UNIT-I

DATA COMMUNICATIONS

The word **Data** refers to **Information.**

Data Communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software(programs).

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

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**

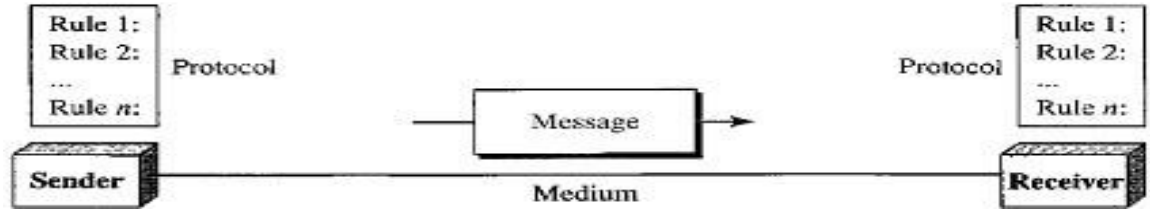
   The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**.

   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.

Five components of data communication



Note: The term ***TELECOMMUNICATION*** includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for "far").

DATA REPRESENTATION

Information comes in different forms such as text, numbers, images, audio, and video, where text numbers images can be represented in bit pattern.

Text

- In data communications, text is represented as a bit pattern, a sequence of bits (0's or1's).
- Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.
- The prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world.
- The American Standard Code for Information Interchange (ASCII) developed in the United States, now constitutes the first 127 characters in Unicode.

Numbers

- Numbers are also represented by bit patterns.
- A code such as ASCII is not used to represent numbers.
- The number is directly converted to a binary number to simplify mathematical operations.

Images

- Images are also represented by bit patterns. An image is composed of a matrix of pixels (picture elements) where each pixel is a small dot.
- The size of the pixel depends on the *resolution.* Example: An image can be divided into 1000 pixels or 10000pixels.
- If the number of pixels is more there is a better representation of the image (better resolution) but more memory is needed to store the image.
- After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image.
- There are several methods to represent color images. RGB and YCM
- In RGB each color is made of a combination of three primary colors: *red,* green and blue.
- In YCM a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

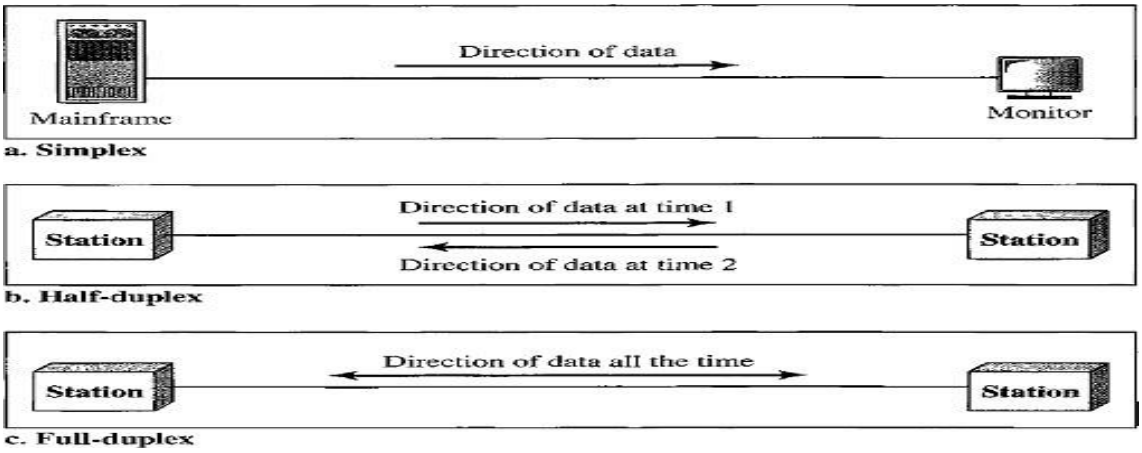
- Audio refers to the recording or broadcasting of sound or music.
- Audio is by nature different from text, numbers, or images. It is continuous, not discrete.
- Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal.

Video

- Video refers to the recording or broadcasting of a picture or movie.
- Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

DIRECTION OF DATA FLOW

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



Simplex

- In simplex mode, the communication is unidirectional (i.e. one direction only).
- Only one of the two devices on a link can transmit; the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Examples - **Keyboards** and **Monitors,** the keyboard can only introduce input, the monitor can only accept output.

Half-Duplex

- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.
- In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- The half-duplex mode is used, where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.
- **Examples** - Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

- In full-duplex mode (or duplex), both stations can transmit and receive simultaneously.
- In full-duplex mode signals going in one direction share the capacity of the link: with signals going in the other direction
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving, or the capacity of channel is divided between signals traveling in both directions.
- The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel must be divided between the two directions.
- **Example -** Telephone network. Two people talk and listen at the same time.

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.

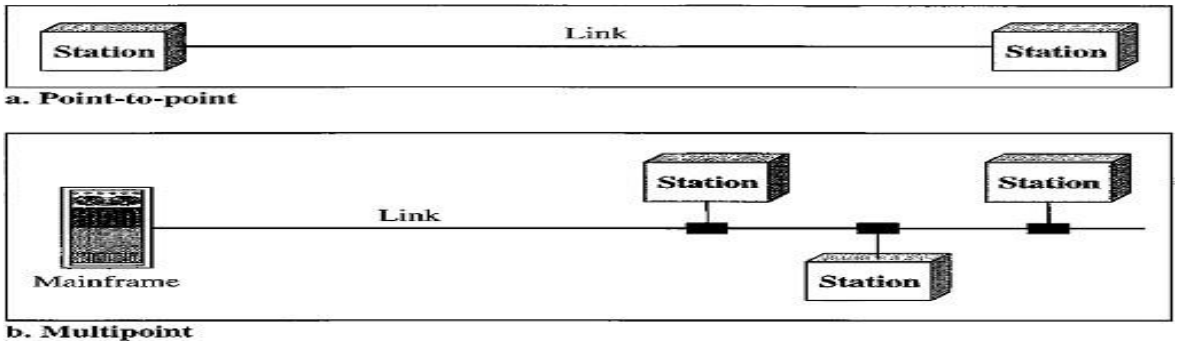
A **Node** can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

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

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



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.

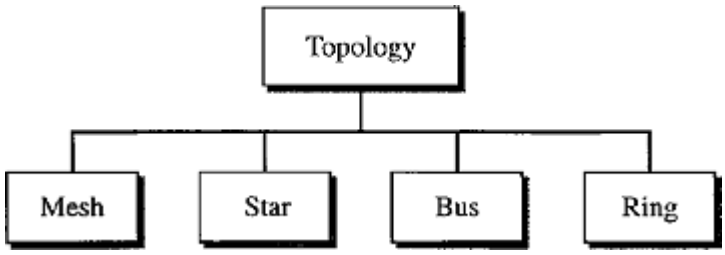
Multipoint (or) Multi-drop Connection

- 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 timeshared connection.

NETWORK TOPOLOGIES

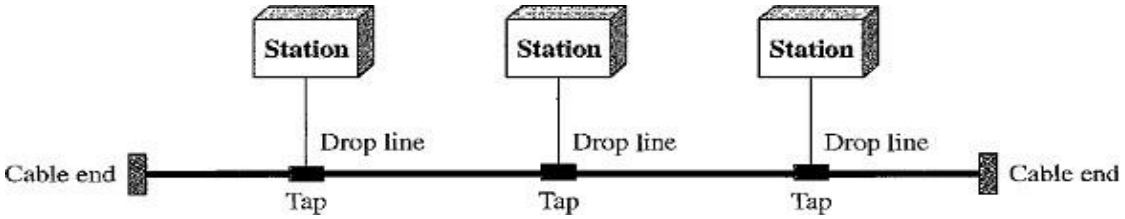
The term physical topology refers to the way in which a network is connected physically.
Two or more devices connect to a link. Two or more links form atopology.
There are four basic topologies are present:

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



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:

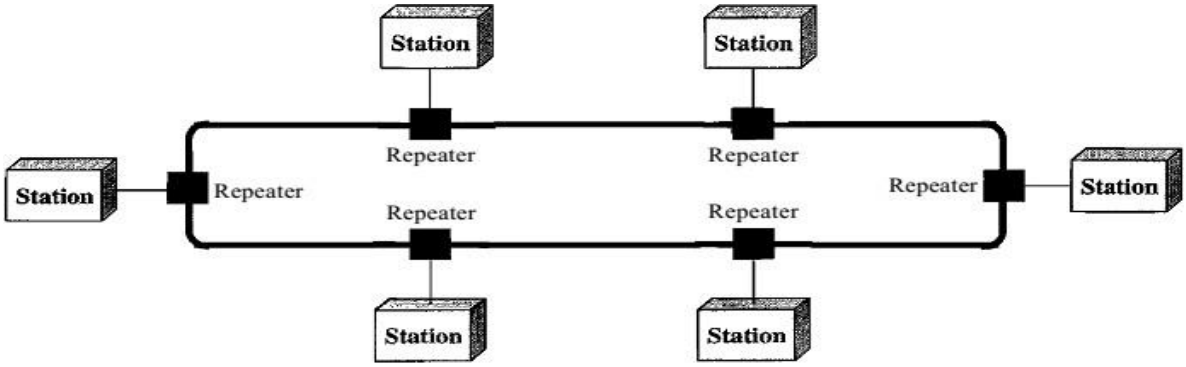
1. Installation is easy. Bus Backbone cable can be laid along the most efficient path and then connected to the nodes by drop lines of various lengths.
2. A bus uses less cabling than mesh or star topologies.

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:

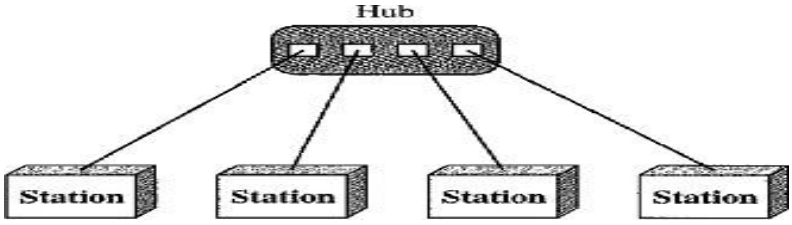
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
2. To add or delete a device requires changing only two connections.
3. The only constraints are media and traffic considerations (maximum ring length and number 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.

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.

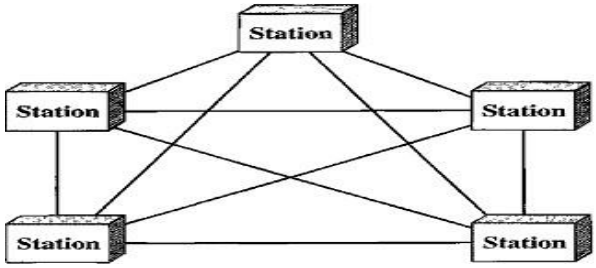
Uses:

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

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:

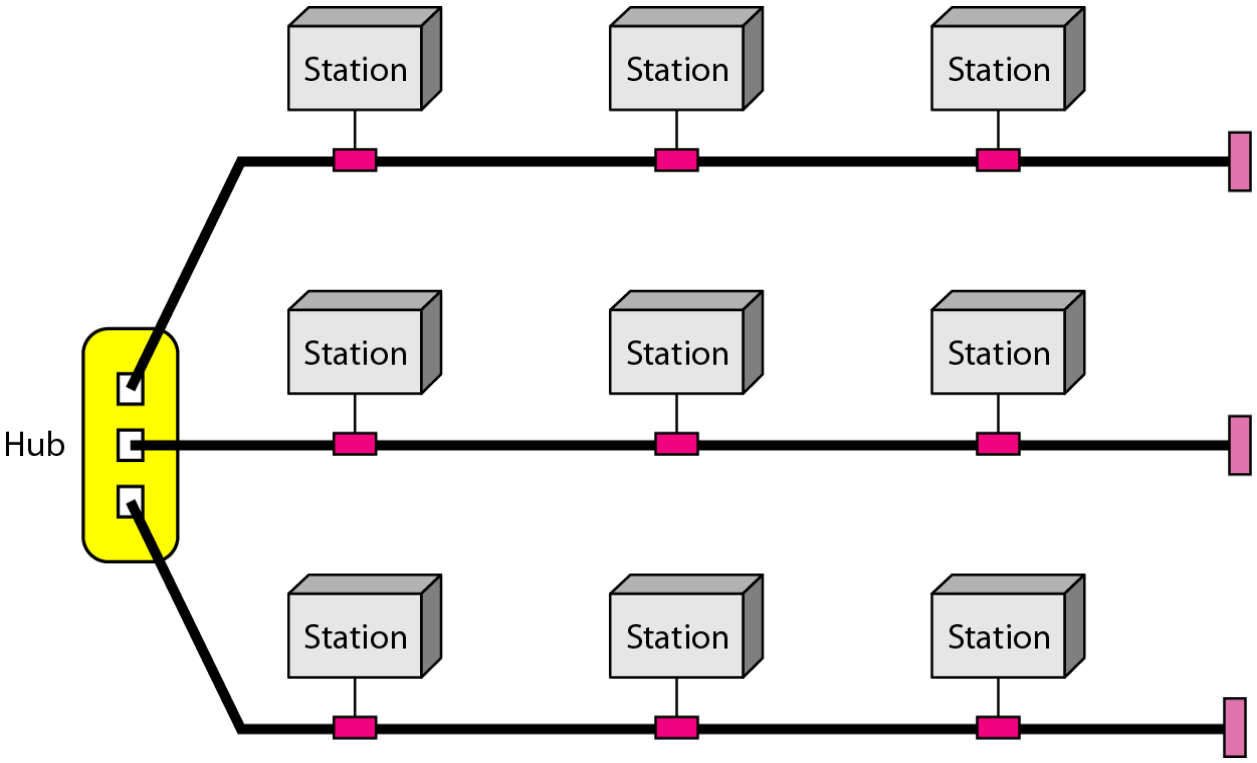
1. **High Cost:** Every device must be connected to every other device then there is a high amount of cabling and huge number of I/O ports required, this will make installation and reconnection are difficult.
2. The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.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

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



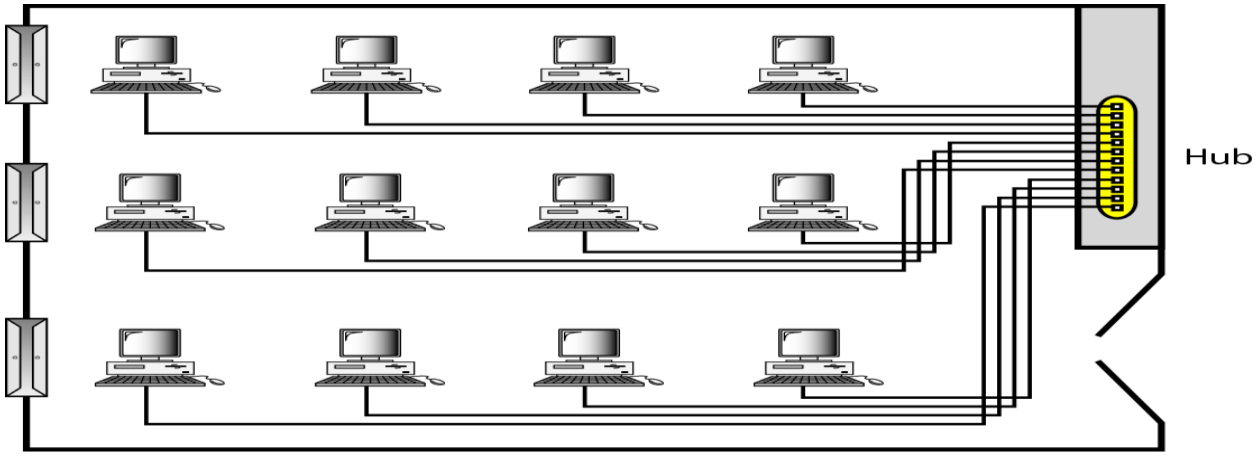
CATEGORIES OF NETWORKS

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.

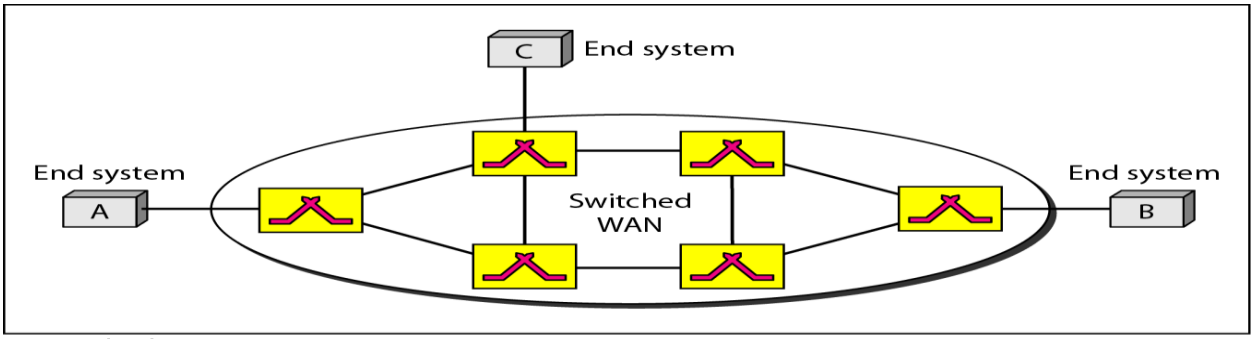


Wide Area Network

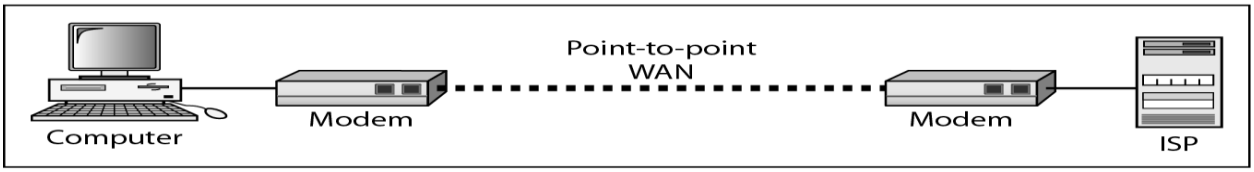
A Wide Area Network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

The switched WAN connects the end systems, which usually comprise a router (inter-networking connecting device) that connects to another LAN or WAN.

The point-to-point WAN is often used to provide Internet access. A line leased from a telephone provider that connects a home computer or a s mall LAN to an Internet service provider (lSP).



a. Switched WAN



b. Point-to-point WAN

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.

PROTOCOLS AND STANDARDS

PROTOCOLS

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. For communication to occur, the entities must agree on a protocol.

The key elements of a protocol are:

1. Syntax
2. Semantics
3. Timing.

Syntax

- The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
- For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

- The word *semantics* refers to the meaning of each section of bits. How are a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- For example, does an address identify the route to be taken or the final destination of the message?

Timing

- The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent.
- For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

STANDARDS

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Data communication standards fall into two categories: **de facto** and **de jure**.

De facto (meaning "by fact" or "byconvention")

Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

De jure (meaning "by law" or "by regulation")

Those standards that have been legislated by an officially recognized body are de jure standards.

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

1. ISO (International Organization for Standardization)
2. IEEE (Institute of Electrical and Electronics Engineers)
3. ANSI (American National Standards Institute)
4. ITU-T (International Telecommu ///l,lnication Union-Telecommunication StandardsSector)
5. EIA (Electronic Industries Association)

International Organization for Standardization (ISO)

- The ISO is a multinational and standard setting body whose membership is drawn mainly from the standards creation committees of various governments throughout the world.
- The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.

Institute of Electrical and Electronics Engineers (IEEE)

- The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world.
- International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering.
- As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.

American National Standards Institute (ANSI)

- Despite its name, the American National Standards Institute is a completely **Private, Nonprofit Corporation** not affiliated with the U.S. federal government.
- It oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States.
- The organization also coordinates U.S. standards with international standards so that American products can be used worldwide.
- Even though it is not affiliated with U.S. federal government all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.

International Telecommunication Union-Telecommunication Standards Sector (ITU-T)

- By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility.
- The United Nations responded by forming a committee International Telecommunication Union (ITU) as part of its the Consultative Committee for International Telegraphy and Telephony(CCITT).
- This committee was devoted to the research and establishment of standards for tele communications in general and for phone and data systems in particular.
- On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector(ITU-T).

Electronic Industries Association (EIA)

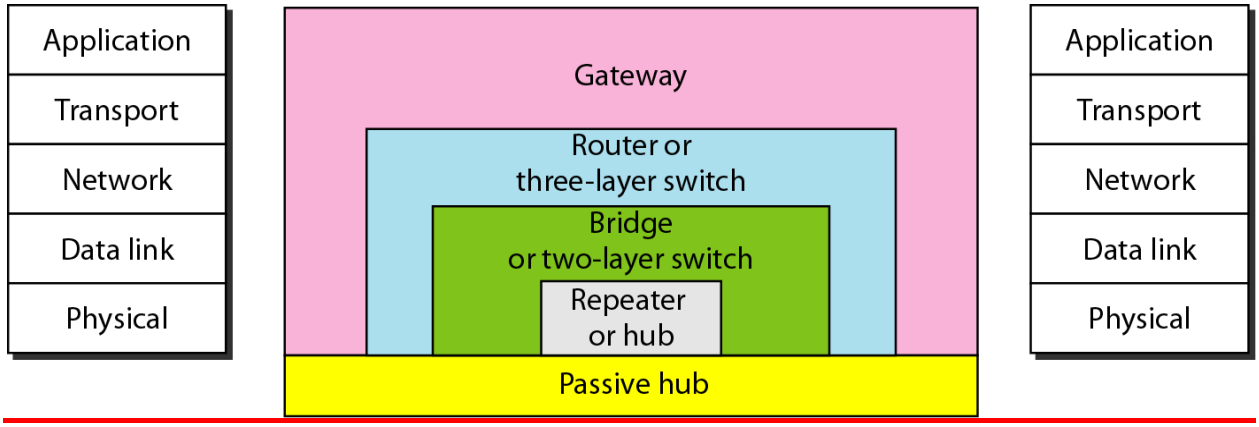
- Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of electronics manufacturing concerns.
- Its activities include public awareness education and lobbying efforts in addition to standards development.
- In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

Internet Standards

- An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet.
- It is a formalized regulation that must be followed.
- There is a strict procedure by which a specification attains Internet standard status.
- A specification begins as an Internet draft.
- An **Internet draft** is a working document (a work in progress) with no official status and a 6-monthlifetime.
- Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment** (RFC).
- Each RFC is edited, assigned a number, and made available to all interested parties.
- RFCs go through maturity levels and are categorized according to their requirement level.

CONNECTING DEVICES/NETWORK DEVICES

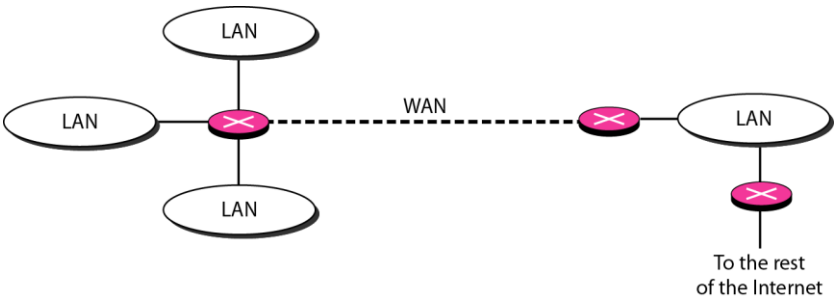
Connecting devices into five different categories based on the layer **in** which they operate **in** a network, as shown **in** Figure 15.1.



The five categories contain devices which can be defined as
1. Those which operate below the physical layer such as a passive hub.
2. Those which operate at the physical layer (a repeater or an active hub).
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
5. Those which can operate at all five layers (a gateway).

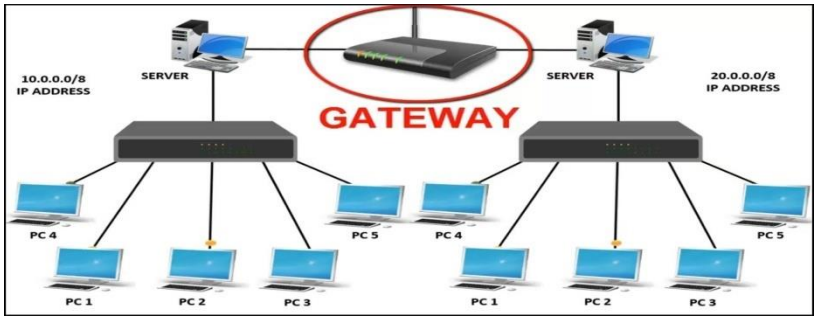
Routers

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols. We discuss routers and routing in greater detail in Chapters 19 and 21. Figure 15.11 shows a part of the Internet that uses routers to connect LANs and WANs.



Gateway

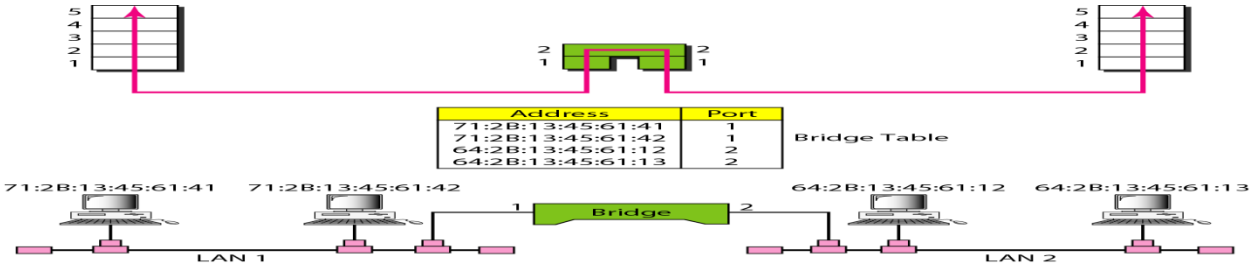
A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model. The gateway connecting the two systems can take a frame as it arrives from the first system, move it up to the OSI application layer, and remove the message. Gateways can provide security.



Bridges

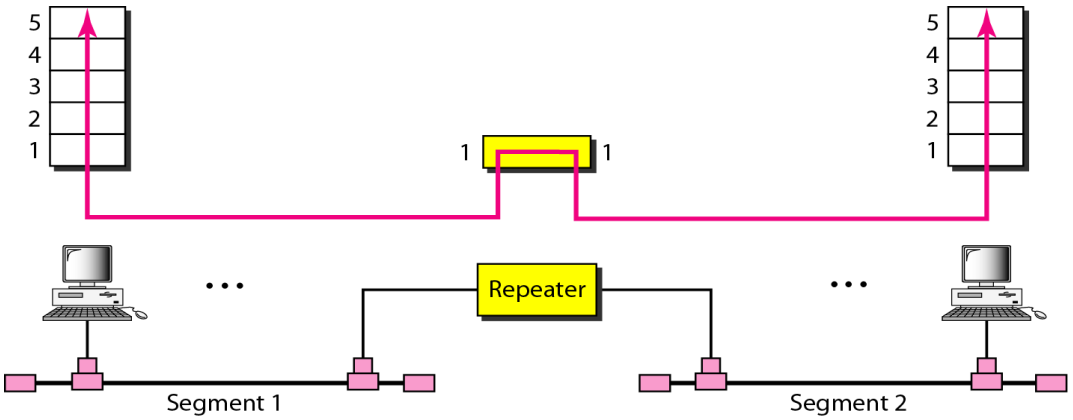
A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port. A bridge has a table that maps addresses to ports.



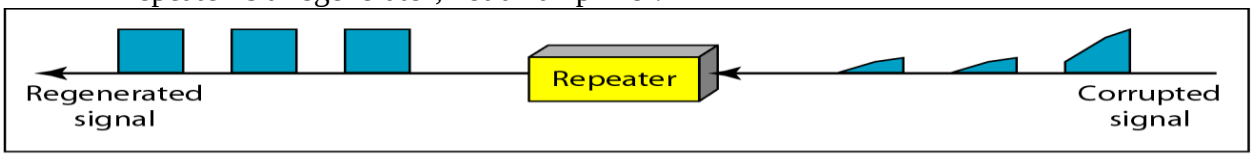
Repeaters

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN, as shown in Figure 15.2.

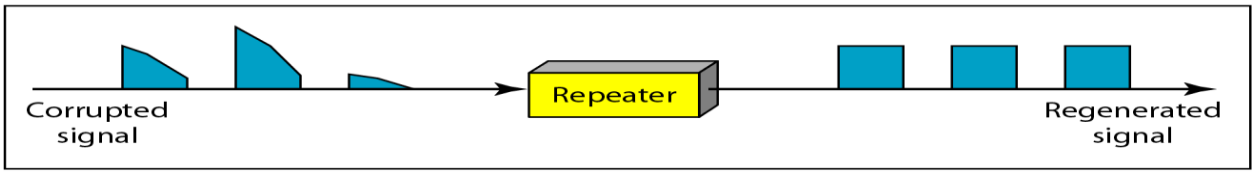


A repeater does not actually connect two LANs; it connects two segments of the same LAN. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.

- A repeater forwards every frame; it has no filtering capability.
- A repeater is a regenerator, not an amplifier.



a. Right-to-left transmission.



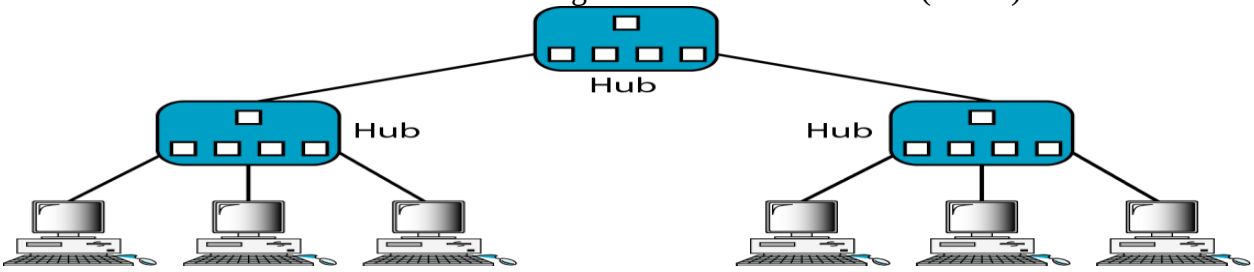
b. Left-to-right transmission.

Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches.In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. This type of a hub is part of the media; its location in the Internet model is below the physical layer.

Active Hubs

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. We have seen examples of hubs in some Ethernet implementations (lOBase-T, for example). However, hubs can also be used to create multiple levels of hierarchy, as shown in Figure 15.4. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).



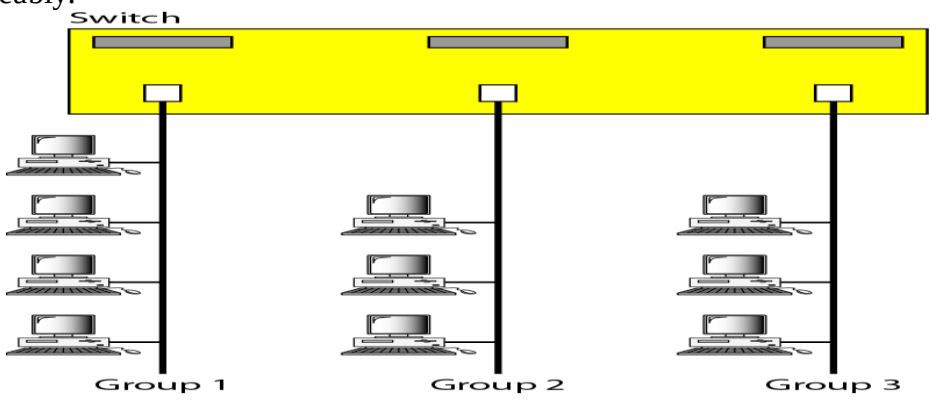
Two-Layer Switches

The **two-layer switch** performs at the physical and data link layers. A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can

connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision, as we saw in Ethernet).A two-layer switch, as a bridge does, makes a filtering decision based on the MAC address of the frame it received.

Three-Layer Switches

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding. In this book, we use the terms *router* and *three-layer switch* interchangeably.



NETWORK MODELS

There are two types of network models are used:

1. ISO/OSI Model.
2. TCP/IP protocol model

ISO/OSI Model

- **ISO** is the **Organization**. **OSI** is the **Model**. ISO was established in 1947. OSI was first introduced in1970.
- The **International Standards Organization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection model**.
- An **Open System** is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- **The purpose** of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

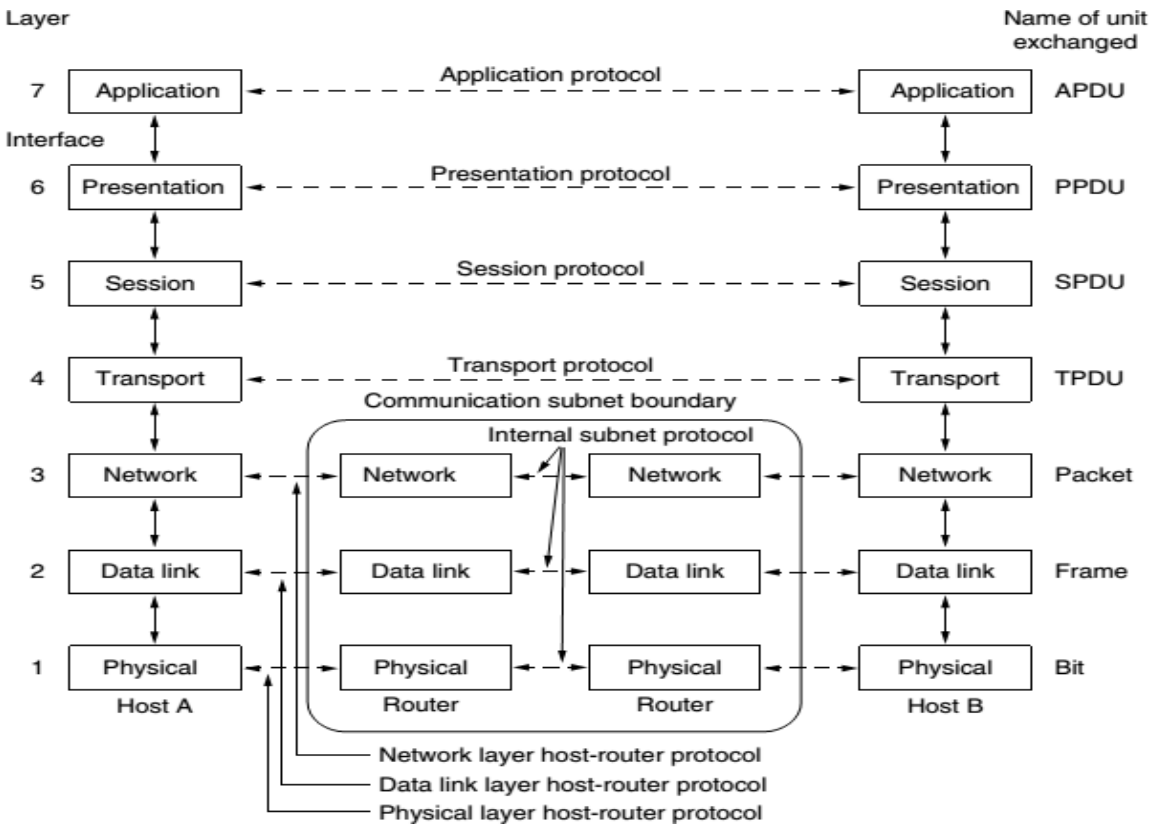
The OSI model is a **Layered Frame work** for the design of network systems that allows communication between all types of computer systems.

It consists of seven ordered layers. Each layer defines a part of the process of moving information across a network.

Below figure shows the layers involved when a message is sent from host A to host B. A host may be a device or node or a computer. Within a single machine, each layer calls upon the services of the layer just below it.

Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

APDU, PPDU, SPDU, TPDU are packet data units of Application, Presentation, Session, Transport layers respectively.

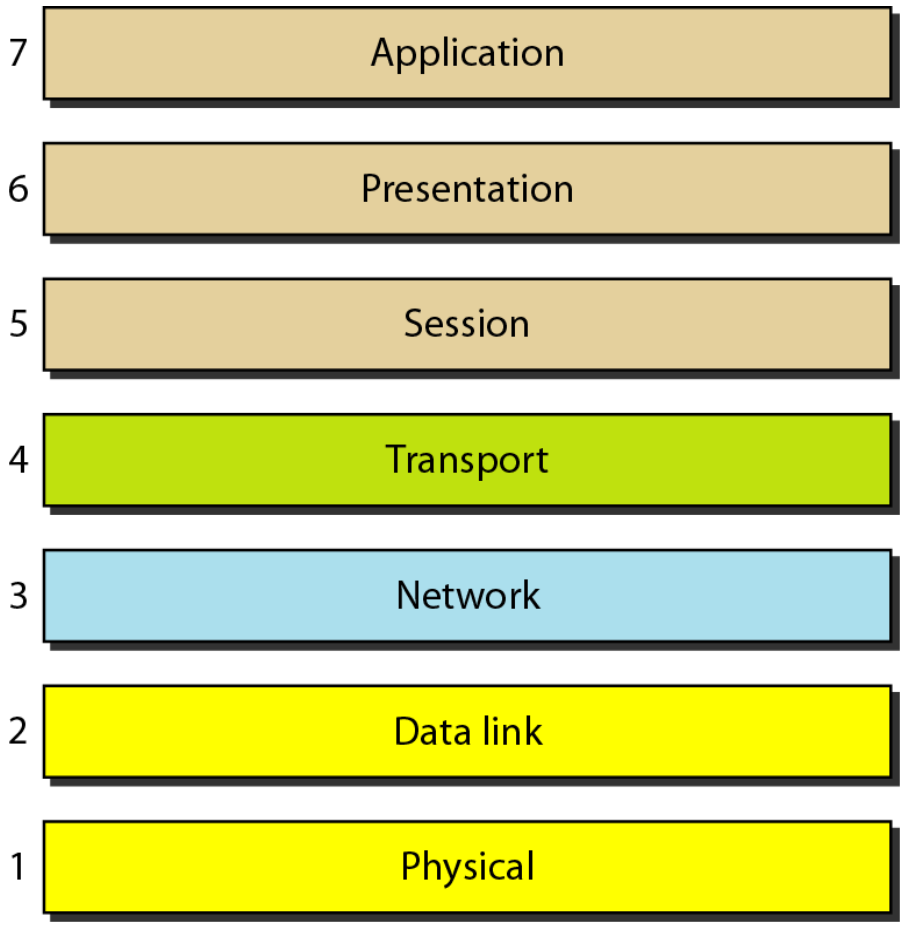


Interfaces Between Layers

- The passing of the data and network information between the layers in the device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it. These interfaces provide modularity to the network.

The Seven Layers in OSI Model are:

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



These seven layers can be categorized into 3 groups:

1. **Physical, Data Link,** and **Network Layers** are the network support layers: they deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing, and transport timing and reliability.

   Note: Physical layer is implemented in hardware whereas Data link and Network layers are combination of hardware and software.
2. **Session, Presentation,** and **Application Layers** can be thought of as the user support layers. These are almost always implemented in software. They allow interoperability among unrelated software systems.

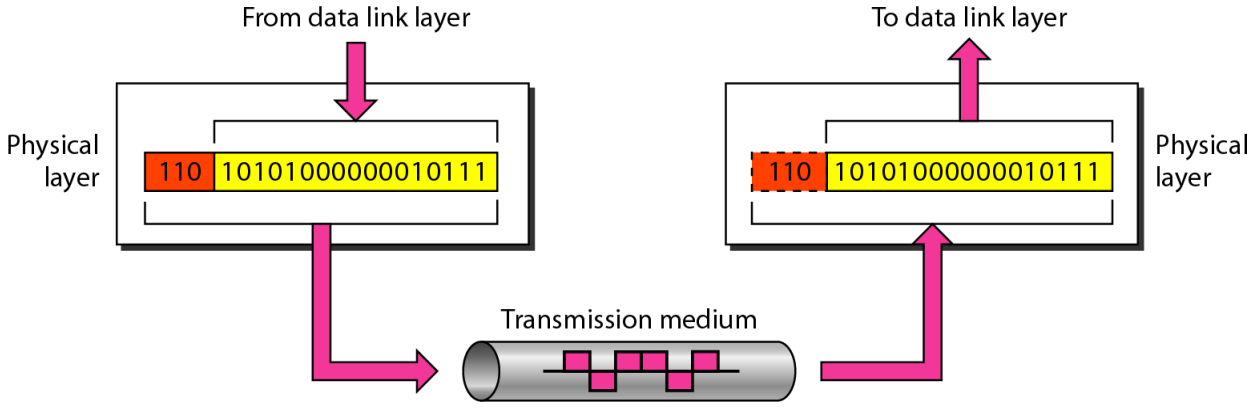
3. **The Transport Layer** links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.

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

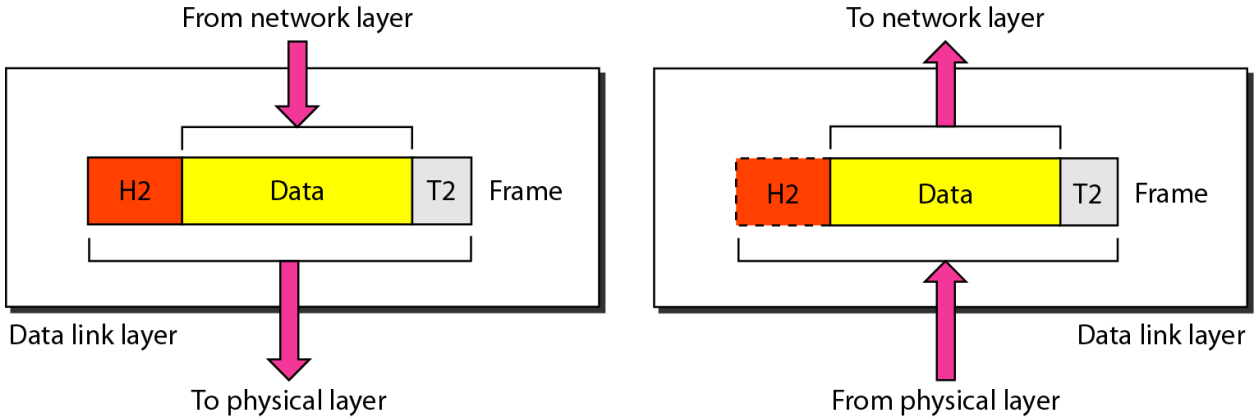
The data link layer is responsible for moving frames from one node to the next node.

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.

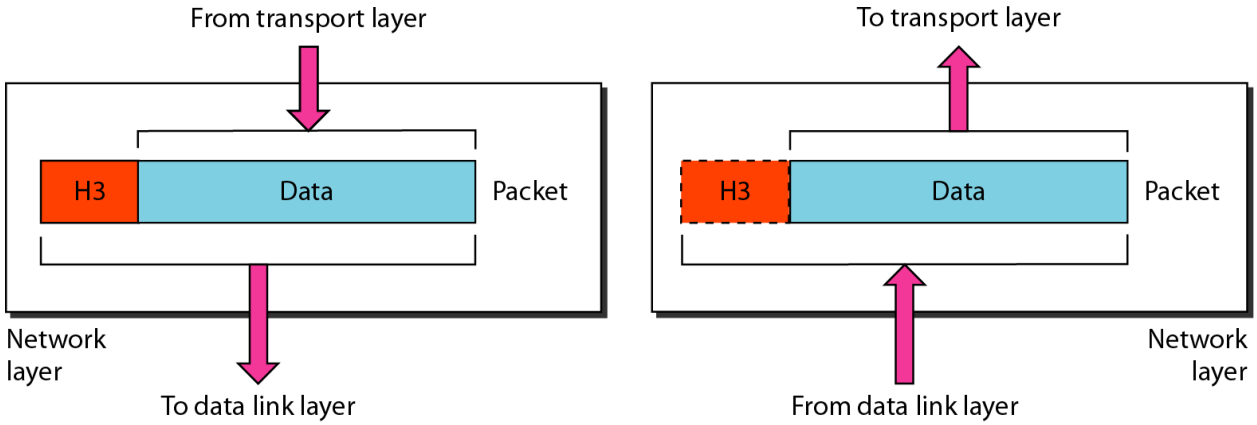
Responsibilities of the Network layer include the following:

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.



<u>Transport Layer</u>

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

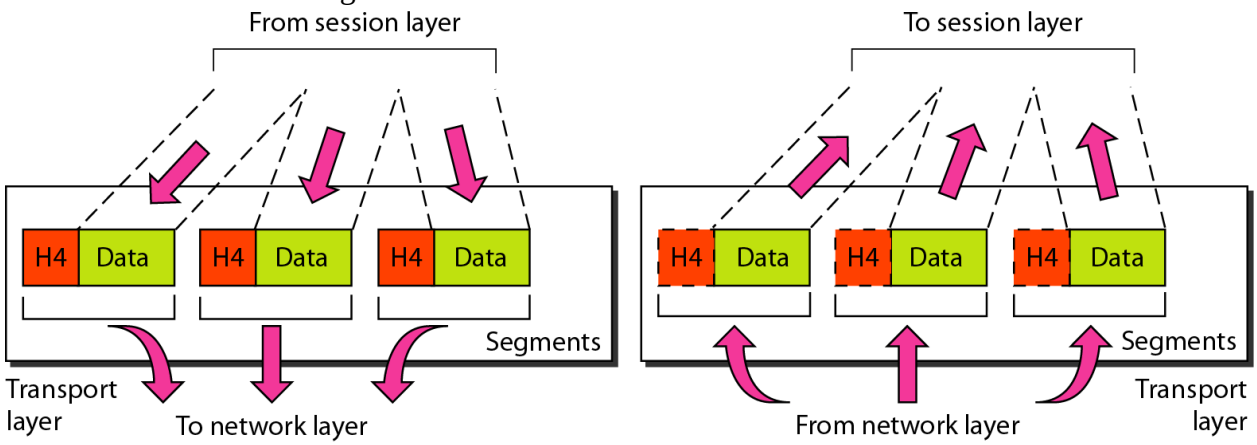
- A message is divided into transmittable segments, with each segment containing a sequence number.
- These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and the sequence numbers are used for identifying and replace packets that were lost during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

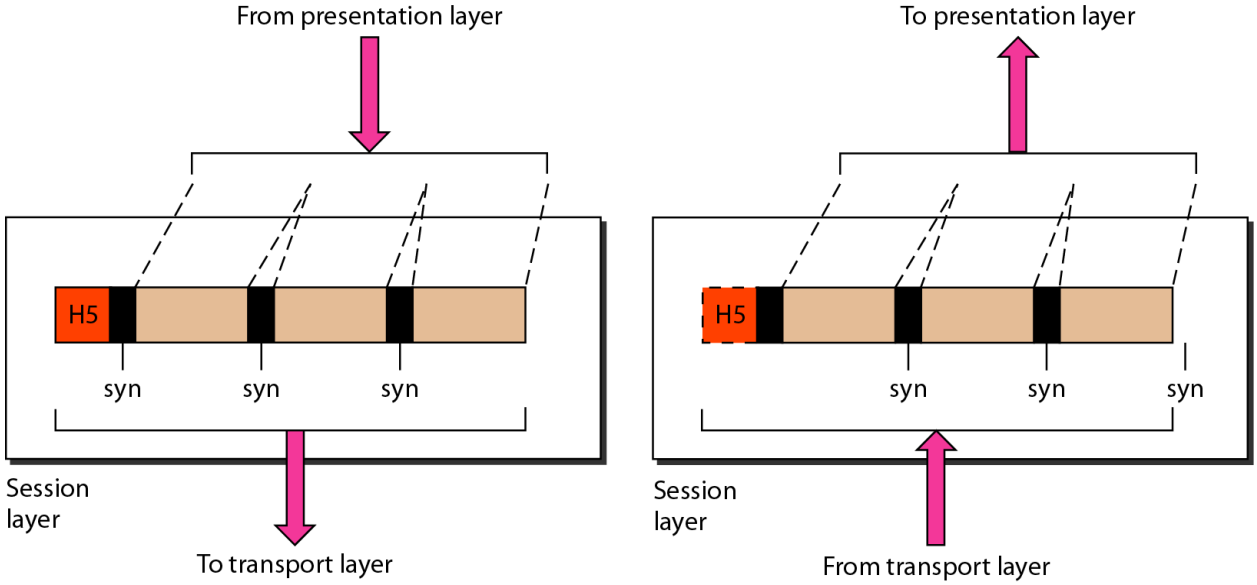


Session Layer

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

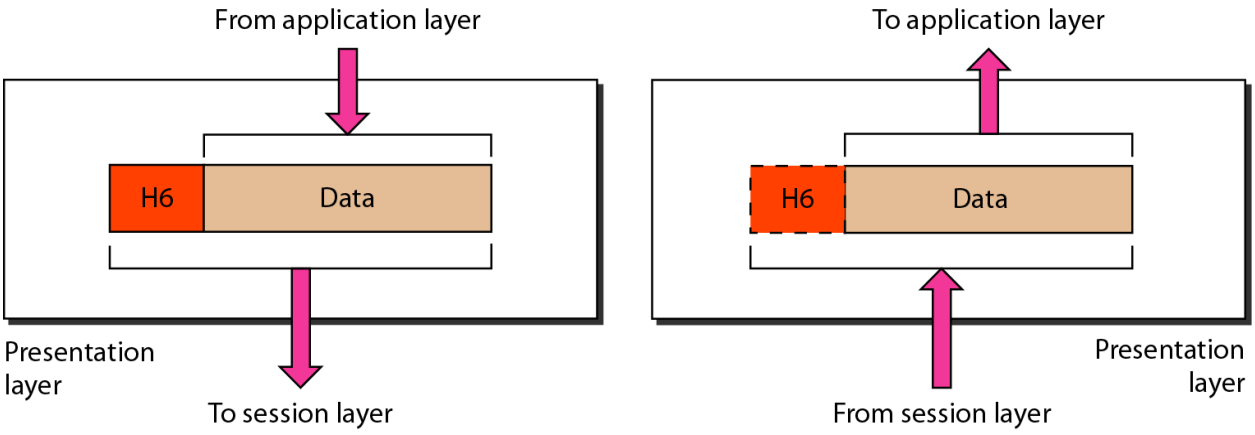
- The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers etc. The information must be changed to bits streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible 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.



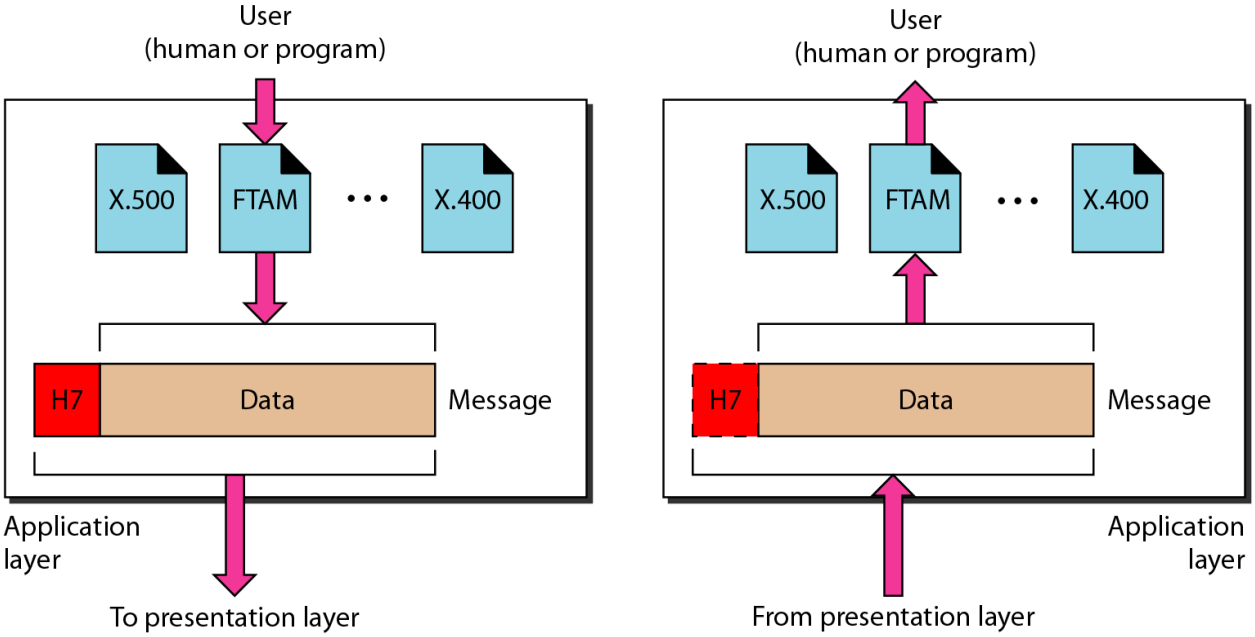
Application Layer

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.



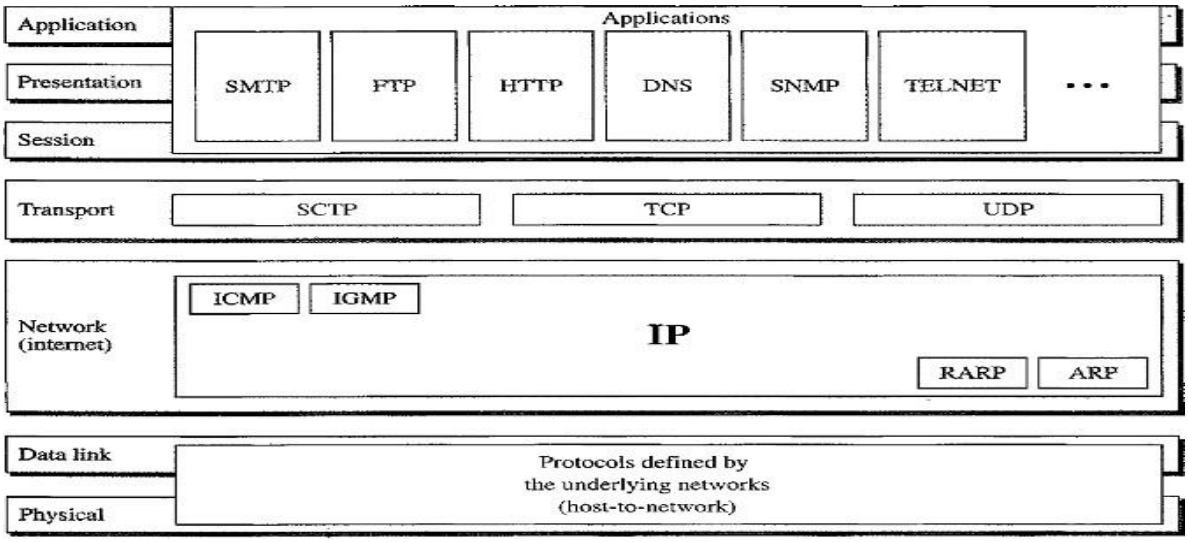
TCP/IP PROTOCOL SUITE

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

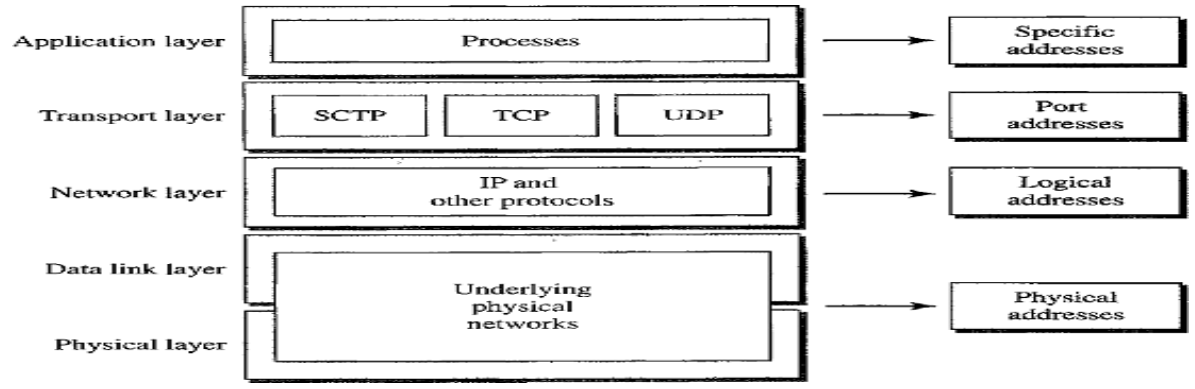
On top of the transport layer is the **application layer**. It contains all the higher-level protocols such as:

- **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.

ADDRESSING in TCP/IP

Four levels of addresses are used in an internet employing the *TCP/IP* protocols

1. Physical Addresses or Link Address
2. Logical Addresses or IP Address
3. Port Addresses
4. Specific Addresses



Physical Addresses (or) **Link address**

- The physical address is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer. It is the lowest-level address.
- The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network.
- **For example, Ethernet** uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC) such as **07:01:02:01 :2C:4B.**

Logical address

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- Logical addressing is a universal addressing system in which each host can be identified uniquely, regardless of the underlying physical network.
- A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example: **198.20.30.1** where each number is a 8 bit binary number.

127.0.0.1 is local host IP address.

Port Address

- The address assigned to a process is called a **Port Address**. A port address in TCP/IP is **16 bits** in length.
- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet.
- Computers are devices that can run multiple processes at the same time.
- The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).
- For these processes to receive data simultaneously, we need to provide different addresses for different processes. The addresses which are assigned to different processes is called Port addresses.

Process	Port Number
FTP	21
TELNET	23
SMTP	25
DNS	53
HTTP	80
IMAP	143
SNMP	161
HTTPS	443

Specific Addresses

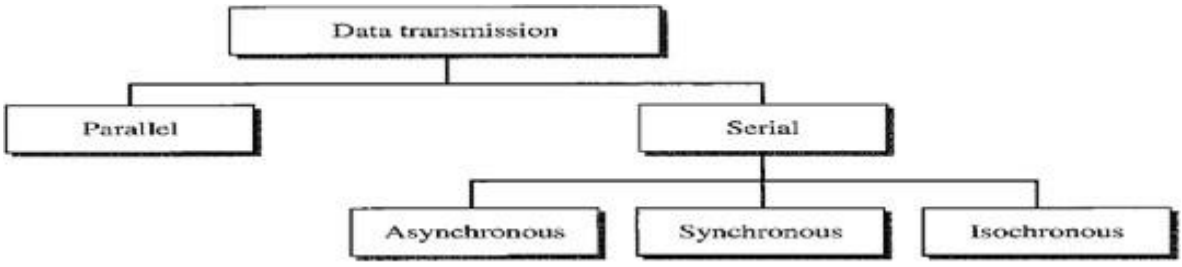
Some applications have user-friendly addresses that are designed for that specific address.

Examples: E- mail address such as dccn@gmail.com, Universal Resource Locator (URL) such aswww.google.com

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.

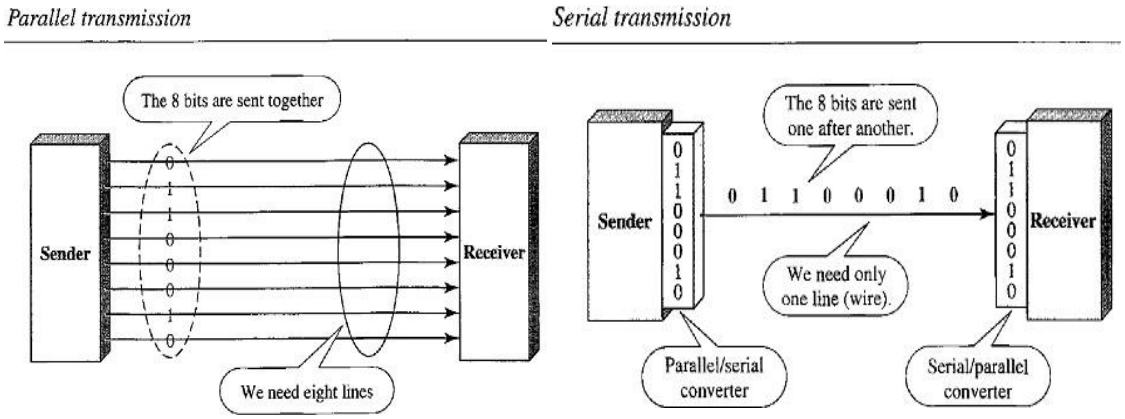
The mechanism for parallel transmission is a conceptually simple one: Use **n-wires** to send **n-bits** at one time.

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.

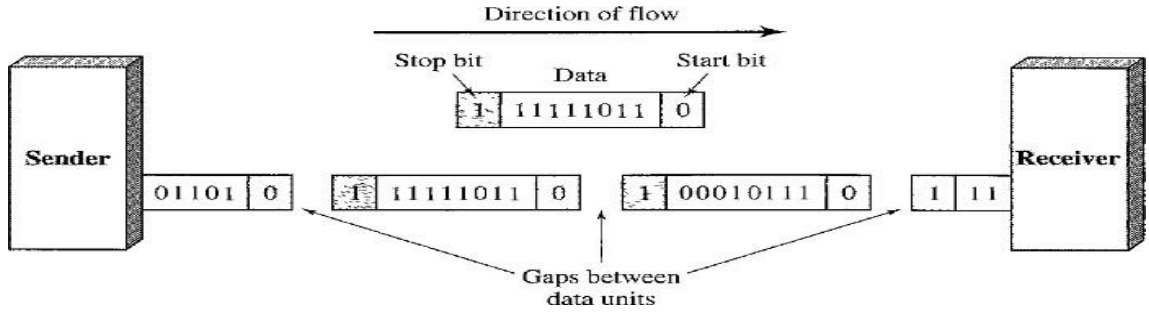
Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel- to-serial) and between the line and the receiver (serial-to-parallel).

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.



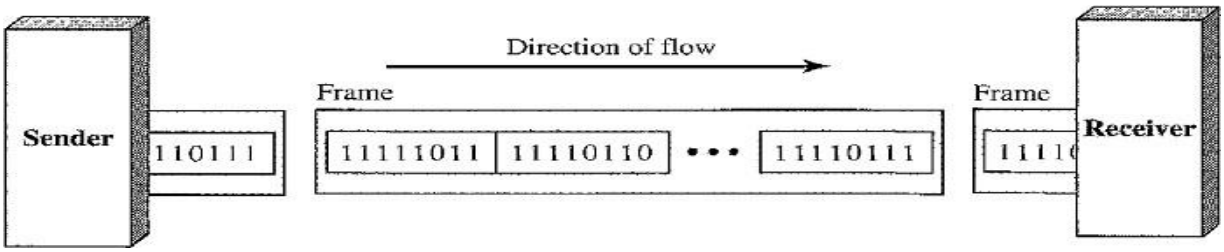
- In asynchronous transmission, we send one start bit (0) at the beginning and one or more stop bits (1's) at the end of each byte. There may be a gap between each byte.
- The start and stop bits are used because the sending system handles each group independently whenever the group is ready it will 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

Modulation and Demodulation

Converting digital Signal to analog signal is called Modulation, whereas demodulation is converting Analog signal to digital signal.

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.

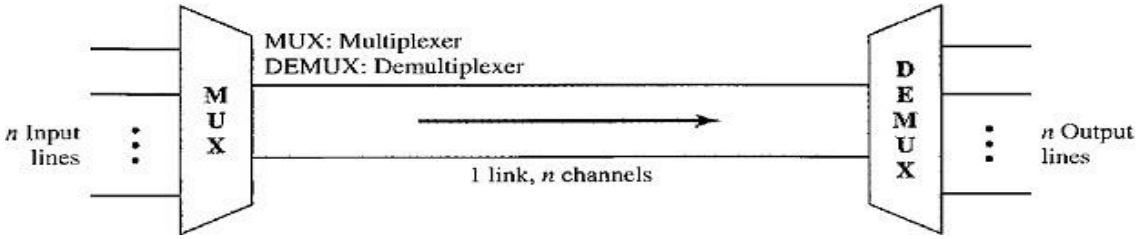


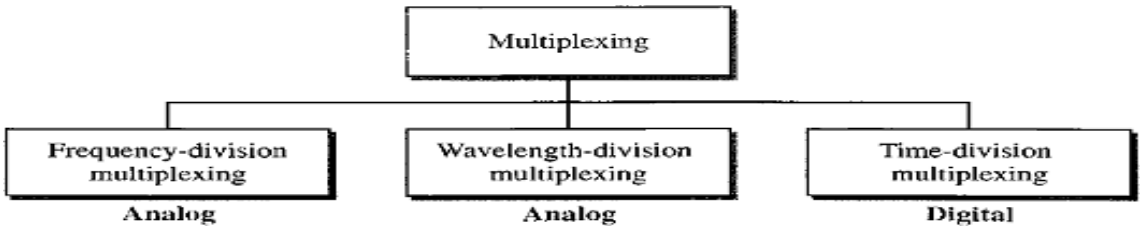
Fig: Dividing the link into channels

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.
- **Channels** can be separated by strips of unused bandwidth called **Guard Bands.**
- **Guard bands** are used to prevent signals from overlapping.
- In addition, carrier frequencies must not interfere with the original data frequencies.

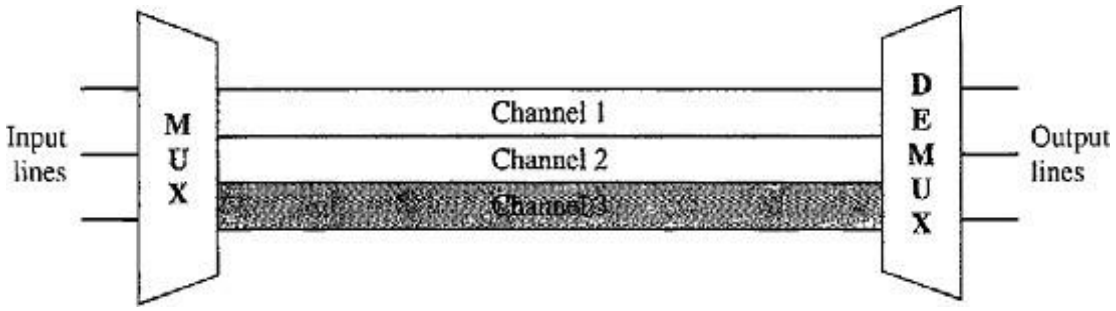
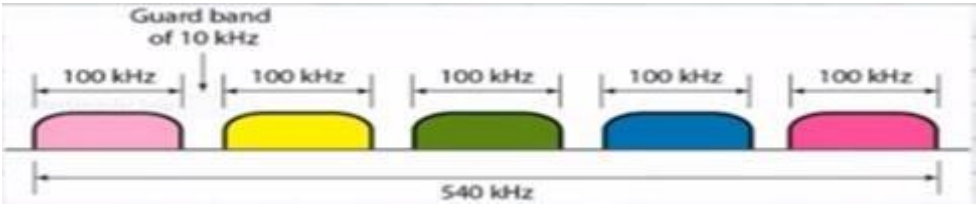


Fig: Frequency Division Multiplexing



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

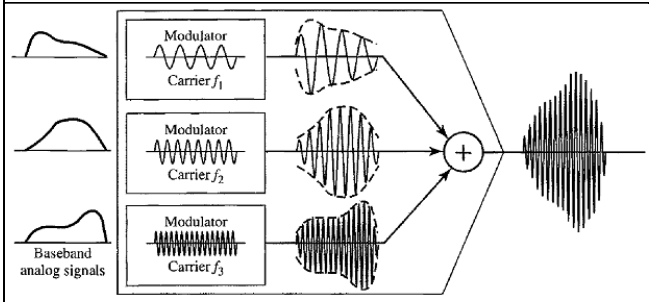
Multiplexing Process

- 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.

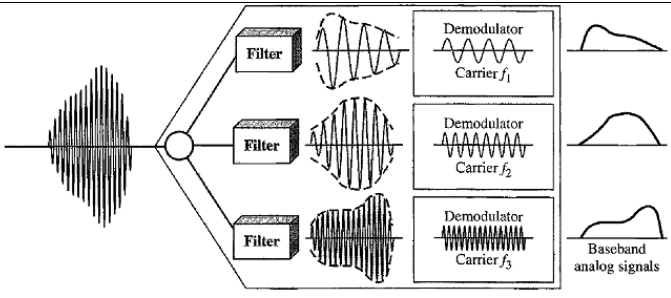
Demultiplexing Process

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

FDM Multiplexing

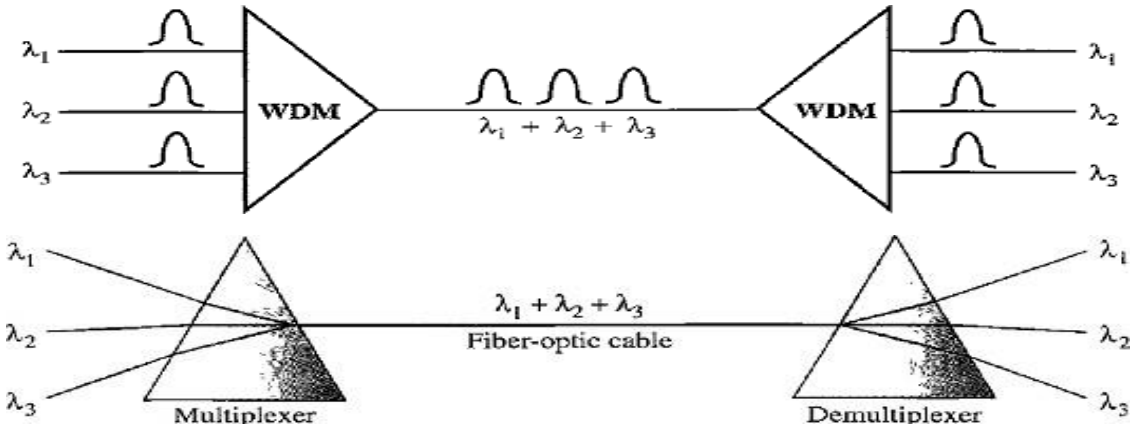


FDM Demultiplexing



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.
- The combining and splitting of light sources are easily handled by a **Prism**. A Prism bends a beam of light based on the angle of incidence and the frequency.
- A multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies.
- 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.

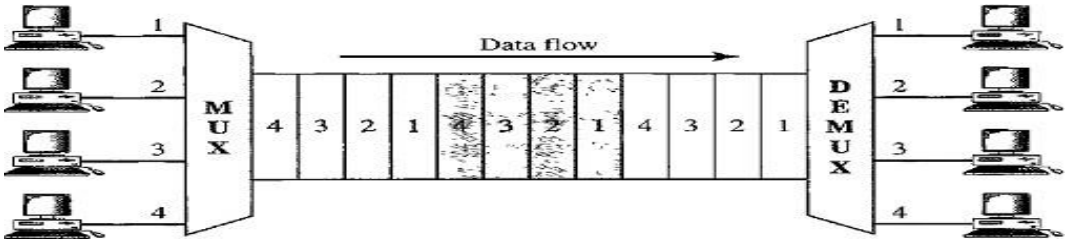
Disadvantages: Expensive than FDM.

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.

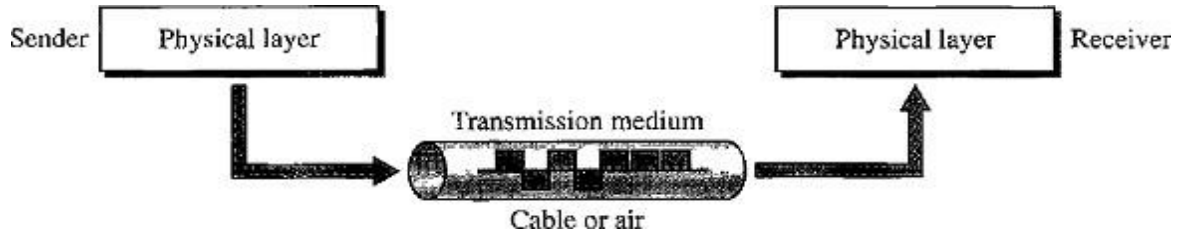


In the above figure all the data in a message from source 1 always go to one specific destination either of 1, 2, 3, or 4. The delivery is fixed and unvarying.

TRANSMISSION MEDIA

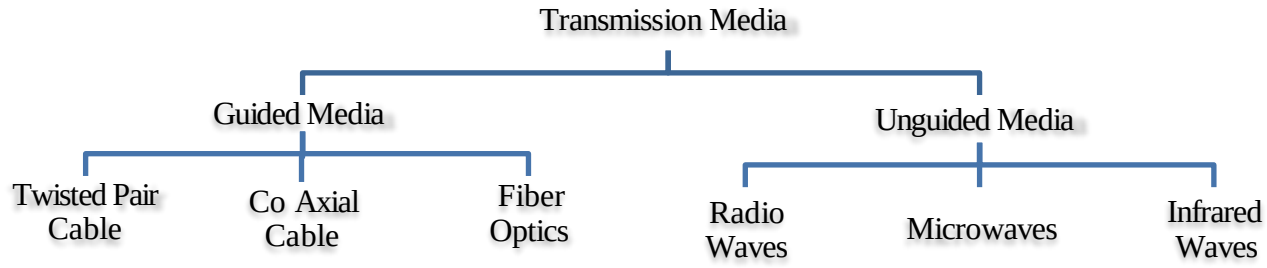
Transmission media are actually located below the physical layer and are directly controlled by the physical layer.

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

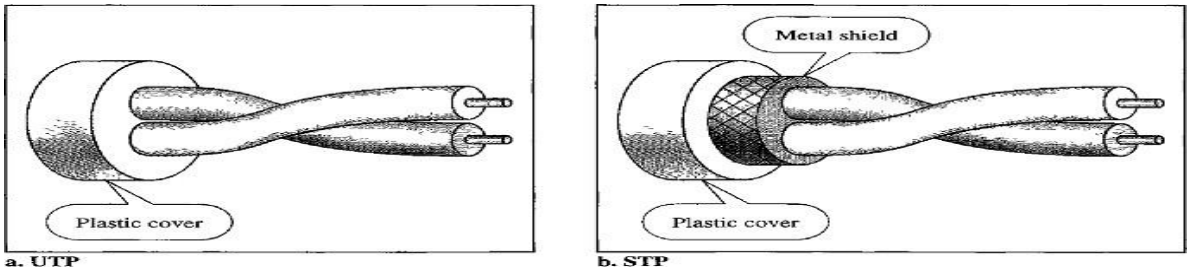
A signal traveling along this media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form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

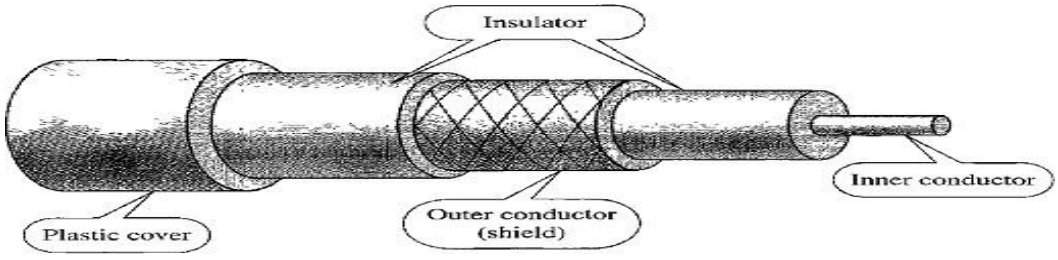
- Twisted-pair cables are used in telephone lines to provide voice and data channels. Most widely used in Internet connections.
- The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

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

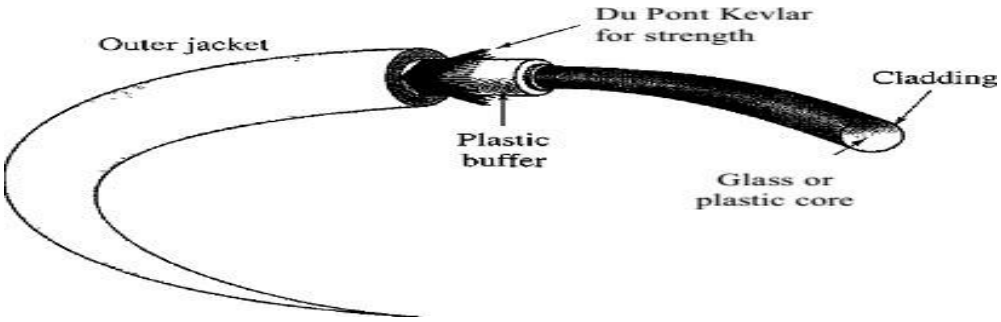
Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

Applications

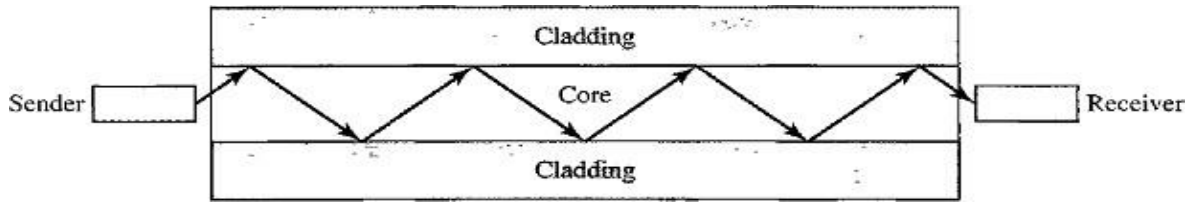
Coaxial cable was widely used in analog telephone networks, digital telephone networks, Cable TV networks, Ethernet LAN.

Fiber-Optic Cable

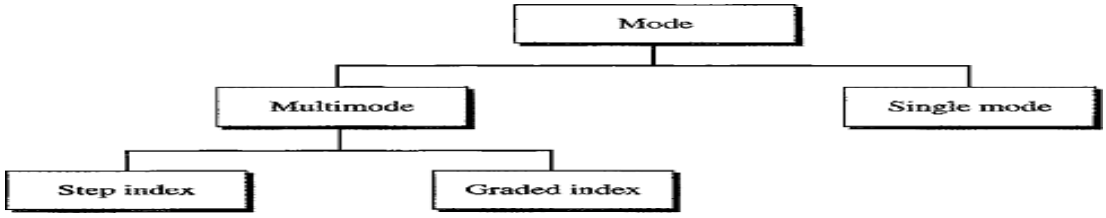
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable.
- Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center 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

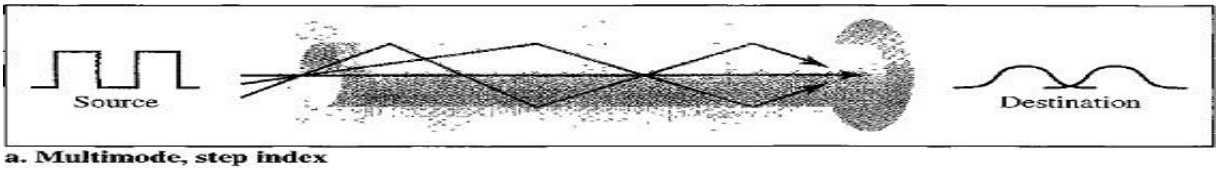
In this mode multiple beams from a light source move through the core in different paths.

Multimode Step-Index Fiber:

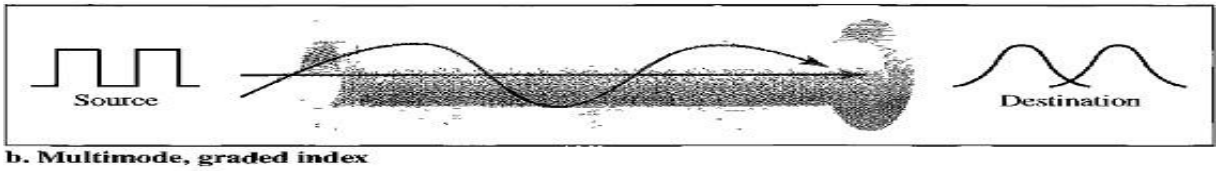
- The density of the core remains constant from the center to the edges.
- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.
- At the interface, there is an abrupt change due to a lower density; this alters the angle of 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:

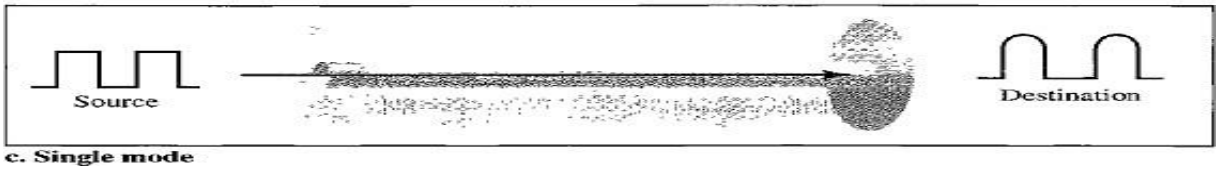
- It decreases the distortion of the signal through the cable.
- The word *index* here refers to the index of refraction.
- The index of refraction is related to density. A graded- index fiber is one with varying densities.
- Density is highest at the center of the core and decreases gradually to its 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 Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

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.

Advantages

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

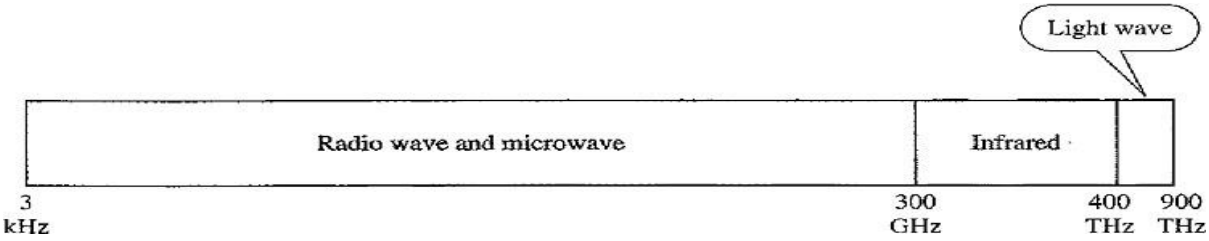
- **Higher bandwidth**. Fiber-optic cable can support higher bandwidths than either twisted-pair or coaxial cable.
- **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need 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.

Disadvantages

- **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)

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.

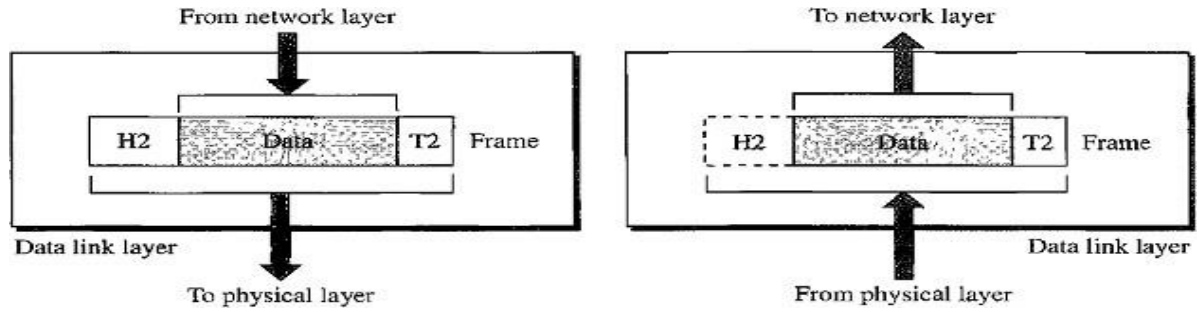
Applications

- 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

DataLinkLayer

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

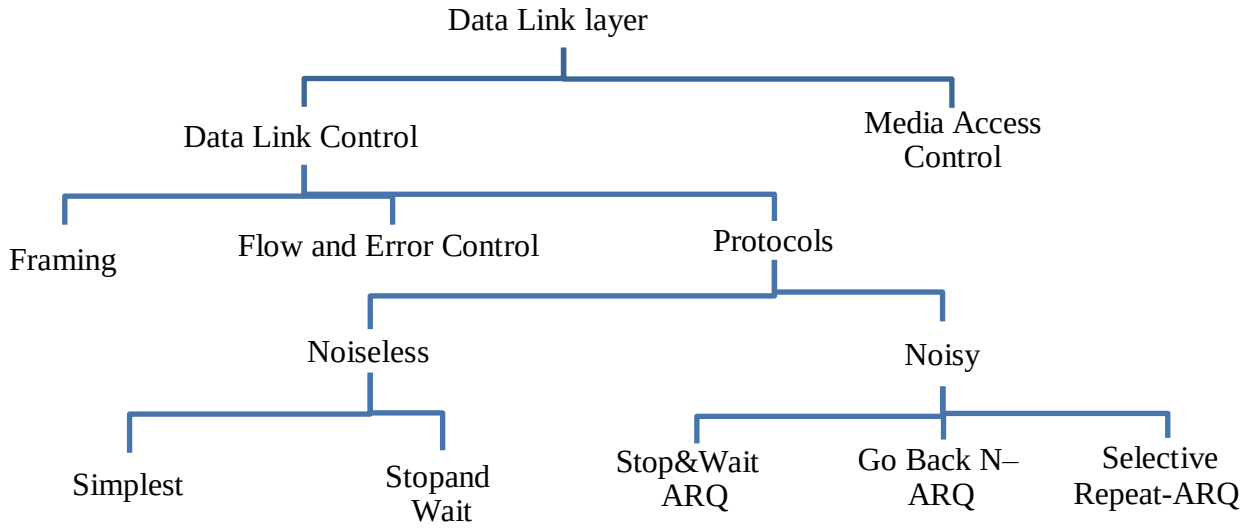
The data link layer also adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged, duplicate, or lost frames.

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.

FUNCTIONS OF DATA LINK LAYER

The functionality and sub functionalities of Data Link Layer are given below:



Note:

1. Physical layer transfers bits in the form of a signal from the source to the destination.
2. The data link layer converts bits into frames, so that each frame is distinguishable from another.

Framing

- Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.

- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

- If the message is large we will divide the message into several frames. Because larger frames causes flow and error control problems, if any single bit error occurs we have to retransmit the entire message this consumes a lot time.
- If a message is divided into smaller frames the single bit error can effect only one frame.

Framing can be done in 2ways:

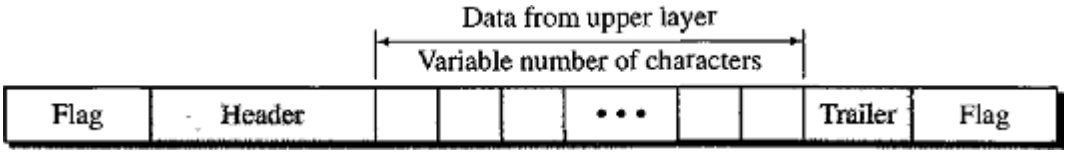
- **Fixed size framing:** The size of the frame is fixed for all the frames. There is no need to define the boundaries of a frame.
- **Variable size framing:** In variable-size framing, we need a way to define the end of the frame and the beginning of the next frame.

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.

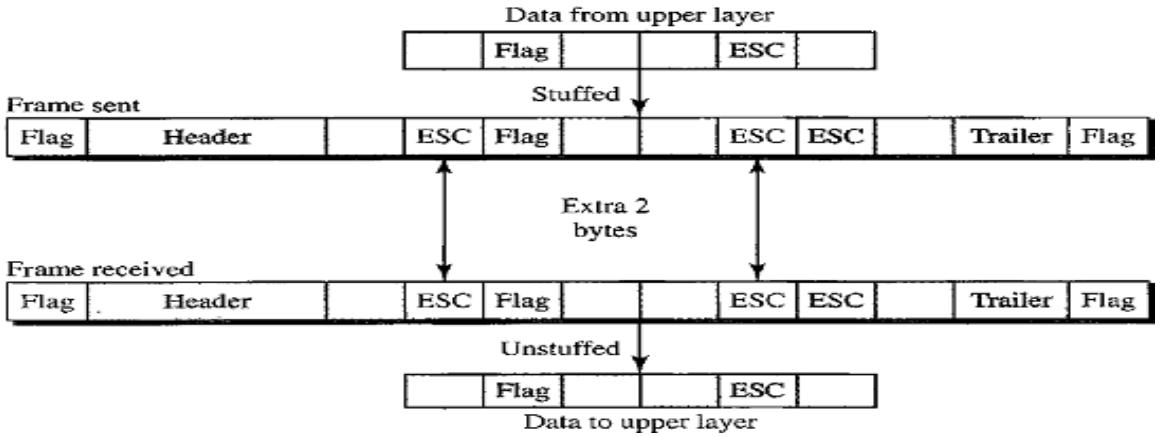
Disadvantages of Character Stuffing

- 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.

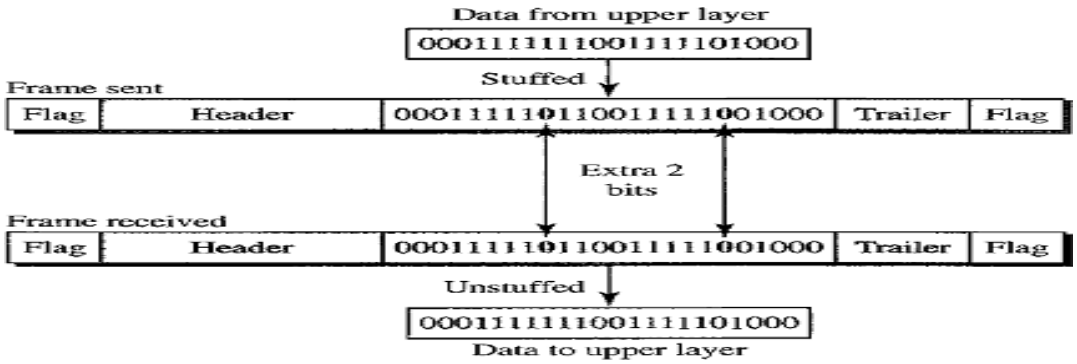
The solution for this problem is using ***Bit Oriented Approach.***

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 Detection and Correction

Data can be corrupted during transmission.

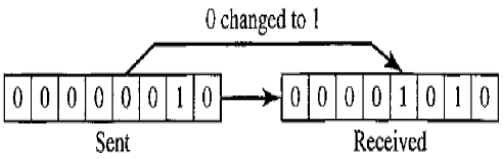
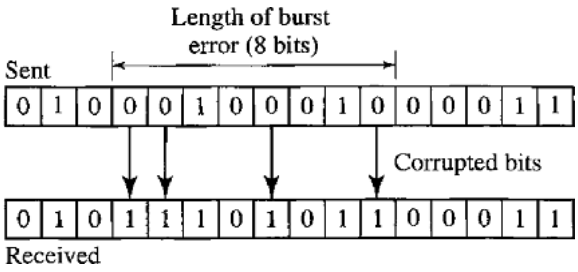
Some applications require that errors be detected and corrected. That means:

- Networks must be able to transfer data from one device to another with acceptable accuracy.
- For most applications, a system must guarantee that the data received are identical to the data transmitted.
- Any time data are transmitted from one node to the next, they can become corrupted in passage.
- Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

Note: Some applications can tolerate a small level of **Error**.
For Example: Random errors in audio or video transmissions may be tolerable, but when we transfer text, we expect a very high level of accuracy.

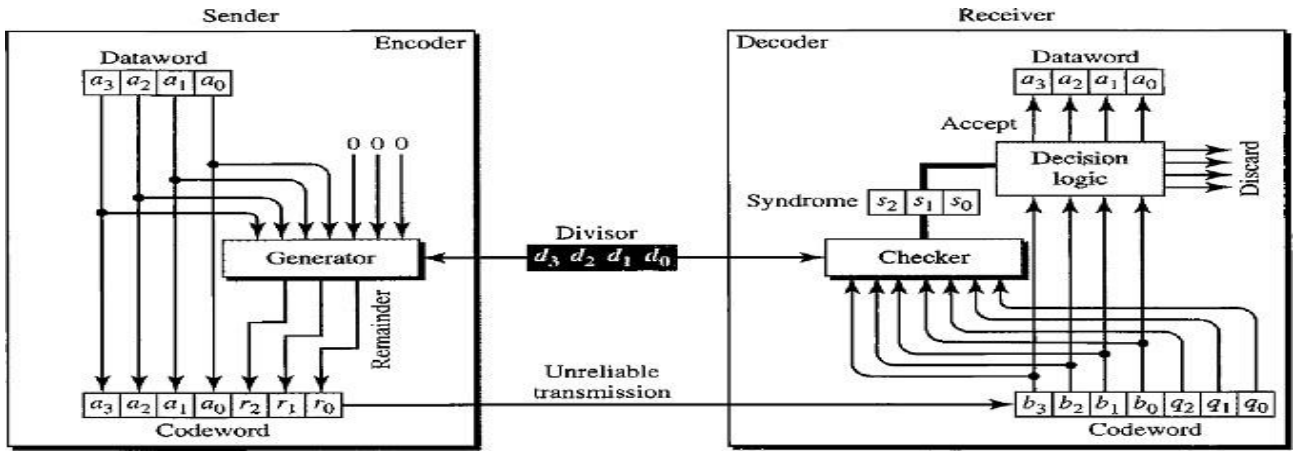
Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference.(Noise in the interface makes errors)

Single Bit Error	Burst Error
Only 1 bit of a given data unit (such as a byte , character , or packet) is changed from1 to 0 or from 0 to1. 	2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1. 

- A burst error is more likely to occur than a single-bit error.
- The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits.
- The number of bits affected depends on the data rate and duration of noise.
- For example, if we are sending data at I kbps, a noise of 11100 s can affect 10bits; if we are sending data at 1Mbps, the same noise can affect 10,000 bits.

Cyclic Redundancy Check(CRC)



CRC is used in networks such as LANs and WANs. We can create cyclic codes to correct errors. The above figure is a possible design for the encoder and decoder.

CRC Encoder

- **In** the encoder, the dataword has **k bits** and the codeword has **n bits**.
- The size of the dataword is augmented by adding**(n–k)numberof0'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 sender and reciever.
- The generator divides the augmented dataword by the divisor **(modulo-2division)**.
- The quotient of the division is discarded;
- The remainder (**$r_2 r_1 r_0$**) is appended to the dataword to create the codeword.
  Let us take
  k=4 bits
  n=7bits
  Appended Dataword Size = **(n-k)** = 3.
  Divisor Size= **(n-k+1)**=4.

Decoder

- The decoder receives the possibly corrupted codeword.
- A copy of all *n* bits is fed to the checker which is a replica of the generator.
- The remainder produced by the checker is a syndrome of *n-k* (3here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function.
- If the syndrome bits are all 0‟s, the 4 leftmost bits of the codeword are accepted as the dataword (interpreted as no error); otherwise, the4bits are discarded (error).

Example: A CRC code with C(7,4)

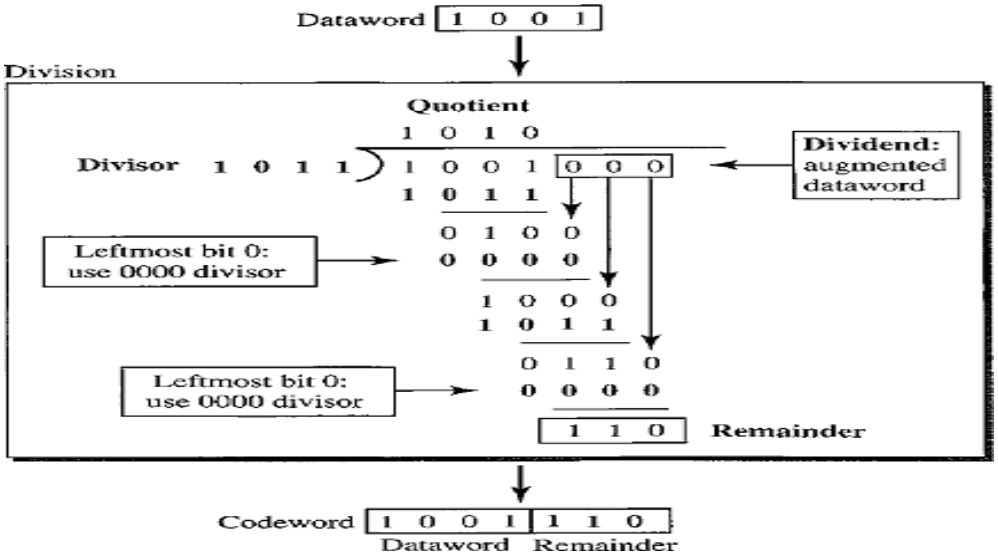
Dataword	*Codeword*	*Dataword*	*Codeword*
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111

In the above table the dataword size is 4 and codeword size is 7.Codeword can be obtained by applying the CRC procedure as we mentioned above. Now let us check for the dataword1001and how we get codeword1001110.

Encoder

The encoder takes the dataword and augments it with **(n–k)** number of 0"s.It then divides the augmented dataword by the divisor. Let us take the divisor1011.

The value1011 will agreed by both sender and receiver.



Note: We use XOR operation in the above division.

- As in decimal division, the process is done step by step.
- In each step, a copy of the divisor is XORed with the 4 bits of the dividend.
- The result of the XOR operation (remainder) is 3 bits is used for the next step after 1 extra bit is pulled down to make it 4 bits long.
- If the left most bit of the dividend is 0, the step cannot use the regular divisor; we need to use an all-0"s divisor.
- When there are no bits left to pull down, we have a result.
- The 3-bit remainder forms the check bits ($r_2r_1r_0$). They are appended to the dataword to create the codeword.

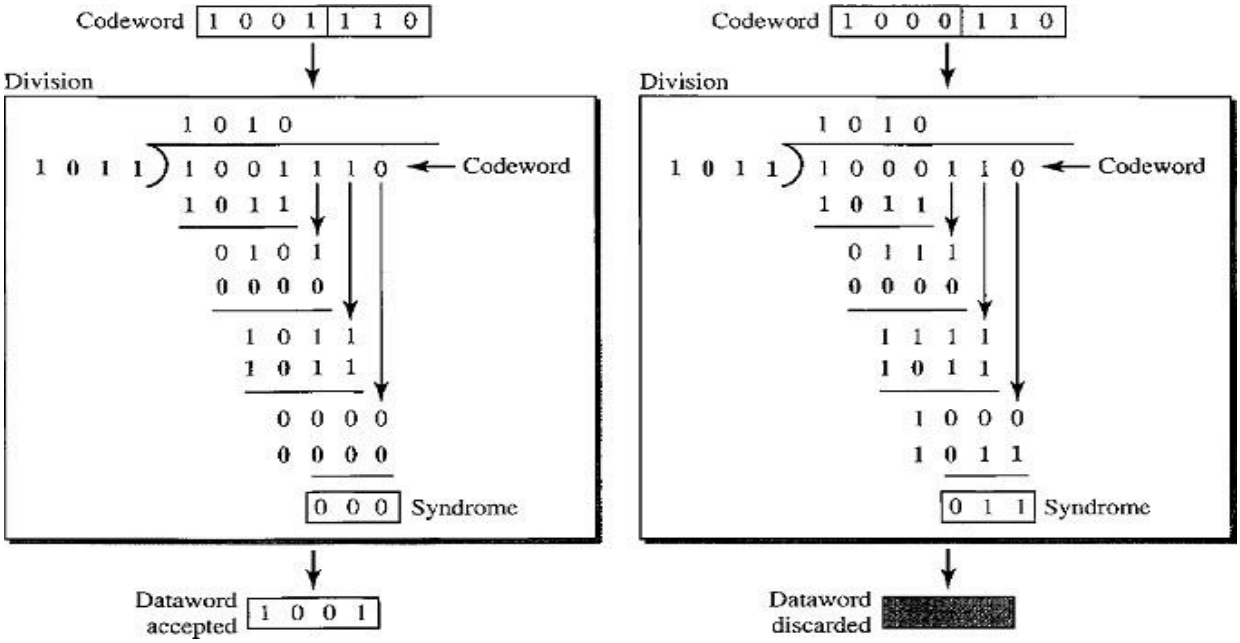
Decoder

- The codeword can change during transmission.
- The decoder does the same division process as the encoder.

- The remainder of the division is the syndrome.
- If the syndrome is all 0"s, there is no error; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded.

The below figure shows two cases:

- The left-hand figure shows the value of syndrome when no error has occurred; the syndrome is 000.
- The right-hand part of the figure shows the case in which there is one single error. The syndrome is not all0"s (it is011).



CHECKSUM

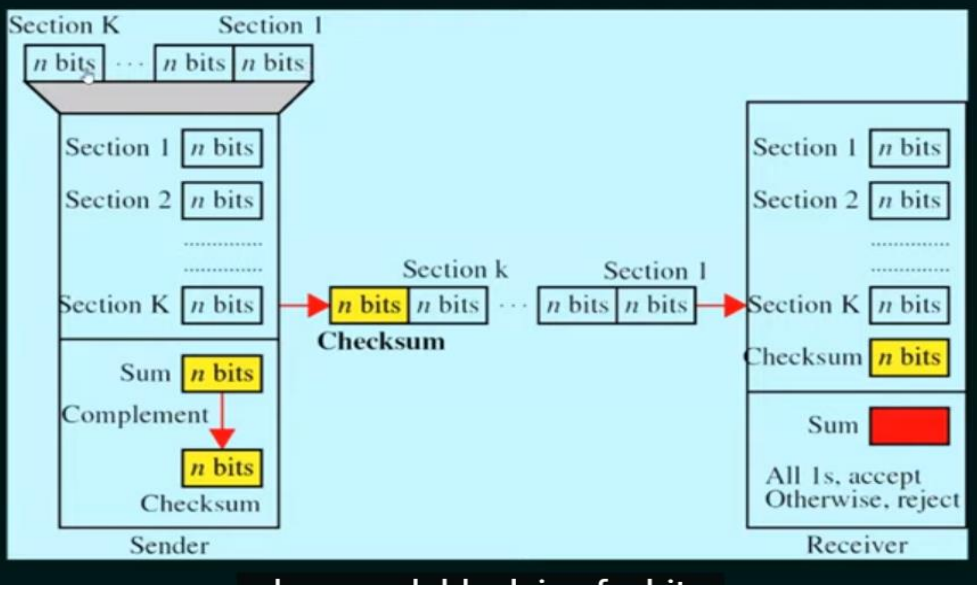
The checksum is used in the Internet by several protocols although not at the data link layer. However, we briefly discuss it here to complete our discussion on error checking.

The checksum is based on the concept of redundancy. Several protocols still use the checksum for error detection

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

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

CHECKSUM



CHECKSUM – OPERATION AT SENDER SIDE

1. Break the original message in to 'k' number of blocks with 'n' bits in each block.
2. Sum all the 'k' data blocks.
3. Add the carry to the sum, if any.
4. Do 1's complement to the sum = Checksum.

CHECKSUM – OPERATION AT RECEIVER SIDE

★ Collect all the data blocks including the checksum.

★ Sum all the data blocks and checksum

*Perform 1'S Complement on the result.
* If All 0's then data is accepted.

Checksum – Example

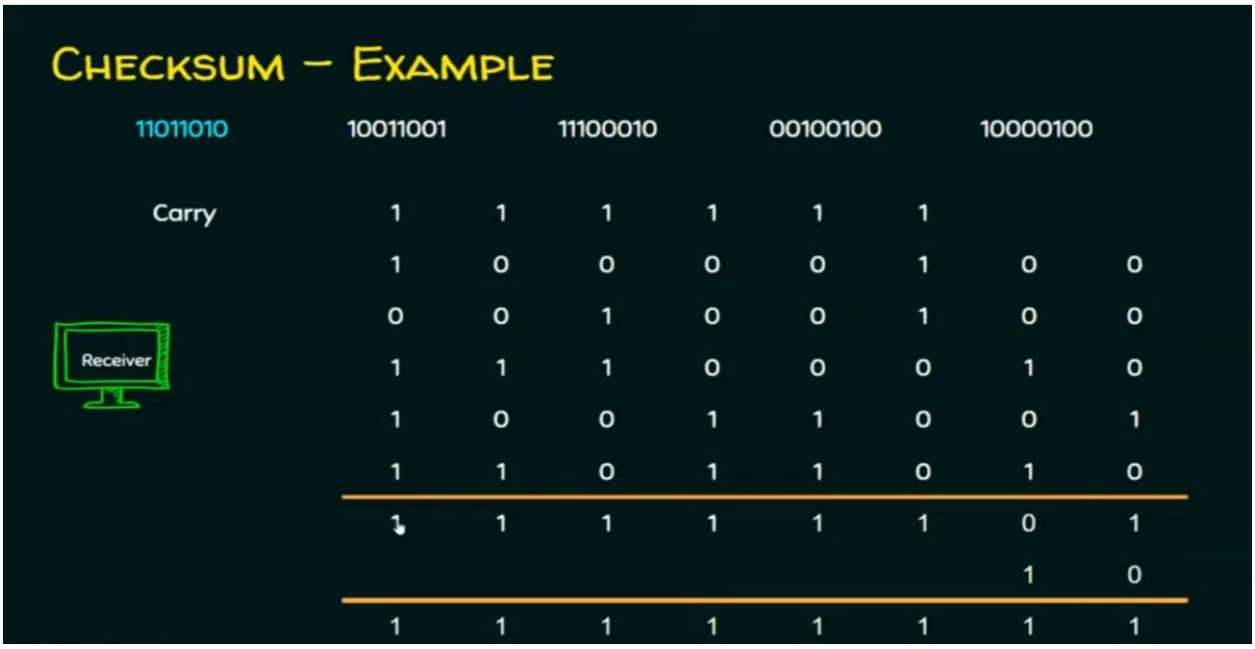
Consider the data unit to be transmitted is:

10011001111000100010010010000100

10011001	11100010	00100100	10000100

Checksum – Example

10011001		11100010		00100100		10000100		
Carry	1	1	1	1	1			
	1	0	0	0	0	1	0	0
	0	0	1	0	0	1	0	0
	1	1	1	0	0	0	1	0
	1	0	0	1	1	0	0	1
	0	0	1	0	0	0	1	1
							1	0
	0	0	1	0	0	1	0	1
1's Complement	1	1	0	1	1	0	1	0



HAMMING CODE

Hamming code is a liner code that is useful for error detection up to two immediate bit errors. It is capable of single-bit errors.

In Hamming code, the source encodes the message by adding redundant bits in the message. These redundant bits are mostly inserted and generated at certain positions in the message to accomplish error detection and correction process.

The process used by the sender to encode the message includes the following three steps:

- Calculation of total numbers of redundant bits.
- Checking the position of the redundant bits.
- Lastly, calculating the values of these redundant bits.

When the above redundant bits are embedded within the message, it is sent to the user.

Step 1) Calculation of the total number of redundant bits.

Calculation of total numbers of redundant bits.

Let assume that the message contains:

n– number of data bits

p – number of redundant bits which are added to it so that np can indicate at least (n + p + 1) different states. Here, (n + p) depicts the location of an error in each of (n + p) bit positions and one extra state indicates no error. As p bits can indicate 2^p states, 2^p has to at least equal to (n + p + 1).

Step 2) Placing the redundant bits in their correct position.

The p redundant bits should be placed at bit positions of powers of 2. For example, 1, 2, 4, 8, 16, etc. They are referred to as p_1 (at position 1), p_2 (at position 2), p_3 (at position 4), etc.

Step 3) Calculation of the values of the redundant bit.

The redundant bits should be parity bits makes the number of 1s either even or odd.

The two types of parity are ?

- **Total numbers of bits in the message is made even is called even parity.**
- The total number of bits in the message is made odd is called odd parity.

Here, all the redundant bit, p1, is must calculated as the parity. It should cover all the bit positions whose binary representation should include a 1 in the 1st position excluding the position of p1.

P1 is the parity bit for every data bits in positions whose binary representation includes a 1 in the less important position not including 1 Like (3, 5, 7, 9, ….)

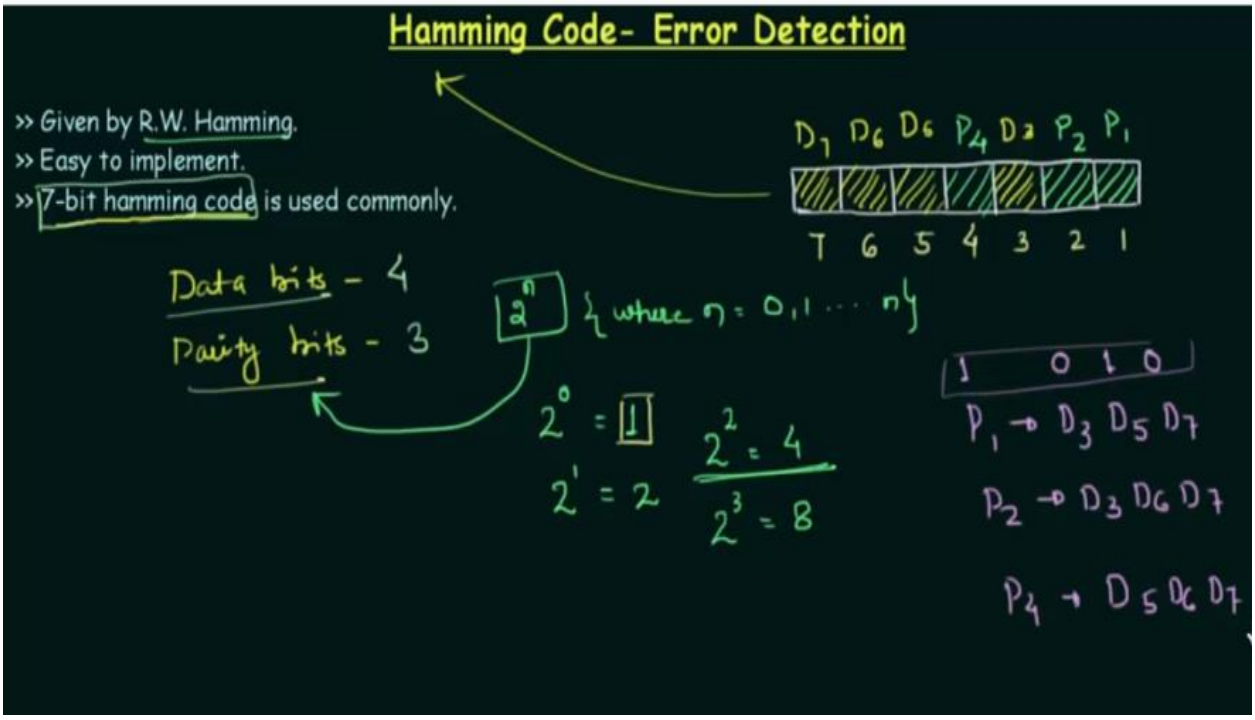
P2 is the parity bit for every data bits in positions whose binary representation include 1 in the position 2 from right, not including 2 Like (3, 6, 7, 10, 11,…)

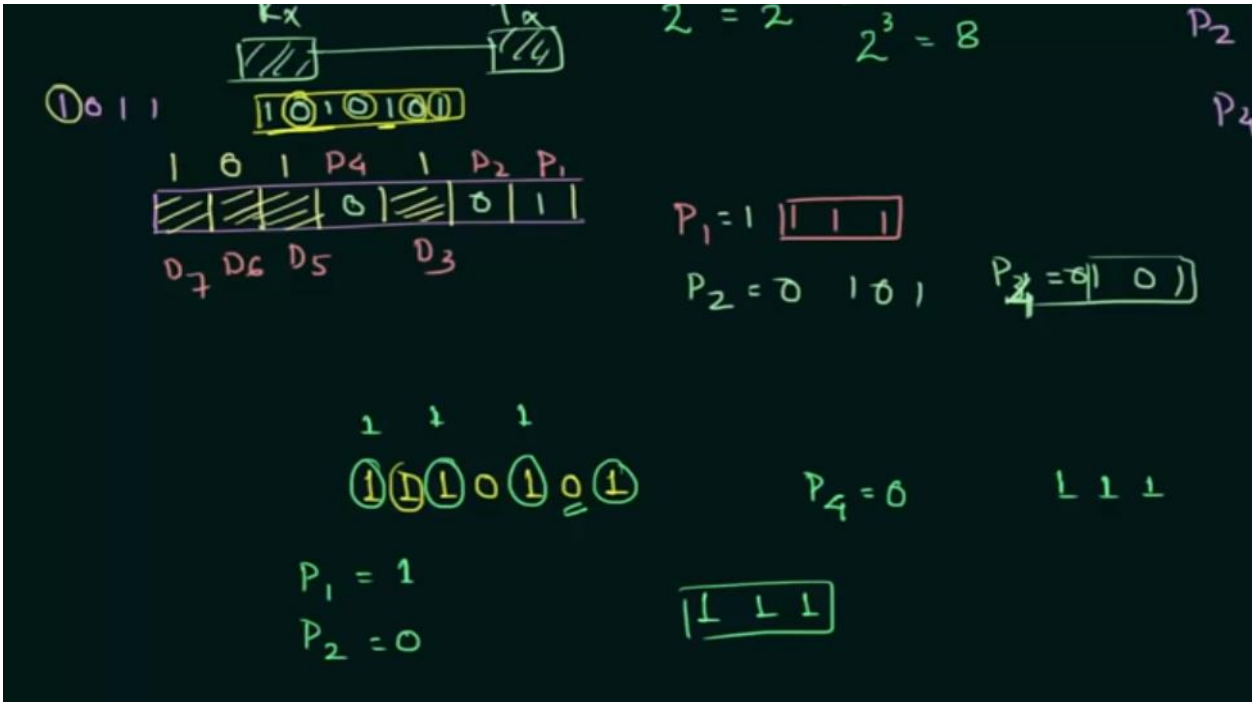
P3 is the parity bit for every bit in positions whose binary representation includes a 1 in the position 3 from right not include 4 Like (5-7, 12-15,…)

Receiver gets incoming messages which require to performs recalculations to find and correct errors.

The recalculation process done in the following steps:

- Counting the number of redundant bits.
- Correctly positioning of all the redundant bits.
- Parity check

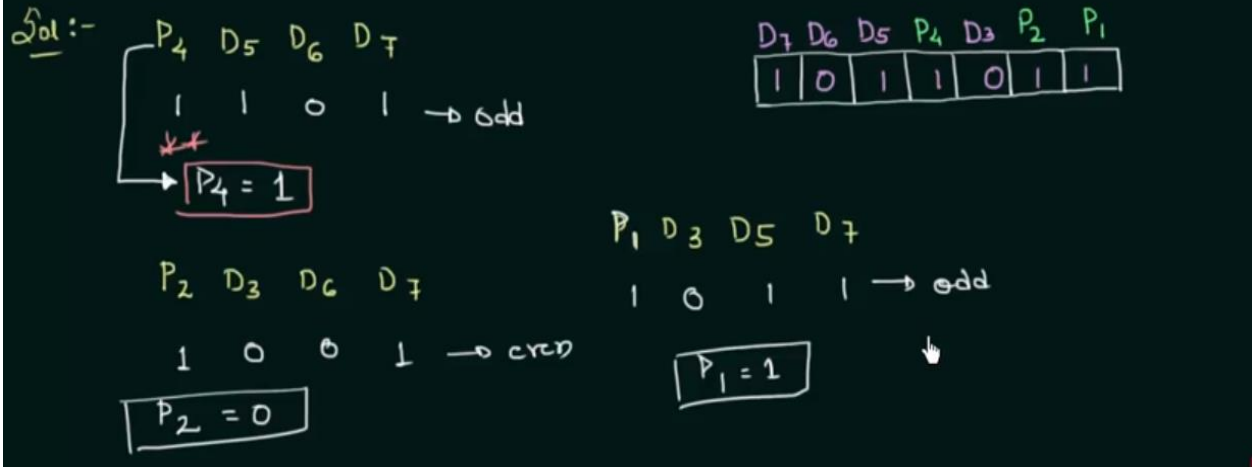


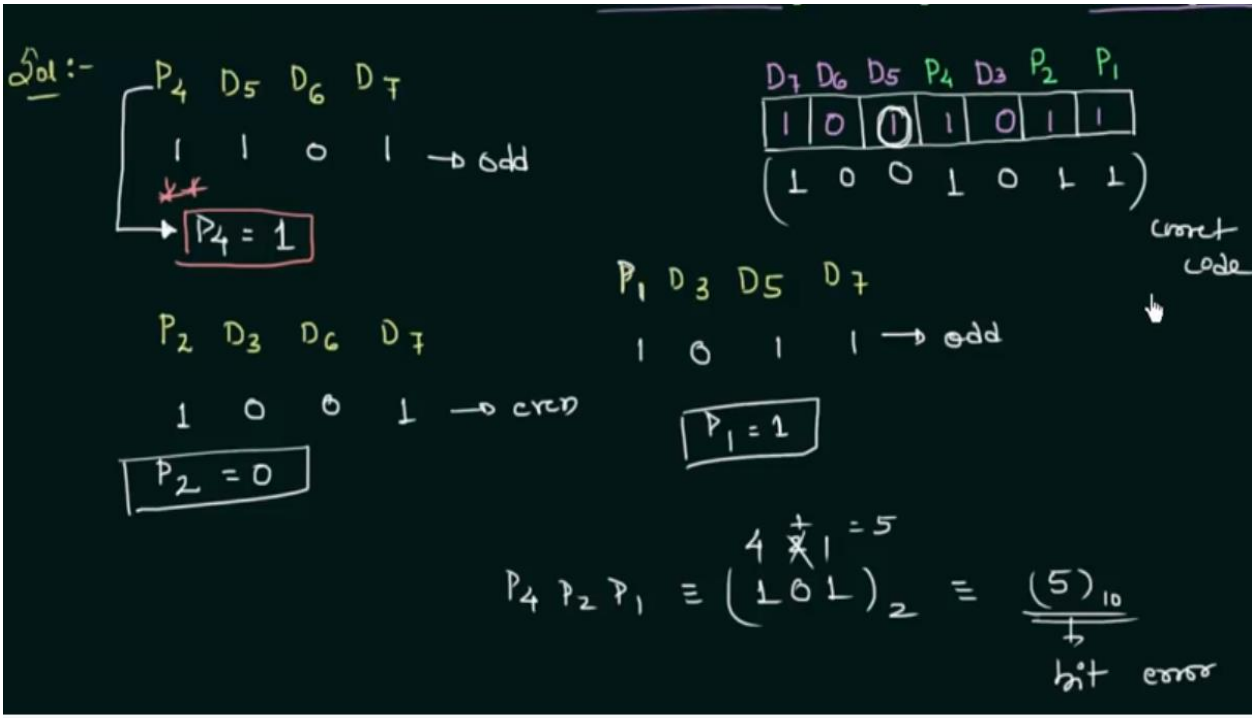


Hamming Code-Error Correction

Ex:- If the 7-bit hamming code word received by a receiver is 1011011. Assuming the even parity state whether the receivrd code word is correct or wrong. If wrong locate the bit having error

Sol:-




Sol :-
P4 D5 D6 D7
1 1 0 1 → odd
P4 = 1
D7 D6 D5 P4 D3 P2 P1
1 0 1 1 0 1 1
(1 0 0 1 0 1 1)
correct code
P2 D3 D6 D7
1 0 0 1 → even
P2 = 0
P1 D3 D5 D7
1 0 1 1 → odd
P1 = 1
4 2 1
P4 P2 P1 ≡ (1 0 1)2 ≡ (5)10
bit error