Half-duplex

Direction of data all the time

Station   Station

c. Full-duplex

NETWORKS

A **Network** is a set of devices (also called as nodes) connected by communication links. (or)
A **Network** is two or more devices connected through links.

A **Node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

A **Link** is a communications pathway that transfers data from one device to another.

CATEGORIES OF NETWORKS

There are 3 categories of networks depend on its size:
1. Local Area Networks(LAN)
2. Metropolitan Area Networks(MAN)
3. Wide Area Networks(WAN)

Local Area Networks

- A Local Area Network (LAN) provides short-distance transmission of data over small geographic areas that may comprise a single office, building, or campus.
- **Size:** LAN size is limited to a few kilometers.
- **Speed:** Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range but now speeds are increased to 100 or 1000Mbps.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
- A local area network (LAN) is usually privately owned.
- LAN will use only one type of transmission medium.
- The most common LAN topologies are bus, ring, and star.
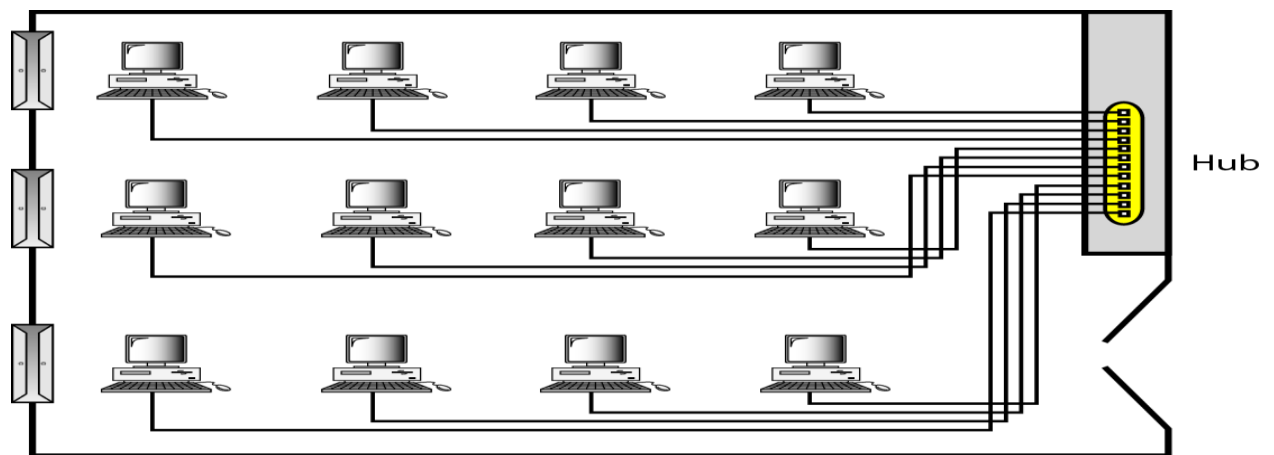
Metropolitan Area Networks

A Metropolitan Area Network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

It is designed for customers who need a high-speed connectivity to the Internet, and have endpoints spread over a city or part of city.

Example of a MAN is the part of the telephone company network that can provide a high- speed DSL line to the customer.
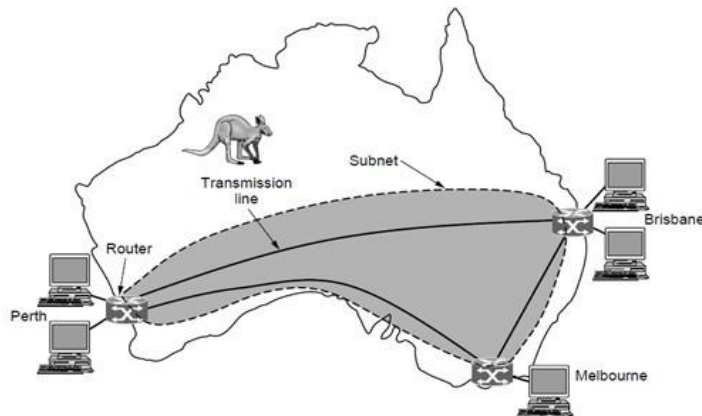
A metropolitan area network based on cable TV
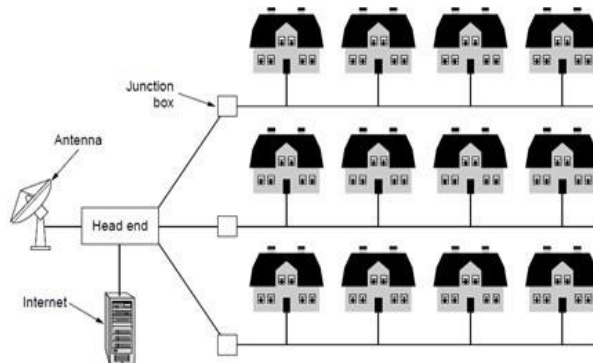
Wide Area Network

A Wide Area Network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

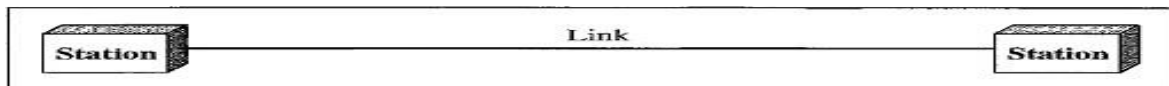# WAN that connects three branch offices in Australia.
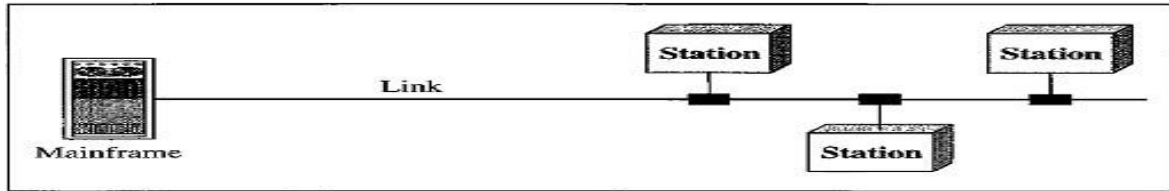

Type of Connection

Two devices must be connected in some way to the same link at the same time for occurring of communication. There are two possible types of connections:

1. Point-to-Point Connection

2. Multipoint Connection

a. Point-to-point

b. Multipoint

Point-to-Point Connection

- A Point-to-Point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- Point-to-Point connections use an actual length of wire or cable to connect the two ends and microwave or satellite links.
- Example: When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint (or) Multi-drop Connection

- A multipoint connection is more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a time shared connection.
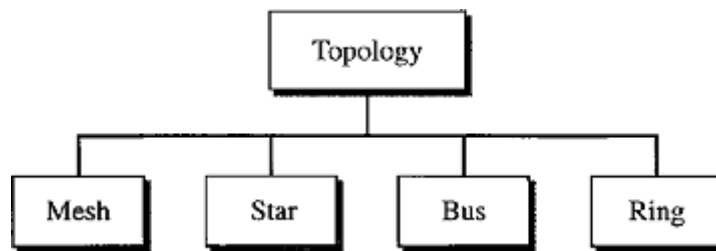
NETWORK TOPOLOGIES

The term physical topology refers to the way in which a network is connected physically.

Two or more devices connect to a link. Two or more links form a topology.

There are four basic topologies are present:

1. Bus
2. Ring
3. Star
4. Mesh

Mesh Topology

* In a mesh topology, every device has a **Dedicated Point-to-Point** link to every other device. (i.e.) for each node there is a link to all other nodes.
* The term **Dedicated** means that the link carries traffic only between the two devices it connects.

Advantages:

1. A mesh topology is robust. If one link becomes unusable, it does not affect the entire system.
2. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
3. **Privacy or Security.** When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.
4. Point-to-Point links make **Fault Identification** and **Fault Isolation** easy.
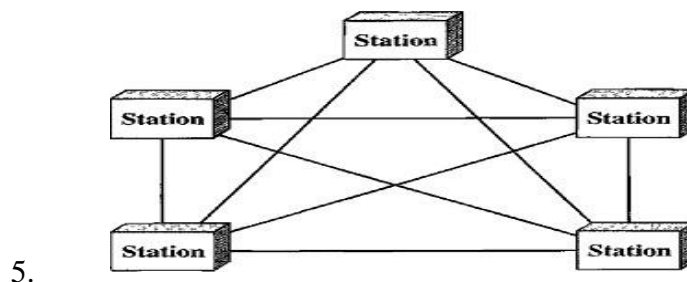
5.

Disadvantages:

1. **High Cost:** Every device must be connected to every other device then there is a high amount of cabling and huge number of I/O ports required, this will make installation and reconnection are difficult.
2. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
3. More hardware (i.e. cables) and space is required

Example: Telephone offices and Police stations.

Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

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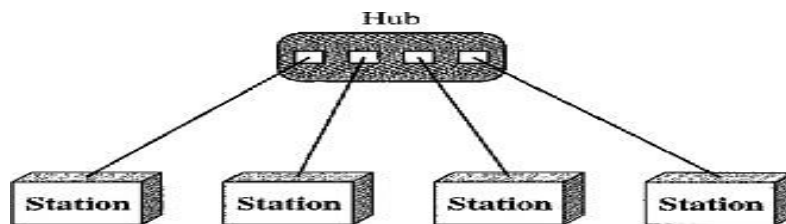
Advantages:

1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure
2. Less cabling is required than mesh topology.
3. Star topology is robust, If one link fails, only that link is affected. All other links remain active.
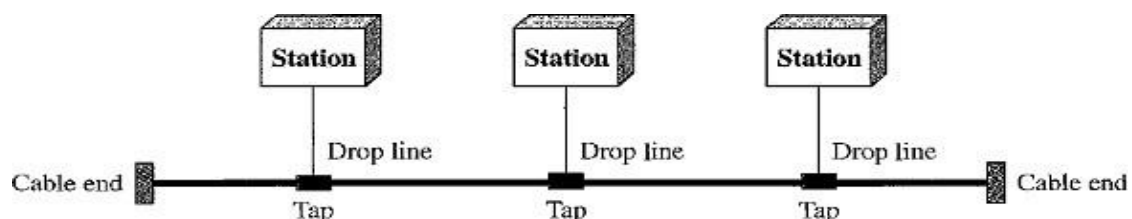
Disadvantages:

1. If hub fails entire processing will be stopped working.

Uses:

2. It is used in High-speed LAN's often use a star topology with a central hub.

Bus Topology

- A **bus topology** is multipoint connection, one long cable acts as a **backbone** to link all the devices in a network. Here the cable is called the bus.
- Bus topology was the one of the first topologies used in the design of early local area networks.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that splices into (attached to) the main cable.

Advantages:

1. Installation is easy. Bus Backbone cable can be laid along the most efficient path and then connected to the nodes by drop lines of various lengths.
2. A bus uses less cabling than mesh or star topologies.

Disadvantages:

1. All the devices are connected to bus backbone cable, so that if the backbone cable fails the entire system fails.

2. Difficult Reconnection and Fault Isolation. It is difficult to add new devices.
3. There is a limit on the number of taps a bus can support and on the distance between those taps.
4. More heat is generated if the number of taps is more. Heat degrades the quality of signal.

Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.
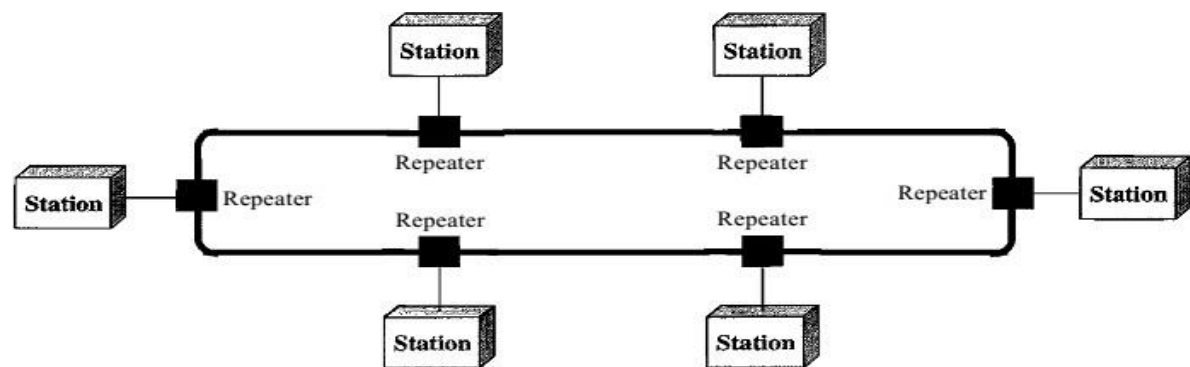
Advantages:
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. The only constraints are media and traffic considerations (maximum ring length and number of devices).

Disadvantage:
1. Unidirectional traffic can be a disadvantage.
2. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

Hybrid Topology

It is a combination of two or more topologies for example star topology with each branch connecting several stations in a bus topology

Station Station Station

Station Station Station

Hub

Station Station Station
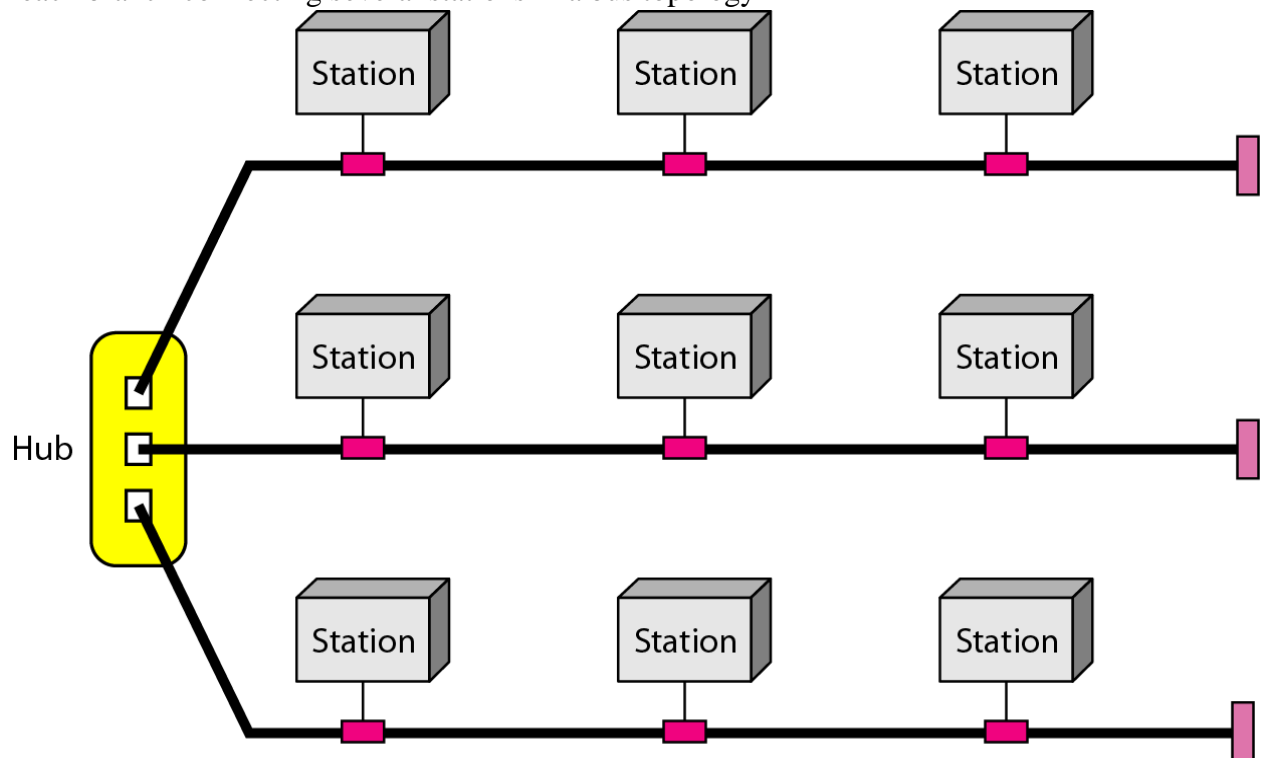
ISO/OSI MODEL:

This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers

The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has seven layers.

The **principles** that were applied to arrive at the seven layers can be summarized as follows:

1. A layer should be created where a different abstraction is needed.

2. Each layer should perform a well-defined function.

3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.
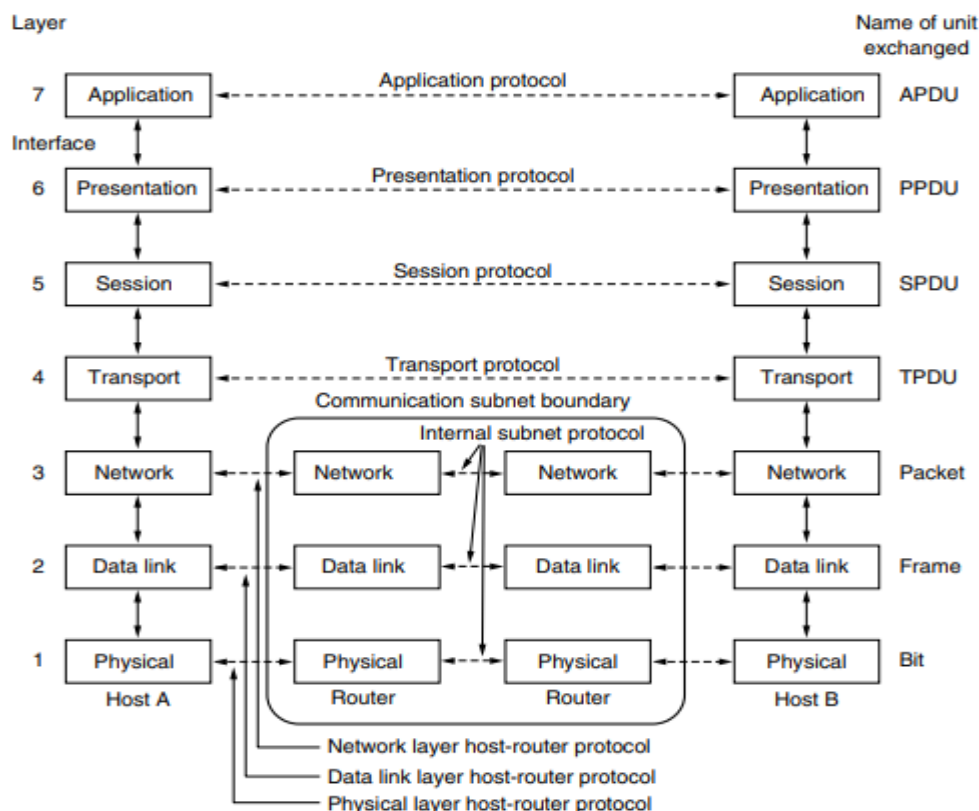
Fig 1: OSI Model

NOTE:

- Layers 1-4 relate to communications technology.

- Layers 5-7 relate to user applications.

Physical Layer
The **Physical Layer** is concerned with transmitting raw bits over a communication channel.

Physical Layer is responsible for:
- It defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
- It also defines the type of transmission medium.
- It defines the data transmission rate, synchronization of data between sender and receiver.
- It defines type of connection (point-to-point or multipoint), type of topology, type of transmission mode, type of dataflow (simplex, half duplex, duplex).
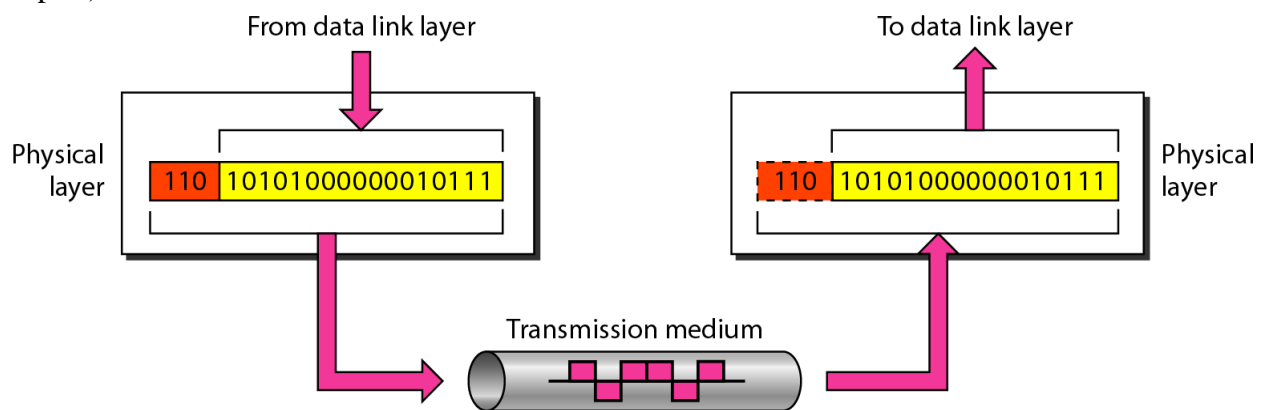
The Data Link Layer
The data link layer is responsible for moving frames from one node to the next node.

The **main task** of the Data link layer is **Error Free Transmission**. At the sender the data link layer break up the input data into **data frames** and transmits the frames sequentially.

Frame is typically a few hundred or a few thousand bytes.

Other responsibilities of the data link layer include the following:
- **Framing** - The data link layer divides the stream of bits received from the network layer into manageable data units called frames
- **Physical addressing -** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and receiver of the frame.
- **Flow control** - If the rate at which the data are received by the receiver is less than the rate at which data sent by the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control** - The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also

uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

- **Access control** - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.
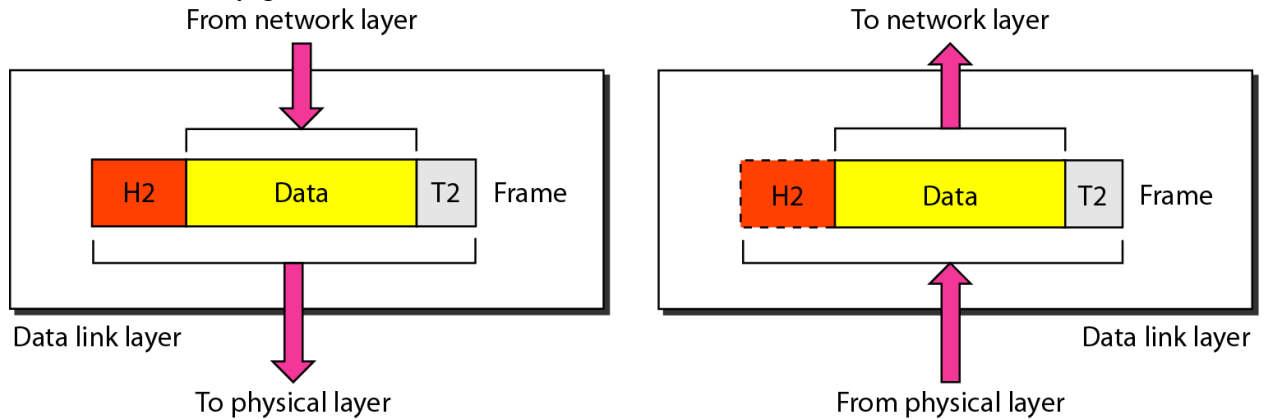
Network Layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host through single or multiple networks.

Note: If two systems are connected to the same network then there is usually no need for a network layer.

If the two systems are connected to different networks with connecting devices between the networks then there is a need for the network layer to accomplish source-to-destination delivery.

Responsibilities of the Network layer include the following:

Logical addressing

- The physical addressing is implemented by Data- link layer, whereas logical addressing is implemented by network layer.
- Data- link layer handles the addressing problem locally, but if packets passes the network boundary there is a need for logical addressing system to help distinguish source and destination systems.
- The network layer adds a header to the packet coming from the upper layer that includes the logical addresses of the sender and receiver.

Routing

- When independent networks or links are connected to create inter- networks (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route the packets to their final destination.

From transport layer / To transport layer

H3 | Data | Packet

Network layer / Network layer

To data link layer / From data link layer
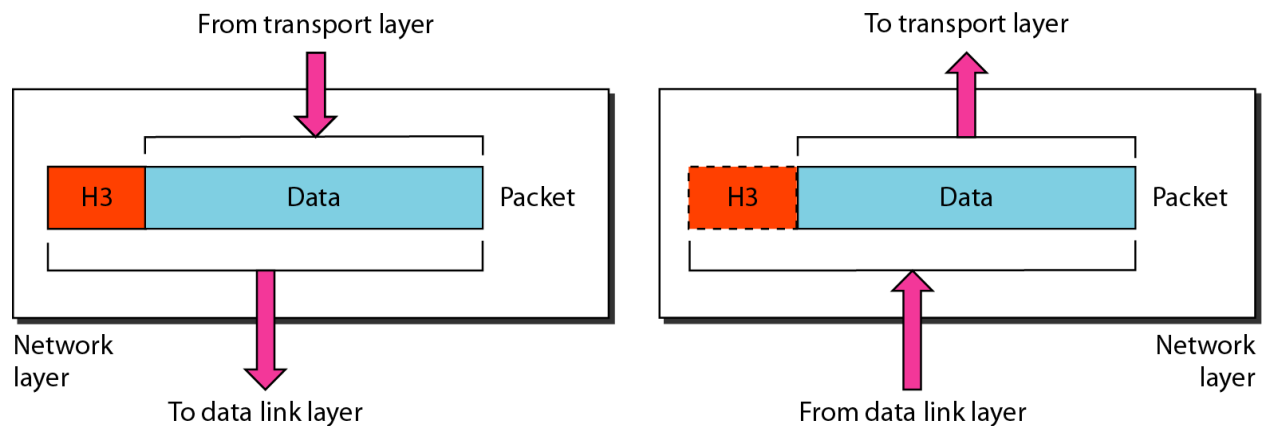
Transport Layer

The transport layer is a true end-to-end layer; it carries from the source to the destination.

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

Responsibilities of the Transport Layer Include:

Port addressing (or) Service point addressing

- Source-to-Destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
- The transport layer header must therefore include a type of address called a *service-point address* (or port address).
- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and Reassembly

- A message is divided into transmittable segments, with each segment containing a sequence number.
- These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and the sequence numbers are used for identifying and replace packets that were lost during transmission.

Connection control

- The transport layer can be either connectionless or connection oriented.
- A **Connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A **Connection-Oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.
- After all the data are transferred, the connection is terminated.

Flow control and Error control

- Like the data link layer, the transport layer is responsible for flow control.
- Flow control at this layer is performed end to end rather than across a single link.
- Like the data link layer, the transport layer is responsible for error control.

- Error control at this layer is performed Process-to-Process rather than across a single link.
- Error control achieved through **Retransmission.**
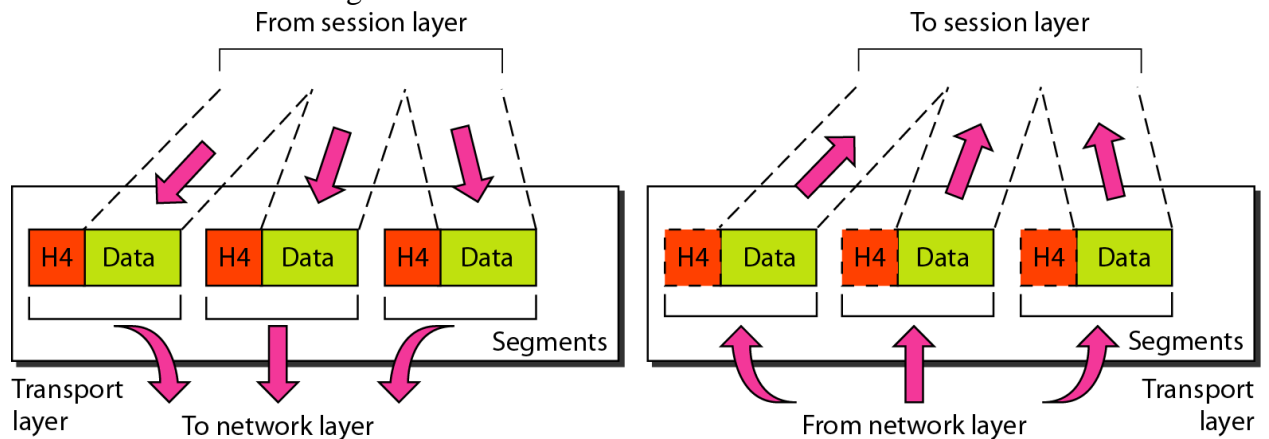
Session Layer

The session layer allows users on different machines to establish **sessions** between them. The session layer is the network *dialog controller.* It establishes, maintains, and synchronizes the interaction among communicating systems.

Responsibilities of the session layer include the following

- **Dialog Control** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. Check-Pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery
- **Token management** prevents two parties from attempting the same critical operation simultaneously.
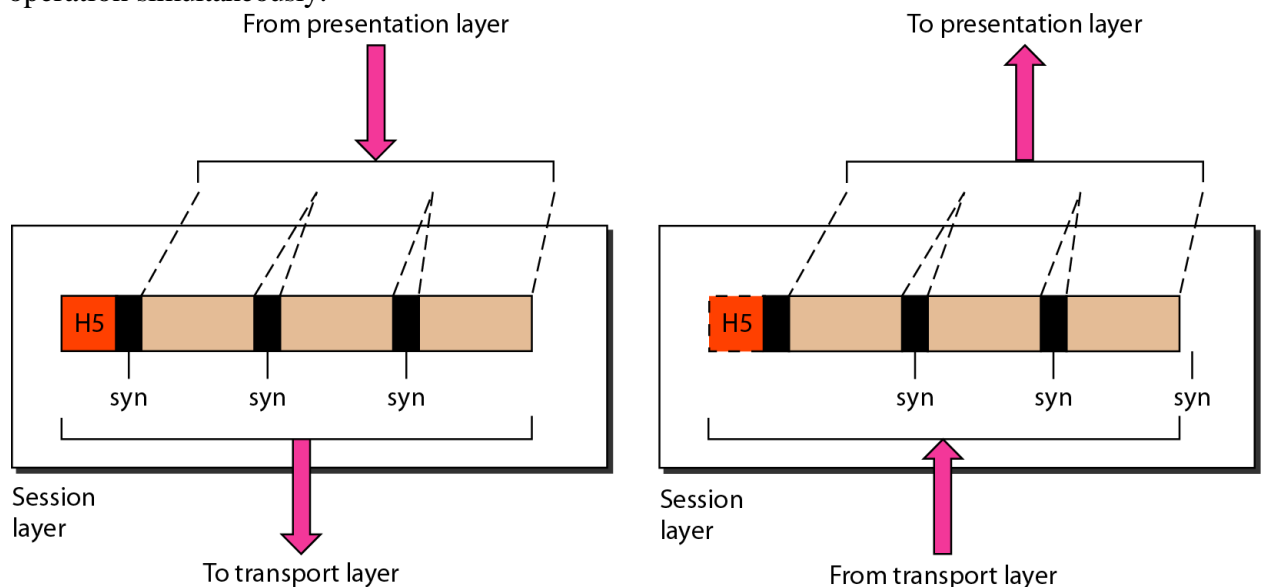
Presentation Layer

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

The presentation layer is responsible for **Translation, Compression, and Encryption**. **Translation**

- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers etc. The information must be changed to bits streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- The presentation layer at the sender changes the information from its sender-dependent format into a common format.
- The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Encryption
- Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.
- Decryption reverses the original process to transform the message back to its original form. Encryption and Decryption is done for privacy of the sensitive information.

Compression
- Data compression reduces the number of bits contained in the information.
- Data compression becomes particularly important in the transmission of multimedia such as text, audio and video.
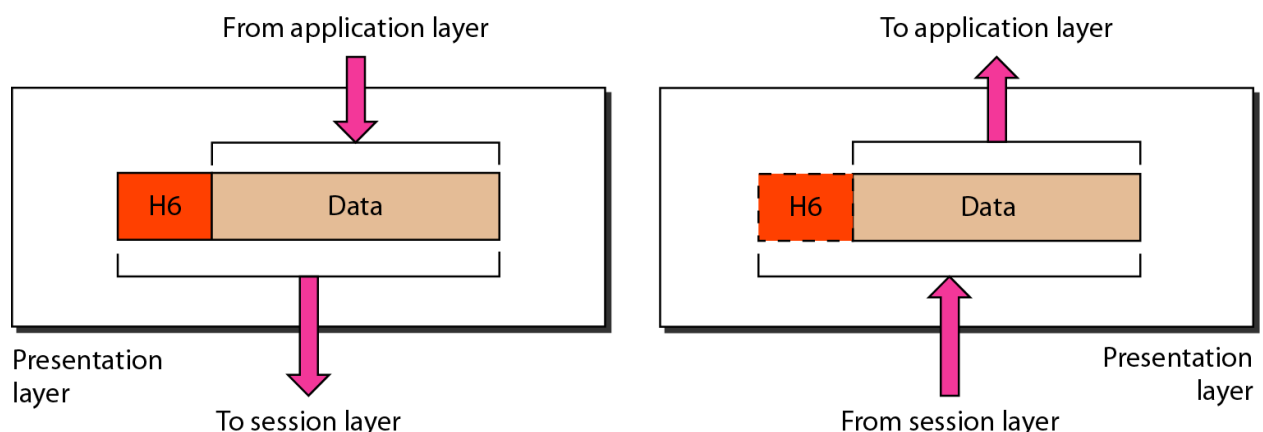
Application Layer

The application layer is responsible for providing services to the user.

The **application layer** contains a variety of protocols that are commonly needed by users. The application layer enables the user to access the network.

Specific services provided by the application layer include the following:
- **A network virtual terminal** is a software version of a physical terminal,

and it allows a user to log on to a remote host.

- **File** transfer, access, and management in a remote host.
- **Mail services** such as email forwarding and mail storage.
- **Directory services** are an application provides distributed database sources and access for global information about various objects and services.

User
(human or program)

X.500   FTAM   ● ● ●   X.400

| H7 | Data | Message

Application
layer

To presentation layer

User
(human or program)

X.500   FTAM   ● ● ●   X.400

| H7 | Data | Message

Application
layer

From presentation layer
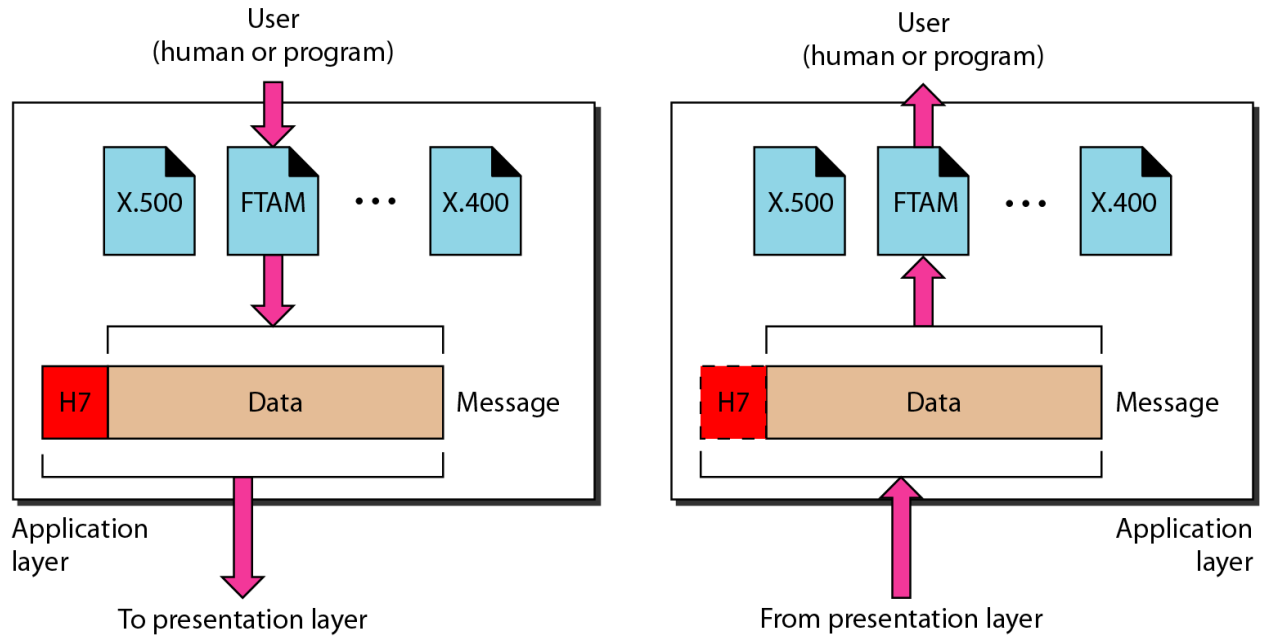
TCP/IP PROTOCOL SUITE

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

The original TCP/IP protocol suite was defined as having four layers:
1. Host-To-Network Layer
2. Internet Layer
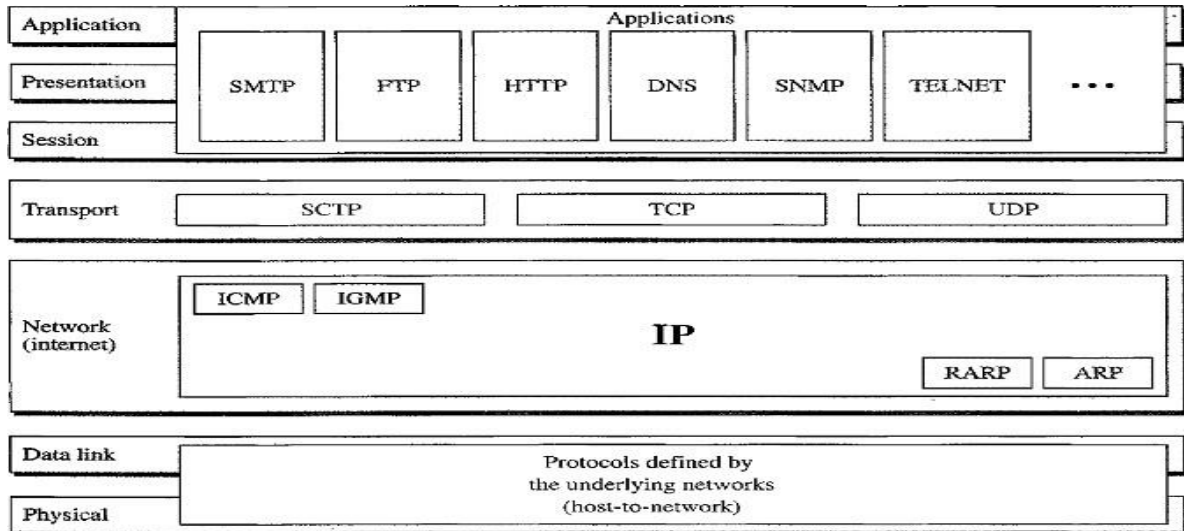3. Transport Layer
4. Application Layer

Layers comparison in TCP/IP and OSI:
- **Host-to-Network** layer is equivalent to the combination of the **Physical** and **Data link** layers.
- The **Internet Layer** is equivalent to the **Network layer**.
- The **Transport layer** is similar in both OSI and TCP/IP, except that in TCP/IP it will take care of part of the duties of the session layer.
- The **Application Layer** is roughly doing the job of the **Session, Presentation** and **Application** layers.

Functionality in TCP/IP and OSI:
- *TCP/IP* is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- **OSI model** specifies which functions belong to each of its layers, the layers of the *TCP/IP* protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term *hierarchical* means that each upper- level protocol is supported by one or more lower-level protocols.

Host-to- Network Layer
- At the Host-to-Network layer is a combination of Physical Layer and Data-link layer in OSI model.
- It is an interface between hosts and transmission links.
- **TCP/IP** does not define any specific protocol. It supports all the standard and proprietary protocols.
- A network in a TCP/IP internetwork can be a local-area network or a wide-area network.

Internet Layer (or) Network Layer
- In this layer *TCP/IP* supports the Internetworking Protocol (IP). The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.
- It is an unreliable and connectionless protocol-a best-effort delivery service.
- The term *best effort* means that IP provides no error checking or tracking.
- The transmission is unreliable (i.e.) there is no guarantee for the data.
- IP transports data in packets called *datagrams,* each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

IP uses four supporting protocols
1. ARP (Address Resolution Protocol)
2. RARP(Reverse Address Resolution Protocol)
3. ICMP(Internet Control Message Protocol)
4. IGMP(Internet Group Message Protocol)

Address Resolution Protocol (ARP)

- ARP is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known.
- On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC).

Reverse Address Resolution Protocol (RARP)

- RARP allows a host to discover its logical address when it knows only physical address.
- It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol (ICMP)

- ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- ICMP sends query and error reporting messages.

Internet Group Message Protocol (IGMP)

- IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer

Transport layer in *TCP/IP* has three protocols:

1. **TCP** (*Transmission Control Protocol)*
2. **UDP**(*User Datagram Protocol)*
3. **SCTP**(Stream Control Transmission Protocol)

Note: UDP and TCP are transport level protocols responsible for delivery of a message from one device to another device, whereas IP is a host-to- host protocol meaning that it can deliver a packet from one physical device to another.

Transmission Control Protocol

- TCP provides full transport- layer services to applications. TCP is a reliable stream transport protocol.
- The term *stream* means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.
- At the sending side for each transmission TCP divides a stream of data into smaller units called *Segments*. Each segment includes a sequence number for reordering at the destination side. Segments are carried across the internet inside of IP datagrams.
- For every segment there is a corresponding acknowledgement to be sent from the destination to the source.
- At the receiving side TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

User Datagram Protocol

- UDP is unreliable, connectionless protocols for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

- It is also widely used for client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

Stream Control Transmission Protocol

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

Application Layer

On top of the transport layer is the **application layer**. It contains all the higher-level protocols such as:

- **Telnet protocol** used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
- **File Transfer Protocol (FTP)** used for file transfer.
- **Simple Mail Transfer Protocol (SMTP)** used for mail services.
- **Domain Name System (DNS)** used for mapping host names onto their network addresses.
- **Hyper Text Transfer Protocol (HTTP)** used for fetching pages on the World Wide Web (WWW).
- **Real-time Transport Protocol (RTP)** used for delivering real-time media such as voice or movies.

TRANSMISSION MODES

Transmission modes are two types:
1. Parallel Transmission
2. Serial Transmission
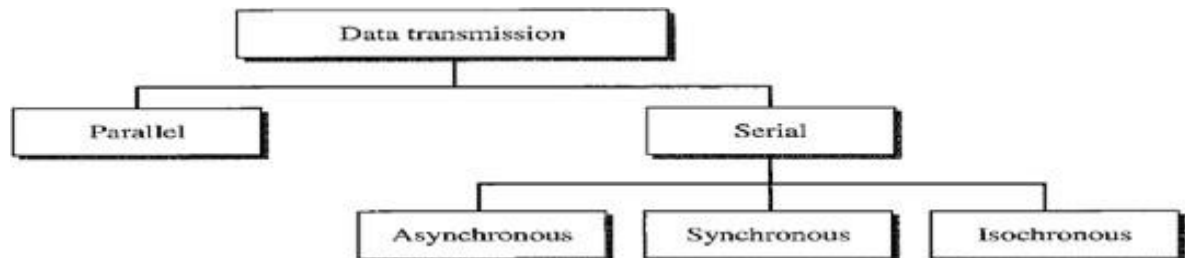
Parallel Transmission

Parallel Transmission is defined as sending n bits of data at a time instead of transmitting one bit at a time.

The mechanism for parallel transmission is a conceptually simple one: Use **n-wires** to send **n-bits** at one time.

Advantage: Speed of the transmission is increased.

Disadvantage : Cost of equipment is increased for this reason parallel transmission is usually limited to short distances.

Serial Transmission

In serial transmission one bit follows another, so we need only one communication channel rather than **n channels** to transmit data between two communicating devices
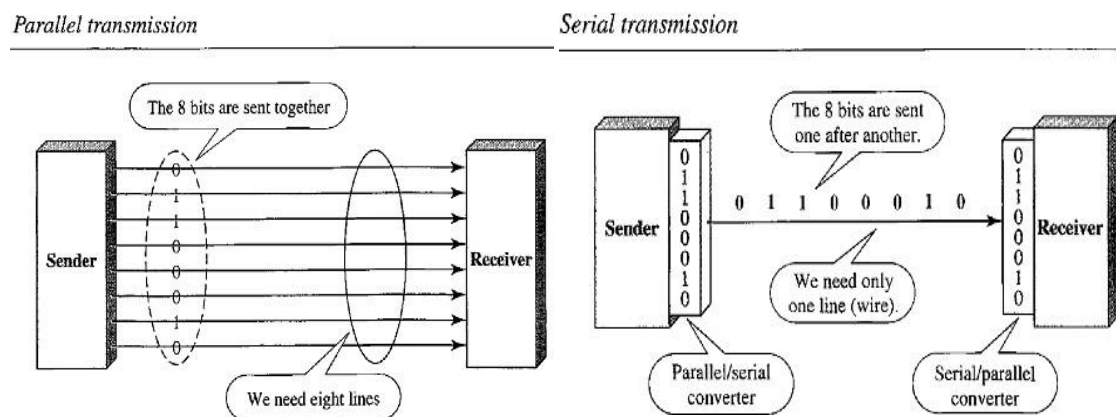
**Advantage:** Reduces the cost transmission equipment because we need only one communication channel.

Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel- to-serial) and between the line and the receiver (serial-to-parallel).

Serial transmission categorized into 3 types:
1. Asynchronous Transmission
2. Synchronous Transmission
3. Isochronous Transmission

Asynchronous Transmission

- The timing of signal is not important in Asynchronous transmission. Information is received and translated by agreed upon patterns.
- As long as those patterns are followed, the receiving device can retrieve the information without regard to the order in which it is sent.
- Patterns are based on grouping the bit stream into bytes. Each group contains 8 bits is sent along the link as a unit.
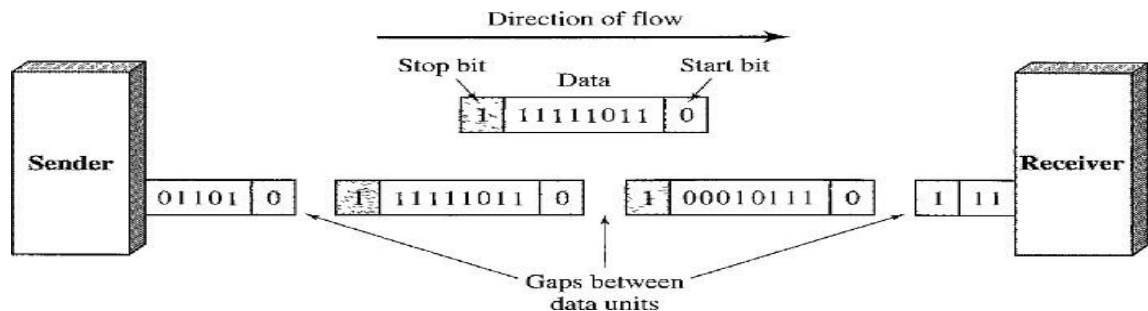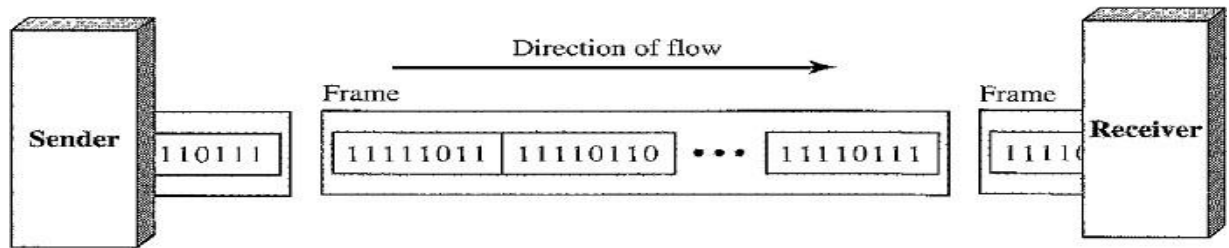

- In asynchronous transmission, we send one start bit (0) at the beginning and one or more stop bits (1's) at the end of each byte. There may be a gap between each byte.
- The start and stop bits are used because the sending system handles each group independently whenever the group is ready it will transmitted through the link.
- Without synchronization, the receiver cannot use timing to predict when the next group will arrive.
- To alert the receiver to the arrival of a new group the extra bits 0 and 1 are added.
- At the receiver side when the receiver detects a start bit, it sets a timer and begins counting bits as they come in. After *n* bits, the receiver looks for a stop bit. As soon as it detects the stop bit, it waits until it detects the next start bit
- **Start** and **Stop** bits and the **Gap** alert the receiver to the beginning and end of each byte and allow it to synchronize with data stream. This mechanism is called **Asynchronous.**
- The transmission is slow because of addition of start, stops and gaps between bit streams. Hence it is used for low speed communications.
- Example: The connection to the keyboard to the computer is application of Asynchronous transmission.
- Apart from slower transmission Asynchronous transmission is cheap and effective.

Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.

That means:

- The bit stream is combined into longer "**Frames**," which may contain multiple bytes.
- Each byte is introduced onto the transmission link without a gap between the byte and the next byte.
- It is left to the receiver to separate the bit stream into bytes for decoding purposes.
- Data are transmitted as an unbroken string of 1s and 0's, and the receiver separates that string into the bytes, or characters and receiver needs to reconstruct the information.

In synchronous transmission **Timing** plays very crucial role. When the information comes from sender, the receiving device **accurately count the bits** and group them into 8 bits because we don't have any extra bits to identify starting and ending of byte. This process is called **Byte Synchronization**.

Advantage: Speed of the transmission is increased as compared to Asynchronous transmission because there are no extra bits to be add or remove at the sender side and receiver side respectively.

It is useful for **High Speed Application** such as transmission of data from one computer to another computer.

Note:

1. Byte Synchronization is accomplished at Receiver side.
2. Although there is no gap between characters in synchronous serial transmission, there may be uneven gaps between frames.

Isochronous Transmission
- The isochronous transmission guarantees that the data arrive at a fixed rate.
- In real- time audio and video, in which synchronous transmission fails such as uneven delays between frames, are not acceptable.
- **For example**, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames.
- For this type of application, synchronization between characters is not enough; the entire stream of bits must be synchronized.

Multiplexing

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

As data and telecommunications use increases the data traffic is also increases.

We can accommodate this increase by continuously adding the individual links each time a new channel is needed, or we can install higher-bandwidth links and use each to carry multiple signals.
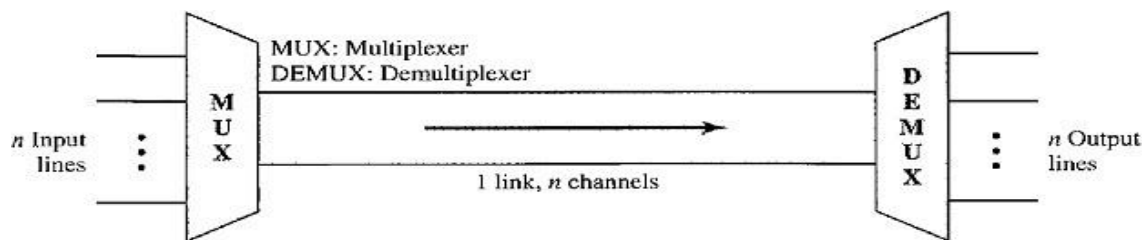

Fig: Dividing the link into channels

In a multiplexed system, *n* lines share the bandwidth of one link.
- **Link** refers to the physical path.
- **Channel** refers to the portion of a link that carries a transmission between a given pair of lines.
- The lines on the left direct their transmission streams to a **Multiplexer (MUX)**, which combines them into a single stream (many-to-one).
- At the receiving end, that stream is fed into a **Demultiplexer (DEMUX)**, which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.

Multiplexing is categorized into 3 types:
1. Frequency Division Multiplexing
2. Wavelength Division Multiplexing
3. Time Division Multiplexing
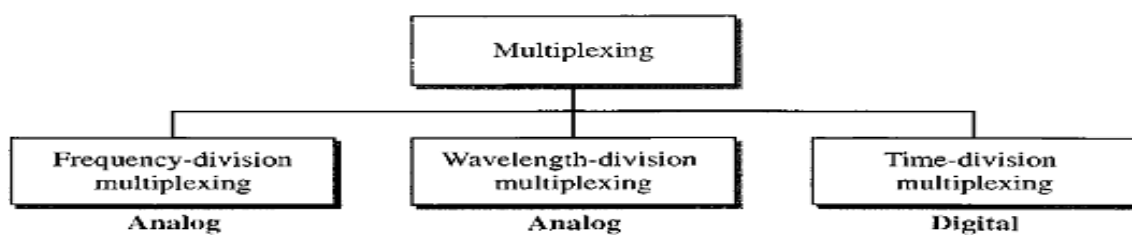
Frequency Division Multiplexing(FDM)

FDM is an analog multiplexing technique that combines analog signals.

That means:
- FDM is an analog technique that can be applied when:
  Bandwidth of link (in Hz) >= Combined bandwidth of the signal to be transmitted.
- In FDM, signals generated by each sending device modulate different carrier frequencies.
- These modulated signals are then combined into a single composite signal

that can be transported by the link.

- **Carrier frequencies** are separated by sufficient bandwidth to accommodate the modulated signal.
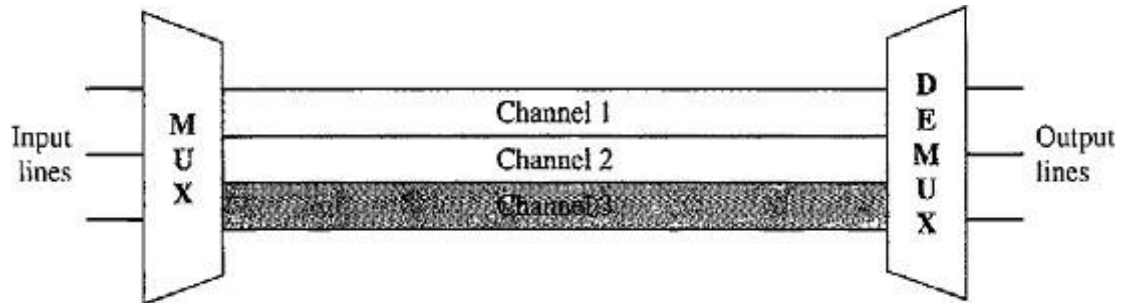- These bandwidth ranges are the channels through which the various signals travel.

Fig: Frequency Division Multiplexing

In the above figure, the transmission path is divided into three parts, each representing a channel that carries one transmission.

Multiplexing Process

- Each source generates a signal of a similar frequency range.
- Inside the multiplexer, these similar signals modulate different carrier frequencies (f1, f2, f3).
- The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

Wavelength-Division Multiplexing (WDM)

- WDM is an analog multiplexing technique to combine optical signals. WDM is designed to use the high-data-rate capability of fiber-optic cable.
- The optical fiber data rate **higher than** the data rate of metallic transmission cable
- Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.
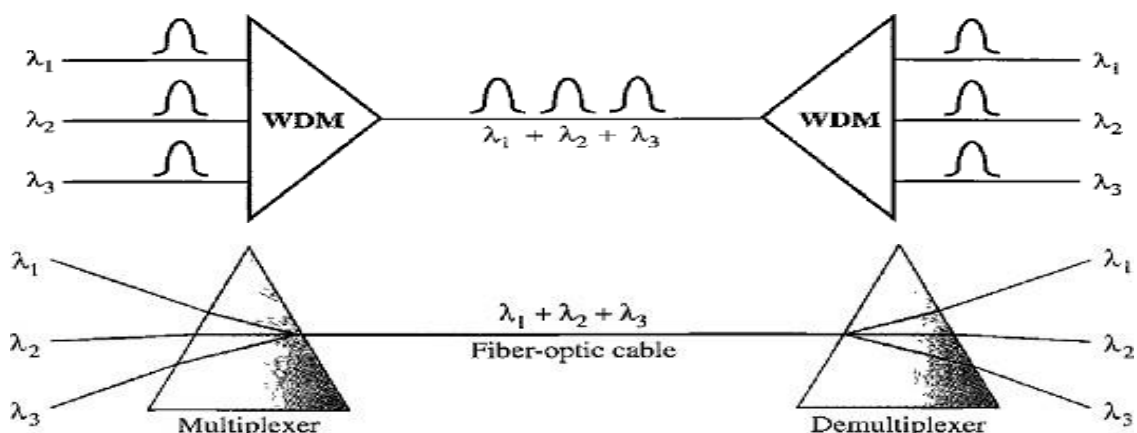
- Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.

- A demultiplexer can be made to divide wider band of frequencies by decomposing the light beams into narrow band frequencies.

Advantages: High Speed and High frequency, uses narrow bands of light sources.

Disadvantages: Expensive than FDM.

Time-Division Multiplexing (TDM)

TDM is a digital multiplexing technique for combining several low-rate channels into one high-rate channel. Digital data from different sources are combined into one timeshared link

(i.e.) The **data rate** capacity of transmission medium **>=** The **data rate** required by sending and receiving devices.

TDM is a digital process that allows several connections to share the high bandwidth of a link. Each connection occupies a portion of time in the link.
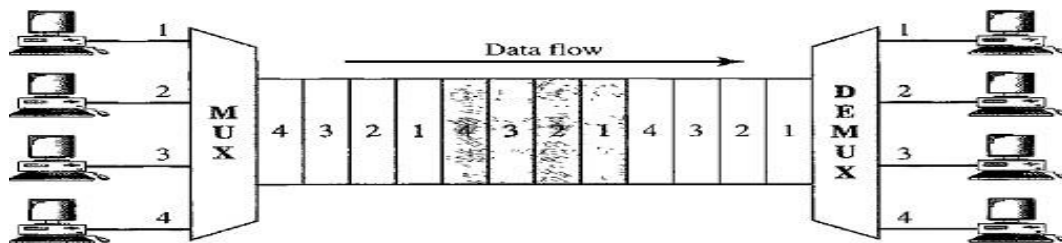
In the above figure all the data in a message from source 1 always go to one specific destination either of 1, 2, 3, or 4. The delivery is fixed and unvarying.

TRANSMISSION MEDIA

Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. In data communications the information is usually a signal.

Transmission media can be categorized into following ways:
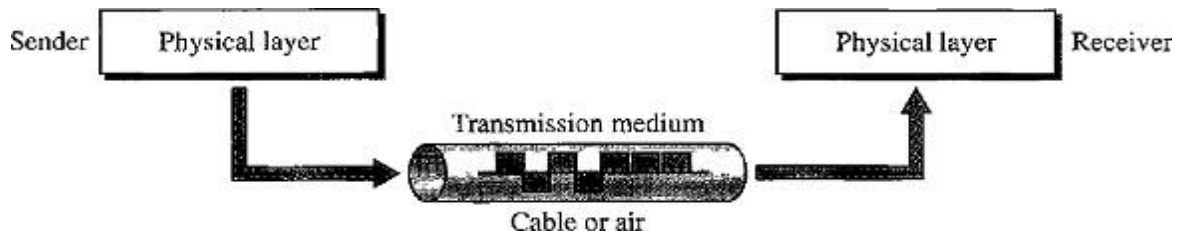- **Guided or Wired Media**: Twisted pair cable, Coaxial cable, Fiber Optic cable.
- **Unguided or Wireless Media**: Radio Waves, Micro waves, Infrared Waves.
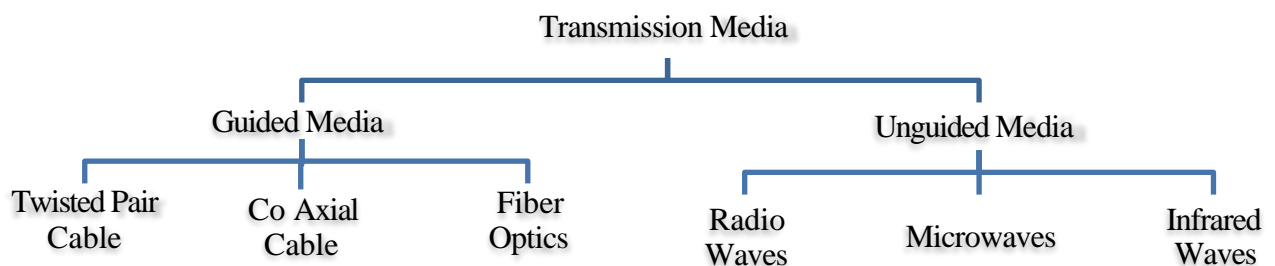
Guided or Wired Media

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

Twisted-Pair Cable

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

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.
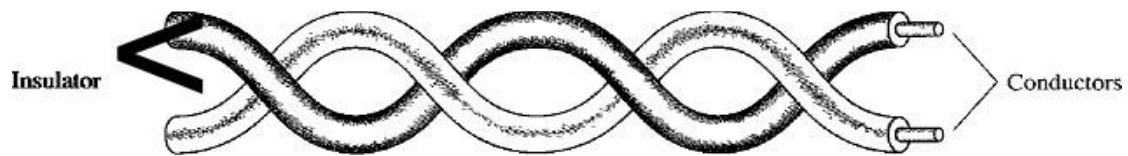
The signal sent by the sender on one of the wires, interference (noise) and crosstalk mayaffect both wires and create unwanted signals.

a. UTP

b. STP
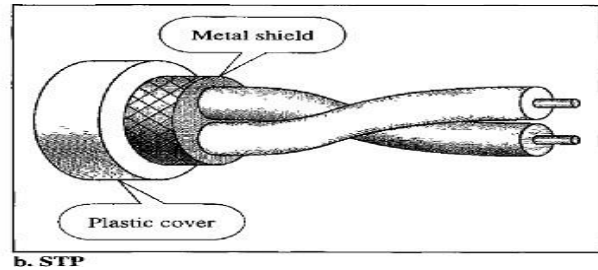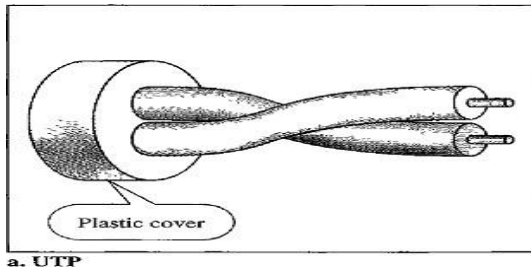
STP v/s UTP

Shielded Twisted Pair (STP) cable has a **metal foil** or braided mesh covering that encases each pair of insulated conductors. A twisted-pair cable can pass a wide range of frequencies. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Unshielded Twisted pair (UTP) cables don't have the metal foil covering the cables. The most common UTP connector is RJ45 (Registered Jack45).

Applications

- Twisted-pair cables are used in telephone lines to provide voice and data channels. Most widely used in Internet connections.
- The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

Note: When there is an electric signal interference UTP signal performance is degraded.

Hence we use STP, the shield protects from interference of electric signals.

Coaxial Cable (Coax)

Coaxial cable carries signals of higher frequency ranges than those in twisted pair cable.
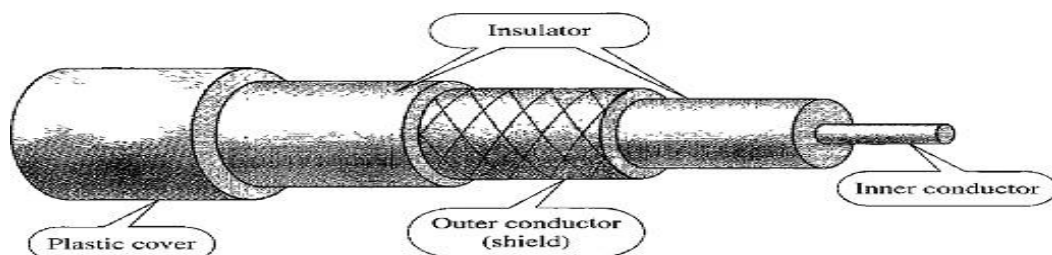
- Coaxial cable has a central core conductor of copper wire enclosed in an insulating sheath.
- Insulating sheath encased in an outer conductor of metal foil.
- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications.

Category	Impedance	Use
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications
Coaxial cable was widely used in analog telephone networks, digital telephone networks, Cable TV networks, Ethernet LAN.

Fiber-Optic Cable
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable.
- Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.
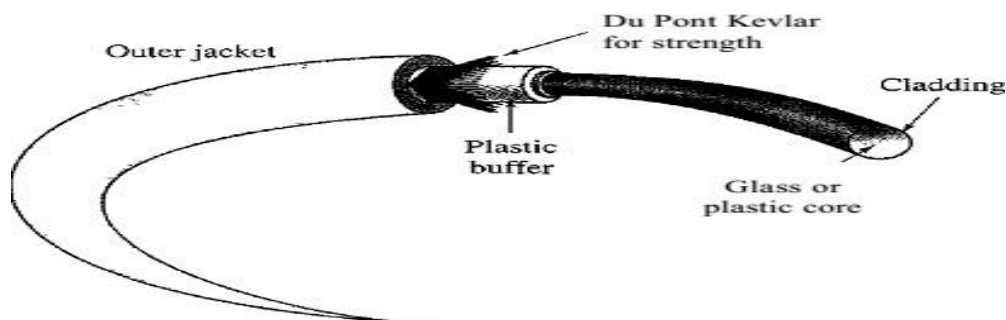
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.
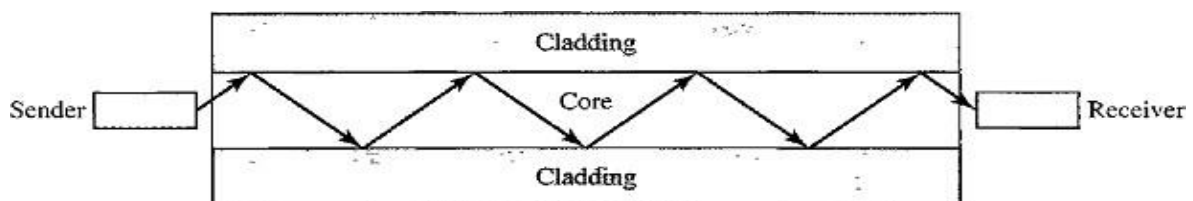
Propagation Modes
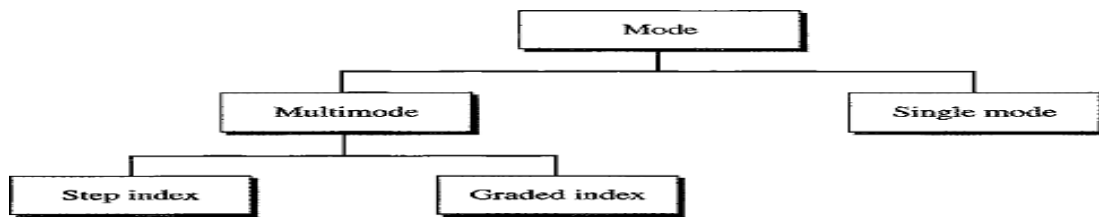
Multimode Propagation

In this mode multiple beams from a light source move through the core in different paths.

Multimode Step-Index Fiber:

- The density of the core remains constant from the center to the edges.
- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion.
- The term *step index* refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

Multimode Graded-Index Fiber:

- It decreases the distortion of the signal through the cable.
- The word *index* here refers to the index of refraction.
- The index of refraction is related to density. A graded- index fiber is one with varying densities.
- Density is highest at the center of the core and decreases gradually to its lowest at the edge.
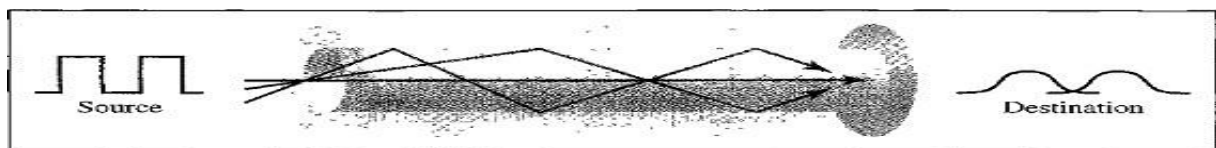
a. Multimode, step index
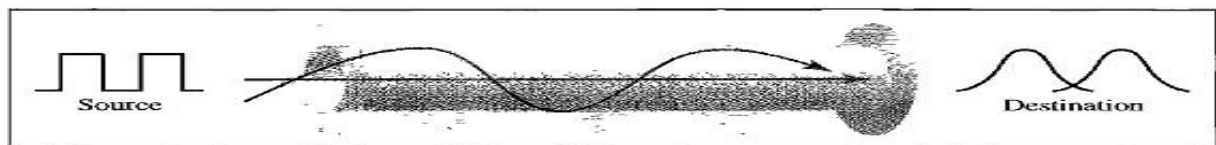
b. Multimode, graded index
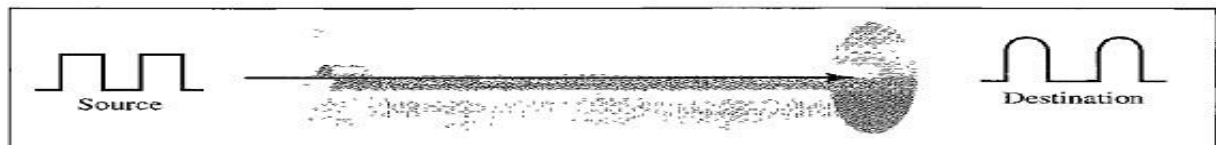
c. Single mode

Single-Mode Fiber:

- It uses step- index fiber and a highly focused source of light that limits beams to a small range of angles close to the horizontal.
- The single mode fiber is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction).

- The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal.
- In this case, propagation of different beams is almost identical, and delays are negligible.
- All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.

Fiber Optic Cable Connectors

- The **subscriber channel** (SC) **connector** is used for cable TV. It uses a push/pull locking system.
- The **straight-tip** (ST) **connector** is used for connecting cable to networking devices.

Performance: The performance is such that we need 10 times less repeaters when we use fiber-optic cable.

Application: Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.

<u>**Advantages**</u>

Fiber-optic cable has several advantages over metallic cable Twisted pair or coaxial.

- **Higher bandwidth**. Fiber-optic cable can support higher bandwidths than either twisted- pair or coaxial cable.
- **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- **Immunity to electromagnetic interference** .Electromagnetic noise cannot affect fiber- optic cables.
- **Resistance:** Glass is more resistant to corrosive materials than copper.
- **Light weight.** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping**: Fiber-optic cables are more immune to tapping than copper cables.

<u>**Disadvantages**</u>

- **Installation and maintenance:** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation**: Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost:** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high the use of optical fiber cannot be justified.

UNGUIDED MEDIA(or) WIRELESS COMMUNICATION

Unguided media transport **Electromagnetic Waves** without using a physical conductor. This type of communication is often referred to as wireless communication. Electromagnetic spectrum ranging from **3 kHz to 900 THz** used for wireless communication.
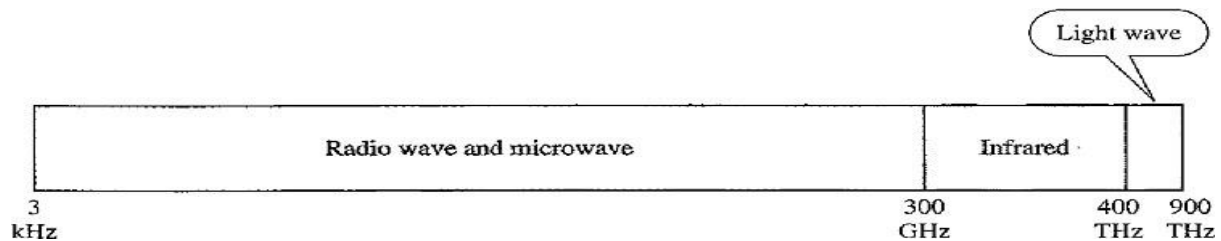
Categories of Wireless Communication:

- Radio Waves (3kHz –1GHz)
- Microwaves (1GHz- 300 GHz)
- Infrared Waves (300 GHz - 400 THz)
  Propagation Methods:
  - In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.
  - In sky propagation, higher-frequency radio waves radiate upward into the ionosphere where they are reflected to earth. This type of transmission allows for greater distances with lower output power.
  - In line-or-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.
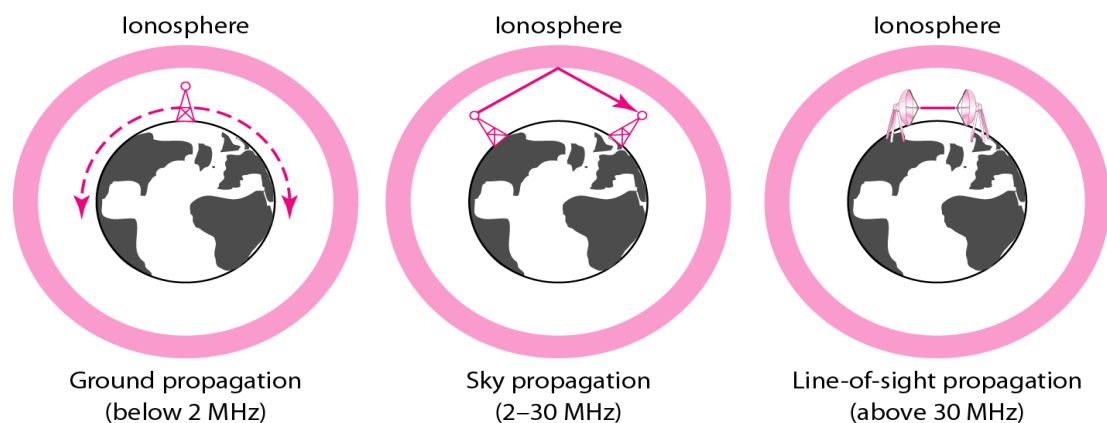
Radio Waves

- Radio waves ranges between 3 kHz and 1 GHz. Radio waves are Omni-directional.
- When an antenna transmits radio waves, they are propagated in all directions. Hence the sending and receiving devices don't have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves can travel long distances, hence it is used in long distance AM Radio broadcasting.
- Radio waves of low and medium frequencies can penetrate walls.

Disadvantage

- The Omni-directional property has a **disadvantage**; the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

- Radio waves leads to low data rate for digital communication.

Applications

- Radio waves are used in Multicasting applications such as AM Radio and FM radio, Television, Maritime Radio, Cordless Phones, and Paging.

Micro waves

- Electromagnetic waves having frequencies between 1GHz and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned.
- Microwaves need unidirectional antennas that send out signals in one direction.Two types of antennas are used for microwave communications: the parabolic dish and the horn.
- Microwave propagation is line-of-sight. Repeaters are often needed for long distance communication.
- Higher data rates are possible due to assigning of wider sub-bands.

Advantage

The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

Disadvantage

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

Applications

Microwaves used in Uni-casting communication between sender and receiver such as cellular phones, satellite networks and wireless LANs.

Infrared Waves

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication upto few meters.

Advantages

Infrared waves having high frequencies cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

Disadvantage

- We cannot use Infrared waves for long range communication.
- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

- Due to its wide bandwidth, it can be used to transmit digital data at high data rate.
- It can be used in Communication between devices such as keyboards, mice, PCs, and printers

Data Link Layer

The responsibility of the **Physical Layer** is to transmit the unstructured raw bit stream over a physical medium.

The responsibility of **Data-Link Layer** is to transforming raw transmission facility into a **Link** responsible for node-to-node communication (hop-to-hop communication).

Responsibilities of the Data Link Layer include:
1. Framing
2. Physical Addressing
3. Flow control
4. Error control
5. Media Access Control.

Framing

The data link layer divides the stream of bits received from the network layer into manageable data units called frames. In simple terms data link layer is responsible for moving frames from one node to another node.

Physical Addressing

The data link layer adds a header to the frame to define the addresses of the sender and receiver of the frame.

Flow Control

If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error Control

The data link layer also adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate, or lost frames.

Media Access Control

When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Framing

- Framing in the data link layer is breaking up the bit stream into frames.
- Framing can be done in 2ways:
- **Fixed size framing:** The size of the frame is fixed for all the frames. There is no need to define the boundaries of a frame.
- **Variable size framing:** In variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.

There are 2 approaches are used for variable size framing:
1. Character Stuffing(A Character-Oriented Approach)
2. Bit Stuffing(A Bit-Oriented Approach)

Character Stuffing/Byte Stuffing

In a character stuffing, data to be carried are 8-bit characters from a coding system such as ASCII. The Frame format in Character Stuffing is given below:
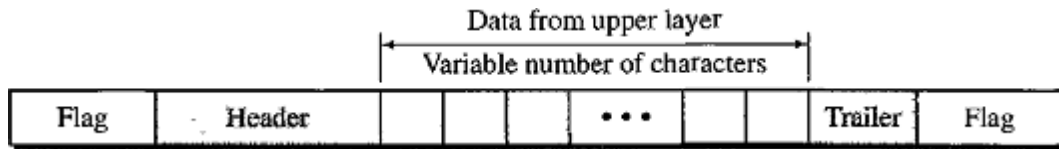
Character Stuffing uses: Header, Trailer and a Flag.

- **Header** carries the source and destination addresses and other control information.
- **Trailer** carries error detection or error correction redundant bits, are also multiples of 8 bits.
- To separate one frame from the next, an 8-bit (I-byte) flag is added at the beginning and the end of a frame. The flag signals receiver either start or end of a frame.

Disadvantages of Character Stuffing

- Character oriented framing is useful for text transfer not useful for audio video etc.
- Any pattern used for the flag could also be part of the information.
- If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame and the treats then exit bit as new frame.

To fix this problem a **Byte Stuffing** strategy is introduced.

- In byte stuffing a special byte is added to the data section of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte called Escape character (ESC).
- Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Figure shows the byte stuffing and Unstuffing:
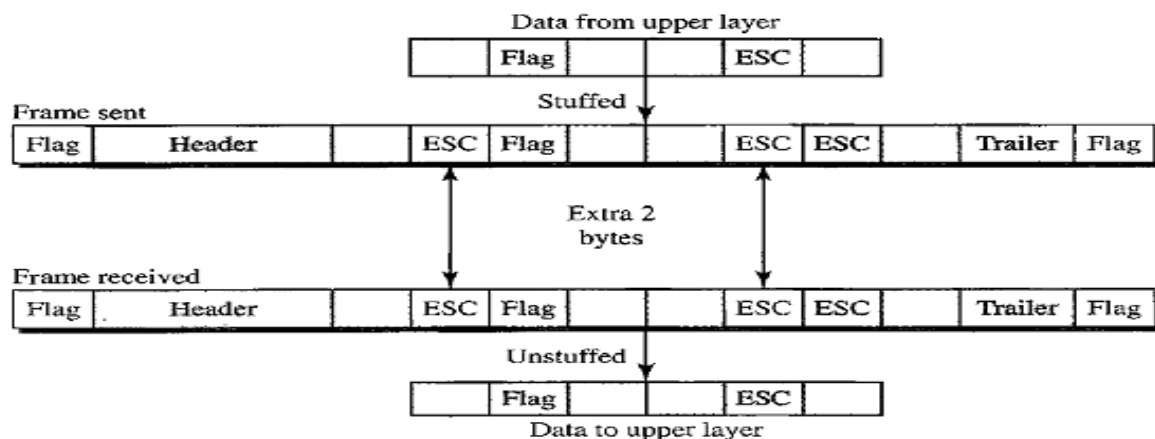
Problems with Byte Stuffing

- If the text contains one or more escape characters followed by a flag, the receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame.

Solution

- To solve this problem, the escape characters that are part of the text must also be marked by another escape character.

Disadvantages of character/Byte stuffing Procedure

- The universal coding systems (Unicode) in use today have16-bit and 32-bit characters that conflict with 8-bit characters.
- Character stuffing deals with 8-bit characters but today's systems using 16 bits, 32 bits and 64 bit characters hence there will be conflict.

The solution for this problem is using **Bit Oriented Approach.**

Bit_stuffing

- In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on.
- In addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other.
- Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame is give below figure:

- In bit stuffing, if a 0 and five consecutive1-bits are encountered, an extra0 is added.
- This extra stuffed bit is eventually removed from the data by the receiver.

Note: the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. (i.e.) when 0**11111**00 is a part of the data, then also we have to add "0" after five 1"s .Hence the data will be 0**11111**000
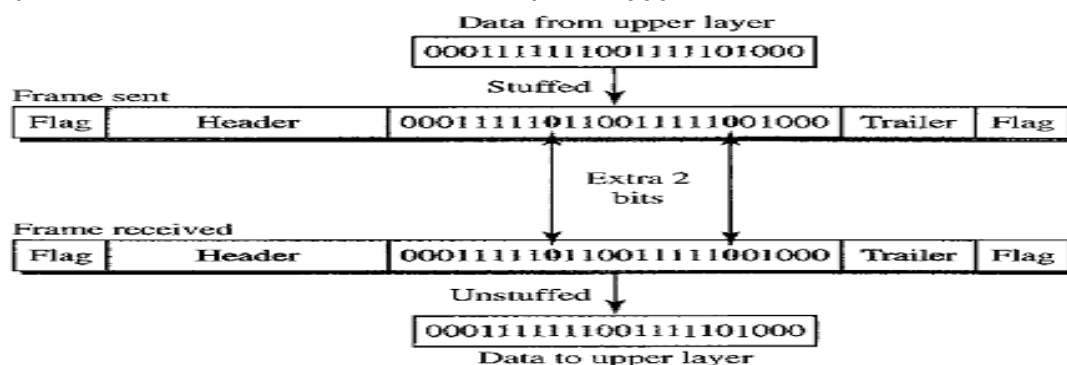
Advantages of Bit Stuffing

If the flag like pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken as a flag by the receiver. The real flag 01111110 is not stuffed by the sender and is recognized by the receiver.

Error is a condition when the receiver's information does not match the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Error Detection:
To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

1. **Checksum**

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum – Operation at Sender's Side
- Firstly, the data is divided into k segments each of m bits.
- On 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.

Checksum – Operation at Receiver's Side
- 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.
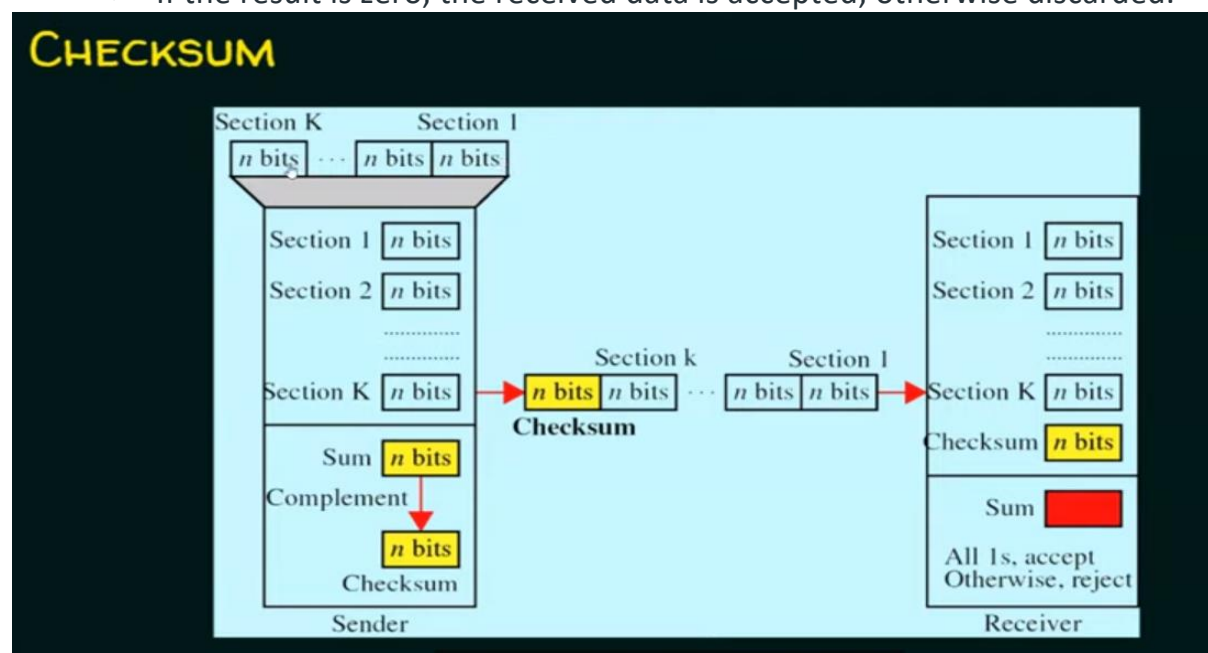
Example:

The first step is to perform the bit addition of the given data bits at the sender side.

Sender Side:

1	0	0	1	1	0	0	1
1	1	1	0	0	0	1	0
0	0	1	0	0	1	0	0
1	0	0	0	0	1	0	0

0	0	1	0	0	0	1	1
						1	0

0	0	1	0	0	1	0	1

Note: The extra carry bits are added to the summation result.

2. Perform the 1's Complement for the bit addition result, thus obtaining the checksum value.

Sender Side:

0	0	1	0	0	1	0	1

1's Complement

⬇

Checksum	1	1	0	1	1	0	1	0

3. Integrate the checksum value and the original data bit and begin the data transmission to the receiver.

11011010	10011001	11100010	00100100	10000100

4. The receiver side will begin the Checksum Checker method, repeat the bit addition, and perform the 1's complement.

Receiver Side:

1	0	0	1	1	0	0	1
1	1	1	0	0	0	1	0
0	0	1	0	0	1	0	0
1	0	0	0	0	1	0	0
1	**1**	**0**	**1**	**1**	**0**	**1**	**0**

1	1	1	1	1	1	0	1
						1	0

1	1	1	1	1	1	1	1

5. If the complement result is 0, the data received is correct and without any error.

Receiver Side:

1	1	1	1	1	1	1	1

1's Complement

Checksum	0	0	0	0	0	0	0	0

Result: No error in the data received from the sender side.

1's Complement

Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

  Design:
- **In** the encoder, the data word has **k bits** and the codeword has **n bits**.
- The size of the data word is augmented by adding **(n−k)number of 0's** to the right-hand side of the word.
- The **n-bit** result is fed into the generator.
- The generator uses a divisor of size **n-k+1** predefined and agreed by both the sender and receiver.
- The generator divides the augmented data word by the divisor **(modulo-2 division)**.
- **The quotient of the division is discarded;**
- **The remainder ($r_2r_1 r_0$)is appended to the dataword to create the codeword.**

Polynomials:
- A pattern of Os and 1s can be represented as a polynomial with coefficients of 0 and 1. The power of each term shows the position of the bit; the coefficient shows the value of the bit.

Figure 10.21 *A polynomial to represent a binary word*

| 1 | 0 | 0 | 0 | 0 | 1 | 1 |

$$1x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + Ix^1 + Ixo$$

a. Binary pattern and polynomial

| 1 | 0 | 0 | 0 | 0 | 1 | 1 |

$$x^6 + x + 1$$

b. Short form
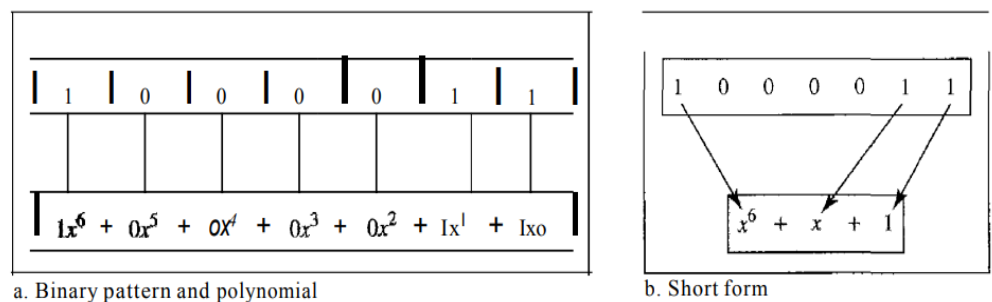
Example:

- **Let us take k=4 bits n=7 bits**
- **Appended Dataword Size = (n-k) = 3.**
- **Divisor Size=(n-k+1)=4.**

Example:

Codeword 1 0 0 1 | 1 1 0

Division

```
          1 0 1 0
1 0 1 1 ) 1 0 0 1 1 1 0   ← Codeword
          1 0 1 1
          0 1 0 1
          0 0 0 0
            1 0 1 1
            1 0 1 1
              0 0 0 0
              0 0 0 0
                0 0 0   Syndrome
```

Dataword accepted 1 0 0 1

Codeword 1 0 0 0 | 1 1 0

Division

```
          1 0 1 0
1 0 1 1 ) 1 0 0 0 1 1 0   ← Codeword
          1 0 1 1
          0 1 1 1
          0 0 0 0
            1 1 1 1
            1 0 1 1
              1 0 0 0
              1 0 1 1
                0 1 1   Syndrome
```

Dataword discarded

Example 2:

original message
1 0 1 0 0 0 0

@ means X-OR

Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1 0 0 1   4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001 | 1010000 000
@1001
      0011000000
      @1001
        01010000
        @1001
          0011000
          @1001
            01010
            @1001
              0011
```

Message to be transmitted

1 0 1 0 0 0 0 000
        + 0 1 1
1 0 1 0 0 0 0 1 1

```
1001 | 1010000011
@1001
      0011000011
      @1001
        01010011      ← Receiver
        @1001
          0011011
          @1001
            01001
            @1001
              0000
```

Zero means data is accepted

<u>**Error Correction**</u>:

Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver.

Redundant bits – Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:
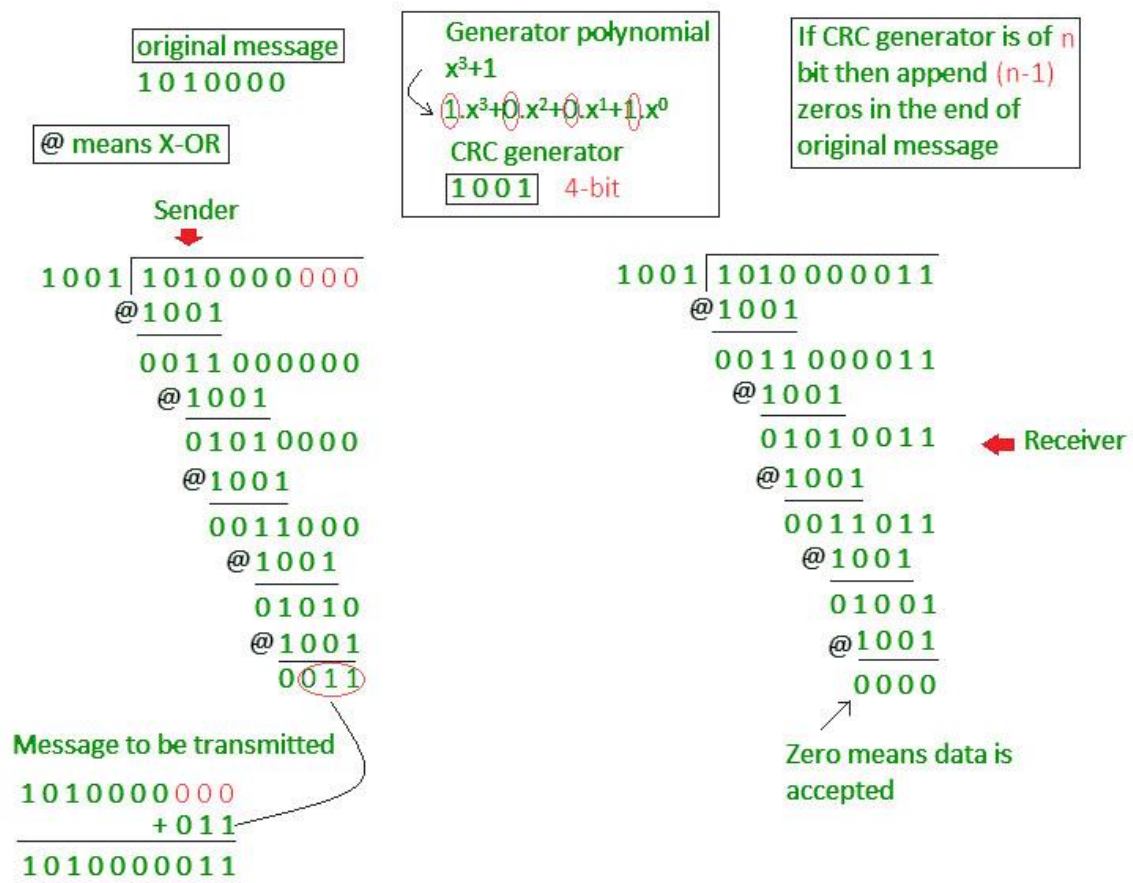
```
2^r ≥ m + r + 1
 where, r = redundant bit, m = data bit
```

m=7

$2^4 \geq 7 + 4 + 1$ Thus, the number of redundant bits= 4 **Parity bits.**

There are two types of parity bits:

1. **Even parity bit:** In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.
2. **Odd Parity bit –** In the case of odd parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

General Algorithm of Hamming code: Hamming Code is simply the use of extra parity bits to allow the identification of an error.
1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form. **a.** Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc). **b.** Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc). **c.** Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc). **d.** Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47,

etc). **e.** In general, each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

| Position	R8	R4	R2	R1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1

R1 -> 1,3,5,7,9,11
R2 -> 2,3,6,7,10,11
R3 -> 4,5,6,7
R4 -> 8,9,10,11

Determining the position of redundant bits – These redundancy bits are placed at positions that correspond to the power of 2.
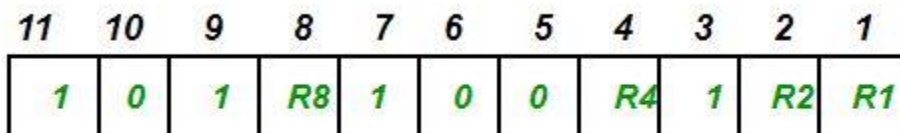As in the above example:

- The number of data bits = 7

- The number of redundant bits = 4
- The total number of bits = 11
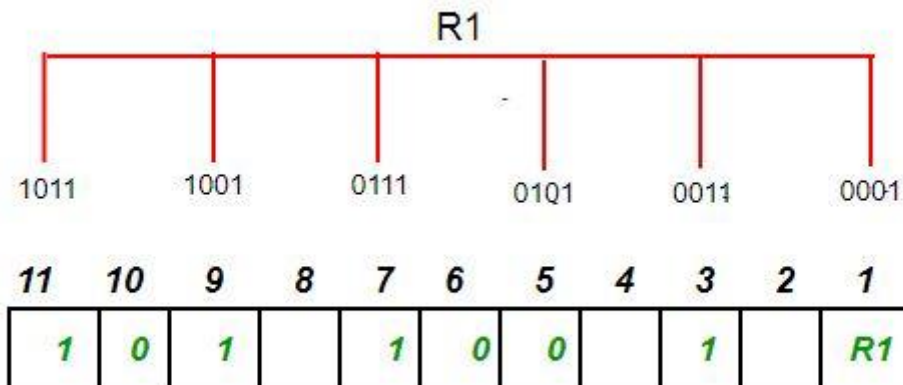- The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8

11	10	9	8	7	6	5	4	3	2	1
D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1

Redundant bits
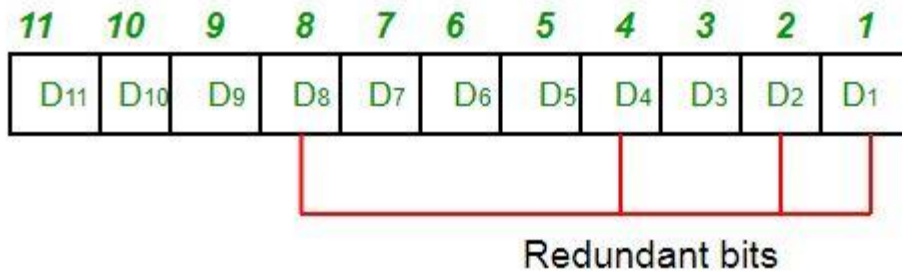
- Suppose the data to be transmitted is 1011001, the bits will be placed as follows:

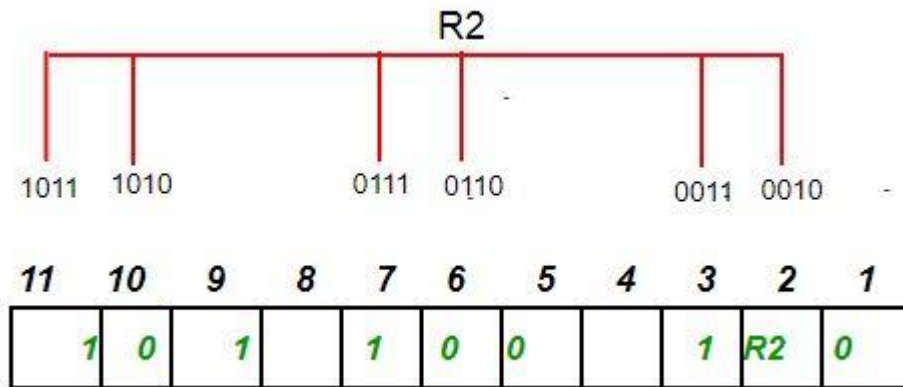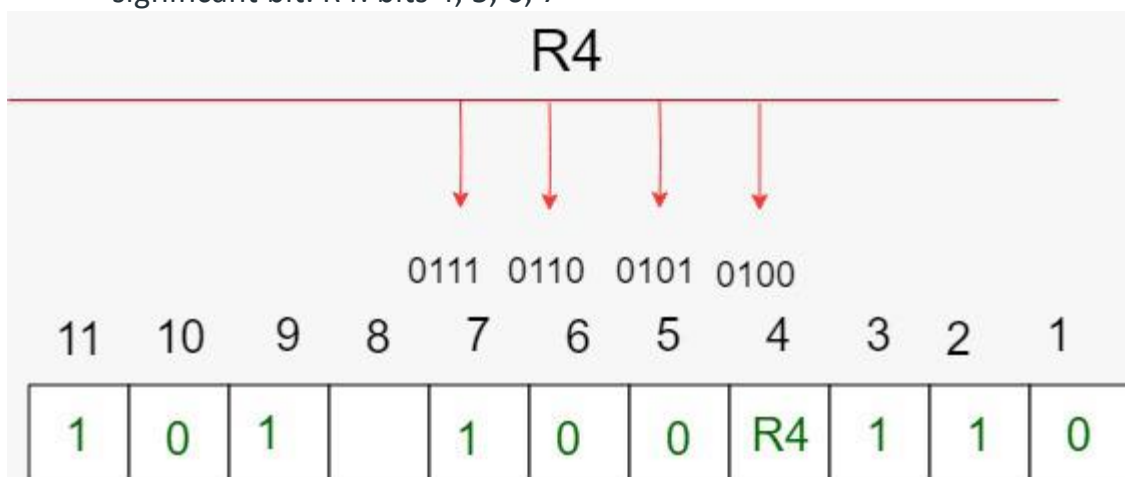| 11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	R4	1	R2	R1

Determining the Parity bits:

- R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position. R1: bits 1, 3, 5, 7, 9, 11

R1

| 1011 | 1001 | 0111 | 0101 | 0011 | 0001 |

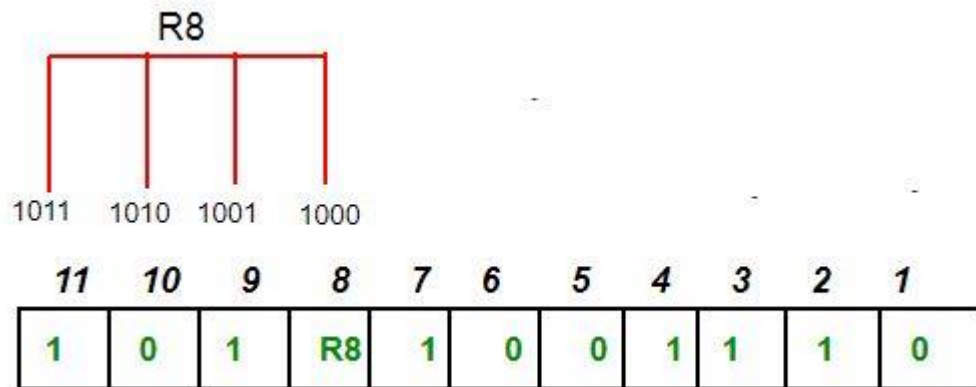| 11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1		R1

- To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0
- R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit. R2: bits 2,3,6,7,10,11

3

R2

| 1011 | 1010 | | | 0111 | 0110 | | | 0011 | 0010 | - |

11	10	9	8	7	6	5	4	3	2	1
	1	0	1		1	0	0		1	R2	0

- To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1
- R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit. R4: bits 4, 5, 6, 7

R4

0111 0110 0101 0100

| 11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0	R4	1	1	0

1. To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1
2. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit. R8: bit 8,9,10,11

	R8									

1011 1010 1001 1000

11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	1	1	1	0

- To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0. Thus, the data transferred is:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Error detection and correction: Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:
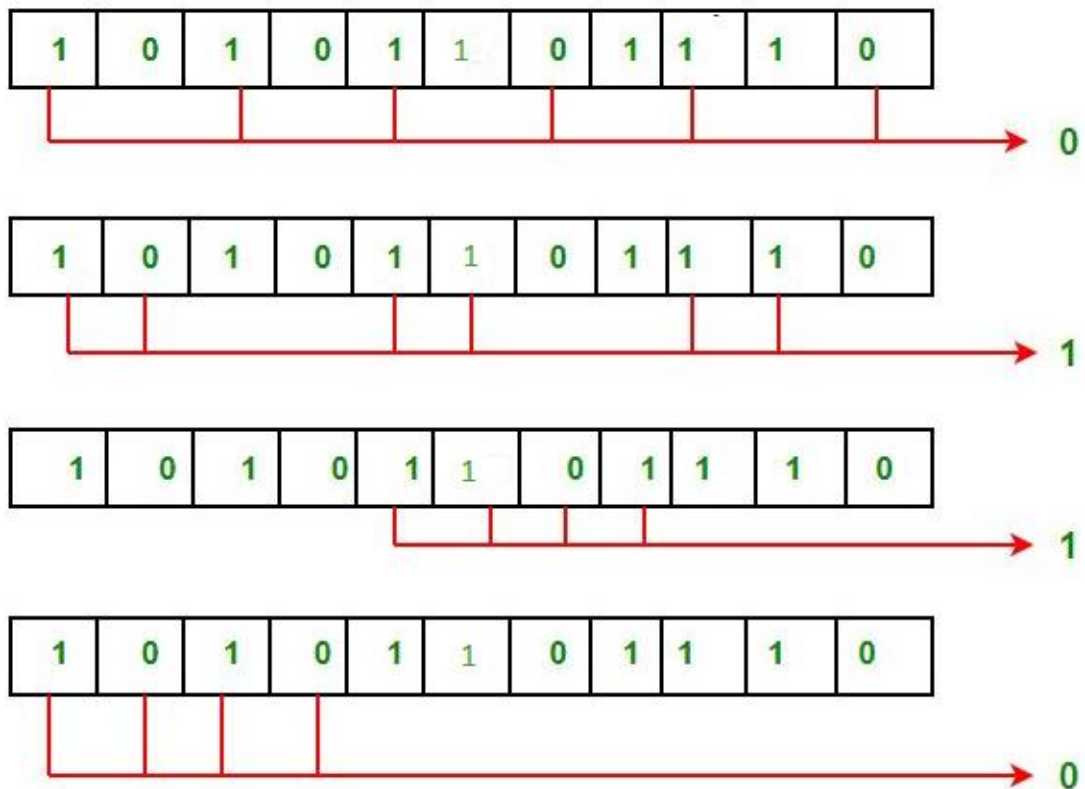
For all the parity bits we will check the number of 1's in their respective bit positions.

For R1: bits 1, 3, 5, 7, 9, 11. We can see that the number of 1's in these bit positions are 4 and that's even so we get a 0 for this.

For R2: bits 2,3,6,7,10,11 . We can see that the number of 1's in these bit positions are 5 and that's odd so we get a 1 for this.

For R4: bits 4, 5, 6, 7 . We can see that the number of 1's in these bit positions are 3 and that's odd so we get a 1 for this.

For R8: bit 8,9,10,11 . We can see that the number of 1's in these bit positions are 2 and that's even so we get a 0 for this.

The bits give the binary number 0110 whose decimal representation is 6. Thus, bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.