Networking

A computer network consist of two or more electronic devices/communication devices that are linked in ordered to share resources, exchange files and allow electronic communication.

The computer on a network may be linked through cabels, telephone lines, radio waves, satellite or infrared light beams.

The transparency of the communication link is brought about by interfacing software known as protocol. which enables a user in one location to freely access a computer system in another location.

Advantages of Network-

(i) The computers on one network can share hardware devices like printer, scanner etc.

(ii) Data and software can be shared within a computer on a network.

(iii) Files can be transferred from one computer to another

Disadvantages of Network-

(i) Data and information are prone to be stolen by the computer hackers.

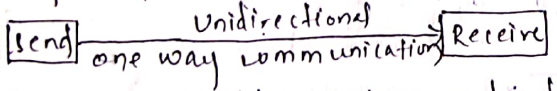
(ii) A computer network can be affected by network worm virus.

(iii) Computers depend on a servers, if the server has any defect none of the system will function.

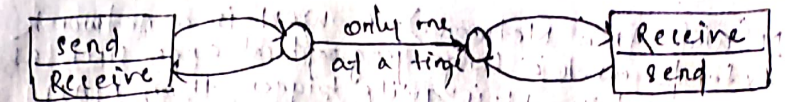
Mode of Data Transmission-

Transmission mode means transferring of data between two devices. It is also known as communication mode. There are three types of transmission mode-

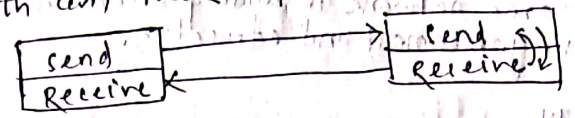
(i) Simplex Mode - In this mode, the communication is unidirectional. We cannot send a message back to the sender. For example, loudspeaker, television, and remote keyboard and monitor.



(ii) Half-Duplex Mode - In this mode data can be sent in both direction but one at a time, that is when the sender is sending the data then at that time we cannot send the sender our message. For example, walkie-talkie,



(iii) Full Duplex Mode - In this mode the data can be sent in both direction simultaneously. Telephone network is the best example of it, which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



Types of Network

A computer network is a group of computers linked each other that enable the computers to share their resources, data and application. A computer network categorized by their size and area. Computer networks are of four types:-

(i) PAN (Personal Area Network) - PAN is a computer network that enables communication between computer devices near to a person. PANs are wired such as USB. or they can be wireless such as infrared, bluetooth etc. Wireless PAN includes cellphone handsets, wireless keyboard, wireless mic, printer etc.

(ii) LAN (Local Area Network) - LAN is a group of computers connected to each other in a small area such as building, office etc. LAN is used to connect two or more personal computers through a communication device or medium such as twisted pair, coaxial cable. etc. The data is transferred at an extremely faster in local area network.

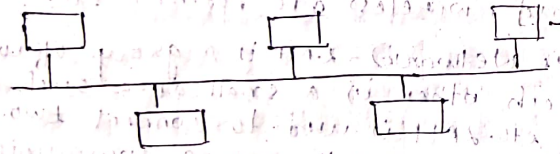
(iii) MAN (Metropolitan Area Network) - A metropolitan area network is a network that covers a large geographical area by interconnecting various LANs. A MAN, various LANs are connected to each other through a telephone line exchange. It has a higher range than LAN.

(iv) WAN (Wide Area Network) - A WAN is a network that extends over a large geographical area such as states or countries. It is quite bigger than MAN. WAN is not limited to a single location, but it is spane over a large geographical area through a telephone line, fibre opticcables or satellite links. The Internet is one of the biggest one in the world. A wide area network is widely used in the field of business, government and education.

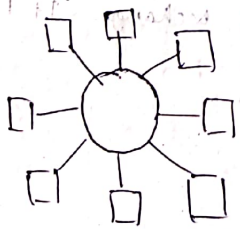
Network Topology

Network Topology is the symmentic description of the network arrangement, connecting various nodes (sender and receiver) through lines of connection. There are various types of network topogy. They are as follows:-

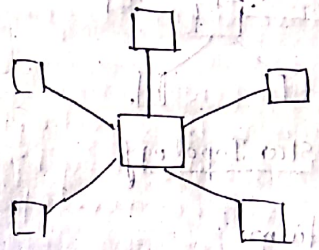
(i) Bus Topology - Bus Topology is a network type in which every computer and network device is connected to single cabel. When it has exactly two end points, then it is called linear bus topology. It is used in small network. It is easy to expand to two cabels together. The disadvantage of bus topology is that if the cabel fails then whole network fail.



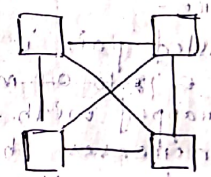
(ii) Ring Topology - It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Data is transferred in a sequential manner that is bit by bit. If someone wants to send some data to the last node in a ring topology with hundred nodes, then the data will have to pass through 99 nodes to reach the hundredth node.



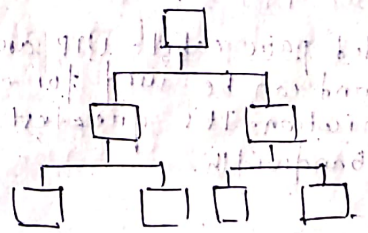
(iii) Star Topology - In this type of topology all the computers are connected to a single hub through a cabel. This hub is central node and all other nodes are connected to a single central node. Every node has its own dedicated connection to the hub. It provide fast performance with few nodes and low network traffic. If the hub fails, then the whole network is stopped because all the nodes depend on the hub.



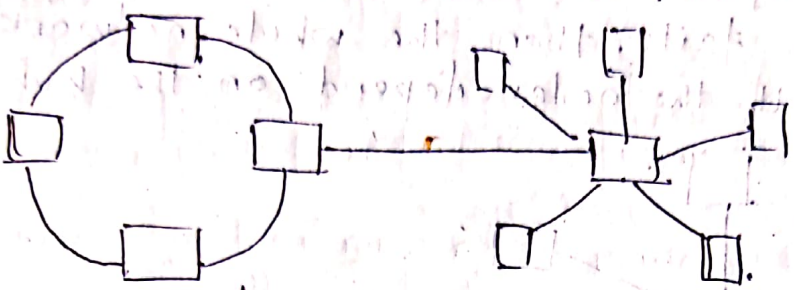
(iv) Mesh Topology - All the network nodes are connected to each other in mesh topogy. Mesh has $n(n-1)/2$ physical channels (cabels) to link 'n' devices. The installation and configuration can be a bit difficult. The cabelling cost is more as compared to other topologies.



(v) Tree Topology - It has a root node and all other nodes are connected to it forming a hierarchy. It is also called as hierarchical topology. It should atleast 3 levels to the hierachy. Error detection is easily done but it can be costly. If more nodes are added then maintenance become difficult.



(VI) Hybrid Topology - It is a topology which is a mixture of two or more topologies. For example, if in an office, in one department ring topology is used and in another star topology is used, connecting this topologies will result in Hybrid Topology.



Ring Topology

Star Topology

Data Transmission Medium

A transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission media is broadly classified into two typ

(1) Guided Media - It is also known as wired or bounded media. It is defined as the physical medium through which the signal are transmitted. Various types of guided media are -

(a) Twisted pair cabel - A twisted pair is a pair of copper wires, with diameters of ~~0.4 to 0.8 mm~~ 0.4-0.8 mm, twisted together and wrapped with a plastic coating. The twisting increases the electrical noise immunity, and reduces the error rate of the data transmission. This twisting process serves to improve the performance of the medium by containing the electromagnetic field within the pair. In certain applications copper covered still, copper alloy, nickel or gold plated copper, metallic conductors are employed. It can be classified into two types:

(i) Unshielded Twisted pair cabel - UTP are the flexible low cost media and can be used for either voice or data communication. It's greatest disadvantage is the limited bandwidth.

(ii) Shielded Twisted Pair Cabel (STP) - STP differs from UTP in that a metallic shield or screen surrounds the pair. The shield itself is made of aluminium, steel or copper.

(b) Coaxial Cabel - Coaxial cabel contains two conductors parallel to each other. The inner conductor is made up of copper and the outer conductor is made up of coppermesh. The two conductors are separated by insulation. A layer of non conductive material such as PVC or ~~Teflon~~ teflon that protects the entire ~~co~~ cabel. Coaxial cabel includes shield for improve performance and therefore is expensive. Cabel TV networks use coaxial cabel. In general coaxial cabel enables longer distance transmission at higher data rates than twisted pair cabel. but is more expensive.

(c) Optic Fibre Cabel - Optical Fibre cabel is a cabel that uses electrical signal for communication. It carries the transmitted information from a fluctuating beam of light in a glass fibre rather than as an electrical signal on a wire. fibre optic transmission systems are opto-electric in nature. A combination of optical and electrical electromagnetic energy is involved. The signal originates as an electrical signal, which is translated into an optical signal, which is reconverted into an electrical signal at the receiving end. Thin glass fibre is very clear and designed to reflect light internally for efficient transmission. Plastic jacket allows fibre to bend without breaking. Light emitting diode (LED) or Lazers injects light into fibre for transmission. Light sensitive receiver at the other end translates light back into data.

(2) Unguided Media - An unguided transmission media transmits the electromagnetic waves without using any physical media. Therefore, it is also known as wireless transmission. Energy travels through the air rather than copper or glass. Unguided transmission is broadly classified into three types -

(a) Radio waves - Radio waves are the electromagnetic waves that are transmitted in all the direction of free space, they are omnidirectional. The radio waves can travel through walls through an entire building. Depending upon the frequency, they can travel long distance or short distance. Satellite is one of the example of long distance communication. The range is frequency of radiowaves is from ~~30Hz~~ 30Hz to 300GHz. An example of radio wave is ~~fm~~ FM radio (Frequency modulation)

(b) Microwave Transmission - Microwaves are a form of electromagnetic radiation with wavelength ranging from about 300 MHz to 300GHz. They have shorter wavelength compare to radio waves. Microwaves are unidirectional as the sending and receiving antenna is to aligned. i.e. the waves send by the sending antenna are narrowly focused. There are several frequency ranges assign to microwave system. All of which are in the Gigahertz. They are used in radar, communication and for heating in microwave ovens.

(c) Infrared Transmission - An infrared transmission is a wireless technology used for communication over short ranges such as data transfer b/n two cell phones, TV remote operation etc. The frequency of the infrared in the range from 300GHz to 400THz

NETWORK DEVICES

The devices which are responsible for creating a physical network of computers and other peripheral devices are called as network devices. These are meant to distribute and channelize the electric signals throughout the network. following types of network devices are -

(1) Network Interface Card (NIC) - It is hardware device which connects a computer with the network. They are installed on the motherboard of the computers and are responsible for sending and receiving information from network devices via this card.

(2) Hub - A hub is a network device that connects several nodes to a network. Computers and other devices of a network are connected to the ports of a hub by twisted pair cabels. Hubs are design to take data from one connected device, transmit them to the other appended/end devices without altering any of the transmitted packets received. There are two types of hubs -

(a) Active Hubs - Active hubs regenerate a signal before forwarding it to all the ports of the device.

(b) Passive Hubs - Passive hubs donot regenerate the signals.

(3) Switch - A switch is an intelligent hub. It has the same function as that of a hub but the difference betn two is in the way they re-transmit the received information. A switch sends the information selectively only to those computers for which it is intended.

(4) Repeater - When the data is transmitted over a network for long distances, the data signal gets weak upto certain distance. If the signal becomes weak it cannot reach its destination. Repeater is such a device which can restrengthen the data signal before it gets too weak. Repeater regenerate the received signal and retransmits it to its destination.

5) Bridge - Bridges are networking devices that connect networks. Sometimes it is necessary to divide networks into sub-nets to reduce the amount of traffic on a network.

6) Routers - A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a network layered device. When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined it searches in its routing cabel to get know how to reach the destination and then forwards the packet.

4) Gateway - It is a passage to connect two networks together that may work upon different networking model. The term gateway is applied to any device, system or software application that can perform the function of translating data from one format to another. It understands the address architecture used in different networks and translate between these addresses architecture.

TRANSMISSION IMPAIRMENTS

Impairments cause various modifications that degrade the signal quality. A binary 1 may be changed into binary 0 and vice-versa due to bit error. There exist three causes of impairment, they are :-

(1) Attenuation - When signal amplitude degrades along a transmission medium this is called signal attenuation. Attenuation is the loss of signal power of signal while traversing a transmission media including electronic circuitry and is measured in terms of decible (db). The signal degrades so much that it becomes difficult to obtain the original signal. The electronic circuitry also tends to take away some of the signal power in the form of heating of the copper, metal etc. The attenuation includes a number of factors like transmitting and receiving antennas, transmitter powers, modulation techniques, atmospheric conditions etc.

(2) Distortion - Distortion is the change in shape or form of a signal, when a signal travels through a electronic circuitry and transmission media. A signal produces harmonic frequency as when it passes through non-linear electronic circuitry and it becomes composite signal. The signal will include some harmonic distortion or unwanted frequencies. A signal to distort and change its original shape while paring over a transmission media.

(3) Channel Noise - It is a small amount of background interference in the channel or unwanted electromagnetic energy. This unwanted electromagnetic energy is referred as noise. The information and data is nothing but signal in electromagnetic form. Hence, noise degrades the quality of information and data. The noise may be classified as external or internal noise based upon the sources. Noise generated inside channel or receivers is known as internal noise. External noise is generally picked up from electrical appliances, atmosphere and even outer space.

ANALOG AND DIGITAL DATA AND SIGNALS

Data communication and networks deal with data or information transmission. Data can be represented in many ways such as human voice, a group of numbers, images, texts and sound etc. There are two ways to communicate, display, store or manipulate ~~informa~~ information. They are referred to as analog and digital.

Analog - Analog is based explained by the transmission of signal such as sound or human speech, over an electrified copper wire. Analogous variations in electrical or radiowaves are created in order to transmit the analog information signal for video or audio over a network, from a transmitter to a receiver. At the receiving end an approximation (analog) of the original information is presented. A voice grade channel is approximately 4000 Hz (4 KHz). Approximately 3.3 KHz used for the voice signal itself. The remaining bandwidth is used for the purpose of network signalling and control in order to maintain separation between information channels.
A cabel television video channel is approximately 6 MHz. Approximately 4.5 MHz is used for information transmission while the balance is used to separate the various adjacent channels using the common analog coaxial cabel system.

Digital - Computers are digital in nature. Computers process store and communicate information in binary form i.e. in the combination of 1s & 0s.

ISO-OSI Reference Model

The open system interconnection or OSI model was developed by the international organisation for standardisation. ISO develop the OSI Model to help data transfer between network nodes. OSI is a set of guidelines for application developers to create and implement applications for computer networks.

The seven layers of OSI Model are categorized into two level grouping. The physical, datalink, network and transport layers, which are the lower layers of the OSI Model deal with the formatting, encoding and transmission of data over the network. The higher layers of the model - session, presentation and application layers deal with user interface and implement the applications that run over the network, knowing how data is delivered from one place to another.

(1) Physical Layer - Layer 1 of the OSI Model is a physical layer in which the frames are converted into series of bits so that they may be transmitted across a transmission media to the destination. The physical layer specifies the representation of the bits as a voltage, current and phase or frequency. It basically uses four types of bit signalling approaches. The series of bits are resembled at the receiving end which are RZ (Return to zero) by using pulse signaling, NRZ (Non-Return to Zero). The physical layer functions are

(a) Describing hardware specification - It includes specifications of cabels, connectors, radio transmitter, NIC etc.

(b) Encoding and signaling - It supports various encoding and signalling functions to convert data from bitstream to frame and vice versa. to send over the network.

(c) Data Transmission Mode - It is responsible for transmitting and receiving data over the physical media.

(2) Data link layer (DLL) - The datalink layer is the second layer of OSI model and it provides functional means to exchange data between network entities. The DLL is also known as the link layer because it provides link to many wireless and wired Local Area Network (LAN) technologies. The DLL is conceptually sub-divided into logical link control and medium access control. The key functions of DLL are:-

(a) Logical Link Control (LLC) - This layer deals with the function that enables control and establishment of logical links between local devices on a computer network.

(b) Error detection and handling - The data link layer also deals with error that occur at the lower levels of the network stack. A cyclic redundancy check (CRC) is used to allow the host receiving data to detect if it was received correctly.

(c) Media Access Control (MAC) - It's role is to control and manage the medium to avoid conflicts because the design of a computer network is based on the shared medium that may be composed of a single network cable or series of cable that is connected to a single medium. Here we use CSMA for ethernet and token passing for the token ring network.

(d) Physical Addressing - Each device on a network is provided with a unique no. called MAC address, which is used by the data link layer protocol to ensure that the data intended for a specific machine.

(e) Data Framing - Messages of higher layer are encapsulated at this layer into frames so that they may be send across the network at the physical layer.

(3) Network Layer - The network layer is the first layer in the OSI model that deals with the actual obtaining of data from the computers. While the data link layer is only concerned with devices that are situated on the same network local to each other. The key functions of the network layer are as follows:

(a) Logical Addressing - The devices communicating across a network have logical addresses which are known as Layer-3 addresses. Internet Protocol (IP) is an example of Layer-3 addressing Data link addressing that deals with only local physical devices; the logical addresses at layer-3 are independent of particular hardware and unique across an entire inter-network.

(b) Routing - It is the key function of layer-3 in which data is routed across interconnected networks to deliver finally at the host destination. It's function at the network layer is to handle incoming packets from various sources and determine routes for their final destination.

(c) Datagram Encapsulation - The network layer function to encapsulate messages received from higher layers by placing them into datagrams with a network layer header. The datagram are also referred to as packets.

(d) Fragmentation and reassembling - The network layer passes down messages to the data link layer for transmission through the physical layer over the transmission media to the other networks on the local networks. The network layers also splits large packets into smaller packets according to the limits imposed on the length of the packet by the data link layer. This process is known as fragmentation. The main role of the network layer is to accept packets from a source and deliver them to a destination machine.

(4) Transport Layer - The basic role of the transport layer is to transport data but it involves high level functions as compared to the same functions delivered by the lower layers. The layers 1, 2 and 3 primarily deal with packaging, addressing, routing and delivery of data and the layer 4 acts as an interface between the application at the higher layers. Some important functions of transport layer are -

(a) Process level Addressing (End to End) - The transport layer is also deals with the addressing issue but quite differently in which it is used to differentiate between software programs and different application

(b) Multiplexing and Demultiplexing - It enables a sending device to multiplex the data received from many application program for transport and demultiplex the data receive while acting as the receiving site.

(c) Segmentation, Packaging and Reassembly - The transport layer segments the large amounts of data (series of bits) into smaller pieces on the source machine to transmit it across the network, and then reassemble them on the destination machine.

(d) Connection establishment, management and termination - The connection oriented protocols at the transport layer establishes a connection, maintain it as data sent over it and then terminate the connection when it is no longer required for the series of communication.

(e) Flow Control - This function manages the mismatch in speed between the sender and the receiver end.

(5) Session Layer - The session layer is the lowest layer of the upper three layers and deals mainly with software application issue. A session is a logical linking of two software application processes to exchange data over a specified period of time. The session layer is responsible for establishing, maintaining the dialogues between communicating applications. for ex - remote logging, remote file transfer etc. It is also responsible for orderly recovery from failures by implementing appropriate check-pointing mechanism. The primary task of session layer protocols is to provide the necessary ways to establish, manage and terminate session.

(6) Presentation Layer - It is responsible for any issues that may arise where data send from one system needs to be viewed in a different way by the other system. The presentation layer performs functions related to the syntax and semantics of the information transmitted. Some of the specific functions of presentation layer are -

(a) Translation (Code conversion) - It is the responsibility of the presentation layer to hide this differences between different machines for a seamless and an easy exchange of data between two host working on different machines.

(b) Compression and Decompression - compression and decompression are also carried out at presentation layer. To improve the throughput of data. however this functions are optional.

(c) Encryption / Decryption - Some types of encryption and decryption are performed at the presentation layer, to ensure the security of the ~~layer~~ data as it passes down the protocol stack. These are also optional.

ASCII - American Standard Code for Information Interchange
EBCDIC - Extended Binary Coded Decimal Interchange Code

(4) Application Layer - The application layer provides support services for user and application task which are programs that actually implement the functions performed by users to accomplish various task over the network. It allows the user to use the network. The application layers provides user interface to communicate with the computer. The application layer provides a variety of protocols that are commonly needed. Some of the most popular application layer protocols are -

Protocol	Port No.	TCP/UDP
Echo	7	TCP/UDP
FTP (File Transfer Protocol)	20/21	TCP
Secure Shell	22	TCP
Telnet	23	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Control Protocol)	67/68	UDP
SMTP (Simple Mail Transfer Protocol)	25	TCP
HTTP	80	TCP
POP	110	TCP
NTP (Network Time Protocol)	123	UDP
HTTPS	443	TCP
RIP (Routing Information Protocol)	520	UDP

Difference bet^n TCP and UDP

TCP	UDP
⇒ Connection oriented	Connection less
⇒ Reliable	Less Reliable
⇒ Error control	Error control is optional.
⇒ Slow Transmission	Fast Transmission
⇒ Overhead	Less overhead
⇒ Flow control, congestion control	No flow control, no congestion control

Internet Protocol stack

A protocol is a set of rules that govern how system communicate. A set of protocols used in the communication network can be termed as a protocol stack. A protocol stack is an arranged chain command of software layer beginning from the application layer from where the data is sent to the position where sending bits of information on the wire at the lowest level which is datalink layer.

TCP/IP - This internet protocol suit commonly known as Transmission control Protocol and Internet Protocol. The TCP layer handles the message path. The message is broken down into smaller units called packets or datagrams which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver end and reassembled into the original message.

The main purpose and the task of IP is delivery of datagrams from the source host to the destination host, based on their addresses.

PPP (Point to Point Protocol) - A host to network or router to router link is provided by the PPP which also includes a security mechanism. Where linking through standard telephone lines by using modem on both end is concern.

FTP (File Transfer Protocol) - This facilitates transfer of text and dual files with the help of a TCP connection. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server.

Telnet - It is a networking protocol and software program used to access remote computer and terminals over the network. TELNET enables the local host to log on to distant host and utilize their resources.

SMTP - The basic function of SMTP is to send email messages from a nearby host to a distant server with the help of a TCP connection. SMTP permits two programs for exchanging mails through the network.

HTTP (Hypertext Transfer Protocol) - This protocol sends hypertext pages (web pages) with the help of the World Wide Web. HTTP is a server and client communication protocol, which is primarily set of rules for formatting and transferring web page data over the WWW.

UDP (User Datagram Protocol) - The basic purpose of the simple protocol, is to send and receive datagram (groups of data are called datagram) to a distant system. UDP is not a dependable protocol and there is always a risk of the change in order of the datagram that are sent through it when receive.

SS7 (Signalling System 7) - SS7 is a protocol designed for public switched telephone system for providing services and setting of calls. The various value added features such as providing intelligence to PSTN services. PSTN services come under the service of SS7. Etc is

Functions of SS7 -

(a) It controls the network. The SS7 network set-up and tears down the call.

(b) It handles all the routing decisions and supports all telephony services including call forwarding, caller ID, remote network management and local number proportability (LNP).

P7

Rate of Data Transmission

Channel - A channel may be defined as a path between transmitter and receiver. This path may be physical or logical in nature. The path provides a message through the passage for the information of data from transmitter to receiver.

Bandwidth - Bandwidth determines how fast data flows on a given transmission path. Bandwidth is expressed as dataspeed in bits per second (bits) in digital system. In analog system bandwidth is expressed as a difference between higher frequency and lower frequency.

Channel Bandwidth - Channel Bandwidth may be simply defined as the size of the range of frequencies that can be transmitted through a channel. It may defined as the volume of information per unit time that a computer, person or transmission medium can handle. It is measured in Hertz (Hz).

Throughput - It may be defined as the number of bits, characters or blocks passing through a data communication system over a period of time.

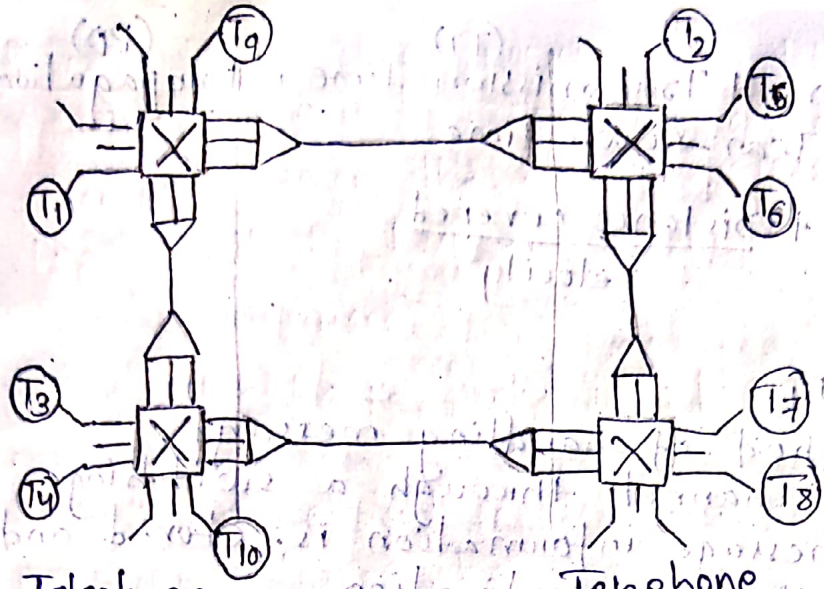
$$\text{Throughput} = \frac{\text{Packet length in bits}}{\text{transmission time + Propagation time}}$$

Bitrate - Bitrate is the number of bits (0 or 1) transmitted during 1 second.

Baudrate / Data Rate - The number of signals changes per unit of time to represent the bits is called the data rate of the modem. That rate is expressed in terms of a unit known as a baud.

CIRCUIT SWITCHING

Circuit switching is the type of communication method in which a dedicated communication path is established between two devices through one or more intermediate switching nodes. Most widely used example of circuit switching is public switched telephone network (PSTN). The major disadvantage of this communication technique lies in it 100% dedicated connection that offers poor efficiency. Circuit switching employs a circuit switching node, which is a full-duplex.



Physical Layer
Contiguous flow
No Header
Efficiency less
Delay less

Switching Techniques

(i) Space Division switching - This kind of switch was specially dereloped for an analog environment. The characteristics of this type of switches are that they require separate physical path for each connection and use metallic or semiconductor gates

(ii) Crossbar Switch - It is a simplest possible space division switch where each packet takes a different path through the switch depending on its destination.

(iii) Time Division Switching - This technique based on multiplexing was dereloped for digital transmission Due to multiplexing all transmitted signals are time multiplexed to be carried by a single transmission path. Circuit switching communication intended routes between two end points are pre-defined so as to enable the originating switch to select the best route for each call.

(iv) Time space Time (TST) Switching - It allows sending messages both on input & output ~~trunks~~ trunks and is therefore more flexible. This feature gives it a lower call blocking probability.

Trunk - Trunks are trans mission medea that handle the communication betn offices. A trunk normally handles hundreds or thousands of connections through multiplexing.

Total Time = setup Time + Transmission Time (TT) + Propagation (PD)
Delay Time + Tear Down Time

$$TT+PD = \frac{\text{Amt of msg}}{\text{Bandwidth}} + \frac{\text{Distance covered}}{\text{velocity}}$$

MESSAGE SWITCHING

It refers to a method of handling message information over a channel through a switching node where the message information is stored and forwarded to reach the destination.
A connection from the source to destination need not to be established.
A message is sent from one switching node to another when the link connecting them establish a connection.
When the link is established, the message is stored and will be forwarded only when the next connection is established for succeeding node.
This process is repeated until it reaches its final goal. For ~~storing~~ storing the data it uses harddisk or RAM.

PACKET SWITCHING

⇒ In this type of data network the source of Data Terminal Equipment (DTE) device, all user date is to be transmitted into one or message units called packets. These packets are of different length and size, and each packet is given an address and the necessary control information.
⇒ In each switching node packets are received, stored and passed on to the next node.
⇒ Every switching node consist of a routing directory. This directory specifies the outgoing link to be used for every network addresses.
⇒ Packet switching categorized into two parts :-
(I) Datagram Switching (II) Virtual Circuit Switching
⇒ ~~Datagram switching~~ Virtual Circuit switching works in datalink layer of OSI model.
⇒ Datagram switching works in network layer of OSI model.

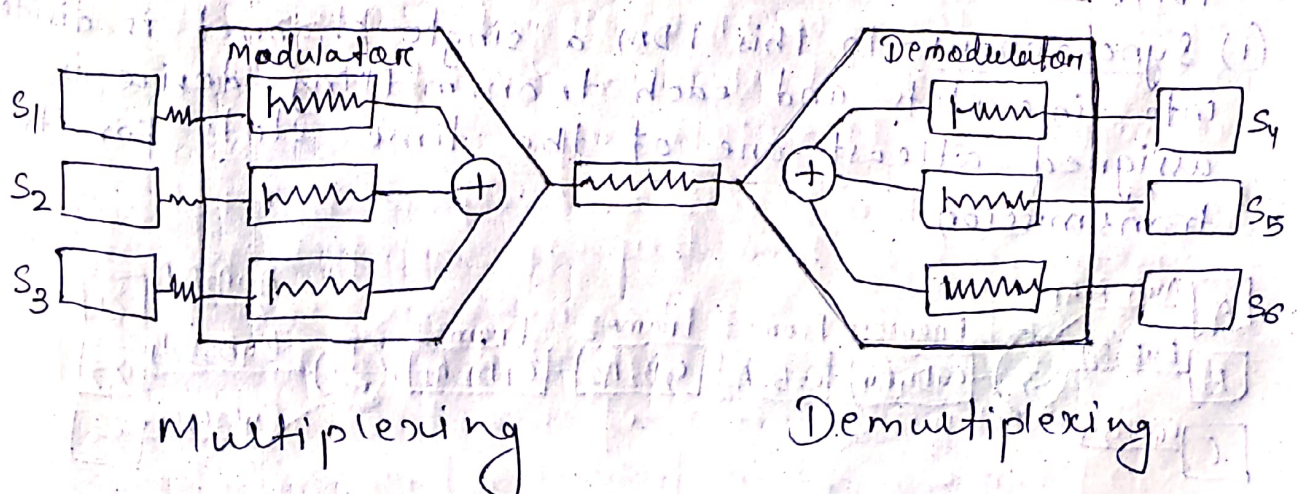
⇒ It follows the strategy of stop and forward.
⇒ It uses pipeline (parallel dataflow method.
⇒ Here the efficiency is high.
⇒ Delay also their as compare to circuit switching.
Total Time = n(TT) + PD

Differentiate between Datagram switching vs Virtual Circuit switching :-

Datagram Switching	Virtual Circuit Switching
⇒ Connection less	Connection oriented
⇒ No reservation	Reservation.
⇒ Out of order	Same order / In order
⇒ High overheader	Less overheader
⇒ High risk of packet loss	Less in packet loss

Multiplexing - Multiplexing is the process where multiple channels are combined for transmission over a common transmission path. Following are the ways to multiplex -

(a) Frequency Division Multiplexing (FDM) - In FDM, multiple channels are combined onto a single aggregate signal for transmission. The channels are separated in the aggregate by their frequency. Between channels there are always some unused frequency spaces which are known as Guard Bans. Today such systems are still in use with analog transmission.



(b) Warelength Division Multiplexing (WDM) - WDM may be defined as the fibre optic transmission technique that employs two or more optical signals having different warelengths to transmit data simultaneously in the same direction over one fibre and is separated by warelength at the distant end later on. WDM allows transmission of analog or digital signals upto a few GHz or GBits per second (Gbit/s)

Transmitter Receiver

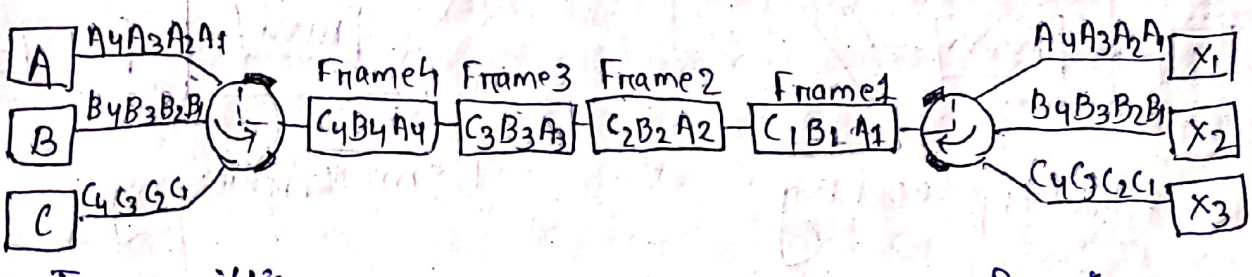
(Warelength Division Multiplexing)

WDM is an analog multiplexing techniques to combine optical signals.

(c) Time Division Multiplexing - There are two alternative technologies of multiplexing for digital sources. These are time division multiplexing (TDM) and Code Division Multiplexing (CDM).

TDM provides a means for merging data ~~for~~ from varied sources into a single channel to support communication over a microware system or telephone lines. TDM can be implemented in two ways, these are synchronous TDM and asynchronous TDM.

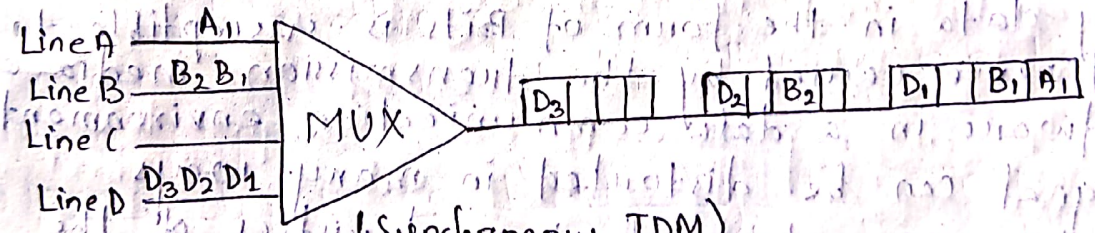
(1) Synchronous - In this TDM a single channel is divided into time slots and each transmitting device is assigned atleast one of the time slots for its transmission.



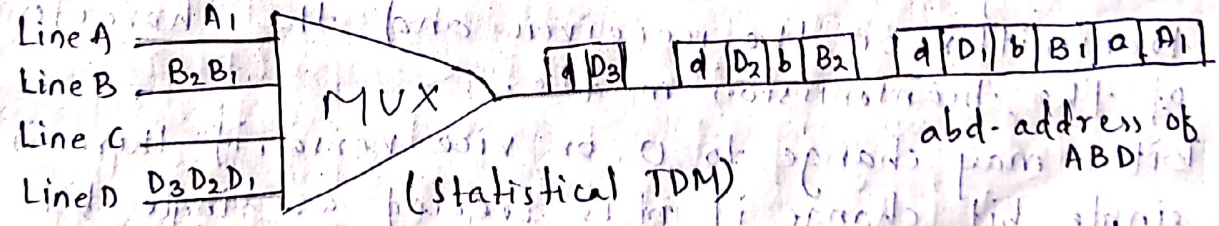
Transmitter Receiver

The same time slot is allocated by the multiplexer to each device at all the times whether the device is active or idle. These different time slots are group into frames. A frame consists of one complete cycle of time slots.

(c) Statistical Time Division Multiplexing (STDM) - Asynchronous TDM is popularly known as Statistical TDM.
In case of TDM, time slots are allocated to channels, even if they have no information to transmit. This is just wastage of the bandwidth. To overcome the inefficiency of standard TDM, a technique known as STDM has been developed, where time is allocated to lines, only when it is required. The intelligent device statistically compensates for normal idle time so that more lines can be connected to a transmission media.



(Synchronous TDM)



(Statistical TDM)

(d) Code Division Multiplexing - CDM is widely used in so called second generation and third generation wireless communication. This is a combination of analog to digital conversion and spread spectrum technology.
CDM may be defined as a form of multiplexing where the transmitter encodes the signal we in a pseudocode pseudo random sequence. On the other hand, the receiver knows about the code generated and transmitted by the transmitter and therefore can decode the received signal.
Code division multiplexing assign each channel its own code to separate them from each other.

The disadvantage of CDM is that each user's transmitted bandwidth is largen than the digital data rate of the source.
The main advantage of CDM is protection from interference and tapping as only the sender and the receiver know the spreading code.

Error Detection and Correction

The memory and network technology are not entirely reliable and are to errors while communicating data.
Data processing and transmission systems experience errors due to several reasons. Some of the reason are due to the physical medium that produces noise, distortion and attenuation.

Types of Errors:-

Binary data in the form of Bits is susceptible to interference caused by the transmission media or hardware in a data communication environment.
A signal can be distorted in many ways including the electrical characteristics of the transmitter or the receiver and the characteristic of the transmission media.
Bit 1 may change to 0 or vice versa, if there is a single bit change it is treated as single bit error while if there are multiple bit change it is known as multiple bit error or burst error.
An example of such situation where in an ASCII code 00010101 for NAK (Negative Acknowledgement) is transmitted, if it is received as 00000101, it will mean ENQ (ENQuiry).

Burst Error- When error occured in multiple consecutive bits then they are called burst error. For example, in computer network, sometime packets are lost or corrected due to a burst error. A typical cause of burst error is interference, obtain from lighting or electrical discharge.

Example - If the bits 101010 transmitted and changes to the bits 111011 is receiving end. Then the total no. of bits changes 2 bits. The total length in bits changes is 5 bit.

Detection - Error detection is the first step towards error correction and is simpler than error correction

Redundancy Method - It is the simplest type of error detection mechanism in which the same data string is transmitted twice.

The receiving device performs a bit by bit mapping of both the received data string to detect whether both the received data strings are same or not.

This system involve quite a lengthy process because bits strings are transmitted twice and bit by bit mapping takes enormous time.

The process of introducing these extra bits is called redundancy.

There are three types of redundancy processes :-

(i) Parity Check - (iii) Cyclic Redundancy Check (CRC)

(ii) Check Sum

They are referred to as Error Detection and correction (EDAC) or Error Checking and Correction (ECC).

* Parity Check - A parity check is the process that ensure accurate data transmission between nodes during communication.

A parity bit is appended to the original data bits to create an even or odd bit number; the number of bits with value 1.

The source then transmits the data via a link, and bits are checked and verified at the destination. Data is considered accurate if the number of bits (even or odd) matches the number of transmitted from the source.

→ m+1 bit (m: no. of bit in message + 1 extra bit)
→ Even ~~or odd~~ parity (no. of '1's should be even)
→ It can detect all single bit errors in code word.
→ Can detect only all the odd no. of error in code word.

4 bits of code word			
0000	0	1000	1
0001	1	1001	0
0010	1	1010	0
0011	0	1011	1
0100	1	1100	0
0101	0	1101	1
0110	0	1110	1
0111	1	1111	0

Hamming code - The bit position in a Hamming code word can be numbered from one through 2^{i-1}. Any position whose number is a power of two is a check bit and the remaining positions are information bits.

Cyclic Redundancy Check - It is a technique that provides a data string to packets of information that can be utilized for error detection.
In the OSI Network Model, CRC is added to a packet frame at the datalink Layer (DLL).
The data integrity of a received packet or frame is checked via a polynomial algorithm and then match with the result that is performed by the sender. It included in a (most often 16 bits) field appended to the frame.
It uses a dividend polynomial, which is initially preset to zero, and the ones and zeroes of the data string become the coefficient of the dividend polynomial.
The receiving station compares the transmitted remainder with its own computed reminder and an equal condition indicates no error occurence.

→ Most widely used and powerful method
→ It can detect all odd errors, single bit & burst error.
→ It can detect errors equal to the maximum degree of polynomial.
→ total bit (m+r)
(m: no. of bits in message + R: Redundant bits)

Ex: x^4+x^3+1 (Divisor) = $1.x^4+1.x^3+0.x^2+0.x^1+x^0.1$ = 11001

```
11001 | 10101010100000 → 0010
        11001
        -----
        011000
         11001
         -----
         00001101 0
             11001
             -----
             0001100 0
                11001
                -----
                00010
```

(5-1) = 4 bit
so add 4 bit

Replace 0000 to 0010

```
11001 | 10101010100010
        11001
        -----
        011000
         11001
         -----
         00001101 0
             11001
             -----
             0001100 1
                11001
                -----
                00000
```

At the receiver end

Checksum - It is a simple type of redundancy check that is used to detect errors in data. While transmitting a data over a network, sometimes very minor errors occur. In this method an algorithm calculates the binary values in a packet of data and stores the result with the data.
When the data is retrieve from memory or receive at the other end of a network, a new checksum is calculated and compared with the existing checksum.

The sender follows the step -

(i) The unit is divided into K section, each of 'n' bits.

(ii) All sections are added using 1's complement to get the sum.

(iii) The sum is complemented and becomes the check sum.

(iv) The checksum is sent with the data.

The receiver subdivides the data unit and adds all the segments and complement the result. The receiver follows the steps -

(i) The data unit is divided into K section, each of 'n' bits.

(ii) All sections are added using 1's complement to get the sum.

(iii) The sum is complemented.

(iv) If the bits in result is 0, the data also accepted otherwise they are rejected.

Example - 10011001 11100010 00100100 10000100
1 2 3 4

K = 4, n = 8

1 - 10011001
2 - 11100010
(1) 01111011
→ 1
01111100
3 - 00100100
10100000
4 - 10000100
(1) 00100100
→ 1
00100101 - sum
1's comp - 11011010 - checksum

Now, this checksum value will be added and send with the actual data.

10011001 11100010 00100100 10000100 11011010
1 2 3 4

1 - 10011001
2 - 11100010

① 01111011
↳ 1

01111100
3 - 00100100

10100000
4 - 10000100

① 00100100
↳ 1

00100101
Check sum - 11011010

11111111
1's comp - 00000000 — Error free

Now, the received data is accepted, there is no error.

Hamming Code Detection and Correction

Positions	7	6	5	4	3	2	1
bits	d_3	d_2	d_1	P_2	d_0	P_1	P_0
	1	0	1	0	0	1	0

$P_2 = d_3 \oplus d_2 \oplus d_1$, $1+0+1 = 0$
$P_1 = d_3 \oplus d_2 \oplus d_0$, $0+0+1 = 1$
$P_0 = d_3 \oplus d_1 \oplus d_0$, $1+1+0 = 0$

Parity Position - $2^n \rightarrow 2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$
1, 2 and 4 positions have parity bits
P_0 = one odd place, P_1 = two places, P_2 = 4 places.

Example of redundancy bits calculation. (XOR operation)

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

$r_1 = 1, 3, 5, 7, 9, 11$
$= 1 \quad 0 \quad 1 \quad 0 \quad 1$
$= 0$

Address r1: 1 0 0 r_8 1 1 0 r_4 1 r_2 r_1 (1)

Address r2: 1 0 0 r_8 1 1 0 r_4 1 r_2 1 (0)

$r_2 = 2, 3, 6, 7, 10, 11$
$= 1 \quad 1 \quad 1 \quad 0 \quad 1 = 0$

Address r_4: 1 0 0 r_8 1 1 0 r_4 1 0 1 (0)

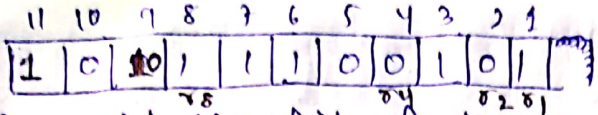
$r_4 = 4, 5, 6, 7$
$= 0 \quad 1 \quad 1 = 0$

Address r_8: 1 0 0 1 1 1 0 0 1 0 1

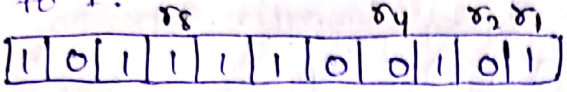
$r_8 = 8, 9, 10, 11$
$= 1 \quad 0 \quad 0 \quad 1 = 1$

Receiver End - 1 0 0 1 (0)
(Parity check by receiver XOR operation)

Ex-



Suppose the bit of the position 9 has been changed to 1.



At the receiving end all the redundant bit should be checked and recalculate.

$r_1 = 1, 3, 5, 7, 9, 11 = 1101111 = 1$

As the even parity is invalid so it refers to 1.

$r_2 = 2, 3, 6, 7, 10, 11 = 0111101 = 0$

As the even parity is valed so it refers to 0.

$r_4 = 4, 5, 6, 7 = 0011 = 0$

$r_8 = 8, 9, 10, 11 = 1101 = 1$

$1 \times 2^0 + 0 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 = 1 + 0 + 0 + 8 = 9$

After converting the binary form into decimal number, we get the position where a data bit is changed.

Then, change the bit of position 9.

Data Link Control

The datalink layer needs to pack into frames. so that each frame is distinguisable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another.

(1) **Framing** - A frame is a digital data transmission unit that includes frame synchronisation i.e., a sequence of bits or symbols making it possible for the receiver to detect the beginning and end of the packet in the stream of symbols of bits.

(2) If a receiver is connected to the system in the middle of the frame transmission, it ignores the data until it detects a new frame synchronisation sequence.

The complete datalink layer messages are called frames.

Typically, framing focuses on the concept how does a receiver know where a message begins and ends. Frames helps to send data (complete message) and not just bits of the message.

Methods of framing -

The four method of framing are widely used as follow

(a) Character Count - This method uses a field filed in the header for specifying the no. of characters in the frame.

When the data link layer at the destination, encounters a character count, it decides the no of characters to be followed, and hence this is the end of the frame.

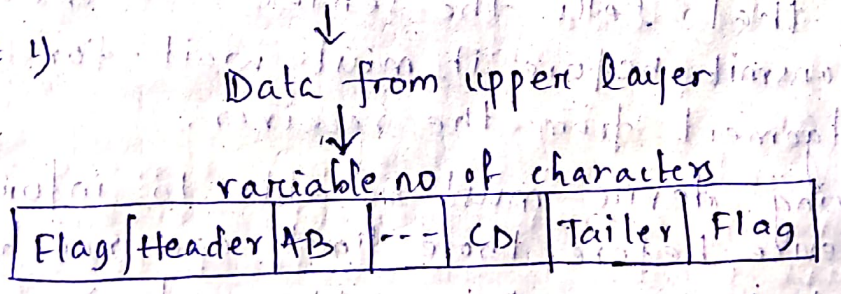
The general format of this method is as follows.

Count | Count characters | Count | Count characters | ...

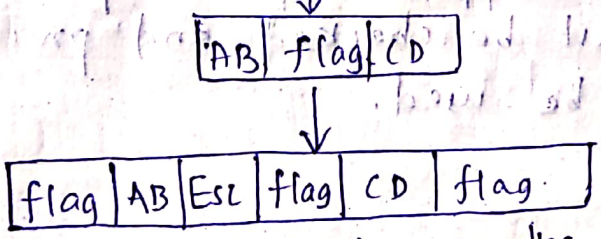
(b) Character Stuffing - In character stuffing method, beginning and end of frame is marked by the special character.

Each characters begins with the ASCII character sequence and also end with ASCII character sequence like - Datalink Escape, flag, Start of text, end of text

Ex : 1)

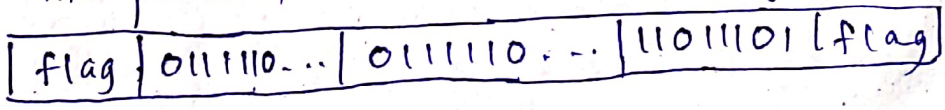


Ex : 2)



Here, 'Esc' is used to ignore the flag within the data.

(c) Bit stuffing - Bit stuffing is the process of adding one extra zero whenever five consecutive 1s follow a zero in the data, so that the receiver does not mistake the pattern 0111110 for a flag.



(d) Byte Stuffing - Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

* The most important responsibilities of the datalink layer are error control and flow control.

Error Control - Error Control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damage in transmission and coordinates the transmission and of those frames by the sender.

Error control in datalink layer is implemented simply: anytime an error is detected is an exchange, specified frames are transmitted. This process is called automatic repeat request (ARQ).

Flow Control - Flow Control coordinates the amount of data that can be sent before receiving acknowledgement and is one of the most important duties of the datalink layer.

In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

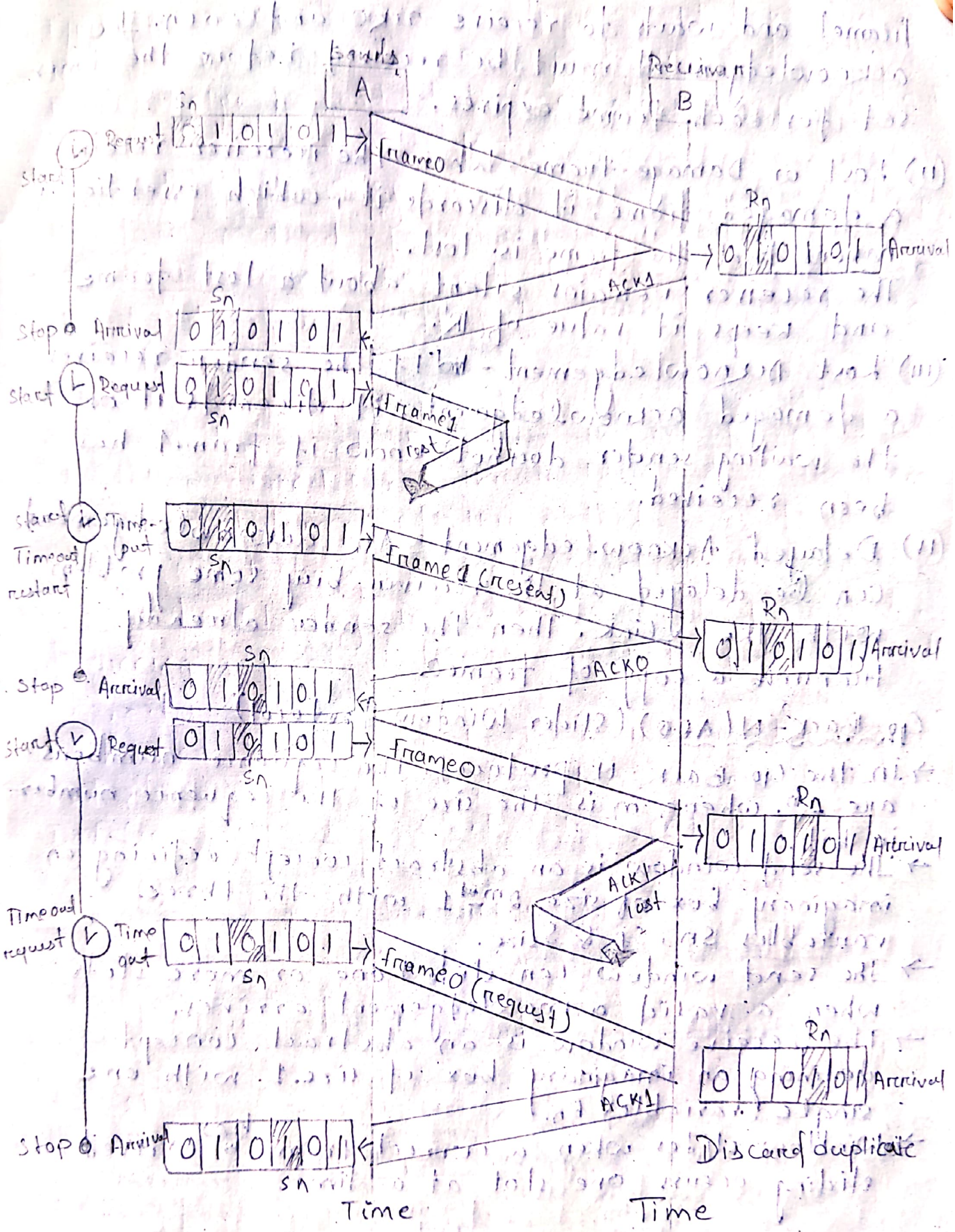
The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stopped temporarily.

Incoming data must be checked and processed before they can be used.

Stop and Wait (ARQ)

Round Trip Time

Time out Time



Operations:-

In the transmission of frame, we can have four situations:- Normal operation, The frame is lost, The acknowledgement is lost or the acknowledgment is delay.

(1) Normal Operation - In a normal transmission the sender sends frame 0 and wait to receive acknowledgement 1. When ack1 is received, it send,

frame1 and waits to receive ack0 and so on. The acknowledgement must be received before the timer set for each frame expires.

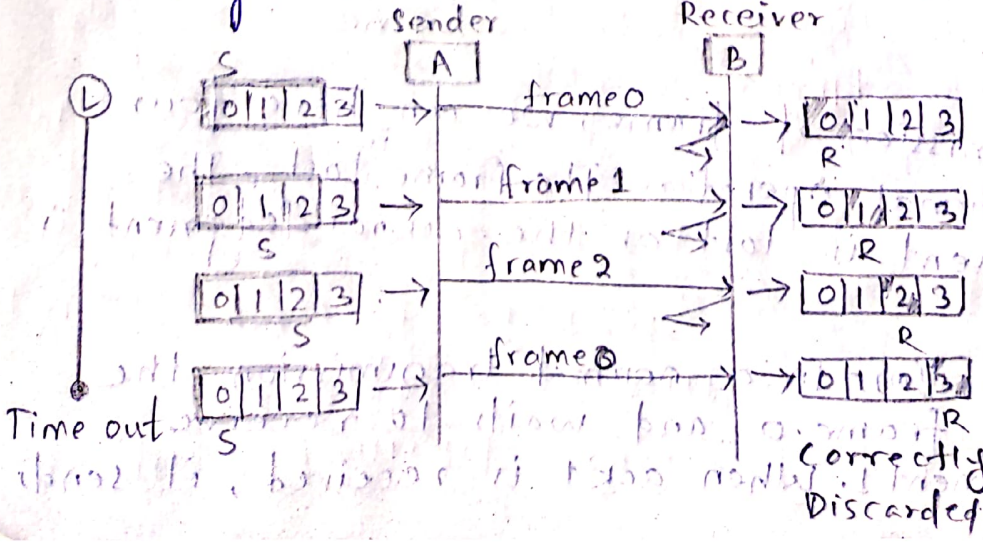
(ii) Lost or Damage frame - When the receiver receives a damaged frame, it discards it, which essentially means that the frame is lost.
The receiver remains silent about a lost frame and keeps it value of R.

(iii) Lost Acknowledgement - If the sender receives a damaged acknowledgment, it discards it or the waiting sender does not know if frame1 has been received.

(iv) Delayed Acknowledgement - An acknowledgement can be delayed at the receiver buy some problem with the link. Then the sender already transmit a copy of frame0.

Go-Back-N (ARQ) (Slider Window Protocol)

→ In the Go-Back-N protocol, the sequence numbers are 2^m, where m is the size of the sequence number in bits.
→ The send window is an abstract concept defining an imaginary box of size $2^m - 1$ with the three variables Sn, Sf & Ssize.
→ The send window can slide one or more slots when a valid acknowledgement arrives.
→ The receive window is an abstract concept defining an imaginary box of size 1 with one single variable R_n.
→ Window slides when a correct frame has arrived, sliding occurs one slot at a time.



operations -

In the transmission of the frames in Go-Back-N protocol, there are four various situations -

(i) Normal Operation - The sender keeps track of the outstanding frames and updates the variables and windows as the acknowledgements arrives.

(ii) Damaged or Lost frame - If the frame is lost or damaged during transmission (suppose frame2 is lost) and the next frame (frame3) is reached to the receiver, then it is discarded because the receiver is expecting frame2 not frame3 (according to its window size). After the timer for frame2 expires at the sender side, the sender sends frame2 and frame3.

(iii) Damaged or Lost Acknowledgement - If an acknowledgement is damaged or lost, we can have two situations. If the next acknowledgement arrives before the expiration of any timer, there is no need for re-transmission of frames because acknowledgements are cumulative in this protocol. ACK4 means ack1 to ack4. So, if ack1, ack2, ack3 are lost, ack4 covers them.
If the next acknowledgement arrives after the time out, the frame and all the frames after that are resent.

(iv) Delayed Acknowledgement - A delayed acknowledgemen also triggers the resending of frames.

NOTE: In Go-Back-N(ARQ) the size of the sender window ~~has~~ must be less than 2^m; the size of the receiver window is 1.
Go Back-N also known as sliding.

Select Repeat(ARQ)

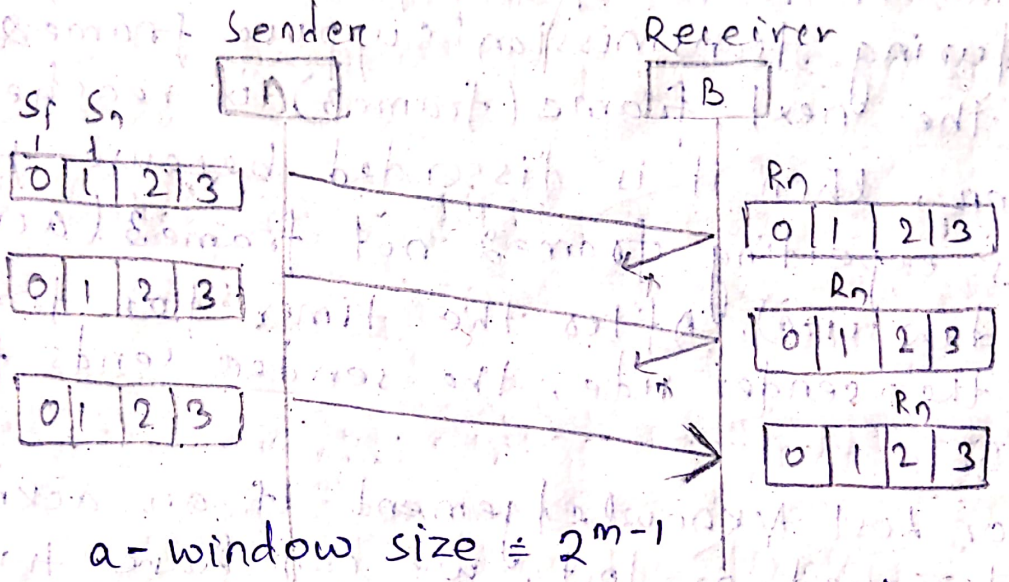
→ In Go-Back-N(ARQ), it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes.

→ This enforces the sender to ~~for~~ retransmit all the forms which are not acknowledged.

→ In selective repeat, the receiver while keeping of sequence no., buffer the frames in memory and sends NACK (Negative Acknowledgement) for only frame which is missing or damaged.

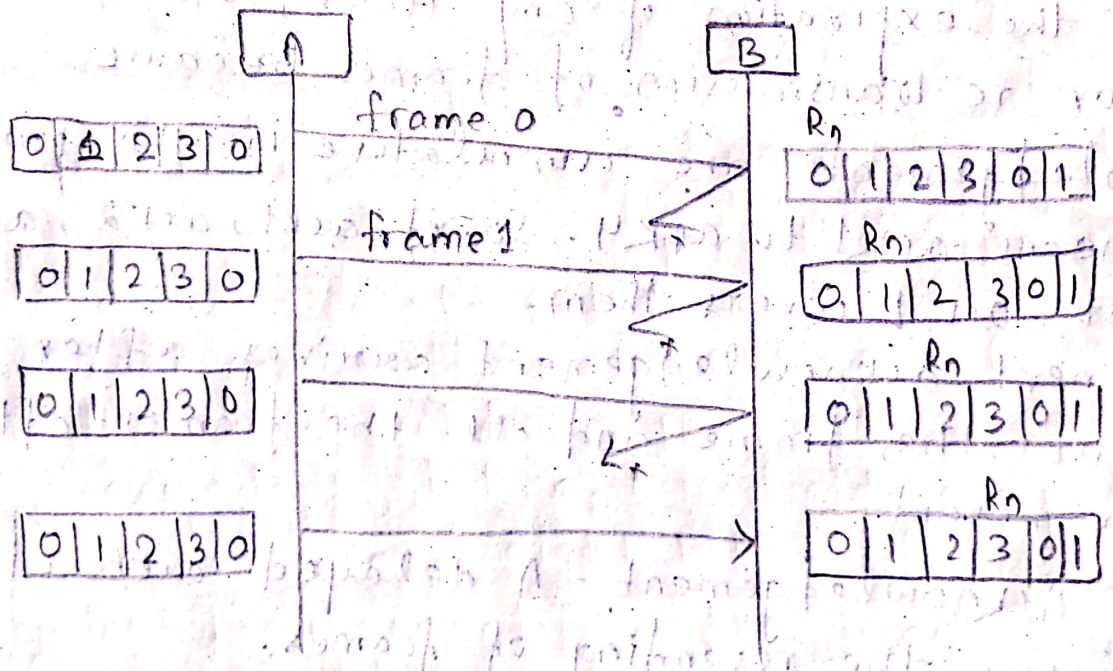
→ The sender in this case, sends only packet for which NACK is received.

* Window size- 2^{m-1}



a- window size ≤ 2^{m-1}

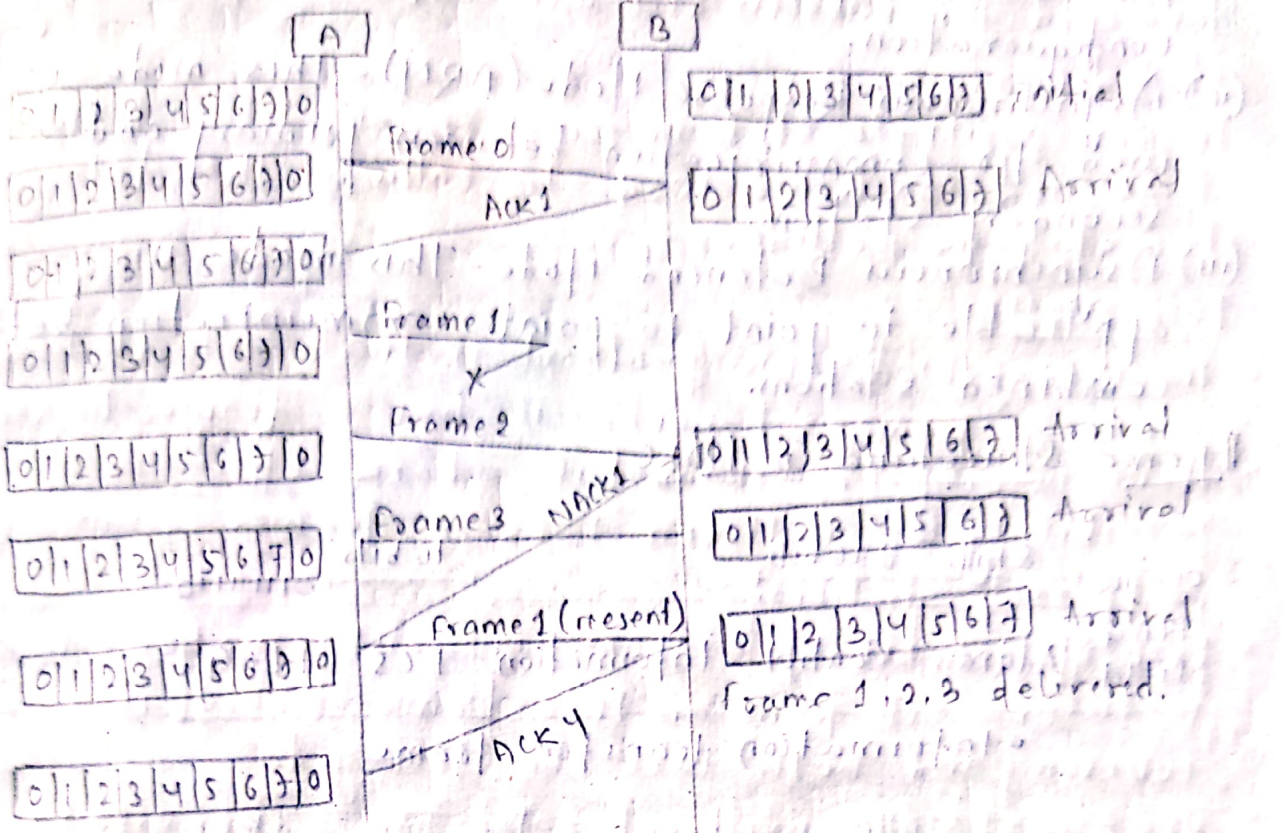
If both sender's & receiver's window size is equal



b- window size > 2^{m-1}

When receivers window size is more than sender's window size.

Out of Order Frame



HDLC Protocol (High Level DataLink)

→ The High level datalink Protocol developed by ISO.

→ HDLC is a bit-oriented datalink protocol, and it is designed to satisfy many of data control requirements.

→ HDLC protocol has three stations defined
(i) Primary station (ii) secondary station
(iii) Combined station.

→ Primary station - The primary station is responsible for the initialization of link, controlling the data flow between primary and secondary station.

→ The secondary station responsible for logical disconnection of the stations, start transmission etc.

→ This station acts as a transperancy between the stations which means any of the two stations can send or receive the data anytime.

Operations Mode of HDLC Protocol -

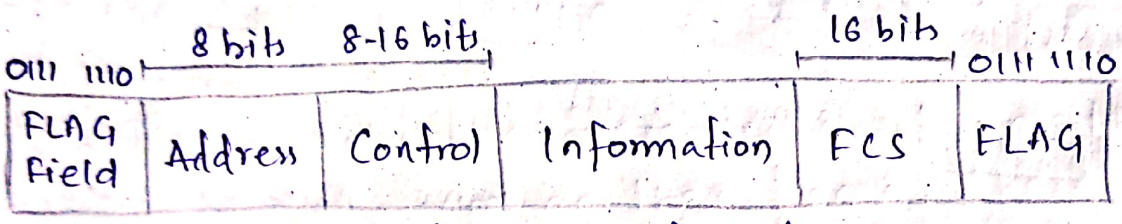
Three modes of operations are defined for the HDLC Protocol as follows -

(i) Normal Response Mode (NRM) - This mode is suitable for point-to-point as well as point-to-multipoint configuration.

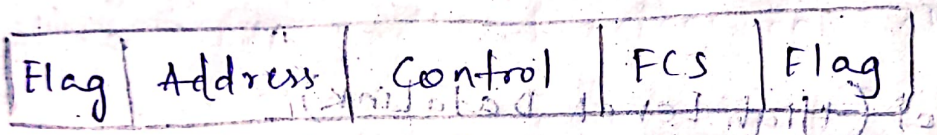
(ii) Asynchronous Response Mode (ARM) - This mode is used for communication between primary and secondary stations.

(iii) Asynchronous Balanced Mode - This mode is applicable to point-to-point communication between combined stations.

Frame Structure in HDLC



- Information transfer frame



- Supervisory frame

- Flag - This field is used for indicating the start and end of a frame. A special eight-bit sequence 01111110 is referred to as a flag. Every frame starts and ends with a flag.
- Address - This fields contains the address of the secondary station. This field may contain one or more eight-bit addresses.
- Control - This field identifies the function and purpose of the frame. Depending on the protocol, an eight-bit or a sixteen-bit control field is used.
- Data - This field contains the user data to be transmitted. It can be arbitarily long or empty.

Point-to-Point Protocol (PPP)

→ The most common protocols for point-to-point access is the PPP.

→ Today, millions of internet users who need to connect their home computers to the server of an Internet service Provider (ISP) use PPP.

→ PPP provides several services –

(i) PPP defines the format of the frame to be exchange between devices.

(ii) It defines how network layer data are encapsulated in the datalink frame.

(iii) It defines how to devices can authenticate each order.

(iv) PPP provides connections over multiple links.

PPP Frame –

→ PPP is a byte-oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are –

(i) Flag - 1 byte that marks the beginning and the end of the frame.

The bit pattern of the flag is 01111110.

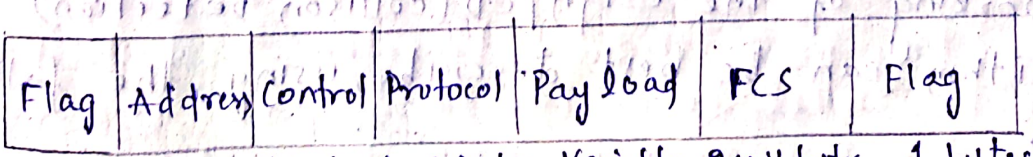
(ii) Address - 1 byte which is set to 11111111 in case of broadcast.

(iii) Control - 1 byte set to a constant value of 11000000

(iv) Protocol - 1 or 2 bytes that define the type of data contain in the payload field.

(v) Payload - This carries the data from the network layer. This may be negotiated between the end points of communication.

(vi) FCS - It is a 2 bytes of 4 bytes checked sequence frame for error detection. The standard code used is CRC.



ALOHA - ALOHA is the earliest random excess method developed for wireless LAN but can be used on any shared medium.
In this, multiple stations can transmit data at the same time and can hence lead to collison. The data from two stations collide.

Pure ALOHA

- The idea behind this protocol is that each station sends a frame whenever it has a frame to send.
- There is only one channel to share, there is possibility of collison between foames from different stations.
- Even if one bit of a foame co-exist on the channel with one bit from anothea foame, there is a collison and both will be destroyed.
- The pure ALOHA protocol relies on acknowledgements from the receivers.
- If the acknowledgement donot arrive after time-out period, the stations assume that the frame has been destroyed and resents the frame.
- f) collison involves two or more station.
- The randomness will have avoid more collison, called back-off time.

Carrier Sense Multiple Access (CSMA)

- The chance of collison can be reduced if a station senses the medium before trying to use it.
- In CSMA, the station is first sense the medium it is ideal or not then sends the data, otherwise it waits till the channel become ideal (listen before talk).
- It is meaningful to stop the transmission after hearing the collison information.
- The working of the CSMA/CD (collison Detection) algorithm can be best describe, using the following steps -

Step 1: Before starting the transmission, station senses the medium for the presents of any transmission from other station.

Step 2: If the medium is idol, the station starts transmission and goes to step 4; otherwise it goes to step 3.

Step 3: If the medium is busy, it continuously listens until the channel becomes ~~intend~~ idle, then it starts immediately.

Step 4: If collison is detected during the transmission a brief jamming signal is transmitted to inform all the stations to stop transmission immediately.

Step 5: After transmitting the jamming signal, the station waits for a random time and attends to start from step 1 again

Carrier Sense Multiple Access with Collison Avoidance

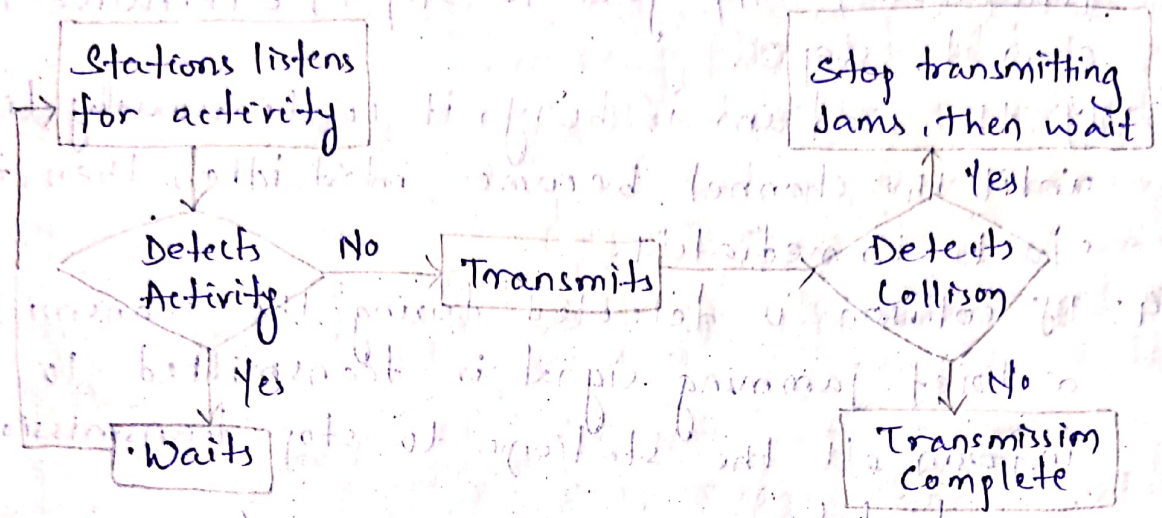
- The process of collison detection involves sender receiving acknowledgement signals.
- To avoid collisons on wireless network, carrier sense multiple access with collison avoidance (CSMA/CA) was invented for this network.
- In contrast to the CSMA/CD protocol, which handles transmissions only after a collison has taken place, CSMA/CA works to avoid collisons prior to their occurences.
- Collisons are avoided through the use of CSMA/CA three strategies as follows -

(i) Interframe space - station waits for medium to become idle. and if found idle it doesnot immediately send data rather it waits for a period of time called interframe space or IFS.

(ii) Contention Window - It is the amount of time divided into slots. A station which is ready to send frame chooses random no. of slots as wait time.

(iii) Acknowledgement - The positive acknowledgments and time out timer can help guarantee a successful transmission of the frame.

Collison Detection - CSMA/CD



Q|OS

Routing - Routing refers to the process of moving data from one host computer to another by selecting the shortest and most reliable path intelligently.

→ An IP Gateway, on the other hand, is the router that accomplishes the act of routing data between two networks.

→ It is important to know that the both host & IP routing performs nothing functions and comparable implementation of the IP protocol are necessary at both sides.

→ Bridging and routing are different in a distinct way. While bridging occurs at the datalink layer or layer 2 of OSI reference model, routing takes place at the network layer or layer 3 of OSI model.

Characteristics -

(1) The routing protocols and algorithm tend to provide optimal routes over the network for communicating host so that the network could be used effectively and efficiently.

(ii) To deliver the packets from source host to destination host, there exist few key design issues, so that the network could select a route accross the network between end nodes with the following characteristics -

- Correctness - The correctness function of the router should provide a valid route, visible path and save links. Route validity ensures that if a route exist for a destination, a usable route should also exist for the route in the network. If this condition is not satisfied, the users will experience a failure in connectivity.
  The visible path ensures that the details of an existing path between two nodes should be propagated by the routing protocol.
  Link safety ensures route availability without taking into consideration the order in which routing message are exchanged.
- Simplicity - The routing should provide simple methods to compute paths to the destination so that the overhead is as low as possible.
- Robustness - It is the property of a network which defines the expectancy of a network to run continuously for many years.
  Robustness is the capability of the network to route the packets to the destination through some routes in case of hardware and software failures.
- Stability - It describes the ability to tackle the changing conditions of the network without influencing network performance.
  The routing algorithms should provides stability under all possible circumstances.

- Fairness - fairness refers to equal priority given to all nodes or hosts on the network for transmitting their packets.
  This is generally done on a first come first serve basis.
- Optimality - The routing algorithms should provide optimal throughput and least mean packet delays.
- Efficiency - The routing algorithm keeps on adding some processing overhead at each node. Such overhead tends to network efficiency.

IP Address -

→ An Internet Protocol (IP) is a unique address which provides a universal address across the network.
→ It is addressed to the data packets which transmit over the network working with the IP Protocol.
→ The IP address consists of 4 parts and each is separated by a dot.
→ format of IP address is xxx.xxx.xxx.xxx
→ Each xxx is a number between between 0 and 255 stored in 8 bit and can have 2^8 values.
→ for example- some of the addresses are 127.0.0.1 and 192.168.0.1.
→ The computer converts these decimal-dotted notation into binary form.
→ The 32 bits are considered as NTT.
→ The NTT contains two components as Network Identifier and host identifier.

Network Identifier- It starts from the left most bit which is used to identify the network. This process is called network prefix.
The four numbers in an IP address are called octets because in binary form each has 8 position.
An octets contains 2 two sections in which the network identifier n recognises, The first octets to identify the network that a system unit belongs to.

Features of IP Address -

→ It poorides a unique address over a network we cannot get the same IP address for two system units.

→ An IP address contains a default network whose address is 0.0.0.0 which is used to the default network.

→ An IP address poorides a look back address except for class A, class B, class C, class D and class E. The IP address 127.0.0.1 is called look back address which help the host computer to send a message back to itself.

→ IP performs the task of routing data packets over a network and provides if network address which specifies the location of source and destination node in the network topologies of a routing system.

Class full IP address -

There are 5 main address classes such as Class A, Class B, Class C, Class D and Class E.

⇒ Class A - 0 represents the Class A address. The next 9 seven bits represents the Network number and remaining 24 bits identifies the host Class A can composed many host addresses.

- An IP address whose first octate is between 1 to 126 is a class X address.
- 0 is reseored as a part of the default address and 127 is reserved for Internal Look Back testing.
- Format : Network. host. host. host
  Default Subnet Mask : 255.0.0.0

⇒ Class B - The first two bits of address are 10 which identify Class B, next 14 bits for network and last 16 bits identifies the host.

- It uses 16 bits for both the network address and host address.
- Class B address can be poorided to 16,384 networks with upto 65,534 host per network.

- Any address whose first octate is in the range 128 to 191 is a Class B address.
  format : Network. Network. Host. Host
  Default SubNet Mask : 255. 255. 0. 01

⇒ Class C - Class C are meant for small networks. The first 3 octate specifies a particular network and the last one octate specifies host Id.

- The first octate range of 192 to 223 in it is Class C address.
  The first 3 bits of addresses are 110 which identify Class C, the next 21 bits for network and the last 3 bits identify the host.
  format : Network: Network. Network. Host.
  Default SubNet Mask : 255.255. 255. 0

⇒ Class D - It defines IP multicast addresses. Multicast IP address have their first octates in the range 224 to 239.

- The first 4 bits of addresses, 1110 form a multicast address. It shares common applications such as videoconferencing.

⇒ Class E - The first 4 bits of the address, 1111 are called Class E addresses, value is greater than 239 and addresses is reserved. These addresses where reserved for experimental used.

IP V-4 (Internet Protocol version-4)

→ IP v-4 was the primary version brought into action within the ARPANET (Advance Research Project Agency Network) in 1983. IP v-4 addresses are 32 bit longer integer which will be expressed in decimal notation.

→ Technically, IP addresses are 32 bit long string. These strings are being separated with dot into 4 decimal number from 0 to 255 in decimal.

→ For example, IP v-4 addresses 11000000101010000000101000 011001 is expressed as 192.168.10.25 in dotted decimal notation.

→ The steps to convert an IP v-4 address from binary dotted notation to decimal notation.

(i) Break 32 bit long address into segments of 8-bit blocks.
11000000 10101000 00001010 00011001

(ii) Write decimal equivalent of each segment
192 168 10 25

(iii) Separate the blocks with periods or dots.
192.168.10.25

Classification of IP v-4 Address -

(i) Unicast - This is a unique address globally for the identification of the device, to connect to the network. It includes a subnet prefix and a host id portion.
- Sub-net Prefix - It is basically a network identifier or network address portion of an IP address.
- Host_id - It identifies a network node to which some devices are interfaced.

(ii) Multicast - It is used for one or more network interfaces located on various sub-nets.

(iii) Broadcast - It is allocated to all network interfaces located on various sub-nets and is used for one to everyone on a sub-net communication.

IP v-6 (Internet Protocol Version-6)

→ IP v-6 is a network layer protocol that allows communication to take place over the network.
→ IP v-6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IP v-4 due to the global exponantionally growing Internet users.
→ An IP v-6 address consist of 8 groups of 4 hexadecimal digits.
→ Example of IP v-6, address 3001:0da8:75a3:0000:0000:8a2e:0370:7334
→ With 128 bit address space, it allows 340 undecillion.
→ IP v-6 also called IP NG (Internet Protocol Next Generation).

Types of IP v-6 Address

(i) Unicast Address - It identifies a unique node on a network and usually refers to a single sender or a single receiver.

(ii) Multicast - It represents a group of IP devices and can only be used as the destination of datagram.

(iii) Any cast Address - It is designed to set of interfaces that typically belongs to different nodes.

Frame Relay - Frame relay is a packet switching network protocol technique that is design to work at the datalink layer of the network.

→ It is used to connect local area network (LANs) and transmit data across wide area network (WAN)
→ Frame relay is considered to be a protocol which must be carried over a physical link.
→ It offers high speed transmission. It is so called because a frame (a datapacket) is relayed successively between transmission devices.
→ It allows transmission of different size packet and dynamic bandwidth allocation.
→ It provides a congestion control mechanism to reduce the network overheads due to congestion.
→ It doesnot have an error control and flow control management mechanism.

Characteristics of frame Relay -

→ frame relay service is one that supports the transportation of data.
→ frame relay is a connection less service, meaning that each data packet passing through the network contains address information.
→ frame relay is a service that is provided with a variety of speeds from 56 KBPs upto 25 MBPs.
→ frames are variable in length and goes upto 4096 bytes
→ frame relay is considered to be a broadband ISDN (Integrated service Digital Network) service.

ATM (Asynchronous Transfer Mode)

→ The purpose of ATM is to provide high speed, low delay multiplexing and switching networks to support any type of user traffic, such as voice, Data or video application.

→ ATM is a new networking technology and its features are considered significant in the networking industry.

→ ATM has been universally accepted as the best transfer mode and an alternative for Broadband Integrated services Digital Network (BISDN).

→ ATM is designed to provide fast packet (cell) switching over various types and speeds of media at valuable rates from 64 KBPs to 2 GBPs and beyond.

→ ATM provides good bandwidth ~~flexibity~~ flexibility and can be used efficiently from desktop computers to Local Area and wide Area Network.

→ ATM is a connection-oriented packet switching techniques in which all packets are of fixed length.

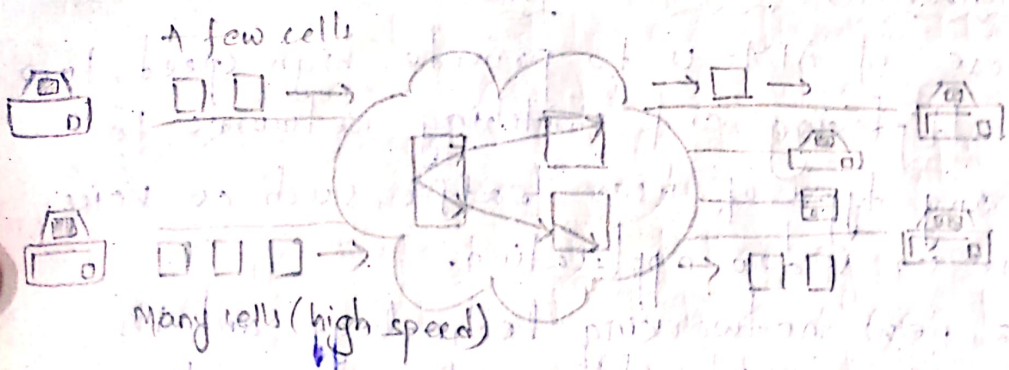
Characteristics of ATM -

The following are the primary features of ATM -

→ The transport speeds of most ATM applications are most often 155 MBPs and 622 MBPs.

→ ATM is a flexible service made possible by the size of the packets (cells). The cell size for all applications is 53 bytes.

→ The small cell size allows a variety of applications to run of on ATM network including voice, video and data.



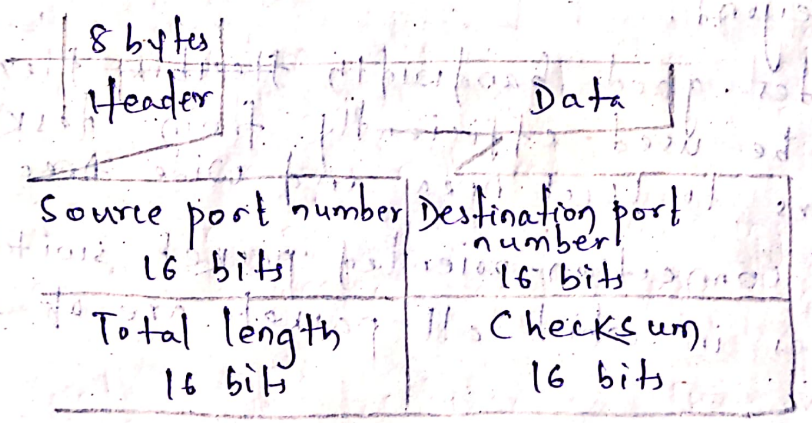
ATM Network

User Datagram Protocol (UDP)

→ The UDP is called a connection-less, unreliable transport protocol.

→ It doesnot add anything to the service of IP except to provide process-to-process communication instead of host-to-host communication.

→ The UDP packet structure is as follows :-



UDP : User Datagram Protocol

UDP Operations :

(i) Connection-less services - UDP provides connection-less services which means that each datagram sent by UDP is an independent datagram. There is no relationship between the different user datagram even if they are coming from the same source process and going to the same destination.

(ii) Flow and error Control - The sender doesnot know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded.

(iii) Encapsulation and Decapsulation - To send a message from one process to another, the UDP protocol encapsulates and decapsulates message in an IP Datagram.

(iv) Queing - Queing in UDP simply refers to requesting port number for client processes and using the port number for process-to-process delivery of message.

(v) Uses of UDP -

→ UDP allows very simple data transmission without any error detection.

→ UDP is used for management processes such as SNMP (Simple Network Management Protocol).

→ UDP is used for some route updating protocol such as RIP.

→ UDP is used by Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to systems dynamically.

→ UDP is an ideal protocol for network applications where latency is critical such as gaming and voice and video communication.

Transmission Control Protocol (TCP)

→ TCP is a transport layer protocol for process-to-process communication like UDP.

→ It is a connection-oriented, reliable transport protocol.

→ It uses flow and error control mechanisms at the transport layer.

TCP services:

(i) Process-to-process communication - TCP provides process-to-process communication using port number

(ii) Stream Delivery Service - It allows the sending process to deliver data as a stream of bytes and allows a receiving process to obtain data as a stream of bytes.

(iii) Full-duplex communication :- TCP offer full-duplex services in which data can flow in both directions at the same time.

(iv) Connection-oriented services - When a process at site A wants to send and receive data from another process at site B the following occurs -
(a) The two TCPs establish a connection between them.
(b) Data are exchanged in both directions.
(c) The connection is terminated.

(v) Reliable Service - TCP is a reliable transport protocol. It uses an acknowledgement mechanism to check the safe arrival of data. This is possible due to efficient error control mechanism.

TCP features and its characteristics :-

To support the services of TCP, following are some features :-

→ Numbering system :- TCP keeps track of segments being transmitted or received. There are two fields called sequence number and the acknowledgement number for numbering the bytes within the segments and acknowledgement respectively.

→ Flow control - The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overloaded with data.

→ Error control - To provide reliable service, TCP implements an error control mechanism which considers a segment as the unit of data for error detection.

→ Congestion control - The amount of data sent by a sender is not only control by the receiver, but is also determined by the level of congestion in the network

Domain Name system (DNS)

→ DNS is a distributed database that provides email routing information. It is used by TCP/IP protocols. These protocol maps between IP addresses and host name.

→ The Domain name extension is defined as the complete address of hosting services provided on the sites.

→ The internet configuration used numeric IP address which was a very cumbersome task. To overcome this problem, symbolic host names came into existence.

→ A name space is organised in two ways, either hierarichical or flag. The address mapping of host name are maintain by network information center (NIC).

→ Hierarichical name space involves the nature and name of the organisation.

→ A fully qualified domain name contains a sequence of levels, separated by dots.

→ The first part defines the nature of an organisation, the second part signifies the name of the organisation the third part refers to the department of the organisation.

→ If the domain name ends in a dot, it shows that the name is not complete. It is refer to as a fully Qualified Domain Name (FQDN).
for example :- MyDir. MyDept. MyCorp. Com

→ If the domain name doesnot end in a dot, that is called Partially Qualified Domain Name (PQDN)
for example :- MyDept. MyDer. MyComp

→ List of all IP addresses are maintained centrally by Internet Corporation for Assigned Names and Numbers (ICANN).

→ DNS provides the protocol which allows the client and server to communicate with each other.

→ DNS is able to quickly translate the text of the IP addresses from a directory of billions of such

addresses and that too within a fraction of second.
→ The Internet is divided into more than 200 Top Levels Domain (TLDs). Those domains are further partition into sub-domains. Examples of TLD are countries like .in, .jp, .us, .pk, etc. There are certain TLD, which comes under the category of Generic TLD. and they are .com, .net, .alt, .edu, etc.
→ The DNS namespace defines an inverted tree types structure.
→ Certain terminologies in relation as follow-
- Root - The DNS tree grows from top to down, The root domain is the parent of all the domains in the hierarchy.
- Branch - It refers to any text closest part of DNS hierarchy and describes a domain with sub-domains
- Leaf - Beneath the leaf no object is defined and therefore it is an end object.

Simple Mail Transfer Protocol (SMTP)

→ SMTP is an application layer protocol, is used to send to email messages across the Internet.
→ It utilizes the TCP as the transport control to send email to a destination mail exchanger, refer to as mail server.
→ A client machine sends email to a mail exchanger. Mail exchanger are nothing but the software application program to support SMTP, such as Sendmail or Microsoft exchange with for IT datagrams that arrive on the network interface with a TCP pood number of 25.
→ The data send using SMTP is a 7 bit ASCII data.
→ Multipurpose Internet Mail Extensions (MIME) defines a mechanism for encoding text and binary data as 7-bit ASCII within the mail envelope.

Networking security - Freedom from Risk and Danger
→ Freedom in terms of computer security is the prevention of or protection against -
(i) Access to information by unauthorized recipients
(ii) Alteration of that information.
→ Security is the ability of a system or protect information and system resources with respect to confidentiality and integrity.
→ Computer security is frequently associated with three core areas - CIA (C - Confidentiality, I - Integrity and A - Authentication)
(1) Confidentiality - Knowing that information is not accessed by unauthorized person.
(2) Integrity - It means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, either accidental or malicious. Knowing the information is not allowed by unauthorized person in a way that is understandable by authorized users.
(3) Authentication - Authentication means that the receiver needs to be sure of the sender's identity and that an imposter has not send the message. Knowing that users are the persons they claim.
Access Control - Ensuring that access only these resources and services that entitled to access and that quality users are not denied access to services that they accept to receive.
Non-repudiation - It means that a receiver must be able to prove that a received message came from a specific sender. The sender must not be able to deny sending a message that he/she, did sent.

Availability - It is ensuring that a system is operational and functional at a given moment, provided through redundancy.

Privacy - Privacy means that the senden and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. The concept of how to achieve privacy has not changed for thousands of years, the message must be encrypted. That is the message must be rendered unintelligible to unauthorized parties. A good privacy technique guarantees to some extent that a potential intruder cannot understand the contents of the message.

Cryptography - It is the science of secret writing with the intention of keeping the data secret.

→ Cryptography is classified into symmentric cryptography and asymmentric cryptography.

Private Key - In the private key, the same key (secret key) is used for encryption and decryption. This key is symmentric because the only key is copied or shared by another party to decrypt the cipher text. It is faster than public key cryptography.

Public key - In a public key, two keys are used. one key is used for encryption and another key is used for decryption. Here, one key (public key) is used to encrypt the plain text to convert it into cipher text and another key (private key) is used by the receiver to decrypt the cipher text to read the message.

Private Key	Public Key
→ The private key is faster.	It is slower than private key.
→ In this, the same key and algorithm are used to encrypt and decrypt the message.	In this, two keys are used. One key is used for encryption and another key is used for decryption.
→ In private key cryptography, the key is kept a secret.	One of the two keys is kept a secret.
→ Private key is symmentrical because there is only one key that is called a secret key.	Public key is assymentrical because there are two types of key - private and public keys.
→ In this, the sender and the receiver need to share the same key.	In this the sender and receiver don't need to share the same key.
→ It is an efficient technology.	It is an inefficient technology.
→ It is used for large amounts of text.	It is used for only short messages.
→ There is the possibility of losing the key.	There is less possibility of key loss, as the key is held publicly.

IEEE 802.11

→ It is also known as Wireless Fidelity (WiFi).

→ Like ETHERNET and Token Ring ~~is a~~ siblings, 802.11 is designed for use in a limited geographical area (Homes, office buildings, campuses).

→ Primary challenge is to mediate access to a shared communication media - In this case, signals propagating through space.

→ 802.11 supports additional features:
- Power Management
- ~~Error~~ and security mechanism

→ 802.11 uses 5 GHz radio band (High frequency which has 23 overlapping channels rather than 2.4 GHz frequency band which has only three non overlapping channels.

→ Access Method of IEEE 802.11 wifi: CSMA/CA is used.

Modes of WiFi

→ Connections to these wireless network are usually maintained by NIC or Network adapters.
→ A wireless network adapter is a device that help u to connect two wireless network.
→ It acts as a mediator between the server or other computers and are machine which helps in sending and receiving files.

Wireless connection Mode -

(i) Adhoc Mode - In this mode, the nodes are connected to each other without the presence of any base station or access point. The nodes can communicate directly with each other and also share resources without the presence of any external media (routers etc), provided they are connected on the same network on the same channel.

(ii) Managed Node - In this mode, every node is connected to an access point or base station (routers, etc) and it only receives the data which is sent to it by the access point (AP).

- to connect to a network in managed mode the node automatically changes its channel according to the access point.

Protocol	frequency	Channel Width	Maximum datarate
→ 802.11ax	2.5-5GHz	20, 40, 80, 160 MHz	2.4 Gbps
→ 802.11 ac wave2	5GHz	20, 40, 80, 160 MHz	1.73 Gbps
→ 802.11 ac wave1	5GHz	20, 40, 80 MHz	866.7 Mbps
→ 802.11n	2.4-5GHz	20, 40 MHz	450 Mbps
→ 802.11g	2.4GHz	20 MHz	54 Mbps
→ 802.11a	5GHz	20 MHz	54 Mbps
→ 802.11b	2.4GHz	20 MHz	11 Mbps
→ legacy 802.11	2.4GHz	20 MHz	2 Mbps

Digital Signature and Digital Certificate

Digital signature - A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

→ Key generation algorithm - While performing digital transactions authencity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.

→ Signing Algorithm - To create a digital signature, signing algorithms like email programs create a one way hash of the electronic data which is to be signed. This signing algorithm then encrypts the hash value using the private key. This encrypted hash along with other information like the hashing algorithm is a digital signature.
This digital signature is appended with the data and sent to the verifier.

→ Signature verification Algorithm - Verifier receives digital signature along with the data. It then uses verification algorithm to process on the digital signature and the public key and generate some value.
It also applies the same hash function on the received data and generates the hash value.
Then the hash value and the output of the verification of the algorithm are compared.
If they both are equal then the digital signature is valid as it is invalid.

Digital Certificate - Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

→ A digital certificate is a certificate issued by certificate Authority (CA) to verify the identity of the certificate holder.

→ The CA issues an encrypted digital certificate containing the applicance public key and a variety of other ~~ind~~ identification information.

→ Digital certificate contains -

(i) Name of certificate holder.

(ii) Serial number which is used to uniquely identify a certificate.

(iii) ~~E~~Expiration date.

(iv) Copy of certificate holders publicly.

(v) Digital signature of the certificate issuing authority.

(vi) Digital certificate is also send with digital signature and the message.