COMPUTER NETWORKS

Unit – I

Computer Network means the **interconnection** of a set of **autonomous computers**. The term autonomous means that the function of computers is independent of others. However, these computers can exchange information with each other through the communication channels like copper wire, fiber optics, microwaves, infrared, and communication satellites can also be used.

Components:

The five components that make up a data communication are the message, sender, receiver, medium, and protocol.

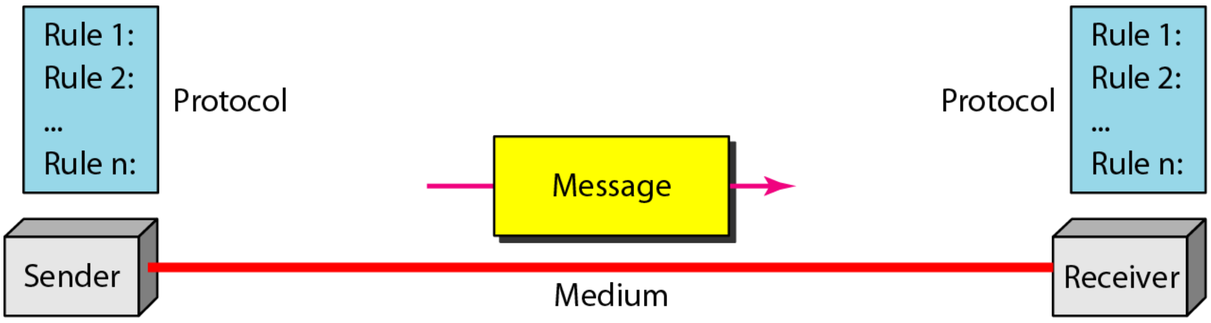
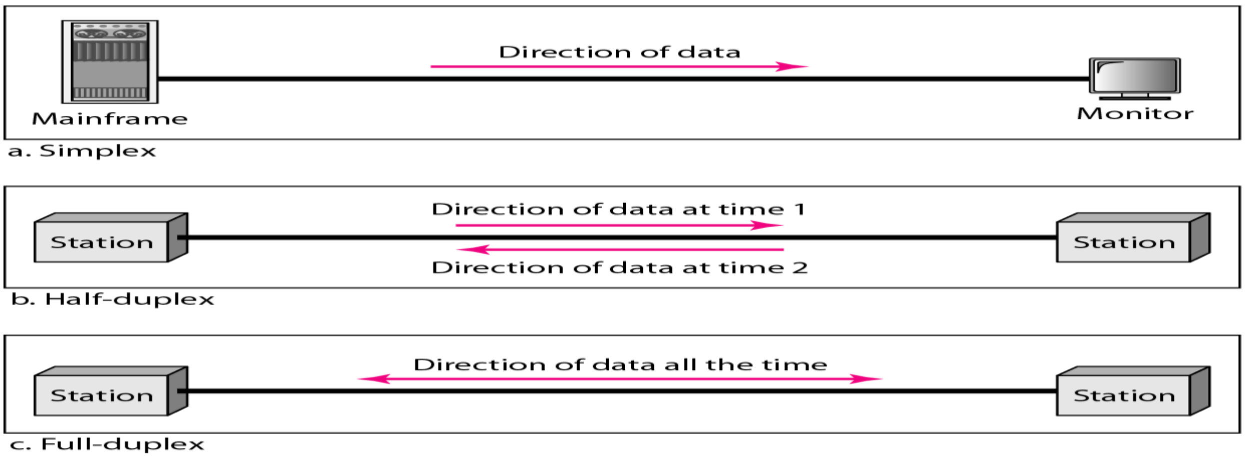


Figure 1.1 Five *components of data communication*

1. **Message:** The message is the information (data) to be communicated. The 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 maintain data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just like a person speaking French cannot be understood by a person who speaks only Japanese.

Data Flow:

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



Simplex :

In simplex mode, the communication is unidirectional, as on a one-way road. Only one of the two devices on a link can transmit; the other can only receive (see Figure a).

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only give input; the monitor can only accept output. The simplex mode can use the entire capacity of the communication channel to send data in one direction only

Half-Duplex :

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

The half-duplex mode is like a one-lane street with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. **Walkie-talkies** are half-duplex system.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.

Full-Duplex :

In full-duplex mode (also called duplex), both systems can transmit and receive simultaneously (see Figure c).

The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. 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 the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is **the telephone network**. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.

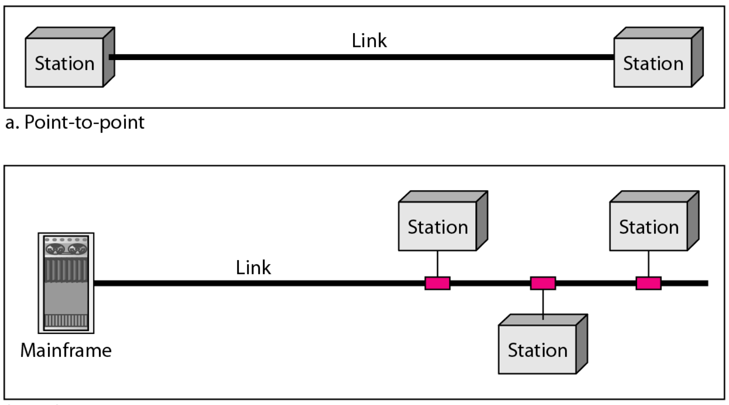
NETWORKS:

A network is a set of devices (often referred to as *nodes)* connected by communication 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.

Physical Structures

Type of Connection:

There are two possible types of connections: **point-to-point and multipoint**.



a. Point-to-point

b. Multipoint

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

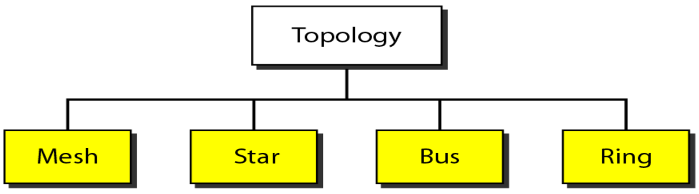
Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure b).

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.

Topology:

The term ***topology*** refers to the way in which **a network is laid out physically: two or more devices connect to a link; two or more links form a topology**. The **topology** of a network is the **geometric representation of the relationship of all the links and linking devices** (usually called nodes) to one another.

There are **four basic topologies possible: mesh, star, bus, and ring**



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

One practical example of a mesh topology is the connection of **telephone regional offices** in which each regional office needs to be connected to every other regional office.

To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - 1 nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to n-1 nodes. However each physical link allows communication in both directions (duplex mode).

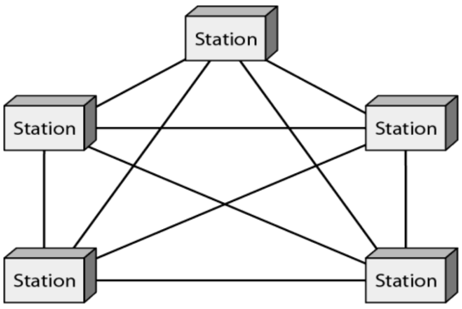


Figure: ***A fully connected mesh topology (five devices)***

Advantages of mesh topology:

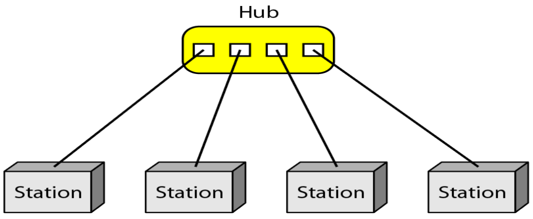
- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not fail the entire system
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the specific recipient sees it. Dedicated links prevent other users from accessing the messages.
- Finally, point-to-point links make fault identification and fault correction easy.

Disadvantages of mesh topology:

- The amount of cabling and the number of I/O ports required are high.
- Every device must be connected to every other device, installation and reconnection are difficult.
- The bulk wiring can be greater than the available space (in walls, ceilings, or floors).
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology: In a star topology, each device has a dedicated **point-to-point link** only to a central controller, usually called a **hub**. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then transfers the data to the other connected device.

The star topology is used in **local-area networks (LANs**),



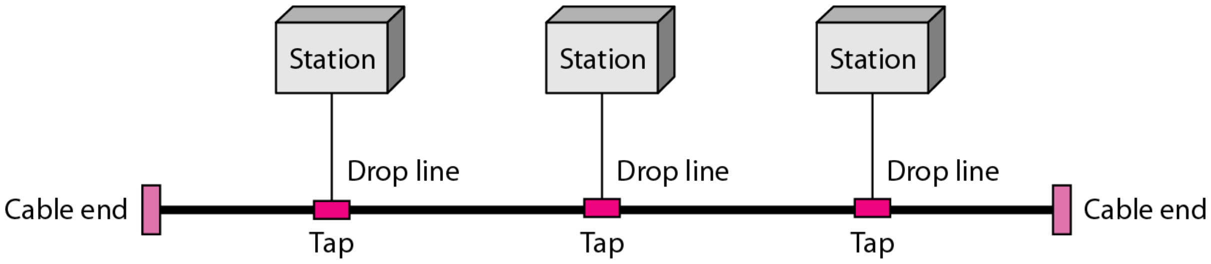
Advantages of star topology

- 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.
- less cabling needs to be housed
- Any additions, moves, and deletions involve only one connection: between that device and the hub.
- If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault correction.

Disadvantages of star topology

- Star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus Topology: A **bus topology** is multipoint. One long cable acts as a **backbone** to link all the devices in a network



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 either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core**. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Bus topology was the one of the first topologies used in the design of early **local area networks**. Ethernet LANs can use a bus topology, but they are less popular now

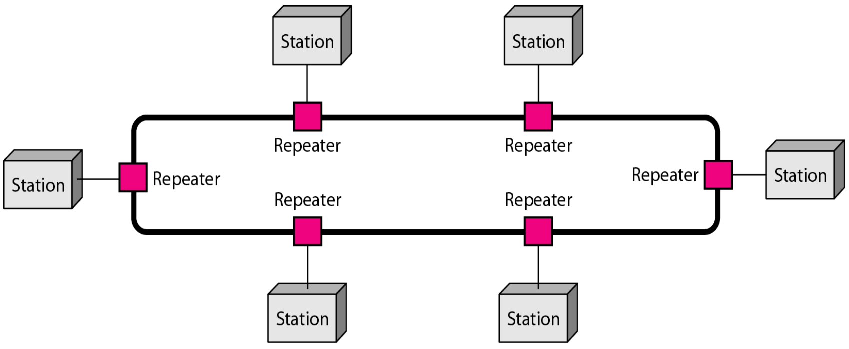
<u>Advantages of bus topology</u>

- ease of installation
- In a bus, this redundancy is eliminated.

<u>Disadvantages of bus topology</u>

- difficult reconnection and fault isolation
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- A fault or break in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

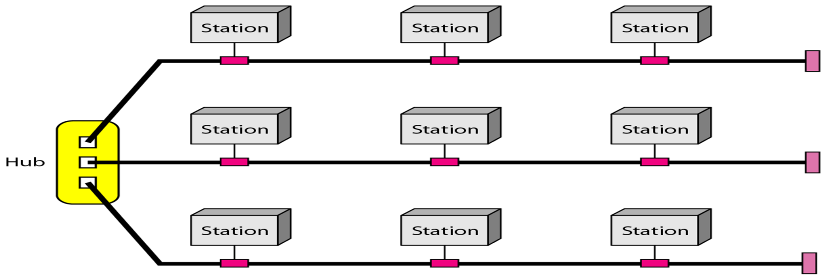
<u>Ring Topology:</u> In a ring topology, each device has a dedicated **point-to-point** connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. **Each device in the ring incorporates a repeater**. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



<u>Advantages of ring topology:</u>

- easy to install and reconfigure
- Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections

Hybrid Topology: A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure

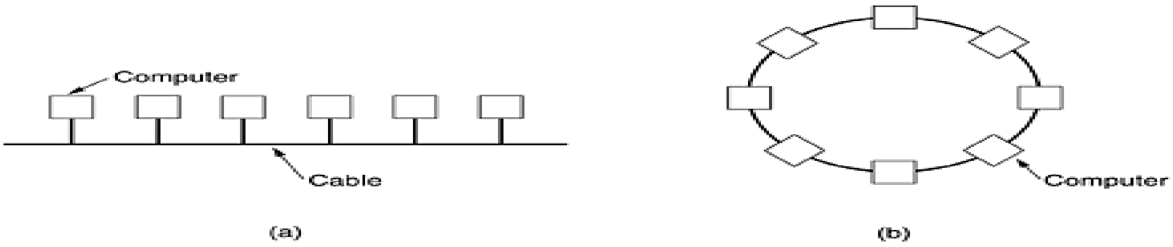


<u>Network Models</u>

There are 3-types of network models they are **Local-area networks**, **Metropolitan area networks** and **wide-area networks**. The type of a network is determined by its size.

Local Area Network

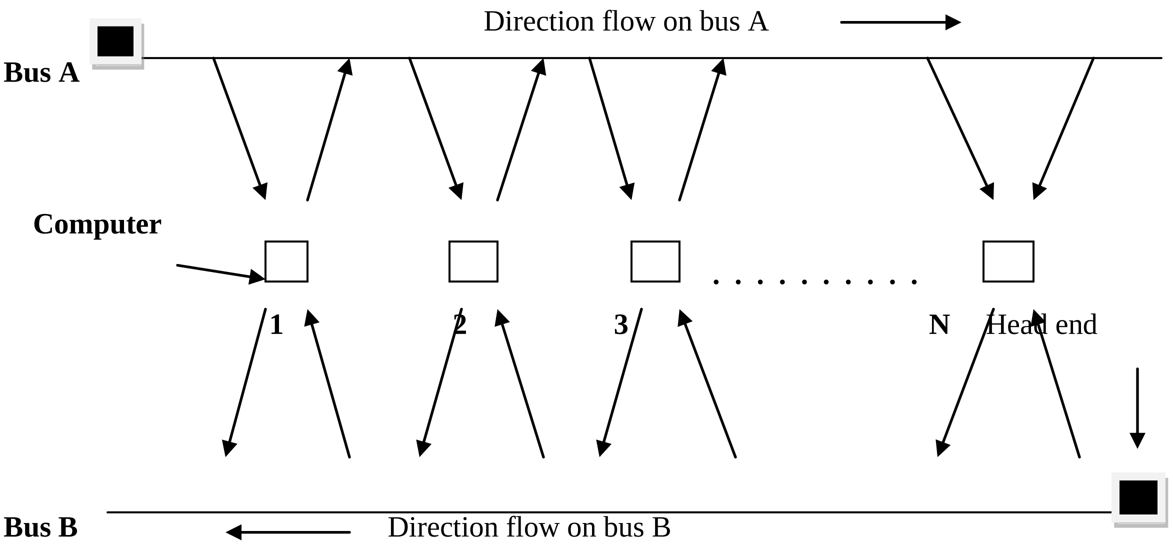
- A local area network is generally called as LANs; these are privately-owned networks with in a single building single or campus of up to a few kilometers in size.
- LANs are widely used to connect personal computers and work stations in company offices and factories to share resources like printers, and to exchange information.
- LANs are different from other networks by three characteristics (1).With their size, (2). With their transmission technology. (3).their topology.
- Currently, LAN size is limited to a few kilometers.
- LANs use a transmission Technology consisting of a single cable to which all the systems are attached, like a telephone lines.
- LANs run at a speed of 10 to 100 Mbps (mega bits/sec), having a low delay and make very few error



- Various Topologies are used for broadcasting the LANs. **The most common LAN topologies are bus, ring, and star**.
- Here it uses IEEE 802.3 popularly known as Ethernet, and IEEE 802.5 IBM Token ring

Metropolitan Area Networks

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally uses similar technology of LAN and covers the area inside a town or a city.
- Here we are using IEEE 802.6 known as DQDB(distributed queue dual bus) which contains to unidirectional buses to which all the computers are connected.
- Both the buses contain Head-End which initiates the transmission. The traffic of right side of the sender uses upper bus. And to send left side uses lower one.
- It is designed for customers who need a high-speed connectivity.

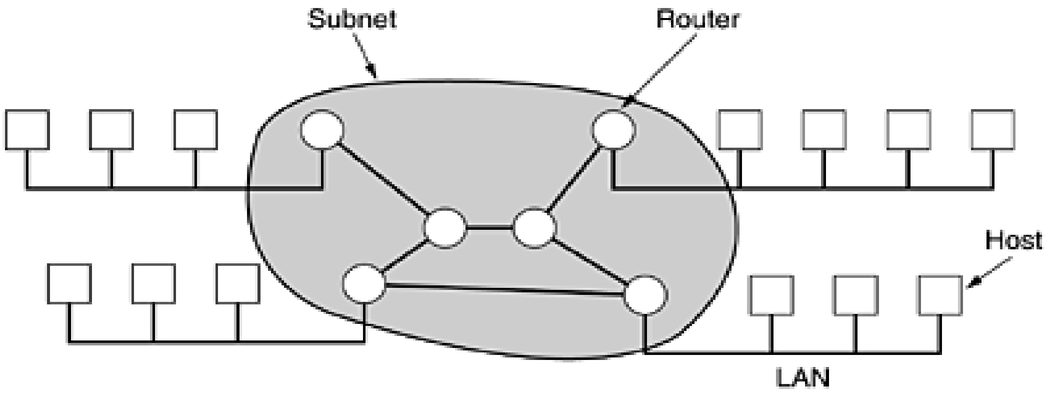


Wide Area Network

WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In WANs systems are connected by a communication subnet or subnet. The job of the subnet is to carry messages from system to the system, just like a telephone which carries words from speaker to speaker

In most wide area networks the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines are also called as circuits, channels or trunks move bits between machines.

The switching elements are specialized computers used to connect two or more transmission lines connecting multiple networks known as routers.



A subnet is a point-to-point, store and forward or packet-switched subnet. Nearly all subnets are **S**tore and **F**orward subnets. Some of the possible topologies for a Point-to-Point subnets are Star, Ring, Tree, etc.

Another possibility of WAN is a satellite, where Each router has an antenna which can send and receive.

THE OSI MODEL

The OSI model is based on the proposal developed by International Standards Organization (ISO) this model is called as ISO-OSI (Open Systems Interconnection) Reference Model because it is used for connecting the open systems. That is the systems which are open for communication with other systems.

It was a first step towards the International standardization of the protocols used in various layers by Day and Zimmermann in 1983.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of **seven** separate but related layers, each of which defines a part of the process of moving information across a network.

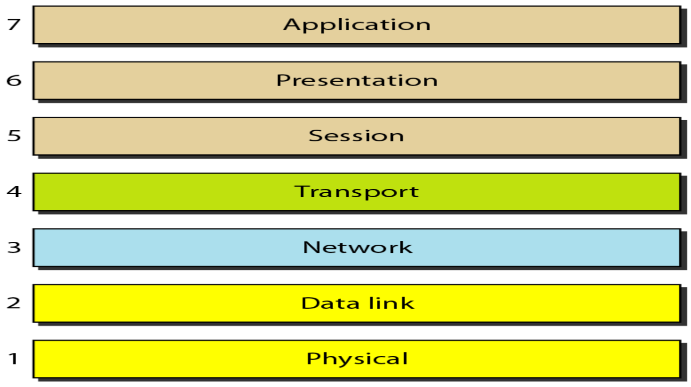


Figure: ***Seven layers of the OSI model***

The Following Figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

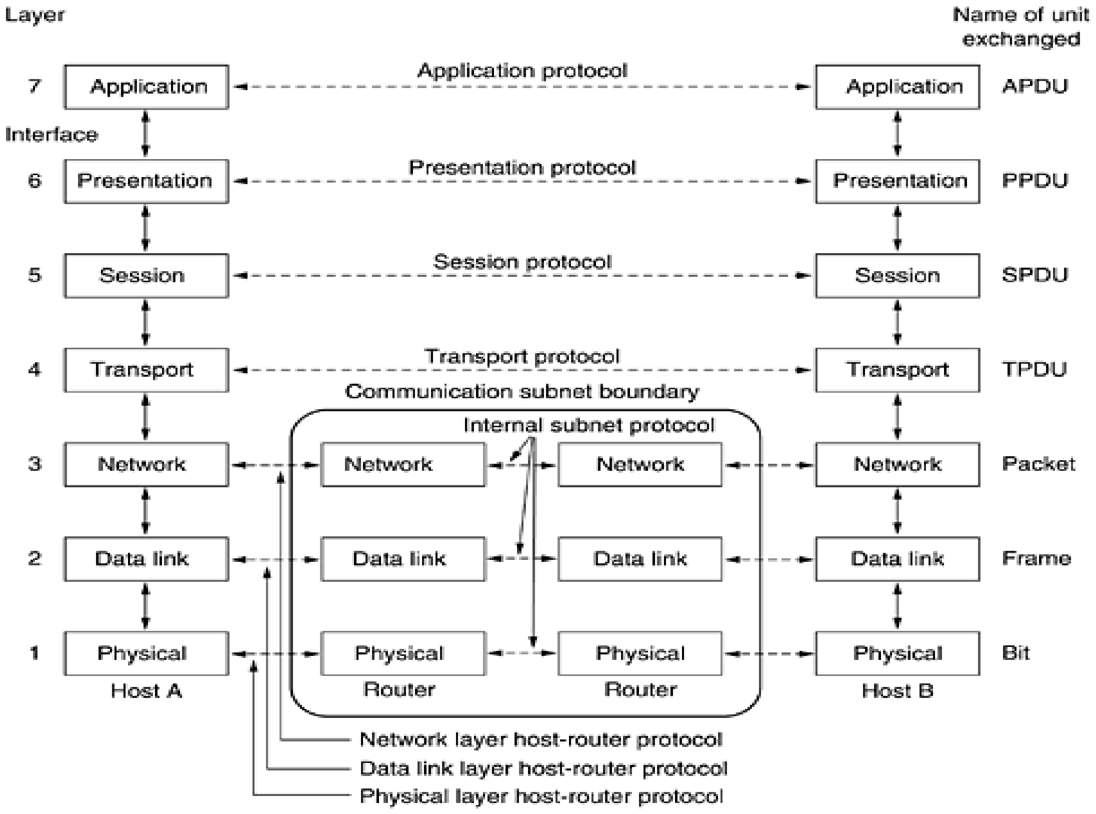


Figure: ***The OSI reference model***

The seven layers of the OSI model are divided into **three subgroups**.

Layers 1, 2, and 3-physical, data link, and network layers are known as **network support layers;** Because 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**).**

Layers 5, 6, and 7-session, presentation, and application layers are known as **the user support layers**; they allow interoperability among unrelated software systems.

Layer 4, 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. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

LAYERS IN THE OSI MODEL : Physical Layer :

The physical layer is used for transmitting the raw bits over a communication channel. Here if the system at one side sends 1bit, it is received by the other side also as a 1bit, not as a 0 bit. The functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.

Following figure shows the position of the physical layer with respect to the transmission medium and the data link layer.

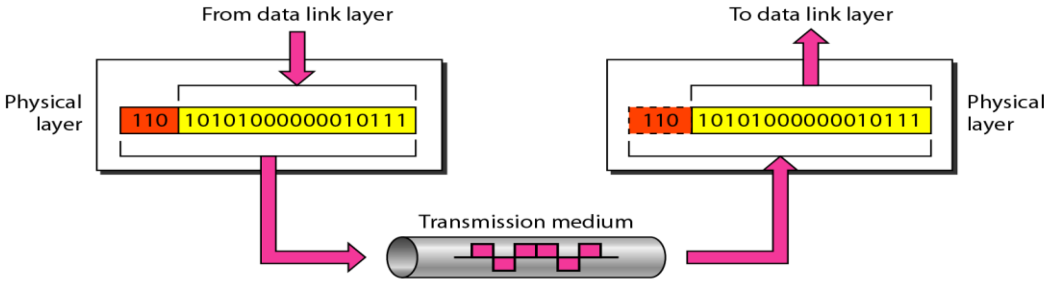


Figure: *Physical layer*

The physical layer is also concerned with the following:

- **Representation of bits:** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical.
- **Data rate:** It represents that how many number of bits can be transferred in each second is also defined by the physical layer.
- **Synchronization of bits:**The sender and receiver both must have to use the same bit rate but also must be synchronized at the bit level.

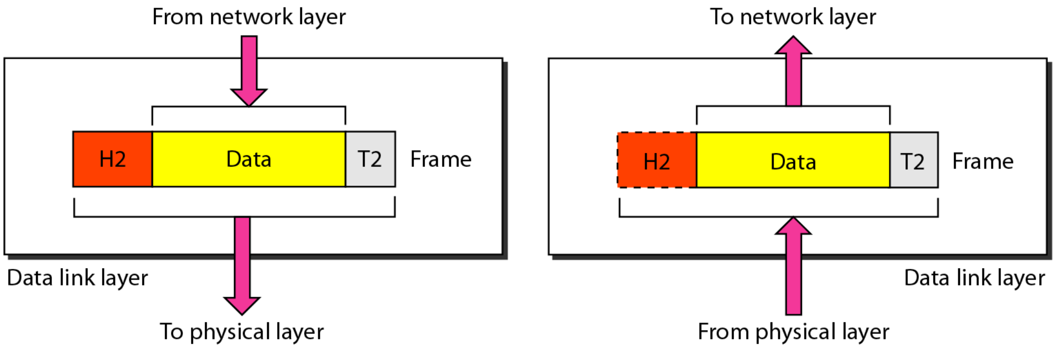
- **Line configuration:** The physical layer is concerned with the connection of devices to the media. In a **point-to-point** configuration, two devices are connected through a **dedicated link**. In a **multipoint** configuration, a link is **shared** among several devices.
- **Physical topology**: The physical topology defines how devices are connected to make a network. Ex: mesh topology, a star topology, a ring topology, a bus topology, a hybrid topology.
- **Transmission mode**: The physical layer also defines the direction of transmission

between the two devices as Simplex, Half-duplex, and Full-duplex.

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear as an error-free to the upper layer (network layer).

Following Figure shows the relationship of the data link layer to the network and physical layers.



- **Framing:** The data link layer divides the stream of bits received from the network layer into 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/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control:** If the rate at which the data is absorbed by the receiver is less than the rate at which data is transferred by thesender, the data link layer uses a flow control protocols to maintain same data transfer rate between sender and the receiver
- **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and correct the 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 to send the data at any given time. Otherwise there is a chance of collision. For this purpose a special sub layer in the data link layer known as medium access sub layer will deal this one.

Network Layer:

The network layer is responsible for the delivery of a packet from source to destination, possibly across multiple networks. The network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is no need for a network layer. However, if the two systems are attached to different networks with connecting devices between the networks, there is often a need for the network layer to maintain source-to-destination delivery.

Following Figure shows the relationship of the network layer to the data link and transport layers.

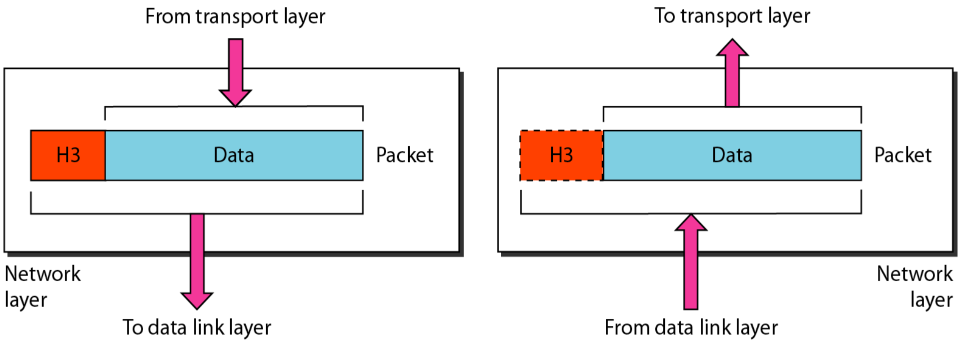


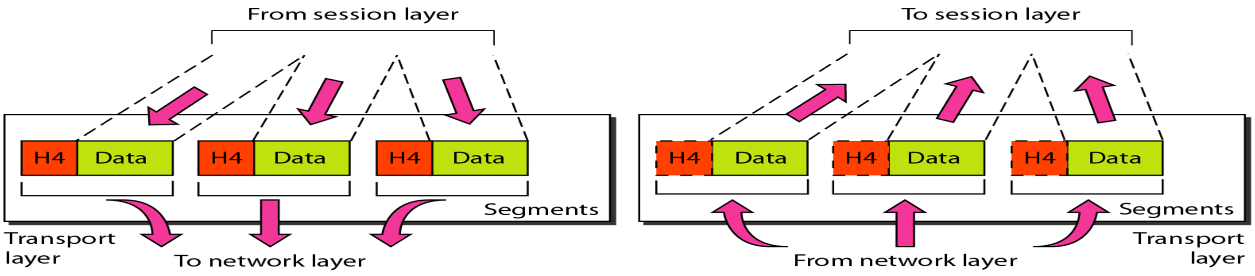
Figure: ***Network layer***

Other responsibilities of the network layer include the following:

- **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing:** When independent networks or links are connected to create internetworks(network of networks) or a large network, the connecting devices (called *routers or switches)* route or switch the packets to their final destination.
- **Congestion Control:** If there is traffic in one way of network for transferring the data. It is known as Congestion, Here we have to find another path for transferring the data by the use of congestion control protocols

Transport Layer:

- The transport layer is responsible **for process-to-process delivery of the entire message**.
- A process is an application program running on a host.
- Whereas the network layer maintainsource-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Following Figure shows the relationship of the transport layer to the network and session layers.



Transport layer

Other responsibilities of the transport layer include the following:

- **Service-point addressing:** Computers often run several programs at the same time. For this reason, 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.
- **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 to identify and replace packets that were lost in 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:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

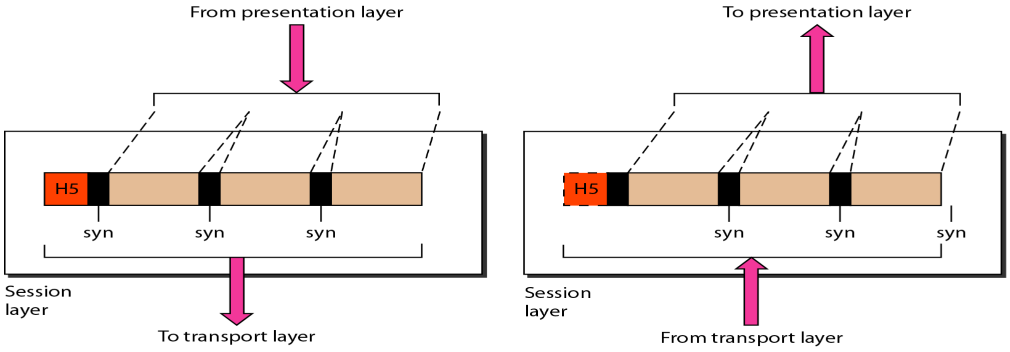
<u>Session Layer:</u>

Session layer allows users on different machines to establish the Sessions , maintain the sessions and synchronize the sessions.

The session layer is responsible for dialog control.

Specific responsibilities of the session layer include the following:

- **Dialog control**: one of the services of the session layer is to manage dialogue control. Sessions allow traffic in one direction or both the directions at the same time. In a network we are having many numbers of systems. If more than one system want to perform the operation, on that case which system will have the priority is the service provided by session layer, it is known as token management
- **Synchronization:** The session layer allows a concept of checkpoints, that if we are transferring a file which may take 2hours between two machines. After the completion of 1 hour if the system crashes, automatically already transferred data will be lost. For that purpose such a huge data will be divided into checkpoints.
- Following Figure illustrates the relationship of the session layer to the transport and presentation layers.



Session layer

Presentation Layer:

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Following Figure shows the relationship between the presentation layer and the application and session layers.

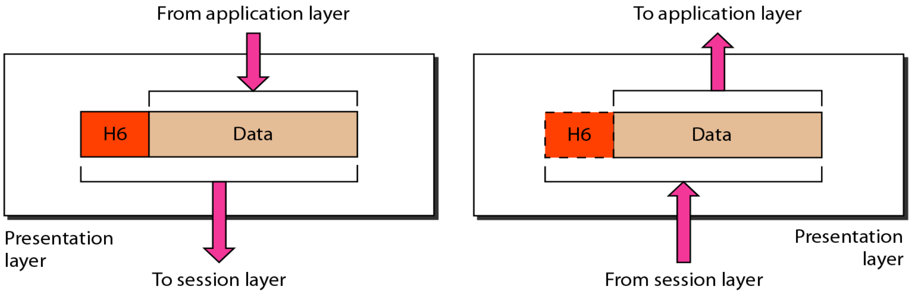


Figure: *Presentation layer*

Specific responsibilities of the presentation layer include the following:

- 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, and so on. The information must be changed to bit 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:** To carry sensitive information, a system must be able to ensure privacy. 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.
- **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 enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- The application layer is responsible for providing services to the user.

  Following Figure shows the relationship of the application layer to the user and the presentation layer..

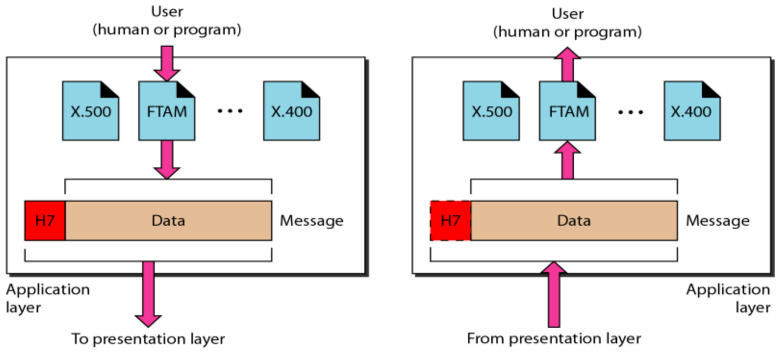
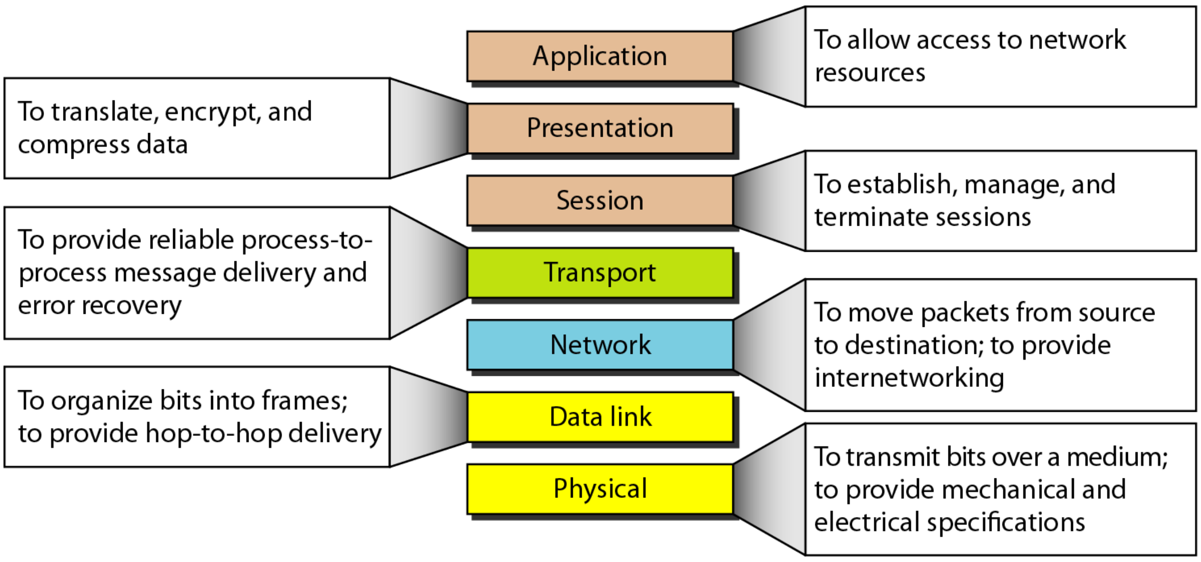


Figure: *Application layer*

Specific services provided by the application layer include the following:

- **Network virtual terminal**. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management**. This application allows a user to access files in a remote host to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services**. This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

Summary of Layers:

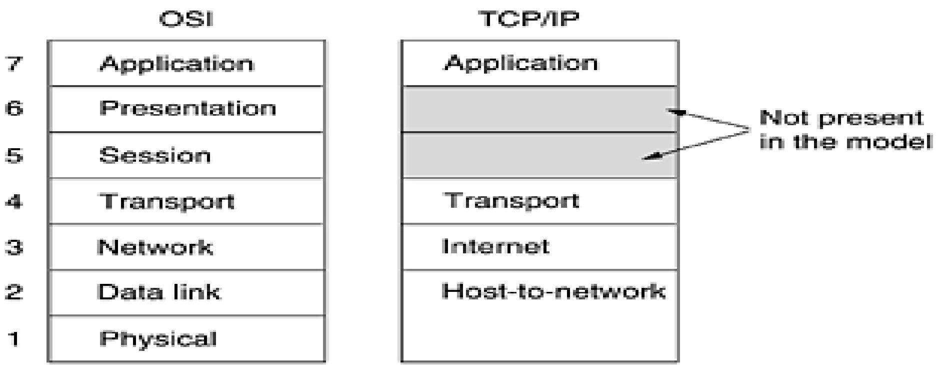

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

The TCP/IP Reference Model :

Let us now turn from the OSI reference model to the reference model used in the grandparent of all wide area computer networks,

The ARPANET, and its successor, the world wide Internet. It is useful to mention a few key aspects of it now. The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundreds of universities and government installations, using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed. This architecture later became known as the **TCP/IP Reference Model**, after its two primary protocols.

The TCP/IP reference model



The Internet Layer:

All these requirements led to the choice of a packet-switching network based on a connectionless internetwork layer. This layer, called the **internet layer**, Its job is to permit hosts to inject packets into any network and have them travel independently to the destination They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called **IP** (**Internet Protocol**). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer.

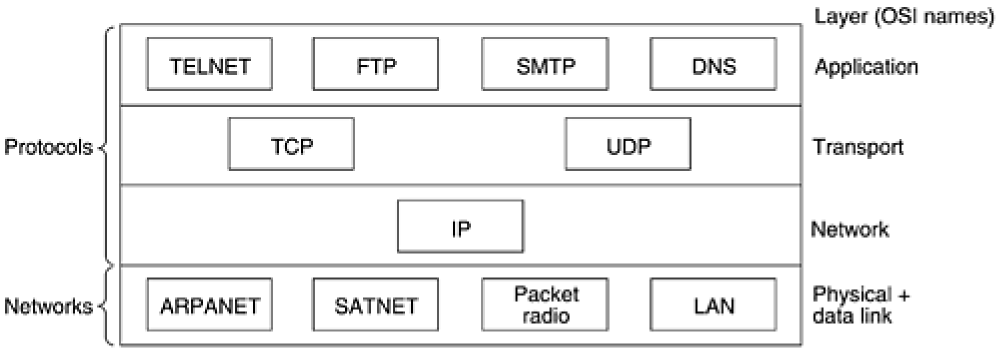
The Transport Layer:

The layer above the internet layer in the TCP/IP model is now usually called the **transport layer**. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, **TCP** (**Transmission Control Protocol**), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot transfer data accurately to a slow receiver with more messages than it can handle.

The second protocol in this layer, **UDP** (**User Datagram Protocol**), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. 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 (SCTP): The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

TCP/IP PROTOCOL SUITE:



- The TCP/IP protocol suite was developed prior to the OSI model.
- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having **four** layers: **host-to-network, internet, transport, and application**
- However, when TCP/IP is compared to OSI, we can say that the 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 application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.
- we assume that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport

functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the *application layer*

- *TCP/IP* is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

  At the transport layer, *TCP/IP* defines three protocols: **Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP)**. At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

The Application Layer:

The TCP/IP model does not have session and presentation layers. No need for them was perceived, so they were not included. Experience with the OSI model has proven that they are of little use to most applications.

On top of the transport layer is the **application layer**. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years. HTTP, The protocol for fetching pages on the World Wide Web.

The Host-to-Network Layer:

Below the internet layer is a great void. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

A Comparison of the OSI and TCP/IP Reference Models:

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented layers, provide users a transport service.

Despite these fundamental similarities, the two models also have many differences. In this section we will focus on the key differences between the two reference models. It is important to note that we are comparing the *reference models* here, not the corresponding *protocol stacks*. Three concepts are central to the OSI model:

1. Services.
2. Interfaces.
3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicitly. Each layer performs some services for the layer above it. The *service* definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.

A layer's *interface* tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, says nothing about how the layer works inside.

Finally, the peer *protocols* used in a layer are the layer's own business. It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services). It can also change them at will without affecting software in higher layers.

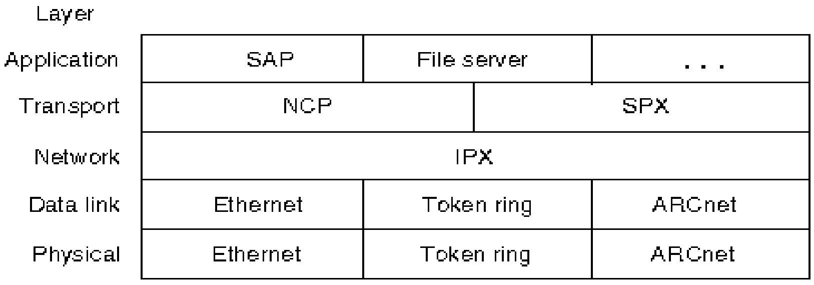
These ideas fit very nicely with modern ideas about object-oriented programming.

The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like. For example, the only real services offered by the internet layer are SEND IP PACKET and RECEIVE IP PACKET.

EXAMPLE NETWORKS:

NOVELL NETWARE: The most popular network system in the pc world is **Novell Netware.** It was designed when the companies are using the network of PCs than the main frame. In the network of PCs each user has a desktop PC functioning as a client, and some other systems works as servers, providing file services, database services. Novell Netware is based on a client server model.

Novell Netware is like an OSI, but is not based on it. It looks like a TCP/IP than the OSI Reference Model.



Layer			
Application	SAP	File server	. . .
Transport	NCP	SPX	
Network	IPX		
Data link	Ethernet	Token ring	ARCnet
Physical	Ethernet	Token ring	ARCnet

Fig 1: The Novell NetWare reference model.

The physical and data link layers can be chosen from among various industrial standards like Ethernet, IBM Token ring and ARCnet. The network layer runs an unreliable connectionless internetwork protocol known as IPX (Internet Packet Exchange). It passes packets transparently from source to destination, even if the source and destination are on different networks. IPX is functionally similar to IP, except that it uses 12-byte addresses instead of 4-byte addresses.

Above to the IPX comes a connection-oriented transport protocol called NCP (Network Core Protocol) it also provides various services like data transport. It is also known as a heart of Netware. A second protocol.SPX (sequenced Packet Exchange) is also available, it provides only transport.

The session and the presentation layers doesn't exist here, various application protocols are present in the application layer. Application layer contains a SAP (service advertising protocol). The packets are seen and collected by a special agent processes running on the router machines.

The format of an IPX packet is shown in the below fig. The *checksum* field is rarely used, since the below data link layer also provides a checksum. The packet length field tells tha actual length of the entire packet is header plus data. The transport control field counts that how many networks the packet has transferred. When this count exceeds a maximum value, then the packet is discarded. The packet type field is used to specify type of various packets.

The two addresses which contain 12 byte addresses each contain 32-bit network number, a 48-bit machine number and a 16-bit local address on that machine.

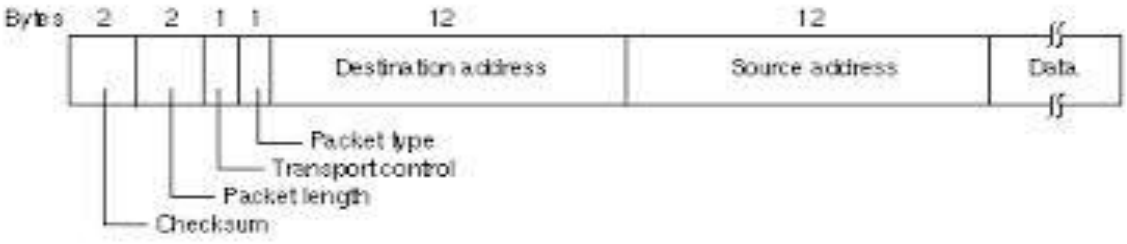


Fig. 2: A Novell NetWare IPX packet.

<u>The ARPANET</u>: ARPA (**Advanced Research Projects Agency).**ARPA was created in response to the Soviet Union's launching "Sputnik" with a mission of advanced technology. Some universities got the idea of packet switching, which was suggested by Paul Baran. After some discussions ARPA decided to build a packet switching network, consisting of a subnet and host computers

The subnet would consist of minicomputers called **IMP**s (**Interface Message Processors**) connected by 56-kbps transmission lines. For high reliability, each IMP would be connected to at least two other IMPs. The subnet was to be a datagram subnet, so if some lines and IMPs were destroyed, messages could be automatically rerouted along alternative paths.

Each node of the network consists of an IMP and a host;A host could send messages of up to 8063 bits to its IMP, then IMP break these into packets of at most 1008 bits and forward them independently toward the destination. So the subnet was the first electronic store-and-forward packet-switching network.

ARPA then put out a tender for building the subnet. Twelve companies bid for it. After evaluating all the proposals, ARPA selected BBN, and awarded it a contract to build the subnet and write the subnet software. BBN chose to use specially modified Honeywell DDP-316 minicomputers with 12K 16-bit words of core memory as the IMPs. The IMPs did not have disks, The IMPs were interconnected by 56-kbps lines leased from telephone companies.

The software was split into two parts: subnet and host. The subnet software consisted of the IMP end to the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability. The original ARPANET design is shown in below figure.

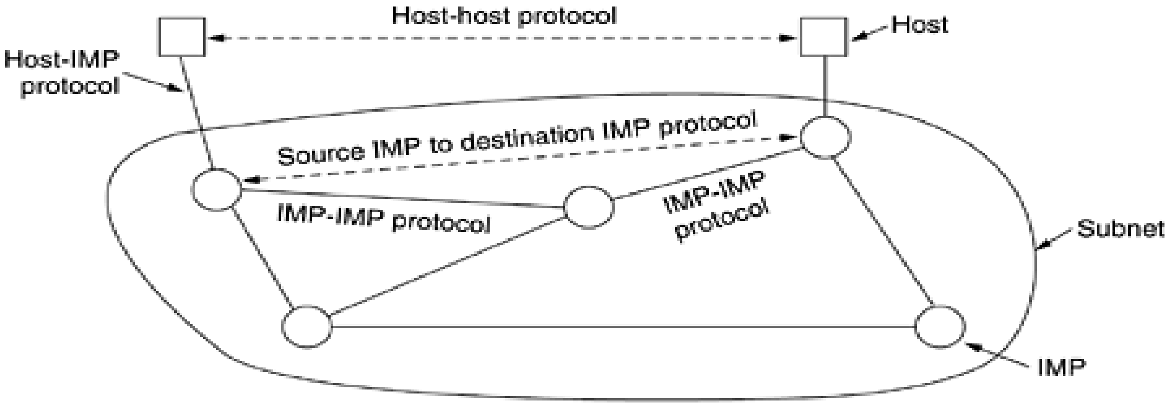


Fig 3: The original ARPANET design

<u>NSFNET</u>: NSF (the U.S. National Science Foundation) saw the enormous impact that the ARPANET was having on university research, allowing scientists across the country to share data and collaborate on research projects. This lack of universal access prompted NSF to set up a virtual network,

CSNET, Centered around a single machine at BBN that supported dial-up lines and had connections to the ARPANET and other networks. NSF decided to build a backbone network to connect its six supercomputer centers,

Each supercomputer was given a little brother, consisting of an LSI-11 microcomputer called a **fuzzball**. The fuzzballs were connected with 56-kbps leased lines and formed the subnet, the same hardware technology as the ARPANET used. The software technology was different however: the fuzzballs spoke TCP/IP right from the start, making it as a first TCP/IP WAN.

NSF also funded some 20 regional networks that connected to the backbone to allow users at thousands of universities, research labs, libraries, and museums to access any of the supercomputers and to communicate with one another. The complete network, including the backbone and the regional networks, was called **NSFNET**. It connected to the ARPANET through a link between an IMP and a fuzzball.

Consequently, NSF encouraged MERIT, MCI, and IBM to form a nonprofit corporation, **ANS** (**Advanced Networks and Services**). In 1990, ANS took over NSFNET and upgraded the 1.5-Mbps links to 45 Mbps to form **ANSNET**.

During the 1990s, many other countries and regions also built national research networks, often patterned on the ARPANET and NSFNET. These included EuropaNET and EBONE in Europe, which started out with 2-Mbps lines and then upgraded to 34-Mbps lines.

<u>INTERNET</u>: The number of networks, machines, and users connected to the ARPANET grew rapidly after TCP/IP became the only official protocol on January 1, 1983. When NSFNET and the ARPANET were interconnected, the growth became exponential.

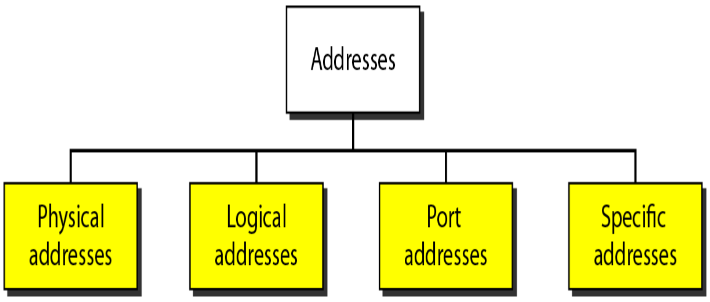
Traditionally the Internet and its predecessors had four main applications:

1. **E-mail.** The ability to compose, send, and receive electronic mail has been around since the early days of the ARPANET and is enormously popular. Many people get dozens of messages a day and consider it their primary way of interacting with the outside world, far outdistancing the telephone and snail mail. E-mail programs are available on virtually every kind of computer these days.
2. **News.** Newsgroups are specialized forums in which users with a common interest can exchange messages. Thousands of newsgroups exist, devoted to technical and nontechnical topics, including computers, science, recreation, and politics. Each newsgroup has its own etiquette, style, and customs, and woe betide anyone violating them.

3. **Remote login.** Using the telnet, rlogin, users anywhere on the Internet can log on to any other machine on which they have an account.
4. **File transfer.** Using the FTP program, users can copy files from one machine on the Internet to another. Vast numbers of articles, databases, and other information are available this way.

ADDRESSING

Four levels of addresses are used in an internet employing the *TCP/IP* protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses



Physical Addresses

- The physical address, also known as the **link 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.

Logical Addresses

- 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.
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- The logical addresses are designed for this purpose. 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.

Port Addresses

- 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.
- 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 a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a **port address**. A port address in TCP/IP is 16 bits in length.

Specific Addresses

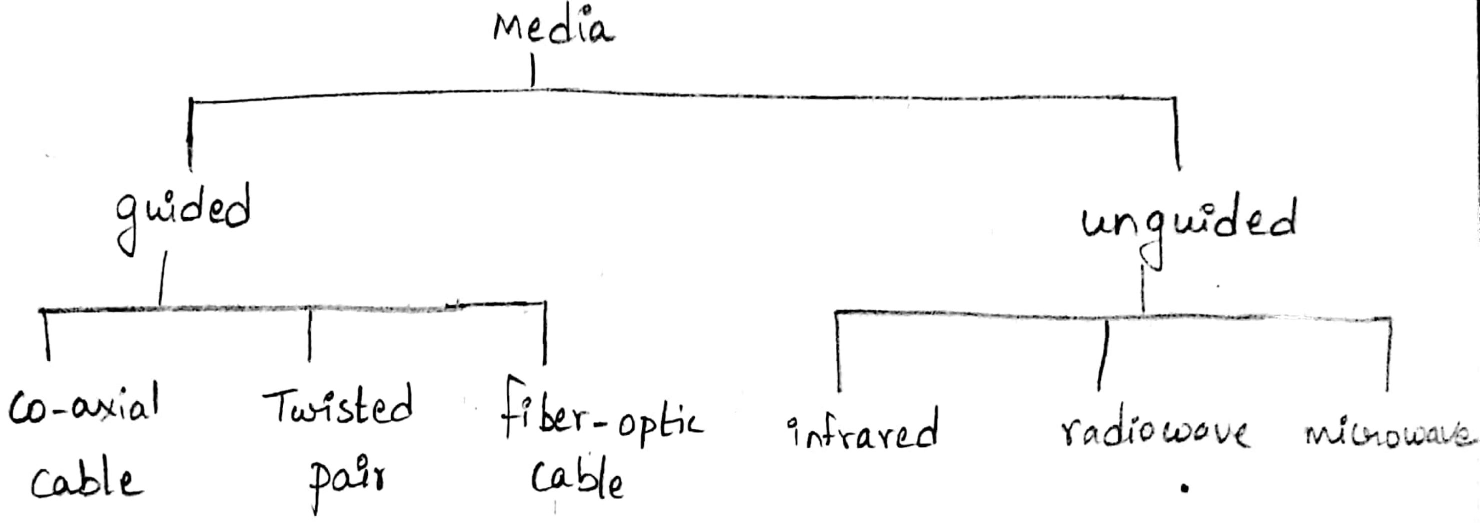
Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address (for example, sacet@ac.in) and the Universal Resource Locator (URL) (for example, www.sacet.ac.in).

Transmission media :-

→ Transmission medium: It is the physical path between the sender & receiver in a data transmission system.

- It is included in the physical layer of the OSI protocol.

Ex:- free space, metallic cable, fiber-optic cable



Guided Transmission media :

- It uses a cabling system that guides the data signals along a specific path.
- Data signals are bound by the cabling system.
- So, it is also known as Bound Media.
- Only the devices physically connected to the medium can receive data signals propagating through a guided transmission media.

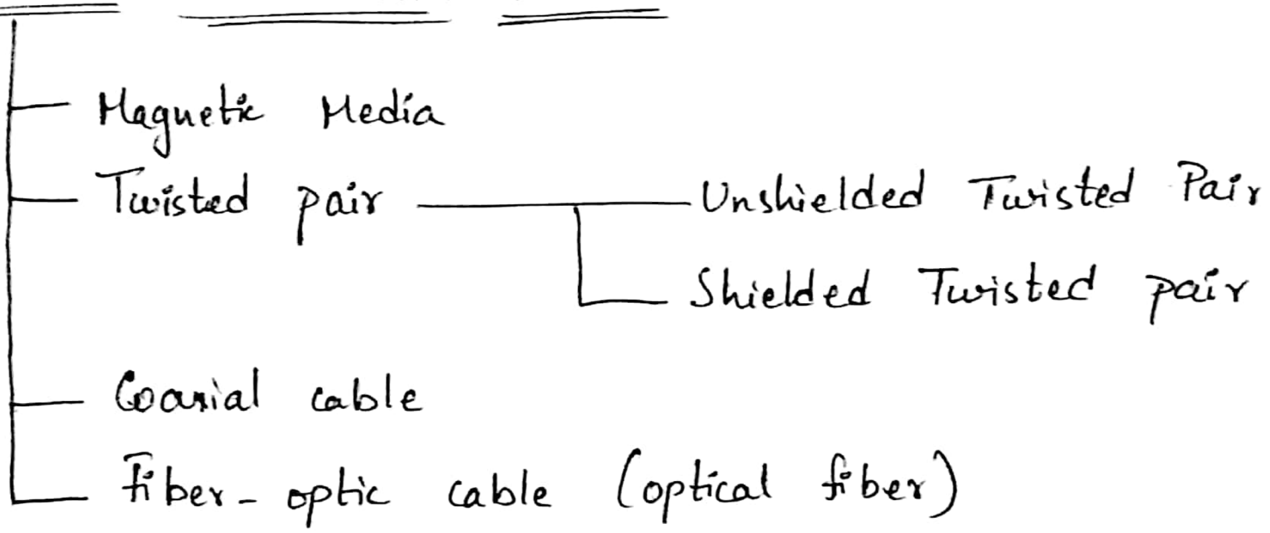
Ex:- Copper wire, optical fiber.

Unguided Transmission media:

- It consists of a means for the data signals to travel but nothing to guide them along a specific path.
- The data signals are not bound to a cabling system. So, they are called Unbound media

Ex:- Wireless Systems.

Guided Transmission media :



(1) Magnetic Media:

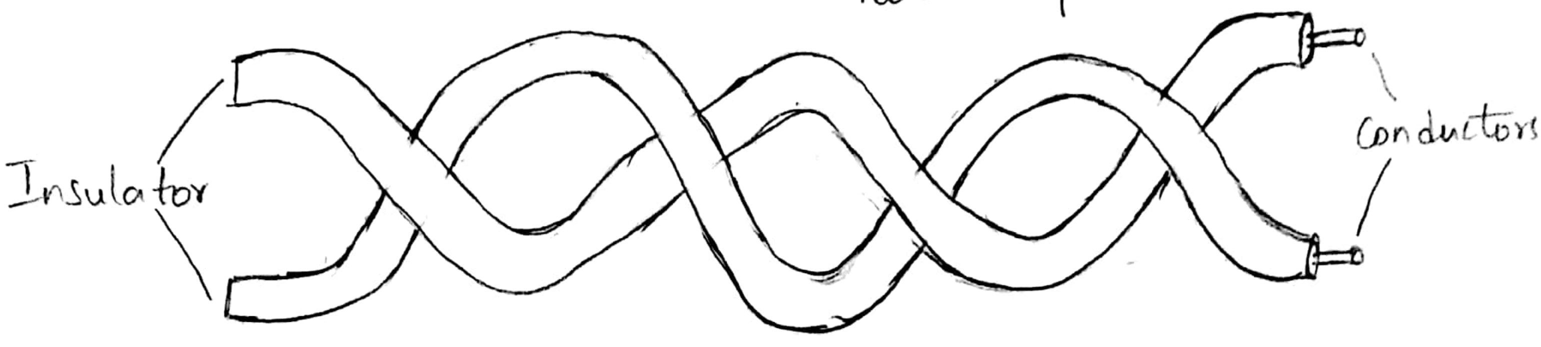
- In this, data is transported from one computer to another by writing the data onto magnetic tape or removable media. (eg., recordable DVDs)
- Then physically transport the tape or disks to the destination machine, and read them back in again.

(2) Twisted pair :

- It is the simplest, oldest and low priced cable medium.

∴ It is made up of two insulated copper wires about 1mm thick, twisted around each other.

Twisted-pair cable.



- Twisted pairs can be used for transmitting either analog or digital signals.
- The bandwidth depends on the thickness of the wire and the distance travelled.
- Two basic types of twisted-pair cable exist.

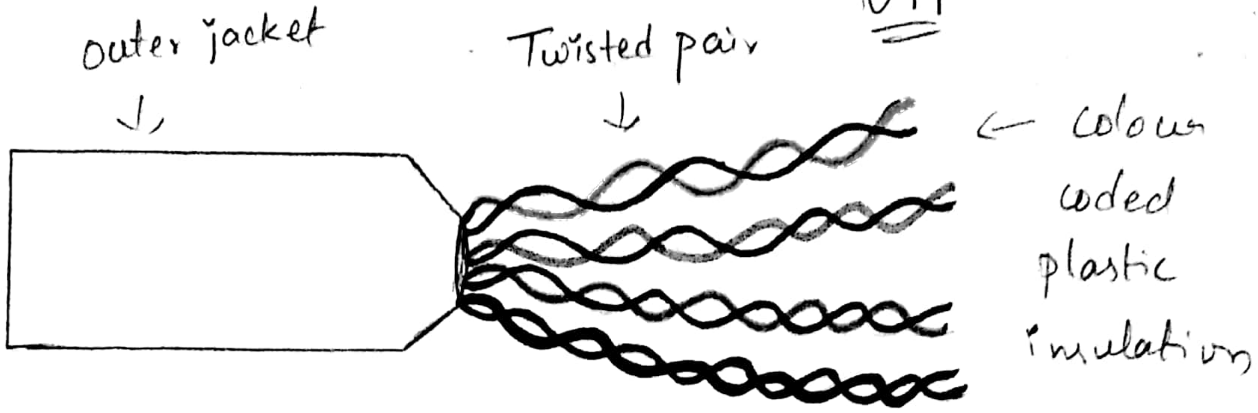
  Unshielded Twisted Pair (UTP)

  Shielded Twisted Pair (STP)
- Transmission links may be simplex or Half Duplex or Full Duplex in mode.

Unshielded Twisted pair :

- It is one of the most popular LAN cables.
- This cable consists of 4 twisted pairs of metal wires (ie., 8 wires in the ~~t~~cable).

UTP



- Each pair is twisted with a different number of twists per inch to eliminate interference from adjacent pairs and other electrical devices
- Each twisted pair consists of two metal conductors that are insulated separately with their own coloured plastic insulation.
- UTP cable relies on cancellation effect produced by twisted wire pairs to limit the signal degradation caused by electromagnetic interference and radio frequency interference.
- RJ-45 connector: UTP cable is installed using a RJ-45 connector. (Registered- Jack Connector). RJ-45 is an eight-wire connector used commonly to connect computers onto a LAN, esp ethernet.

- UTP cables are suited for both data & voice transmissions commonly used in telephone systems.

- They are also widely used in DSL lines, 10BaseT, 100Base-T LAN.

Adv:- It is the cheapest media
Easy to Install and maintain
It occupies less space
It is the fastest copper-based medium today.

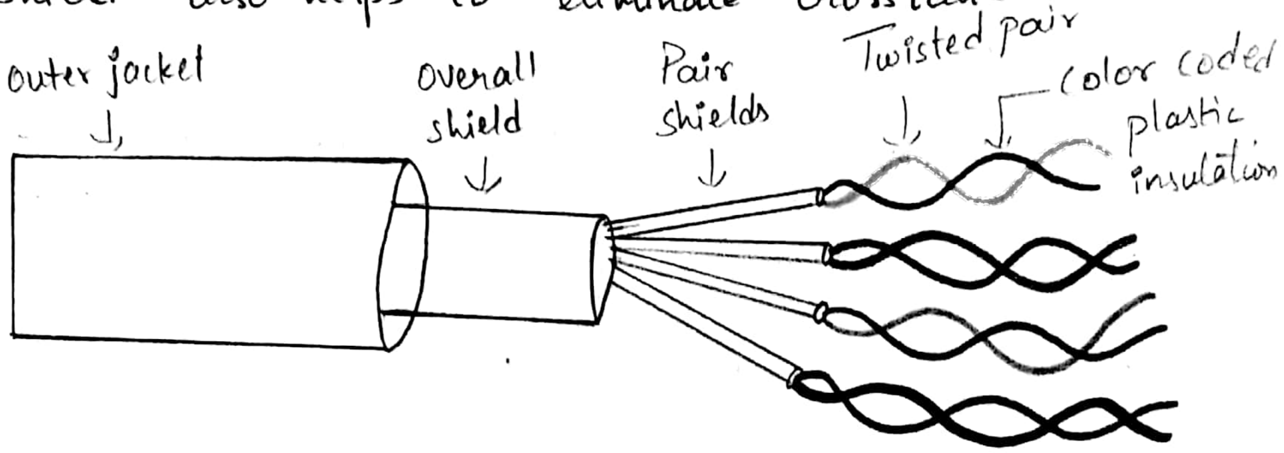
- Different categories of UTP are:-

Category	Maximum Data Rate	Intended Use
1	1 Mbps	Voice only
2	4 Mbps	4 Mbps Token Ring
3	16 Mbps	10 BaseT Ethernet
4	20 Mbps	16 Mbps Token Ring
5	100 Mbps (2-pair)	100 BaseT Ethernet
	1000 Mbps (4-pair)	1000BaseTX
5e	1000 Mbps (2-pair)	1000 BaseT
6	1000 Mbps (2-pair)	1000 BaseT & faster broadband applications.
6a	10000 Mbps (2-pair)	Future standard that will provide for 10 Gbps Ethernet.

Shielded Twisted Pair (STP)

- This cable has a metal foil or braided-mesh covering that occurs each pair of insulated conductors.
- The metal foil is used to prevent infiltration of electromagnetic noise.
- This shield also helps to eliminate cross-talk.

STP

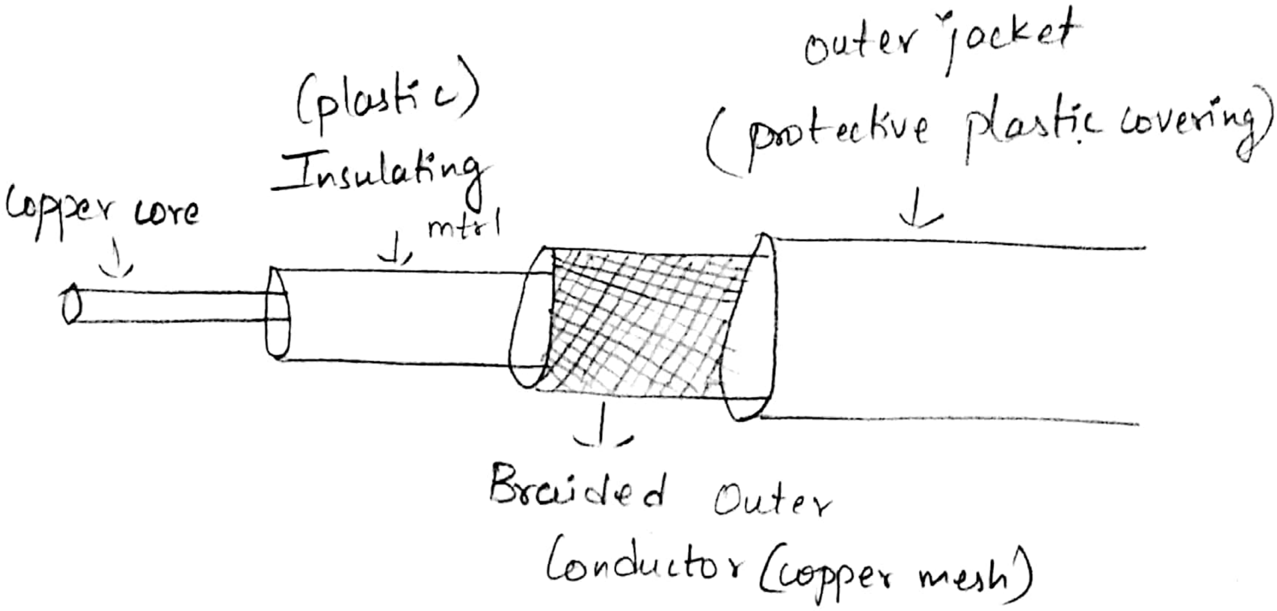


- STP reduces electrical noise both within the cable and from outside the cable.
- STP is suited for environments with electrical interference and also provides better performance at higher data rates.
- But the extra shielding makes STP cable quite bulky and more expensive than UTP cables.

Coaxial Cable :

- It is one of the common transmission medium (called as ~~Co~~ coax) in current day data communication.

- They are relatively inexpensive, but most costly than UTP on a per-unit length.



- A coaxial cable consists of four components:

① A core copper wire, which serves as a primary channel.

② A electric plastic insulator which surrounds the copper.

③ A braided outer conductor which is a copper mesh, It is used to protect from etechical electromagnetic interference.

④ The last layer is outer jacket which is protective plastic covering. It is used to protect the inner layers from physical damage such as fire and water.

- Although coaxial cable is difficult to install, it is highly resistant to signal interference.

- It can support greater cable lengths b/w n/w devices and greater bandwidth than twisted-pair cable.

- Coaxial cables are capable of transmitting data at a fast rate of 10Mbps.
- There are two varieties of ~~ca~~ coaxial cable:

  Thicknet

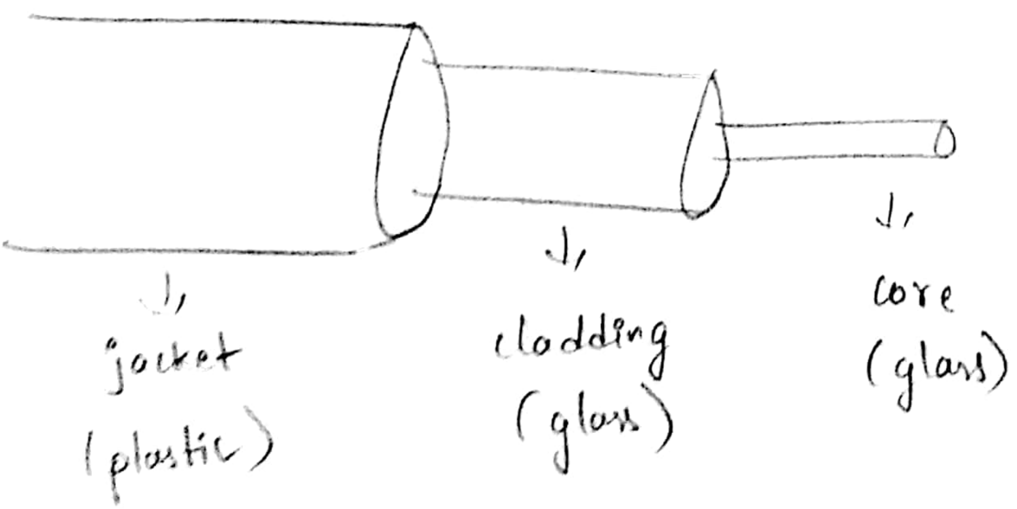
  Thinnet

- Categories of Coaxial Cable

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

- The most common type of connector is BNC connector.

Fiber-optic cable:



- Optical fiber consists of thin glass fibers that can carry information in the form of visible light.
- It consists of very narrow strand of glass or plastic called the core.
- Around the core is a layer of dense glass or plastic called the cladding, whose refractive index is less than that of the core.
- The outer most layer of the cable is known as jacket, which shields the cladding & the core from moisture, crushing & abrasion.
- Optical fibers transmit a beam of light by means of total internal reflection.
- When a light beam from a source enters the core, the core refracts the light & guides the light along its path.
- The cladding reflects the light back into the core & prevents it from escaping through the medium.
- Fiber optic cable support two modes of propagating light, they are:-

<u>Multimode</u>: In this mode, many beams from a light source traverse along multiple paths & at multiple angles.

Single mode : The beams propagate almost horizontally.

- LED or LASER acts as the source converting electric pulse to light pulses & photodiode acts as receiver doing vice versa.

- Fiber optic cable uses 3 types of connectors. They are:-

SC (Subscriber Connector): It is used to connect cable TV.

ST (Straight Tip) - It is used to connect n/w devices

MT-RJ (Mechanical Transfer - Registered Jack) — It is used for N/w applications.

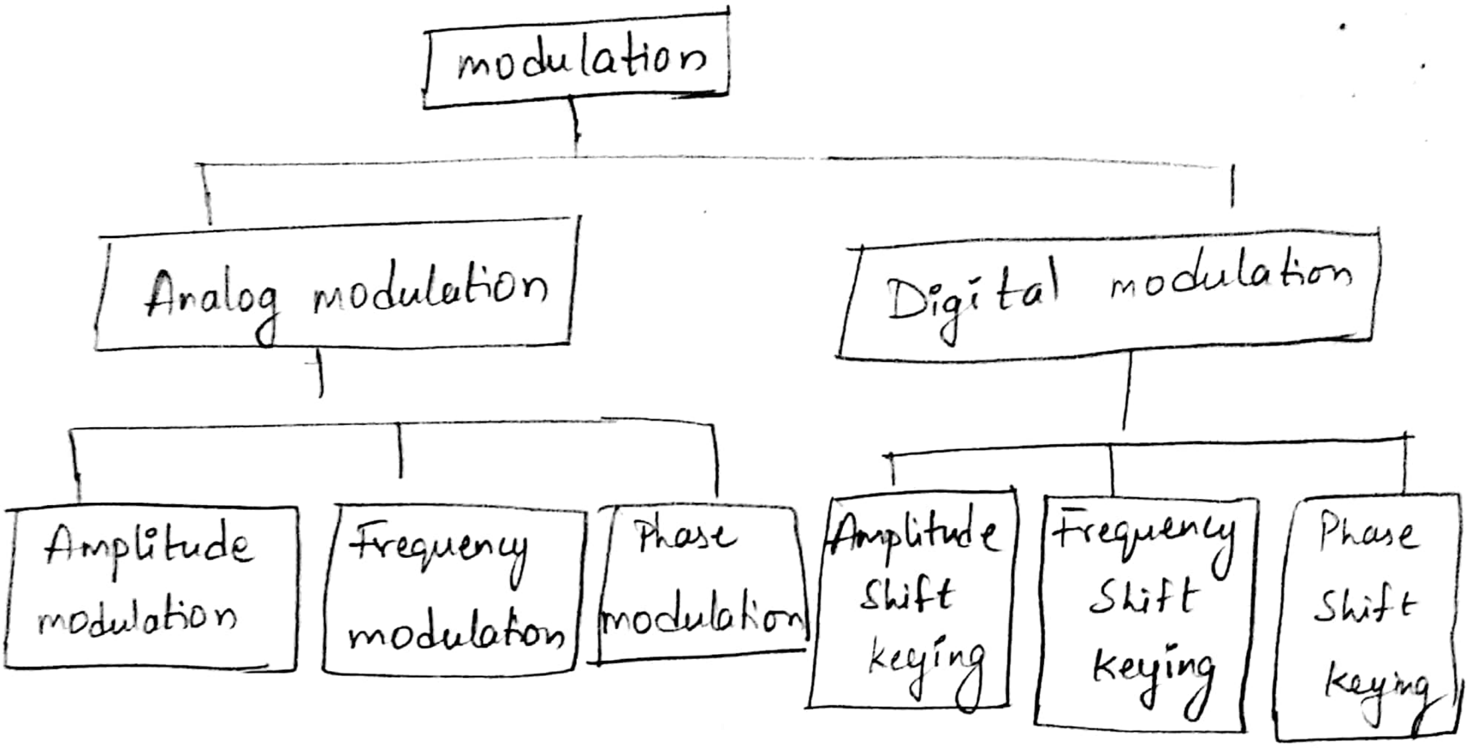
Twisted-pair cable	Coaxial cable	Optical fiber
- Transmission of signals takes place in the electrical form over the metallic (copper wires) conducting wires.	- Transmission of signals takes place in the electrical form over the inner conductor of the cable (copper core)	- Signal transmission takes place in an optical form over a glass fiber.
- In this medium, the noise immunity is low.	- Coaxial having higher noise immunity than twisted pair cable.	- Optical fiber has highest
- Twisted pair cable can be affected due to external magnetic field.	- Coaxial cable is less affected due to external magnetic field.	- Not affected by the external magnetic field.

- cheapest medium	- Moderate expensive	- Expensive
- Low Bandwidth	- Moderately high bandwidth	- Very high bandwidth
- Attenuation is very high.	- Attenuation is low	- Attenuation is very low.
- Installation is easy	- Installation is fairly easy	- Installation is difficult.

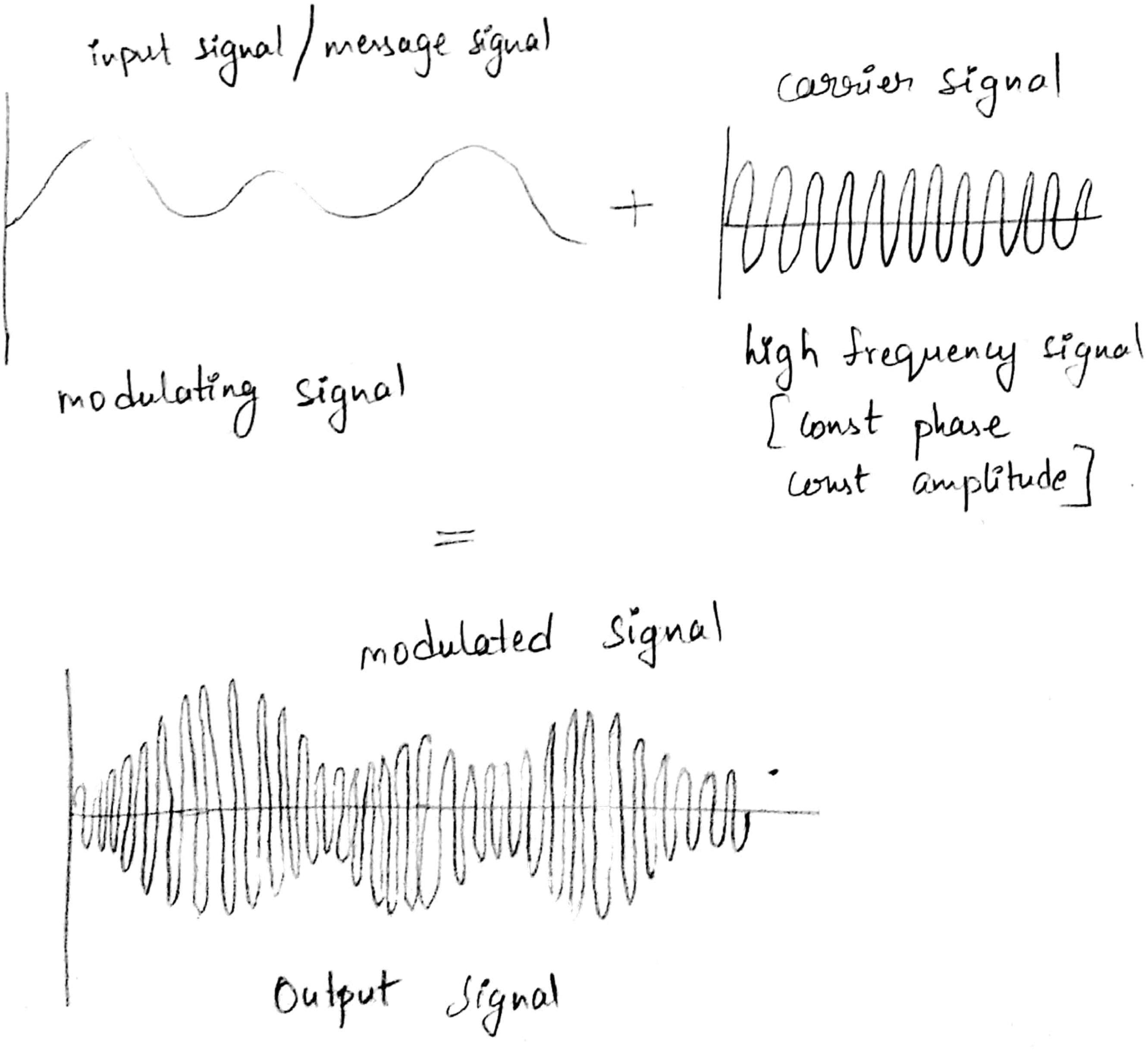
Digital Modulation and Multiplexing

Modulation :- It is nothing but, a carrier signal varies in accordance with the message signal. Modulation technique is used to change the signal characteristics.

- It is a process of encoding information from a message source in a way that is suitable for transmission. This is achieved by altering the characteristics of a wave.
- In the modulation process, a parameter of the carrier wave is varied in accordance with the modulating signal.
- The receiver demodulates the received modulated signal & gets the original information signal back.
- Modulation is of two types :—



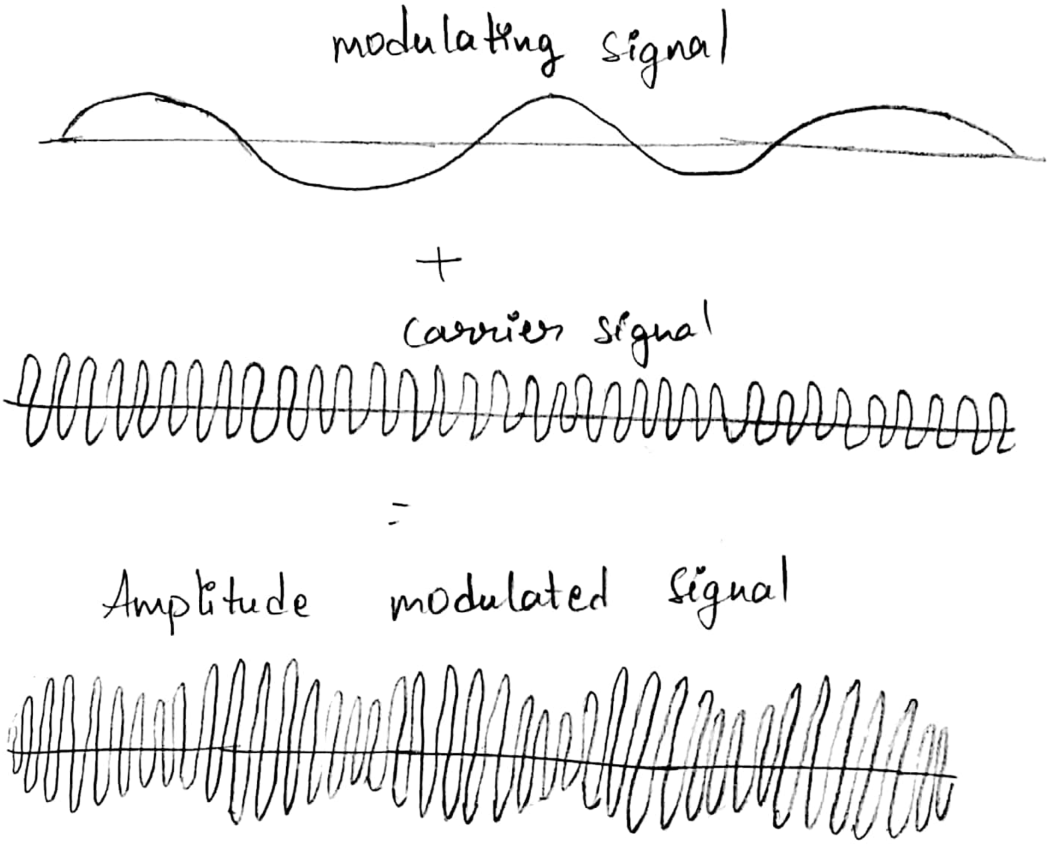
modulation process



① **Analog modulation** : If Analog signal is used as carrier signal, it is said to be Analog modulation.

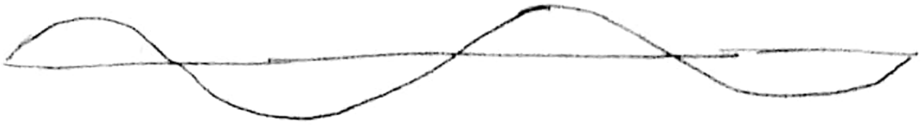
Analog modulation techniques:

ⓐ **Amplitude modulation** : It is a process of varying amplitude of carrier signal accordingly with the amplitude of input signal.



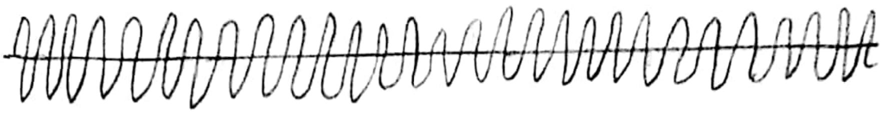
ⓑ **Frequency Modulation** : It is a process of varying frequency of carrier signal according to the frequency of the input signal.

- frequency of carrier signal changes with modulating signal modulating signal



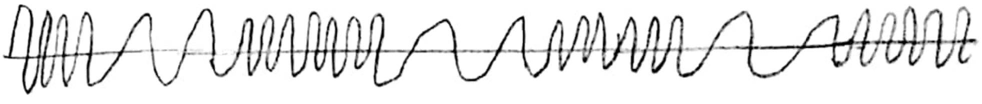
+

carrier signal



=

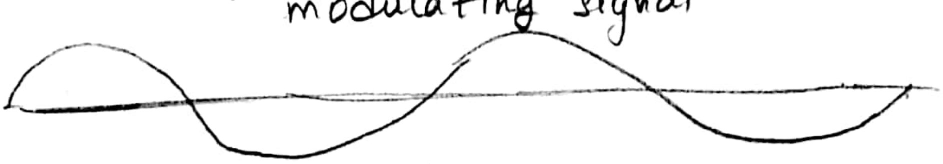
Frequency modulated signal



© Phase modulation : It is a process of varying phase of carrier signal according to the phase of input signal.

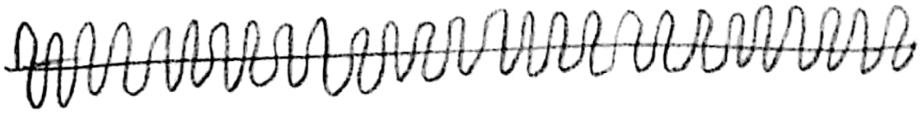
- phase of carrier signal changes with the modulating signal.

modulating signal



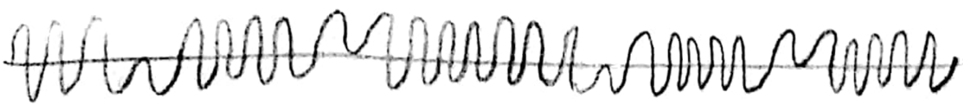
+

carrier signal



=

Phase modulated signal



(2) **Digital modulation** : It is a special kind of modulation where the $\overset{i/p}{\text{message}}$ signal (modulating signal) is of digital in nature (binary signal) & the carrier wave to be modulated is of analog in nature.

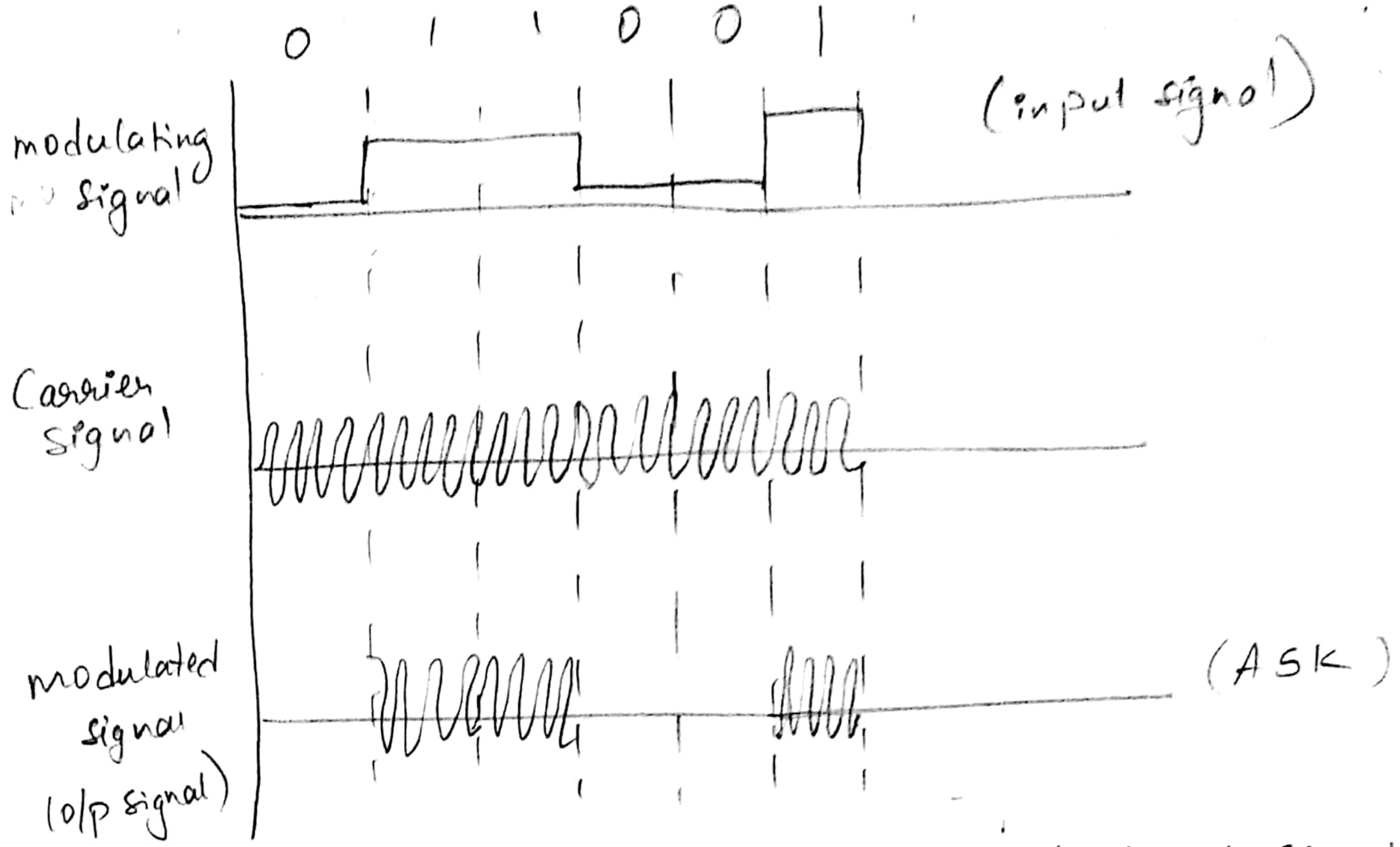
i/p signal / modulating signal + carrier signal = Modulated Signal
(digital signal) (Analog signal) (Analog signal)

- In digital modulation, switching of the amplitude, frequency or phase of the carrier signal is done.

- Digital modulation techniques : ASK
PSK
FSK

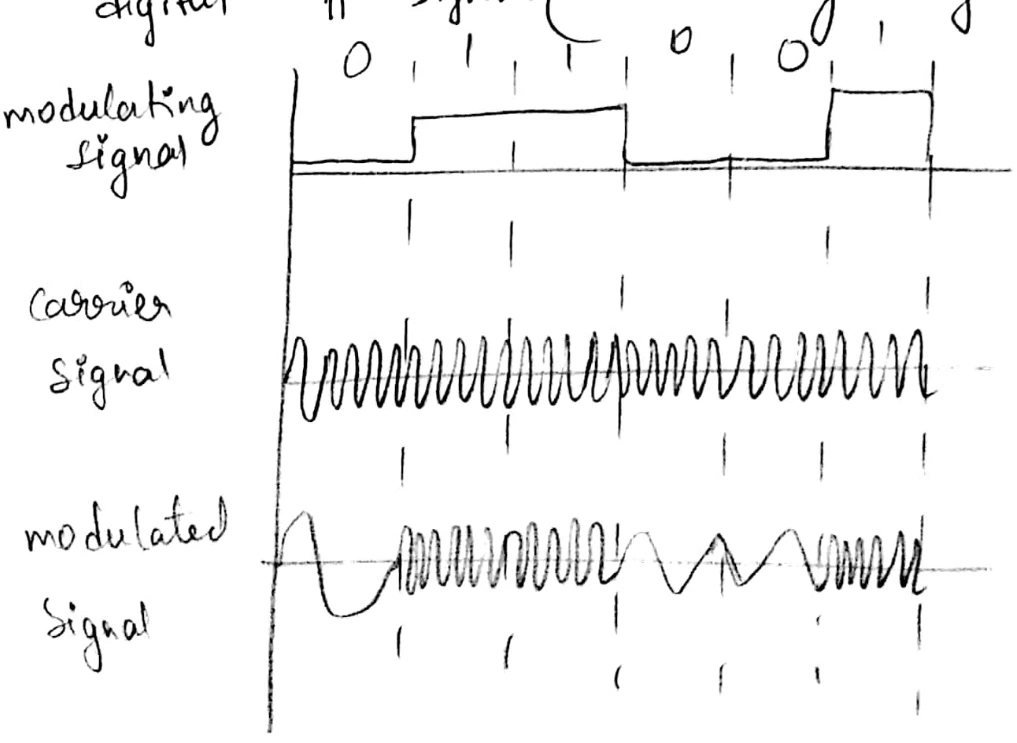
- ASK, PSK, FSK are analogous to AM, PM, FM resp.
- The only diffrence is that the modulating signal is digital in ASK, PSK, FSK & analog in AM, PM, FM.

(a) **Amplitude shift keying** : In ASK, the amplitude of the carrier wave is changed according to the digital input signal (modulating signal).



If i/p data = 0 → No amplitude in o/p Signal
data = 1 → amplitude of carrier wave is propogated

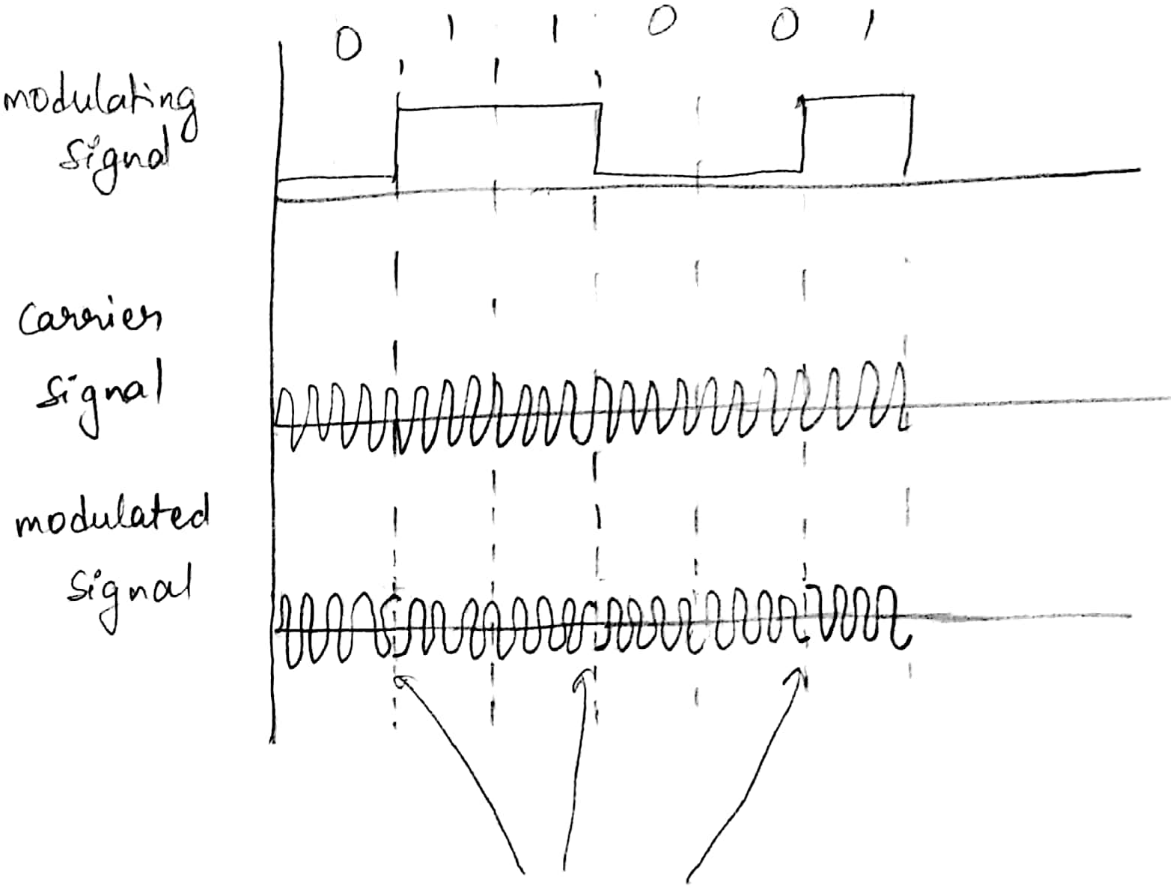
(B) <u>Frequency Shift keying</u> :- In FSK, the frequency of the carrier wave is changed according to the digital i/p signal (modulating signal).



If data = 0 → low frequency

If data = 1 → high frequency

ⓒ **Phase Shift keying** : In PSK, phase of the carrier wave is changed according to the i/p digital signal.

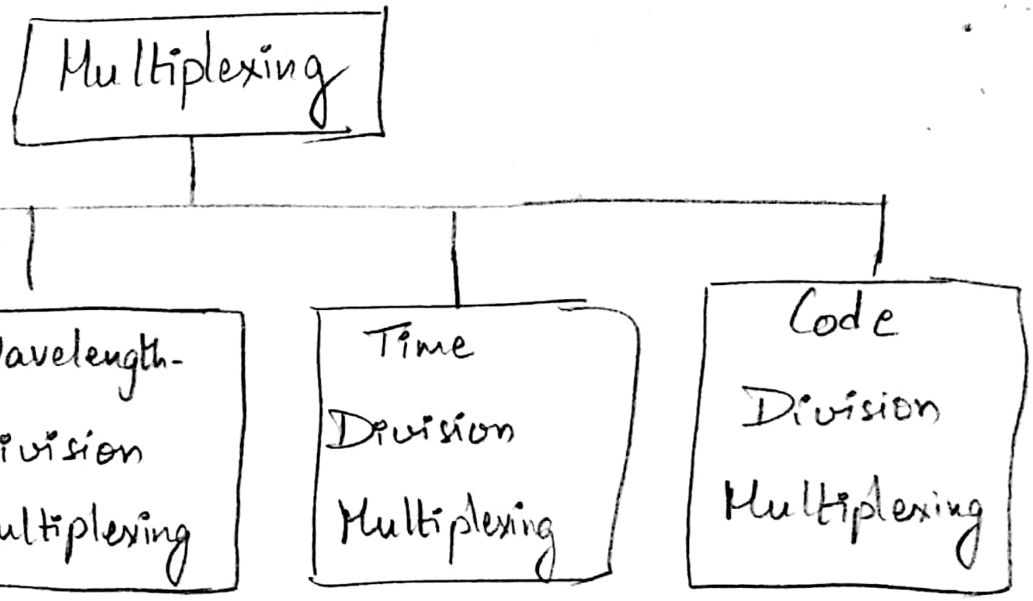


phase shift of π (180°) -> when data changes from 0 to 1 / 1 to 0

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

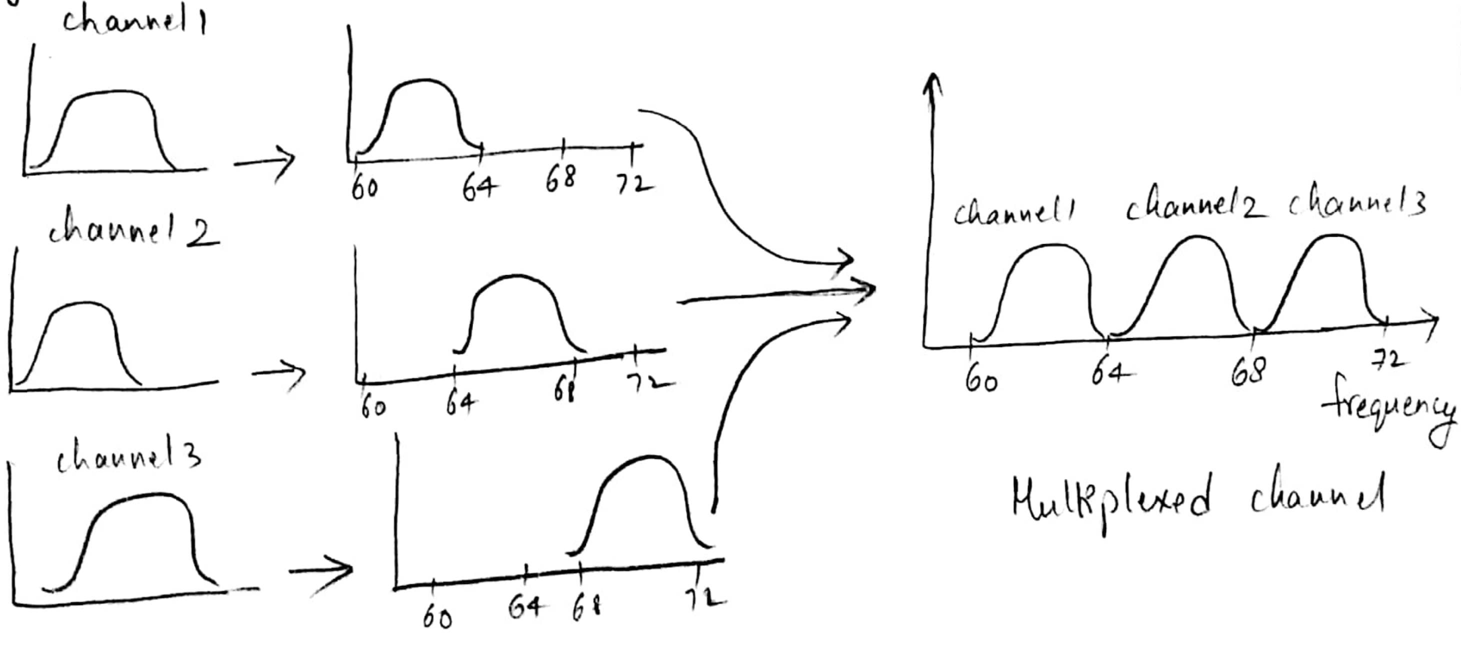
- A single data link is shared among multiple users.
- It is much more convinient to use a single wire to carry several signals than to install a wire for each & every signal. This kind of sharing is called multiplexing.
- Categories of Multiplexing :—

Multiplexing Techniques:


Multiplexing
Frequency-Division Multiplexing
Wavelength-Division Multiplexing
Time Division Multiplexing
Code Division Multiplexing

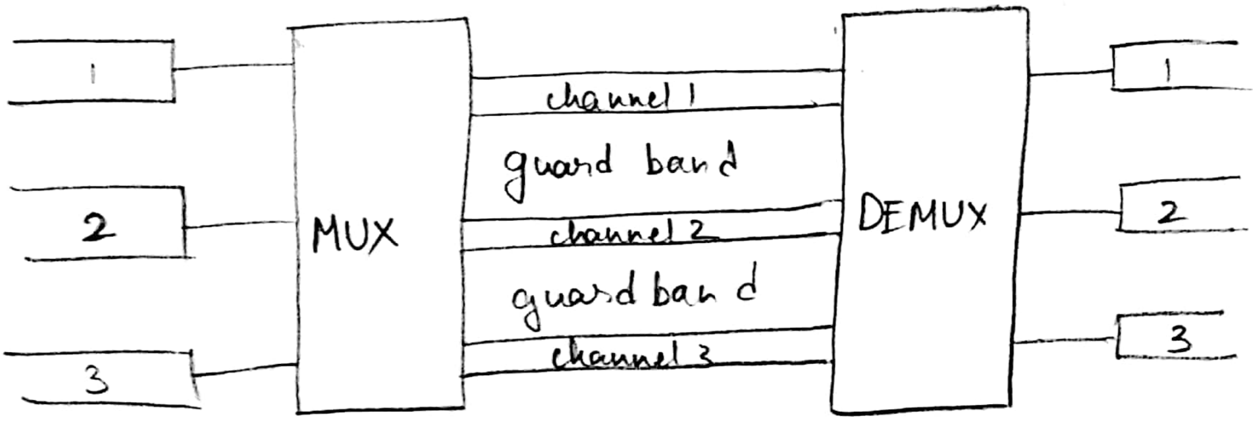
ⓐ Frequency-Division Multiplexing:

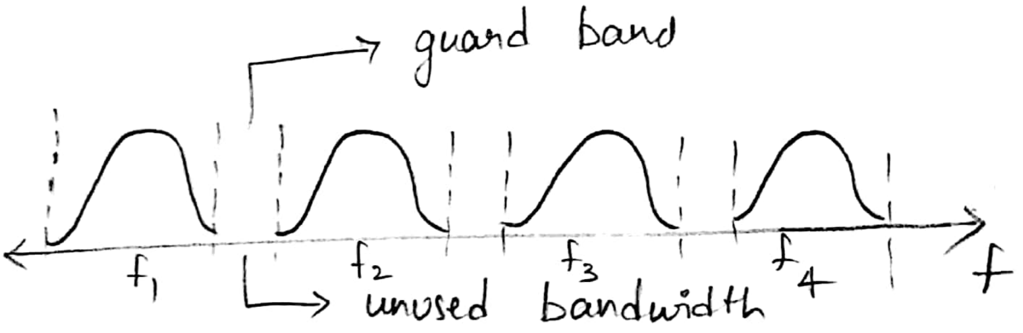
- In FDM, all users use the same channel at the same time but they are alloted different frequencies to prevent signal interference.
- There is a possibility of crosstalk in FDM since all signals are transmitted simultaneously.



input signals

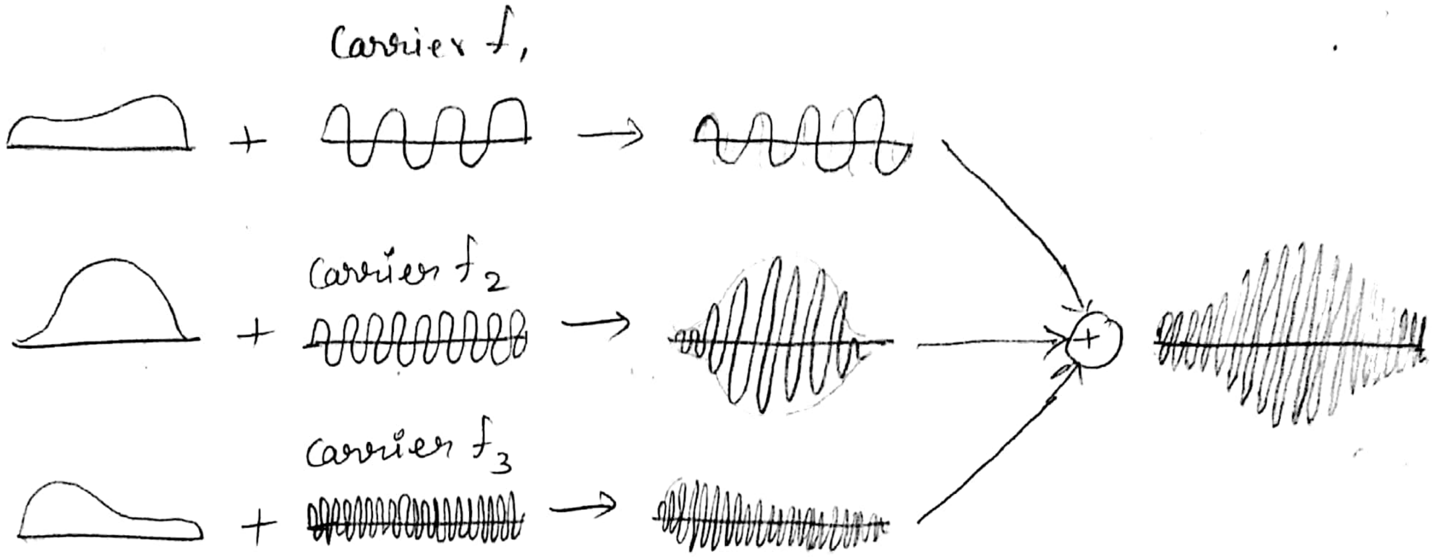
- If the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted, then FDM technique is used.
- Since signals are transmitted simultaneously, there is a possibility of overlapping and interference.





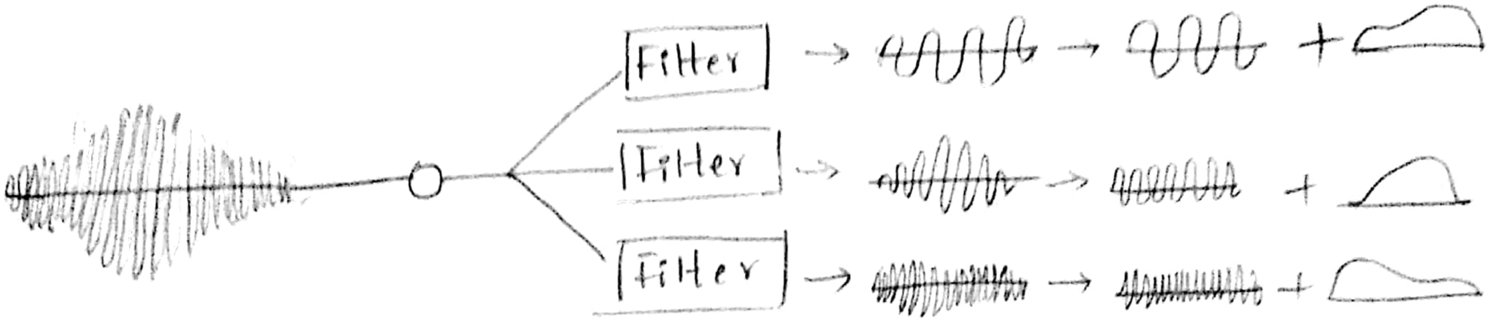
Multiplexing process : At the sender, multiplexing is done.

- In FDM, signals generated by each sending device modulate different carrier frequencies.
- These modulated signals are then combined into a single composite signal.



Demultiplexing process : At the receiver, demultiplexing is done.

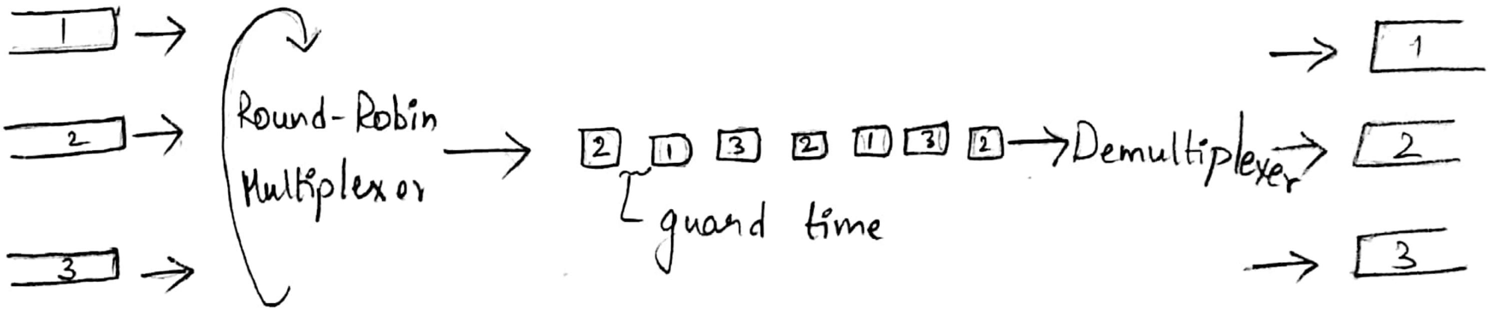
- demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals.
- The individual signals are then passed to a modulator that separates them from their carriers & passes them to the o/p lines.

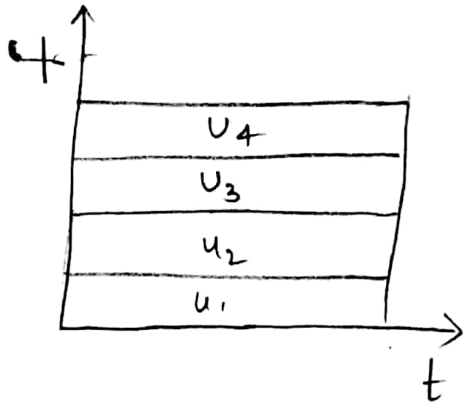


(b) Time-Division Multiplexing :

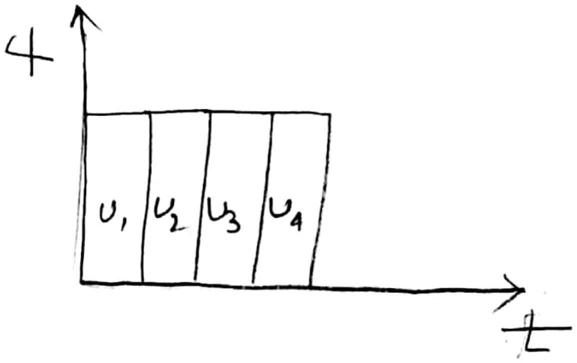
- In TDM, the users take turns (in a round-robin fashion) each one periodically getting the entire bandwidth for a little burst of time.
- Total time available in the link is divided b/w several users.
- Each user is alloted a particular time interval called time slot or time slice during which the data is transmitted by the user.
- Thus each sending device takes control of entire bandwidth of the channel for fixed amount of time.
- These time slots are separated by small intervals of

of guard time which is similar to the guard band in FDM.





FDM



TDM

- TDM is of two types :- Synchronous TDM
  Asynchronous TDM

Synchronous TDM : Each device is given same time slot to transmit the data over the link, irrespective of the fact that the device has any data to transmit or not.

Asynchronous TDM :- It is also known as Statistical TDM.

- In this, time slots are not fixed i.e., the slots are flexible/variable.

⑤ **Code Division Multiplexing:-** It is widely used in so-called 2G & 3G wireless communication.

- It is a combination of analog-to-digital conversion and spread spectrum technology.
- It is also known as CDMA (Code Division Multiple Access)
- CDMA allows each station to transmit over the entire frequency all the time.
- In CDM, each station is assigned a code called clip sequence. Transmission occurs in the foll way:-
- If a station needs to transmit a '1' bit, then it sends its chip sequence.
- If a station needs to transmit a '0' bit, then it sends negation of its chip sequence.
- Consider a station A and its chip sequence,

$$A = (-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$$

If 'A' needs to transmit bit '1', then it sends

$$(-1\ -1\ -1\ +1\ +1\ -1\ +1\ +1)$$

If 'A' needs to transmit bit '0', then it transmits

$$\text{negation} \Rightarrow (+1\ +1\ +1\ -1\ -1\ +1\ -1\ -1)$$

- All chip sequences are pairwise orthogonal means that the normalized inner product of any two distinct chip sequences, S and T is '0'.

- chip sequences has the following properties:

$S \cdot T = 0$ $S \cdot \overline{T} = 0$ $S \cdot \overline{S} = -1$

$S \cdot S = 1$ $\overline{S} \cdot T = 0$

- Consider 4 stations A, B, C, D & their chip sequences:

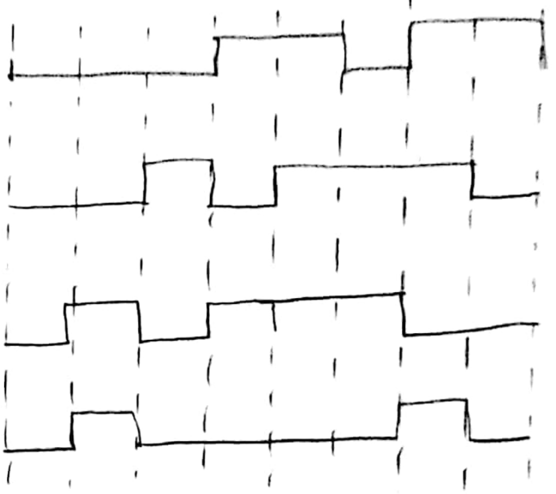
$A = (-1 -1 -1 +1 +1 -1 +1 +1)$

$B = (-1 -1 +1 -1 +1 +1 +1 -1)$

$C = (-1 +1 -1 +1 +1 +1 -1 -1)$

$D = (-1 +1 -1 -1 -1 -1 +1 -1)$

chip sequences



Signals the sequences represent

- The foll are the six examples of one or more stations transmitting '1' bit at the same time.

$S_1 = C$ [station 'c' transmits a '1' bit]

$S_2 = B + C$ [both B & C transmit '1' bit]

$S_3 = A + \overline{B}$ [A transmits '1' & B transmits '0']

$S_4 = A + \overline{B} + C$ [A transmits '1', B transmits '0', C transmits '1']

$S_5 = A + B + C + D$ [A transmits '1', B transmits '1', C transmits '1', D transmits '1']

$S_6 = A + B + \overline{C} + D$ [A transmits '1', B transmits '1', C transmits '0', D transmits '1'].

- Their chip sequences are as follows:-

$\therefore S_1 = C = (-1 +1 -1 +1 +1 +1 -1 -1)$

$S_2 = B + C = (-1 -1 +1 -1 +1 +1 +1 -1) + (-1 +1 -1 +1 +1 +1 -1 -1)$

$= (-2 \; 0 \; 0 \; 0 \; +2 \; +2 \; 0 \; -2)$

$S_3 = A + \overline{B} = (-1 -1 -1 +1 +1 -1 +1 +1) + (+1 +1 -1 +1 -1 -1 -1 +1)$

$= (0 \; 0 \; -2 \; +2 \; 0 \; -2 \; 0 \; +2)$

$S_4 = A + \overline{B} + C = (-1 -1 -1 +1 +1 -1 +1 +1) + (+1 +1 -1 +1 -1 -1 -1 +1)$

$+ (-1 +1 -1 +1 +1 +1 -1 -1)$

$= (-1 +1 -3 +3 +1 -1 -1 +1)$

$S_5 = A + B + C + D = (-1 -1 -1 +1 +1 -1 +1 +1) + (-1 -1 +1 -1 +1 +1 +1 -1) +$
$(-1 +1 -1 +1 +1 +1 -1 -1) + (-1 +1 -1 -1 -1 -1 +1 -1)$

$= (-4 \; 0 \; -2 \; 0 \; +2 \; 0 \; +2 \; -2)$

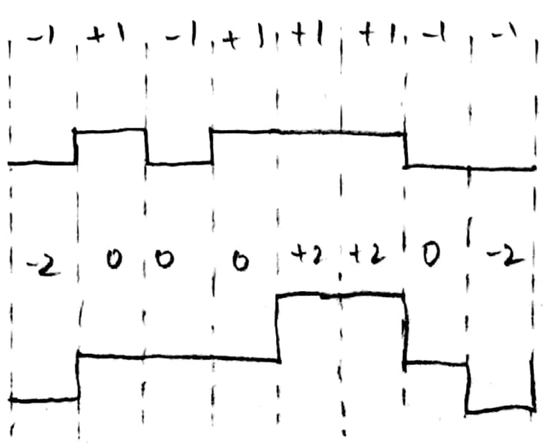
$S_6 = A + B + \overline{C} + D = (-1 -1 -1 +1 +1 -1 +1 +1) + (-1 -1 +1 -1 +1 +1 +1 -1) +$
$(+1 -1 +1 -1 -1 -1 +1 +1) + (-1 +1 -1 -1 -1 -1 +1 -1)$

$= (-2 \; -2 \; 0 \; -2 \; 0 \; -2 \; +4 \; 0)$

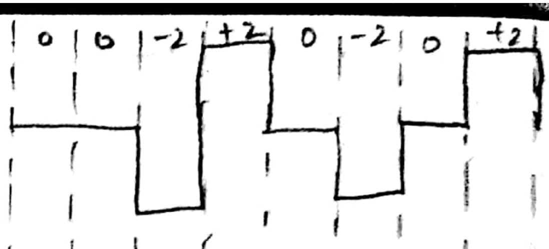
- signal representation of above examples is as follows:-

$S_1 = (-1 +1 -1 +1 +1 +1 -1 -1)$

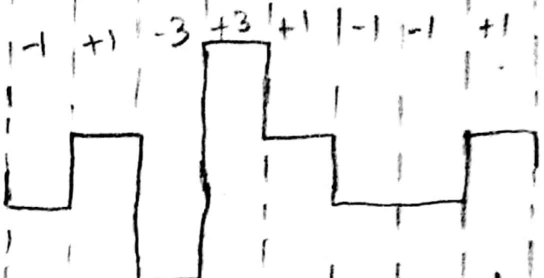
$S_2 = (-2 \; 0 \; 0 \; 0 \; +2 \; +2 \; 0 \; -2)$



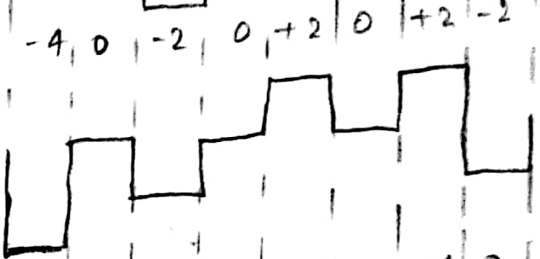
$S_3 = (0\ 0\ -2\ +2\ 0\ -2\ 0\ +2)$



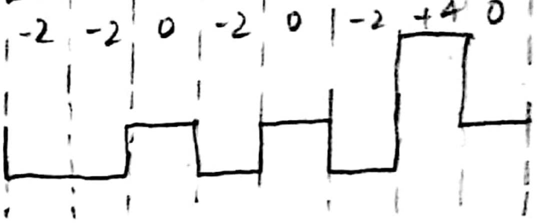
$S_4 = (-1\ +1\ -3\ +3\ +1\ -1\ -1\ +1)$



$S_5 = (-4\ 0\ -2\ 0\ +2\ 0\ +2\ -2)$



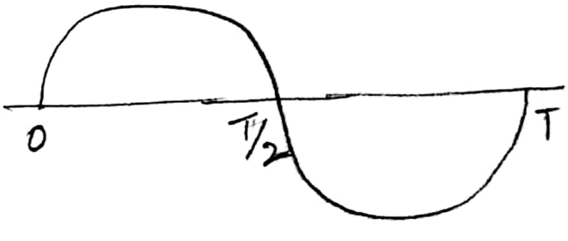
$S_6 = (-2\ -2\ 0\ -2\ 0\ -2\ +4\ 0)$



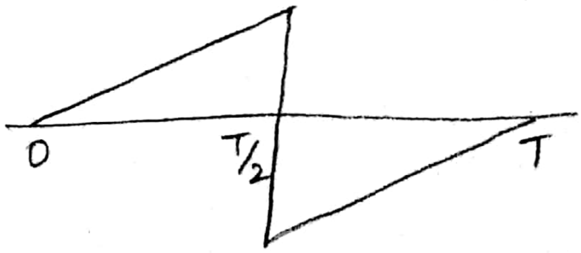
Fourier Analysis, Bandwidth Limited Signals, Max Data rate of channel

- periodic waveform: It is one which repeats the exact same shape again & again. It doesn't change its shape, stay the same for the waveform's whole duration.
- there are five periodic waveforms:- They are:-

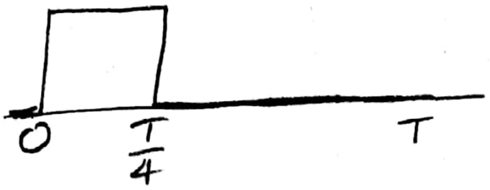
ⓐ Sine wave



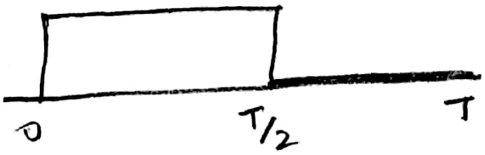
ⓑ sawtooth wave



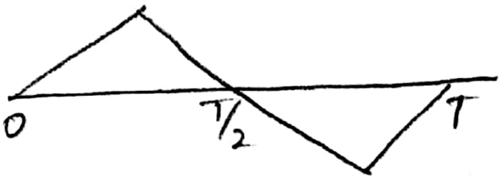
ⓒ. pulse wave



ⓓ Square wave



ⓔ Triangle wave



- Information can be transmitted on wires by varying some physical property such as voltage or current.
- We represent this voltage or current as a single-valued function of time, $f(t)$.
- Then we can model the behaviour of the signal & analyze it mathematically
- This analysis is done in the following concepts :-

  Fourier Analysis

  Bandwidth Limited Signals

  Maximum Data Rate of a chanel.

Fourier Analysis :-

- In early 19th century, the French mathematician Jean-Baptiste Fourier proved that any reasonably behaved periodic function, $g(t)$ with period T, can be constructed as the sum of a number of sines and cosines.

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi n f t) + \sum_{n=1}^{\infty} b_n \cos(2\pi n f t) \quad — ①$$

$f = \frac{1}{T}$ is the fundamental frequency

a_n, b_n = sine & cosine amplitudes

c = constant

Such a decomposition is called a Fourier series

- The a_n amplitudes can be computed for any given $g(t)$ by multiplying both sides of eq ① by $\sin(2\pi k f t)$ & then integrated from 0 to T.
- Similarly by multiplying ① by $\cos(2\pi k f t)$ & integrating from 0 to T we can derive b_n.
- By just integrating both sides of the equation, we can find c,

$$\therefore \quad a_n = \frac{2}{T}\int_0^T g(t) \sin(2\pi n f t)\, dt$$

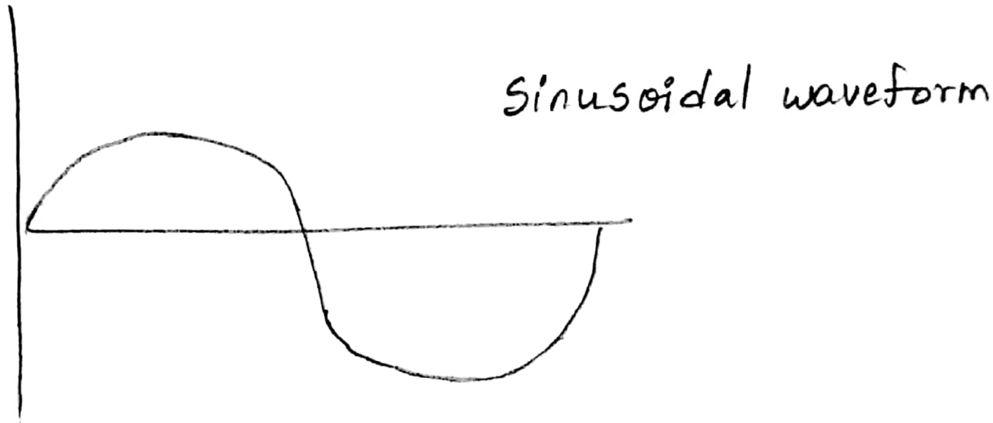
$$b_n = \frac{2}{T}\int_0^T g(t) \cos(2\pi n f t)\, dt$$

$$c = \frac{2}{T}\int_0^T g(t)\, dt.$$

Bandwidth Limited Signals :

Fundamental frequency :

- A fundamental waveform (or first harmonic) is the sinusoidal waveform that has the supply frequency
- The fundamental is the lowest or base frequency 'f' on which the waveform is built.
- Consider a basic 1st harmonic AC waveform.



- Harmonics :- They are voltages or currents that operate at a frequency that is an integer multiple of fundamental frequency.

Ex :- If fundamental frequency = 50 Hz

1st harmonic frequency = 50 Hz

2nd harmonic frequency = 100 Hz

3rd harmonic frequency = 150 Hz ..... etc.

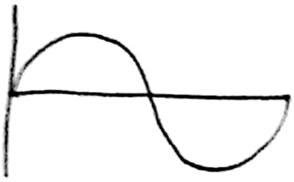
- So, if the fundamental frequency = f

1st harmonic frequency = f
2nd harmonic frequency = 2f
3rd harmonic frequency = 3f . . . . . etc.

- Harmonics are unwanted higher frequencies which superimposed on fundamental waveform creating a distorted wave pattern.

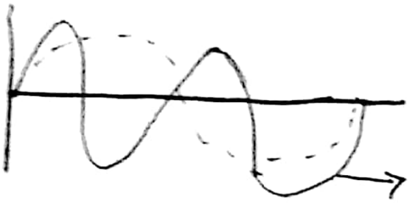
- Waveforms due to Harmonics :

(1)



1st harmonic : f

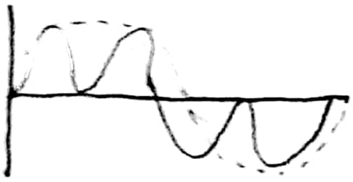
(2)



2nd harmonic : 2f

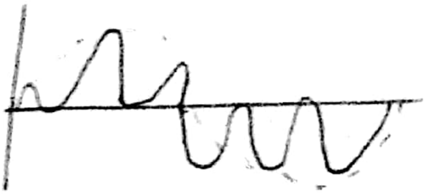
→ distorted wave due to harmonics

(3)



3rd harmonic : 3f

(4)



4th harmonic : 4f

- Bandwidth : The range of frequencies that are used for transmitting a signal without being attenuated is called the band width.

$$B = f_{max} - f_{mini}$$

Ex :- If max frequency = 1000,
min frequency = 100

$$B = 1000 - 900$$

$$\boxed{B = 900}$$

- <u>baseband</u> <u>signals</u>: Signals that run from 0 upto a maximum frequency are called baseband signals.

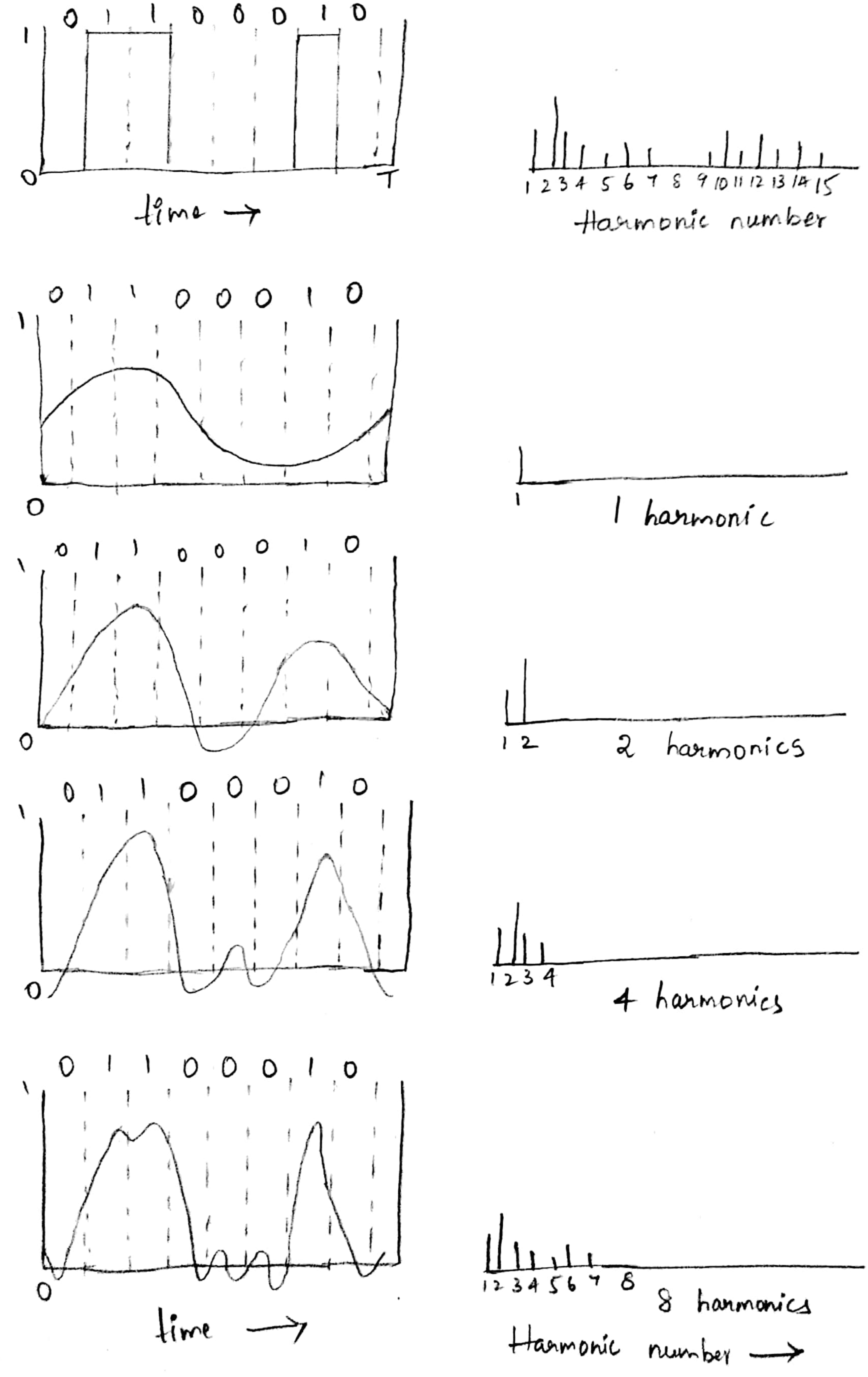
$f_{min} = 0$, f_{max} then $B = f_{max} - f_{mini}$

$$\boxed{B = f_{max}}$$

- <u>Bandpass</u> <u>and</u> <u>passband</u>: Bandpass is an electronic filter that allows frequencies within a particular range to pass through it while ~~detecting~~ deleting other frequencies. The output of bandpass filter is <u>passband signal</u>.

- <u>Bandwidth</u> <u>-limited</u> <u>signal</u>: A signal is called bandwidth-limited or simply band-limited when the amplitude of the spectrum goes to zero whenever its frequency crosses the allowable limits.

Ex :- Data is 01100010



Maximum Data Rate of a channel :

- Limiting the bandwidth limits the dato rate.

Nyquist theorem :- The maximum data rate of a channel can be calculated for an error-free/ noiseless channel by using the foll equation.

$$\boxed{\text{max data rate} = 2B\log_2 V \text{ bits/sec}}$$

B = Bandwidth

V = discrete signal levels.

This equation is applicable for error-free channel.

Shannon's theorem : For a noisy channel, the maximum data rate of a channel is calculated by using the foll equation.

$$\boxed{\text{max dato rate} = B\log_2(1+S/N)}$$

The amount of noise present is measured by the ratio of signal power to noise power. called SNR (Signal-to-Noise Ratio).(S/N)

UNIT-III

The Data Link Layer

Data link layer Design Issues

i, Services provided to the N/w layer

ii, Framing

iii, Error Control

iv, Flow Control

i, Services provided to the N/w layer

- Unacknowledged Connectionless Service
- Acknowledged Connectionless Service
- Acknowledged Connection-oriented Service.

(a) Acknowledged Connectionless Service: It consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

Ex:- Ethernet.

- If a frame is lost due to noise, no attempt is made to detect the loss or recover from it.
- This service is used when the error rate is very low.

(b) Acknowledged Connectionless Service

- There are no logical connections used b/w the sender and the receiver.

- Each and every frame sent is individually acknowledged.
- So, the sender knows whether a frame has arrived correctly or been lost.
- If it has not arrived within a specified time interval it can be sent again.
- This service is useful over reliable channels such as wireless channels Ex:- 802.11 (wifi).

Ⓒ Acknowledged Connection-Oriented Service:

- In this service, source and destination establish a connection before any data is transferred.
- Each frame sent over the connection is numbered, & the data link layer guarantees that each frame sent is received.
- It guarantees that each frame is received exactly once and that all frames are received in right order.
- This service is used over long, unreliable links such as a satellite channel or long-distance telephone circuit.

(ii) Framing: The DLL should detect and correct the errors.

- For this purpose, DLL will break up the bit stream into discrete frames, compute a short token called a checksum for each frame & include the checksum in the frame when it is transmitted.

- When the frame arrives at the destination, the checksum is recomputed.
- If the newly computed checksum is different from the one contained in the frame, DLL finds that error has occured & retransmits the frame.
- After dividing the data into frames, we should be able to identify the starting & ending of each frame.
- There are four methods for this purpose:

Framing methods
- Byte Count
- Flag bytes with byte stuffing
- Flag bits with bit stuffing
- Physical layer coding violations

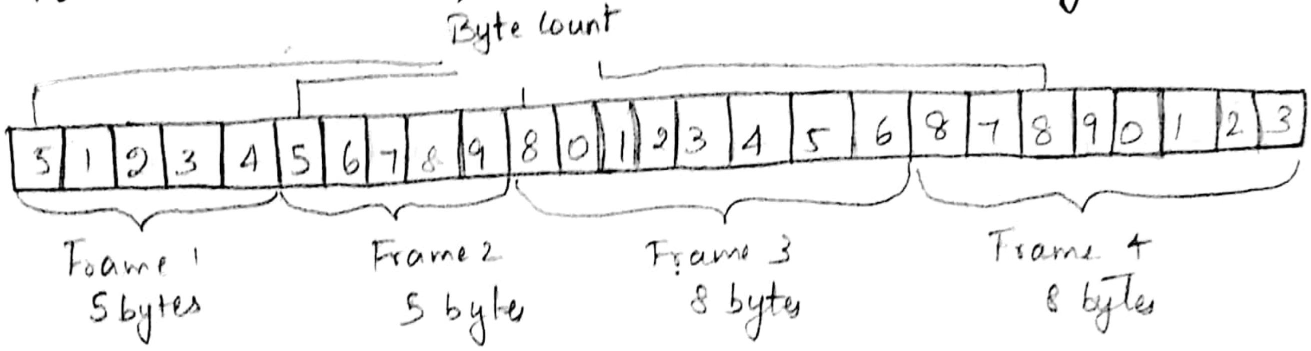
(a) Byte Count :- This method uses a field in the header to specify the number of bytes in the frame.

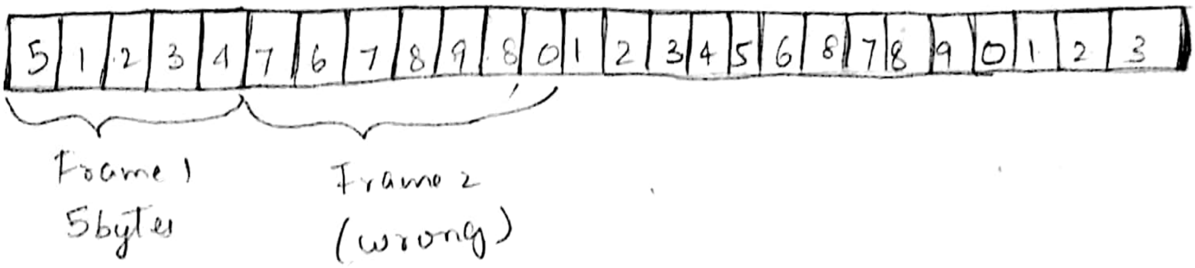
- When the DLL at the destination sees the byte count, it knows how many bytes follow & hence where the end of the frame is.
- This problem occurs if the byte count is changed by any transmission errors.

Ex:- if the byte count of 5 becomes 7 due to error, the destination will get out of synchronization.

- It will be unable to locate the correct start of next frame.

- Using checksum destination determines the error has occured, but retransmission is not possible since we are unable to locate the correct start of the frame.
- For this reason, this method is rarely used.





(b) <u>Flag bytes with byte stuffing</u>:

- In this method, a special byte called flag byte is used as both the starting & ending delimiter of each frame.
- Two consecutive flag bytes indicate the end of one frame and the start of the next.
- If the receiver looses synchronization, it can just search for two flag bytes to find the end of current frame & the start of the next frame.

- Ithere may be a situation in which the flag byte occurs in the data.
- One way to solve this problem is to insert a special escape byte (ESC) just before each flag byte in the data.
- Thus, a framing flag byte can be distinguished from the flag byte in the data by the absence or presence of escape byte before it.
- The DLL on the receiving end removes the escape bytes before giving the data to the N/w Layer.
- This technique is called byte stuffing.

A frame delimiter with flag bytes

FLAG	Header	Payload field	Trailer	FLAG

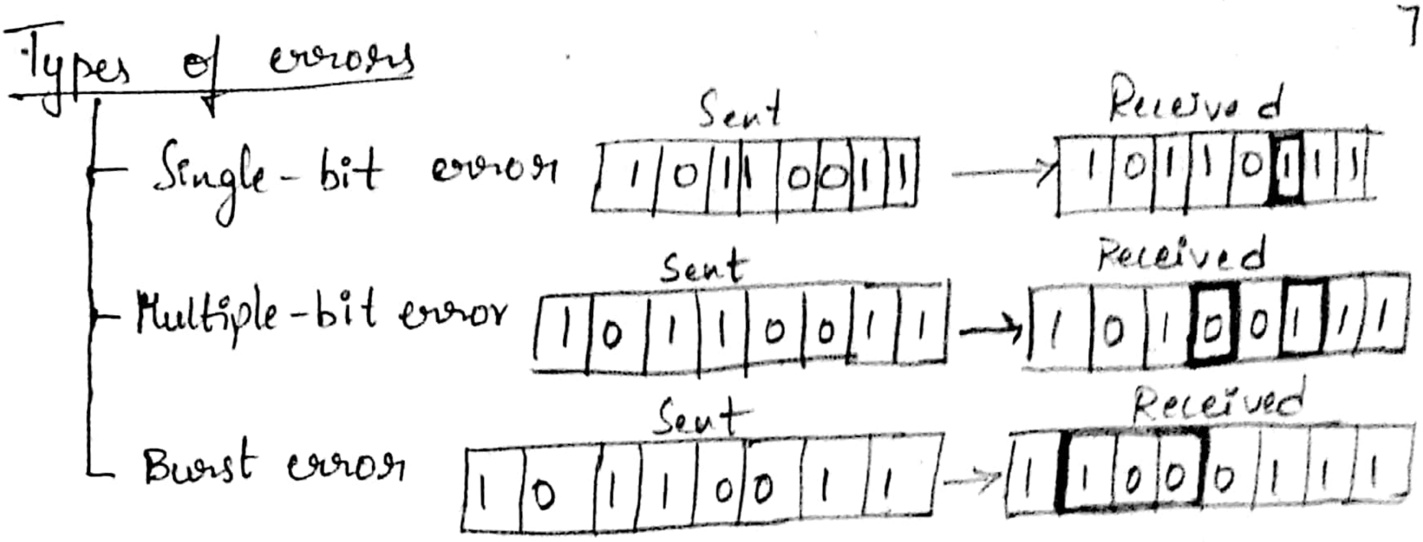
original bytes		After stuffing
A FLAG B	→	A ESC FLAG B
A ESC B	→	A ESC ESC B
A ESC FLAG B	→	A ESC ESC ESC FLAG B
A Esc ESC B	→	A ESC ESC Esc ESC B

Four examples of byte sequences before & after byte stuffing

(iii) Error Control :

- To ensure reliable delivery, the sender should be provided with some feedback about what is happening at the receiver.
- For this purpose, receiver sends special control frames having positive or negative acknowledgement
- If the sender receives positive acknowledgement, it means that the frame has transmitted safely.
- If the sender receives negative acknowledgement, it means the frame is lost and the sender must retransmit the frame.
- But if the ACK frame is lost, the sender indefinetely waits for +ve/-ve ACK & may hang forever.
- To overcome this, timers are used in DLL
- When the sender transmits a frame, it also starts a timer.
- The timer is set to the time interval required for the data to reach the destination and the ACK to reach the source.
- If the timer expires, it means that either the frame is lost or ACK is lost, then the sender retransmits the frame.
- Sequence numbers are used to distinguish b/w the original frame & the retransmitted frame.

- Types of errors



(iv) Flow Control : Flow is controlled by sending the data according to the capability of the receiver.

There are two ways:-

(a) Feedback-based flow control : In this, the receiver sends some feedback to the receiver. This feedback includes:-

- when to send the data.
- how much data the sender can transmit.
- at what rate data can be transmitted.

(b) Rate-based flow control :- In this, there is a built-in mechanism that limits the rate at which senders can transmit data, without using feedback from the receiver.

Error Detection & Correction.

- Error Correcting codes
- Error Detecting Codes

Error - Correcting codes:

- Hamming codes
- Binary convolutional codes
- Reed - Solomon codes
- Low - Density Parity check codes.

Hamming codes:

Haming distance: Consider two codewords

10001001 & 10110001

it is possible to determine how many corresponding bits differ. To determine how many bits differ, XOR the two codewords and count the number of '1' bits in the result.

XOR

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

Ex:-
```
1 0 0 0 1 0 0 1
1 0 1 1 0 0 0 1
---------------
0 0 1 1 1 0 0 0
---------------
```

3 bits differ (No of 1's = 3)

- The number of bit positions in which two codewords differ is called the Hamming distance.

- It means that if two codewords are at a Hamming distance 'd' apart, it will require 'd' single-bit errors to convert one into the other.

$$\text{Codeword} \longrightarrow \underset{\text{(Message bits)}}{m} + \underset{\text{(Check/redundant bits)}}{r}$$

- The number of check bits is calculated using the relation: $(m+r+1) \leq 2^r$

Ex :- $m = 110$

$\Rightarrow (m+r+1) \leq 2^r$

$\Rightarrow (3+r+1) \leq 2^r$

$\Rightarrow (4+r) \leq 2^r$ if $r = 3$,

$\Rightarrow 7 \leq 2^3$

$\Rightarrow \boxed{7 \leq 8} \longrightarrow \boxed{r = 3} \Rightarrow$

r_1	r_2	r_3
2^0	2^1	2^2

Codeword $\Rightarrow m + r$

$\Rightarrow 3+3 = 6$

r_3	r_2	r_1	
0	0	1	1
0	1	0	2
0	1	1	3
1	0	0	4
1	0	1	5
1	1	0	6

Hamming code

1	2	3	4	5	6
r_1	r_2	M_1	r_3	M_2	M_3
2^0	2^1	$1+2$	2^2	$1+4$	$2+4$

$\Rightarrow$

1	2	3	4	5	6
r_1	r_2	1	r_3	1	0

$\Rightarrow r_1 = 3+5 = M_1 + M_2 = 1 \text{ XOR } 1 = 0$

$\boxed{r_1 = 0}$

$\Rightarrow r_2 = 3+6 = M_1 + M_3 = 1 \text{ XOR } 0 = 1$

$\boxed{r_2 = 1}$

$\Rightarrow r_3 = 5+6 = M_2 + M_3 = 1 \text{XOR } 0 = 1$

$\boxed{r_3 = 1}$

Hamming code ⇒ $0\underline{11}110$ ⇒ transmitted.

$r_1\ r_2\ M_1\ r_3\ M_2\ M_3$

(1) If the codeword is received as 010110

(data is received with one-bit error)

Calculate r_1, r_2, r_3 (check bits)

$r_1 = M_1 + M_2 = 0 \text{XOR} 1 = 1$ × r_1 is wrong [In receive data, $r_1 = 0$]

$r_2 = M_1 + M_3 = 0 \text{XOR} 0 = 0$ × r_2 is wrong

$r_3 = M_2 + M_3 = 1 \text{ XOR } 0 = 1$ ✓

So, error is detected in the codeword.

$r_1\ r_2\ M_1\ r_3\ M_2\ M_3$

(2) If the received codeword is 011100

$r_1 = M_1 + M_2 = 1 \text{XOR} 0 = 1$ × {In received data, $r_1 = 0$] So r_1 is wrong.

$r_2 = M_1 + M_3 = 1 \text{ XOR } 0 = 1$ ✓

$r_3 = M_2 + M_3 = 0 \text{ XOR } 0 = 0$ × r_3 is worong.

So, the codeword is received with an error.

Hence error is detected.

. Error Detecting codes :

- Error Correcting codes are used when the error rate is low.
- Error Detecting codes are used when the error rate is high.

Error-Detecting codes

- Parity
- Checksums
- Cyclic Redundancy Checks (CRCs)

(a) Parity :- It can detect single-bit errors.

there are two types :- even parity
odd parity

Data word Original data	even parity	Codeword Transmitted data	odd parity	Codeword transmitted data
1011010	0	10110100	1	10110101
100101	1	1001011	0	1001010

If transmitted data is | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | → parity bit

~~Bo~~ At the receiver,

If the received data is | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | → parity bit

Receiver calculates the parity bit

⇒ parity bit = 1 [Consider even parity]

the transmitted parity bit & receiver calculated parity bit are not equal. So, error is occured.

Scanned by CamScanner

Cyclic Redundancy Check (CRC):

- Polynomial code : bit strings are representations of polynomials with coefficients of 0 and 1 only
- When the polynomial code is employed, the sender and receiver must agree upon a generator polynomial G(x).
- The result is a checksummed frame to be Transmitted T(x).

Ex :- Frame M(x) = 1101011111

Generator G(x) = 10011

code to be appended at the end of M(x)

= [(No of bits in G(x)) − 1] = 5 − 1 = 4 (0000)

Sender side

```
10011 ) 11010111110000 (1100001111
        10011
        -----
         10011
         10011
         -----
          00001
          00000
          -----
           00011
           00000
           -----
            00111
            00000
            -----
             01111
             00000
             -----
              11110
              10011
              -----
               11010
               10011
               -----
                10010
                10011
                -----
                 00010
                 00000
                 -----
                 (0010)
```

Transmitted frame T(x) =

11010111110010

Receiver side :

```
10011 ) 11010111110010 ( 1100001110
        10011
        -----
         10011
         10011
         -----
          00001
          00000
          -----
           00011
           00000
           -----
            00111
            00000
            -----
             01111
             00000
             -----
              11110
              10011
              -----
               11010
               10011
               -----
                10011
                10011
                -----
                 00000
                 00000
                 -----
                   (0)
```

At the receiver, the above calculation is done. If the remainder is '0'. It means there is no error.

Elementary Data link protocols :

- All the design issues/functions of DLL are fulfilled using some protocols. They are :-

ⓐ Unrestricted Simplex protocol

ⓑ Simplex stop-and-wait protocol for an Error-free channel

ⓒ Simplex stop-and-wait protocol for a Noisy channel.

ⓐ Unrestricted Simplex protocol :

- It is also called as Utopian Simplex protocol.
- This protocol can be used if the following conditions exist :-

① Data are transmitted in one direction only.

② Both transmitting (Sender) and receiving (receiver) systems are always ready

③ Processing time can be ignored.

④ Infinite buffer space is available

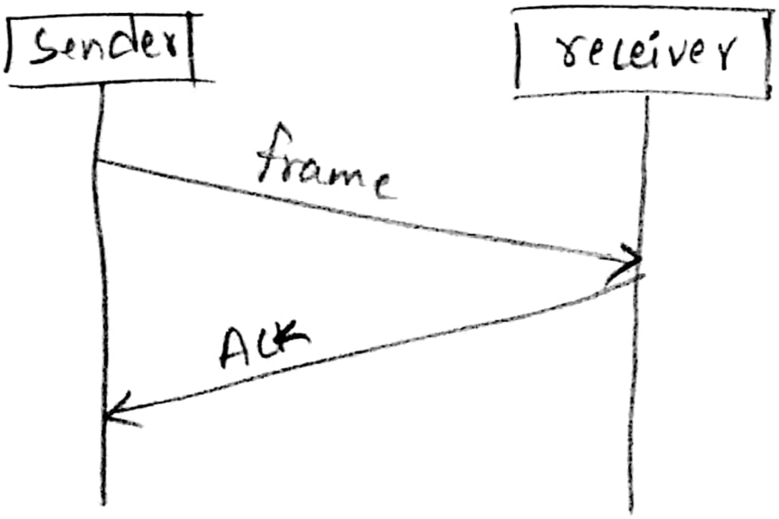
⑤ Communication channel never damages or looses frames.

⑥ No sequence numbers or Acknowledgements are used here.

- This protocol is unrealistic because it does n't handle either flow control or error control.
- Its processing is close to that of an unacknowledged connectionless service.

(b) Simplex stop-and-wait protocol for an Error-free channel :-

- The communication channel is assumed to be error free.
- The data traffic is half-duplex.
- In this protocol, receiver provides a feedback to the sender.
- It means that when the sender sends the data, the receiver receives it & sends a little dummy frame back to the sender giving permission to the sender to transmit the next frame.
- After having sent a frame, the sender is required by the protocol to wait until the dummy (ACK) frame arrives.
- Protocols in which the sender sends one frame & then waits for an ACK before proceeding to the next frame are called stop-and-wait protocols.



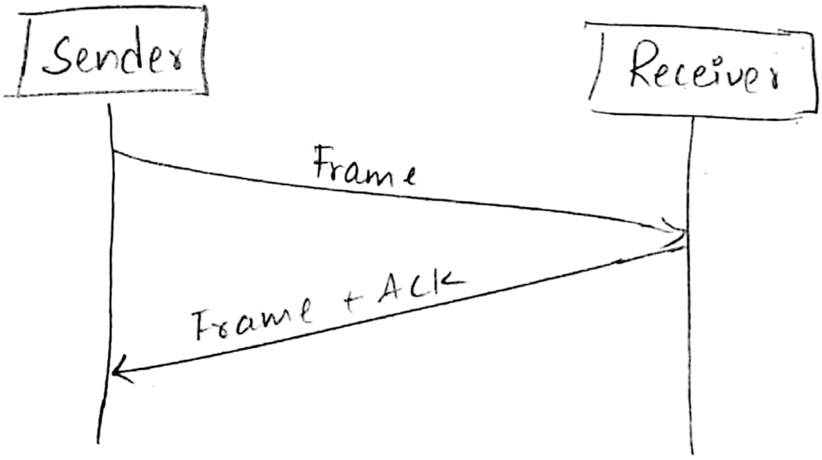
(c) Simplex stop-and-wait protocol for a Noisy channel :

- Consider the communication channel is a Noisy channel (ie., the channel that makes errors).
- Frames may be either damaged or lost completely.
- If a frame is damaged, the error is detected by using the checksum.
- If the data is lost or the ACK is lost, the send it can be identified by using timers.
- When the sender transmits a frame, it also starts a timer.
- If the timer expires, then the sender retransmits the frame.
- Sequence numbers are used to distinguish b/w the original frame & the retransmitted frame.
- Protocols in which the sender waits for a +ve ACK before advancing to the next data item are often called ARQ(Automatic Repeat ReQuest) or PAR (Positive Acknowledgement with Retransmission).

- Sliding Window Protocols.

Piggybacking: when a data frame arrives, instead of immediately sending a separate ACK, the receiver waits until the next frame.

- The ack is attached to the outgoing data frame.
- The technique of temporarily delaying outgoing acknowledgements so that they can be attached onto the next outgoing data frame is known as piggybacking



adv :- better use of channel bandwidth

disadv :- If the receiver waits too long, then at the sender the timer will be off & the sender retransmits the frame.

- sending window :- At any instant of time, the sender maintains a set of sequence numbers corresponding to the frames it is permitted to send.

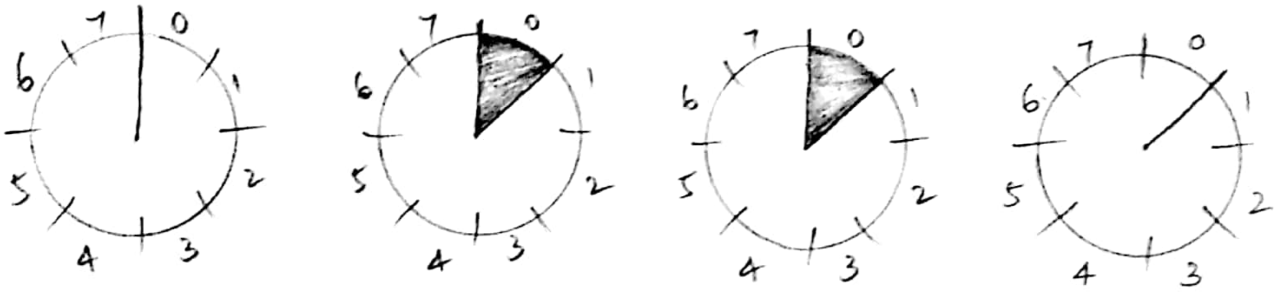
- receiving window : At any instant of time, the receiver maintains a set of frames it is permitted to receive.
- Sequence number range is 0 to 2^n-1

Sliding window protocols

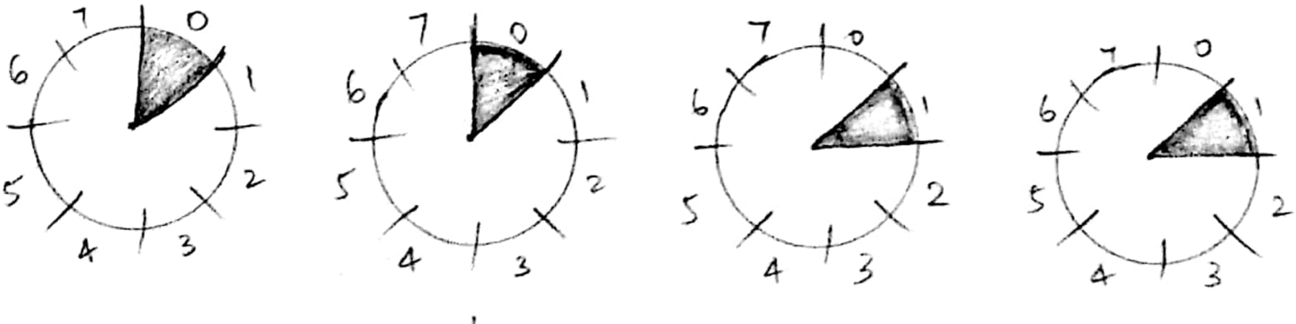
- one-bit sliding window protocol
- A protocol using Go-Back-N
- A protocol using Selective Repeat.

ⓐ one-bit sliding window protocol :

Sender



Receiver



(a) (b) (c) (d)

- The above example has a sliding window of size 1, with a 3-bit sequence number.

  ↳ sequence number range is 0 to $2^3 - 1$

  $= 0$ to 7

(a) Initially

(b) After the first frame has been sent

(c) After the first frame has been received

(d) After the first Ack has been received.

(a) <u>Sender</u> :- Initially when data transmission is not yet started.

<u>Receiver</u> :- waiting for a frame of sequence num = 0.

(b) <u>Sender</u> :- Sender sends a frame of sequence num = 0

<u>Receiver</u> :- waiting for a frame of sequence num = 0

(c) <u>Sender</u> :- Sender waiting for an Ack for frame of seq num = 0

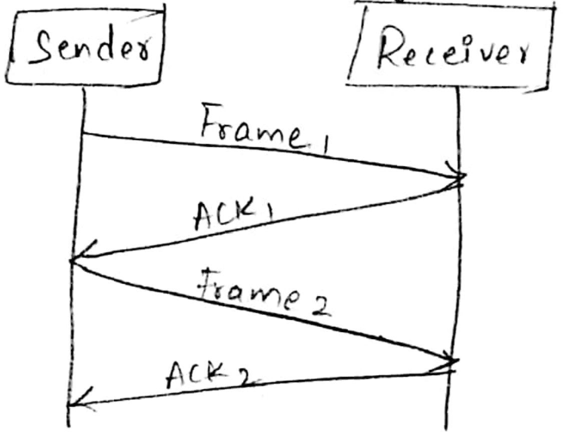
<u>Receiver</u> :- sends the Ack and waits for the next frame of seq num = 1

(d) <u>Sender</u> :- Data transmission of frame with seq num = 0 is completed & not sending any data (idle).

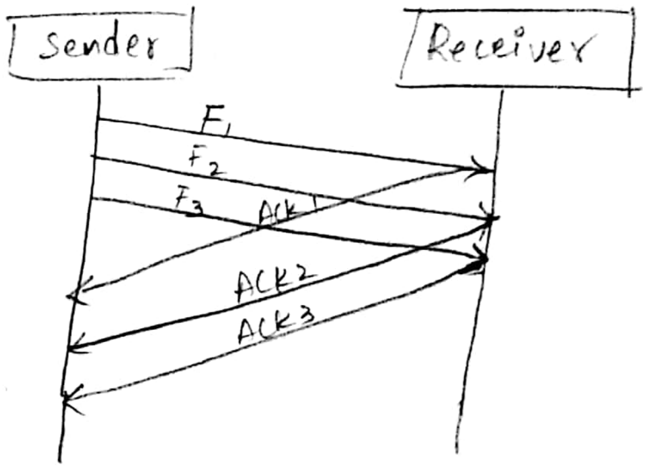
<u>Receiver</u> : waiting for a frame of seq num = 1.

Pipelining :- It is a technique in which multiple frames are sent at a time without waiting for the corresponding individual acknowledgements.

no pipelining



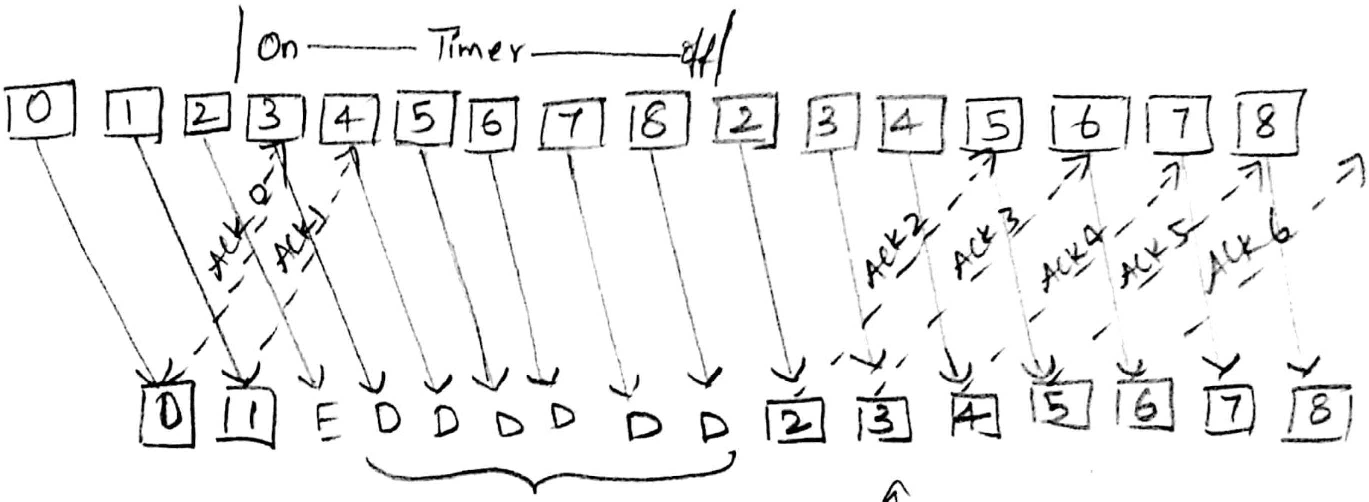
pipelining



(b) A protocol using Go-Back-N :-

- In this protocol, the sender retransmits all the frames that are transmitted after the damaged/lost frame.
- It error rate is high, it wastes a lot of bandwidth.
- In this protocol, the receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.
- It is a mechanism to detect & control the errors.
- Go-Back-N protocol is shown in the below diagram.
- Frame 2 is lost, so all the frames followed by frame 2 are deleted (discarded).
- All the frames from frames2 to 8 are retransmitted.

- Go-Back-N protocol performs pipelining. Hence all the frames from 0 to 8 are sent at a time without waiting for individual acknowledgements.
- The damaged or discarded frames will be retransmitted after all the 8 freames are transmitted.



Frames discarded

Go-Back-N for Frame lost and delayed ACK

receiver's window size is 1

(c) A protocol using selective repeat.

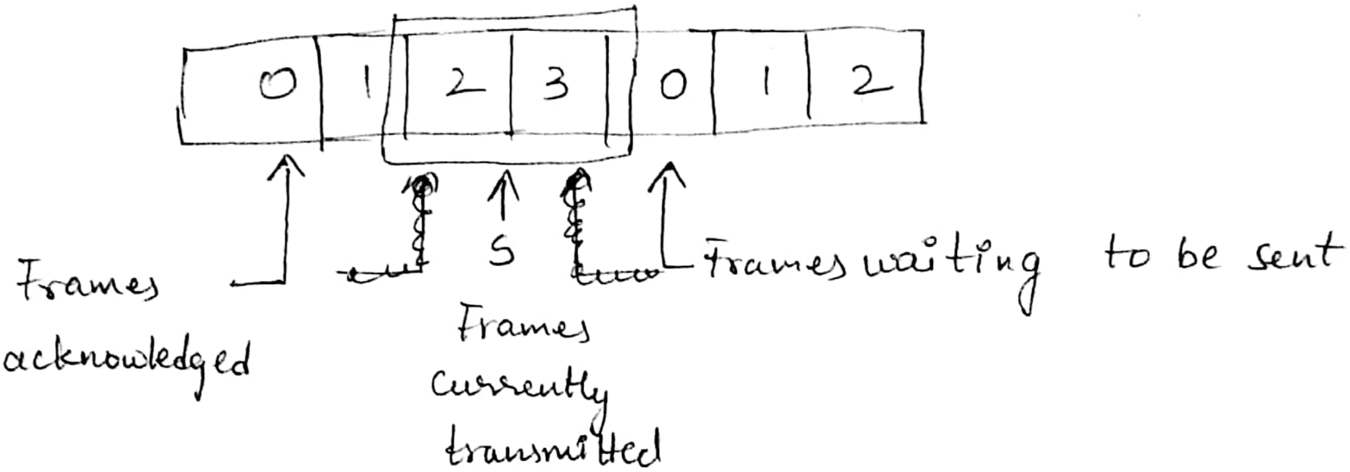
- The go-back-n protocol works well if errors are rare, but if the channel has high error rate, it wastes lot of bandwidth on retransmitted frames.
- An alternative approach is selective repeat.
- The selective repeat protocol retransmits only that frame which is damaged or lost.
- The sender maintains a buffer (Sender window) having the

sequence numbers of the frames that the sender is allowed to send.

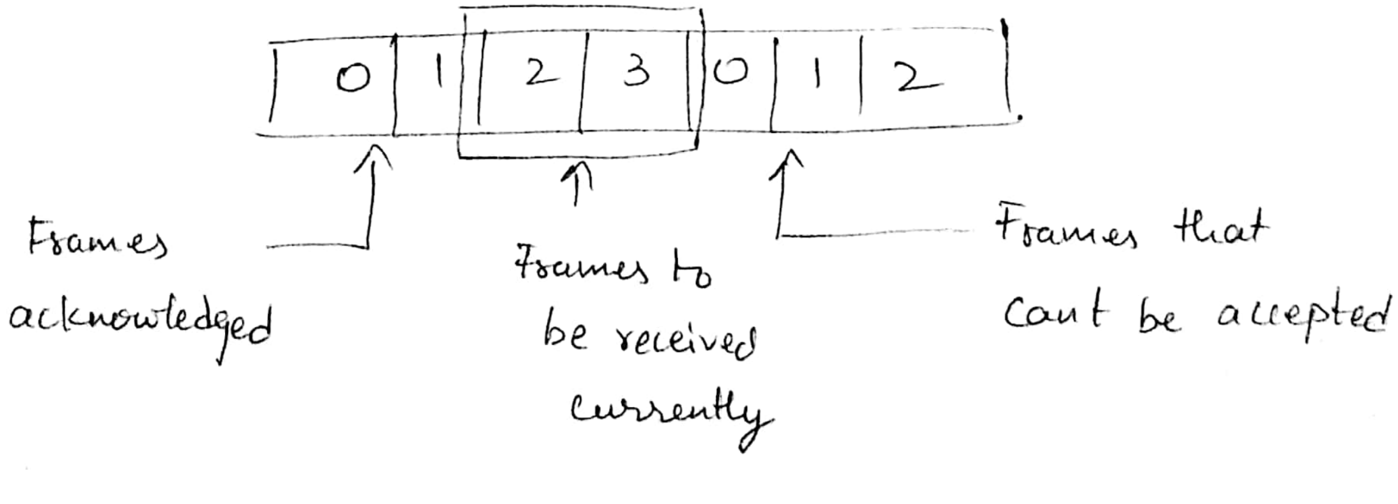
- The receiver also maintains a buffer (receiver window) having the sequence numbers of the frames that the receiver is allowed to receive.

- In this protocol, receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.

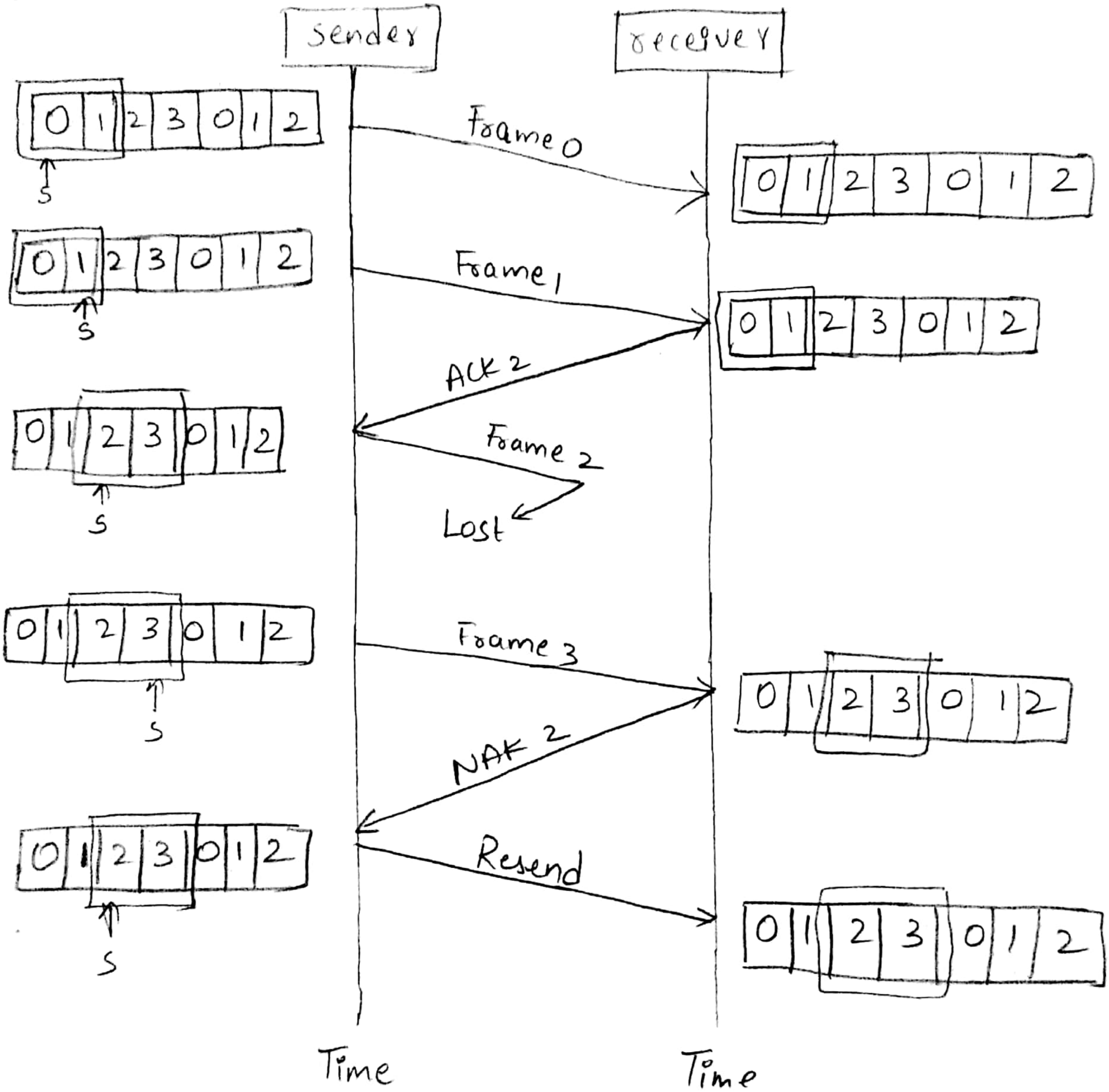
Sender window :



receiver window :



∴ The selective repeat protocol is shown in the below example. The Frame 2 is lost, only that frame is retransmitted.



UNIT - IV

The Medium Access Control Sublayer:-

(1) **The channel Allocation Problem**: There are two types of channel Allocations: they are:-

Static channel Allocation

Dynamic channel Allocation

(a) **Static channel Allocation**: It is a way of allocating a single channel among multiple users by using one of the multiplexing schemes such as FDM. (Frequency Division Multiplexing).

- If there are N users, the bandwidth is divided into N equal-sized portions with each user being assigned one portion.

Ex: FM radio stations, each station gets a portion of FM band.

- When the number of senders is large or the traffic is heavy, FDM presents some problems:

(i) If the spectrum is cut into N regions and fewer than N users are currently interested in communicating, large piece of valuable spectrum will be wasted.

(ii) If more than N users want to communicate, some of them will be denied permission for lack of bandwidth.

- Hence dividing the single available channel into some number of static sub channels is inefficient.

ⓑ <u>Assumptions for Dynamic Channel Allocation</u> :-

There are five key assumptions :-

(i) <u>Station model</u> :- The model consists of 'N' independent stations (eg:- computers, telephones) each with a program or user that generates frames for transmission.

- The expected number of frames generated in an interval of Δt is $\lambda \Delta t$, where λ is a constant.
- Once a frame has been generated, the station is blocked & does nothing until the frame has been successfully transmitted.

(ii) <u>Single channel Assumption</u> :

- A single channel is available for all communications.
- All stations can transmit on it & can receive from it.

(iii) <u>Collision Assumption</u> : If two stations are transmitted simultaneously, they overlap & the resulting signal is damaged. This event is called a collision.

- All stations can detect that a collision has occured.
- A collided frame must be transmitted again later.

(iv) · Continuous or slotted time :

- In Continuous time, frame transmission can begin at any instant.
- Alternatively, time may be slotted or divided into discrete intervals (called slots).
- Frame transmissions must begin at the start of the slot. If the slot is already Started, the sender should wait until the next slot.
- If a slot contain '0' frames, it corresponds to an idle slot.

  " " '1' frame, it corresponds to a successful transmission.

  " , more frames, " " " " collision.

(v) Carrier Sense or No Carrier Sense :

- With the carrier Sense assumption, stations can identify if the channel is in use before trying to use it.
- No station will attempt to use the channel while it is sensed as busy.
- The station can use the channel while it is sensed as idle.

Multiple Access Protocols :- There are three protocols. 4

ALOHA
Carrier Sense Multiple Access Protocols (CSMA)
Collision - Free Protocols

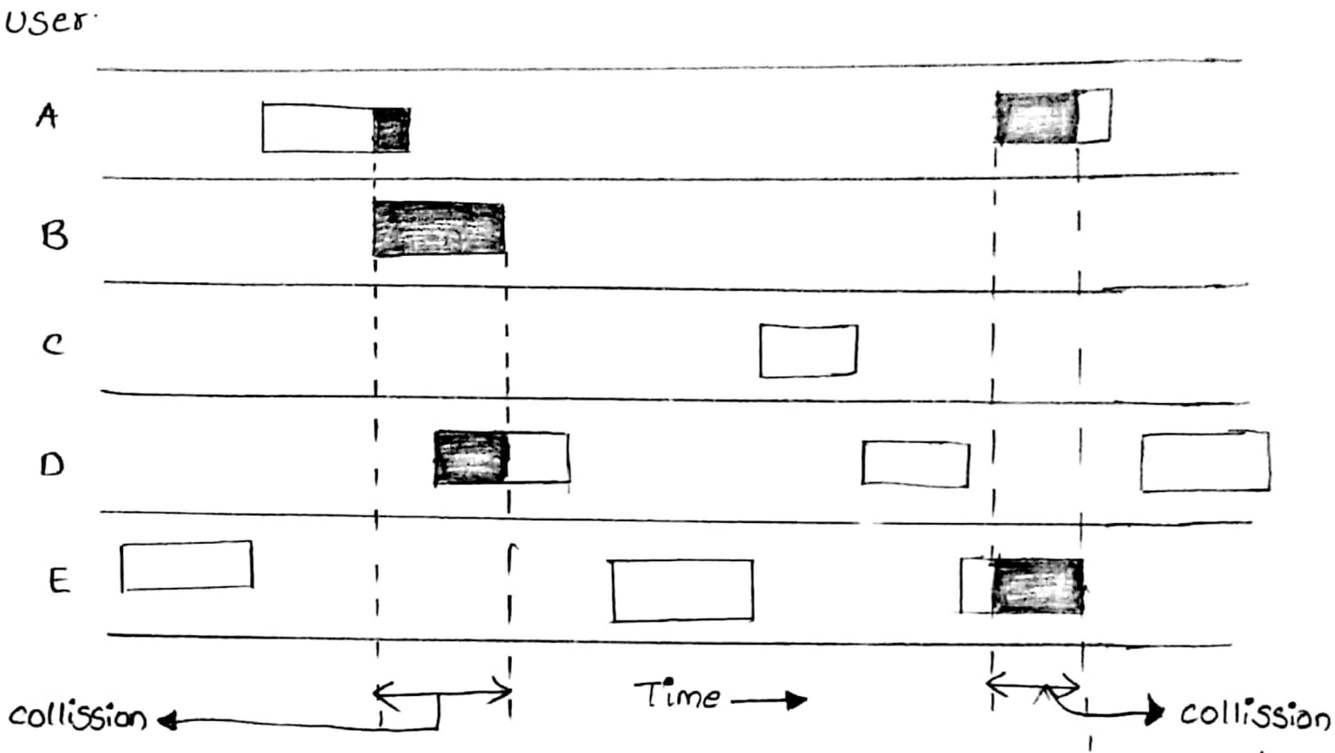
ALOHA :-

- Norman Abramson proposed a method to solve the channel allocation problem called the 'ALOHA' system.
- There are two categories in ALOHA system. They are:-
  Pure Aloha
  Slotted Aloha

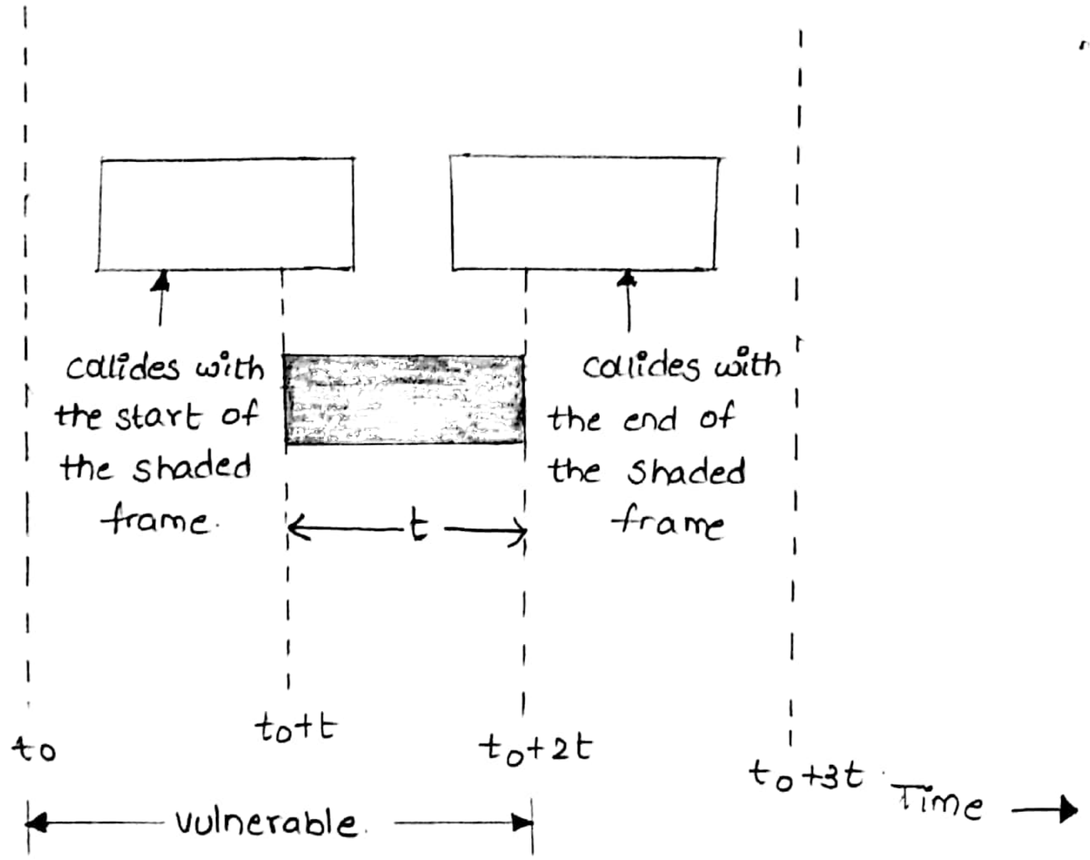
Pure Aloha :-

- In pure aloha, users transmit whenever they have data to be sent.
- There may be collisions & the colliding frames will be damaged.
- If the frame was destroyed, the sender waits a random amount of time & retransmits it again.
- The waiting time must be random or the same frames will collide over and over.
- Systems in which multiplo users share a common channel in a way that can lead to conflicts are

. known as contention systems.



- In the above diagram, all the frames are of equal length.
- Whenever two frames try to ocupy the channel at the same time, there will be a collision & both the frames will be damaged
- If the first bit of a new frame overlaps with ~~the~~ just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.
- The checksum cannot distinguish between a total loss or a near miss.


collides with the start of the shaded frame.
collides with the end of the shaded frame
t
to
to+t
to+2t
to+3t
Time
vulnerable

- Let the mean frame (new) generated by different number of users per frame time be 'S' (frames without collisions). The value of S can be therefore either 0 or 1.

$$\boxed{0 <= S <= 1}$$

- Let the mean frames (new + retransmitted) generated by different number of users per frame time without collisions be 'G'. The value of 'G' is obviously greater than or equal to 'S'

$$\boxed{G >= S}$$

- At low load, S=0

. There will be few collisions. So, few retransmissions are required. So, $\boxed{G = S}$

- At high load, $S = 1$
  There will be many collisions, so more retransmissions are required. So, $\boxed{G > S}$.
- If P_0 is the probability that a frame doesn't suffer from any collision, then

$$\boxed{S = G P_0}$$

For pure aloha, $P_0 = e^{-2G}$

$$\therefore \boxed{S = G e^{-2G}}$$

- If $P_r[K]$ is the probability that 'k' frames are generated during a given frame time, then

$$\boxed{P_r[K] = \frac{G^k e^{-G}}{k!}}$$

- With pure aloha, 18% channel utilization is made.

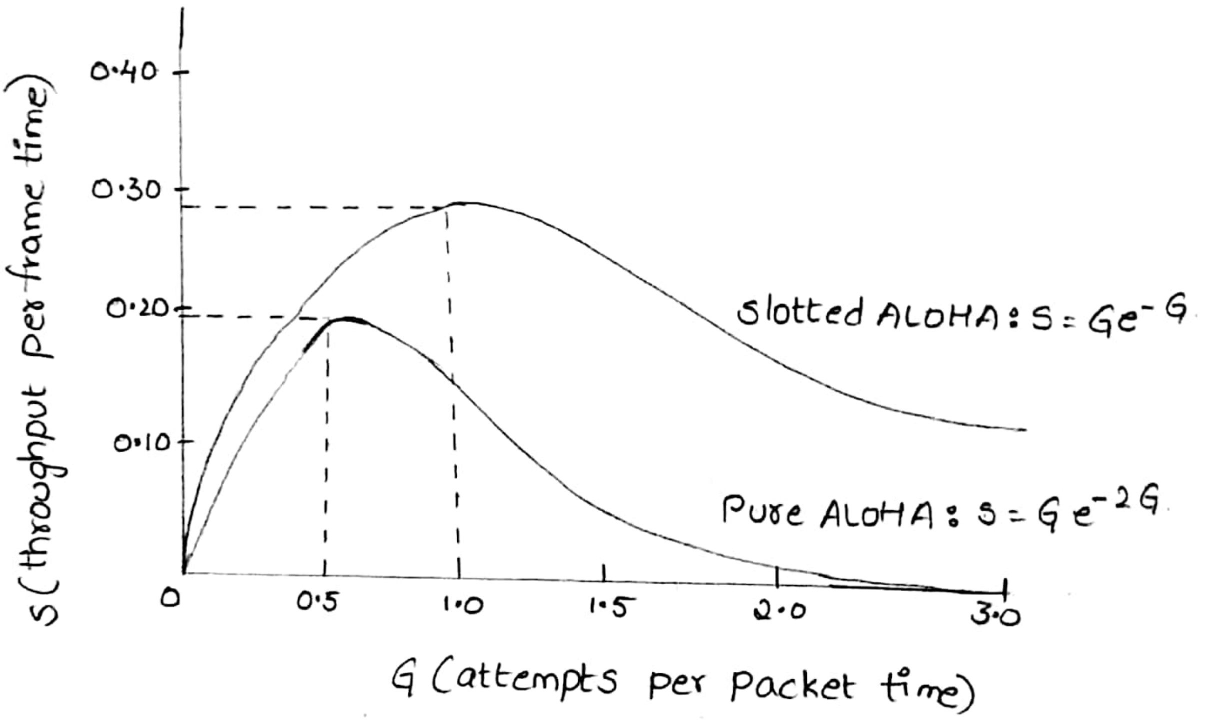
Slotted Aloha :

. In slotted aloha, the time is divided into discrete intervals called slots, each interval corresponding to one frame.

- This approach requires the users to agree on slot boundaries.
- The user is required to wait for the beginning of the next slot.
- The probability of no other traffic during the same slot is e^{-G} which leads to

$$\boxed{S = Ge^{-G}}$$

- In slotted aloha, 36% of channel is utilized.



Carrier Sense Multiple Access Protocols:

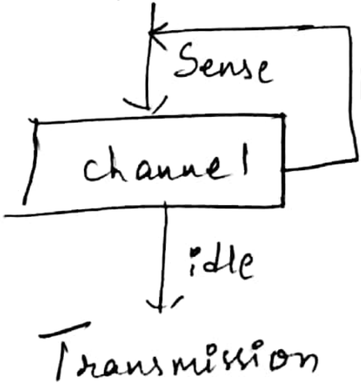
Carrier Sense protocols: Protocols in which stations listen for a carrier (ie, transmission) & act accordingly are called carrier sense protocols

- There are three types of Carrier sense protocols.

They are :- 1- persistent CSMA
Non- persistent CSMA
p- persistent CSMA

ⓐ 1- persistent CSMA :

- When a station has data to send, it first listens to the channel, if channel = busy then the station waits until it becomes idle.
- When the channel is idle, it transmits a frame. If a collision occurs, the station waits for a random amount of time & retransmits.
- It is called 1-persistent because the station transmits with probability = 1.



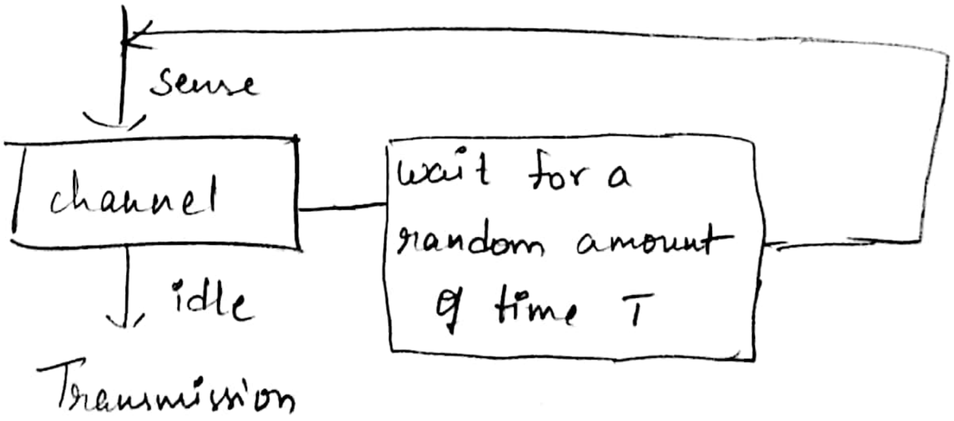
Problems :-

- If a station becomes ready to send (just after another station begins), it senses the channel to be idle (bcz of propagation delay of the first) & will begin sending, which results in a collision.

- If two stations become ready in the middle of third station's transmission, both will politely wait until the transmission ends & both will begin transmitting exactly simultaneously, resulting in a collision.

Non-persistant CSMA :

- A station senses the channel before sending.
- If channel is idle, it starts the transmission.
- If channel is busy, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- Instead, it waits a random amount of time & then repeats the algorithm.



P-persistant CSMA :

- It applies to slotted channels.

- When station is ready to send, it senses the channel."

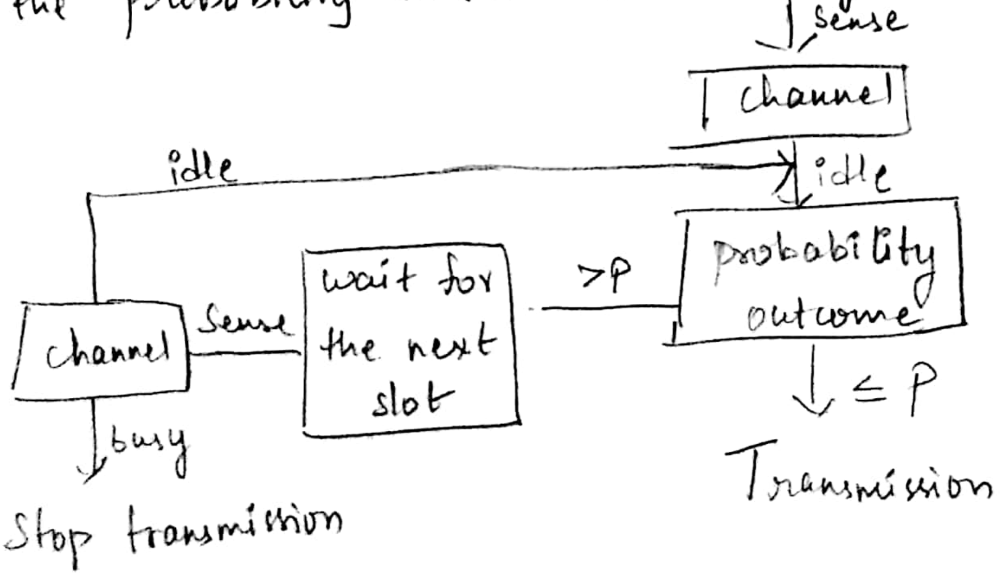
- If the channel is busy, station waits until the channel becomes idle.

- If the channel is idle, the station calculates the probability outcome, if it is less than or equal to 'p' [which is the predefined probability value], then the station performs the transmission.

- If the probability outcome is greater than p, then the station waits until the next time slot and again senses the channel.

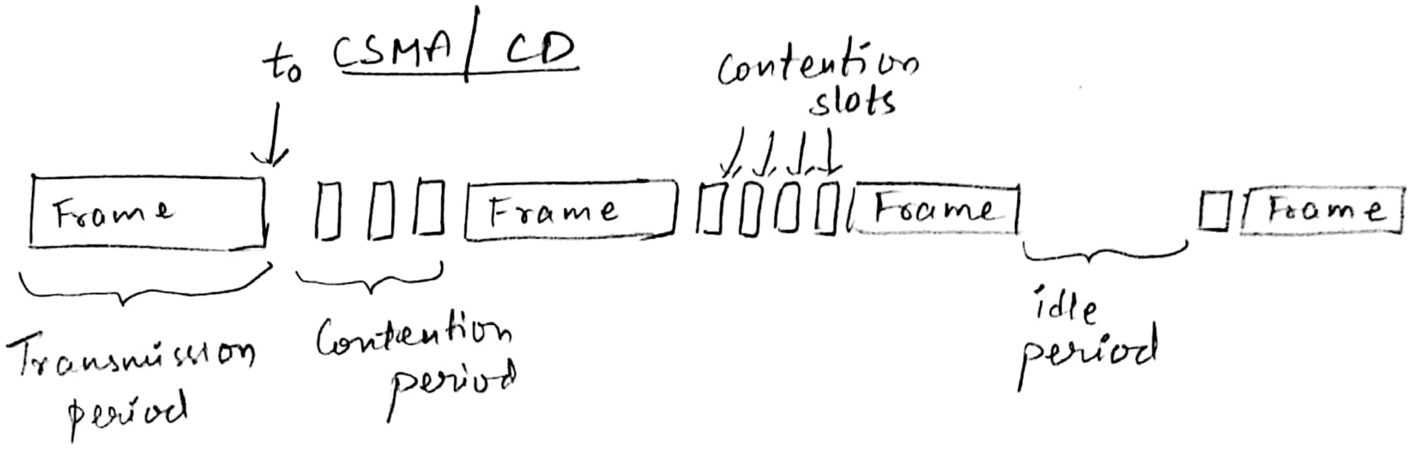
- Now ~~age~~ if the channel is busy, the station stops the transmissions.

- If the channel is idle, it again calculates the probability outcome & the algorithm repeats.



CSMA with collision Detection (CSMA/CD protocol):

- In this protocol, the Stations abort their transmissions as soon as they detect a collision.
- If two Stations sense the channel to be idle & begin transmitting Simultaneously, they will Both detect the collision almost immediately.
- Rather than finish transmitting, their frames, which are damaged any way, they should immediately stop transmitting as soon as the collision is detected.
- Quickly terminating damaged frames saves time & bandwidth.



- At ~~to~~ to, station has finished transmitting its frame.
- Any other station can send the frame now.
- If two or more stations decide to transmit Simultaneously, there will be a collision.

- If a station detects a collision, it aborts its transmission, waits a random period of time & then tries again (assuming that no other station has started transmitting).

- Therefore CSMA/CD model will consist of alternating contention & transmission periods with idle periods occuring when all stations are quiet.

Collision-Free Protocols :

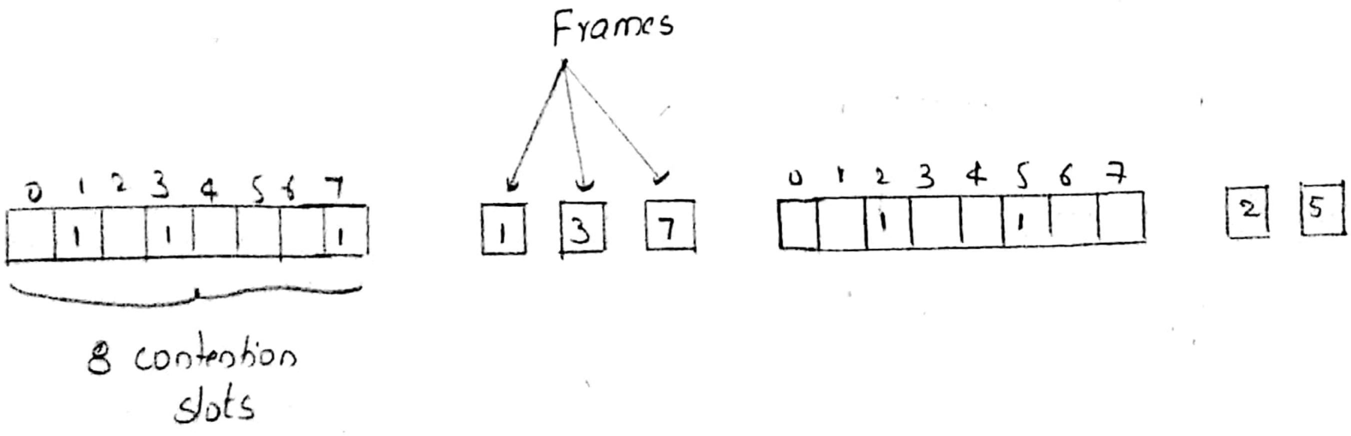
There are three protocols :

Bit-map protocol

Token passing (token ring or token bus protocol)

Binary Count down protocol.

(a) Bit-map protocol :

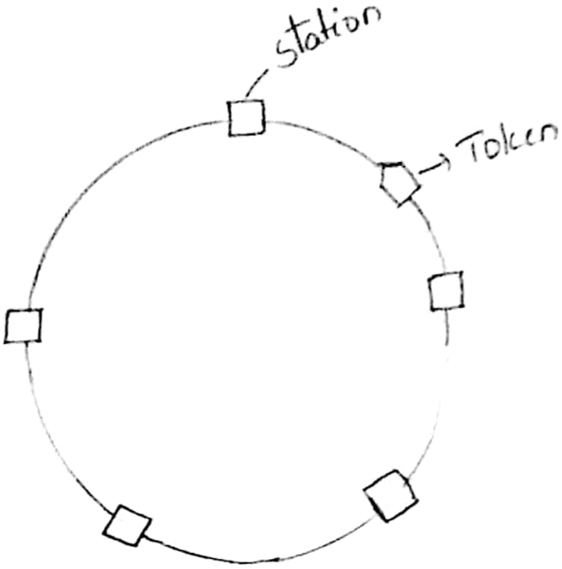


- In this protocol, each contention period consists of exactly 'N' slots.
- If station 0 has a frame to send, it transmits a '1' bit during the zeroth slot.
- No other station is allowed to transmit during this slot.
- Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 during slot 1, but only if it has a frame queued.
- In general, station j may announce that it has a frame to send by inserting a 1 bit into slot j.
- After all N slots have passed by, each station has complete knowledge of which stations wish to transmit.
- If a station becomes ready just after its bit slot has passed by, it is out of luck & must remain silent until every station has had a chance & the bit map has come around again.
- Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

(b) · Token passing :

- In token passing, a small message called a token is passed from one station to the next.
- the token represents permission to send.
- If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station.
- If it has no queued frame, it simply passes the token.
- It is called token ring/token bus protocol.
- The stations are connected one to the next in a single ring.
- Frames are transmitted in the direction of the token.
- they will circulate around the ring & reach whichever station is the destination.
- we do not need a physical ring to implement token passing.
- The channel connecting the station might be a single long bus.

- Each station then uses the bus to send the token to the next station.



(c) Binary Countdown protocol :

	0	1	2	3
0 0 1 0	0	-	-	-
0 1 0 0	0	-	-	-
1 0 0 1	1	0	0	-
1 0 1 0	1	0	1	0
	1	0	1	0

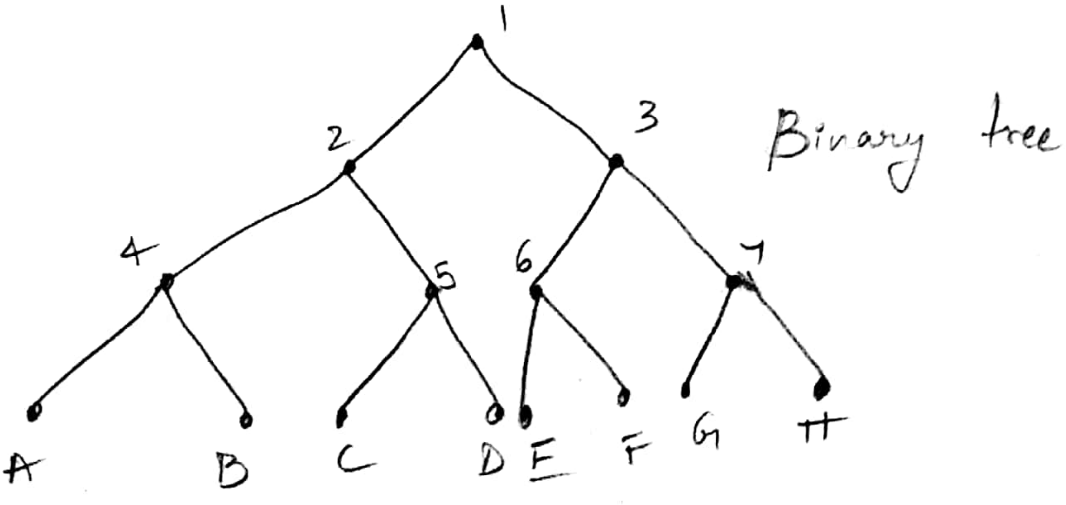
- A station waiting to ose the channel now broadcasts its address as a binary bit string.
- All addresses are assumed to be the same length. The bits in each address position from different stations are BOOLEAN Ored together.
- To avoid conflicts, a rule must be applied: As soon as a station sees that a high order bit position that is 0 in its address has been overwritten with a 1, it gives up.
- For example, if stations 0010, 0100, 1001 & 1010 are trying to get the channel, in the first bit time the stations transmit 0, 0, 1 & 1 resp. These are ORed together to form a 1.
- Stations 0010 and 0100 see ~~that~~ the 1 and know that a higher numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue.
- The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up.
- The winner is station 1010 because it has the highest address.

- Now, station 1010 can transmit a frame, after which another cycle starts.

Limited Contention Protocols :

- In these protocols, we combine the properties of contention - based protocols (CSMA) & collision-free protocols (contention - free protocols)
- Designing a new protocol that uses contention at low load & collision - free technique at high load. Such protocols are called as limited contention protocol.

The Adaptive Tree Walk Protocol :



- Initially all the stations are allowed to try to acquire the channel.
- If any station is able to acquire the channel, it sends its frame

- If there is collision, then all the stations are divided ~~it~~ into two equal groups and only one of these groups compete for slot 1.
- If one of its member acquires the channel then the next is reserved for the other group
- On the other hand, if there is a collision then that group is subdivided and the same process is followed.
- In this protocol, all the stations are organized in a binary tree.

Wireless LAN protocols :

- Consider Wireless LAN is using CSMA, then it just listens for other transmissions & only transmit if the channel is sensed as idle.
- The problems faced while using wireless LAN are:-

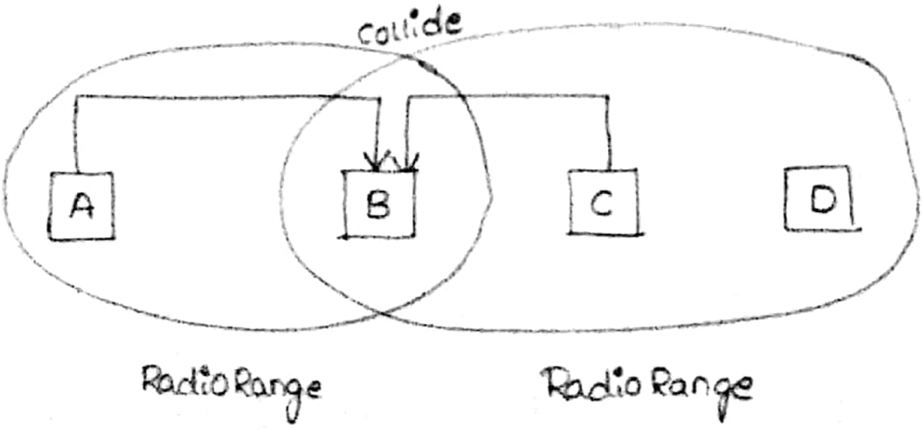
  Hidden Terminal Problem
  Exposed Terminal Problem

- To understand the problems, consider the foll diagram, where four wireless stations are given.

- The radio range is such that A and B are within each other's range and can potentially interfere with one another.
- C can also potentially interfere with both B & D but not with A.

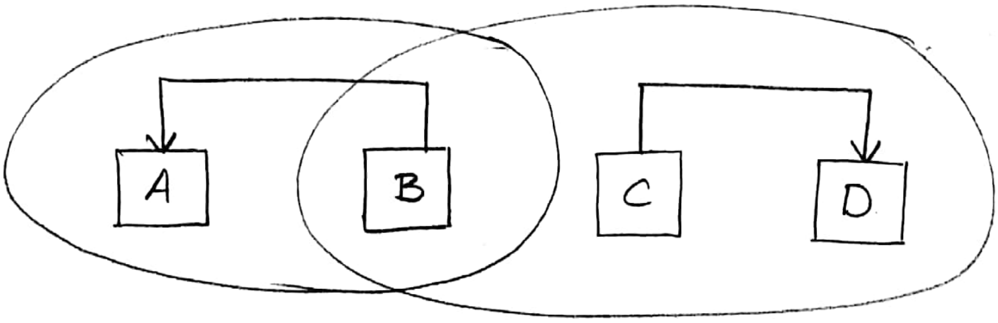
(b) <u>Hidden Terminal Problem</u>:

- Consider that A wants to tranmit to B, C also wants to transmit to B.
- A started transmitting to B.
- When 'C' wants to transmit, it senses the medium, it will not hear A because A is out of range.
- Thus C will falsely conclude that it can transmit to B.
- If C starts transmitting, it will interfere at B, damaging the frame from A.
- The problem araised bcz 'A' is hidden from 'C' hence it is called as hidden terminal problem.



(b) - Exposed Terminal Problem :

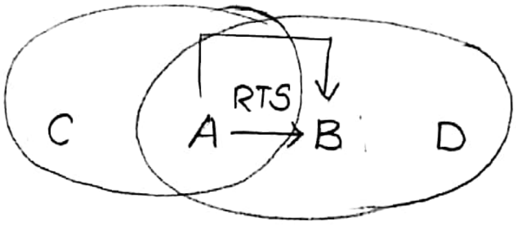
- Consider that 'B' is transmitting to ~~B~~ A and C wants to transmit to D.
- When 'C' wants to transmit, it senses the medium, it will hear a transmission and fasely conclude that it may not send to D.
- So, C stops the transmission to D.
- In this problem, a node is prevented from sending the packets to other nodes bcz of a a neighbouring transmitter.

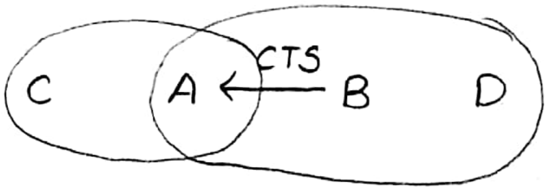


MACA (Multiple Access with Collision Avoidance) :

- A common protocol used for wireless LANs is MACA.
- In this protocol, when A wants to transmit to B, A sends RTS (Request To Send) frame to B.
- This blocks the neighbouring node from transmitting.

- Upon sensing RTS from A to B, C becomes silent.
- B replies 'A' with CTS (Clear To Send) frame. This blocks the neighbouring node from transmitting.
- Upon sensing CTS from B to A, D becomes silent.
- When CTS is received by A, then A starts the transmission.
- So, whenever a sender wants to perform transmission, it should send RTS & receive CTS.





RTS – Request to send

CTS – clear to send.

• Wireless LANS :

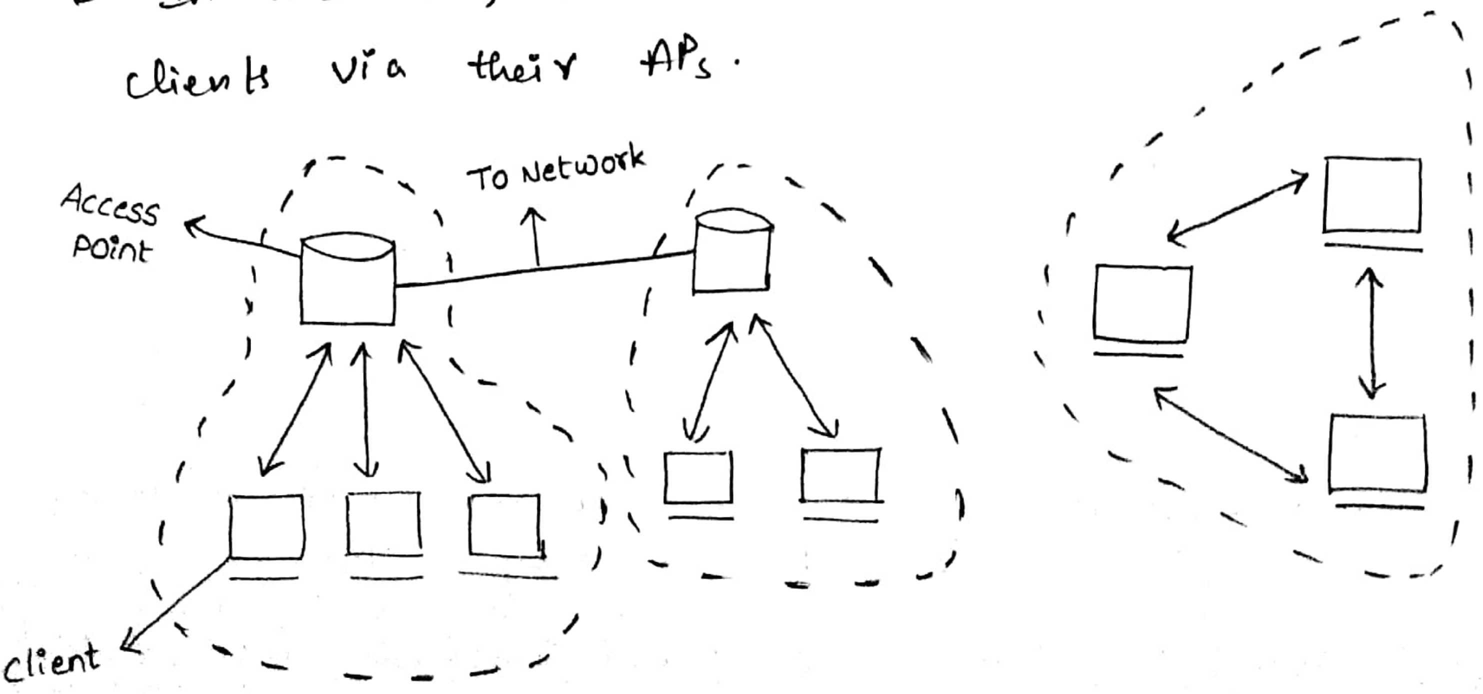
(1) The 802.11 Architecture and Protocol Stack :

802.11 Architecture : 802.11 networks can be used in two modes.

They are:- Infrastructure mode
Adhoc mode.

(a) Infrastructure mode : In this mode, each client is associated with an AP(Access Point) that is in turn connected to the network.

- The client sends & receives its packets via the AP.
- Several access points may be connected together called a distribution system.
- In this case, clients can send frames to other clients via their APs.



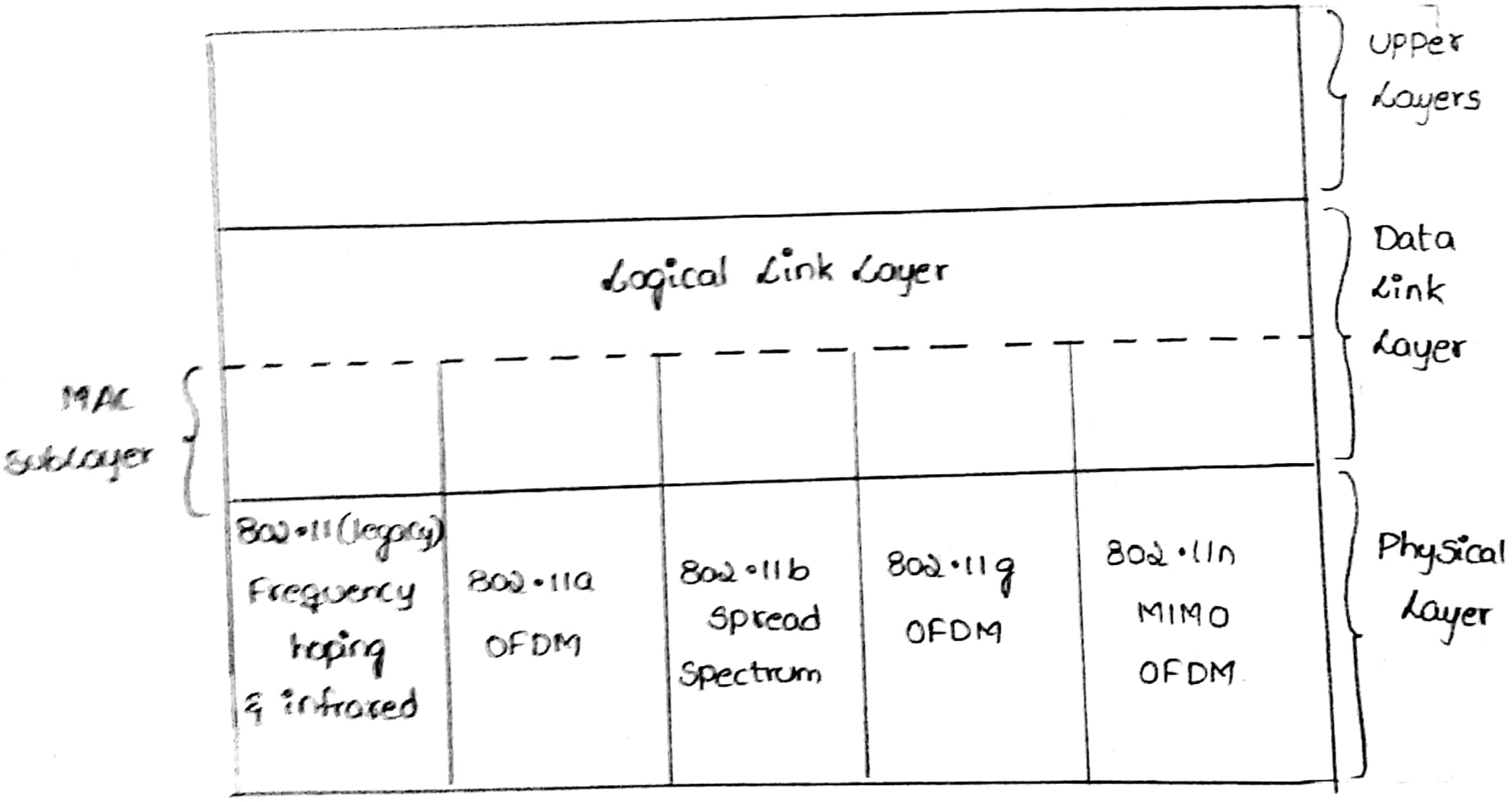
(a) Infrastructure mode

(b) Adhoc mode

(b) Adhoc mode :

- This mode is a collection of computers that are associated so that they can directly send frames to each other.
- There is no access point.

802.11 protocol stack :



802.11 physical layer : Several transmission techniques are included in this layer. They are:-

B of transmitted signal > B of original msg

(a) 802.11 b : It is a spread spectrum method that supports rates of 1, 2, 5.5 & 11 Mbps.

- In real, the operating rate is nearly always 11 Mbps
- It is similar to CDMA system.

(b) • 802.11a : It is a method based on OFDM (Orthogonal Frequency Division Multiplexing) bcz OFDM uses the spectrum efficiently and resists wireless signal degradations.

- Bits are sent over 52 sub carriers in parallel, 48 carrying data & 4 used for synchronization.
- 802.11a can run at eight different rates, ranging from 6 to 54 Mbps.
- these rates are faster than 802.11b rates.

(c) 802.11g :- It copies the OFDM modulation methods of 802.11a. It works as 802.11a.

- It offers the same rates as 802.11a (6 to 54 Mbps).

All the above 802.11 variants can be confusing for customers, so it is common for products to support 802.11a/b/g in a single NIC.

(d) 802.11n : the goal of 802.11n was throughput of atleast 100 Mbps.

- It allows a group of frames to be sent together.
- It uses MIMO (Multiple I/p Multiple O/p) antenna technology.
- In MIMO, it uses multiple antennae at sender and multiple antennae at receiver.

- 802.11n uses upto four antennas to transmit 4 streams of data at the same time.

<u>Data Link Layer</u> :- It consists of two sublayers:

ⓐ <u>MAC sublayer</u> : It determines how the channel is allocated and determines who gets the chance to transmit next.

ⓑ <u>LLC sublayer</u> : Its job is to hide the differences b/w different 802 variants.

<u>802.11 Frame Structure</u> :

Bytes	2	2	6	6	6	2	0-2312	4
	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	check Sequence

	Version = 00	Type =10	SubType = 0000	TO DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
Bits	2	2	4	1	1	1	1	1	1	1	1

• Frame structure consists of 8 fields. They are:-

① Frame Control field : This field is made up of 11 sub fields.

ⓐ Protocol version : It is set to 00. It is there to allow future version of 802·11· to operate at the same time in the same cell.

ⓑ Type : The type of the frame is given. It may be data, control or management frame. For a regular data frame it is set to 10 in binary.

ⓒ Subtype : The subtype of the frame is given. Eg :- RTS or CTS. For a regular data frame subtype field is set of 0000 in binary.

ⓓ To DS and From DS : These bits are set to indicate whether the frame is going to or coming from the N/W connected to the APs, which is called the distribution system.

ⓔ More fragments : This bit means that more fragments will follow.

ⓕ Retry : This bit makes a retransmission of a frame

ⓖ Power management : This bit indicates that the Sender is going into power-save mode.

Scanned by CamScanner

(h) More data : This bit indicates that the sender ~~is~~ ~~going~~ has additional frames for the receiver.

(i) Protected Frame : This bit indicates that the frame body has been encrypted for security.

(j) Order :- This bit tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order.

(2) Duration field : This tells how long the frame and its ACK will occupy the channel.

(3) Address1 (recipient) :- It indicates the add of receiver.

(4) Address2 (transmitter) :- It indicates the add of transmitter.

(5) Address3 : It is an extra field for address.

(6) Sequence field :- It indicates the sequence ~~num~~ number of the frame so that duplicates can be detected.

(7) Data field :- It contains the data to be send or received

(8) Frame check Sequence : It indicates the 32-bit CRC.

UNIT - V

The Network Layer

Network Layer design Issues :

① Store and Forward Packet Switching

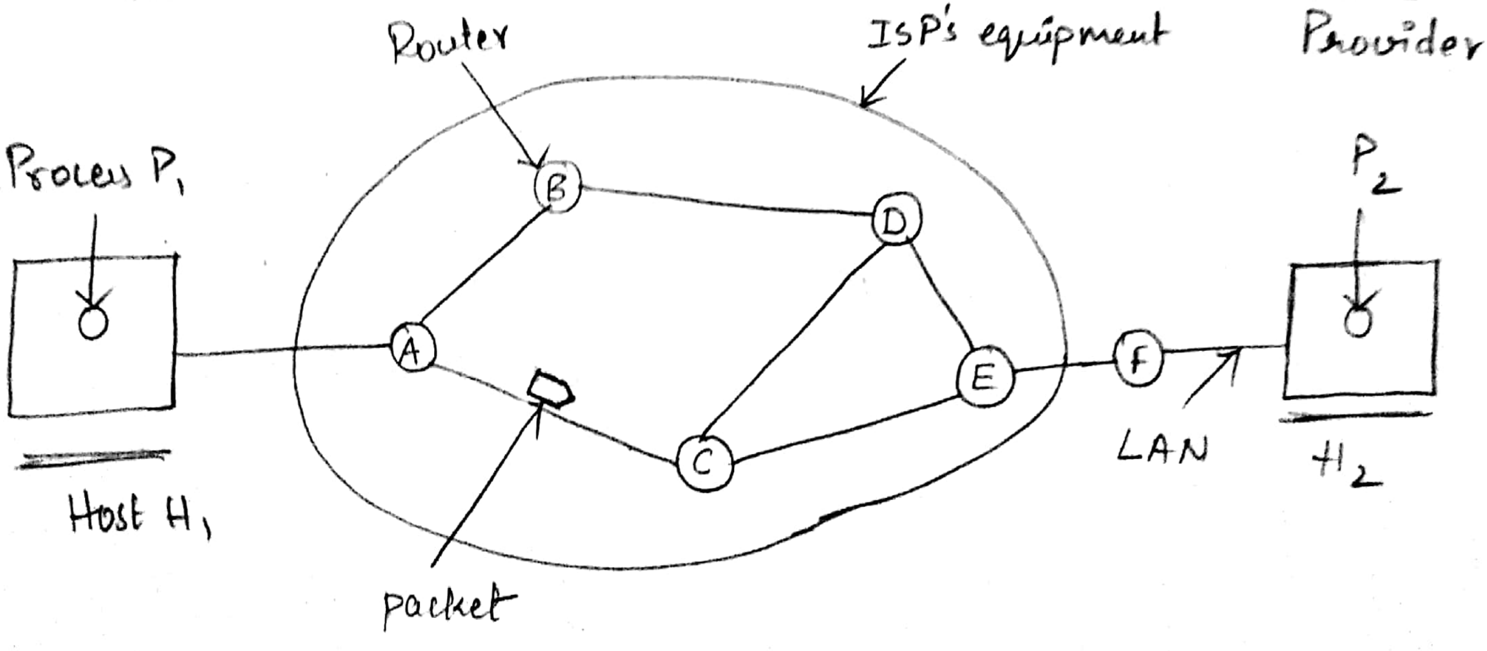
② Services provided to the Transport Layer

③ Implementation of Connectionless Service

④ Implementation of Connection-Oriented Service

⑤ Comparison of Virtual-Circuits & Datagram Networks.

① Store and Forward Packet Switching : ISP: Internet Service Provider



- The major components of Network are ISP's equipment (routers connected by transmission lines) shown inside the oval and Customer's equipment outside the oval.
- Host H₁ is directly connected to one of the ISP's routers.

- H_2 is on a LAN, which might be an office. Ethernet with a router F, owned and operated by the customer.
- Host H_1 transmits the packet to the nearest router
- The packet is stored there until it has fully arrived.
- The link performs error control by verifying the checksum.
- Then it is forwarded to the next router along the path until it reaches the destination host.
- This mechanism is called store-and-forward packet switching.

② Services provided to the Transport Layer:

- The Network Layer provides services to the Transport Layer at the Network Layer/ Transport layer interface.
- The services need to be carefully designed with the following goals:

ⓐ The services should be independent of the router technology.

ⓑ The transport layer should be shielded from the number, type & topology of the routers present.

(c) The Network addresses made available to the transport layer should use a uniform numbering plan.

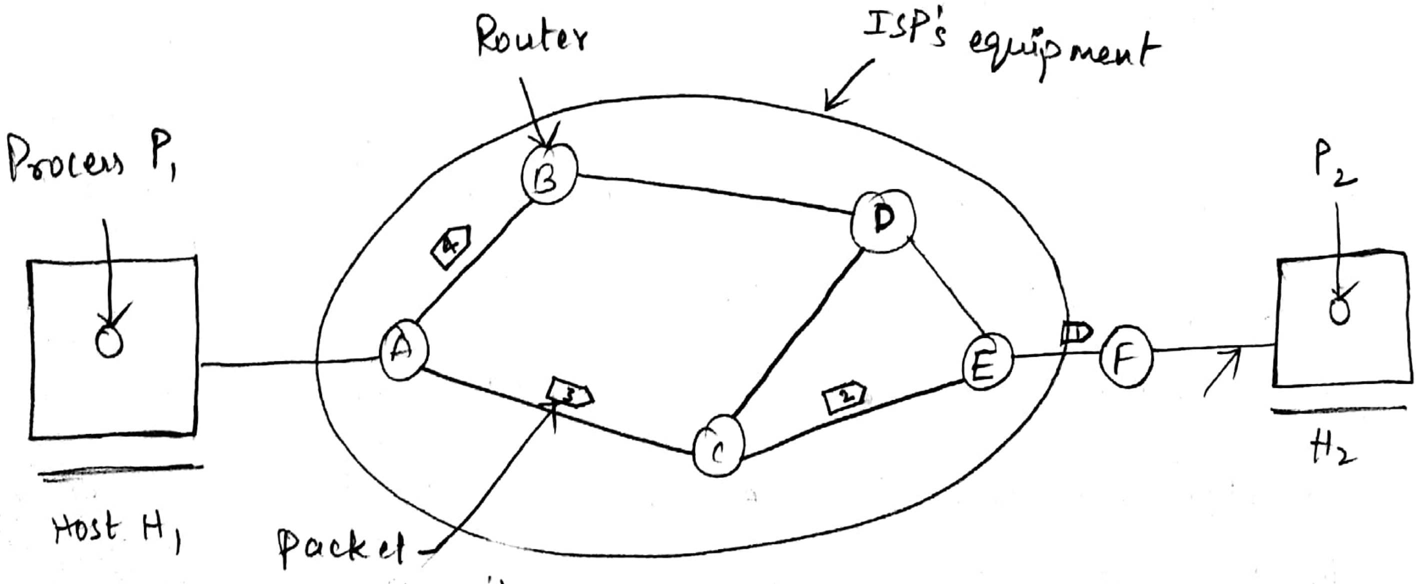
Connection oriented service / connectionless service :

- If the Network layer provides connectionless service, error correction & detection & flow control are done by the hosts themselves.
- Packets are transmitted from source to destination using the primitives SEND PACKET and RECEIVE PACKET where each packet must carry the full destination address, because each packet sent is carried independently. Does not provide Quality of Service (QoS)
- If the Network layer provides connection-oriented service, in case of voice calls & video calls connectionless service lags behind where as connection-oriented service have a good success of telephone Networks.
- With the entry of the following, connectionless service became stronger enough & provided good QoS.

(a) ARPANET (Advanced Research Project Agency of Networks)
(b) ATM (Asynchronous Transfer Mode)
(c) INTERNET
(d) IP (Internet Protocol)

③ Implementation of Connectionless Service :

- If connectionless service is offered, packets are injected into the n/w individually and routed independently of each other.
- No advance setup is needed ie., predefined path is not required.
- In connectionless service, packets are called datagrams and the network is called a datagram n/w.



A's table (initially)

A	—
B	B
C	C
D	B
E	C
F	C

Dest Line

A's table (later)

A	—
B	B
C	C
D	B
E	B
F	B

C's table

A	A
B	A
C	-
D	E
E	E
F	E

E's table

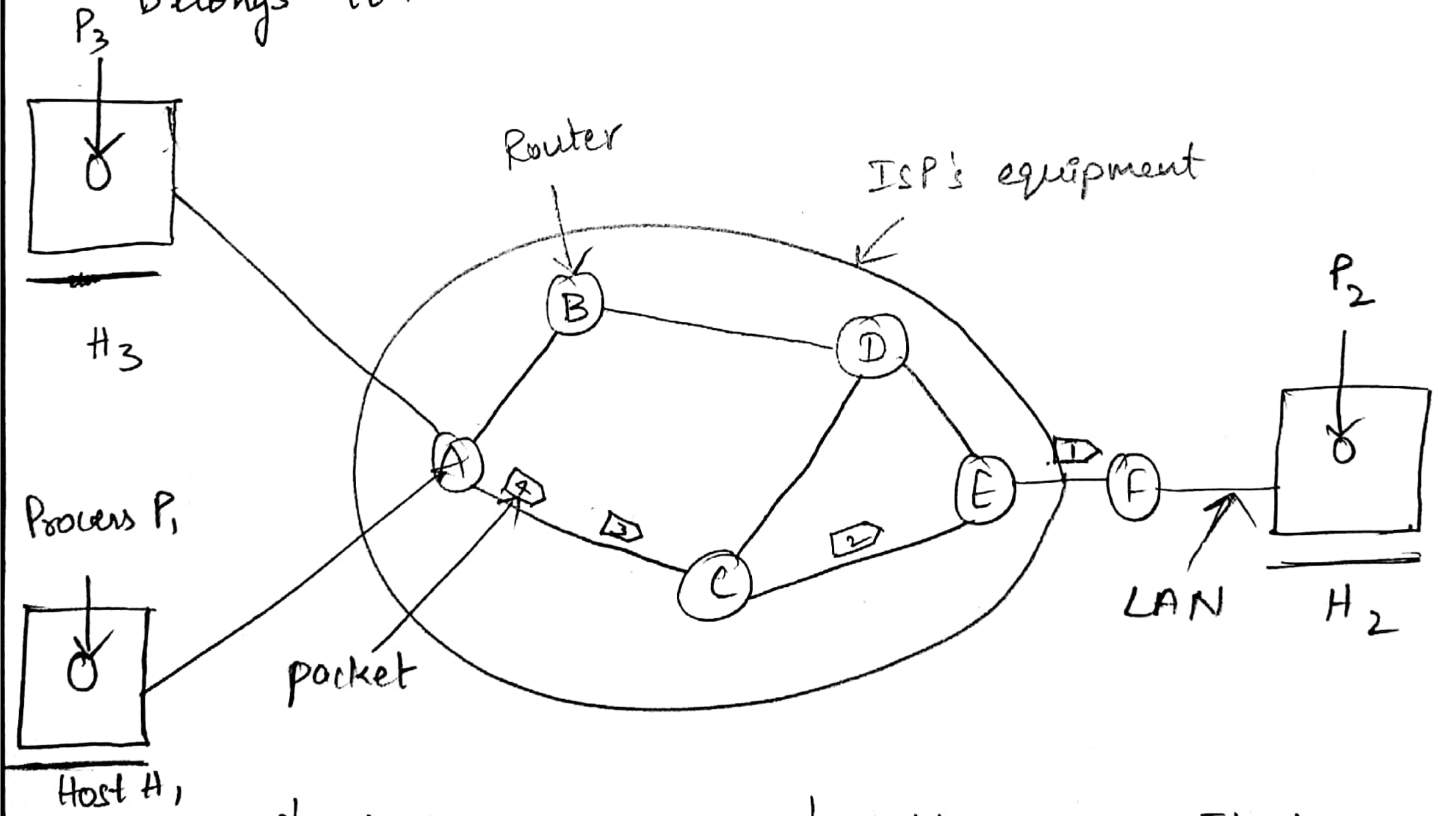
A	C
B	D
C	C
D	D
E	-
F	F

- In the above diagram, suppose that the Process P_1 on Host H_1 has a long message for Process P_2 on Host H_2.
- Assume that the message is four times longer than the maximum packet size, so the n/w Layer has to break it into four packets 1,2,3 & 4.
- Each packet is sent to router A, A has only two outgoing lines - B & C, so every incoming packet must be sent to one of these routers.
- At A, when packets arrived on the incoming link, their checksums are verified, then each packet is forwarded to the next outgoing link.
- Packets 1,2,3 follow the same route ACEF.
- But packet 4, due to traffic it is routed in a different path ABDEF
- The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

4 Implementation of Connection-Oriented Service:

- If connection-Oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent.

- This connection is called a VC (Virtual Circuit) and the netwoork is called a Virtual-Circuit network.
- When a connection is established, a route from source to destination is chosen.
- That route is used for all traffic flowing over the connection.
- When the connection is released, the Virtual-Circuit is also terminated.
- In connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.



A's table

H1	1	C	1
H3	1	C	2

In

Out

C's table

A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

- In the above diagram, host H_1 has established connection 1 with host H_2.
- The first line of A's table says that if a packet bearing connection identifier '1' comes in from H_1, it is to be sent to router C and given connection identifier 1.
- Similarly, the first entry at C routes the packet to E, also with connection identifier 1.
- Consider that H_3 also wants to establish a connection to H_2.
- It chooses connection identifier '1' and establishes VC.
- Here 'A' can easily distinguish connection 1 packets from H_1 and connection 1 packets from H_3, but C cannot do this.
- For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection.
- This process is called label switching.

5 Comparison of Virtual-Circuit & Datagram Networks:

Issue	Datagram N/w	Virtual-Circuit N/w
1 Circuit setup	Not needed	Required
2 Addressing	Each packet contains the full source and destination address.	Each packet contains a short VC number.
3 ~~State information~~		
3 Routing	Each packet is routed independently.	Route is chosen when VC is set up; all packets follow it.
4 Quality of Service (QoS)	Difficult	Easy if enough resources can be allocated in advance for each VC.
5 Congestion Control	Difficult	Easy if enough resources can be allocated in advance for each VC.

Routing Algorithms :

- The main function of N/w Layer is routing packets from source machine to the destination machine.
- The routing Alg is responsible for deciding which output line an incoming packet should be transmitted on.
- Properties in a routing alg :

Correctness	Stability
Simplicity	Fairness
Robustness	Optimality

(1) Correctness. The routing should be done properly and correctly so that the packets may reach their proper destination.

(2) Simplicity : The routing should be done in a simple manner without any complexity.

(3) Robustness : Once a major network becomes operative, it may be expected to run continuously for years without any failures.

- Routing algs should be robust enough to handle hardware & software failures, should be able to cope with changes in the topology and traffic

④ Stability :- The routing algs should be stable under all possible circumstances.

⑤ Fairness :- Every node connected to the n/w should get a fair chance of transmitting their packets. This is generally done on a FCFS basis.

⑥ Optimality : The routing algs should be optimal in terms of throughput & packet delays.

- Routing algs are grouped into two major classes. Non-adaptive routing algorithms & adaptive routing algs.

① Non-adaptive routing alg : ~~96~~ this alg, Do not base their routing decisions on any measurements or estimates of current topology and traffic. The choice of the route is computed in advance & downloaded to the routers when the n/w is booted. This procedure is called Static routing.

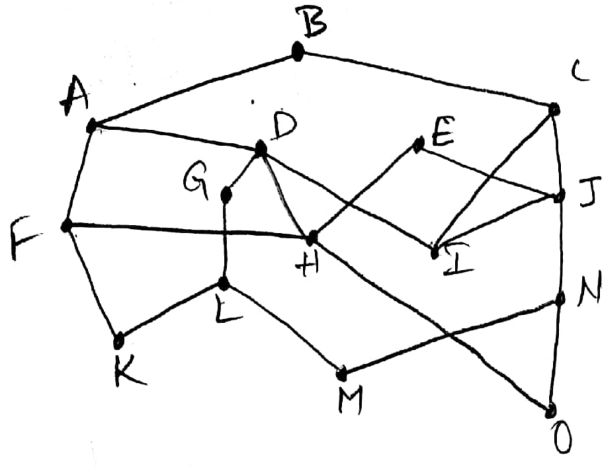
② Adaptive routing Alg : This alg changes their routing decisions according to the changes in topology & traffic. This procedure is called dynamic routing.

Routing Algorithms

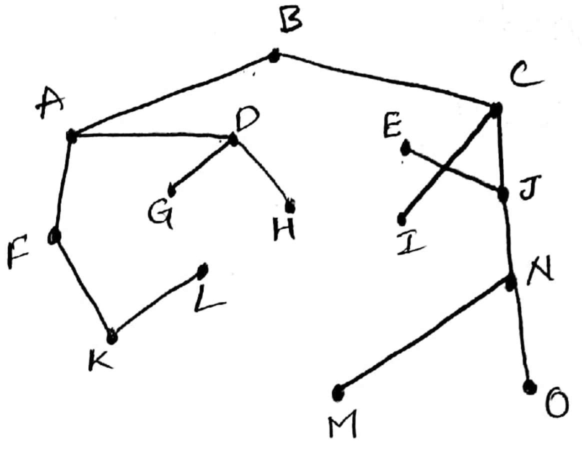
- The optimality principle
- Shortest Path routing
- Flooding
- Distance Vector Routing
- Link State Routing
- Hierarchical Routing
- Broadcast Routing
- Multicast Routing

(1) The optimality principle :

- It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.
- Consider the route from I to J as r_1 route from J to K as r_2
- If a route better than r_2 existed from J to K, it could be concatenated with r_1 to improve the route from I to K.
- In optimality principle, set of optimal routes from all sources to a given destination form a tree rooted at the destination.
- Such a tree is called as a sink tree
- A sink tree is not necessarily unique.
- A sink tree does not contain any loops.



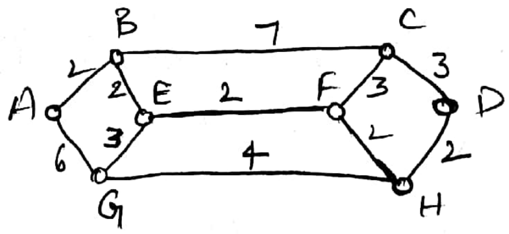
(a)



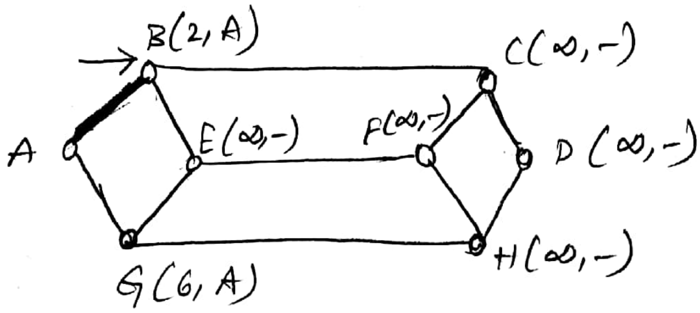
(b)

② Shortest Path Routing Algorithm :

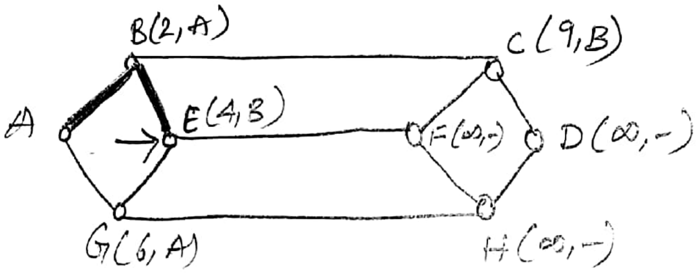
- In this alg, a graph of the N/w is developed, with each node of the graph representing a router and each edge of the graph representing a communication line or link.
- To choose a route b/w a given pair of routers, the alg just finds the shortest path b/w them on the graph.
- The cost of the link may be a function of distance, bandwidth, average traffic, Communization cost, delay etc.



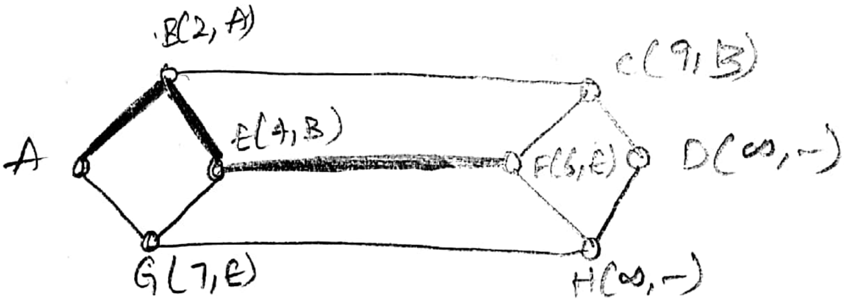
step1 :



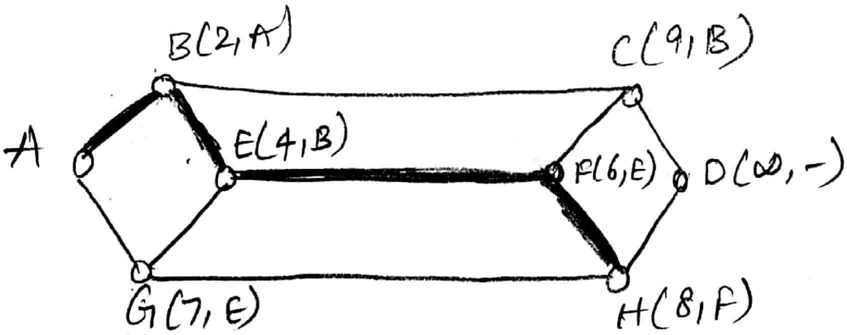
step 2 :



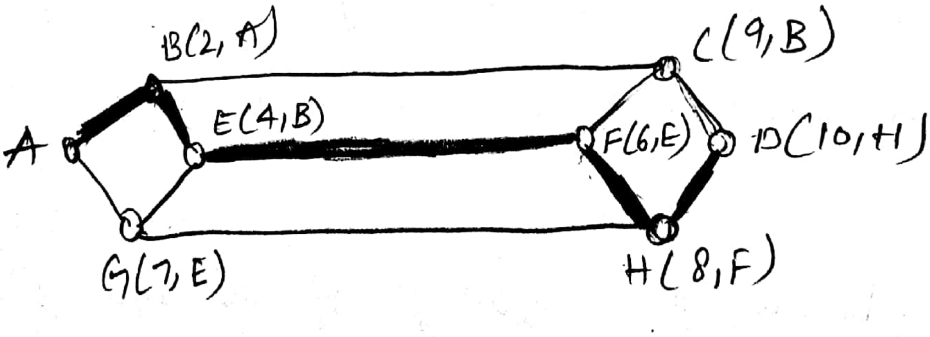
step 3 :



step 4 :

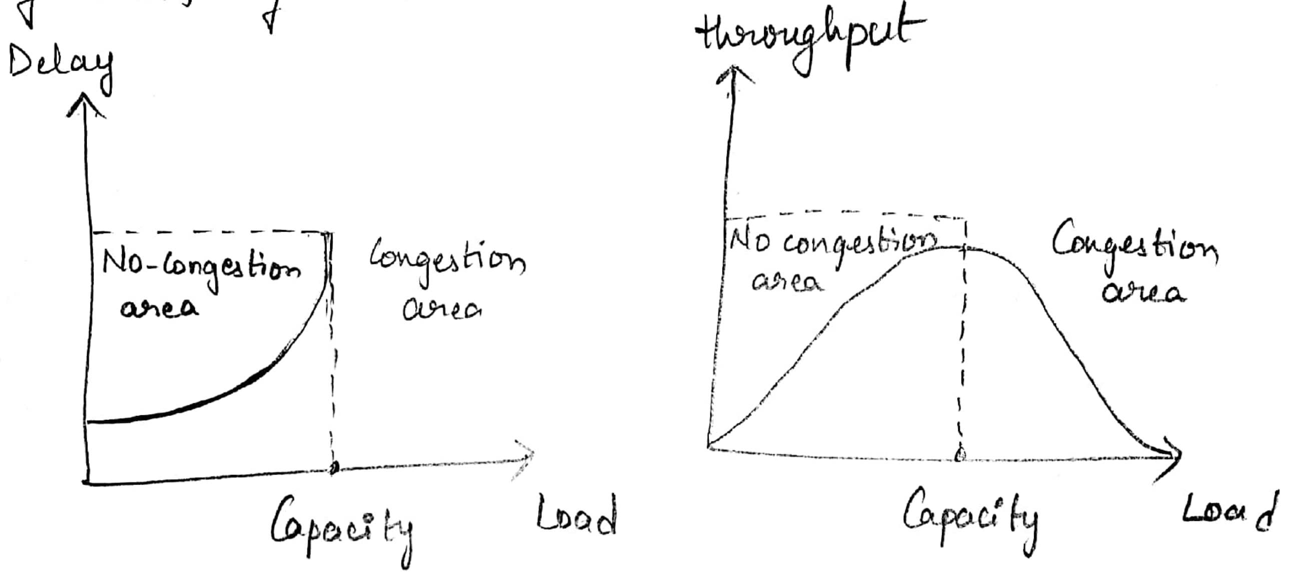


Step 5 :



Congestion Control :

- Too many packets present in a network causes packet delay and loss that degrades performance. This situation is called Congestion.
- Congestion at the network layer is related to two issues, throughput and delay.
- N/w performances with packet delay & throughput as functions of load :



- When the load is less than the N/w capacity, the delay is minimum.
- When the load reaches N/w capacity, the delay increases.
- Delay becomes infinite when the load is greater than the capacity.
- When load is below the capacity of the N/w, the throughput increases ~~pro~~ proportionally with the load.

- When the load exceeds the network capacity, the queues become full and the routers will discard some packets. So, the throughput decreases.
- Discarding packets does not reduce the number of packets in the n/w because the sources retransmit the packets using time-out mechanisms, when the packets do not reach the destinations.
- Congestion Control is of two types:-

Congestion Control

- open loop congestion control
  - policies
    - Retransmission policy
    - Window policy
    - Discarding policy
    - Acknowledgement policy
    - Admission policy
- closed loop congestion control
  - policies
    - Back pressure
    - Choke packets
    - Implicit signaling
    - Explicit signaling
      - Forward signaling
      - Backward signaling

<u>open loop congestion Control</u> : In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or destination.

① ~~Retransmission policy~~

- The policies that can prevent congestion are:-

① Retransmission policy : It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

- This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion & also able to optimize efficiency.

② Window policy:- The type of window at the sender side may also affect the congestion.

- Several packets in Go-back-n window are resent, although some packets are received succesfully at the receiver-
- This duplication increase the congestion in the network.
- Therefore, selective repeat window should be adopted as it sends only the specific packet that is lost.

③ Discarding policy:- A good discarding policy adopted by the routers is the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive packets and also able to maintain the quality of a message.

- In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of audio file.

④ Acknowledgement policy: Since acknowledgements are also part of the load in the network, the ack policy imposed by the receiver may also affect congestion.

- Several approcches can be used to prevent congestion related to acknowledgement.
- ~~Th~~ One of the approach is:- The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.

⑤ Admission policy: Admission policy can also prevent congestion in virtual-circuit networks.

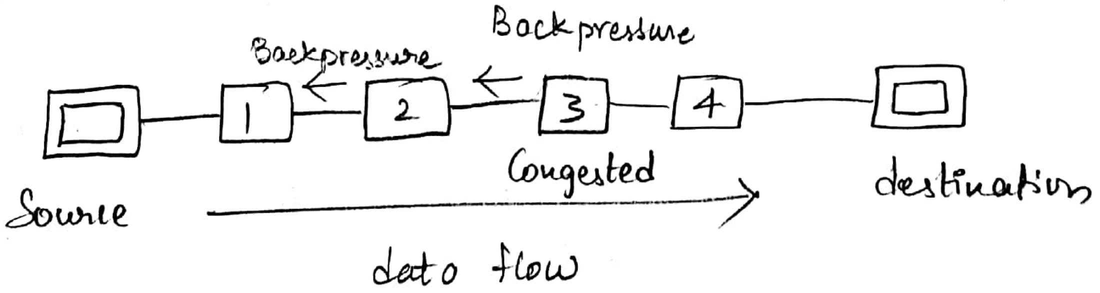
- Switches in a flow should first check the resource requirement of a network flow before transmitting it further.
- If there is a chance of congestion or there is congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All these policies are adopted to prevent congestion before it happens in the network.

Closed loop Congestion control : In closed loop congestion control, policies are used to treat or reduce congestion after it happens.

(1) Backpressure : It is a technique in which a congested node stops receiving packet from (previous) upstream node.

- This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes.
- Backpressure is a node-to-node congestion control technique that propagate in the opposite directions of data flow.
- The backpressure technique can be applied only to virtual-circuit where each node has information of its above upstream node.

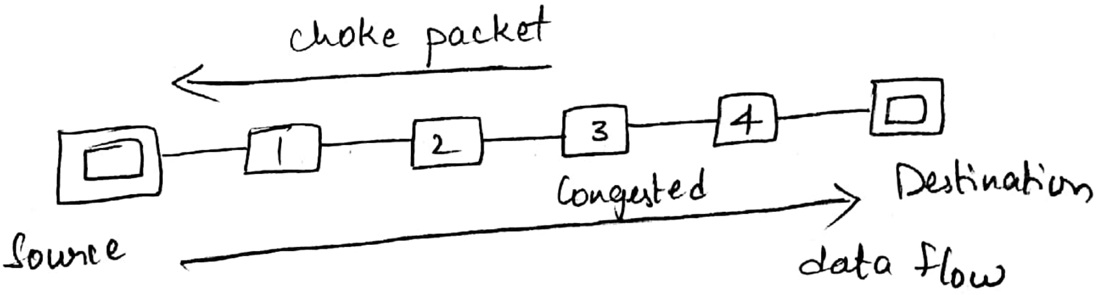


- In the above diagram, the 3rd node is congested and stops receiving packets as a result 2nd node also becomes congested due to slowing down of the output data flow.

- Similarly Ist node may get congested and informs the source to slow down.

② Choke packet technique : This technique is applicable to both virtual circuits as well as datagram subnets.

- A choke packet is a packet sent by a node to the source to inform it of congestion.
- Each router monitor its resources and the utilization at each of its output lines.
- Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic.
- But the intermediate nodes through which the packets has traveled are not warned about congestion.



③ Implicit Signaling : In implicit signaling, there is no communication b/w the congested nodes & the source.

- The source guesses that there is congestion in a network.
- For example, when sender sends several packets and there is no acknowledgement for a while, the source assumes that there is congestion.

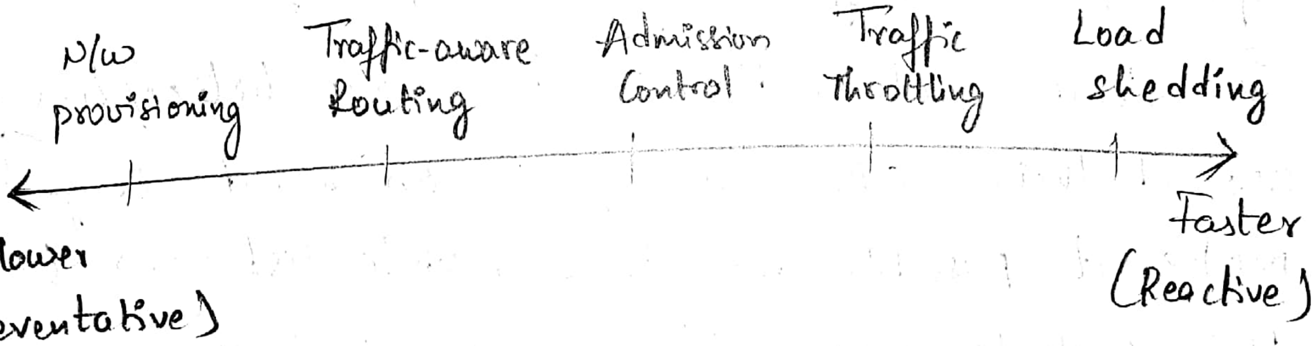
4) Explicity Signaling : In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion.

- The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet.
- Forward Signaling: In this, signal is sent in the direction of congestion ie to the destination.
- The destination is warned about congestion. the receiver in this case adopt policies to prevent further congestion.
- Backward Signaling: In this, signal is sent in the opposite direction of the congestion. The source is warned about congestion & it needs to slow down

Congestion Control algorithms :

Approaches to Congestion Control

- The presence of congestion means that the load is greater than the resources can handle.
- Two solutions can be used : either increase the resources or decrease the load.
- These solutions can be used either to prevent congestion or react to it once it has occurred.
- Different approaches are :-



① N/W provisioning :-

- In this approach, resources are added dynamically when there is congestion.

ways to add resources :-

ⓐ turning on spare routers or enabling lines that are normally used only as backups.

(b) purchasing bandwidth on the open market.

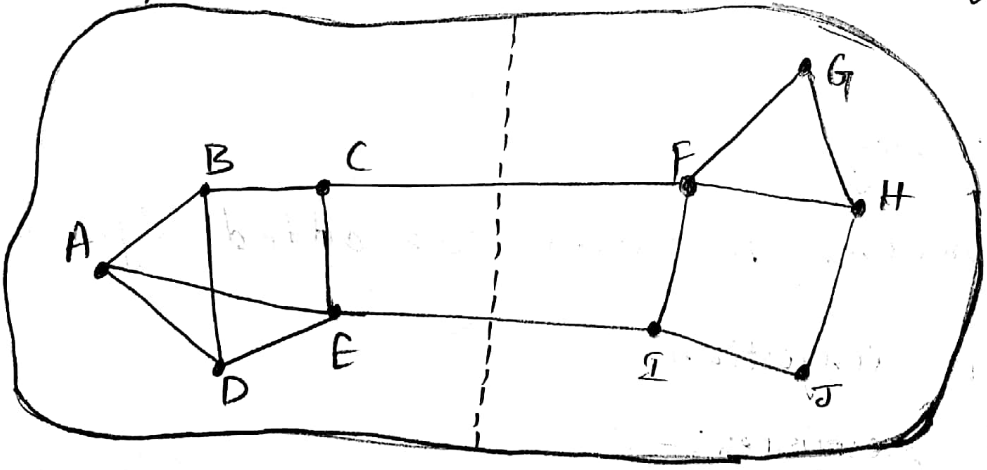
(c) links & routers that are regularly heavily utilized are upgraded.

- This is called provisioning & happens on a time scale of months, driven by long-term traffic trends

(2) Traffic-Aware Routing: This is done in the foll ways:-

- Routes can be changed by shifting the traffic from heavily used paths to lightly used paths.
- Splitting the traffic across multiple path can also be done.

Ex: Some local radio stations have helicopters flying around their cites to report on road congestion to make it possible for their mobile listeners to route their packets (cars). This is called traffic-aware routing.



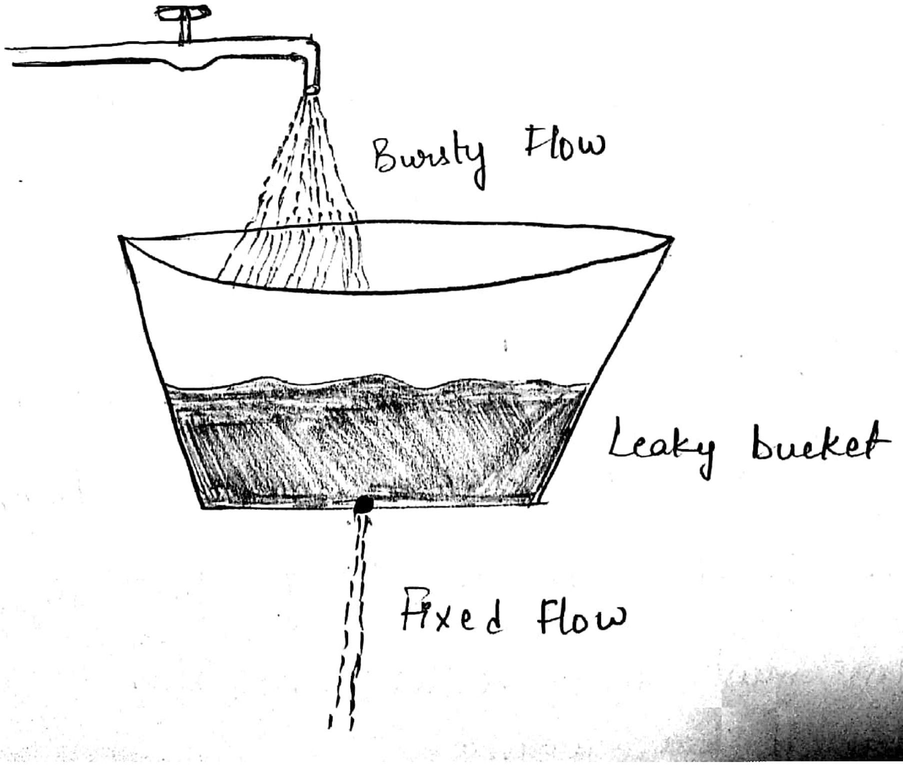
- Consider a network which is divided into two parts, east and West, connected by two links CF & EI.

- Suppose most of the traffic between East and West is using the link CF, the that link is congested.
- Then that traffic should be shifted to other link EI or the traffic should be splitted b/w CF & EI
- So that the congestion can be controlled.

③ Admission Control :- This technique is widely used in virtual-circuit networks.

- It states that : do not set up a new virtual circuit unless the N/w can carry the added traffic without becoming congested.
- Admission control can be done by using leaky bucket or token bucket.

Leaky bucket :



- **Leaky Bucket Algorithm:**

- Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate.
- When the bucket is full with water additional water entering spills over the sides and is lost.
- Similarly, each network interface contains a leaky bucket & the foll steps are involved in leaky bucket algorithm:

① When host wants to send packet, packet is thrown into the bucket.

② The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.

③ Bursty traffic is converted to a uniform traffic by the leaky bucket.

④ In practise the bucket is a finite queue that outputs at a finite rate

④ **Traffic Throttling:** This approach can be used in both datagram networks and virtual-circuit networks.

- This approach is done in the foll two steps:

Step 1:- Routers must determine when congestion is approaching before it has arrived.

→ For the router to determine congestion, it should monitor the following things:

ⓐ utilization of output links

ⓑ Buffering of queued packets inside routers

ⓒ Number of packets that are lost due to insufficient buffering.

- The queuing delay inside routers can also determine the congestion.
- If there is congestion, the queuing delay increases.
- The queuing delay can be calculated by the foll formula

$$d_{new} = \alpha d_{old} + (1-\alpha) s$$

α = constant
S = queue length.

This is called an EWMA (Exponentially Weighted Moving Average)

Step 2: Routers must deliver timely feedback to the sender that are causing the congestion.

Different schemes use different feedback mechanisms, They are :- choke packets [in closed loop Congestion Control)

Explicit Congestion Notification [Explicit Signaling]

Hop-by-Hop Backpressure [Back pressure in closed loop]

(5) Load shedding :-

- Load shedding means that when routers are being overloaded by packets that they cant handle they just throw them away.
- Packet drop is done in two ways:-

(a) wine : In this method it is assumed that old packet is better than new packet. ~~th~~ So, the new packet is discarded.

(b) milk :- In this method, it is assumed that new packet is better than old packet. So, the old packet is discarded.

Random Early Detection : In this method, Congestion is detected earlier and the packets the discarded.

- Packets should be discarded before all the buffer space is exhausted.
- To determine when to start discarding, routers maintain a running average of their queue lengths.
- When the avg queue length on some link exceeds, a threshold, the link is said to be congested & small fraction of packets are dropped at random.

802.11 Services : 802.11 standard defines the foll services.

(a) **Association Service** : This service is used by the mobile stations to connect themselves to APs. (Access Point)

(b) **Reassociation service** : This service lets a station change its preferred AP.

(c) **Diassociate service** : It is used to break the relationship b/w station and AP.

(d) **Authentication** : Stations must authenticate before they can send frames via the AP. There are two schemes for authentication :- They are:

- **WEP (Wired Equipment Privacy)** : In this scheme, authentication is done with a pre shared key before association
- **WPA2 (WiFi Protected Access 2)** : AP will talk to an authentication server that has a username and password database to determine if the station is allowed to access the N/w.

(e) **Distribution service** : Once the frames reach the AP, this service determines how to route them.

- If the destination is local to the AP, the frames can be sent out directly over the air.
- Otherwise, they will have to be forwarded.

(f) Integration service : This service handles any translation that is needed for a frame to be sent outside the 802-11 LAN, or to arrive from outside the 802-11 LAN.

(g) Delivery Service : This service allow stations to transmit & receive data using the protocols.

(h) Privacy Service : 802-11 is not guaranteed to be reliable. It must deal with detecting & correcting errors.

- For information sent over a wireless LAN to be kept confidential, it must be encrypted.
- This service manages the details of encryption & decryption
- The encryption Alg is based on AES (Advanced Encryption Standard).

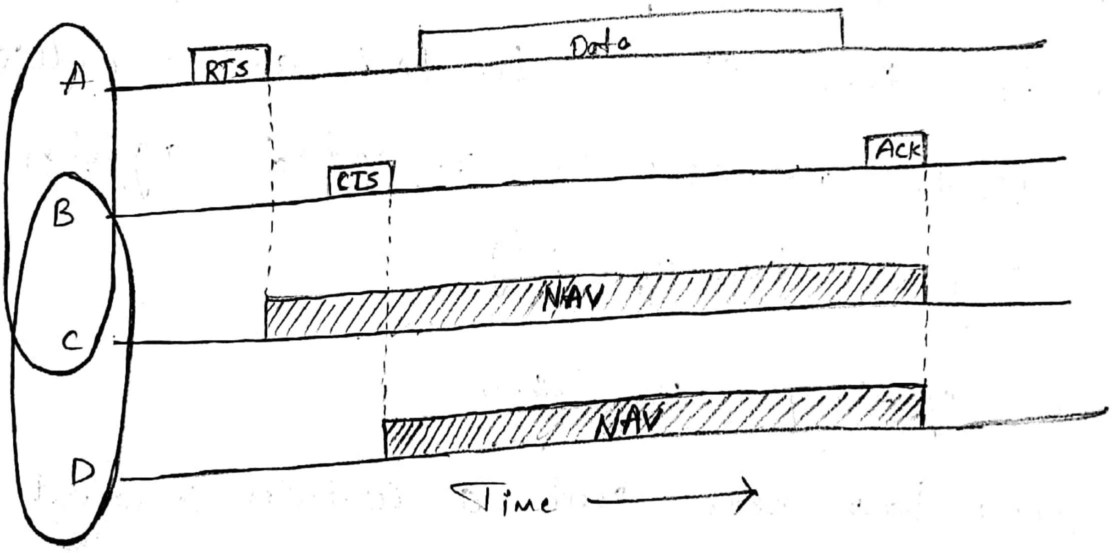
(i) QoS traffic Scheduling service : This service handles the traffic with different priorities.

(j) Transmit power control service : This service gives stations the information they need to meet regulatory limits on transmit power that vary from region to region.

(k) Dynamic frequency selection service : It gives the stations information they need to transmit on different frequencies

802.11 MAC Sublayer Protocol :

- To overcome hidden terminal problem and exposed terminal problem, 802.11 defines channel sensing ~~to~~ whz consist of both physical sensing & virtual sensing.
- With physical sensing, each station checks the medium to see if there is a valid signal.
- With virtual sensing, each station keeps a logical record of when the channel is in use by tracking the NAV (Network Allocation Vector).
- NAV field indicates that the channel will be busy for the period indicated by NAV.
- RTS/CTS mechanism is also used along with the NAV field.

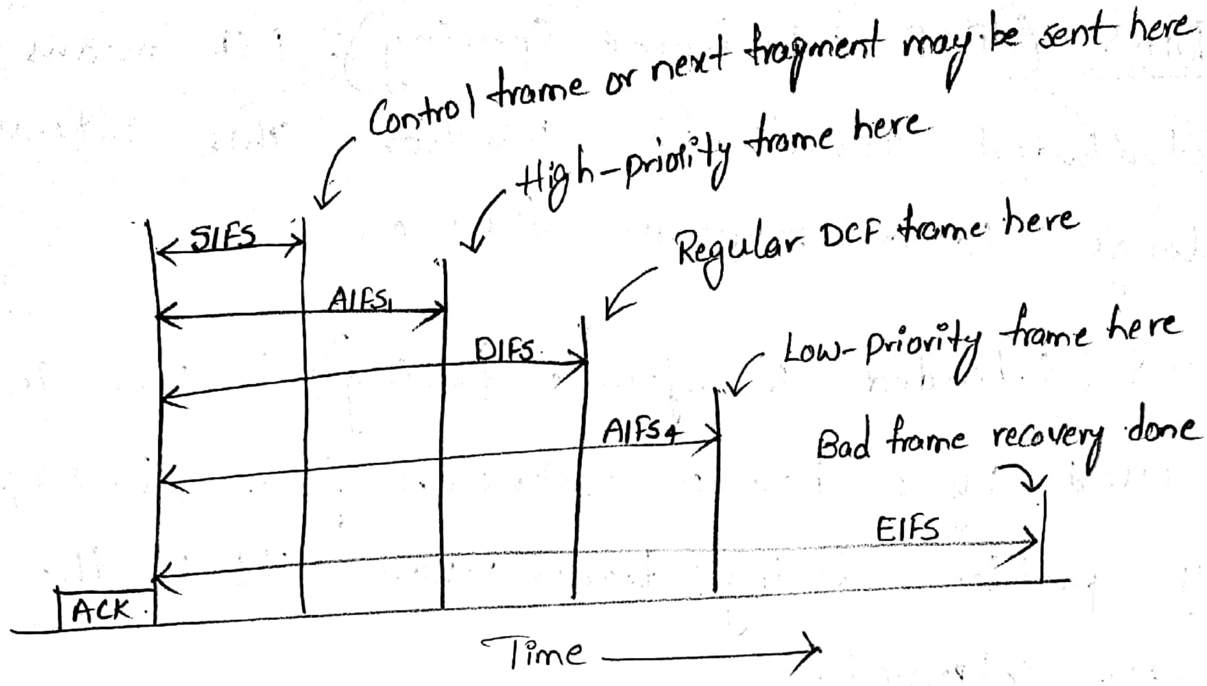


Virtual channel sensing using CSMA/CA

- In the above example, C is a station within range of A, also within range of B, D is a station within range of B but not within range of A.
- Now consider that A wants to send to B.
- Then A sends an RTS frame to B to request permission to send it a frame.
- When B receives RTS, it answers with a CTS frame to indicate that the channel is clear to send.
- When A receives CTS frame, it sends its frame and starts an ACK timer.
- When B receives the data, it responds with an ACK frame.
- If A's ACK timer expires before the ACK gets back to it, then it is treated as a collision & the whole protocol is repeated again after using a backoff Alg.

Interframe spacing in 802.11

- After a frame has been sent, a certain amount of idle time is required before any station may send a frame to check that the channel is no longer in use.
- The different time intervals for diff kinds of frames is as follows.



Interframe Spacing in 802.11

- Five intervals are shown in the above diagram.

ⓐ SIFS (Short Interframe Spacing) : It is the shortest interval. This interval belongs to a control frame. (Ex:- CTS, RTS).

ⓑ AIFS (Arbitration Interframe Spacing) : In AIFS, two intervals are included for two different priority levels.

- $AIFS_1$ is smaller than DIFS but longer than SIFS. $AIFS_1$ belongs to high-priority frames.

- $AIFS_4$ is larger than ~~DF~~ DIFS. It belongs to low-priority frames.

(c) DIFS : (DCF Interframe Spacing): DCF means Distributed Coordination Function. This interval belongs to a regular frame.

(d) EIFS (Extended Interframe Spacing) : This interval is used by a bad or unknown frame, to report any problem during transmission. It is the largest interval.

Ethernet (802.3) :

- There are two kinds of Ethernet. They are:-

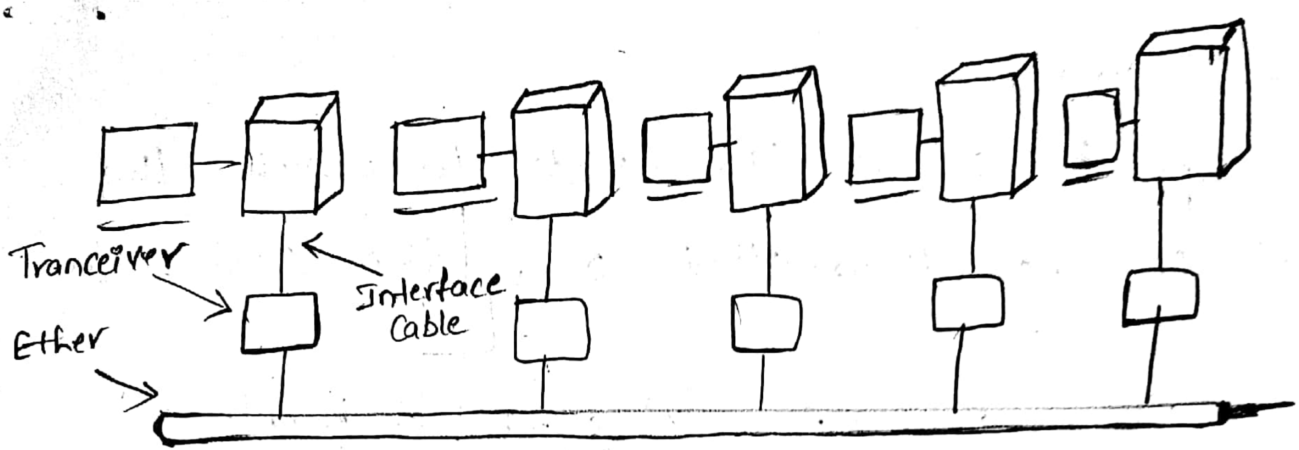
Classic Ethernet : It solves the multiple access problem.
speed rate: 3 to 10 Mbps

Switched Ethernet :- In this, devices called switches are used to connect different computers.

Speed rate - 100 Mbps called Fast Ethernet
1000 Mbps called Gigabit "
10,000 Mbps called 10-gigabit "

Classic Ethernet Physical Layers :-

- There are two kinds of Classic Ethernet. They are:- Thick Ethernet and Thin Ethernet.



Architecture of Classic Ethernet

Thick Ethernet

- It uses thick cable for interconnection
- It is also called Thicknet
- It is called 10Base5

transmission speed = 10 Mbits/sec

Cable length = 500 m

Thin Ethernet

- It uses thinner coaxial cable.
- It is also called Thinnet
- It is called 10Base2
- ~~It is called~~

transmission speed = 10 Mbits/s

Cable length = 200 m

Repeater: To allow larger Networks, multiple cables can be connected by repeaters.

- It is a physical layer device that receives, regenerates and retransmits signals in both directions.
- It regenerates the signal over the same N/w.
- When the signal becomes weak, repeater copies the

the signal bit by bit & regenerate it to its original strength.

- It helps to extend the length to which the signal can be transmitted over the same n/w.

Classic Ethernet MAC Sublayer Protocol

802.3 Frame Format :

8		6	6	2	0-1500	0-46	4
Preamble	SOF	Destination Address	Source Address	Type/Length	Data	Pad	Checksum

- Preamble : This is seven bytes long & it consists of a pattern of alternating one's & zero's, this informs the receiving stations that a frame is starting as well as enabling synchronization.

- SOF (Start of Frame delimiter): This consists of one byte & contains and alternating pattern of one's & zero's but ending in two ones. The last two 1 bits tell the receiver that the rest of the frame is about to start

- Destination address : It is 6 bytes long. This field contains the address of station for which the data is to be sent. The left most bit indicates whether the destination address is an individual address or group address.
  - An individual address is denoted by zero, group address is denoted by one.
  - the next bit in DA indicates whether the address is globally administered or local.
  - If the address is globally administered, the bit is zero. locally administered, the bit is one.
  - The remaining 46 bits are used for DA.
- Source address : It is 6 bytes long. It is the address of sending station. As it is always an individual address, the left most bit is always a zero.
- Type :- It is 2 bytes long. It indicates the frame type.
- Data & pad : It contains the data, it may be upto 1500 bytes long. If the data is above 1500 byte then padding field is used for more data.
- Checksum: It is 4 bytes long. It contains a 32-bit CRC.

CSMA/CD with Binary Exponential Alg:

- It is used to schedule retransmissions after collisions.
- If a collision takes place b/w 2 stations they may restart transmission as soon as they can after the collision.
- This will always lead to another collision and form an infinite loop of collisions leading to a collision.
- To prevent this, backoff Alg is used.

Backoff Alg:

- The stations involved in collision randomly pick an integer from the set K ie., {0,1}. This set is called the contention window.
- If the stations collide again bcz they picked the same integer, the contention window size is doubled & it becomes {0,1,2,3}.
- Now the stations involved in second collision randomly pick an integer from the set {0,1,2,3} & wait that number of time slots before trying again.

- Before they try to transmit, they listen to the channel & transmit only if the channel is idle.
- This causes the station which picked the smallest integers in the contention window to succeed in transmitting its frame.
- So, Backoff alg defines a waiting time for the stations involved in collision ie., for how much time the station should wait to re-transmit

Fast Ethernet :

- The ethernet whose speed is 100 Mbit/s, it is called as Fast ethernet.
- It belongs to IEEE 802.u standard.
- It consists of three sub-standards. They are:-

(a) 100Base - T4 :-

- It uses four pairs of category 3 UTP cables.
- Two of the four pairs are bi-directional the other two pairs are unidirectional.
- Of the four pairs, one is always to the hub, one is always from the hub and other two are switchable to the current transmission direction. (Sending, receiving)
- Cable length is less than 100m.

Gigabit Ethernet.

- The ethernet whose speed is 1000 Mbits/s, it is called as Gigabit Ethernet.
- It belongs to IEEE 802.3 ab/z standard.
- It supports two different modes. They are:-

  Full - duplex mode
  Half - duplex mode

Full - duplex mode : In this configuration, there is a central switch connected to computers.

- All lines are buffered so that each computer and switch is free to send frames whenever it wants.
- The sender does not have to sense the channel to see if anybody else is using it, hence CSMA/CD protocol is not used.

Half-duplex mode :

- It is used when the computers are connected to a hub rather than a switch.
- A hub does not buffer the incoming frames.
- In this mode, collisions are possible. so, CSMA/CD protocol is required.

- It consists of four sub-standards.

(a) 1000 Base - SX :

- It uses Fiber optic cable which is a multimode fiber
- The cable length is maximum 550 m.

(b) 1000 Base - LX :

- It uses Fiber optic cable which may be single mode or multimode.
- the cable length is maximum 5000 m.

(c) 1000 Base - CX :

- It uses 2 pairs of STP cables.
- The cable length is maximum 25 m.

(d) 1000 Base - T :

- It uses 4 pairs of category 5 UTP cables.
- the cable length is maximum 100 m.

10 - Gigabit Ethernet :

- Ethernet whose speed is 10,000 Mbits/s, it is known as 10- Gigabit Ethernet.
- It supports only full-duplex operation.
- So CSMA/CD is not used.

- It consists of 5 sub-standards :-

ⓐ **10GBase-SR** :

- It uses Fiber-optic cables.
- It uses a multimode fiber.
- The cable length is max 300m.

ⓑ **10GBase-LR** :

- It uses Fiber-optic cables.
- The fiber used is only single-mode fiber.
- The cable length is max 10 km.

ⓒ **10GBase-ER** :

- It uses fiber-optic cables.
- The fiber used is only single-mode fiber.
- The cable length is 40 km.

ⓓ **10GBase-CX4** :

- It uses 4 pairs of twinaxial copper cables.
- The cable length is maximum 15m.

ⓔ **10GBase-T** :

- It uses 4 pairs of category 6a UTP cables.
- The cable length is maximum 100m.

Ethernet Performance :

- Consider that 'k' stations are ready to transmit

$$\boxed{A = kp(1-p)^{k-1}}$$

p = probability of each station transmitting during a contention slot.

A = probability that some station acquires the channel in that slot.

- Channel efficiency = $\dfrac{P}{P + 2T/A}$

P = time taken for frame to transmit

2T = duration of each slot.

- Channel efficiency in terms of F, B, L :

channel efficiency = $\dfrac{1}{1 + 2BLe/cF}$

B = Network Bandwidth

L = Cable length

F = Frame length

c = Speed of Signal propagation

e = Number of contention slots per frame.

Scanned by CamScanner

UNIT - VI

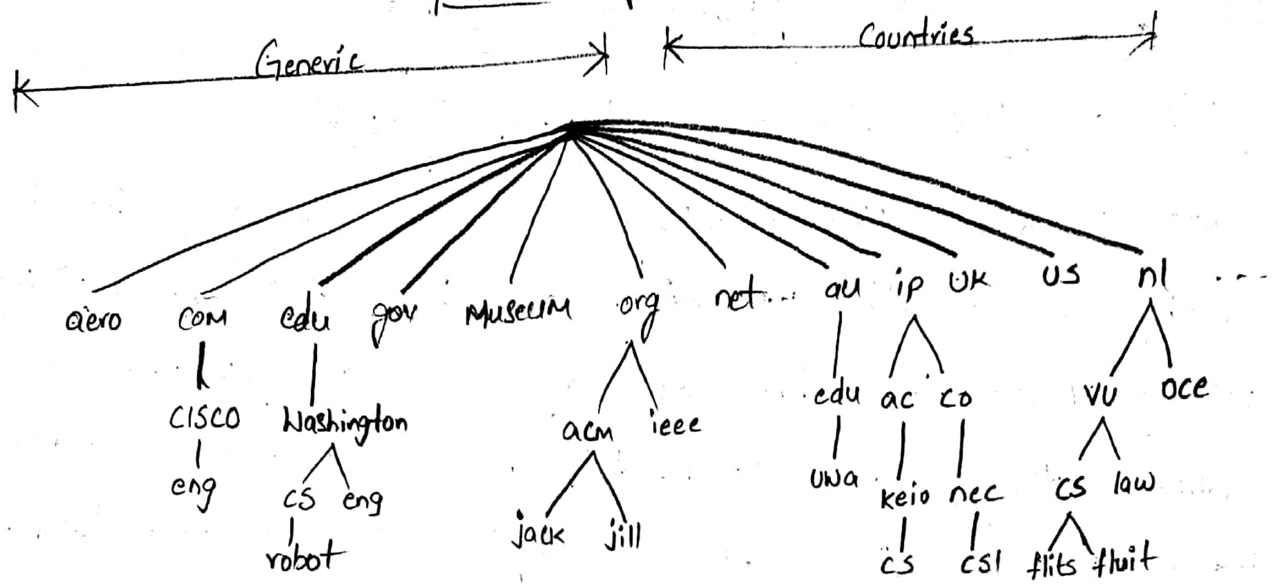
The Application Layer

DNS - The Domain Name System:

- DNS handles the naming system within the internet.
- Webpages, mailboxes etc can be referred by using N/w IP addresses of the computers on which they are stored, but these addresses are hard for the people to remember.
- If we are browsing a company's web pages from 128.111.24.41, but if the company moves the web server to a different ~~company~~ ~~moves~~ machine with a different IP address, everyone needs to be told the new IP address.
- Hence, a web server might be known as www.gmail.com regardless of its IP address.
- Since N/w can understand only numerical addresses, some mechanism is required to convert the names to N/w addresses.
- Such a mechanism is DNS.
- It is used for mapping host names to IP addresses.
- To map a name onto an IP address, an application program called a library procedure called the resolver.

DNS Name Space :

A portion of Internet domain Name Space



- For the internet, the top of the naming hierarchy is managed by an organization called ICANN (Internet Corporation for Assigned Names & Numbers).
- Internet is divided into 250 top-level domains.
- Each domain is partitioned into subdomains & these are further partitioned & so on.
- All these domains can be represented by a tree as shown in the above diagram.
- The top-level domains are divided into two categories : generic and countries.
- The generic domain include original domains The country domains include one entry for every country.

- The top-level domains are run by ~~registers~~ registrars appointed by ICANN.
- If the top-level domain name is required, we should go to the corresponding registrar to check if the desired name is available & not used by somebody else.
- If there are no problems, the requester pays the registrar a small annual fee and gets the name.

Domain	Intended Use	Start date	Restricted?
com	commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International Organizations	1988	Yes
mil	military	1985	Yes
net	Network providers	1985	No
org	Non-Profit organizations	1985	No
coop	Cooperatives	2001	Yes
Info	Informational	2002	No
pro	Professionals	2002	Yes
Jobs	Employment	2005	Yes

mobi	Mobile devices	2005	Yes
tel	Contact details	2005	Yes
travel	Travel Industry	2005	Yes

- Each domain is named by its path (www. google.com)
- The components are separated by "dot".
- Domain names are case-insensitive, so edu, Edu, EDU mean the samething.
- Each component name can be upto 63 characters long & full path names must not exceed 255 characters.
- To create a new domain, permission is required of the domain in which it will be included.
- Eg :- If a university jntuk needs to start a website under the domain edu, it must ask the manager of the edu domain to assign it ~~for~~ jntuk.edu.
- In this way, name conflicts are avoided & each domain can keep track of all its sub-domains.

Domain Resource Records :

- Every domain whethere it is a single host or top-level domain, can have a set of resource records.
- For a top-level domain, these records are DNS database.
- For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist.
- When a resolver gives a domain name to DNS, it gets the resource records associated with that name.
- the function of DNS is to map domain names onto resource records.
- The format of resource record is :-

Domain_name Time_to_live Class Type Value.

- Domain_name : It tells the domain to which the record applies.
- Time_to_live : This field gives an indication of how stable the record is. When information is highly stable, it is assigned a large value,

Such as 86,400 (no of sec in 1 day). When information is highly volatile, it is assigned a small value, such as 60 (1 minute).

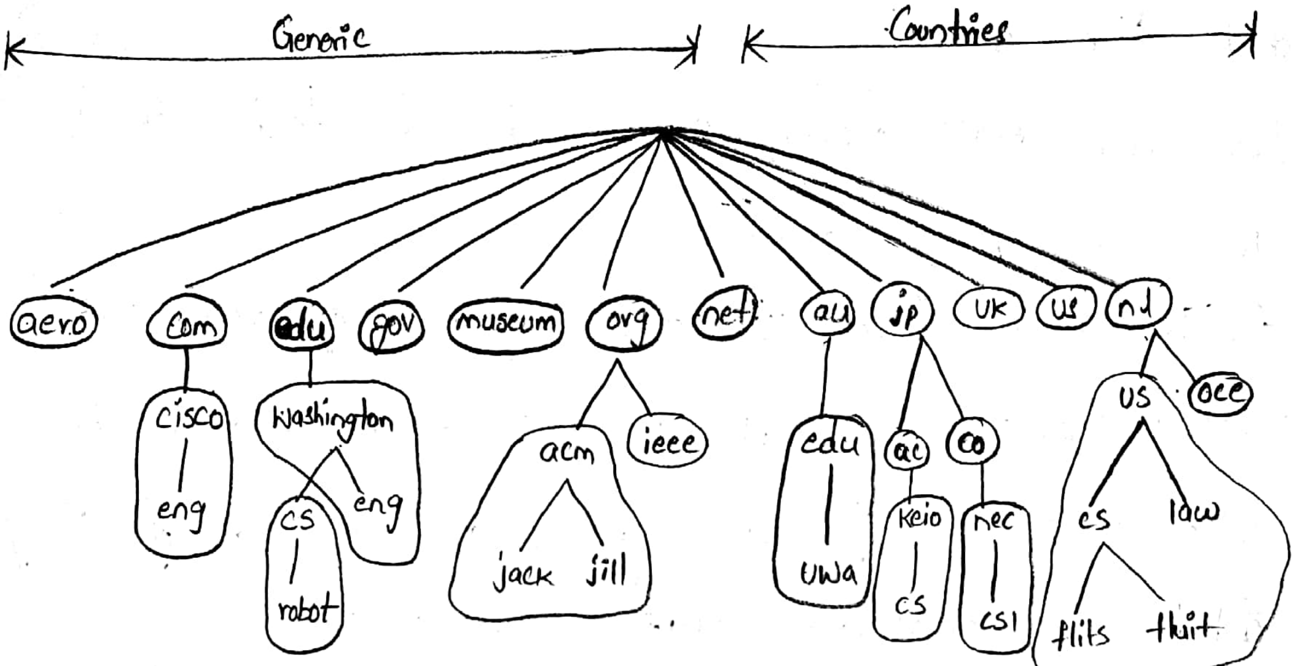
- Class : For Internet information, it is always IN.
- Type:- It tells the kind of the record.

There are many kinds of DNS records. They are:-

Type	Meaning	Value
SOA	Start of authority	parameters for the zone
A	IPV4 add of a host	32-bit Integer
AAAA	IPV6 add of a host	128-bit Integers
MX	Mail Exchange	willing to accept mail.
NS	Name Server	name of the server for the domain
CNAME	Canonical name	alias domain name
PTR	Pointer	pointer to 6IP add
SPF	Sender Policy Framework	Text encoding of mail sending policy.
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text.

DNS resource record types

Name Servers :

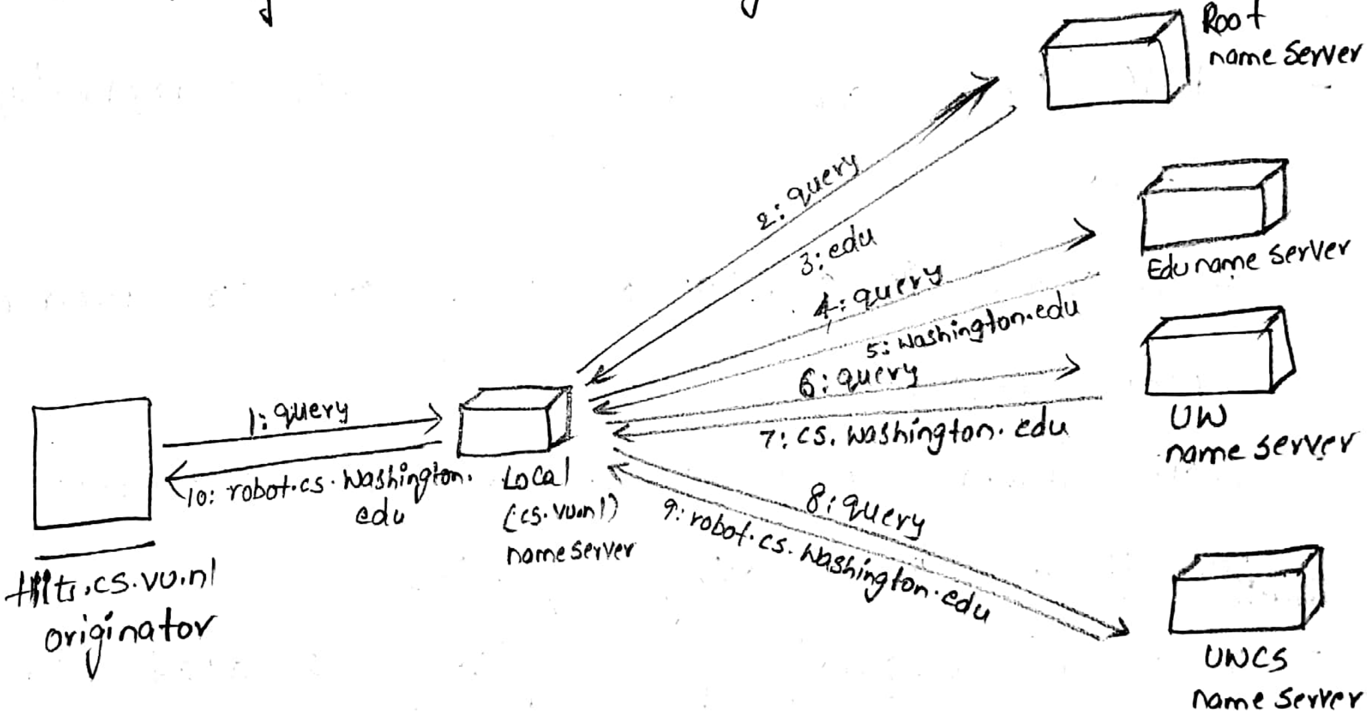


Part of DNS name space divided into zones

- DNS Name space is divided into non overlapping zones.
- Each zone is associated with one or more name servers.
- Name Server is a server on the Internet specialized in handling queries.
- When we request for anything related to domain name, it forwards it to one of the name servers
- In response, the DNS Server sends back the IP add
- If a single name server is used for the entire

DNS db, it is very difficult to respond for all the queries.

- So, the DNS name space is divided into non overlapping zones.
- Each zone contains some part of the tree.
- Every zone consists of its own name server.
- the process of looking up a name & finding an add is called name resolution.
- Consider that flits.cs.vu.nl wants to find the IP address of robot.cs.washington.edu.



Example of resolver looking up a remote name in 10 steps.

step1 :- Query is sent to the local name server.

step2 :- local name server forwards the query to the root name server. these name servers have information about each top-level domain. It returns the IP add of edu domain. which cs.washington.edu is located.

step 3 :- local name server forwards the query to edu name server. It returns the IP add of UW name server.

Step 4 :- Now the local name server forwards the query to UW name server. It returns the IP add of UWCS name server.

step 5 :- local name server forwards the query to UWCS name server. It returns the final answer, which the local name server forwards as a response to flits.cs.vu.nl.

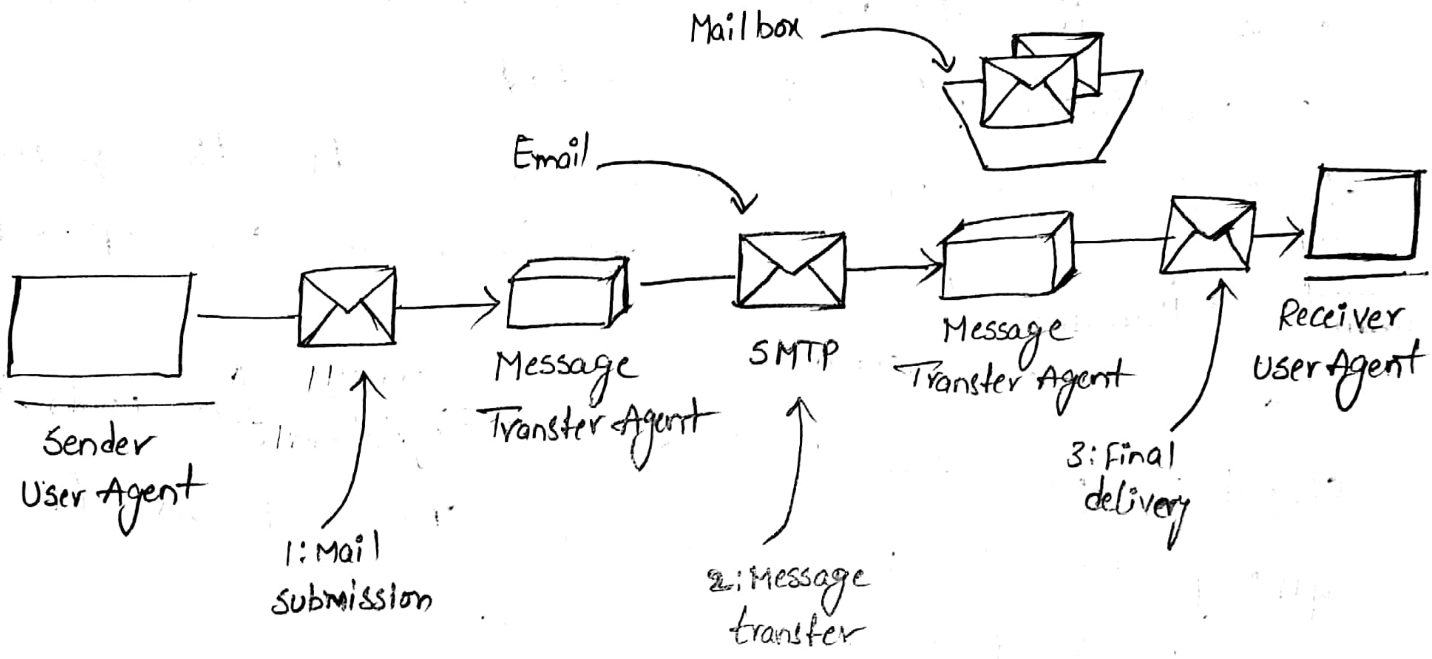
Hence the name has been resolved.

Electronic Mail.

- The architecture of email system consist of two kinds of subsystems : the User Agent
  the Message Transfer Agent.

User Agent :- It allows people to read & send email

Message transfer Agents : It moves the messages from source to destination. They run in the background on mail server machines.



Architecture of email system

ⓐ Mail Submission : The user agent is a program that provides an interface that allows the users to interact with the email system.

- Here the user can compose messages, replies to messages & organize messages.
- The act of sending new messages into the mail system for delivery is called mail submission.

(b) · Message Transfer : The message transfer agent at the sender side forwards the email to the message transfer agent at the receiver side by using SMTP (Simple Mail Transfer Protocol). This is the message Transfer step.

(c) Final delivery : At the receiver side, the user agent and the message transfer agent are linked using mailboxes. They store email that is received for a user. They are maintained. by mail servers.

- The retrieval of mail from the mailboxes is the final delivery.

Email message format.

- It consists of two parts envelope and message.

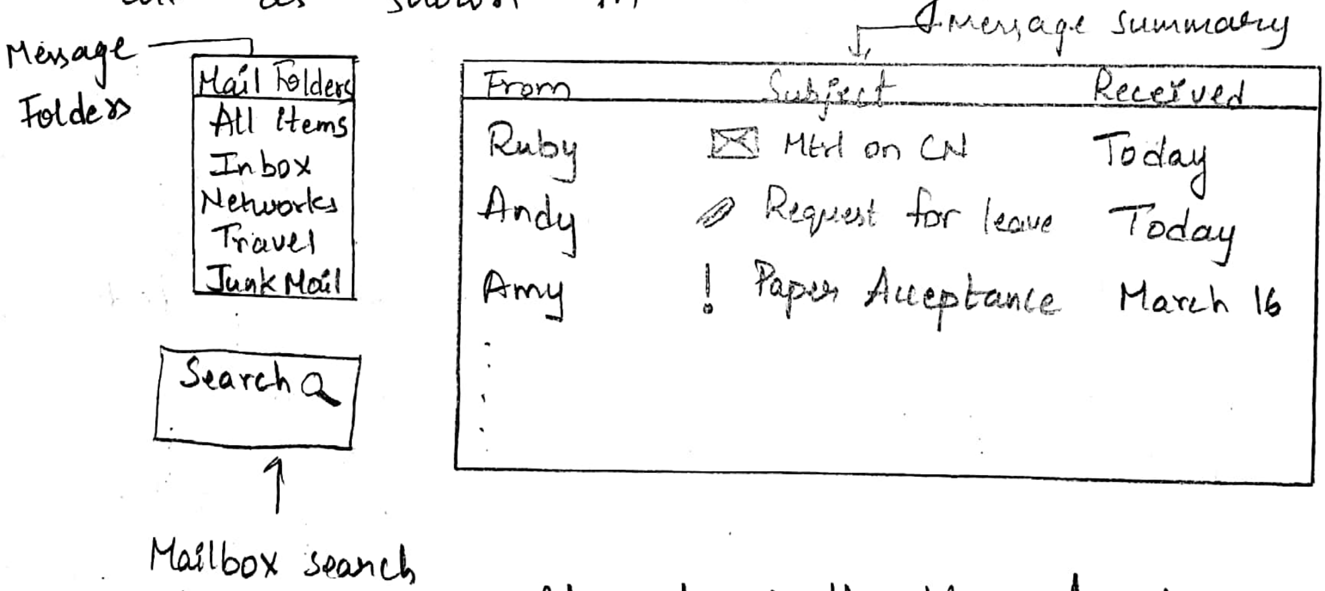
(a) envelope : It contains all the information needed for ~~transfo~~ transporting the message such as destination address, priority and security level.

(b) Message : It consist of two separate parts: the header and the body.

- header : It contains the control information for user agent.
- ~~Message~~ body :- It contains the original message for the receiver.

The User Agent :

- A user agent is a program that accepts a Variety of commands for composing, receiving & replying to messages.
- There are many popular user agents including Google gmail, Mozilla Thunderbird & Apple Mail.
- Most user agents have a menu or icon-driven graphical interface that requires a mouse or a touch interface on Smaller mobile devices.
- The typical elements of a user agent interface are as shown in the diagram.



From	Subject	Received
Ruby	✉ Mtrl on CN	Today
Andy	Request for leave	Today
Amy	! Paper Acceptance	March 16

Elements of the User Agent Interface

- When a user agent is started, it will usually present a summary of the messages in the user's mailbox.
- The user agent present the summary as follows:

- it uses From, Subject and Received fields to display who sent the message, what it is about and when it was received.
- People who fail to include a subject field often discover that responses to their emails tend not to get the highest priority.
- The icons present near the subject might indicate unread mail (the envelope), attached mtrl (the paperclip) & important mail (the exclamation point)
- Many sorting orders are possible. The most common is to order messages based on the time that they were received, most recent displayed first
- User agents provide a short preview of a message, to help users decide when to read further.
- After a message has been read, the user can decide what to do with it. This is called message disposition.
- It includes deleting the message, sending a reply, forwarding the message to another user & keeping the message for later reference.

Message Formats:

RFC 5322 - The Internet Message Format:

Header	Meaning
To:	Email address of primary recipient
Cc:	Email address of Secondary recipient
Bcc:	Email address for Blind carbon copies
From:	Person or ~~A~~ people who created the message
Sender:	Email address of the actual sender.
Received:	Line added by each transfer agent

- **To:** Email add of primary recipient.
- **Cc:** Email add of secondary recipient
  Cc stands for Carbon Copy
  - Email addresses listed here will receive a copy of email that ~~ae~~ we sent to the people listed in the To: field.
  - Everyone listed under the Cc field will see everyone's email addresses that are under the To and Cc field.
- **Bcc:** Bcc stands for Blind Carbon Copy.
  - Email addresses listed here will receive a copy of email that you sent to the people listed in the To: field.

- Everyone listed under the Cc field will see everyone's email address that are listed under the To & Cc field but will not see the addresses listed in Bcc field.
- Each person listed on the Bcc field will not see the email address of other recipients.

- From : It tells who wrote the message.
- Sender :- It tells who sent the message
- Received : It is added by each message transfer agent. It contains the agent's identity, the date & time message was received & other information that can be used for debugging the routing system.
- Return-path : It is added by the final message transfer agent and was intended to tell how to get back to the sender.

In addition to the fields mentioned above, RFC 5322 messages also contain a variety of header fields used by the user agents or human recipients. The most common ones are listed below.

Header	Meaning
Date :	the date & time the message was sent
Reply-To :	Email add to which replies should be sent.
Message-Id :	Unique number for referencing the msg later
In-Reply-To :	Message-Id of the message which this is a reply.
References :	Other relevant message-Ids.
keywords :	User chosen keywords.
Subject :	Short summary of the message for the one-line display

MIME (Multipurpose Internet Mail Extensions)

Header	Meaning
MIME-Version	Identifies the MIME Version.
Content-Description	Human-readable string telling what is in the message.
Content-Id	Unique Identifier
Content-Transfer encoding	How the body is wrapped for transmission.
Content-Type	Type & format of the content.

- MIME Version : It tells the user agent that the received message is a MIME message & which version of MIME it is using.

- Content - Description : It briefly tells what is in the message so that the receiver can decide whether to read the message or not.
- Content - Id : It is used to identify the content. It is a unique number for referencing this message later.
- Content - Transfer - encoding :- It tells how the body is wrapped for transmission through the N/w.
- Content - type : It specifies the nature of the message body. the content type should be mentioned so that the browser will know how to present it.

MIME Content types

Type	Example subtypes	Description
text	plain, html, xml, css	Text in various formats
image	gif, jpeg.	pictures
audio	basic, mpeg, mp4	Sounds
video	mpeg, mp4.	Movies
model	vrml	3D model
application	pdf, js, zip	Data produced by application.
message	http	Encapsulated message
multipart	mixed, alternative, parallel.	Combination of multiple types

Message Transfer :-

SMTP and Extensions :-

- SMTP is a simple ASCII protocol. Using ASCII text makes protocols easy to develop, test & debug.
- Email is delivered by establishing a TCP connection with port number : 25 b/w the sending machine and receiving machine.
- After establishing the TCP connection to port 25, the sending machine operates as client & the receiving machine operates as server.
- Before sending email, the client announces whom the email is coming from & whom it is going to
- If such a recipient exists at the destination, the server gives the client the go-ahead to send the message.
- Then the client sends the message & the server acknowledges it.
- No checksums are needed bcz TCP provide a reliable connection.
- When all the email has been exchanged in both directions, the connection is released.

Disadv of SMTP :

- It doesn't include authentication.

- DNS contains multiple types of records including the MX or mail exchanger record.
- So, a DNS query is sent to get the MX records of the receiver domain.
- This query returns an ordered list of IP addresses of one or more mail server.

Final Delivery:

IMAP (Internet Message Access Protocol).

- One of the main protocols that is used for final delivery is IMAP.
- To use IMAP, the mail servers runs on IMAP server that listens to port 143.
- The user agent runs on IMAP client.
- the client connects to the server & begins to issue commands.
- the client will start a secure transport inorder to keep the messages & commands confidential.
- To have a secure transport, authentication is performed (login).
- Once logged in, different commands are used to

- It doesn't include Encryption.
- To overcome the problems, SMTP was revised to have an extension mechanism.
- The use of SMTP with extensions is called ESMTP (Extended SMTP).

Some SMTP Extensions

Header	Description
AUTH	Client authentication
BINARYMIME	Server accepts binary messages
CHUNKING	Servers accepts large messages in chunks
SIZE	Check message size before trying to send.

Message Transfer :

- Once the sending mail transfer agent receives a message from the user agent, it will deliver it to the receiving mail transfer agent using SMTP.
- To do this, the sender uses the destination address.
- The Message transfer agents runs on the mail server machines.
- So, we should determine the correct mail server to contact, for this purpose DNS is used.

deal with the messages - They are:-

Command	Description
CAPABILITY	List Server Capabilities
LOGIN	Logon to server
AUTHENTICATE	Logon with other method
SELECT	select a folder
EXAMINE	Select a read-only folder
CREATE	Create a folder
DELETE	Delete a folder
RENAME	Rename a folder
LIST	List the available folders
STATUS	Get the status of folder
APPEND	Add a message to a folder
FETCH	Get messages from a folder
SEARCH	Find messages in a folder
COPY	Make a copy of message in a folder.
SUBSCRIBE	Add folder to active set
UNSUBSCRIBE	Remove folder from active set
LSUB	List the active folders
LOGOUT	Logout & close connections