"Computer Networks"

Unit => 1

Computer Network :-

A Computer Network is a set of Computers Connected together for the purpose of Sharing resources. The most Common resource Shared today is Connection to the internet. Other shared resources can include a printer or a file server.

Goals =>

→ Several machines can share printers, tape drives, etc.

→ Reduced cost

→ Resource & load Sharing

→ programs do not need to run on a Single machine

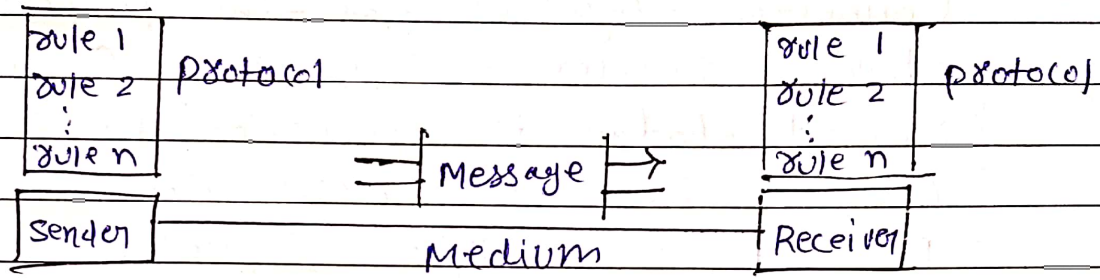
→ High reliability

→ if a machine goes down, another can take over

→ Mail & Communication.

Components =>

A data Communications System has five components



(1) Message =>

The message is the info (data) to be Communicated. Popular form of info include text, no, pictures, audio & video.

(2) Sender =>

The Sender is the device that Sends the data message. It can be a Computer, workstation, telephone handset, television and so on.

(3) Receiver =>

The receiver is the device that receives the message. It ——— and so on.

(4) Transmission medium =>

The transmission medium is the physical path by which

a message travels from Sender to receiver. Some Eg of transmission media include twisted-pair wire, Coaxial Cable, fiber-optic Cable & radio waves.

(5) Protocol =>

A protocol is a set of rules that govern data Communications. It represents an agreement bet^n the Communicating devices. Without a protocol two device may be connected but not Communicating.

Architecture =>

Network architecture is the design of a Communication network.

It is a framework for the Specification of a network's physical Components and their functional organization & Configuration.

The network archi. of the internet is predominantly expressed by its use of the internet protocol suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of Specific types of hardware link.

Classifications & Types =>

There are 3 types of network classification =>

1) LAN (Local Area Network)
2) MAN (Metropolitan Area Network)
3) WAN (Wide Area Network)

LAN :-

LAN is the group of Computers placed in the same room, same floor or the same building so they are connected to each other to form a single network to share their resources such as disk drives, data, CPU, modem etc.

LAN is limited to some geographical area less than 2km.

Most of LAN is used widely is an Ethernet Sys of the bus topology.

Metropolitan Area Network =>

The MAN is a large Computer network that expands a Metropolitan Area or ~~network~~ Campus.

It's geographic area bet^n a WAN and LAN.
It's expand round 50 km devices used are modem & cable.

WAN :-

The WAN is a network which connects the countries, cities or the continents, it is a public communications links.

The most popular eg of a wan is the internet.

WAN is used to connect LAN so the users and the computer in the one location can communicate with each other.

It's covers the large distance (more than 100 Km)

Layer Architecture :-

Protocol Hierarchy :-

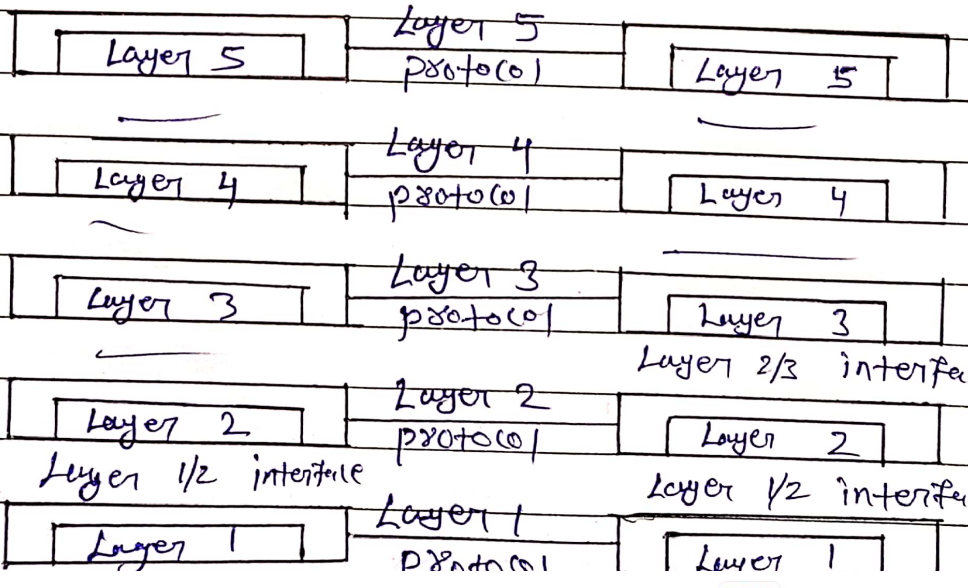
To tackle with the design Complexity most of the networks are organize as a set of layers or levels.

The fundamental idea of layered architecture is to divide the design into small pieces.

The layering provides modularity to the network design.

The main duty of Each layer is to provide offer services to higher layers, & provide abstraction

The main benefits of layered archi. are modularity and clear interfaces.



Layer archi. have several advantages. Some of them are :

→ Modularity and clear interface
→ provide flexibility to modify network ~~issue~~ services.
→ Ensure independence of layers
→ Management of network archi. is easy.
→ Each layer can be analysed and tested independent of other layers.

Connection — oriented Service :—

Connection — oriented services involve setting up a dedicated path bet^n the Source and destination before data transfer begins.

These services ensure that data is delivered in the Correct sequence and without errors.

in a COS, the Handshake method is used to establish the Connection bet^n Sender & Receiver.

Before data transmission starts, COS create a dedicated Communication

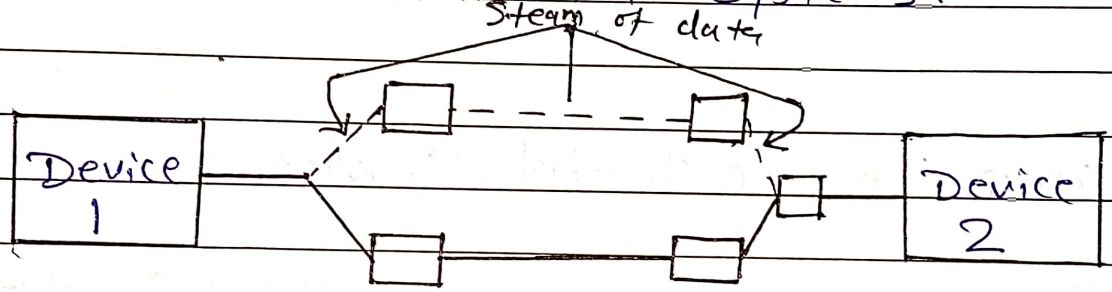
Channel bet^n Senders and the recipients.

One Eg is TCP, which ensures error free and accurate data packet delivery

Eg of COS :-

→ TCP in the TCP/IP Suite.

→ Telephone calls in traditional telecommunication systems.



COS

Key features of COS =>

→ Dedicated Connection
→ Reliable Transmission
→ Sequencing
→ Higher Overhead

Advantages =>

→ Reliable Data Transfer
→ Data Sequencing
→ Error Correction
→ Guaranteed Delivery

Disadvantages :-

→ Higher Latency
→ More overhead
→ Less Efficient for Small Transfers.

Connection Less Service :-

Connectionless Services send data without establishing a dedicated Connection bet the Source and destination.

Each data packet is treated independently and there is no guarantee of delivery or Sequencity

Connectionless Service does not give a guarantee of reliability.

In this, Packets do not follow the same path to reach there destination.

CLS deliver individual data packets without first making a Connection.

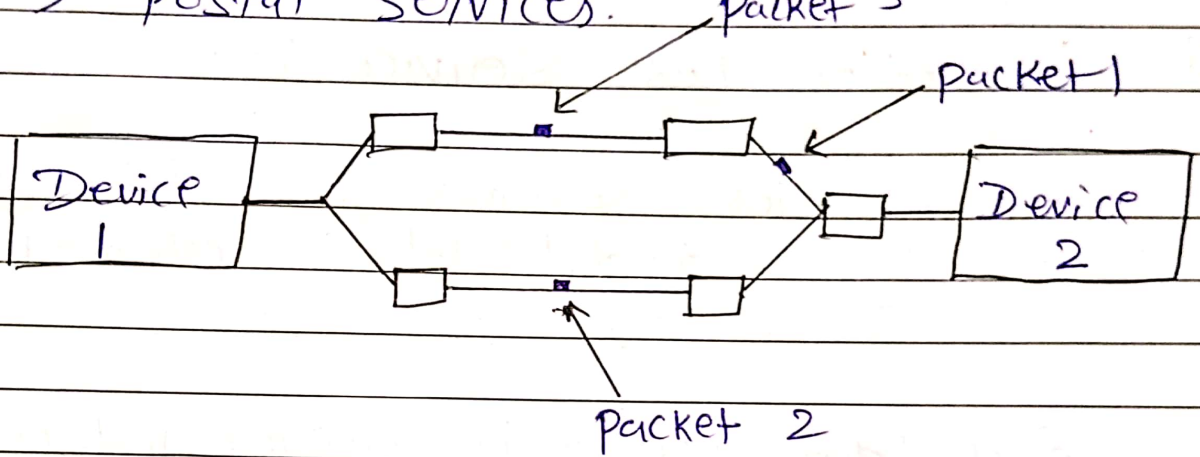
Since each packet is sent Separately, delivery, order and mistake Correction Can not be guaranteed.

As a result the Service is Quicker but less dependable.

Eg =>

→ UDP (User Datagram Protocol) in the TCP/IP suite.

→ Postal Services.



Key Feature =>

→ No Connection Setup
→ Independent packets
→ Faster Transmission
→ Unreliable

Advantages =>

→ Low Latency
→ Efficient for small Transfer
→ Sculable

Disadvantages =>

→ Unreliable
→ No Error handling
→ Unsuitable for large Transfer

COS	CLS
→ Connection-oriented Service is related to the telephone System.	CLS is related to the postal System.
→ COS is preferred by long & steady Comm.	CLS is preferred by bursty Comm.
→ COS is necessary	CLS is not Compulsory
→ COS is feasible	CLS is not feasible
→ in COS, Congestion is not possible	in CLS, Congestion is possible,
→ COS gives the guarantee of reliability	
→ Includes error detection, Correction & transmission	No error handling
→ in COS, Packets follow the same route.	in CLS, packets do not follow the Same route.
→ Ensure data is delivered in the Correct order	Data may arrive out of order or not at all.

→ less Scalable due to the need for maintaining Connections.	Highly Scaluble for large networks with many users.
→ Higher overhead due to Connection setup & Maintenance	Lower overhead as no Connectim is required
→ COs required a bandwidth of a high range	CLS requires a bandwidth of flow range.
→ Eg : TCP	Eg : UDP
→ CO requires authentication	CLS does not require authentication.

ISO/OSI Model :-

Principle =>

The OSI reference model has 7 layers. The principals that were applies to arive at the 7 layers can be briefly Summarized as follows :

-> A layer should be created where a diffexent abstraction is needed.

-> Each layer should perform a well defined function

-> The ~~layer~~ function of each layer should be Chosen with an eye toward defining internationally standardized protocols

-> The layer boundries should be chosen to minimize the info flow across the interface.

Features =>

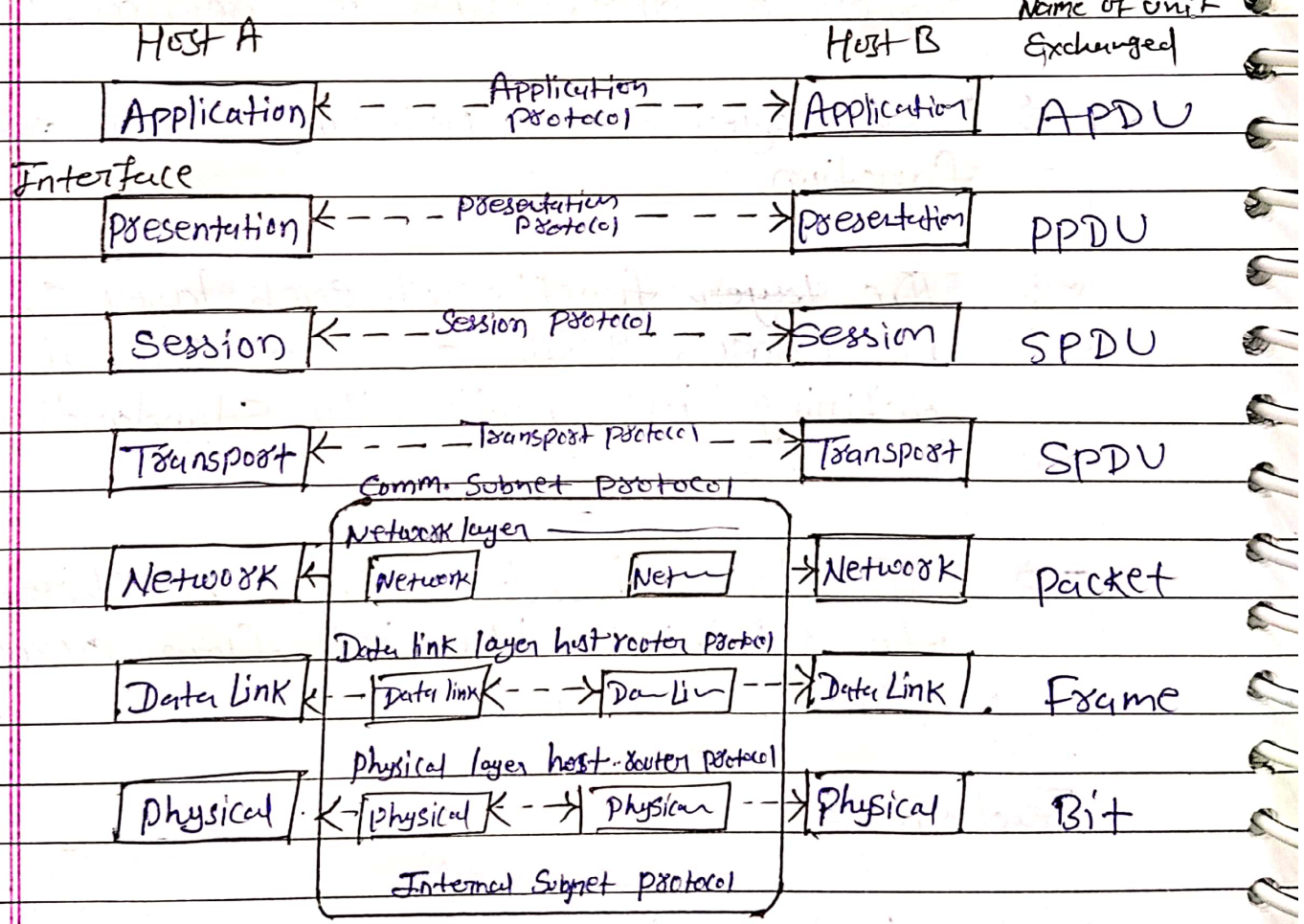
-> Big Pictuie of Comm over network is Understandable through this OSI model

-> We see how hardware & software work together.

→ We can understand new technologies as they are developed.

→ Troubleshooting is easier by separate networks.

→ Can be used to compare basic functional relationships on different networks.



① Physical layer :-

→ It is the lowest layer of OSI model

→ It activates, maintains and deactivates the physical connection.

→ It is responsible for transmission & reception of the unstructured raw data over network.

→ Voltages & data rates needed for transmission is defined in the physical layer.

→ It converts the digital bits into electrical signal or optical signals.

→ Data encoding is also done in this layer.

② Data link layer :-

→ The DLL keeps the data in synchronizes for transmission over the physical layer.

→ The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

→ Transmitting & receiving data frames sequentially is managed by this layer.

→ It creates a logical Connection bet^n devices & Controls data flow, telling the Sender to pause if the receiver's buffer is full.

(3) Network layer :—

→ It routes the signal through different Channels from one node to other.

→ It acts as a network Controller. It manages the Subnet traffic.

→ It decides by which route data should take.

→ It devides the outgoing messages into packets & assembles the incoming packets into messages for higher levels.

(4) Transport Layer :—

→ It decides if data transmissim should be on parallel path or single path.

→ Functions such as multiplexing, segmenting

or splitting on the data are done by this layer.

→ It receives messages from the session layer above it, converts the message into smaller units and passes it on to the network layer.

→ Transport layer can be very complex, depending upon the network requirement.

⑤ Session Layer :-

→ Session layer manages & synchronize the conversation b.etⁿ two different applications

⑥ presentation layer :-

→ Pres layer takes care that the data is sent in such a way that the receiver will understand the info & will be able to use the data.

→ While receiving the data, P.L. transform the data to be ready for the app. layer.

→ languages can be different of the two communicating system. Under this condition P.L. plays a role of translator

→ It performs Data Compression, Data encryption, Data Conversion etc.

⑦ App. layer ⇒

→ It is the topmost layer

→ This layer mainly holds app-programs to act upon the received and to be sent data.

Advantages of OSI Model ⇒

→ OSI model distinguishes well b/n the services, interfaces & protocols.

→ protocols of OSI model are very well hidden.

→ protocols can be replaced by new protocols as technology changes

→ Supports Connection-oriented Services as well as CLS.

Disadvantages ⇒

→ Model was devised before the innovation of protocols.

reference model = RM

→ Fitting of protocols is tedious task

→ It is just used as a reference model.

TCP/IP Reference Model :-

The TCP/IP reference model was developed prior the OSI model. The major design goals of this model were,

→ To connect multiple networks together so that they appears as a single network.

→ To survive after partial subnet hardware failure.

→ To provide a flexible architecture

Unlike OSI R.M., TCP/IP R.M. has only 4 layers. They are,

1. Host - To - Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

① Host - to - Network Layer =>

→ Lowest layer of the all

CL = Connectionless

→ Protocol is used to connect to the host, so that the packets can be sent over it.

→ Varies from host to host and network to network.

② Internet layer =>

→ Selection of a packet switching network which is based on a CL internetwork layer is called a internet layer.

→ It is the layer which holds the whole archi. together.

→ It helps the packet to travel independently to the destination.

→ IP is used in this layer.

→ The various functions performed by the internet layer are:

* Delivering IP packets
* Performing routing
* Avoiding Congestion

③ Transport Layer :-

→
→
→ The applications can read & write to the transport layer.
→ Transport layer adds header info to the data.
→ TL breaks the message into small units so that they are handled more efficiently by the network layer.

→ T.L. also arrange the packets to be sent, in sequence.

④ Application layer :-

The TCP/IP specifications described a lot of app. that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

It defines two end-to-end protocols
- TCP
- UDP

Advantages :—

→ It operated independently.
→ It is scalable.
→ Client/server archi.
→ Supports no of routing protocols.
→ Can be used to establish a connection bet" two Computers.

Disadv :—

→ In this, the transport layer does not guarantee delivery of packets.

→ The model can not be used in any other applications.

→ Replacing protocol is not Easy.

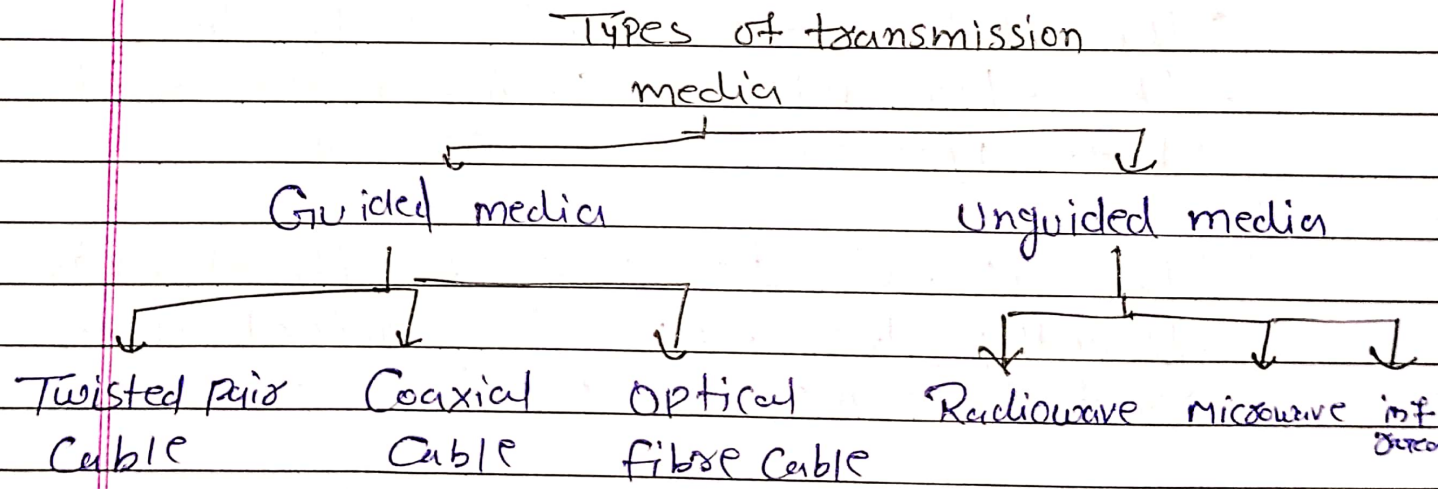
	OSI	TCP/IP	
7	Application	Application	
6	presentation		Not present in the model
5	Session		
4	Transport	Transport	
3	Network	Internet	
2	Data link	Host-to-network	
1	physical		

Physical layer :-

Media :-

Network media refers to the comm channels used to interconnect nodes on a computer network.

Typical ex of network media include copper coaxial cable, copper twisted pair cables & optical fiber cables used in wired networks. and radio waves used in wireless data comm. networks.



Bandwidth :-

Bandwidth describes the max data transfer rate of network or internet connection.

It measures how much data can be sent

Over a specific Connection in a given amount of time.

for eg, a Gigabit ~~Eith~~ Ethernet Connection has a bandwidth of 1000 Mbps.

Bandwidth also refers to a range of frequencies used to transmit a signal.

This type of bandwidth is measured in hertz & is often referenced in Signal processing app.

Data rate :-

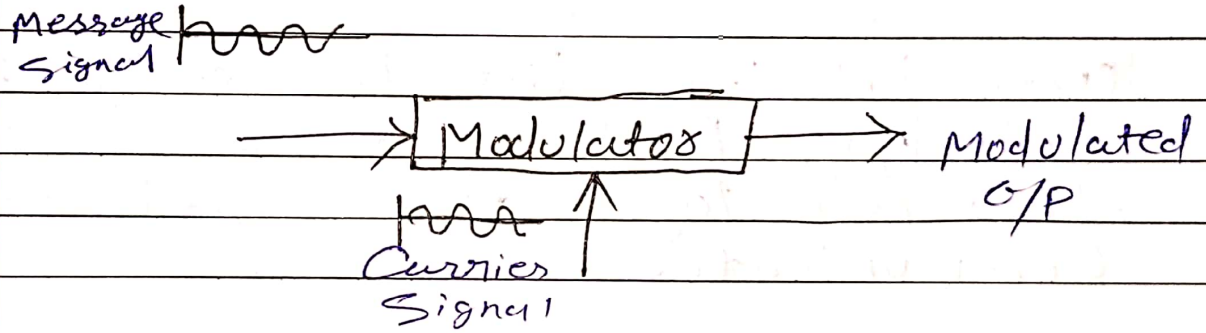
The data rate is a term to denote the transmission speed, or the no of bits per second transferred.

The useful data rate for the user is usually less than the actual data rate transported on the network.

One reason for this is that additional bits are transferred for eg Signalling the address the recovery of timing info at the receiver or error Correction to Compensate for possible transmission errors.

Modulation =>

Modulation plays a key role in Comm. Sys. to encode info digitally in analog world. It is very imp to modulate the signals before sending them to the receiver section for large distance transfer, accurate data transfer & low noise data reception.



Modulation is a process of changing the characteristics of the wave to be transmitted by superimposing the message signal on the high frequency signal.

In this process video, Audio & other data signals modify high frequency signals → also known as Carrier wave.

This Carrier wave can be DC or AC or pulse chain depending on the application used.

Unit => 2

Data Link Layer

NEED :—

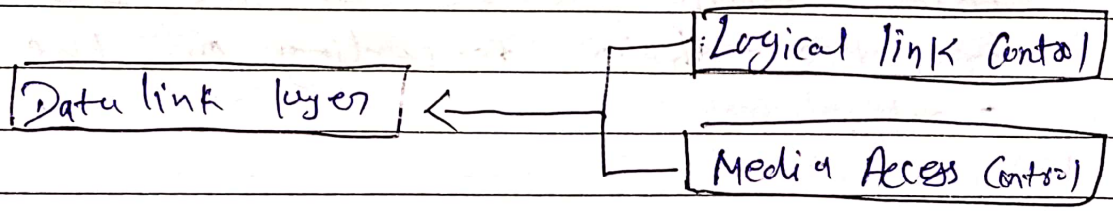
Data link layer is second layer of OSI layered Model. This layer is one of the most complicated layers and has complex functionalities & liabilities.

Data link layer hides the details of underlying hardware & represents itself to upper layer as the medium to communicate.

Data link layer works bet^n two hosts which are directly connected in some sense.

This direct connection could be point to point or broadcast.

Data link layer is responsible for converting data stream to signals bit by bit & to send that over the underlying hardware.



Data link layer has two sub-layers:

→ logical link Control
→ Media Access Control.

Service provided =>

→ Encapsulation of network layer data packets into frames.
→ Frame Synchronization
→ Error Control
→ Flow Control
→ Data packet queuing or scheduling.

Framing =>

Since the physical layer merely accepts & transmits a stream of bits without any regard to meaning or structure, it is up to the data link layer to create and recognize frame boundaries.

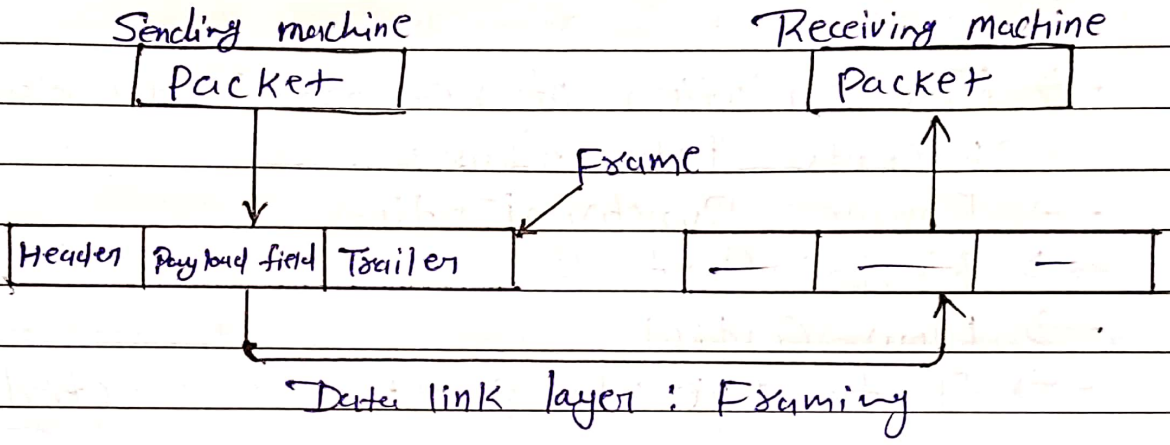
This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

The four framing methods that are widely used are

→ Character Count

→ Starting & ending characters with character stuffing

→ Starting & ending flags, with bit stuffing.



Flow Control :—

Flow control coordinates that amount of data that can be sent before receiving acknowledgement.

→ It is one of the most imp duties of the data link layer

→ Flow control tells the sender how much data to send.

→ It makes the sender wait for some sort of an acknowledgment before continuing to send more data.

→ Flow Control Techniques:

Stop – and – wait, and sliding window.

Error Control :–

Error Control in the data link layer is based on ARQ (automatic repeat request), which is the retransmission of data.

→ The term error control refers to methods of error detection &

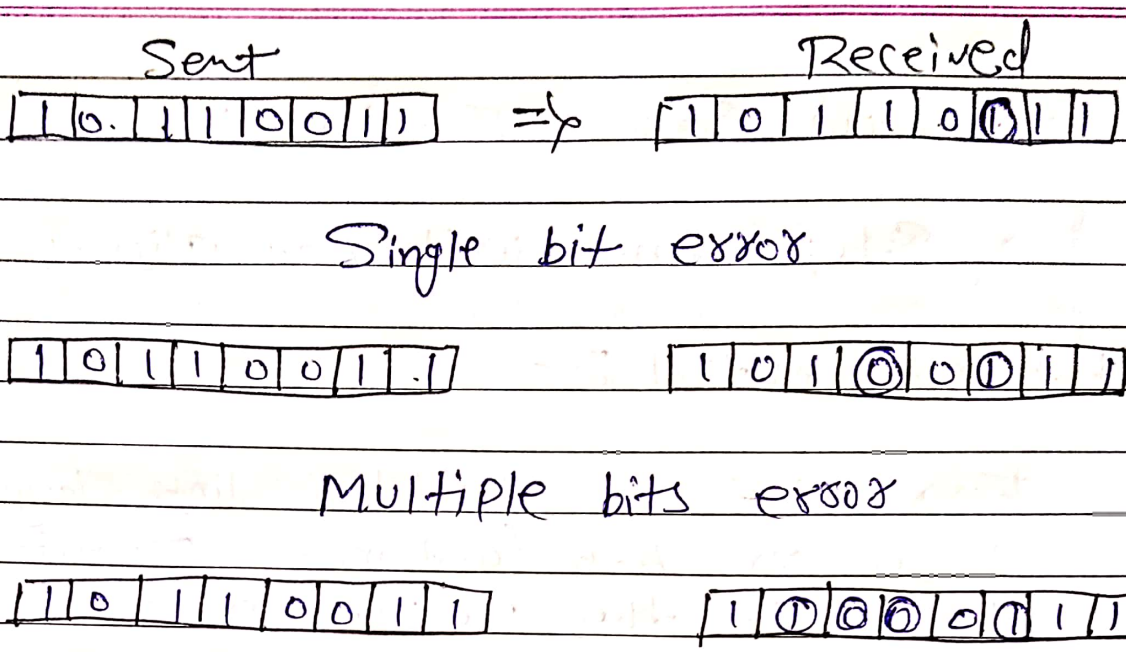
→ Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

→ Flow & error control needs to be done at several layers.

→ for node-to-node links, flow & error control is carried out in the data link layer.

→ for end-to-end point, flow & error control is carried out in the transport layer.

There may be 3 types of errors:



Data link layer protocol ... =>

The basic function of the layer is to transmit frames over a physical comm. link.

Transmission may be half duplex or full duplex.

To ensure that frames are delivered free of errors to the destination station (IMP) a no of requirements are placed on a data link protocol.

The protocol should be capable of performing:

→ The identification of a frame.
→ The transmission of frames of any length up to a given max. Any bit pattern is permitted in a frame.

→ The detection of transmission errors.

→ The retransmission of frames which were damaged by errors.

→ The assurance that no frames were lost.

→ There are mainly two types of Protocol :

① Elementary Data Link protocols :

→ Data are transmitted in one direction only.
→ The transmitting (Tx) & receiving (Rx) hosts are always ready.
→ processing time can be ignored
→ Infinite buffer space is available.
→ No errors occur

(2) Sliding Window Protocol :

A sliding window protocol is a feature of Packet-based data transmission protocols.

Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data link layer(DLL) as well as in the TCP.

The sliding window ~~protocol~~ ARQ has 3 techniques

1. 1-bit
2. Go-Back N
3. Selective Repeat

1-bit =>

One-bit Sliding window protocol is also called Stop & wait protocol.

In this protocol, the sender sends out one frame, waits for acknowledgement before sending next frame, thus the name Stop-&-wait.

Problem with Stop-and-wait protocol is that it is very inefficient. At any one movement, only in frame is in transition.

The Sender will have to wait at least one round trip time before sending next.

The waiting can be long for a slow network such as Satelite link.

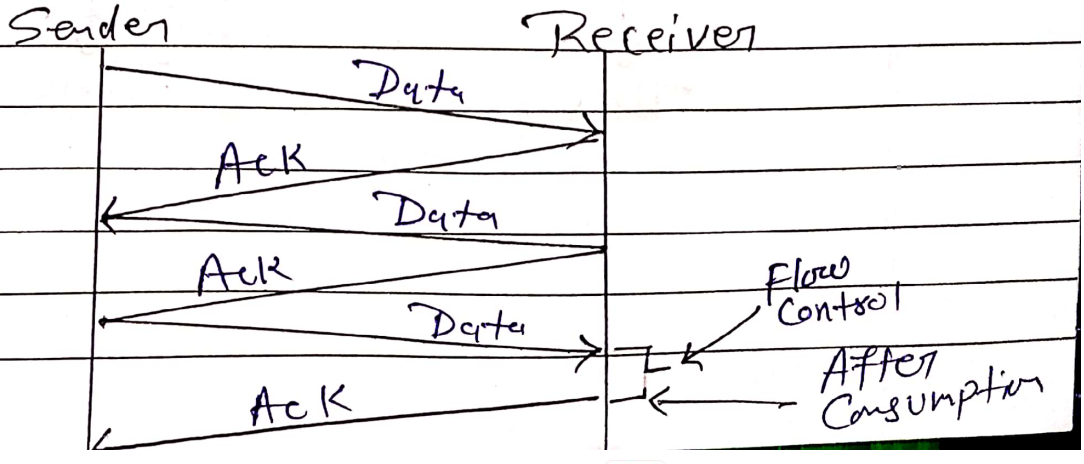
Characteristics :

→ Used in Connection-oriented Comm.

→ It offers error & flow control

→ It is used in Data Link & Transport Layers.

→ Stop and Wait ARQ mainly implements sliding window protocol concept with window size 1.

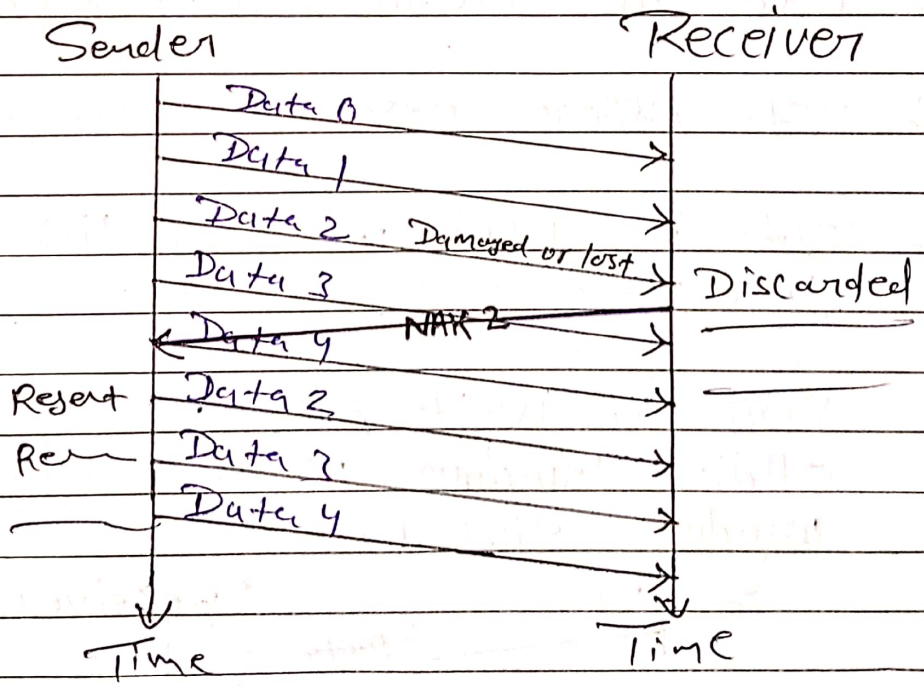


Go-Back N protocol =>

Go-Back N protocol is a sliding window protocol.

It is a mechanism to detect & control the error in datalink layer.

During transmission of frames bet" Sender and receiver, if a frame is damaged, lost or an ack is lost then the action performed by Sender & receiver.



Selective Repeat protocol :

Selective Repeat ~~or~~ is also the Sliding window protocol which detects or corrects the errors occured in datalink layer.

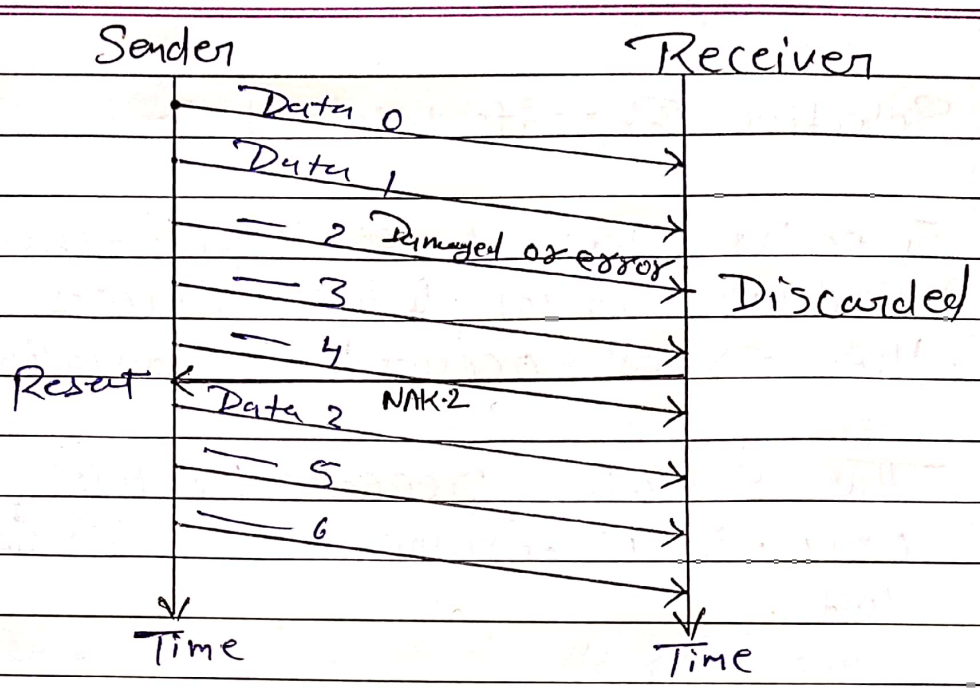
The Selective repeat Protocol retransmits only that frame which is damaged or lost.

In Selective repeat protocol, the retransframed is received out of Sequence. The Selective repeat protocol can perform following actions :

→ The Sender must be Capable of Searching the frame for which the NAK has been received.

→ The Ack no, like NAK no, refers to the frame which is lost or damaged.

→ It requires the less window size as Compared to go-back-n protocol



Hybrid ARQ :-

The HARQ is the use of Conventional ARQ along with an Error Correction technique called 'Soft Combining', which no longer discards the received bad data.

With the 'Soft Combining' data packets that are not properly decoded are not discarded anymore. The received signal is stored in a 'buffer', and will be combined with next retransmission.

That is, two or more packets received each one with insufficient SNIR to allow individual decoding can be combined in such a way that the total signal can be decoded.

Binary exponential backoff :-

The binary exponential backoff algo is primarily used in random access protocols, notably in Ethernet networks & wireless communications like wi-fi.

It functions to manage how devices handle collisions when they attempt to transmit data simultaneously on a shared channel.

How it works =>

① Collision detection :

When two or more devices transmit data at the same time, their signals clash — this is called a collision. Each device can detect this.

② Initialization :

After a collision, devices wait for a random amount of time before trying again. This help avoid another immediate collision.

③ Contention window :
The waiting time is chosen from a range called the contention window.

④ Backoff Calculation :-

Each device picks a random no from the window, then multiplies it by the time slot duration to get the actual wait time.

⑤ Try again :-

After waiting the device tries to send data again. if it collides again the process repeats with a bigger waiting range.

Application =>

→ Network protocols
→ TCP Retransmissions

Advantages =>

→ Reduced Collision probability
→ Adaptability
→ Fairness

Disadvantages =>

→ Capture Effect
→ Complexity
→ potential for increased Delays

Multiple Access protocols :-

M.A.P are method used in C.N to Control how data is transmitted when multiple devices are trying to Communicate over the same network.

These protocols ensure that data packets are sent and received efficiently, without Collisions or interference.

They help manage the network traffic so that all devices can share the Comm. Channel smoothly & efficiently.

The Data link layer is responsible for the transmission of data betⁿ two nodes. It's main function are :

→ Data Link Control
→ Multiple Access Control

Data link Control =>

The data link Control is responsible for the reliable transmission of messages over transmission channels by using techniques like framing, error Control & flow Control.

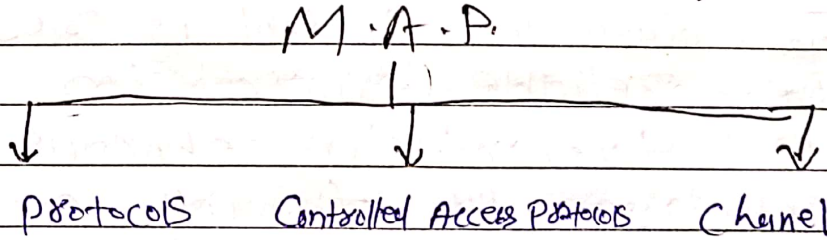
Multiple Access Control =>

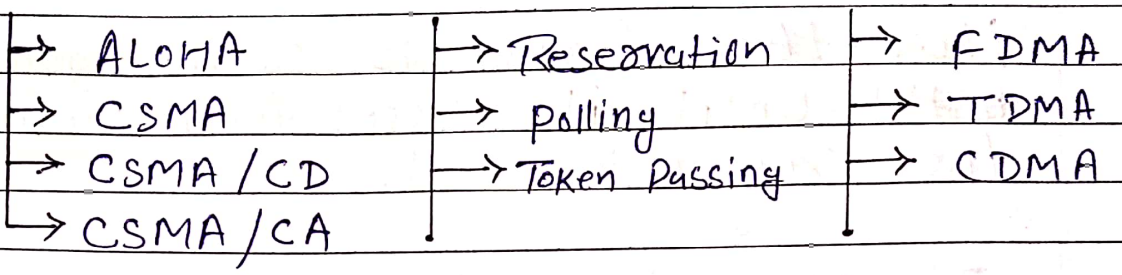
If there is a dedicated link bet" the Sender & Receiver then data link Control layer is sufficient, however if there is no dedicated link present then multiple Stations can access the channel simultaneously.

Hence MAC protocols are required to decrease Collision and avoid crosstalk.

for ey: in a classroom full of students, when a teacher asks a Qus and all the students (Stations) start answering simultaneously (Send data at same time) then a lot of Chaos is Created (data overlap or data lost) then it is the job of the teacher (MAP) to manage the Students & make them ans. one at a time.

M.A.P. Can be Subdivided further as:





Random Access Protocol =>

in this, all stations have same superiority that is no station has more priority than another station. It has two features

→ There is no fixed time for sending data
→ There is no fixed sequence of stations sending data.

ALOHA :-

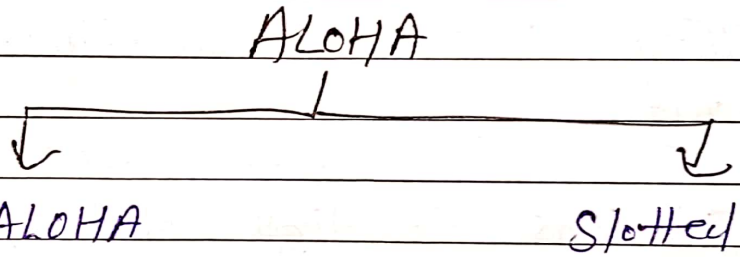
The ALOHA protocol or also known as the ALOHA method is a random access protocol in which every transmitting station or source in a network will send the data wherever a frame is available for transmission.

If we succeed & the frame reaches its destination, the next frame is lined-up for transmission. But remember, if the data frame is not received by the receiver

ACK: acknoledgment

then the frame is sent again until it successfully reaches the receiver's end.

It was designed for wireless LAN but is also applicable for shared medium. in this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.



① Pure ALOHA =>

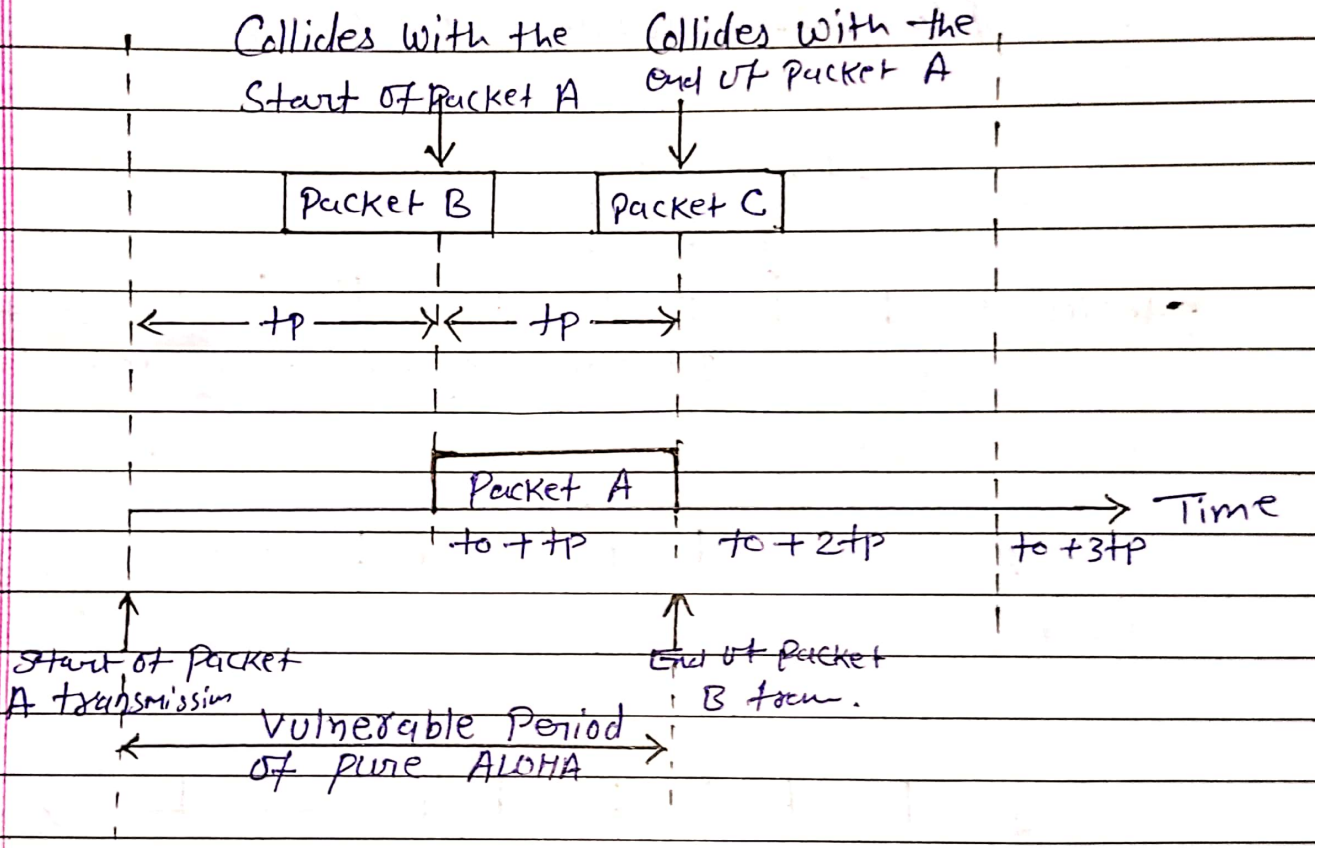
When a station sends data it waits for an ack. if the ack does not come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data.

Since different stations wait for diff amount of time, the prob. of further collision decreases.

Vulnerable Time = 2^* Frame transmission time

Throughput = $G \exp\{-2^* G\}$

Max throughput = 0.184 for $G = 0.5$



② Slotted ALOHA =>

It is similar to pure ALOHA, except that we divide time into slots & sending of data is allowed only at the beginning of these slots.

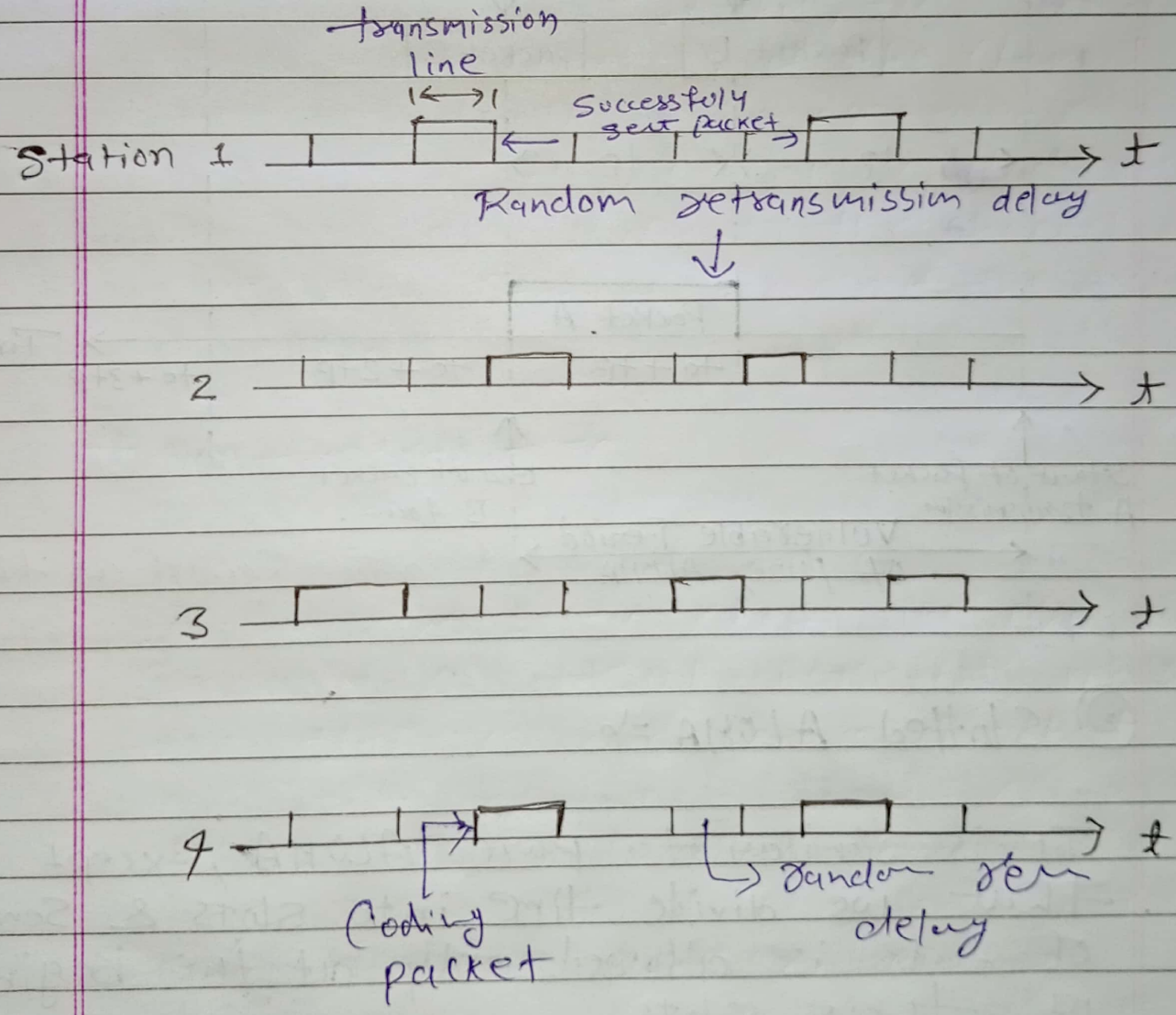
If a station misses out the allowed time, it must wait for the next

Slot. This reduces the prob. of Collision.

Vulnerable Time = Frame transmission time

Throughput $= G_1 \exp\{-*G\}$

Max Throughput = 0.368 for $G=1$

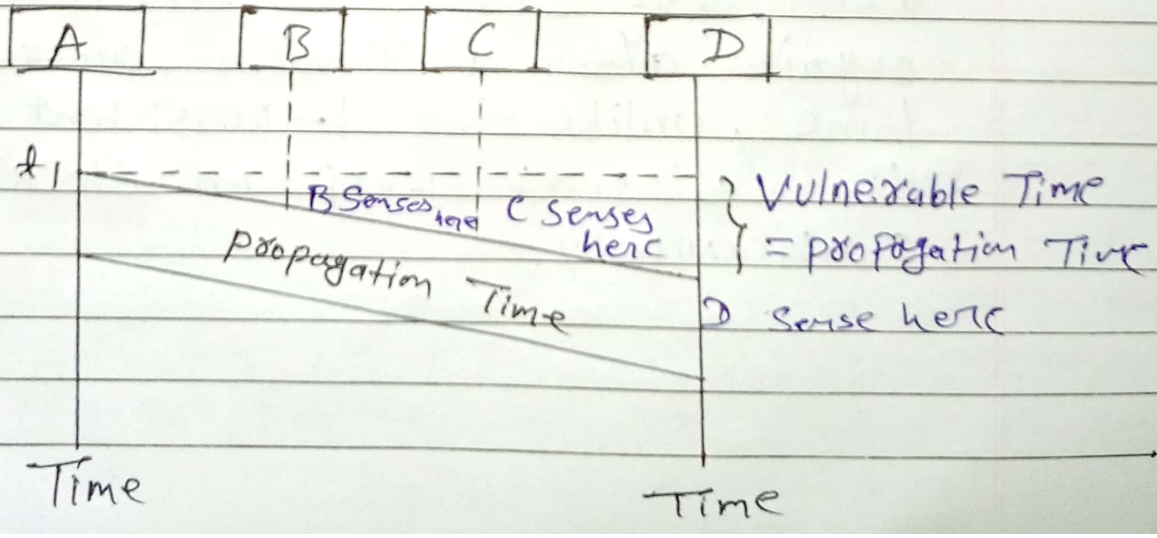


CSMA :-

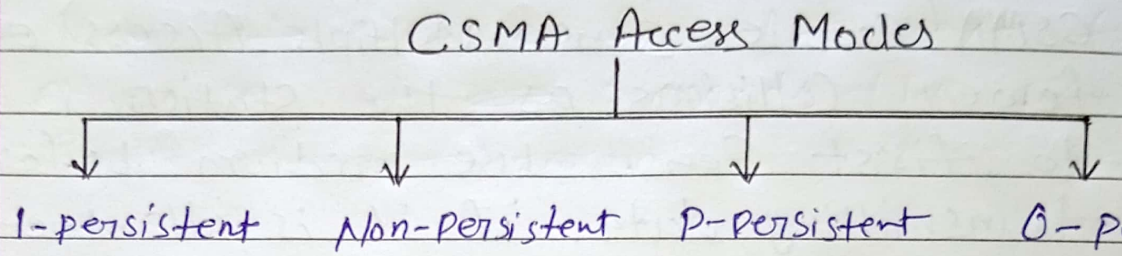
CSMA (Carrier Sense Multiple Access) ensures fewer collisions as the station is required to first Sense the medium before transmitting data. if it is idle then it sends data, otherwise it waits till the channel becomes idle.

However there is still chance of collision in CSMA due to propagation delay.
for eg:

if Station A wants to send data, it will first Sense the medium. if it finds the channel idle, it will start Sending data. However, by the time the first bit of data is transmitted from station A, if Station B requests to send data and senses the medium it will also find it idle & will also send data. This will result in collision of data from Station A & B.



The CSMA has 4 access modes =>



* 1-persistent =>

In this, first the node checks the channel, if the channel is idle then the node or station transmits data, otherwise it keeps on waiting and whenever the channel is idle, the Stations transmit the data frame.

* Non-Persistent =>

In this, the station checks the channel Similarly as the 1-persistent mode, but the only difference is that when the channel is busy it checks it again after a random amount of time, unlike the 1-persistent where the stations keep on checking continuously.

* P-persistent =>

In this, the station checks the Channel ~~Similarly as the 1-persistent mode, but the only difference~~ and if found idle then it transmits the data frame with the probability of P and if the data is not transmitted (1-P) then the station waits for a random amount of time and again transmits the data with the prob. P & this cycle goes on continously until the data-frame is successfully sent.

* O-Persistent =>

In this, the transmission occurs based on the superiority of stations which is decided beforehand & transmission occurs in that order. if the medium is idle, node waits for its time slot to send data.

CSMA/CD :-

CSMA/CD means CSMA with Collision Detection.

in this, whenever the station transmits data-frame it then monitors the channel or the medium to ack the state of the

transmission i.e. Successfully transmitted or failed. if the transmission Succeeds, then it Prepares for the next frame otherwise it ~~does~~ resends the previously failed data frame.

The point to remember here is, that the frame transmission time should be at least twice the Max propagation time, which can be deduced when the distance bet^n the two stations involved in a collision is max.

CSMA/CA =>

CSMA/CA means CSMA with collision avoidance.

To detect the possible collisions, the Sender receives the ack and if there is only one ack pregent (its own) then this means that the data frame has been sent successfully. But, if there are 2 or more ack signals then this indicates that the collision has occured

This method avoid collisions by =>

-> Interframe space
-> Contention window
-> Ack

Unit ⇒ 3

~~Routing Algo ⇒~~

→ ~~In order to transfer the packets from Source to the destination, the network~~

Routing ⇒

→ A router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.

→ A router works at the network layer in the OSI model & internet layer in TCP/IP model.

→ A router in a networking device that forwards the packet based on the info. available in the packet header. & forwarding table.

→ The routing algo are used for routing the packets. The routing algo is nothing but a soft responsible for deciding the optimal path through which packet can be transmitted.

→ The routing algo intializes & maintains the routing table for the process of path determination.

Types of Routing =>

Routing can be classified into 3 categories :

→ static Routing
→ Default Routing
→ Dynamic Routing

What is Routing Algo =>

→ In order to transfer the packets from source to the destination, the network layer must determine the best route through which packets can be transmitted.

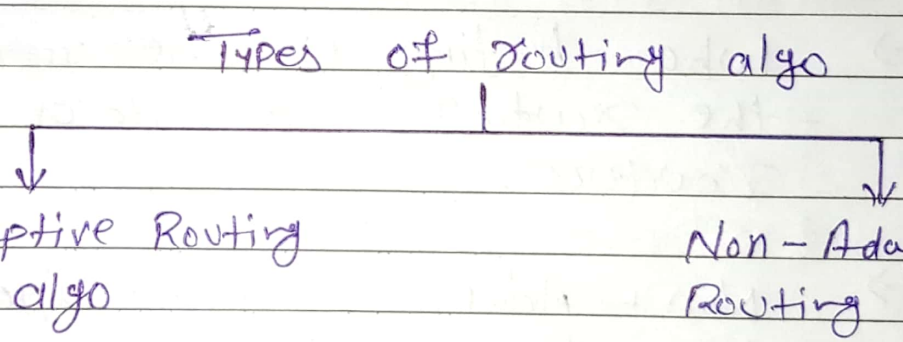
→ Wheter the network layer provides datagram Service or virtual circuit service, the main job of the network layer is to provide the best route. The routing protocol provides this job

→ The routing protocol is a routing algo that provides the best path from the Source to the destination.

The best path is the path that has the "least-cost path" from source to the destination.

→ Routing is the process of forwarding the packets from source to the destination but the best route to send the packts is determined by the routing algo.

Classification of a routing algo =>



Adaptive Routing Algo =>

→ An adaptive routing algo is also known as dynamic routing algo.

→ This algo makes the routing decisions based on the topology and network traffic.

→ The main parameters related to this algo are hop count, distance & estimated transit time.

An adaptive routing algo can be classified into 3 parts :

* Centralized algo
* Isolation algo
* Distributed algo.

Non — Adaptive Routing algo =>

→ Non Adaptive routing algo is also known as a static routing algo.

→ When booting up the network, the routing info stores to the routers.

→ Non — Adaptive routing algo do not take the routing decisim based on the network topology.

The Non-adap Ru algo are two types :

* Flooding
* Random walks.

Least Cost Routing Algo (shortest path algo) :

→ In this the path length bet^n each node is measured as a functim of distance, Bandwidth, average traffic, Communication cost, mean queue length, measured delay etc.

→ By changing the weighing function, the algo then computes the shortest path measured according to any one of a no of criteria or a combination of criteria.

→ For this a graph of subnet is drawn. With each node of graph representing a router & each arc of the graph representing a comm link. Each link has a cost associated with it.

Two algo for computing the shortest path bet^n two nodes of a graph are :-

1. Dijkstra's Algo
2. Bellman-Ford Algo

* Dijkstra's algo =)

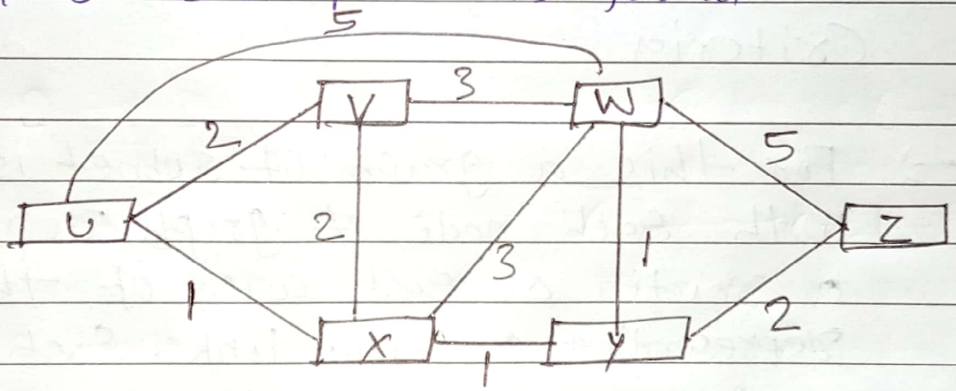
→ Compute the least cost path from one node to all other nodes in the network

→ Iterative algo - After the k^{th} iteration the least cost paths for k destination nodes are found.

→ D(v): Cost of the least cost path from source node to destination v

→ P(v): Previous node of v along the least cost path from source.

→ N': Set of nodes to which the least cost path is found.



Step	N'	D(v),P(v)	D(w),P(w)	D(x),P(x)	D(y),P(y)	D(z),P(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

Bellman – Ford Algo =)

The Bellman – Ford algo is used to find the shortest path from a starting node to all other nodes in a ~~nega~~ weighted graph. It works even if some edge weights are negative.

Bellman – Ford algo is used when you want to detect negative weight cycles (which dijakstra can not handle).

(1) This step initializes distances from source to all vertices as infinite and distance to source itself as 0.

(2) This step calculates shortest distances. Do following |V|–1 times where |V| is the no of vertices in given graph.

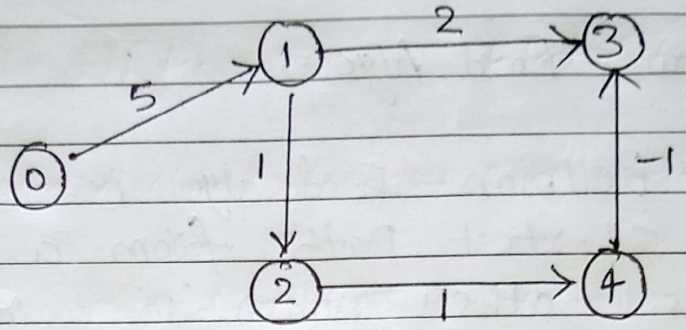
(3) This step reports if there is a negative weight cycle in graph.

Eg =)

Input : Vertices (V) = 5

Edges : [[0,1,5], [1,2,1], [1,3,2], [2,4,1], [4,3,-1]]

src : 0



O/P => [0, 5, 6, 6, 7]

Explanation:

For 0 to 1 mini. distance will be 5. By following path 0 → 1

for 0 to 2 ——— 6. ——— 0→1→2

for 0 to 3 ——— 6. ——— 0→1→2→4→3

for 0 to 4 ——— 7 ——— 0→1→2→4

Hierarchical Routing =>

Hierarchical Routing protocols consist of a hierarchical topology to organize the network and routing info..

Multiple layers and levels are introduced in a network.

Each layer may be assigned a different responsbility like forwarding packets, maintaining routing tables, etc.

HRPs are valuable for large networks, as they provide the capability of organizing network info and reducing the amount of routing info that should be exchanged bet^{n} nodes.

Hence HRPs demonstrate significant scalability and fault tolerance.

This is attributed to their hierarchical structure, which provides redundancy and facilitates the efficient distribution of routing data throughout the network.

Basis	HRPs	Flat Routing Protocol
Topology	Hierarchical topology	Single-level topology
Network	Suitable for large networks	Suitable for small networks
Routing Tables	Uses multiple routing tables to organize network info	The single routing table is used
Scalability	Highly scalable	limited Scalability
Complexity	More complex to set up and maintain	Simpler in Comparison
Optimality	Simple but non-optimal	This can be made optimal by making it more complex.
Scheduling	It is a channel reservation based Sch	It is a Contention based Sch
Collisions	Collisions are avoided	Collisions may occur frequently

Advantages of HRP :—

→ Scalability

→ Better Traffic Control

→ Easy to Manage

Disadvantages :—

→ Complexity

→ Latency

Protocols of Hierarchical Routing :—

There are two well known HRPs :

* Hierarchical State Routing Protocol
* Fisheye State

Broadcast Routing :-

Broadcast Routing is a method used in networking to send data from one source to all devices within a network. Unlike Unicast routing, which sends data to a single recipient, broadcast routing ensures that every node receives the message.

Types of broadcast routing :

→ Flooding
→ Spanning Tree Protocol (STP)
→ Reverse Path Forwarding (RPF)
→ Broadcast Domains.

Importance of Broadcast Routing :

→ Efficient Data Distribution
→ Scalability
→ Reliability
→ Security

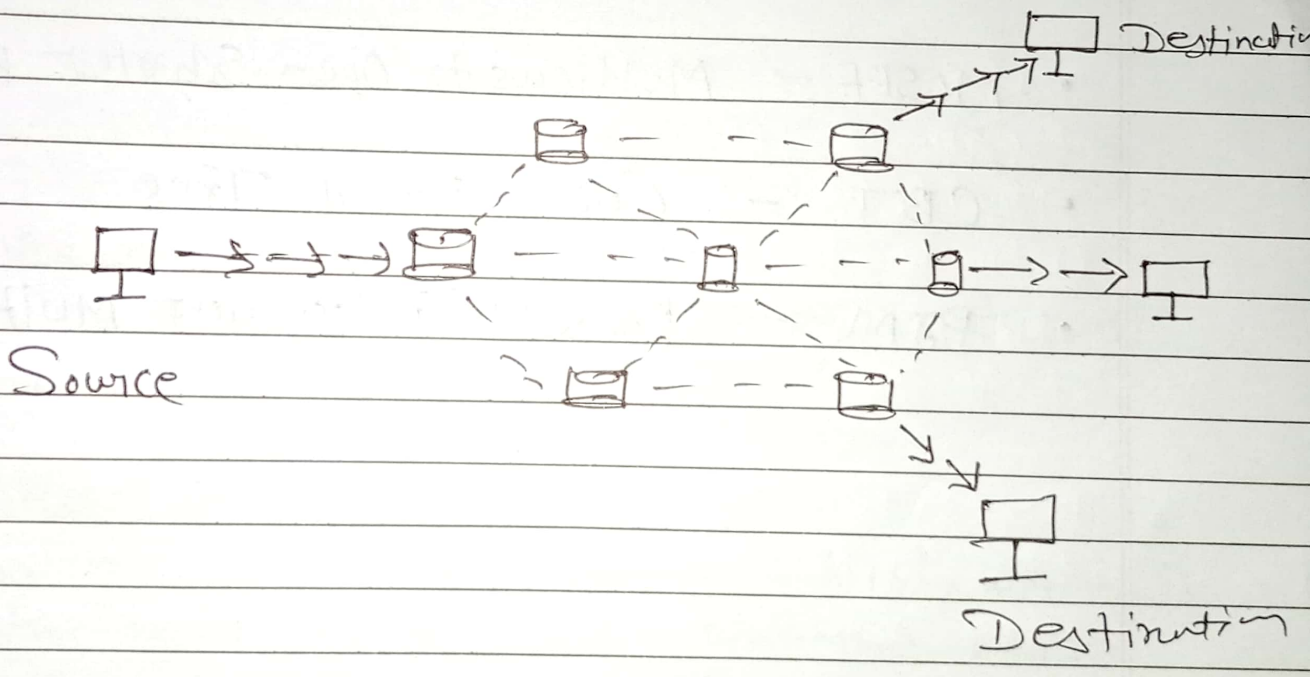
Challenges ~~and~~ :

→ Broadcast Storms
→ Security Concerns
→ Scalability
→ Bandwidth Consumption

Multicast Routing :

Multicast routing is special case of broadcast routing with significance difference and challenges.

In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.



The routers must know that there are nodes, which wish to receive multicast packets then only it should forward. Multicast routing works Spanning tree protocol to avoid looping.

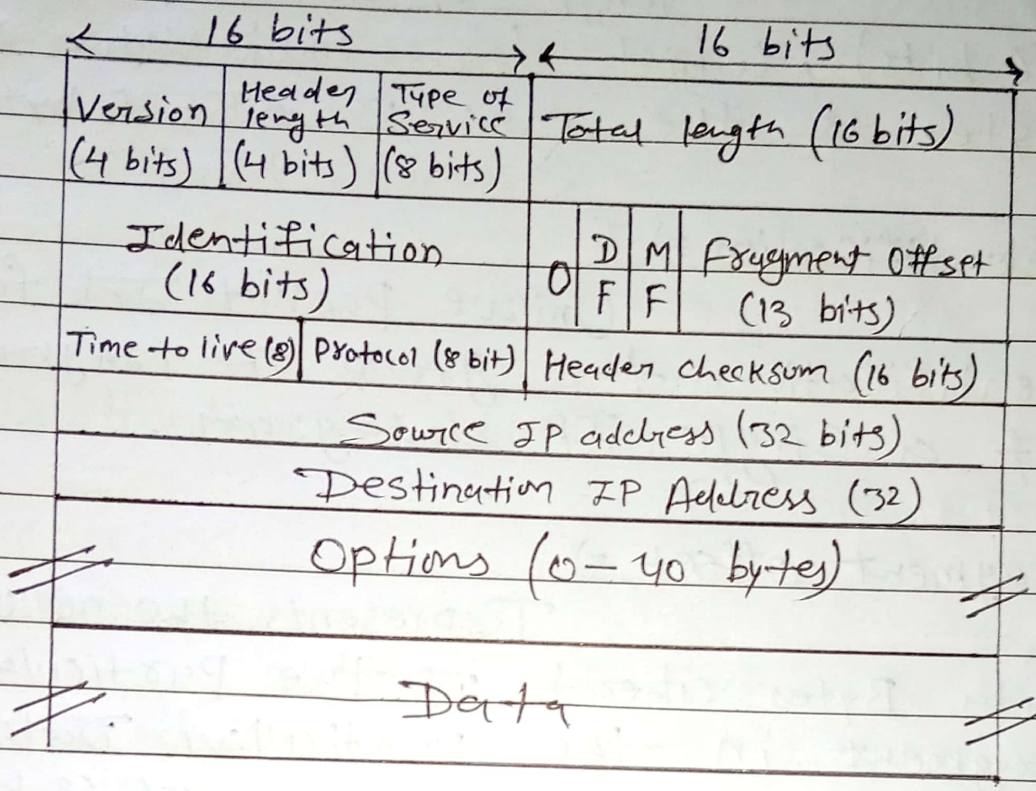
Multicast routing also uses reverse path

Forwarding techniques, to detect and discard duplicates & loops.

Unicast routing protocols use graphs while Multicast routing protocols use trees, ie. spanning tree to avoid loops. The optimal tree is called Shortest path spanning tree.

- DVMRP – Distance vector Multicast routing protocol
- MOSPF – Multicast Open Shortest path first
- CBT – Core Based Tree
- PIM – Protocol independent Multicast

Header format of IPV4 :



Version =>

Version of the IP protocol (4 bits), which is 4 for IPv4.

HLEN =>

IP header length (4 bits), which is the no of 32 bit words in the header. The minimi value of this field is 5 & the max is 15.

Type of Service =>

Low delay, High throughput, Reliability (8 bits).

Total length =)

length of header + Data (16 bits), which has a mini value 20 bytes & the max is 65535 bytes.

Identification =)

Unique packet Id for identification the group of fragments of a single IP datagram.

Fragment offset =)

Represents the no of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of no of 8 bytes, which has the max value of 65,528 bytes.

Time to live =>

Datagram's lifetime, It prevents the datagram to loop through the network by restricing the no of Hops taken by a packet before delivering to the Destination.

protocol =>

Name of the protocol to which the data is to be passed.

Header Checksum =>

16 bits header checksum for checking errors in the datagram header

Source IP Address =>

32 bits IP add of the sender.

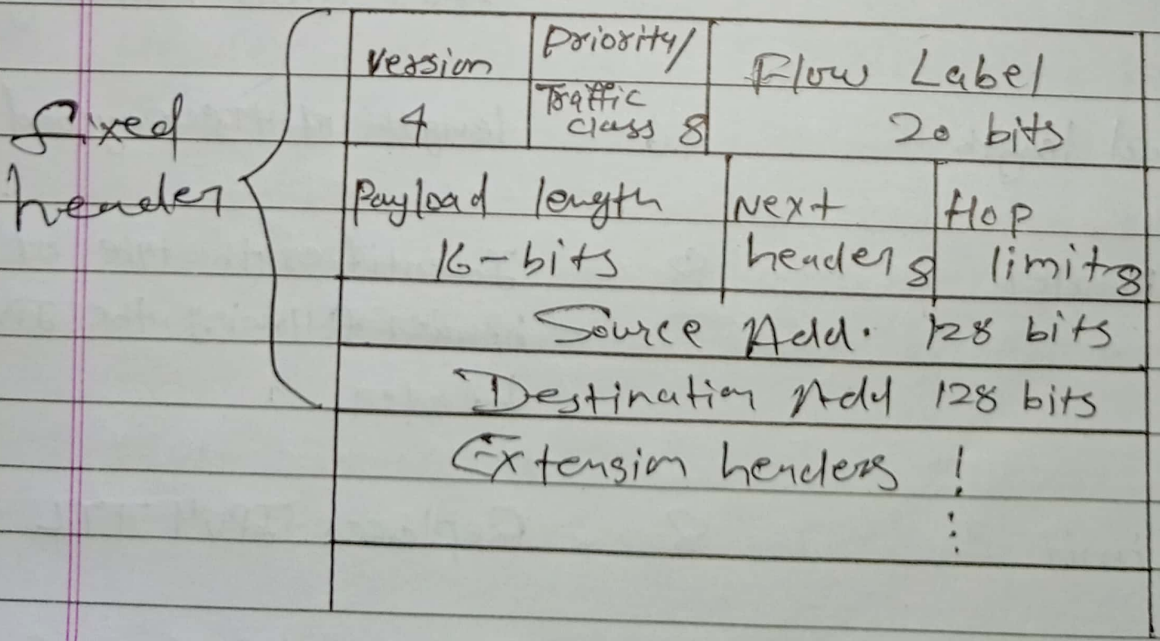
Destination IP Address =>

32 bits IP add of the receiver

Option =>

optional info such as source route, record route. Used by the Network administrator to check whether a path is working or not.

Header format of IPv6 :-



The IPv6 header format is significantly simpler than that of IPv4, designed to improve performance & allow for easier processing.

The IPv6 header is fixed at 40 bytes in length and contains the following fields:

Field Name	Size (bits)	Description
Version	4	IPv6 Version
Traffic Class	8	Similar to Type of Service in IPv4
Flow Label	20	Identifies packet flows for QoS handling
payload length	16	length of the payload
Next Header	8	Identifies the type of header following the IPv6 header.
Hop Limit	8	Replaces IPv4 TTL
Source Add	128	IPv6 add of the sender
Destination Add	128	IPv6 add of the receiver

	IPv4	IPv6
→	Address are 32 bits in length	Add are 128 bits in length
→	Add resource records in DNS to map host names to IPv4 add.	Add resource records in DNS to map host names to IPv6 add.
→	IPsec is optional & Should be supported Externaly	IPSec Support is not Optional
→	Both routers and the Sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets.
→	Header includes a Checksum	Header does not include a checksum
→	Configured either manually or through DHCP	Does not require manual Configuration or DHCP
→	Must Support a 576 byte packet size	Must Support a 1280-byte packet size.

Fragmentation :

Fragmentation is the process of breaking a packet into smaller pieces so that they will fit into the frames of the underlying network.

The receiving sys reassembles the pieces into the original packets.

The term MTU (Max transmission unit) refers to the max amount of data that can travel in a frame.

Diff. network have diff MTU sizes, So packets may need to be fragmented in order to fit within the frames of the network that they transit.

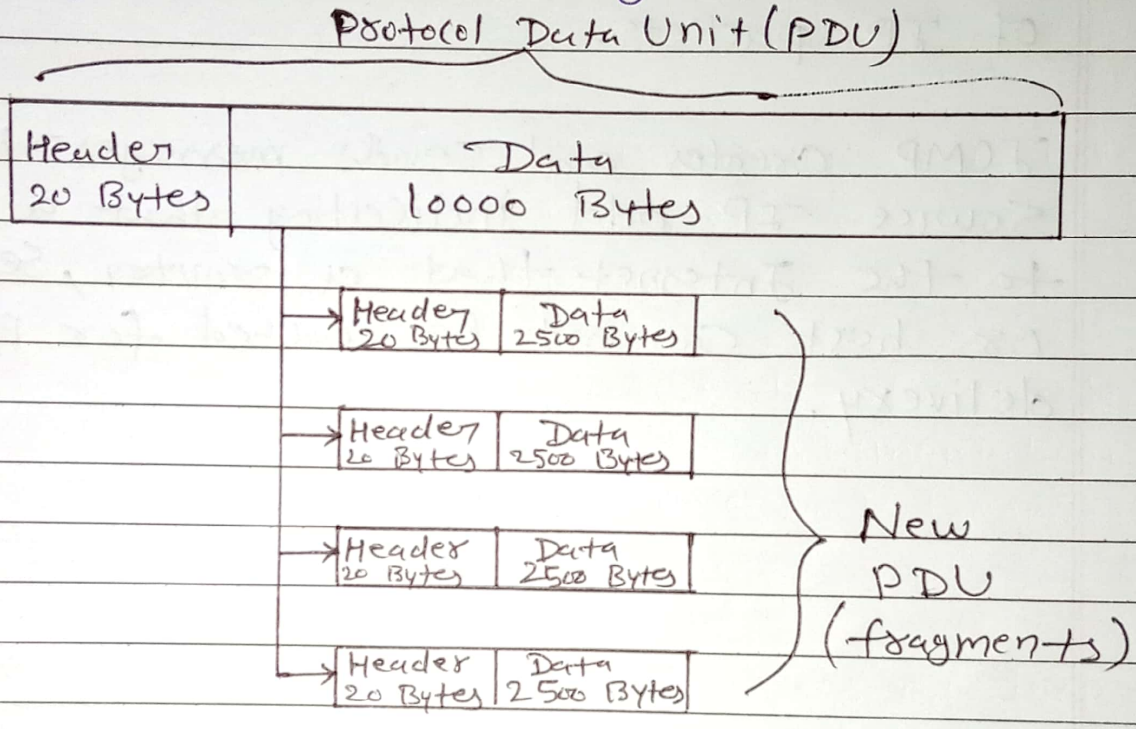
Internetworking Protocols such as IP use fragmentation because each of the networks that a packet may travel over could have a different frame size.

Fragmentation occurs at routers that connect two networks with diff. MTUs

While it is possible to design an internal network with the same MTU size, this is not an option on the internet,

which includes thousands of independently managed interconnected networks.

Fragmentation is always undesirable because it reduces performance. In fact, fragmentation is not allowed in IPV6. Large packets are always preferable.



Reassembly :

Reassembly is the reverse of segmentation Protocol Data Units are put back together in the correct order to reassemble a stream of data in its original form.

ICMP :-

ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the Source IP add when network problems prevent delivery of IP packets.

ICMP creates and sends messages to the Source IP add indicating that a gateway to the Internet that a router, service or host can not be reached for packet delivery.