NETWORK BASICS

Topics :- Introduction to Computer Networks, Network Topologies, LAN, WAN, MAN & Wireless Networks, OSI Reference model, TCP/IP Protocol Suite, Network Performance, Networking Devices, [redacted] Inter Networking

☆ Introduction to Computer Networks :-

We know, Earlier the data have to be transferred through a floppy Disk / CD or if some one wants to get the Data, he/she must have to go to that place (like University, Bank) to access the data which is very complicated. So this give birth to Computer Networks.

Definition :- A group of Computers Connected together by special transmission media, network Adaptors and network operating Systems that Support Communication protocols.

- Applications of Computer Networks :-

(i) Chat Applications or Instant Messangers.

(ii) TELNET :- It is Workstation that allows to access the remote Servers, this enables a user to control the Server and Communicate with other Servers on the Network, it appears as a 'terminal'.

(iii) Database Applications

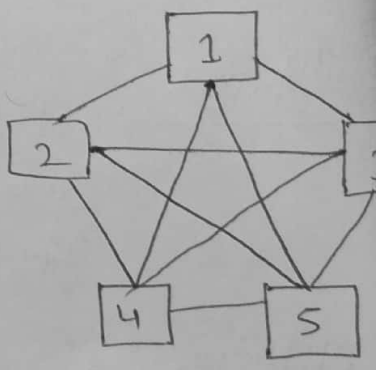
(iv) Electronic mail (E-mail).

* **Network Topologies** :- It refers to the way in which network lai
Out physically or we can say that it i
a Geometric representation of how the nodes and links are
linked in a network.

Types of Topology :- (1) Mesh Topology
(2) Star Topology
(3) Bus Topology
(4) Ring Topology

✓ MESH Topology :- In Mesh Topology Each device has a dedicated link to
Every other Device in the network, the term 'dedicate
means that the link carry traffic only b/w the two Devices and
it also allows bi-directional Communication

ADVANTAGES :- (1) use of Dedicated Links
(2) Robust → ic strong
(3) Provides privacy or Security
(4) fault identification & fault
isolation.



DISADVATAGES :- (1) Installation & reconnection
are difficult.
(2) More wiring required
(3) Very Expensive

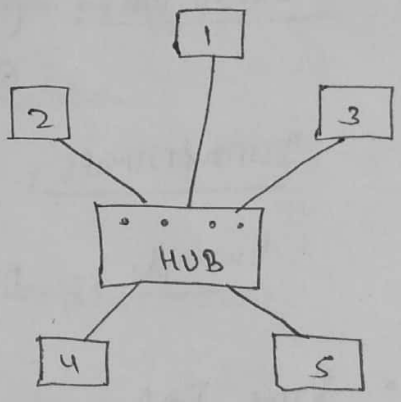
Example :- Telephone regional offices.

- **STAR TOPOLOGY :-** In a Star Topology, there is a Central Controller which we usally called as a Hub, Each device is Connected to it (ie. Hub) through a dedicated link and the devices are not directly Connected to each other.

Unlike Mesh Topology, it doesn't allow direct traffic exchange, in this a Hub acts as an exchanger, it means if one device wants to send data to another, it first send to Controller, than Controller will sent it to device.

ADVANTAGES :-

1. Less Expensive
2. Easy to install and reConfigure
3. Robust
4. Easy fault identification and fault isolation.



DISADVANTAGES :-

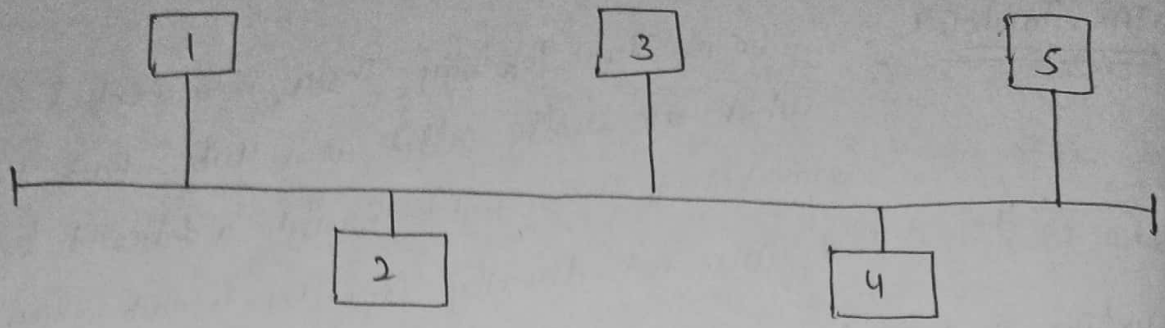
1. Dependant on the Central Devices (i.e. Hub)

Example :-

1. Local Area Networks
2. High Speed LAN's.

- **BUS TOPOLOGY :-** It uses multipoint Configuration, as only cable is linked all the devices to the network, it is called as Bus Cable, and all the Devices are Connected through drop lines and tap.

A dropline is a wire blw Device and main Cable whereas a tap is a Connector which either supplies in a main cable and there is a limitation on the no. of taps a bus can support and distance blw these taps.



As a Signal travels along the back, Some amount of Energy is transform into Heat, ∴ Signal becomes Weaker and Weaker as it tra farther and farther, Hence Distance b/w the taps had to be limited.

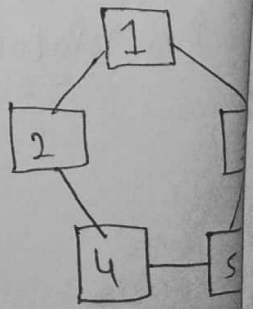
ADVANTAGES :- ① Easy of installation
② Less Cabling.

DISADVANTAGES :- Difficult ME-Connection and fault isolation.

Example :- Ether-net LAN's

- RING TOPOLOGY :- In a Ring Topology, Each Device has a dedicated link other two Devices on each side of it (ie Neighbouring D

A Signal is passed in one direction in the form of ring Device to Device until it Reaches its destination. In each link t is a repeater whose Job is to generate the same bits of information while passing to another device.



ADVANTAGES :- ① Easy to install and Configure
② Fault isolation is required

DISADVANTAGES :- If break down occurs in the ring, Entire System gets disabled

Example :- IBM → International Bussiness machines token ring Network (IEEE 802.5)
↓
Technology used to build local Area Network

★ **Network Types** :- We can classify Computer Networks based on their Size like LAN, WAN, MAN and Wireless Networks.

- **Local Area Network (LAN)** :- It is one of the original Categories of the Network and Simple.
  - Privately owned Network
  - Connects Computers together over small distance (i.e. within buildings)
  - Allows resource sharing (i.e. files or printers in office).
  - High Speed Connectivity & low cost implemantation.
  - Data Rate 100 - 1000 Mbps.
- **Wide Area Network (WAN)** :- It has slightly Complex nature.
  - Usually of global span
  - Contains multiple Smaller Networks (i.e. LAN and MAN)
  - Provides long distance transmission of data
  - Example :- Internet.
- **Metro Politan Area Network (MAN)** :-
  - Size lies b/w LAN & WAN.
  - Spans multiple buildings or colleges.
  - Connects several LANs to form bigger Network.
  - Example :- Telephone Network, Cable TV.

- Wireless Networks :- It is a modern Technology alternative to tradi Wired Networks.
  - No need of Physical Connection.
  - Micro Waves or Radio Waves are used as medium for Connectivity.
  - Application :- Used in Home & Business Computer Networks.

There are Several Type of Wireless Networks :-

(1) Wi-fi :- It is specially popular in home Networks and as a wireless hotspot Technology. A hotspot is any loca where wi-fi access is made publical.

(2) Bluetooth :- A bluetooth is for low power and embedded appli it is used for Connecting mobiles, Computers an other network devices over a short-range, It is deli to primarily support wireless networking for personal d and peripherals including wireless headsets, etc.

(3) Zigbee :- It almost resembles bluetooth and wifi, Zigbee devi are designed to Communicate via Radio frequencies and is of 3 types.

(i) Coordinators :- Controls network formation and Security

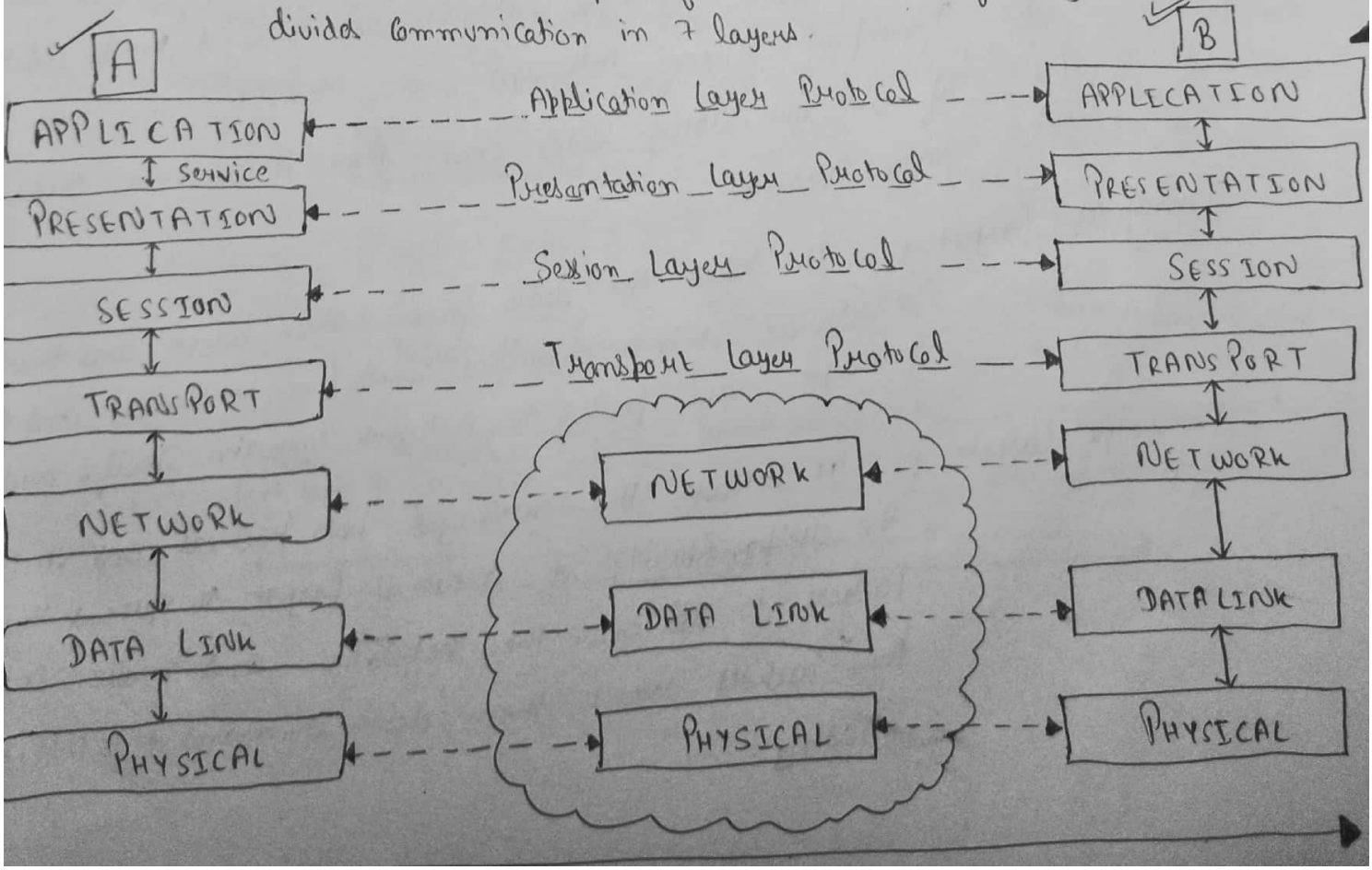
(ii) Routers :- Pass on the Signal and extand the ran

(iii) End devices :- Performing certain tasks such as reading a turning or a light and designed for low power Consumptions.

★ OSI Reffarance Model [7 Layers Explained] :-

Suppose We have two Computers A and B and they are Connected through Computer Networks, Now if A wants to Send Data to B, then data is transferred through some nodes to reach its Destination, and the Data will Send Secured and Correctly, there are some rules which are guided by Something Called protocols and the group of these such protocols are known as Communication model.

OSI :- Open System Interconnection which means Every System participating in this model is open for Communication for any other System. It divides Communication in 7 layers.



- The Bottom three layers are implemented by the nodes and their function is just to transfer the data flow.
- The ToP 4 layers are implemented by End to End Systems.
- Every layer can communicate with layer above or below it or we can say provide Service.
- Application layer :- It is layer where user communicate with syst it provides some protocols through which applications communicate with each other.
  Eg :- FTP Protocol.
- Presentation Layer :- It concerned with the format of data Exchang A (32 bits) ---- Convertion ---- B (64 bits).
- Session layers :- It creates Session for users and also if applic has different transport streams then it binds suc Transport Stream into one
  Eg :- If we are doing Video chat, then it Combines Audi Video streams.
- Transport layer :- It takes the data from session layer and the divide it into smaller units (i.e. messages) and messages are passed to Network layer in specific or
- Network layer :- It breaks the messages into packets and it the responsibility of Network layer to spread th packets to all over the network and make su these packets reach their destination and it is calle Routing.

- Data
- Ph
- P

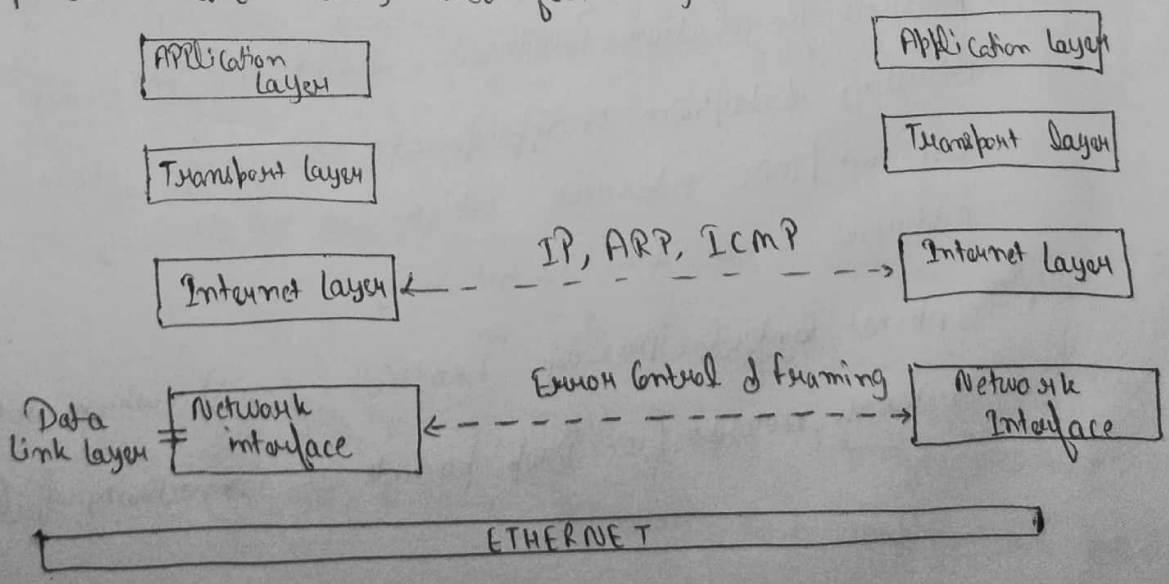
- **Data Link layer** :- It is concerned with transmission of error free data, it breaks the packets into smaller units known as frames and passes these frames over Physical layer. Data Encoding, Framing, Error Correction and detection techniques are applied here.

- **Physical layer** :- It is concerned with Transmission of raw bits over the Communication.

★ **TCP/IP Protocol Suite** :- It is the more Practical model used in the Communication.

It has only 4 layers, it gets this name bcz of 2 important Protocols (Transmission Control Protocol & Internet Protocol).

- It provides end to end Connectivity (i.e. how packets are addressed, Transmitted to the destination and framed)
- It doesn't have a Separate Physical layer, thats why it is hardware independant and mostly used for any virtual hardware technology.



① Network Interface layer :-

- It identifies the network protocol type of the packet.
- Sometimes called as Data Link layer.
- It is used for transferring packets b/w Internet layer interfa of two different hosts on the same link and it perform sev functions like adding header to the frame and transmit over the physical layer
- It can also transmit packets over private networks and tunnel
- This layer provides error control and framing.
- Eg :- Ethernet and PPP framing

② Internet Layer :- It accepts and deliver packets over the inte

- It includes IP, ARP, ICMP
- IP responsible for IP Addressing, host to host Communicati packet formatting and fragmentation (ie Dividing big Datagram or packets into smaller ones).
- Address Resolution Protocol assist the internet Protocol in directing datagram to appropriate receiving system by mapping Ethernet / MAC Addresses which are 48 bit long to the known Addresses which are 32 bit long.
- Internet Control Message Protocol (ICMP) which detects & repo network errors. (ie. Drop packets or Connectivity failure).

③ Transport Layer :- as same as we studied in Transport layer section

But we will study SCTP Protocol here :-

- It is Reliable, Connection oriented multi homed streaming
- It can also support systems which have more than one address
- The Connection b/w the Sender and the Receiver is known as Association and the Data Sent is known as chunks
- SCTP stands for Stream Control Transmission Protocol.

④ Application layer :- This Layer include Protocols Used by most of the applications providing User Services.

- Or exchanging application data over the network Connections established by lower level protocols.
- These data transfers and other services may include basic network support services such as many routing protocols and host configuration protocols.
- Example :- ① HTTP → Hyper Text Transfer Protocol
  ② FTP → File Transfer protocol
  ③ SMTP → Simple mail Transfer protocol
  ④ DHCP → Dynamic host Configuration protocol

☆ **Network Performance** :- Performance means Efficiency with which the Network delivers the data.

Each Network is different in nature and design, Common Metrics to measure Network performance.

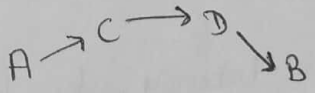
- Band width
- Latency
- Error Rate

⇒ **Bandwidth** :- It is maximum rate at which information can be transferred across the Network. or no. of bits transferred per specific period of time.

⇒ **Latency** :- Time taken to forward the message from one end of the network to the other.

Like Suppose we have a Strong data Connection, but the route taken by data packets is indirect, than response time will be Slower.

A ⟶ B



It is the Sum of three Components :-

(Propagation Delay + Transmit Time + Queuing Delay)

- Speed-of-light propagation Delay :- As speed of light varies from medium to medium

Propagation Delay in optical fibre :-

Distance = 1000 m

Speed-of-light = 3×10^8 m/s

Propagation Delay = $1000 / (3 \times 10^8)$

= 50,000 s

- **Transmit Time** :- It is the amount of time to transmit a unit Data over the Network. It is given by file size divided by Bandwidth.

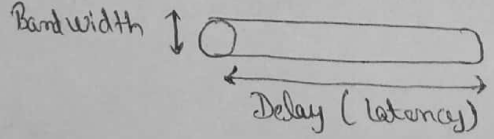
Example :- Size of file = 24 MB.
Bandwidth = 10 Mbps
Transmit time = $(24 \times 10^6 \times 8) / (10 \times 10^6)$
= 19.2 s

- **Queuing Delays inside the Network** :- This Delay occurs du packets generally need to s for sometime before forwarding them to an ou link is Queuing Delay

---

Q- How the product of Delay and Bandwidth helps in Constr High performance Network.

A- Let us take a Hollow pipe to store the data.



- Latency = length of the pipe
- Bandwidth = Diameter of the pipe
- Volume of the pipe = Delay x Bandwidth

Example :-
Latency = 45 ms
Bandwidth = 50 Mbps
Volume = $45 \times 10^{-3} \times 5$
= 280 kB

As the Sender Sends the data through the pipe and Reciever start receiving the data from it., So this Delay Bandwidth product Corresp to How many bits the Sender sends before the first bit actually r by Reciever, Also if Sender doesn't fill the pipe, then it will be as Unutilized Channel.

⇒ Error Rate :- No of bit errors in the received bits of a data stream over a communication channel. It occurs due to Noise, interferance, distortion, etc.

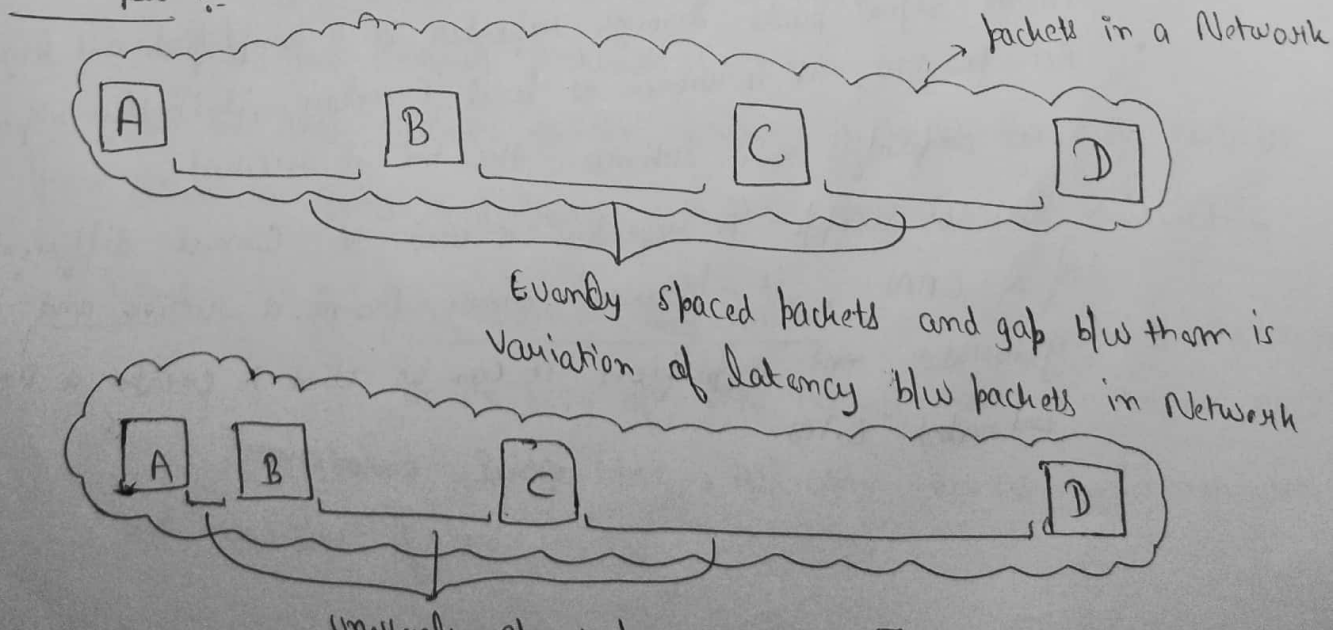
- Bit Error Rate (BER) :-
  - Number of bit errors per unit time
- Bit Error Ratio (BER) :-
  - Number of bits errors / Total no. of transferred bits
  - Unit less measure, expressed as a percentage
    - ↓
    - No units

Note :- The lower is the latency, higher will be the Network performance

However, Error Rate does not much vary from one packet to another, otherwise it may lead to Jittar.

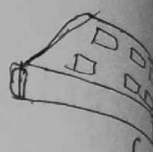
Jittar can be defined as variation in the latency of recieved packets and it is caused due to Network Congestion, Configuration errors and improper Queuing.

Example :-



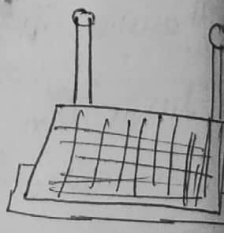
* **Networking Devices** :- They are the physical components used t
Connect the Computer and Devices toge
for sharing information. (also known a
Communication Devices).

① Network Interface Card (NIC)



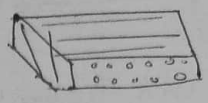
- Enables a Computer to become a part of the Network
- Contains electronic circuitry including wired & wireless Co
- Prepares, Sends and Controls the flow of data
- MAC Address of 48 bit
- Also known as Network Interface Controller, Network Adap
or LAN Adapter.

② Repeater



- Operates at the physical layer.
- Extends the length of the Network.
- Passes the digital signal bit-by bit in both directions
- As the signal passes through repeater it is amplified and regene
- Acc. to ISO, it is known as level-1 relay, it simply repeats, re-amplifies and retimes the bit it receives.
- So To Sumpp A repeater is used to connect different s
of a LAN, it forward every frame it recive and it's
generator not amplifier, it can be used to create a single
extended LAN.

③ HUB :-

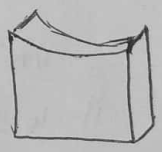


- Works at Data link layer
- Physically Connects networking devices together.
- Transmits the packets to other appended devices without altering any of the Transmitted Packets.
- 2 Types :- (i) Passive Hub :-

It is just like Point of Contact for the wires that make up the physical Network. They are also known as Concentrators.

(ii) Active Hub :- They are also known as Concentrators bcz they Strengthen the signal when it comes & goes from Hub. They are also called Multiport Repeators, All the Hubs have ports into which cables are inserted. (i.e Jacks).

④ Bridge :-

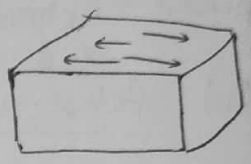


- Works at the Data Link Layer.
- Divides larger networks into Smaller Segments.
- Placed b/w two Physical Network Segments.
- When the data arrives to the bridge, it checks the MAC Address from where it Comes and passes it to the Correct destination
- 3 Types :- (i) Transparent Bridge : It transmits the data on the basis of MAC Address and it is known as Transparent Bridge bcz, all other devices in a network are unaware of it.

- **Source route Bridge** :- They handle all inter LAN frames & hold information on Complete Route from So and Destination and this information help bridges to how to forw the frames.

- **Translational Bridge** :- It is used to Convert the one Network Data format to another and these are to connect dissimilar Networks like Ethernet and ring

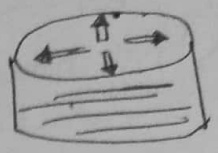
(5) **Switch** :-



- Works at the Datalink layer.
- Provides Connectivity for devices on an Ethernet Network.
- Why to go for Switches when we have hub?
  - Difference lies in the way data frames are handled
  - The hub receives a frame, it forward it to all the ports on it whereas Switch forward it to only that port which it to the destination devices. So Switch devices are more intell than Hub.

- **Methods for Data transmission** :-
  - **Cut-through Switching** :- forward the packets as soon as the received, it is fast and hence reduce latency, but Errors are checked at destin point.
  - **Store & forward** :- check the entire packet for errors before forwarding. but it takes longer time.
  - **Fragment free Switching** :- It is the hybrid of previous two meth it store only 64 bytes before forwardi most of errors come in first 64 bytes.

(6) Router :-



- Operates at Network layer.
- It can be dedicated hardware device for a computer system with more than one network interface and appropriate routings.
- It has Ability to connect dissimilar LANs and also has ability to limit flow of broadcast.
- Every router maintains a routing table.
- It first check the Address where it have to sent the packet by reading the header of the packet and then sent to destination by refering a routing table.

(7) Modem :-

- The word originates from modulator-demodulator.
-

Digital Signals ⟹ Analog Signals (Modulation)

Digital Signals ⟸ Analog Signals (Demodulation)

- Operates in half-duplex mode or in full duplex mode

A half duplex modem must send and receive the signals and provide more bandwidth but slows down communication but full duplex modem has more speed but less bandwidth. and can handle two signal simultaneously by using two carriers.

- It is used for Dial up for LAN and also to connect to Internet Service provider (ISP).

☆ **Internetworking** :- It is combined of 2 words, inter and networking which implies an association b/w totally different nodes or segments.

To Enable Communication, every individual network node or p is designed with a similar protocol or Communication logic, th Transfer Control Protocol (TCP) or internet Protocol (IP). one network Communicates with another network having Constant Com procedures, its called internetworking. Internetworking was deli to resolve the matter of delivering a packet of information th many links.

There is a minute difference b/w extending the network and internetworking. Merely exploitation of either a Switch or a hu attach to 2 LAN is an extention of LAN whereas Connecting Via the Router is an associate degree example of internetwo Internetworking is enforced in layer three (Network layer) of OSI model. The foremost notable example of inter networking that the Internet.

PHYSICAL LAYER

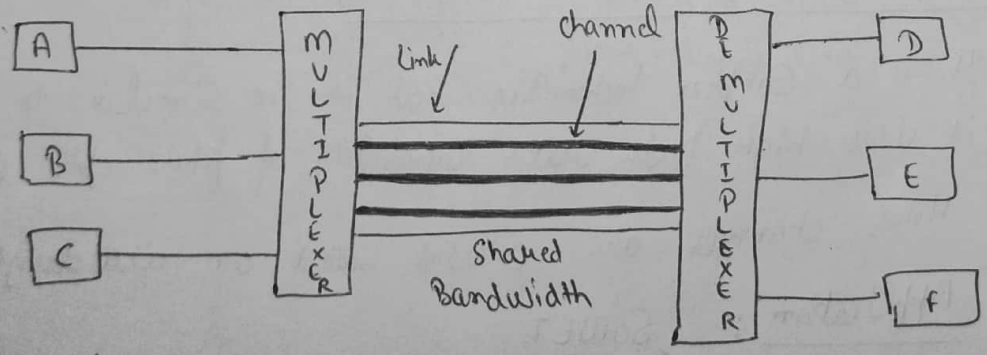
Topics :- Multiplexing , Switching , Transmission Media Types

✱ Multiplexing :-

First of all we want to know why we need Multiplexing?

⇒ In reality, we have a limit on the usage of band width over the network, the main challange we face have is proper utilization of band width, thats why need multiplexing.

- It is used to acheive efficiency by combining several transmission channels into one.
- It Divides bandwidth of low level channel into many high level channel.
- At receiving end, this process is reversed and known as Demultiplexing.



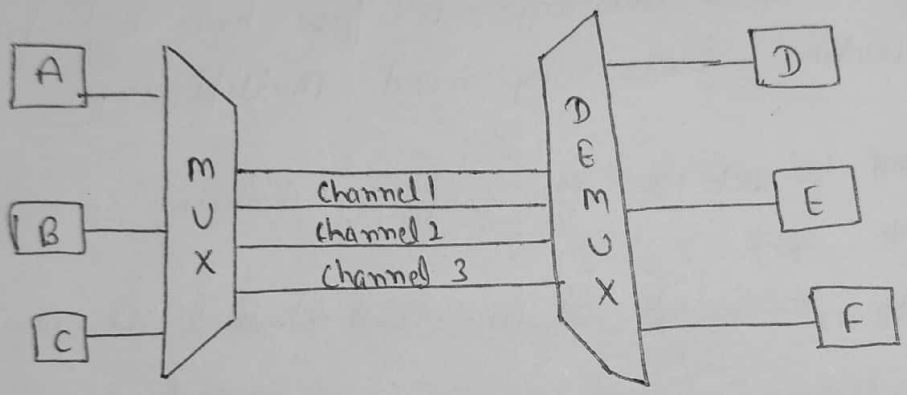
✱A link refers to the physical path and channel refers to the position of the link that carries transmission b/w Devices.

The Device which performs multiplexing is multiplexer and device which performs Demultiplexing is Demultiplexer.

3- Types of Multiplexing Techniques :-

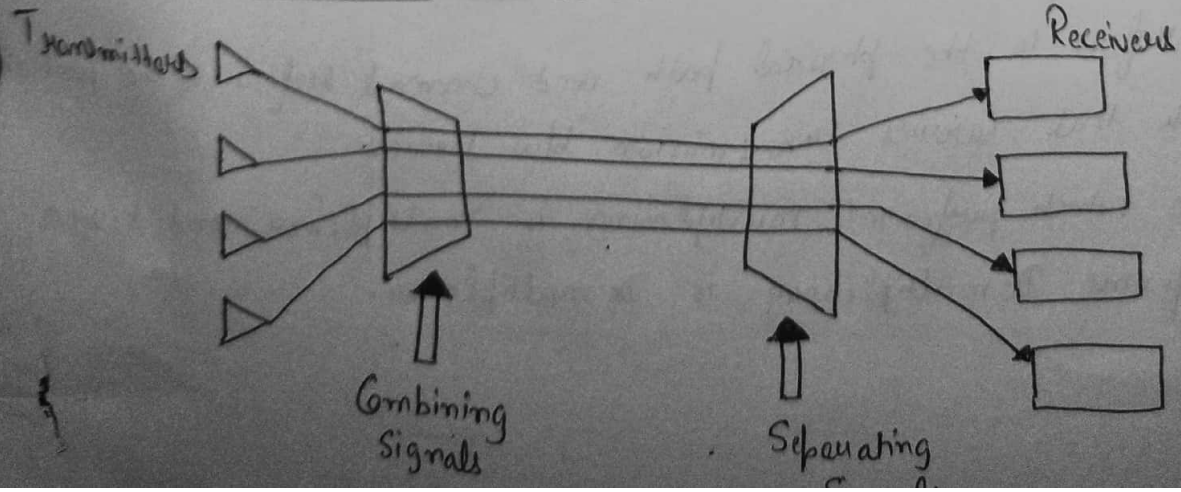
① Frequency Division Multiplexing. (FDM)

- It is analog technique and applied when the bandwidth of a link is greater than the combined bandwidth of the signals to be transmitted.
- Here, channels created based on frequencies which carry information
- Application : AM/FM Radio Systems



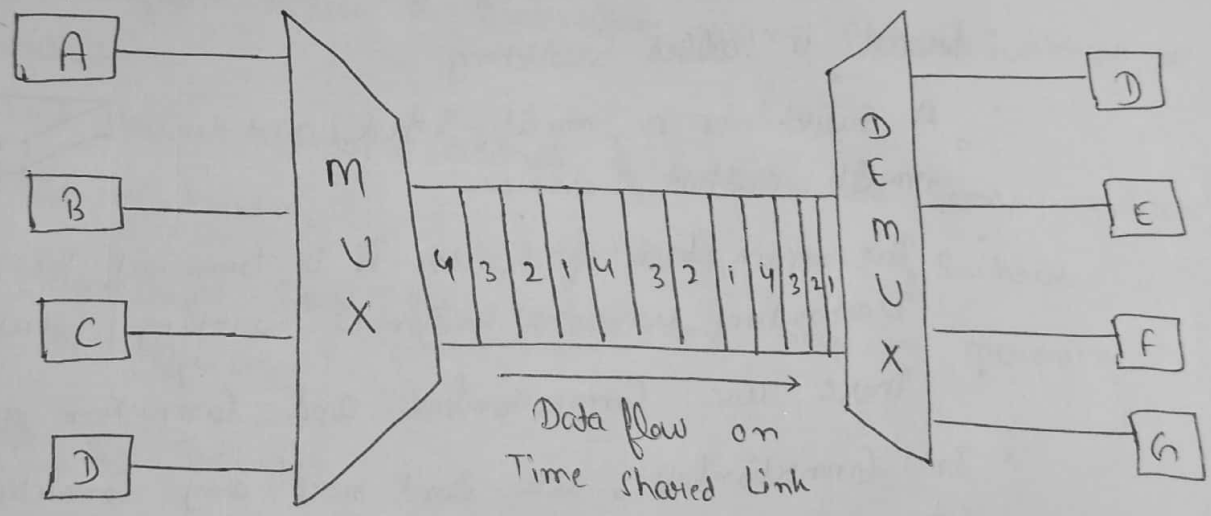
② Wavelength Division Multiplexing (WDM)

- It is a complex technique but it is similar to FDM it uses high Data rate capability of fibre optic cables
- Here, channels are created based on wavelength.
- Application :- SONET.



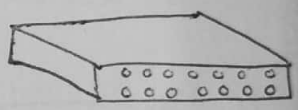
(3) Time Division Multiplexing (TDM) :-

- It is a Digital Technique (ie not Analog)
- In this Multiplexing, Each Connection occupies a position of Time
- In Simple Words, we can see from the figure, If there are four Signals then each Signal is given 1/4 th Time block to transfer the Data (ie. in shared Link).
- Application :- Gsm Telephone System



★ Switching :-

- Now we know if two Devices wants to Communicate with each other, then it must have to establish peer to peer Connection
- And if there are many devices, then we need a central device, which helps in communicating.
- but if there are so many devices along with no. of central device, then it will be difficult to make such a Connections as if we make Connections, then it will be tidious.
- So To Solve this issue, we will use Switches and the process is called Switching.
  - A Switch is a multi-Input and multi output device.

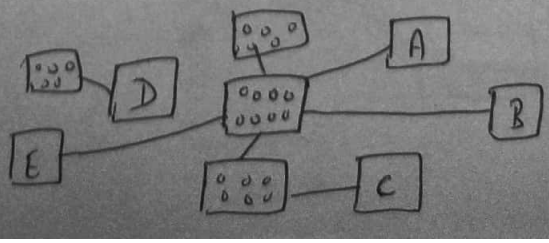


  - The main task of Switch is to transmit the data to Destination which is known as Switching / forwarding.
  - There are Connectionless and Connection oriented Switches
- In Connectionless, we don't need any Connection state b/w devices before the Data transferring but in Connection oriented, it is required to establish a Connection state b/w devices before transmission.

3 Types of Switching :-

① Circuit Switching :-

- It establish Direct Connection b/w devices and it Connection oriented and Connection established is known as Circuit Switched Connection



⇒ ADVANTAGE :- overhead is less bcz data arrives in sequence and Quality is predictable.

⇒ DISADVATAGES :-
- Bandwidth is wasted during no data Transfer.
- Hosts must operate at same rate for Smooth Communication.

Application :- Telephone Network.

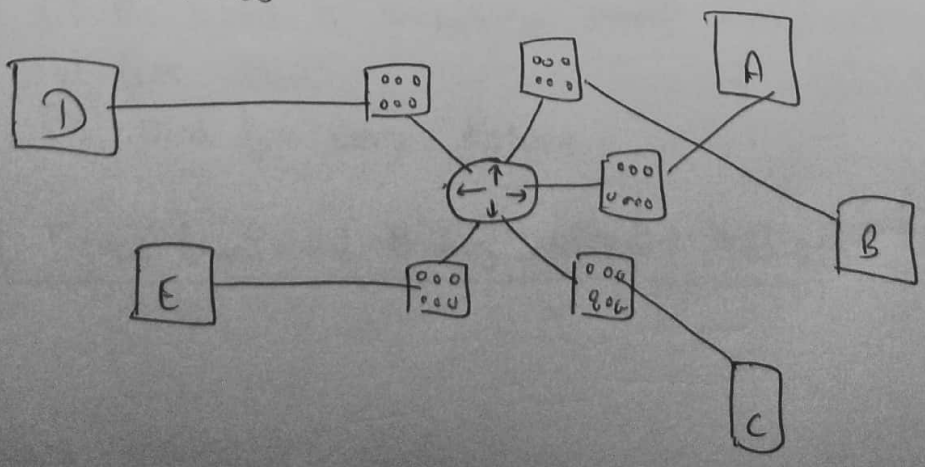
(2) PACKET Switching :-

- Packaging Data in Specially formatted chunks.
- Routed from Source to Destination using Network Switches or Routers.
- Each packet Contains address of receiver and Sender which helps in routing
- Intermediate Node Store packets in internal memory of Switches and helps in increasing Line efficiency

Example :- Internet

Advantage :- Utilizes the overall network Bandwidth

Disadvantage :- Large overhead, bcz Sometimes packets have to be re-transmitted and packets are also not arrived in sequence.

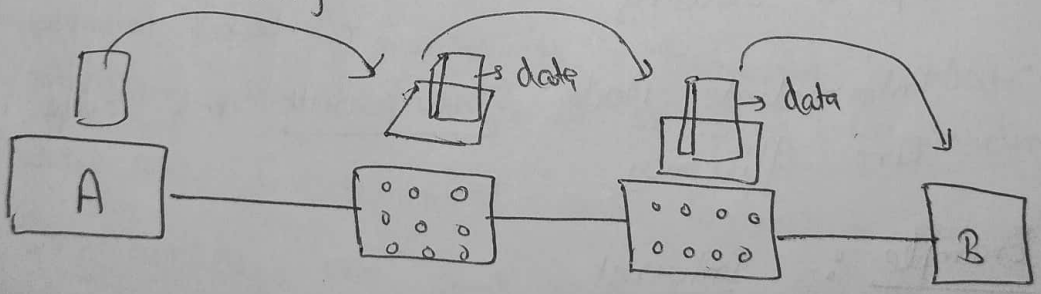


③ **Message Switching** :- It is in b/w Circuit and Packet Switching.

- It Considered one message as a Single Data unit.
- Data is transfered fully in one go.
- And if there is not enough resource to send the large Data then first it will stored in Switch and than forwarded.

Advantage :-
- Substitute to circuit Switching. bcz in circuit Switching the whole path is blocked for 2 entities

DisAdvantage :-
- Requires more storage to accomodate entire message.
- Very slow
- Not Suitable for Streaming media and real time application and Hence replaced by Packet Switching.



Types of Transmission Media :-

In Data Communication Terminology a transmission medium is a physical path b/w the transmitter and receiver i.e. it is the channel through which data is sent from one place to another.

Types :-

① **Guided Media** :- It is also referred as wired or bounded Transmission media. Signals being Transmitted are directed and confined in a narrow pathway by using physical links.

Features :- (i) High Speed
(ii) Secure
(iii) Used for Comparatively Shorter Distances.

Major Types of Guided Media :-
① Twisted Pair Cable
② Coaxial Cable
③ Optical fibre Cable
④ Stripline
⑤ Microstripline

UnGuided Media :- It is also referred as wireless or unbounded Transmission Media. No physical medium is required for the transmission of electromagnetic signals.

Features :- (i) The Signal is broadCasted through air.
(ii) Less Secure
(iii) Used for larger distances.

Major types of Signals transmitted through Unguided Media :-
① Radio Waves
② Micro Waves
③ Infra red Waves

DATA LINK LAYER

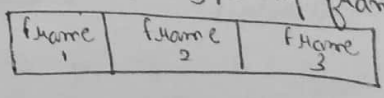
Topics :- Framing, Errors and Flow Control, Error Detection and Correction, Error Detection Methods, Error Correction Methods, Encoding (NRZ, Manchester, 4B/5B), Stop & Wait Protocol, Sliding Window Protocol

★ **Framing** :- We know the Data transmission in physical layer is in the form of bits, on the other hand, Data Link Layer break the bit streams into frames and these frames are having Sender and receiver address.

Now, How can receiver determines the start and end of a frame for this we have Two Types of framing.

① **Fixed Size framing** :- In fixed Size framing, there is no need to define the boundaries of the frame Such type of framing is used in ATM.

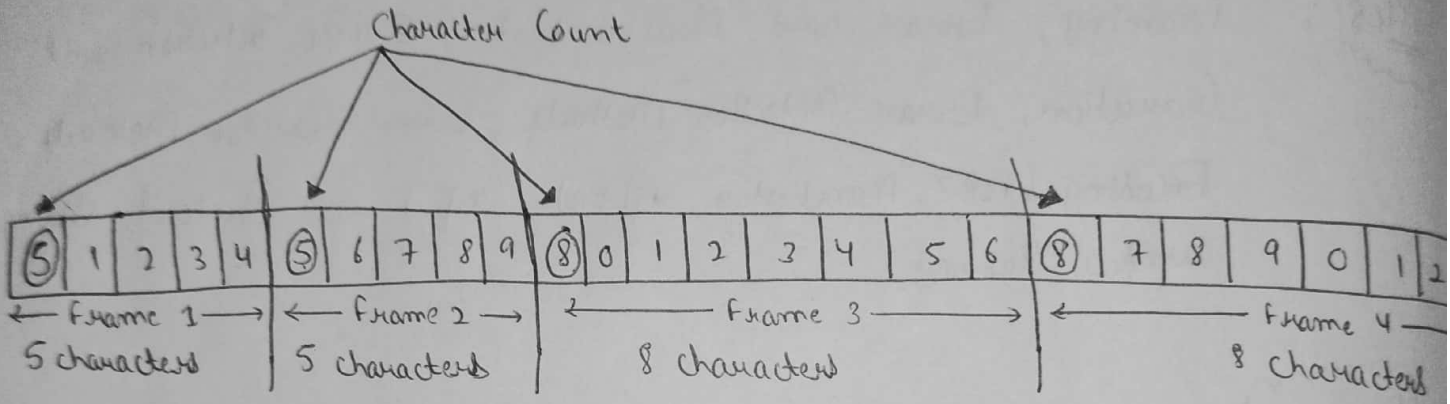
② **Variable Size framing** :- It is widely used in local Area Networks, in this we need to define a end of the frame and begining to the next. There are mainly two broad Categories of variable Size framing (i) character oriented approach
(ii) bit oriented approach



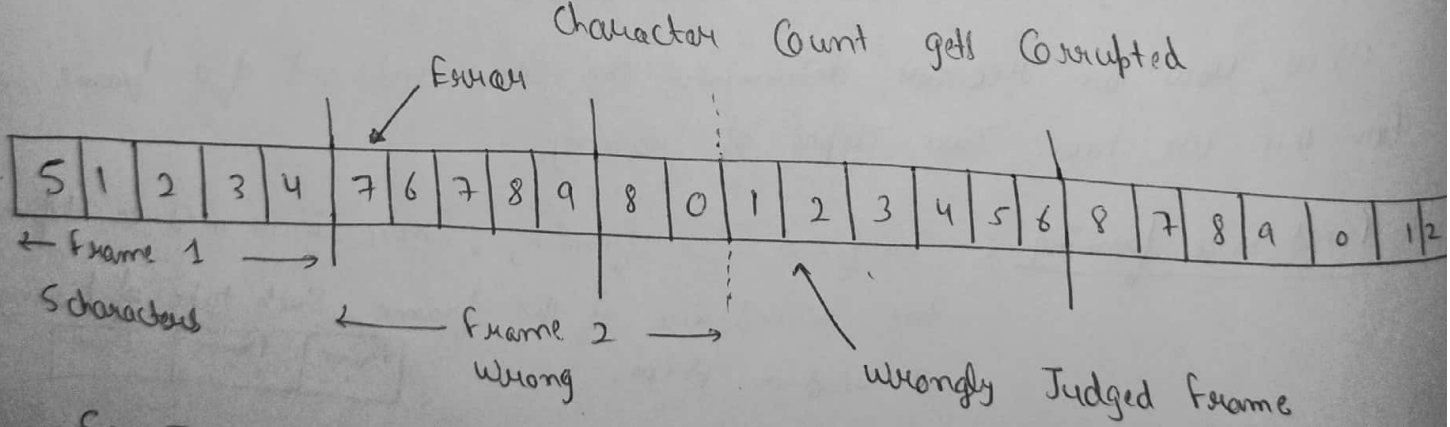
Four framing methods can be used for these approaches :-
(i) Character Count
(ii) Character stuffing
(iii) Bit Stuffing
(iv) Physical layer Coding Violation.

(i) Character Count :- It uses the field in the header to co
ou specify the no. of characters in a fra

Now, in this method, the first value of a frame describes the
no. of characters in that frame and it is for receiver to detern
no. of characters in a frame (ie frame demarkation)



But the trouble arises when character Count value gets corrupted d
transmission



So, To remedy this, we can tell sender to send the whole data
again, so for this reason, this method is rarely used.

(ii) Character Stuffing :-

- Here Each frame starts with ASCII character sequence DLE STX and ends with DLE ETX.

DLE → Data Link Escape
STX → Start of Text
ETX → End of Text

Now, Assume original Data → A B C

then Framing using character stuffing will initialize it with DLE STX and ends it with DLE ETX. bcz However if data changes or corrupted in b/w, the receiver will get the frame acc. to ASCII character sequence.

Framing using character stuffing

DLE STX ABC DLE ETX

But Here the problem is, if the data is Binary, then it will have its own ASCII character

Original Data

A B DLE C D

Framing using character stuffing

DLE STX | A B | DLE | DLE C D | DLE ETX

On seeing this double DLE the receiver wants to know that one DLE is a part of Data itself.

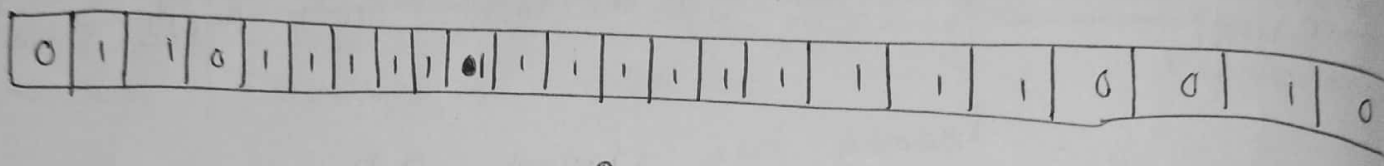
Its Advantage :- This method is tied to 8-bit characters (ASCII) but we need for arbitrary-bit characters, that's why Bit Stuffing come into play.

(iii) Bit Stuffing :- It allows frames to contain arbitrary no. of bits and allows character codes with an arbitrary no. of bits per character

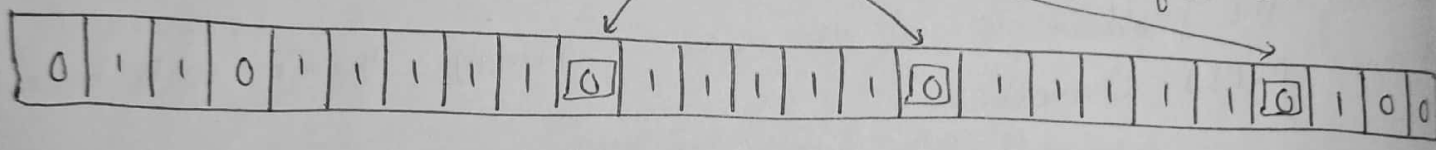
To mark a beggining and ending of frame, we introduce a flag byte which has special bit pattern and this pattern is added to start and end of the frame.

Flag Byte :- 0 1111110

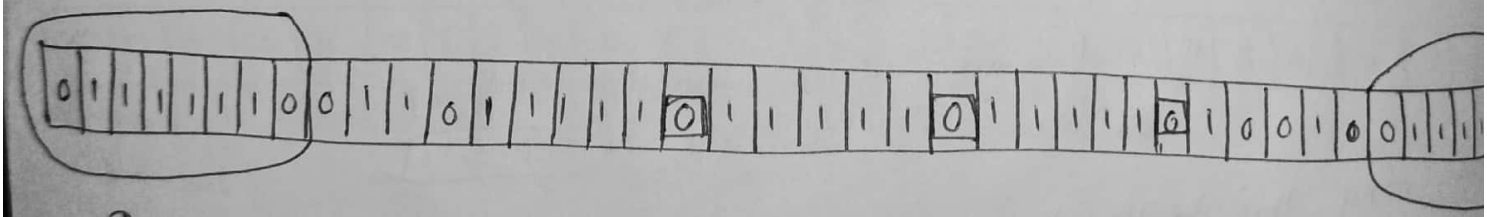
Original Data



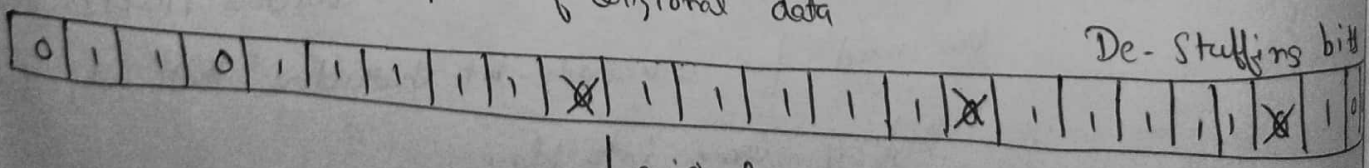
Bit Stuffing :- it will introduce 0, after every five 1's.



Framing using flag byte :-

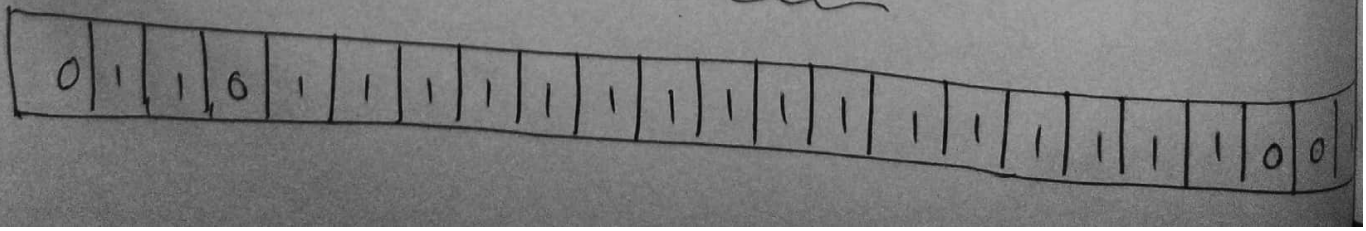


The receivers determines/identifies frame boundaries by seeing the flag. Now, when it sees the 0 after five consecutive ones, it will delete these bits which is not part of original data



De-Stuffing bits

↓ original Data



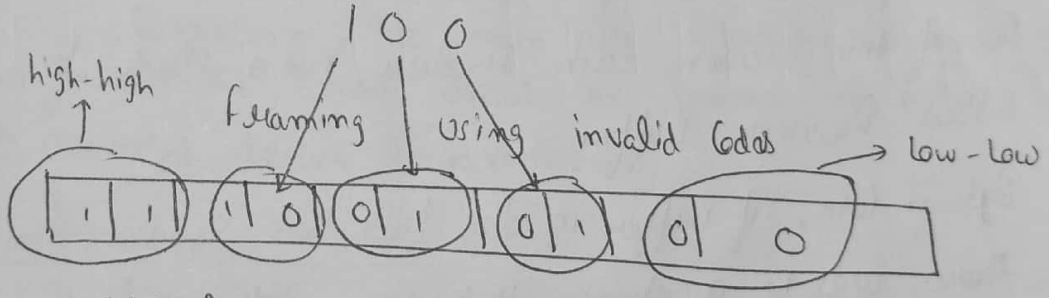
Now, we have Ques. that why we stuff 0 after every five Consecutive 1's, it is bcz, the flag byte has Six Consecutive ones and if data also have Six Consecutive 1's, than the receiver may faces issues while identifying frame boundaries and might declare it to the end of the frame, so To avoid this, we stuff 0 after every 5 Consecutive ones.

iv) Physical Layer Coding Violations :-

- It is applicable to Computer Networks in which encoding on physical medium Contains Some redundancy.

Example :- • Some LAN's encode 1 bit of data using two physical bits.

Original Data



1 bit → high-low pair
0 bit → low-high pair

The Other Combination of low-low and high-high are not used for Data, So these are used to mark boundaries, so the receiver will see Start and end by Seeing these invalid Codes.

Note :- Many Data Link layer protocols use these 4 methods by Combining each other for extra Safety

☆ Flow and Error Control :-

Now, During Communication, it is very important that the Data which is transmitted is error free and this task is done by Data Link layer.

So, Data Link layer works for Flow Control and Error Control

Flow Control :- It is set of Procedures that restrict the amount of Data that Sender can Send before waiting for an acknowledgement. (i.e Sender is allowed to Send packets before the reply of reciever).

Now, it is also important that the Data which is Sent is error free and it is checked at receiving end but it is slow as Compared to the speed of transmission from Sender's end.

Bcz of this reason each reciever has a block of memory, which is Called Receiver Buffer.

Byt in Case, if Buffer is also full but Sender Sends the packet then there will be a chance that Some bits get lost and it is happen when Sender operates on lightly loaded machine and Server operates on highly loaded machine and reciever tells Sender to stop.

"The main reason for flow Control is to increase efficiency of data transfer"

2 Approaches for flow Control :-

① **Feed Back Based flow Control** :- It is used in Data Link layer, Sender will not Sends its next Until, it get feed back from reciever and to Send more Packets.

⇒ **Schemes of feed Back Based flow Control** :-

(i) Stop - Wait Protocol
(ii) Sliding Window Protocol
(iii) Automatic Repeat Request (ARQ)

(2) Rate Based flow Control :- It is used in Network Layer and offered as Traffic Shaping.

It has inbuilt mechanism which controls the rate at which Data is transmitted without getting feed Back from receiver.

- Parameters to control Data flow
  - Average transmission rate for each device (ie. rate of incoming of Packets should be less than rate of outgoing of packets).
  - Each device should assigned a Maximum rate of transmission
  - Limit on the Duration to send the Data at maximum rate.

⇒ Implamentation of Rate based flow Control

- Leaky - Bucket technique.
- Token - Bucket technique.

Error Control :- It Comprised of Error detection and Error Connection, The main task is that the receiver have to tell the Sender about the frames which gets lost or damaged during transmission.

Techniques for Error Detection :-

(i) Parity checking
(ii) Cyclic Redundancy check
(iii) Check Sum

Techniques for Error Corrections :-

(i) Hamming Codes

Note :- If the Data Can't be [redacted] Corrected then it is neccesary for re-transmission of frames and Techniques for re-transmission of frames includes :-

(i) [redacted] Go-Back-N Protocols
(ii) Selective Repeat Protocol

★ Error Detection and Correction :-

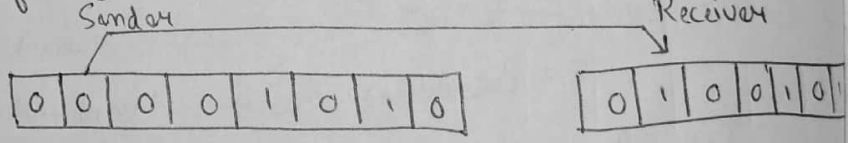
Sometimes During transmission of Data, some errors are occured which we called as transmission errors and Reasons for transmission errors are :-

(i) Thermal Noise
(ii) Signal Distortion
(iii) Cross talk
(iv) Variation in Signal timmings.
(v) Or Sender & receiver are not in Sync

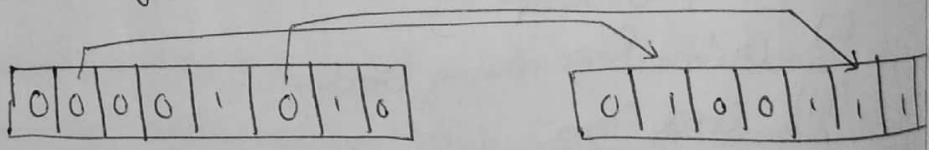
We know Data is transfered in the forms of bits and error occ when these bits gets altered (ie. if 1 changes to 0 or 0 changes to 1

3 Types of Transmission Errors :-

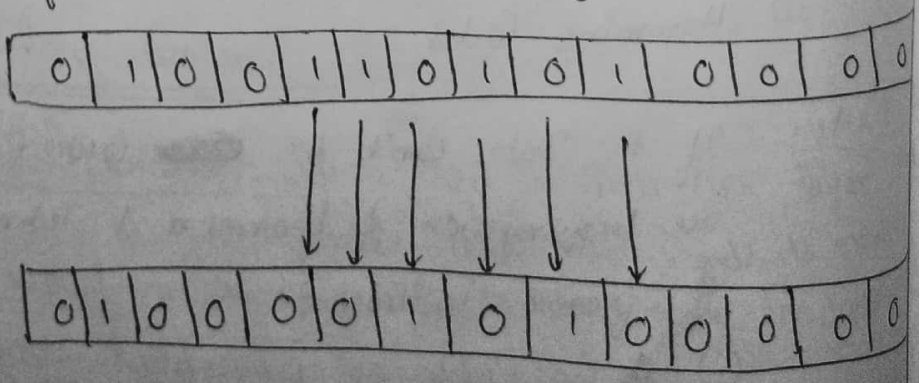
- **Single bit error** : if only one bit is altered.



- **Multiple bit Error** :- if more than one bit is altered



- **Burst Error** :- if more than two 2 Contigous bits are alte



Burst Error Length = 6

* Error Detection Methods :-

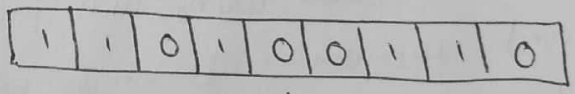
Now, we have Question in my mind, that we have Error Detection and Error Correction techniques than why don't we have a methods which detect and Correct Error at same time, bcz it is not a efficient method as it is time Consuming to deted an error and Correcting it & obtaining the original data, so, re-transmission of Data from Sender after Detecting error is a preffered way.

Error Detection Codes :-

1. Simple parity check
2. Two Dimensional parity check.
3. Check Sum
4. Cyclic Redundancy check (CRC)

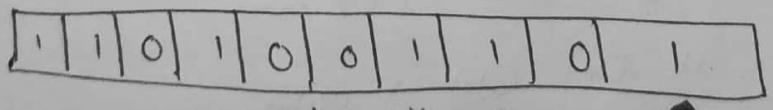
First we will under stand, what is Parity Bit ?

Suppose we have a String of bits



No. of 1 bits = 5

So, if Communicating parts are agreed on Even parity, than a parity Bit will be added of value 1.

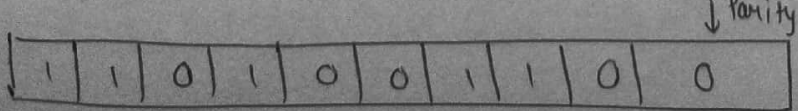


No. of 1 bits = 5

Parity Bit

Even parity
No. of 1 bits should be even

and if there is already even parity & Communication are agreed on Odd parity, than value of 0 will be added or added acc. to maintain its odd parity

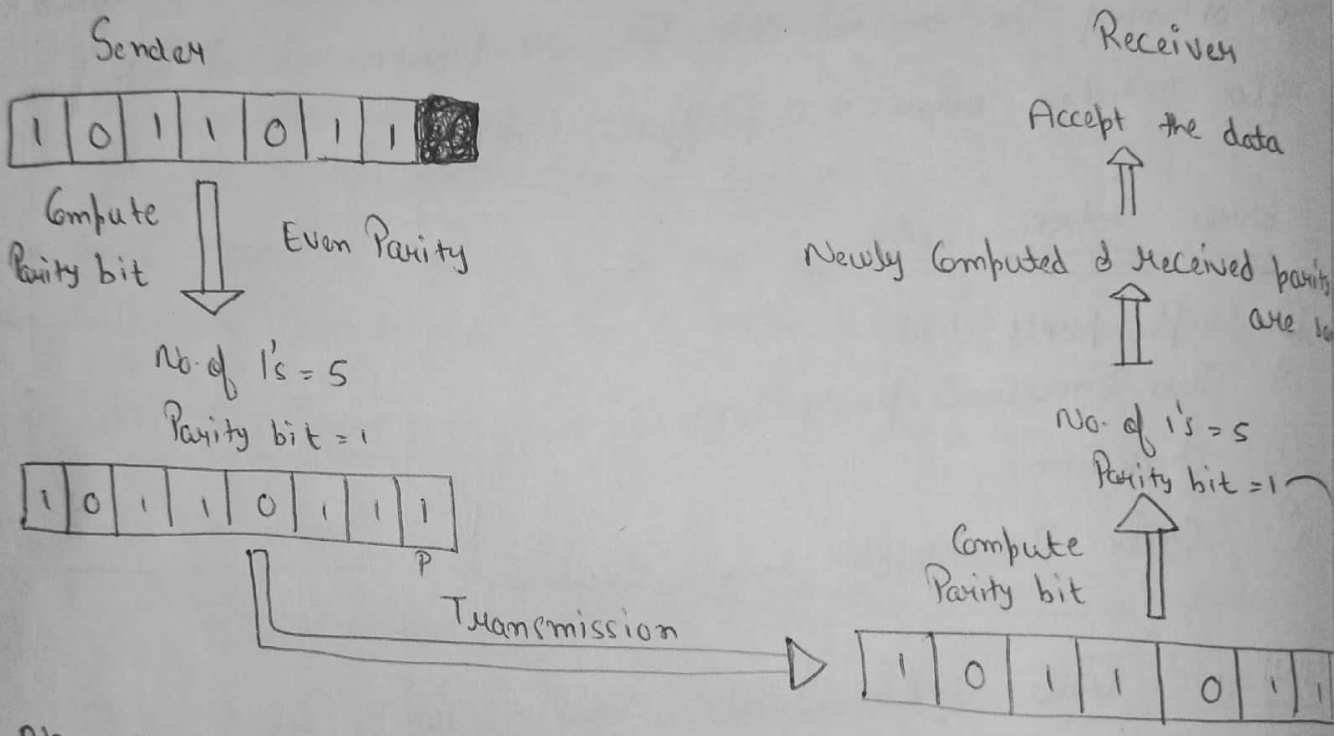


(1) Simple Parity check :-

Now, Lets Suppose Sender wants to send this data 1011011 and both Sender and receiver agreed on even parity.

Now check no. of 1's = 5

So, we have to add Parity bit = 1



now this data along with parity bit will transmit across the net and receiver will know before hand that the last bit is the p bit, then it again counts no. of 1's and compute parity bit, if newly computed & received parity are same, then it accepts the

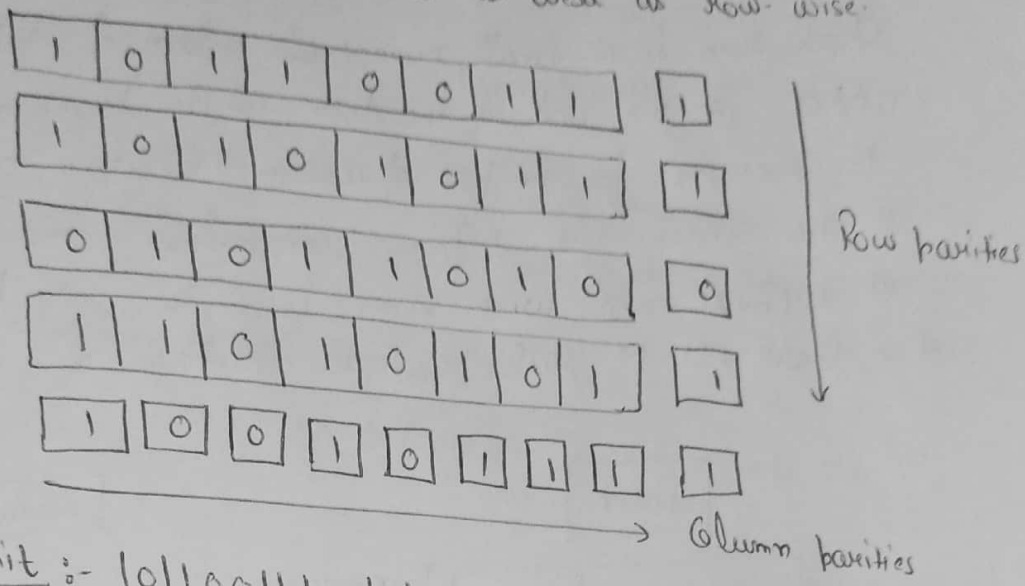
Advantage :- Easy to catch 1 bit error

Disadvantage :- it cant catch multiple errors, hence we can say it catches only single bit errors, not multiple bit burst errors.

② Two Dimensional Parity check :-

- Let us take Data string :- 10110011 10101011 01011010 11010101

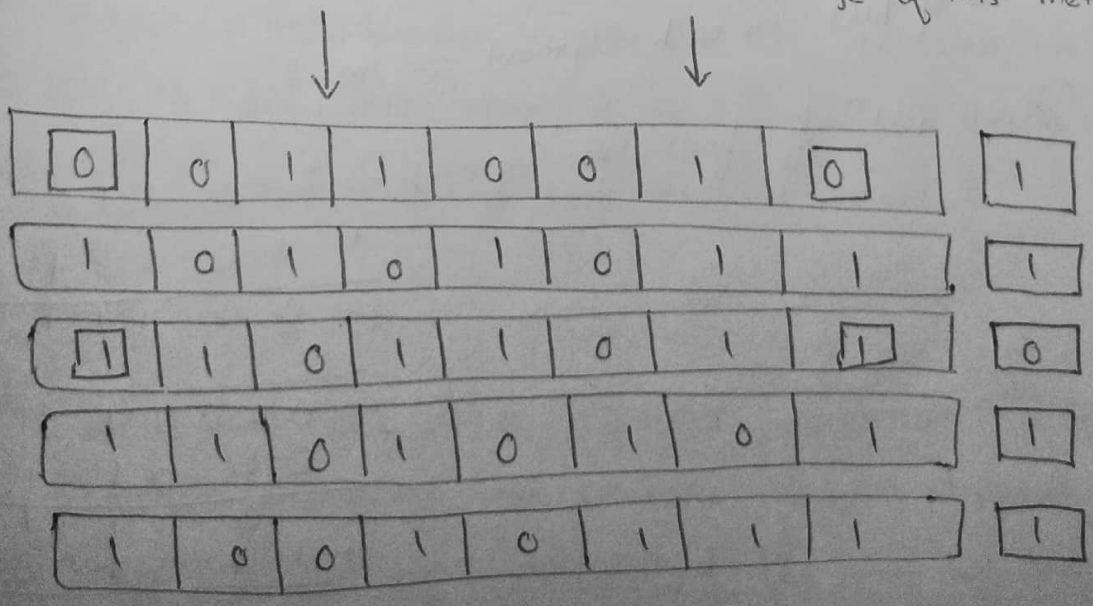
Now Take parities Column-wise as well as row-wise.



- To Transmit :- 101100111 10101011 01011010 11010101 100101111

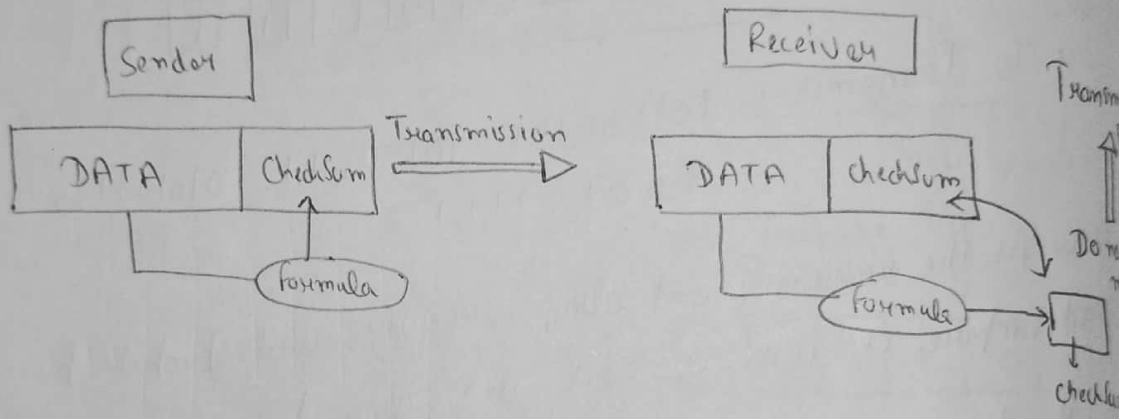
Now At the receiving end also, receiver will Compute parity for 8 bits and Compare it with 9th bit and also for Column

- It detect burst error of n-bits
- If two bits in same position get Corrupted on two rows than error detection is not possible, that is the disadvantage of this method.



③ Check Sum :- This method is widely used for transferring the files over the internet

Check Sum is a small numerical value of data, that will be added at the end of the data while transmitting from sender to receiver for purpose of error detection and it is calculated at the sender end before transmission and then again calculated at receiver end with same formula and if it doesn't match then, there will be will be some chances of transmission error.



⇒ Check Sum Calculation :-

- Data String :- 10110011 | 10101011 | 01011010 | 11010101
- Segments :- k = 4
- No. of bits in each Segment :- m = 8

Now, Add^{n} of first two Segment ⇒

```
  1 0 1 1 0 0 1 1
+ 1 0 1 0 1 0 1 1
-----------------
  0 1 1 1 1 1 1 0
                1
-----------------
  0 1 1 1 1 1 1 1
+ 0 1 0 1 1 0 1 0
-----------------
  1 0 1 1 1 0 0 1
+ 1 1 0 1 0 1 0 1
-----------------
  1 0 0 0 1 1 1 0
+ 1 0 0 0 1 1 1 0
-----------------
  1 0 0 0 1 1 1 1
```

Now Take 1's Complement of result and that will be your checkSum.

Required CheckSum = 0 1 1 1 0 0 0

Now, it will detect errors in two ways

- Approach - 1 :- 1) Perform addition including checksum
  2) Complement the result to check errors

Step-1 :- Addition of all segments :- 1 0 0 0 1 1 1 1

CheckSum :- 0 1 1 1 0 0 0 0

+

1 1 1 1 1 1 1 1

Now, Complement of final result :- 0 0 0 0 0 0 0 0

Now, if final result is zero, then there will not be any error

Now, Verification at Receiver : Approach-2

- Calculate the checkSum of the data part and compare it with the received checkSum
- If both the values are same, accept the data
- This approach is more practical in use as we see, when we download any file, it have some string of no. 8 letters and that is the checksum
- Some of Commonly used checksum methods :-
  1) MD5
  2) SHA-1, SHA-2, etc.

You can get tools and utility softwares, which can calculate MD5, SHA-1 or SHA-2 checksum and compare it with original checksum this way we can ensure integrity of file which we downloaded from the internet.

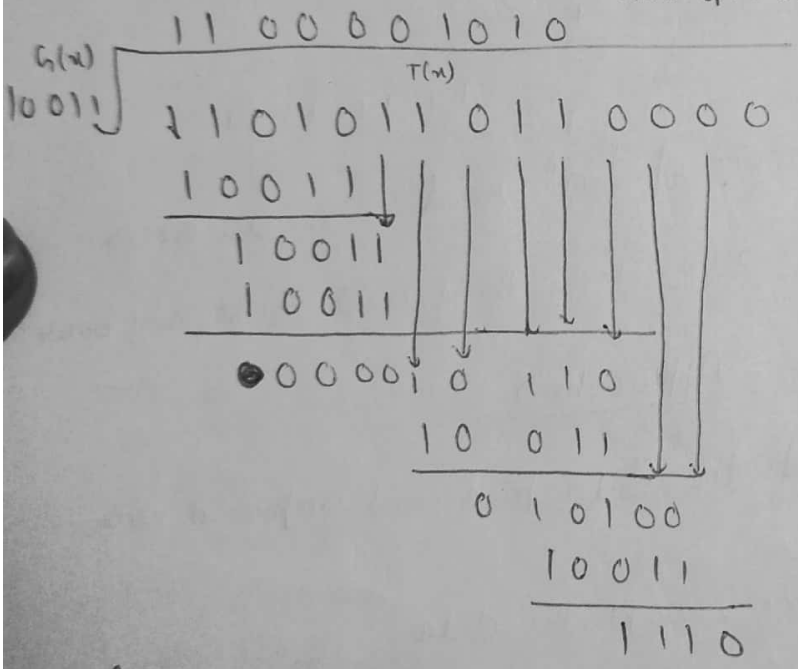
④ Cyclic Redundancy check :-

- Based on binary division
- Redundant bits are appended to data stream
- No remainder = Error free transmission

Now, Assume Data string :- 1101011011

- Let us take Generator polynomial : $x^4+x+1 \Rightarrow 10011$ — G(x)
- it is CRC-4 Polynomial (ie. Degree 4)
- Now Add 4 Zeroes to frame bits
- 1101011011 0000 — T(x)

Now, T(x) | G(x) (by performing XOR operation)



Carry until we have T(x) > G(x) and put 0 in quotient, as many time we carry digit from T(x)

Now add this to data stream

Data to be Sent :-

1101011011	1110

Now at Destination, the receiver will divide it by Generator function.

if the data received is correct, then obviously the remainder should be Zero

Generator functions :-

- CRC-4 x^4+x+
- CRC-12 $x^{12}+x^{11}+x^3+$
- CRC-16 $x^{16}+x^{15}+$
- CRC-CCITT $x^{16}+x^{12}+$

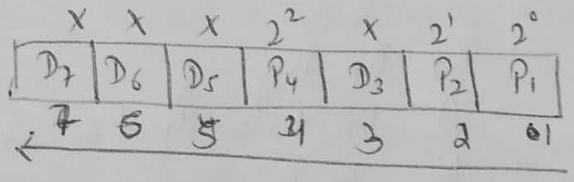
Note :- CRC-16 & CRC- are used for Cat Single bit and double errors.

* Error Correction Methods :-

It is used to detect and correct errors at receiving end. (Hamming Codes)

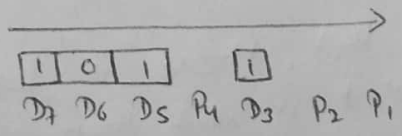
- introduced by Richard Hamming, an American mathematician in 1950
- 7-bit Hamming Codes are used usually
- first convert data to Hamming Codes by appending parity bit

- Now, we will see how to convert 4 bit code to 7-bit Hamming code, but before this, lets see the position for the bit.
- The parity bit will be at position of power of 2 and other bits will be Data bits which sender have to send and the parity bits will be computed acc. to Data bits and its is known as (7,4) Hamming Code



⇒ Generating a Hamming Code :-

- Now, suppose Host A wants to send 1011



Now, P_1 depends upon D_3 D_5 D_7
P_2 ——— D_3 D_6 D_7
P_3 ——— D_5 D_6 D_7

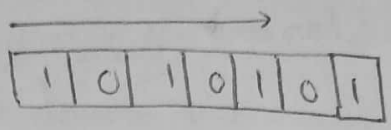
Now, Before Generating Hamming Code, the Sender and Receiver must have to be agreed on even or odd parity bit, Let us suppose they agreed on even parity bit.

Now, $P_1 \rightarrow$ D_3 D_5 D_7
1 1 1 $\Rightarrow P_1 = 1$ [To set even Parity]

$P_2 \rightarrow$ D_3 D_6 D_7
1 0 1 $P_2 \Rightarrow 0$

$P_4 \rightarrow$ D_5 D_6 D_7
1 0 1 $P_4 \Rightarrow 0$

Data have to sent :-



Now, Lets Suppose there is some error;

Now, How Receiver will detect the error and Correct it
This will done with the help of parity bits. Let's take Cond^n

A 1010101 ⟶ B 1010001

Now it will check Values of parity bit at its receiving end (i.e. one by one

At B :- $P_1 \rightarrow$ D_3 D_5 D_7
0 1 1 $P_1 = 0$ but at A, $P_1 = 1$

$P_2 \rightarrow$ D_3 D_6 D_7
0 0 1 $P_2 = 1$ but at A, $P_2 = 0$

$P_4 \rightarrow$ D_5 D_6 D_7
1 0 1 $P_4 = 0$ same as A

Now, it is clear that, there is some error during transmi
Now we will detect in which there was an error, this can be don
parity bits, write those bits from left to right in binary form

P_4 P_2 P_1 0 1 1 → Convert it to decimal → $0+2+1 = 3$

So, 3rd bit will be Corrupted and there will be error in D_3
it must be (1) not '0' bcz Data is in binary form.

★ Encoding (NRZI, Manchester, 4B/5B) :-

Encoding involves the use of a code to change original Data into a form that can be used by an external process or with which a Computer can deal with.

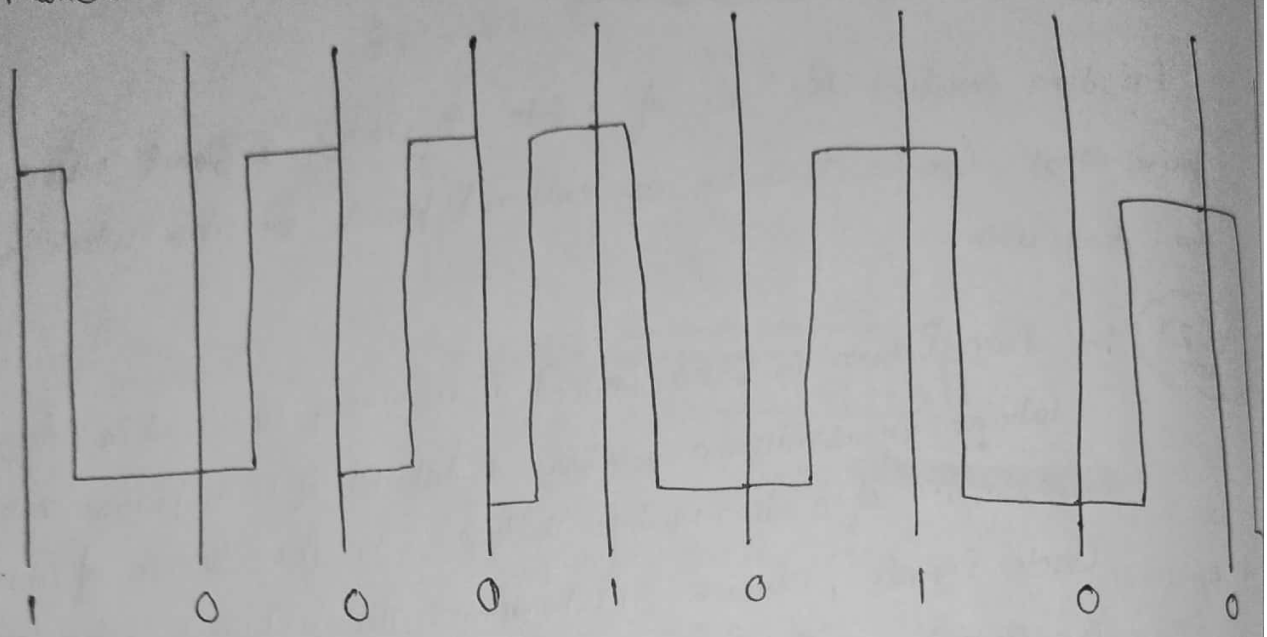
NRZI :- Non Return to Zero (NRZ) is a binary code used in telecommunications transmission, where a data bit of 1 is positive voltage, and a data bit of 0 is negative voltage. In the absence of independent clock signals, certain mechanisms are required when NRZ data is asynchronously coded. NRZI maps binary signals to physical signals during transmission. If a data bit is 1, NRZI transitions at the clock boundary. If a data bit is 0, there is no transition. NRZI may have long series of 0s and 1s, resulting in clock recovery difficulties.

Manchester :- Before understanding Manchester Encoding lets go back a little and understand what is line Encoding. Line Encoding is process of converting digital data into digital signals. This process converts a sequance of bits (data) into digital signal. There are different schemes of Line Encoding.

Manchester Encoding is one of schemes. In Manchester Encoding, the duration of bit is divided into two halves. The voltage remains at one level during the first half and moves to other level in the second half. The transition at the middle of the bit provides synchronisation, so 1 and 0 are designated as :-

0 is ⌋ 1 is ⌈

Consider the bit value 1000101001. This is how it would like if Manchester Encoding is used.



There are advantages to Manchester Encoding. There are is DC Component required because each bit has a positive as well as N voltage Contribution.

4B/5B :- This Coding Scheme is used in Combination with NRZ-I. The problem with NRZ-I was that it had a Synchroni problem for long sequences of zeros. So, to overcome i Substitute the bit stream from 4-bit to 5-bit data group encoding it with NRZ-I. So that it does not have a lo of zeros. The block-coded stream does not have more than th Consecutive zeros. At the receiver, the NRZ-I encoded digi is first decoded into a stream of bits and then decoded again to remo Redundancy bits.

Drawback :- Though 4B/5B encoding solves the problem of Synchro it increases the signal rate of NRZ-I. Moreover, it solve the DC Component problem of NRZ-I.

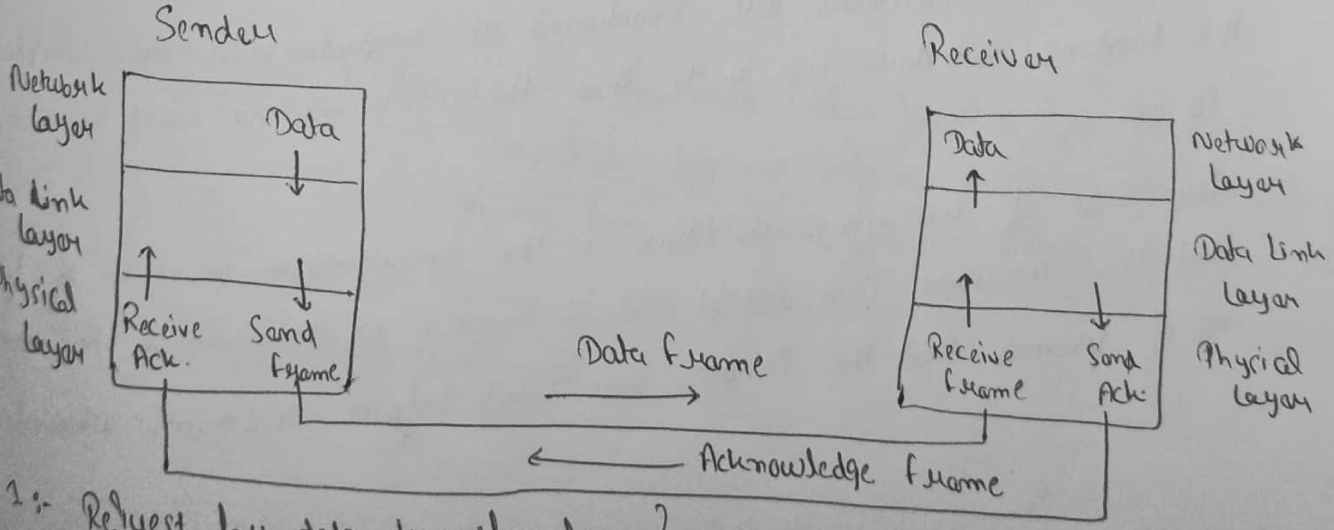
Stop and Wait Protocol :-

Stop-and-Wait Protocol is Data link Protocol for transmission of frames over noiseless channels. It provides unidirectional Data transmission with flow control facilities but without Error control facilities.

Design :-

① Sender Site :- The Data link layer in the Sender Site waits for the Network layer for a data packet. It then checks whether it can send the frame. If it received a positive notification from the physical layer, it makes frames out of the data and sends it. It then waits for an acknowledgement before sending the next frame.

② Receiver Site :- The Data link layer in the receiver site waits for a frame to arrive. When it arrives, the receiver processes it and delivers it to the network layer. It then sends an acknowledgment back to the sender.



Event 1 :- Request for data transfer from Network layer

Event 2 :- Acknowledgement Notification from Physical layer

Action :- Execute Sender Algorithm

Event 1 :- Arrival of frames in physical layer.

Actions :- Execute receiver Algorithm.

★ Sliding Window Protocol :-

Sliding Window Protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window Protocol is also used in Transmission Control Protocol.

In this Protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgement from the receiver. The term sliding window refers to the imaginary boxes to hold frames. sliding window method is also known as windowing.

Working Principle :- In these Protocols, the sender has a buffer called the sending window and the receiver buffer called receiving window.

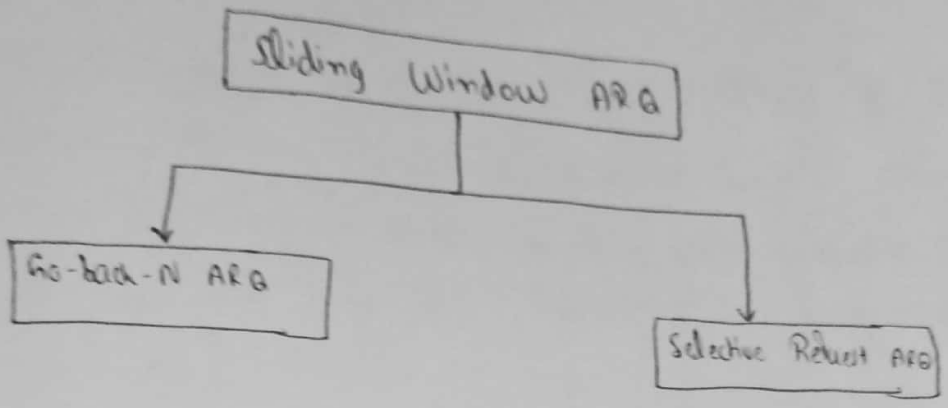
The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n bit field, then the range of sequence numbers that can assigned is 0 to $2^n - 1$. Consequently the size of sending window is $2^n - 1$.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence no. will be 0, 1, 2, 3 and so on.

The size of receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum no. of frames that the sender can send before receiving acknowledge

Two Types of Sliding Window Protocols :-

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories :-



① Go-back-N ARQ :- It provides for sending multiple frames before receiving the acknowledgement for the first frame. It used the concept of sliding window and so is also called sliding window protocol. The frames are sequentially numbered and a finite no. of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are re-transmitted.

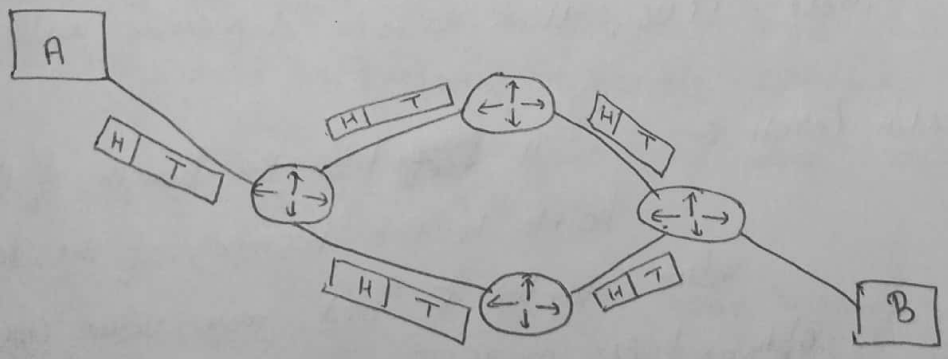
② Selective Repeat ARQ :- This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only erroneous or lost frames are retransmitted, while the good frames are received and buffered.

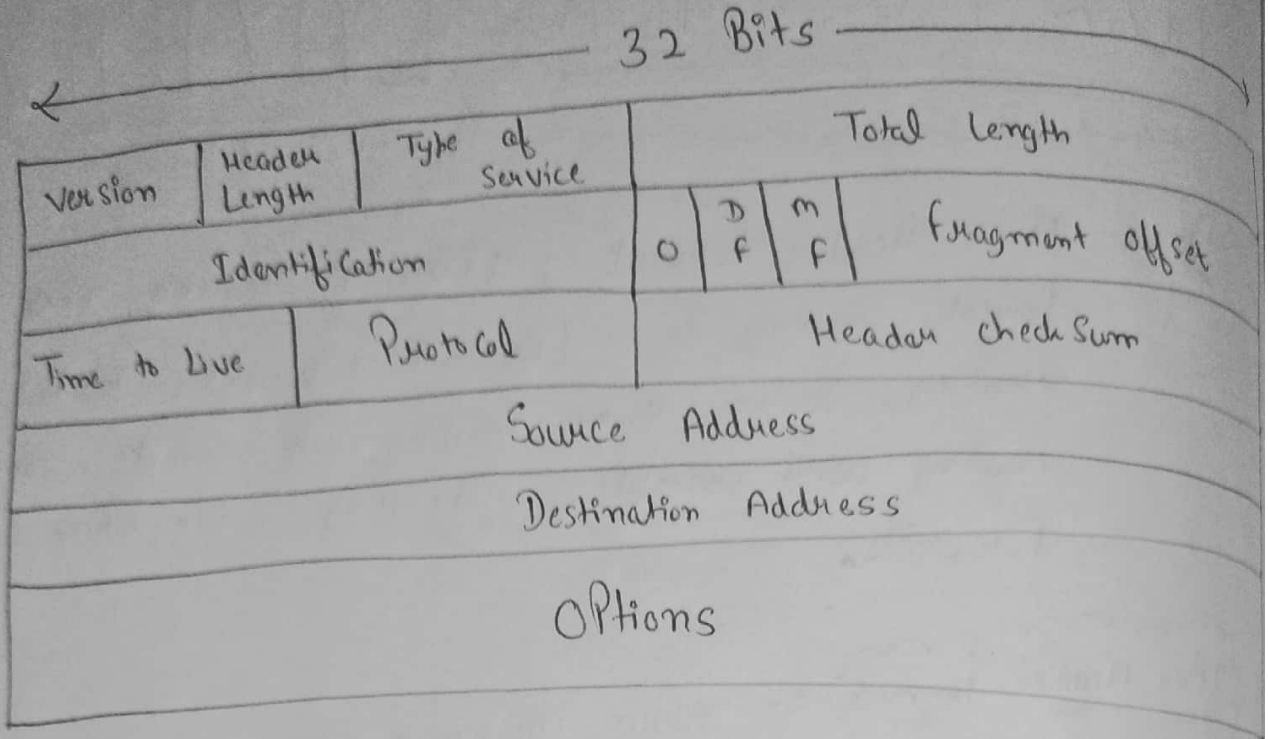
NETWORK LAYER

Topics :- IPv4 Header format , IPv4 Addressing, IPv6 Header format, Routing Basics (Network as Graph) , Shortest Path routing, Distance Vector routing with example , Link State routing with example , Subnetting , Congestion Control, Fire walls.

IPv4 Header format :- Now we know when the Data transmits through network layer from A to B, it is transffered in Datagrams , The Datagram has two parts , a header an a Text

A Text Contains the Real Data to be exchanged and A Header part has Control information.





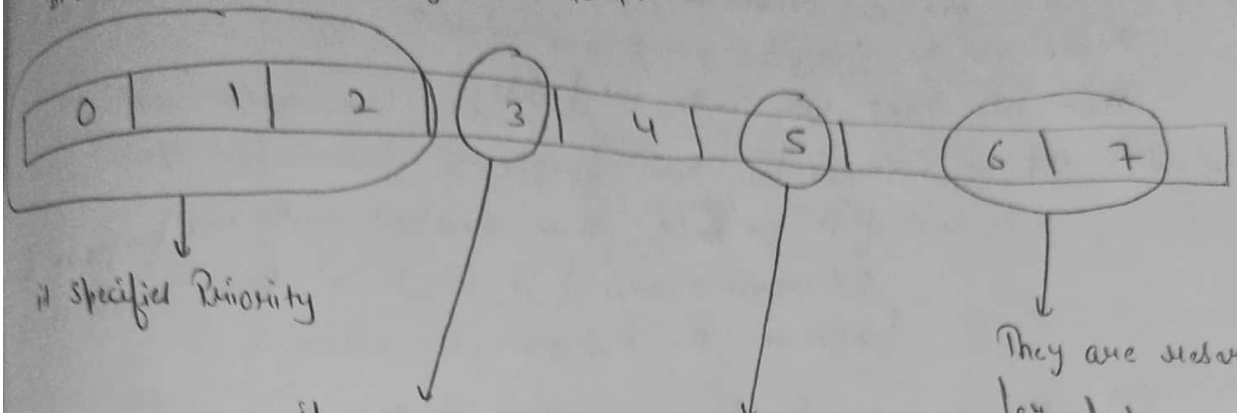
① Version :- . It is a very first field in the Header
. It is 4 bits long
. It tells to which version of Internet protocol, a Dat belongs (ie for IPV4 - 4, IPV6 - 6).

. Now suppose data version is not present and datagr is of IPV4 and if it reaches the node, which only han Handle, IPV6, then whole datagram will be interpreted i

② Header Length :- . It tells the length of the IP Header points to the beginning of the Data, its minim value can be 5 and max. value can be 15, so the option field can be $10 \times 32 = 320$ bits or 40 Bytes long

③ Type of Service :- Using this field a host can tell the server type of service it wants, Hence datagrams are treated equally over the Network, Some datagrams to transmit at higher speed but some have to transmit as error Ex:- In teleconference → speed, In file Transfer → Error free Transf

Now, This feild can be 8 bit long.
Bits are numbered from 0 to 7.



if specified Priority

If it Sets to '1', than Low Delay can be expected but if it is set to '0', than normal Delay is ok.

If it is Set to '1' than high reliability is expected but if Set to '0', than normal Quality of Service will be provided by default.

They are reserved for future use.

③ Total Length :-
- It 16 bits long
- It determines the size of datagram containing the lengths of both Header and Data.
- The Upper limit is $2^{16} - 1 = 65,535$ bytes but in practice most of the hosts and network cant handle such datagrams but all hosts must be prepared to handle 576 bytes atleast.

④ Identification :-
- It is 16 bits long.
- This helps destination node to identify the fragments which belongs to same data Datagram, all fragments of the Datagram will have the same identification value
- Using this key information, the destination reassembles all the fragments of a datagram.

(6) Now we have 3 Control flags :-

The first one is unused bit with value 0, it is reserved and should not be changed

Then we have two single bit fields

(i) DF :- • Stands for Dont fragment
• if it set to '1', then routers will not fragment the Datagram and if it set to '0' then router will fragment the datagram if required

(ii) MF :- • Stands for more fragments
• if its value is '1', then it means more fragm of Datagram have to arrived at destination and the last fragment of Datagram will have the M value set to '0', this way it tells the destination th i, am the last fragment belonging to this datagram.

(7) Fragment Offset :- • It is 13 bits long
• it tells the location of fragment in Dat
• In this way destination will get to know how assemble all the fragments.

(8) Time to Live :- • Maximum Time allowed is 255 Sec
• When a Datagram goes from one node to an is treated as one hop and at each hop the time decremented by one and if it reaches '0' then datag will be discarded.
• And a warning datagram will be sent to sender with this counter it will be very diffi cult to monitor a datagr which we wantbe forever, Such situation occurs when routing tables are corrupted or the routers are not able to fo the Datagram.

(9) Protocol :-
- It is 8 bits long.
- It indicates the next level protocol used in the Data portion of the internet Datagram.
- Now when the Network layer assembles all the Data then protocol will tell which transport process should give it to.

Ex :- TCP → 6
UDP → 17
} assigned No:s

(10) Header Check Sum :-
- It is 16 bits long
- it is used to detect Errors in Header
- it is recomputed at every hop.

(11) Source Address And Destination Address :-
- It is 32 bits long containing source and destination IP Address respectively
- Source Address will acknowledge routers in the Network and Destination Address will helps it to where to send the Datagram.

(12) Options :-
- The options may or may not appear in Datagram.
- It is variable in length.
- Each option is occupying 1 byte code identifying the option.

Lets See options :- (i) Security
(ii) Strict Source routing
(iii) Loose Source routing
(iv) Record route
(v) Timestamp, etc.

⇒ REAL IPV4 Header looks like :-

⊟ Internet Protocol Version 4, Src : 192.168.2.1 (192.168.2.1),
Dst : 239.255.255.250 (239.255.255.250)

Version : 4

Header length : 20 bytes

⊟ Differentiated Services Field : 0x00 (DSCP 0x00 : Default; ECN: 0x00 : Not-ECT (Not ECN-Capable Transport))
0000 00.. = Differentiated Services Codepoint : Default (0x00)
.... ..00 = Explicit Congestion Notification : Non-ECT (Not ECN-Capable Transport) (0x00)

Total Length : 353

Identification : 0x 0000 (0)

⊟ Flags : 0x02 (Don't Fragment)
0... ... = Reserved bit : Not Set
.1.. ... = Don't Fragment : Set
..0. ... = More Fragments : Not Set

Fragment offset : 0

Time to Live : 4

Protocol : UDP (17)

⊞ Header Checksum : 0x c2c8 [validation disabled]

Source : 192.168.2.1 (192.168.2.1)

Destination : 239.255.255.250 (239.255.255.250)

IPv4 Addressing :-

It is very important to know about the device which is connected to the Internet

- IP = Unique Identification number
- It defines one and only one connection to the internet
- On the Internet two devices can never have same Address.
- Device with two connections to the internet via two networks has two IPv4 addressing

- **Two Notations :-** Decimal form & Binary form

A

IP (Decimal) :- 192.168.10.8

IP (Binary) :- 1100 0000 - 1010 1000 - 0000 1010 - 0000 1000

Decimal form is compact and easier to read

Now, **IPv4 Addressing space is divided into 5 classes**

- Special ranges of contigous IP address
- First four bits are most significant bits

IP address space classes :-

- Class A ranges from 0.0.0.0 - 127.255.255.255
- Class B ranges from 128.0.0.0 - 191.255.255.255
- Class C ranges from 192.0.0.0 - 223.255.255.255
- Class D ranges from 224.0.0.0 - 239.255.255.255
- Class E ranges from 240.0.0.0 - 255.255.255.255

A = 0-128

B = 128-192

C = 192-224

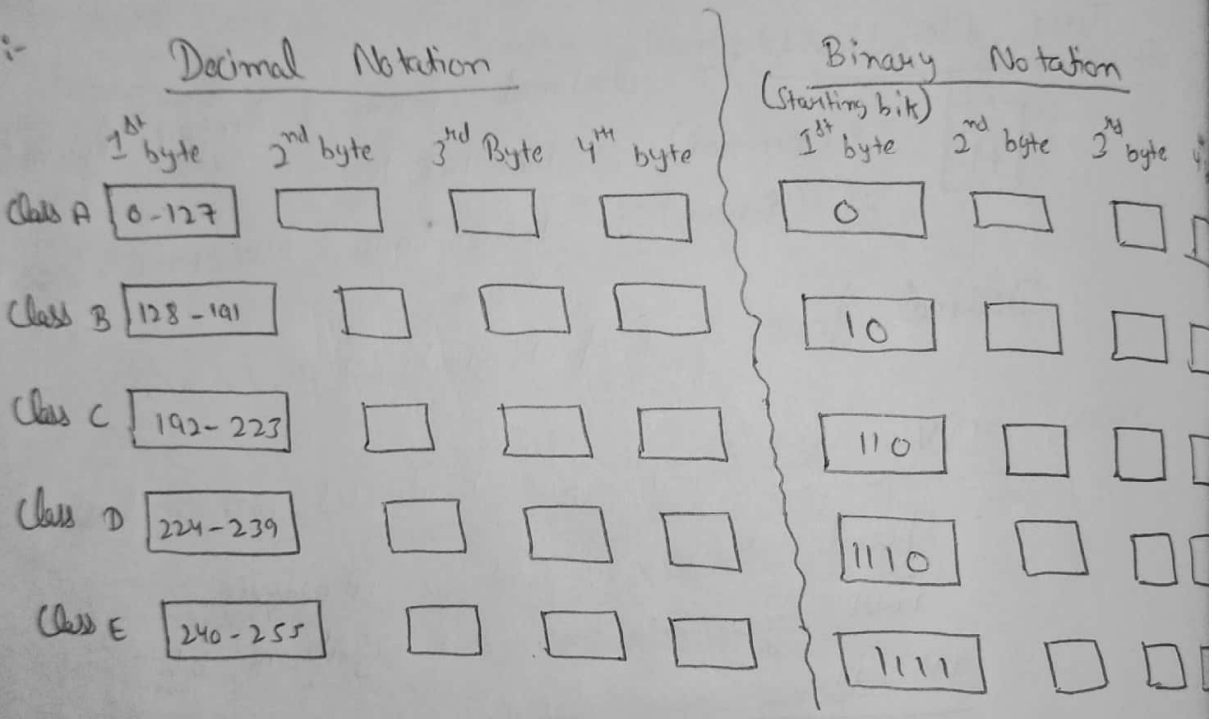
D = 224-240

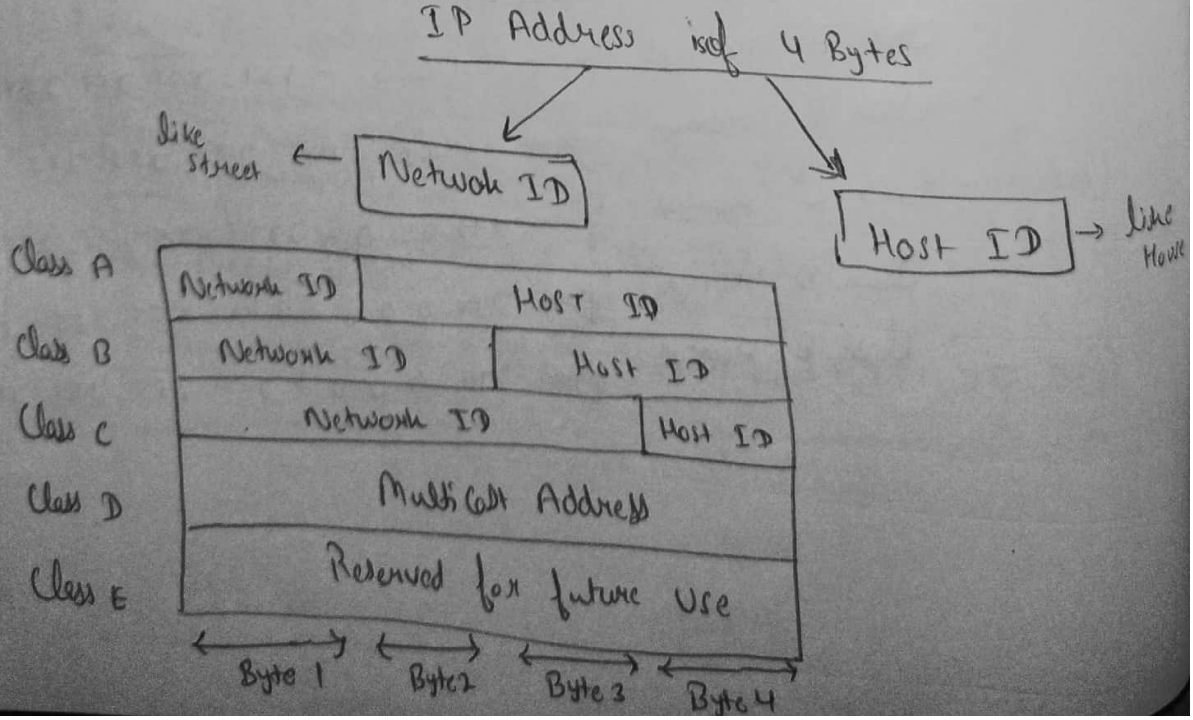
E = 240-256

- Class D addresses are used for multicast addressing
- Class E is reserved for experimental Purposes.
- and some addresses are used for private connections like for an organization or a bank.
- IANA reserved some addresses for these private Networks (i.e. "Internet Assigned Number Authority").

Now, To Determine class By looking at Binary Notation

Trick :-





In class A :- Network ID has 1 byte, it means 8 bits in which left most bit = 0

So, ∴ Total no. of Network ID = 2^7

Host ID has 3 bytes, it means 24 bits

So, ∴ Total no. of Host ID = 2^{24}

In class B :- Network ID has 2 bytes, it means 16 bits in which two left most bits are '1,0'

So, ∴ Total no. of Network ID = 2^{14}

Host ID has 2 bytes, it means 16 bits

So, ∴ Total no. of Host ID = 2^{16}

In class C :- Network ID has 3 bytes, it means 24 bits in which three left most bits are '110'

So, ∴ Total no. of Network ID = 2^{21}

Host ID has 1 byte, it means 8 bits

So, ∴ Total no. of Host ID = 2^8

★ IPV6 Header format :-

Why IPV6 ?

→ ① Need for more IP addresses
- 128 bits long
- 2^{128} addresses are available = 3.4×10^{38} addresses

② it has 8 groups seperated by Colons, in each group there will be four Hexadecimal digits

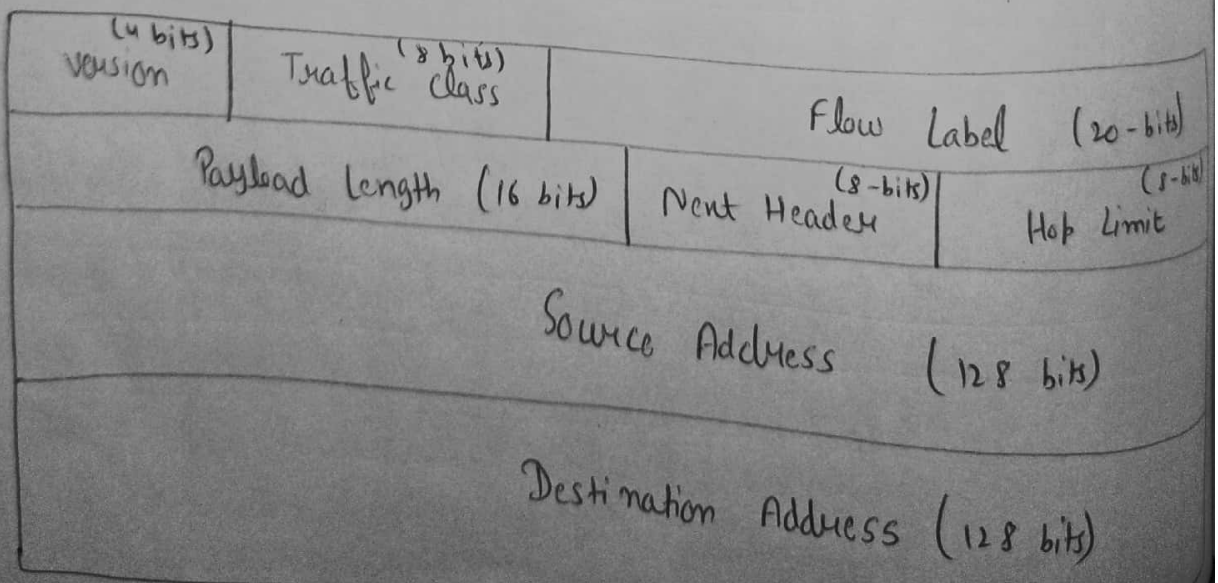
FE80 : 140E : 0956 : FC05 : 0202 : B3FF : FE1E :

③ Header is Simple
- Routers can process faster

④ Better support for options
- Some fields which are compulsory in IPV4, will now optional in IPV6, so that now router can skip these fields and packets will process faster.

⑤ Security → allows complete end to end Security.

⑥ Better Quality Service.



(1) Version :- (a) This tells software running on the node interpreted as Version 6 structure

(2) Traffic class :- (a) It is 8 bits long.
(b) Used to differentiate Payloads with different delivery requirements.
(c) It replace Service type field of IPV4.

(3) Flow label :- (a) It is 20 bits long
(b) Use to label the sequence of packets for its handling by IPV6 routers such as real time service

(4) Payload length :- This tells the length of IPV6 Payload (ie. the part after IPV6 Header), value will be in terms of bytes.

(5) Next Header :- (a) It is similar to protocol field in IPV4
(b) It identified the type of Header.

(6) Hop Limit :- (a) It is 8 bits long.
(b) It is same as time to live in IPV4, that means the life of the datagram is 255 sec and time is decremented by one at each hop and if it goes to '0' then it will be discarded.

(7) Source Address :- It is 128 bits long and have address of sender

(7) Destination Address :- It is also 128 bits long and have address of receiver.

★ Routing Basics (Network as Graph) :-

Routers use routing algorithms to find the best route to a destination. When we say "best route", we consider parameters like the number of hops, time delay and communication cost of packet transmission.

We have two major routing Algorithms :-

① Global routing Algorithms :- In this, every router has complete information about all other routers in the network and the traffic status of the network. These algorithms are also known as LS (Link State) algorithms.

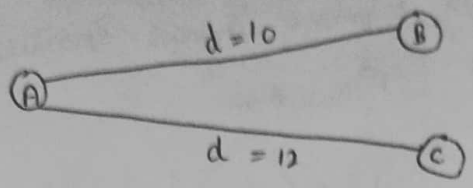
② Decentralized routing Algorithms :- In this, Each router has information about the routers it is directly connected to -- it doesn't know about every router in the network. These algorithms are also known as DV (Distance Vector) algorithms.

★ Shortest Path Routing :-

Data Transfer operations is a crucial aspect in case of networking and routing. So Efficient data transfer operations is a must need, with minimum hardware cost and also minimum time possible.

Lets see a completely new Algorithm unlike Dijkstra's Algorithm

Given a graph and two nodes (source node and Destination node), find the shortest path b/w them



Let's calculate the Distance ratio for each link :

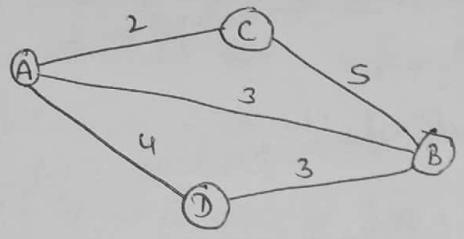
Distance of link AB (d(AB)) = 10

Distance of link AC (d(AC)) = 12

for link AB, Distance ratio of AB - d(AB) | d(AB) + d(AC)

for link AC, Distance ratio of AC - d(AC) | d(AB) + d(AC)

Now, Example :-



Now, All Possible paths are $P_1 = A \rightarrow B$

$P_2 = A \rightarrow C \rightarrow B$

$P_3 = A \rightarrow D \rightarrow B$

Total Distance (D) = $d(P_1) + d(P_2) + d(P_3)$

$= (3) + (2+5) + (4+3)$

$= 17$

Distance ratio for $P_1 = d(P_1) / D = 3/17$

Distance ratio for $P_2 = d(P_2) / D = 7/17$

Distance ratio for $P_3 = d(P_3) / D = 7/17$

So, The shortest Path is $P_1 = [A \rightarrow B]$

Algorithm :- We already done this in DSA Part.

★ **Distance Vector routing** :- A Distance-vector routing (DVR) protocol requires that a router informs its neighbours of topology changes periodically. It is also known as Bellman-Ford Algorithm.

Bellman Ford Basics :- Each router maintains a Distance Vector table containing the distance b/w itself and all possible destination nodes.

- Each router has an ID.
- Associated with each link connected to a router, there is a link cost
- Intermediate hops

Distance Vector Table Initialization –

- Distance itself = 0
- Distance to all other routers = infinity number

Distance Vector Algorithm :-

① A router transmits its distance vector to each of its neighbours in a routing packet.

② Each router receives and saves the most recently received distance vector from each of its neighbours.

③ A router recalculates its distance vector when :

(i) it receives a distance vector from a neighbour containing different information than before.

(ii) it discovers that a link to a neighbour has gone down

The DV calculation is based on minimizing the cost to each Destination

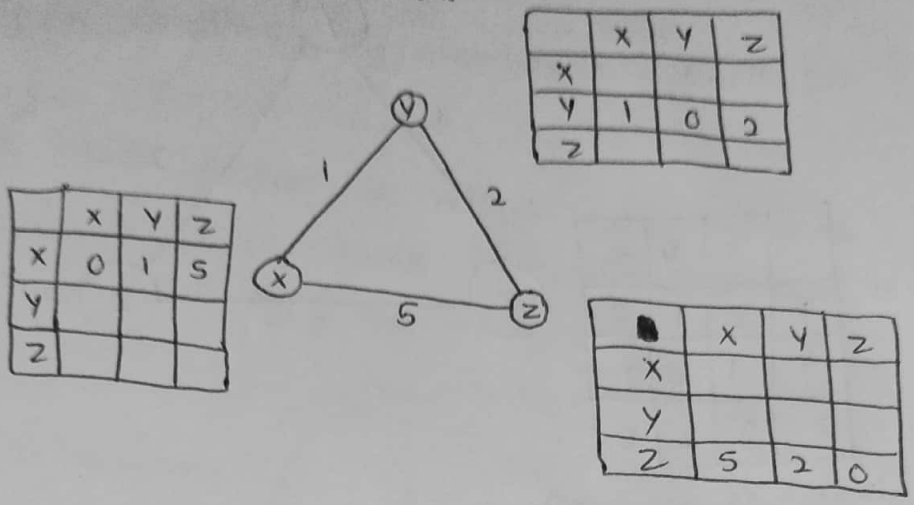
$D_x(y)$ = Estimate of least cost from x to y

$c(x,v)$ = Node x knows cost to each neighbour v

$D_x = [D_x(y) : y \in N]$ = Node x maintains distance vector

Node x also main...

⇒ Example :- Consider 3 routers X, Y and Z. Each router have their Routing table. Every Routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

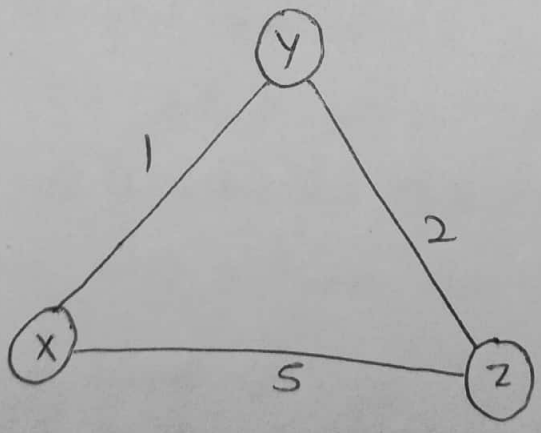
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X, X will share it routing table to neighbours and neighbours will share it routing table to it to X and distance from node X to destination will be calculated using bellman - ford equation

$$D_x(y) = \min\{\{c(x,v) + D_v(y)\} \text{ for each node}\} \quad y \in N$$

As we can see that Distance will be less going from X to Z when Y is intermediate node (hop) so it will be update in routing table X.



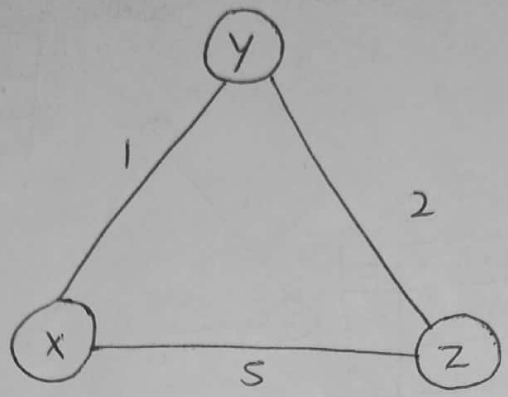
	X	Y	Z
X			
Y	1	0	2
Z			

2 via Y

	X	Y	Z
X	0	1	~~3~~
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Finally the routing table for all-



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

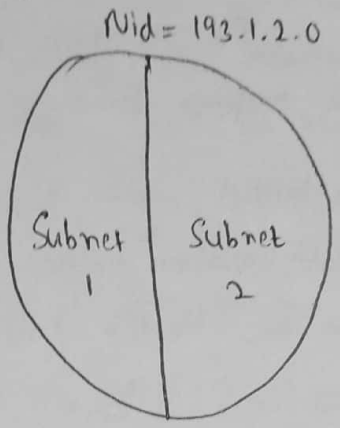
	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Note :- It uses UDP.

★ Link State Routing :-

* **Subnetting** :- When a bigger network is divided into smaller networks, in order to maintain security, then that is known Subnetting. So, maintenance is easier for Smaller Networks.

Now Let talk about dividing a network into two parts :
So to divide a network into two parts, you need to choose one bit for each Subnet from the host ID Part.



Nid = 193.12.10000000

Range = 193.12.00000000
to
193.1.2.01111111

Nid = 193.1.2.10000000

Range = 193.1.2.10000000
to
193.1.2.11111111

Note :- It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

- For Subnet-1 : The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is choosen zero for Subnet id part.

Thus the range of Subnet -1
193.1.2.0 to 193.1.2.127

- For Subnet-2 :- The first bit chosen from the host id part is one and the range will be from (193.1.2.10000000 till you get all 1's in the host ID part ie., 193.1.2.11111111). Thus the range of Subnet -2 :

193.1.2.128 to 193.1.2.255

Note :- ① To Divide a Network into four (2^2) parts you need to choose two bits from host id part for each subnet, ie (00, 01, 10, 11).

② To Divide a Network into eight (2^3) parts you need to choose three bits from host id part for each subnet ie (000, 001, 010, 011, 100, 101, 110, 111) and so on.

* Congestion Control :- A state occurs in the network layer when the message traffic is so heavy that it slows down network response time.

Now Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at a constant rate. When the bucket full of water additional water entered spills over the sides and is lost.

Similarly, each network contains a leaky bucket. The leaky bucket algorithm enforces output patterns at average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. one such algorithm is token bucket algorithm.

In Token bucket algorithm, tokens are generated at each tick. For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduce some amount of flexibility in the system.

* Firewall :- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific rate.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply.

A firewall establishes a barrier b/w secured internal networks and outside untrusted network, such as the Internet.

Firewall use four mechanisms to restrict traffic. one device or application may use more than one of these to provide in-depth protection. The four mechanisms are packet filtering, circuit-level gateway, Proxy Server, and application gateway

(i) Packet Filtering :- A packet filter intercepts all traffic to and from the network and evaluates it against the rules you provide. Typically, the packet filter can access the source IP address, source port, destination IP address and destination port. It is these criteria that you can filter to allow or disallow traffic from certain IP addresses or on certain ports.

ii) Circuit-Level Gateway :- A circuit-level gateway blocks all incoming traffic to any host but itself. Internally, the client machines run software to allow them to establish a connection with the circuit level gateway machine. To the outside world, it appears that all communication from your internal network originated from the circuit-level gateway.

(iii) Proxy Server :- A Proxy Server is generally put in place to boost the network's performance, but it can act as a sort of firewall as well. Proxy Servers hide your internal address so that all communications appear to originate from the proxy server.

A Proxy Server caches Pages that have been requested. If User A goes to yahoo.com, the proxy server sends the request to yahoo.com and retrieves the Web Page. If User B then connects to yahoo.com, the proxy server sends the information it retrieved for User A, So it is returned faster than having to get it from yahoo.com again.

(iv) Application gateway :- It is another sort of proxy server. The inte client first establishes a connection with the application gateway. The application gateway determines if the com should be allowed or not and then establishes a connection wi the destination computer.

TRANSPORT LAYER

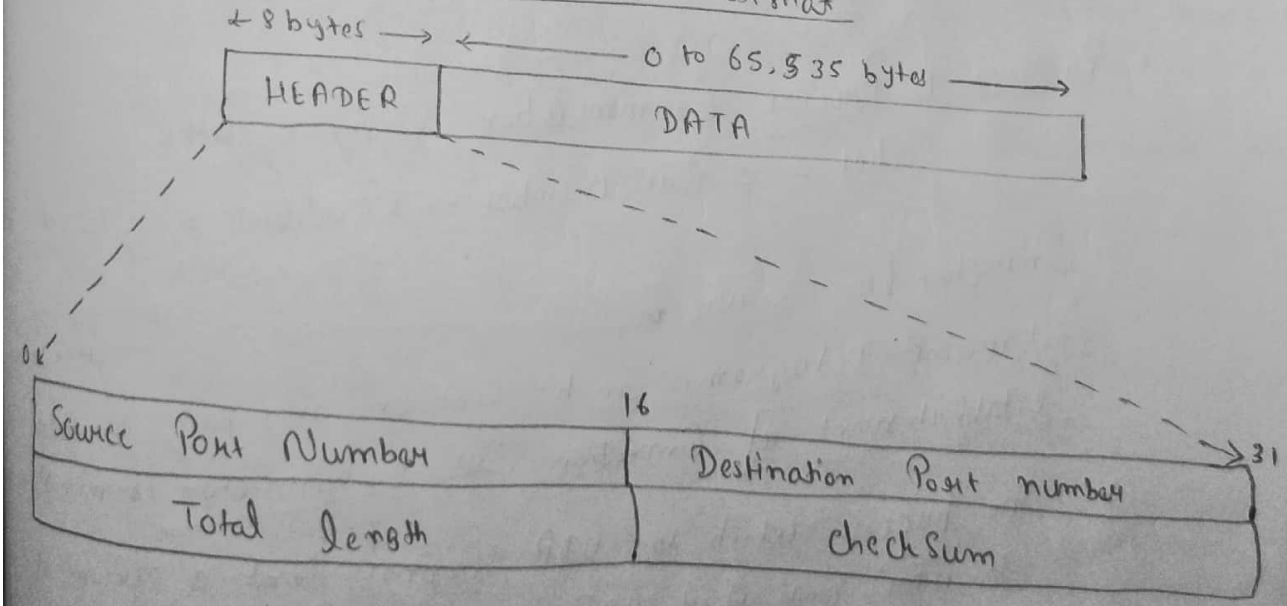
Topics :- UDP, TCP, QoS, Performance related issues.

★ UDP :- User Datagram Protocol

- it is Connectionless protocol of Transport Layer
- it is unreliable, it means if it detects some error, than it will drop the packet silently
- It is very simple protocol and minimum overhead like if we want to send a small message, than it will make small attraction b/w sender & receiver.

Application Layer
⇧
UDP
⇩
Network Layer

UDP Header format



① Source Port number :-
- Acts as a gateway
- 16 bits long
- Range : 0 - 65535

- If the source host is a client sending a request, the port no. will be a temporary port no. chosen by UDP software
- If the source host is a server, then port no. will be a well known port no. Eg :- Telnet - 23, HTTP - 80

② Destination Port number :-
- 16 bits long
- Server - Well known port
- Client - Temporary port

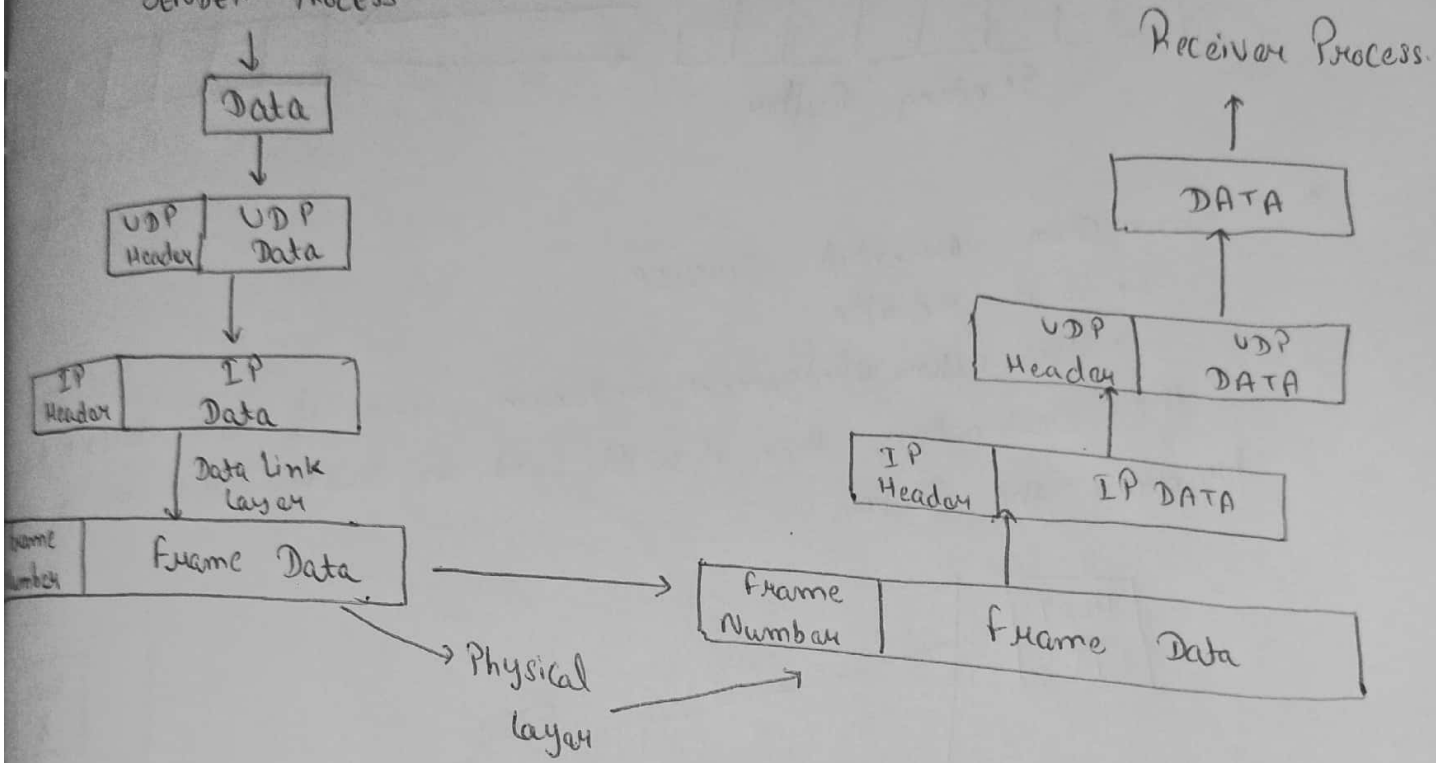
③ Total Length :-
- It is 16 bits long
- It is length of Header + length of Data
- Length of Datagram < 65535

④ Check Sum :- To Detect errors over the datagram

⇒ Services By UDP :-

- Process to Process Communication using Sockets
  Socket = < Port Number + IP address >
  Telnet = 23
  DNS = 53
  TFTP = 69
  HTTP = 80
- Connection less Services, it means Datagrams can be sent on any path as there is no establishment of Connection and no Connection termination proc
- The process which uses UDP cannot send a stream of Data to UDP and expect UDP to chop them into related UDP Datagrams, instead each request must be small enough to fi into one user datagram

- No flow Control
- No Error Control except checksum

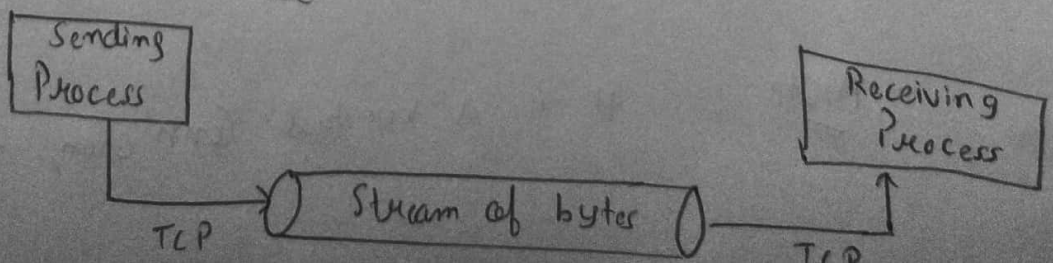


* TCP :- Transmission Control Protocol, it is a Connection-oriented protocol that it establish a connection b/w sender and receiver using same ports.

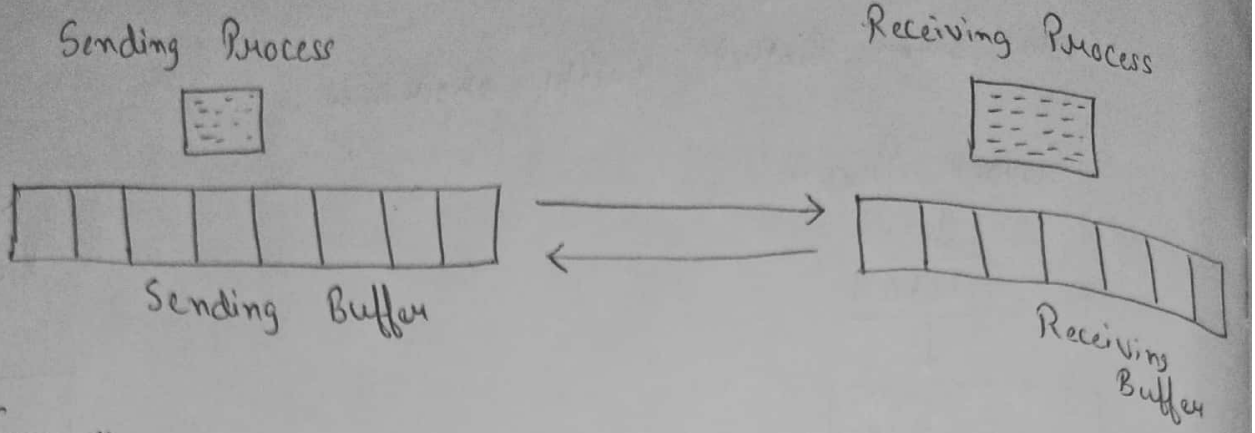
- It is reliable, due to this IP layer (or protocol) also inherits these services

⇒ Services Offered by TCP :-

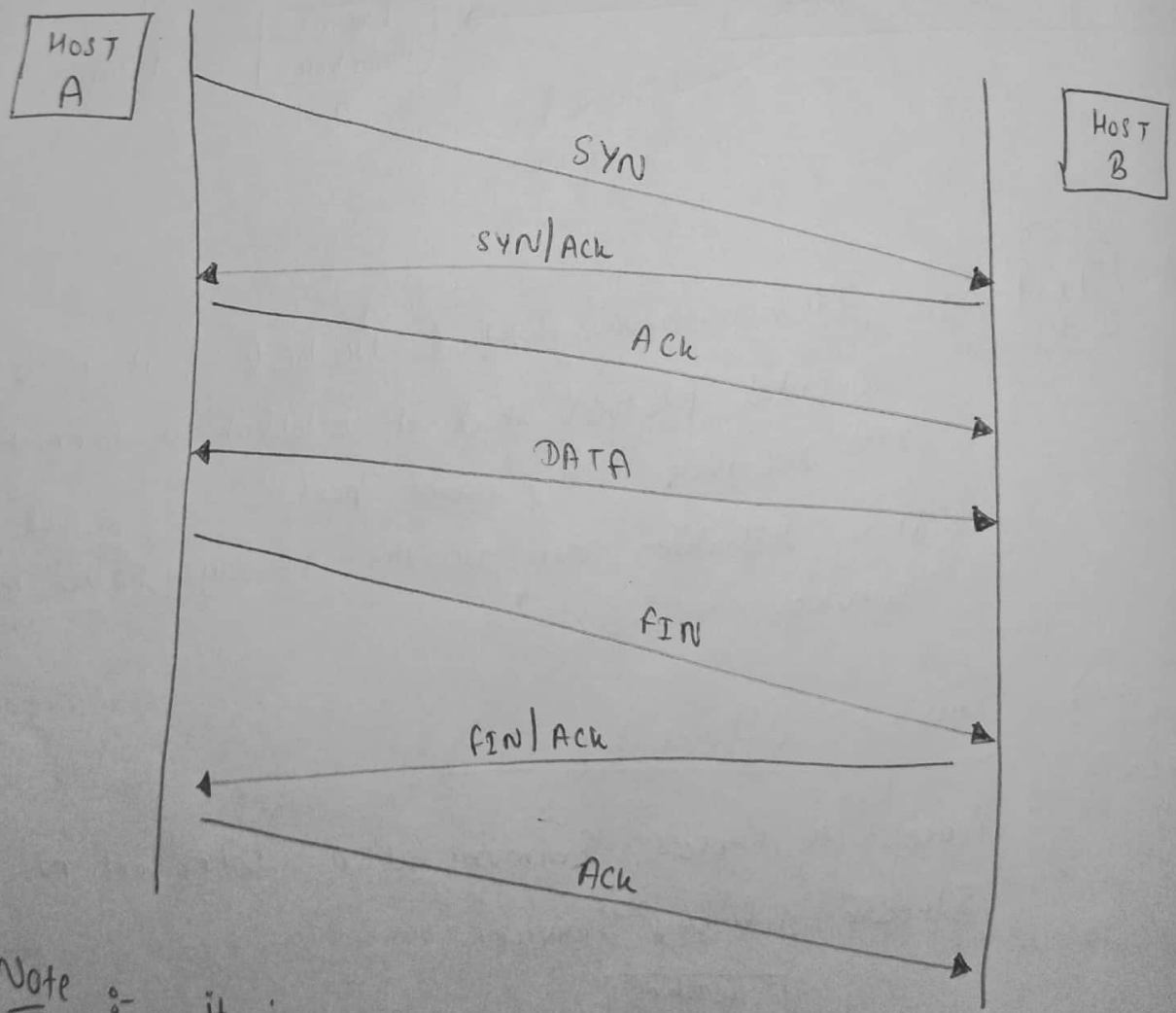
- Process to Process Communication using port no.
- Stream delivery Service.



- Full Duplex Communication :- Data can flow in both direction



- Connection oriented Service
  - it is reliable
  - Uses acknowledgement mechanism, like if data doesn't reach the Destination, than it will send an acknowledgement to re-transmit the Data



- Note :- it is a virtual Connection, not physical Connection

⇒ Features of TCP :-

★ Quality of Service and Network Performance :-

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranted performance to applications, sessions, or traffic aggregates.
Basic Phenomenon for QoS means in terms of packet delay and losses of various kinds.

⇒ Need for QoS :-

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
- Valuable applications should be provided better services than less valuable applications.

⇒ The main challenges to designing a Transport layer protocol are given below :-

1) Dynamic Topology :- Technology is changing day by day and it affects the performance of the transport layer and will be slightly affected by these changes.

2) Power and Bandwidth Constraints :- In a wireless network, two main constraints of power and bandwidth are faced. These constraints affect the transport layer.

3.) To Handle Congestion Control, reliability and flow control Separately :-

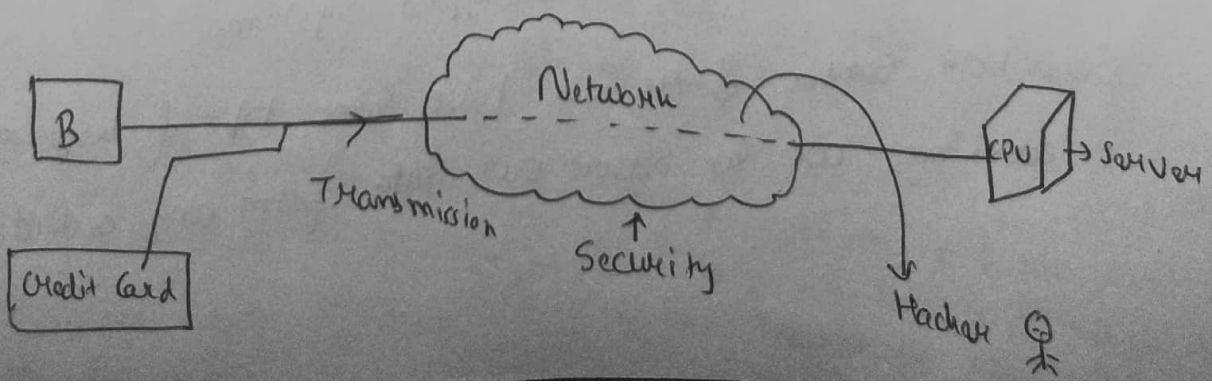
If we handle Congestion Control, reliability and flow control Separately than the performance of the transport layer is increased But to handle these separately is the additional control overhead

APPLICATION LAYER

Topics :- Cryptography Basics [Encryption & Decryption model], Public key Encryption, Private key Encryption, RSA Algorithm, File Transfer Protocol [Features, operations and Implementation], HTTP, Authentication Protocols

★ **Cryptography Basics** :- We know when we transmit the data over the network, than we need some sort of security; we understand this by an example,

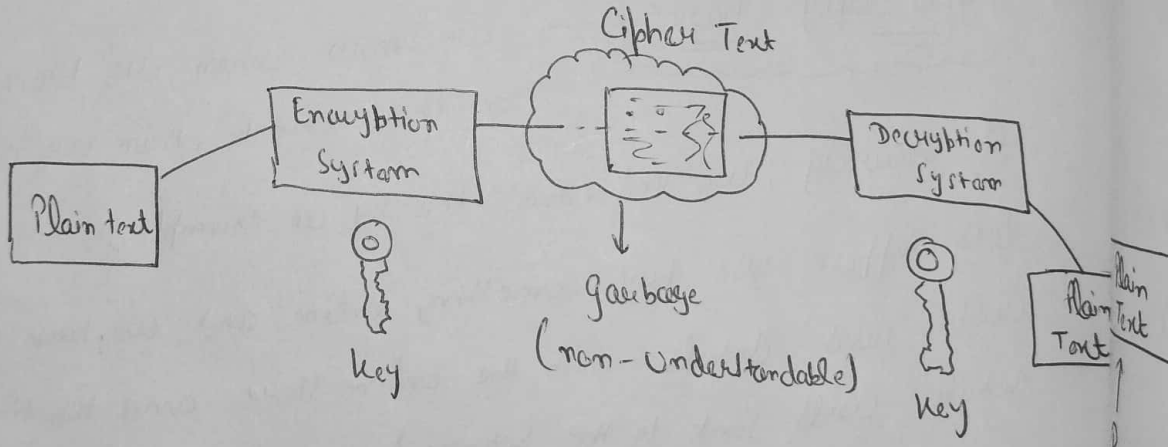
Lets suppose we buy something online and we have to share our credit card details with the online store and this time our card details will sent to the server for verification and it will kept here Secured, but what about during transmission, if there is no Security during transmission, than information will be vulnerable or hacker might hack our data. or such example like :- Personal Emails or Confidential organizations.



So one of the ways to ensure Security is Cryptography. It is field of Security which hides real information during transmission b/w two parties. The message first Converted into some non-understandable text, then again at destination, it will again converted into understable form.

- Encryption :- Converting meaningful information into encrypted data
- Decryption :- Extracting original information from encrypted data.

Model :-



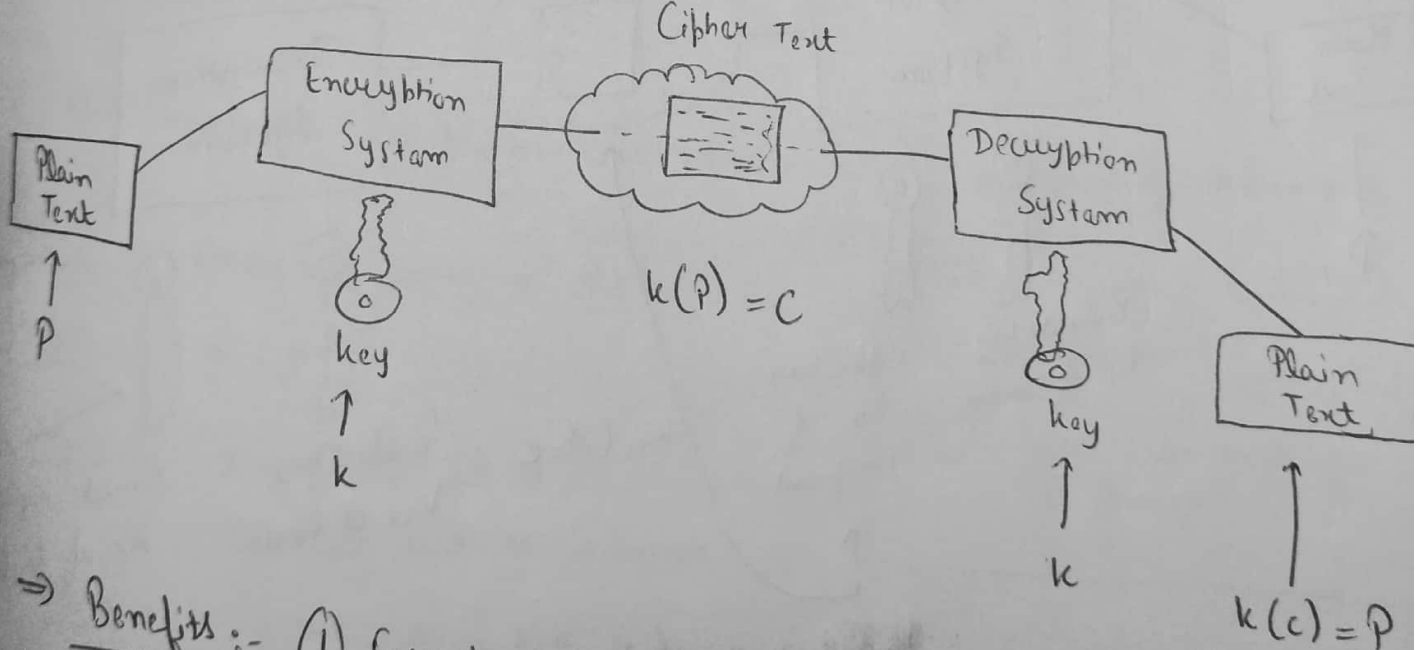
Now, the Plain text first Converted into Cipher Text using Encry System which uses a key and then at receiver end, this cipher will again Converted into Plain Text using Decryption System which used the same key as in encrypted System.

So, both sender & receiver have same type of keys and with this technique, we can secure our data from any outsider.

☆ Private key Encryption :-

It is also known as Symmetric key Cryptography.

- **Encryption Algorithm** :- Converts plain Text to Cipher Text
- **Decryption Algorithm** :- Converts Cipher Text to plain Text.
- Hacker cannot access the data
- Single shared key b/w both parties.
- It is called private key bcz only the Sender and Receiver knows what the key is.
- Here Symmetric means, We used the same key at both ends (ie for Encryption and decryption both).



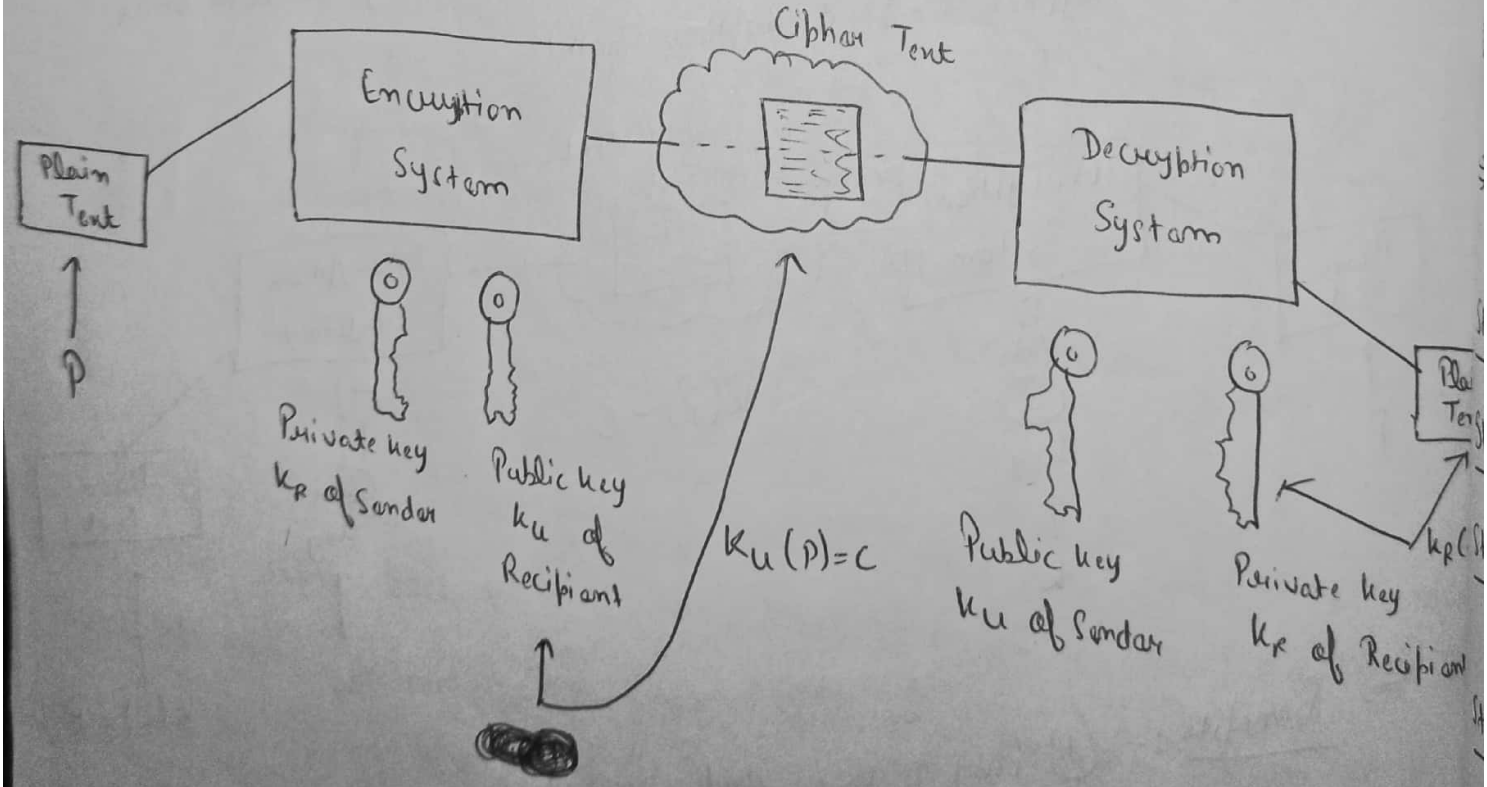
⇒ **Benefits** :- (1) Easy to use and Works faster bcz only one key is required at both the ends.

⇒ **Drawback** :- (1) key Distribution is a major Concern as if we want Send data to 10 different users then we have to distribute the key to 10 receivers and if during distribution hacker can access the key and data as well.

★ **Public key Encryption** :- It is also known as Asymmetric key Cryptography.

- Each participant shares a pair of related keys
- The sender and the receiver will both have two keys, and they will kept one as secret key and other will be public
- Public key → shared Globally → Encryption
- Private key → kept secret → Decryption

⇒ Advantage :- No overhead of Secure key Distribution



Note :- Best application of this system is RSA Algorithm.

☆ RSA Algorithm :-

Principle :- Even though it is easy to compute the product of two large prime numbers, it is extremely difficult to factor the same product into its original primes assuming that the prime numbers are not known before.

Ex :- $19 * 31 = 899$ (Easy !)

$899 = A * B$ (what is A & B ?)

⇒ **RSA involves 3 steps :-**

1. Key Generation
2. Encryption
3. Decryption

⇒ RSA Generates its public and private keys as a pair of values each

Step-1 :- Choose 2 prime no. P & Q

Step-2 :- $n = P * Q$

Step-3 :- $z = (P-1) * (Q-1)$

Here, z will be Co prime

Step-4 :- $1 > e > z$ (e is Co prime to z)

Step :- $(d * e) \bmod z = 1$

Here d is also prime no.

Public key k_u ($\underline{e}$, $\underline{n}$)

Private key k_r ($\underline{d}$, $\underline{n}$)

Note :- We can exchange "e" & "d".

Encryption :- if M is a message then

$$M^e \bmod n = C \text{ (encrypted message)}$$

Decryption :- $C^d \bmod n = M$ (original message)

Example :- Choose, $P = 3$ & $q = 11$

Step 1 :- $n \Rightarrow 3 * 11 = 33$

Step 3 :- $z \Rightarrow (3-1) * (11-1) = 2 * 10 = 20$

Step 4 :- Choose, $e = 7$ (Co-prime to 20)

We can choose (3, 19) or any

Step 5 :- $(d * 7) \bmod 20 = 1$, $\therefore d = 3$

Public key $k_u = (7, 33)$

Private key $k_u = (3, 33)$

Encryption ($M = 2$) :- $2^7 \bmod 33 = 29$ (Encrypted message)

Decryption :- $29^3 \bmod 33 = 2$ (original message)

⇒ **Note** :- This Algorithm is widely used in applications which secure data transmission.

✱ File Transfer Protocol :- FTP

- This protocol is used for transfer of Computer files.
- It is reliable Protocol.
- There will no loss and Corruption of data
- Provide Authentication
- Provide Bi-Direction Transfer
- Also provides Secured file transfer Protocol. (SFTP).
- SFTP is Secured version of FTP where Data sent is encrypted

⟹ **FTP Architecture :-**

✱ Authentication protocols :-

User Authentication is the first most Privacy while responding to the request made by the user to the software application. There are several mechanisms made which are required to authenticate the access while providing access to the data

① Kerberos :- Kerberos is a protocol thats aids in network Authentication. This is used for validating clients/servers during network employing a cryptographic key. It is designed for executing strong Authentication while reporting to applications.

② Light Weight Directory Access Protocol (LDAP) :- It is a protocol that is used for determining any individuals, organizations and other devices during a network regardless of being on public or Corporate internet.

③ OAuth 2 :- As the name suggests it is an authorization framework that promotes granting limited access to the User on its account through an HTTP Service. when a User requests access to resources an API Call is made and after the Authentication token is passed.

(4) SAML :- It stands for Security assertion Markup Language which is based on XML-based authentication data format which provides the authorization b/w an identity provider and Service Provider.

(5) RADIUS :- It stands for Remote Authentication Dial-In User Service. It is a network protocol that provides sufficient Centralized Authentication, Accounting and Authorization for users that use and network services.

The functioning of the protocol occurs when the user requests access to network resources, where the RADIUS Server encrypts the credentials which are entered by the user. After this, the User credentials are mapped through the local database and provide access.