UNIT - II

Data Link Layer

Design Issues:

The data Link Layer has a number of specific functions it can carry out. These functions include

1. providing a well-defined service interface to the network Layer.
2. Dealing with transmission errors.
3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

⇒ The data Link Layer takes the packets it gets from the network Layer and encapsulates them into frames for transmission.

⇒ Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.

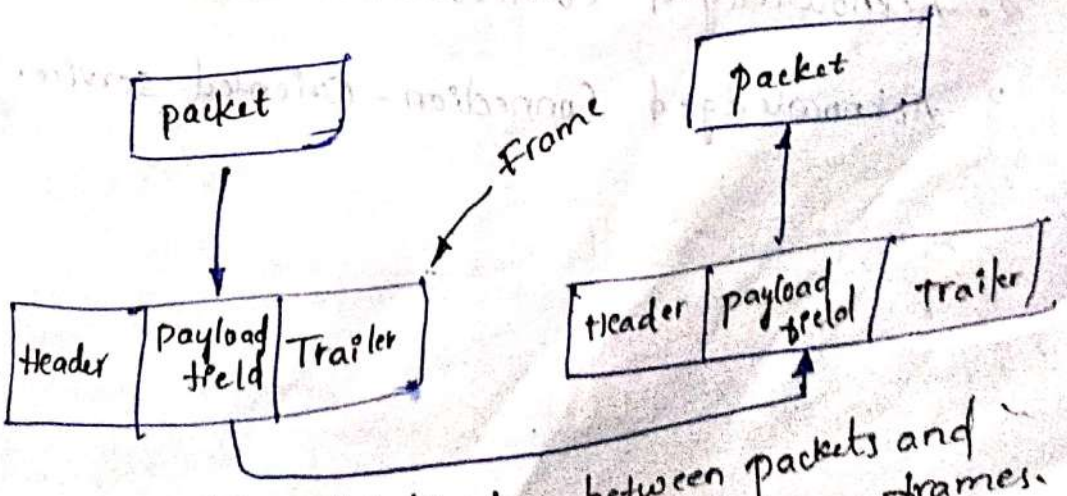


fig: Relationship between packets and frames.

*Services provided to the Network Layer

-> The function of the data link layer is to provide services to the network layer.

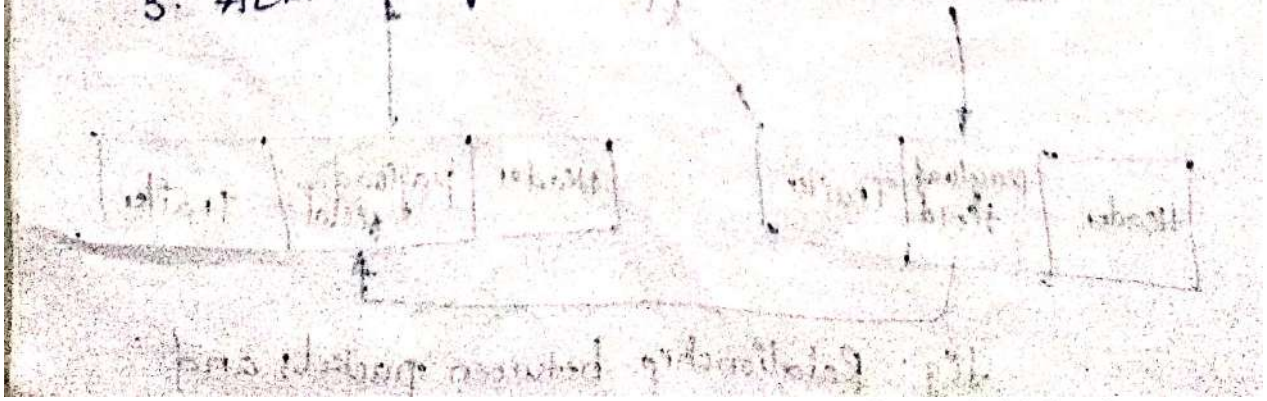
-> The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.

-> On the source machine is an entity, call it as process, in the network layer that hands some bits to the data link layer for transmission to the destination.

-> The job of the data link layer is to transmit the bits to the destination machine so they can be handed over to the network layer.

=> The datalink layer can be designed to offer various services. The actual services offered can vary from system to system. The reasonable possibilities that are commonly provided are

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.



Framing :-

Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits.

=> Framing is a function of the data link layer.

1. Character Count
2. Flag bytes with byte Stuffing
3. Starting and ending flags, with bit Stuffing
4. Physical layer coding violations.

=> The data link layer breaks the bits stream and Calculate the Checksum for each layer. At the destination layer, the checksum is enumerated.

=> Therefore, breaking the bitstream by placing spaces and time gaps is known as framing.

Flow Control :-

Flow Control is done to stop the data flow at the receiver's end.

=> The transmitter will transfer the frames very quickly to the receiver.

=> It doesn't matter if the transmission is error free at some point. The receiver will not be able to control the frames as they will arrive.

⇒ For stopping the transmission, a mechanism is there which requests the transmitter to block the incorrect messages.

Error Control:

⇒ It is done so that there is no copying of the frames for the safe delivery of the frames at the destination.

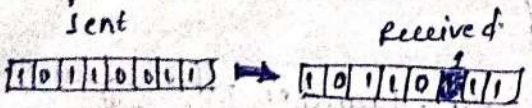
⇒ In addition, positive and negative acceptance is sent about the incoming frames.

⇒ If the sender gets positive acceptance, that means the frame appears safely, while negative appearance means that something is wrong with the frame and the frame will be retransferred.

ERROR DETECTION AND CORRECTION

There are three types of errors:

1) Single bit error

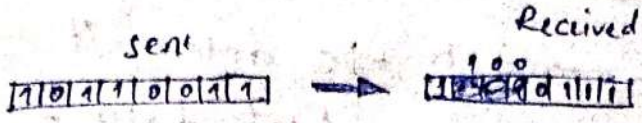


In a frame, there is only one bit, anywhere though, which is corrupt

2) Multiple bits error

Frame is received with more than one bits in corrupted state.

3) Burst error



Frame Contains more than 1 consecutive bits corrupted.

⇒ Error Control mechanism may involve two possible ways:

1) Error detection
2) Error Correction.

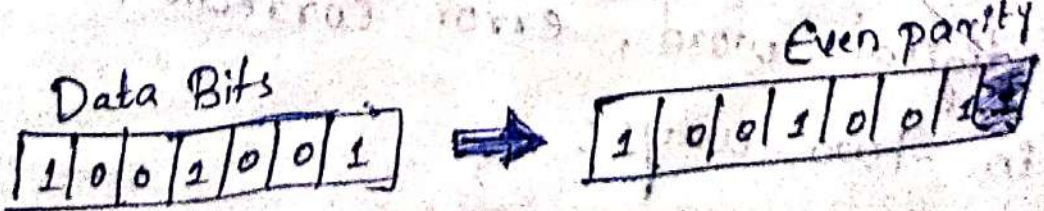
1) Error-detection

Errors in the received frames are detected by means of parity check and cyclic Redundancy check (CRC).

⇒ Parity check:

One extra bit is sent along with the Original bits to make number of 1s either even in Case of even parity, or odd in Case of odd parity.

⇒ The Sender while creating a frame Counts the number of 1s in it.



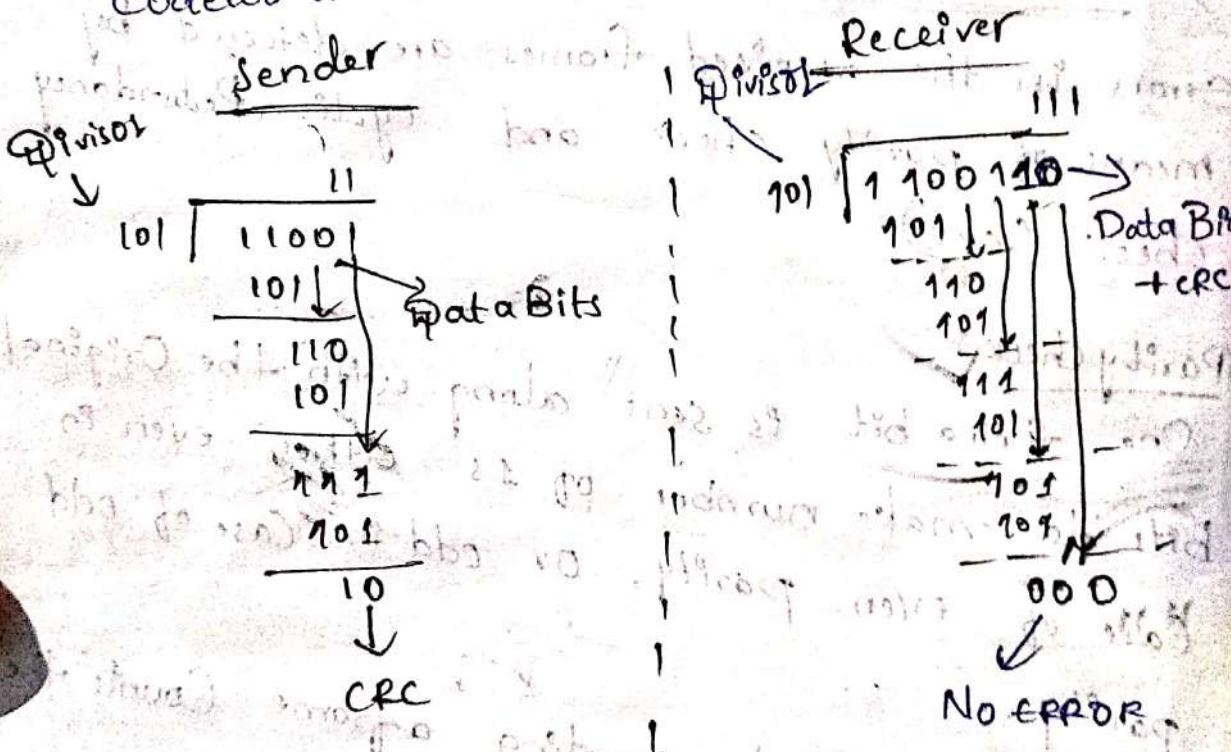
Cyclic - Redundancy check (CRC)

- CRC is a different approach to detect if the received frame contains valid data.

⇒ This technique involves binary division of the data bits being sent.

⇒ Actual data bits plus the remainder is called a codeword.

→ The Sender transmits data bits as codewords.



* Error Correction

In the digital word, error correction can be done in two ways:

1) Backward Error Correction
2) Forward Error Correction.

* Backward Error Correction :

When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.

* Forward Error Correction

When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kind of errors.

⇒ For m data bits, r redundant bits are used. r bits can provide 2^r combinations of information.

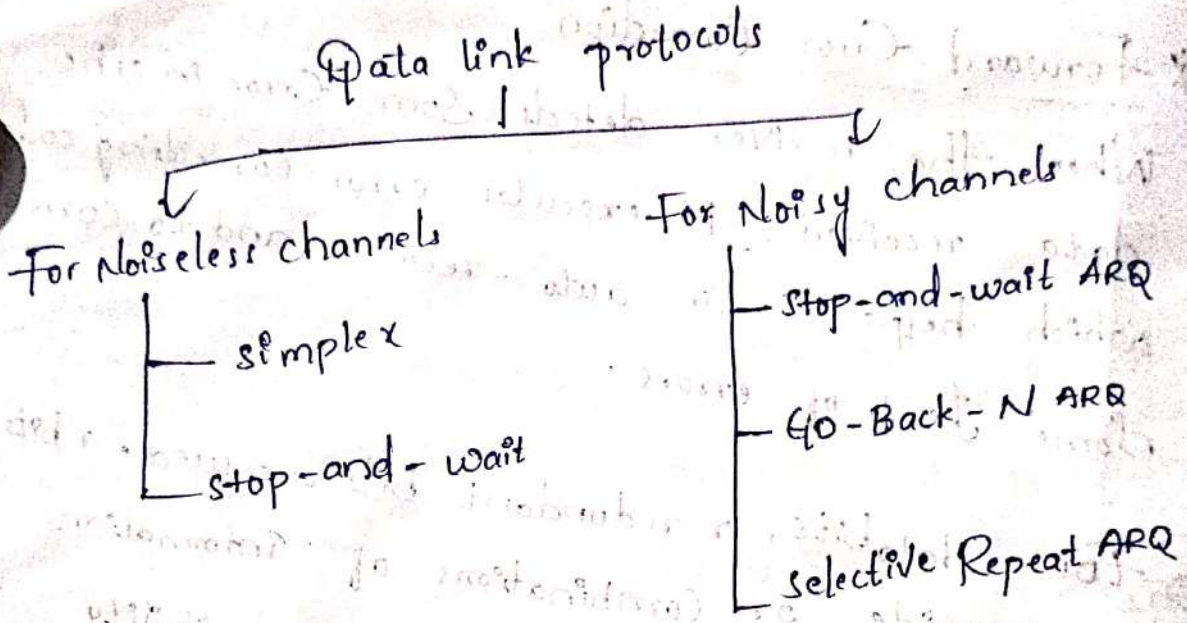
→ In m+r bit codeword, there is possibility that the r bits themselves may get corrupted.

⇒ So the number of r bits used must inform about m+r bit locations plus no-error information. i.e. (m+r+1)

$$\therefore 2^r >= m+r+1$$

* ~~Elementary~~ data Link protocols:

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



* Simplex protocol:

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel. i.e: a channel through which transmission can never go wrong.

⇒ It has distinct procedures for Sender and receiver.

⇒ The Sender simply sends all its data available onto the channel as soon as they are available its buffer.

⇒ It is hypothetical since it does not ~~allow~~ handle flow control or error control.

Stop - and - Wait protocol

Stop-and-wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities.

⇒ However, it provides for flow control so that a fast sender does not drown a slow receiver.

⇒ The receiver has a finite buffer size with finite processing speed.

⇒ The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

* Stop - and - Wait ARQ ⇒ Automatic Repeat Request

Stop-and-wait Automatic Repeat Request (stop-and-wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels.

⇒ The Sender keeps a copy of the sent frame.

⇒ It then waits for a finite time to receive a positive acknowledgement from receiver.

⇒ If the timer expires or a negative acknowledgement is received, the frame is retransmitted.

→ If a positive acknowledgement is received then the next frame is sent.

Go-Back-N ARQ

Go-Back-N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame.

⇒ It uses the concept of "sliding windows, and so is also called sliding window protocol.

⇒ The frames are sequentially numbered and a finite number of frames are sent.

⇒ If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.

* Selective Repeat ARQ

→ This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame.

⇒ However, here only the erroneous or Lost frames are retransmitted, while the good frames are received and buffered.

* Elementary Data Link protocols:

Elementary Data Link protocols are classified into three Categories, as given below.

* protocol 1 - Unrestricted Simplex protocol.
* protcol 2 - Simplex stop and wait protocol.
* protocol 3 - Simplex protocol for noisy channels.

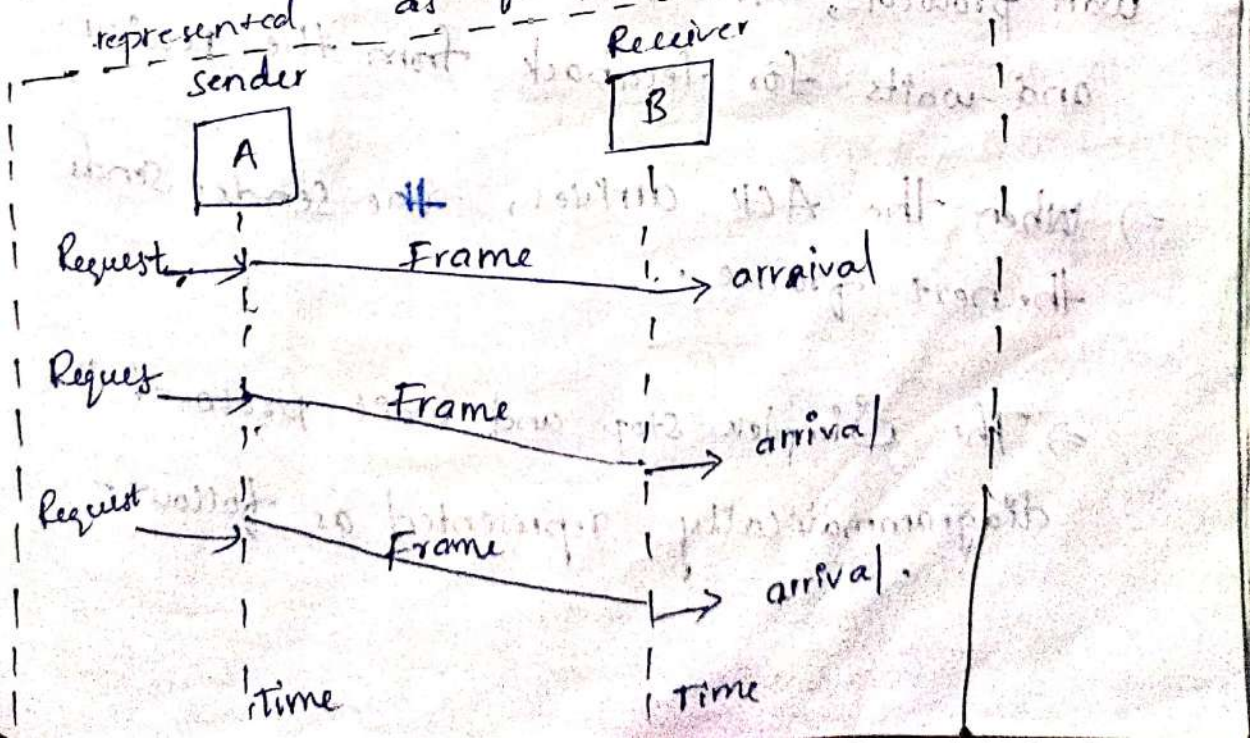
* Unrestricted Simplex protocol

Data transmitting is carried out in one direction only.

⇒ The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored.

⇒ In this protocol, infinite buffer space is available, and no errors are occuring that is no damage frames and no Lost frames.

⇒ The Unrestricted Simplex protocol is diagramatically represented as follows:-



*Simplex Stop and wait protocol

The main problem here is how to prevent the sender from flooding the receiver.

Step1 :- The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

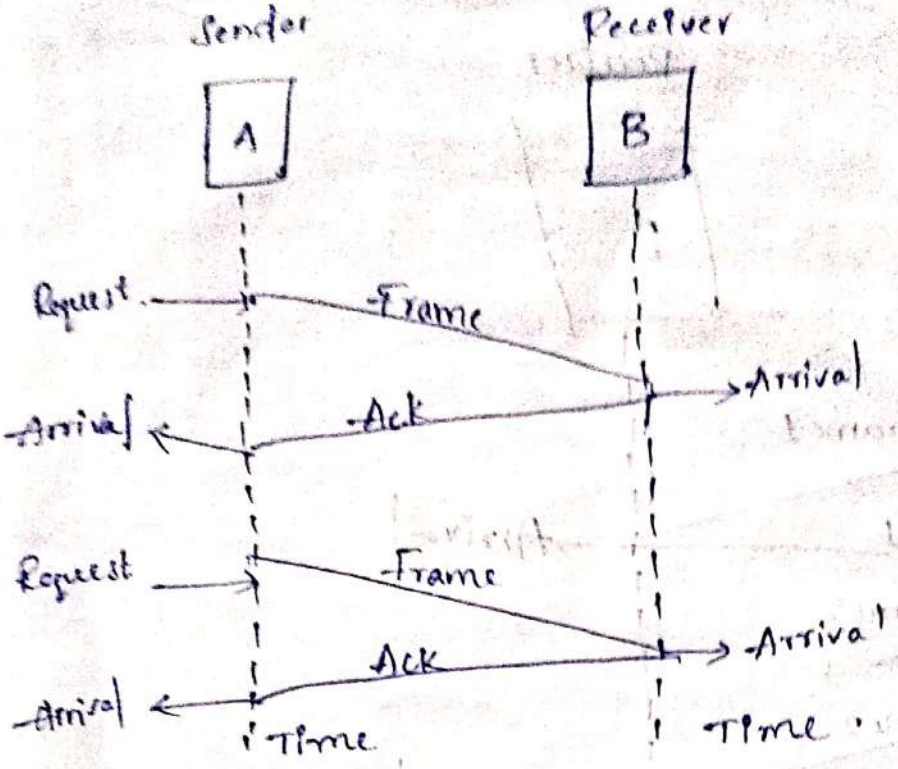
Step2 :- permission to send the next frame is granted.

Step3 :- The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

=> This protocl is called Simplex stop and wait protocol, the Sender sends one frame and waits for feedback from the receiver.

=> When the ACK arrives, the sender sends the next frame.

=> The Simplex stop and wait protocol is diagrammatically represented as follows -



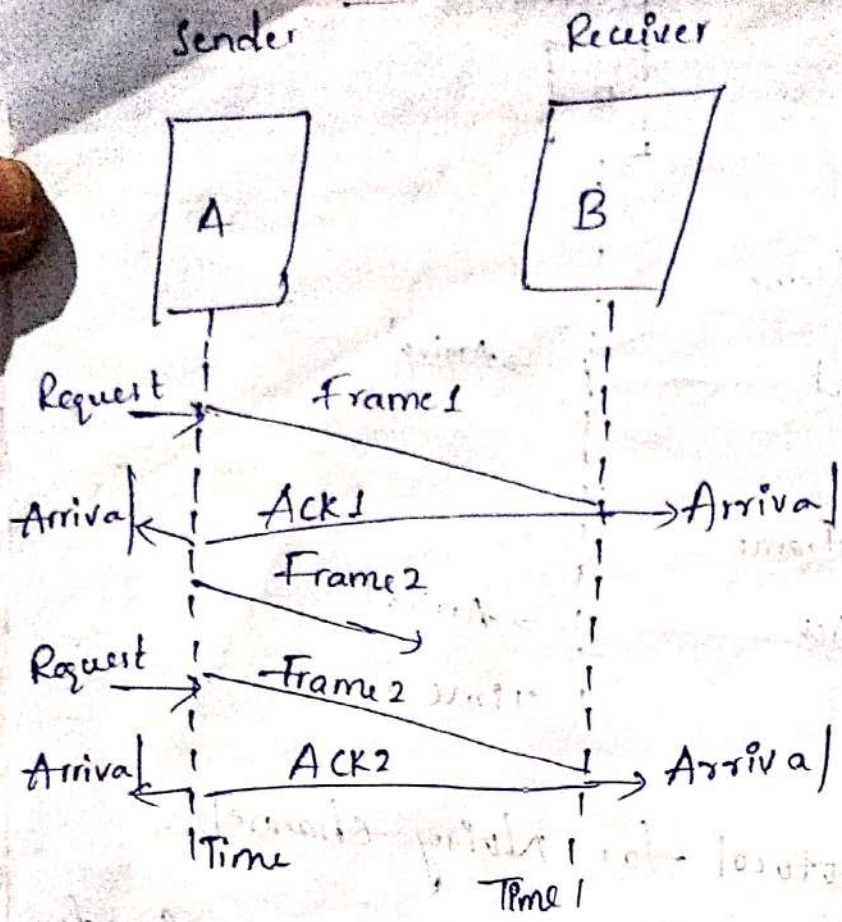
* Simplex protocol for Noisy channel

Data transfer is only in one direction, Consider Separate Sender and receiver, finite processing Capacity and Speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected.

⇒ Every Frame has a unique Sequence number.

⇒ After a frame has been transmitted, the Timer is started for a finite time.

⇒ The Simplex protocol for Noisy channel is diagrammatically represented as follows-



* Sliding Window protocols:

Sliding Window protocols

* In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.
* Working principle: In these protocols, the sender has a butter called the sending window and the receiver has butter called the receiving window
  * It has two parameters
    1. Sequence number
    2. Sliding window
  * It is number given to each outbound frame
  * The range of sequence number is $2^n - 1$
  * Sliding window is an imaginary butter.

CSMA (Carrier sense multiple Access)

FDMA (Frequency Division multiple Access)
TDMA (Time Division multiple Access)
CDMA (code Division " ")

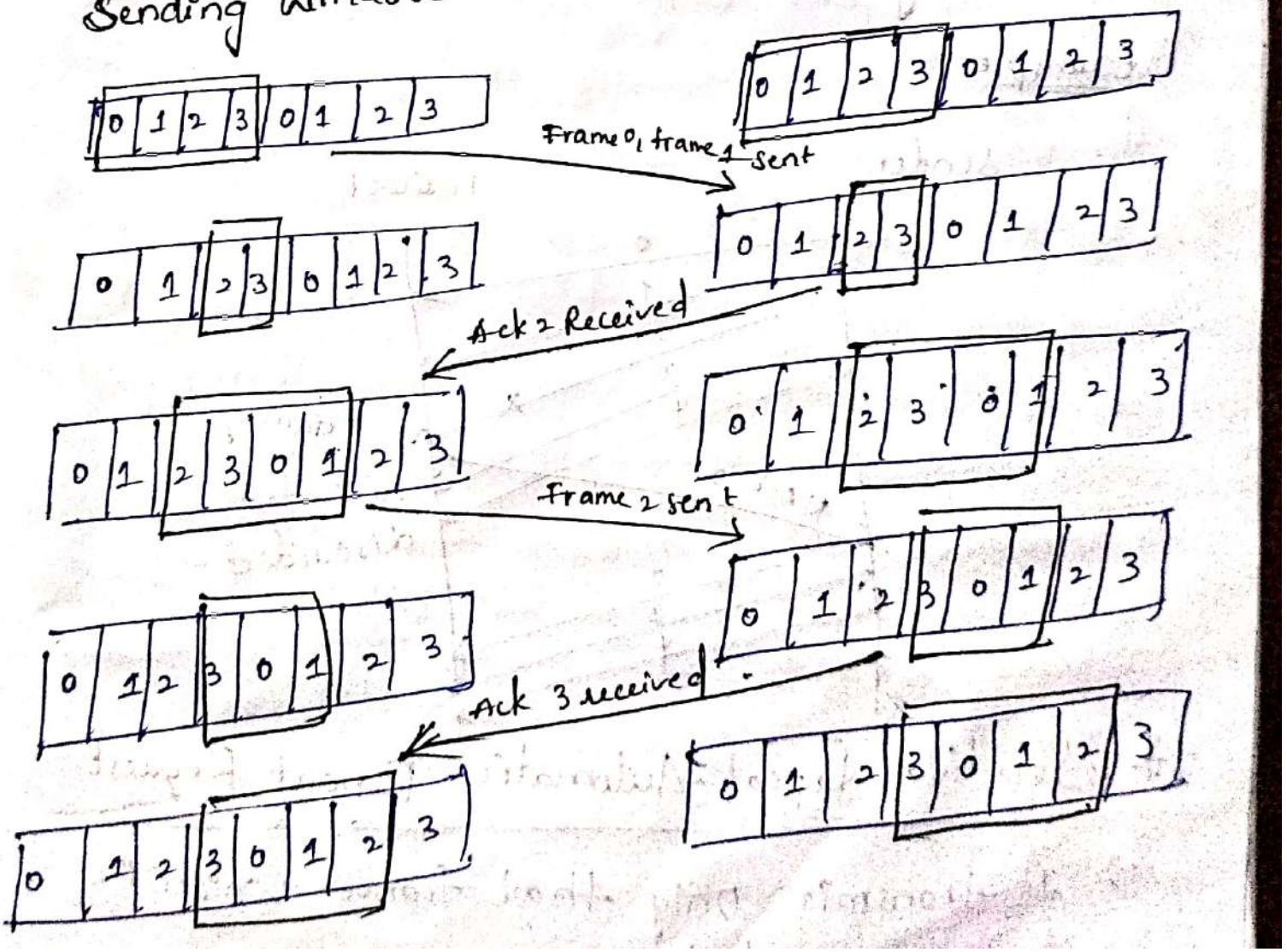
Ex:- If the Sending window size is 4, then the Sequence numbers will be 0,1,2,3,0,1,2,3,0,1 and so on.

Sol

* Suppose that we have Sender window each of size 4. so the Sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. the after sends following diagram shows the position of the windows after sending the frames and receiving acknowledgments.

Sending Window

Receiving Window.



* Types of sliding window protocols.

⇒ The sliding window ARQ (Automatic Repeat request) protocols are of two categories.

i) Go-back-N ARQ

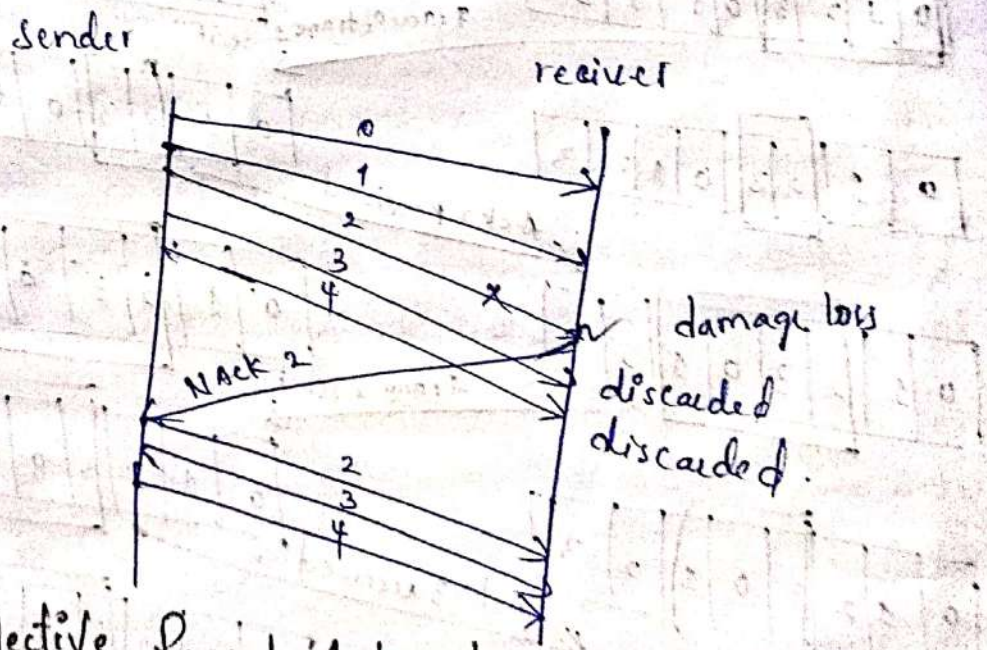
ii) Selective Request ARQ

i) Go-back-N ARQ

⇒ In this protocol we can send several frames before receiving acknowledgments.

⇒ we keep a copy of theese frames until the acknowledgment arrive.

Example :



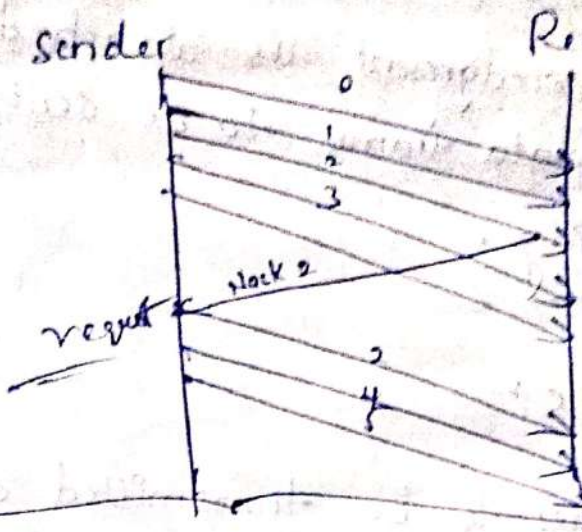
* Selective Repeat :-Automatic Repeat Request

⇒ It transmit only that frame which is damaged or lost.

* The receiver is capable of sorting the frames in proper sequence.

=> The Sender capable of searching the frame which negative Ack has been received.

Example:



* Examples of data Link protocols are:
  1) HDLC - High-Level Data Link Control.
  2) The Data Link Layer in the Internet.

* A One-Bit Sliding Window Protocol:

=> Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames

=> The Sliding window is also used in Transmission control protocol.

=> In these protocols, the Sender has a buffer called the Sending window and the receiver has buffer called the receiving window.

In One-bit sliding window protocol, the size of the window is 1. So the Sender transmits a frame, waits for its acknowledgment, then transmits the next frame.

=> It uses the concept of stop and wait for the protocol.

=> This protocol provides for full-duplex communications.

=> The acknowledgment is attached along with the next data frame to be sent by

Piggybacking.

Working principle:

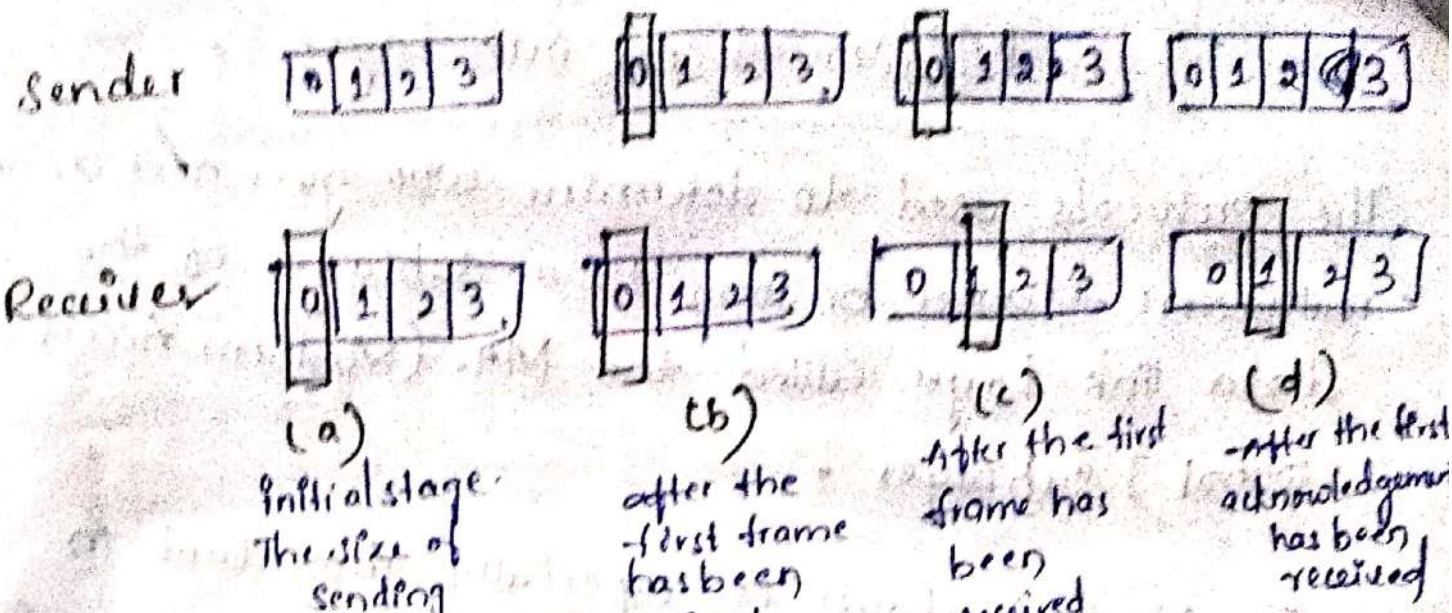
The data frames to be transmitted additionally have an acknowledgment field, ack field that is of a few bits Length.

-> The ack field Contains the Sequence number of the last frame received without error.

-> If this Sequence number matches with the Sequence number of frame to be sent, then it is inferred that there is no error and the frame is transmitted.

-> Otherwise, it is inferred that there is an error in the frame and the previous frame is retransmitted.

Ex:- The following diagram depicts a scenario with sequence numbers 0, 1, 2, 3, 0, 1, 2 and so on. It depicts the sliding windows in the sending and the receiving stations during frame transmission



(a) Initial stage. The size of sending window is 0. The receiving window is 1

(b) after the first frame has been sent

(c) After the first frame has been received

(d) after the first acknowledgement has been received

Example Data Link protocols

1) HDLC - High-Level Data Link Control.

→ HDLC is based upon SDLC (synchronous Data link Control) and provides both unreliable service and reliable service.

→ It is a bit-oriented protocol that is applicable for both point-to-point and multipoint communications.

~~2) The Data link layer in the Internet.~~

2) The Data link Layer in the Internet.

3) PPP - The point-to-point protocols

Medium Access Sub Layer :

The protocols used to determine who goes next on a multiaccess channel be long to a sublayer of the data link Layer called the MAC (Medium Access control) sublayer.

⇒ The MAC sublayer is especially important in LANs, many of which use a multiaccess channel as the basis for communication.

⇒ WANs, in contrast, use point-to-point links, except for satellite networks.

* The channel allocation problem :

~~two types~~

1) ~~static channel Allocation in LANs and MANs.~~

2) ~~Dynamic channel Allocation in LANs and MANs.~~

⇒ Channel allocation is a process in which a single channel is divided and alloted to multiple users in order to carry user specific tasks.

⇒ If there are N number of users and channel is divided into N equal-sized sub channels, each user is assigned one portion.

* Channal allocation problem can be solved by two schemes.

1) Static channel Allocation in LANs and MANs.
2) Dynamic channel Allocation in LANs and MANs.

* Static channel Allocation in LANs and MANs.

→ It is the classical or traditional approach of allocating a single channel among multiple competing Users Frequency Division Multiplexing (FDM)

* Dynamic channel Allocation

⇒ Station Model.

⇒ Single channel Assumption

⇒ Collision Assumption

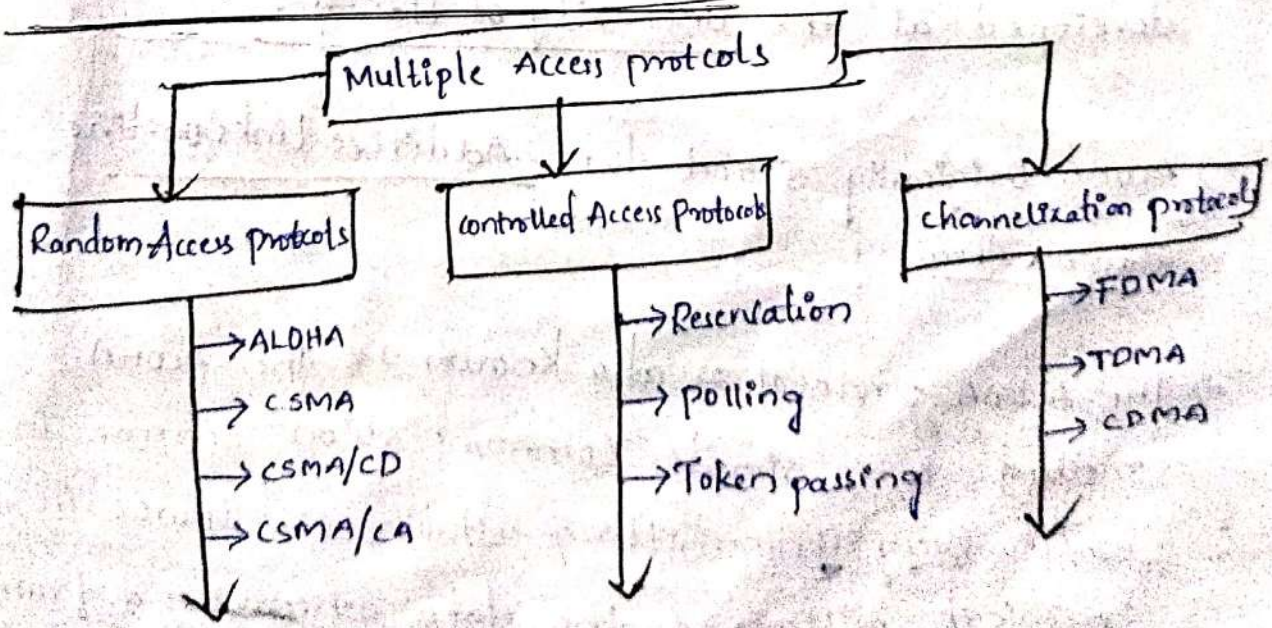
⇒ Continuous Time.

⇒ Slotted Time.

⇒ Carrier Sense

⇒ No Carrier Sense.

* Multiple access protocols:



Random Access Protocol

⇒ The random access protocols consist of the following characteristics:

1. There is no time restriction for sending the data. (you can talk to your friend without a time restriction).
2. There is a fixed sequence of stations which are transmitting the data.

⇒ random-access protocol is further divided into four categories, which are:

1. ALOHA
2. CSMA
3. CSMA/CD
4. CSMA/CA

* ALOHA Random Access Protocol :-

⇒ ALOHA net, also known as the ALOHA system.

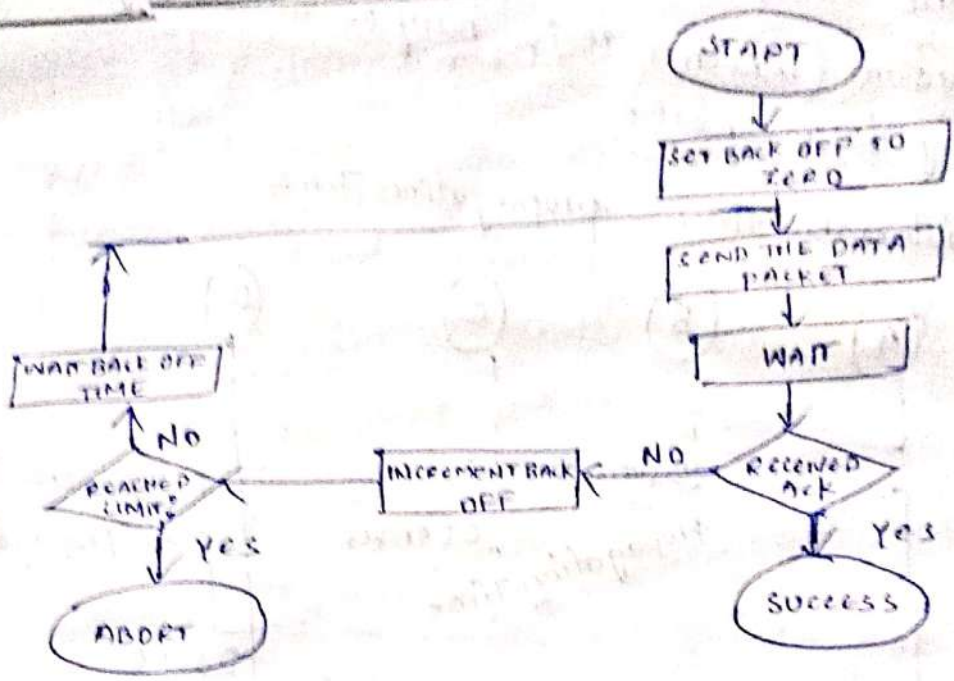
⇒ ALOHA was a pioneering Computer networking system developed at the university of Hawaii.

⇒ ALOHA originally stood for Additive Links on-line Hawaii Area.

⇒ The ALOHA protocol or also known as the ALOHA method is a simple communication scheme in which every transmitting station or source in a network will send the data whenever a frame is available for transmission.

* Whenever we talk about a wireless broadcast system or a half-duplex two-way link, the ALOHA method works efficiently.

Flow chart of Pure ALOHA :



⇒ To minimize these collisions and to optimize network efficiency as well as to increase the number of subscribers that can use a given network, the slotted ALOHA was developed.

⇒ This system consists of the signals termed as beacons which are sent at precise time intervals and inform each source when the channel is clear to send the frame.

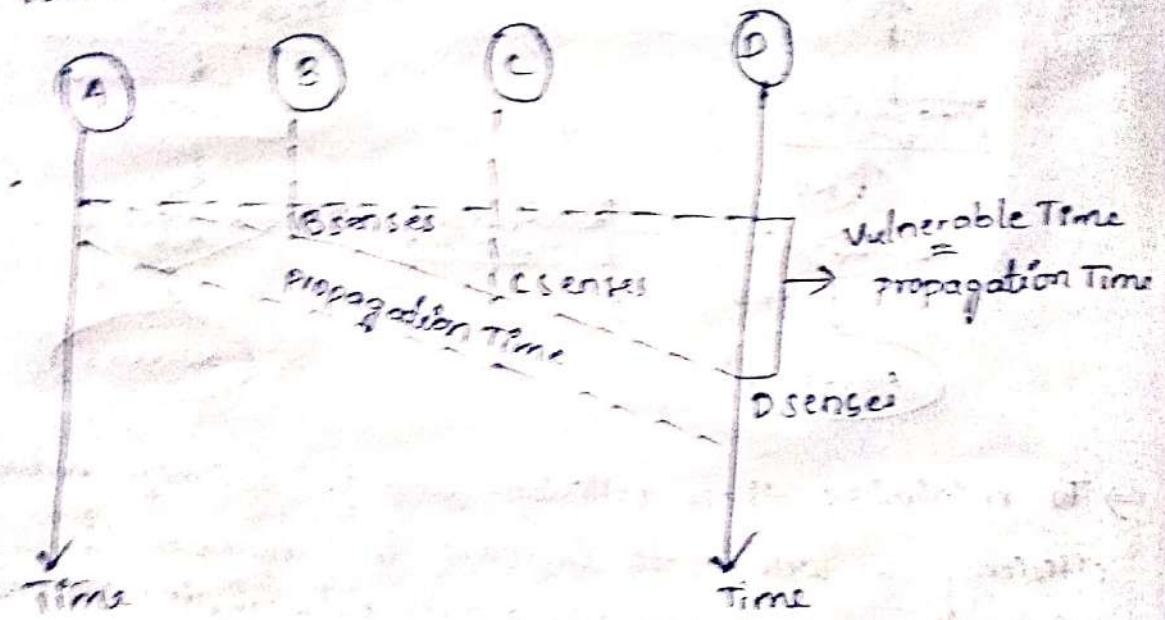
	PURE ALOHA	SLOTTED ALOHA
Data transmission	Stations can transmit the data randomly. Any number of stations can transmit data at any time.	Here, any random station can transmit the data at the beginning of any random time slot.

CSMA (Carrier Sense Multiple Access)

⇒ CSMA Stands for Carrier Sense Multiple Access.

⇒ The CSMA makes each station to first check the medium (whether it is busy or not) before sending any data packet.

* Vulnerable time = propagation Time

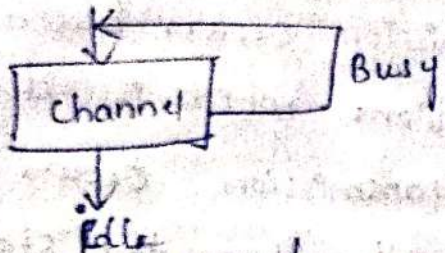


* The CSMA has 4 access modes:

1) 1 - persistent mode:
2) Non-persistent mode.
3) P-persistent mode.
4) O-persistent mode.

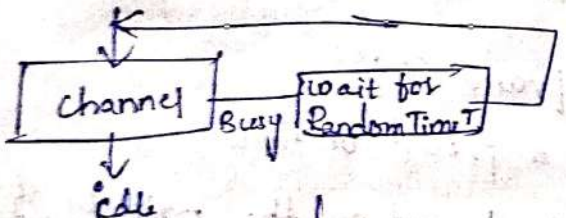
1) 1 - persistent mode: In this, first the node checks the channel, if the channel is idle then the node or station transmits data, otherwise it keeps on waiting and whenever the channel is idle, the stations transmit

the data frame



1-persistent method.

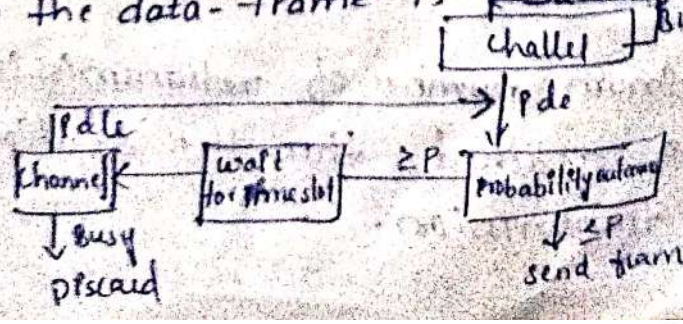
* Non-persistent mode: In this, the station checks the channel similarly as 1-persistant mode, but the only difference is that when the channel is busy it checks it again after a random amount of time, unlike the 1-persistent where the stations keep on checking continuously.



Non-persistant method.

* P-persistent mode:

In this, the station checks the channel 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 probability p and this cycle goes on continuously until the data-frame is successfully sent.



0-persistent

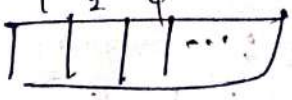
In this, the transmission occurs based on the superiority of stations which is decided beforehand and transmission occurs in that order. If the channel is idle, then the station waits for its turn to send the data-frame.

* CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

* CSMA with collision Detection (or) Avoidance CSMA/CA

* It is used for the wireless networks
* IFS = * Interframe space
  * It is a period on time
  * IF's is based on the priority of time.

contention window:
* Amount of time divided in slots



* Acknowledgement : +ve or -ve.

Algorithm of collision Resolution is:

1. The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
2. The station increments the retransmission counter.
3. If the maximum number of retransmission attempts is reached, then the station aborts transmission.

* Collision Free protocols :-

- Almost collisions can be avoided in CSMA/CD.
- They can still occur during the contention period.

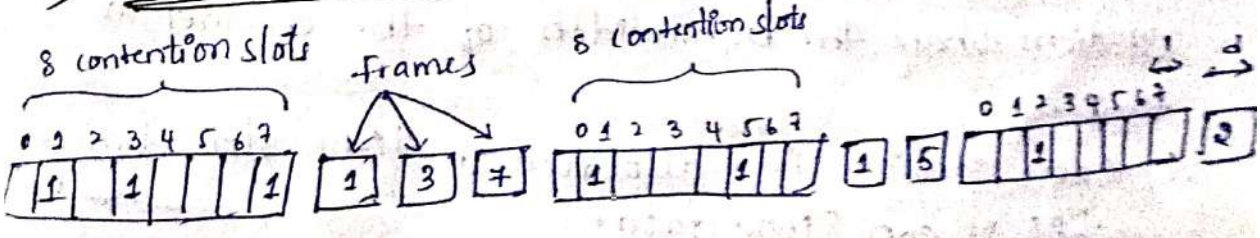
→ The collision during contention period adversely affects the system performance, this happens when the cable is long and length of packet are short.

* Some protocols that resolve the collision during the contention period.

* Bit-map protocol.
* Binary countdown
* Limited Contention protocols.
* The Adaptive Tree Walk protocol.

* Pure and Slotted Aloha, CSMA and CSMA/CD are contention based protocols.

1) Bit-map protocol :-



The basic bit-map protocol :-

⇒ In this collision-free protocol, the basic bit-map method, each contention period consists of exactly N slots.

⇒ If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot.

* channelization protocols

* channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

=) The three channelization protocols are.

1. Frequency-Division Multiple Access (FDMA)
2. Time-Division Multiple Access (TDMA)
3. Code-Division Multiple Access (CDMA).

1. Frequency-Division Multiple Access (FDMA):

* Frequency-division multiple access (FDMA), the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data.

2. Time-Division Multiple Access (TDMA).

* In time-division multiple Access (TDMA), the stations share the bandwidth of the channel in time.

-> Each station is allocated a time slot during which it can send data.

* Controlled Access protocols :

* All the stations consult one another to find which station has to right to send data.

3-types.

1. Reservation Method.
2. Pooling Method.
3. Token passing Method.

1) Reservation Method: A station Needs to make a reservation before sending data.

* Note: If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame.

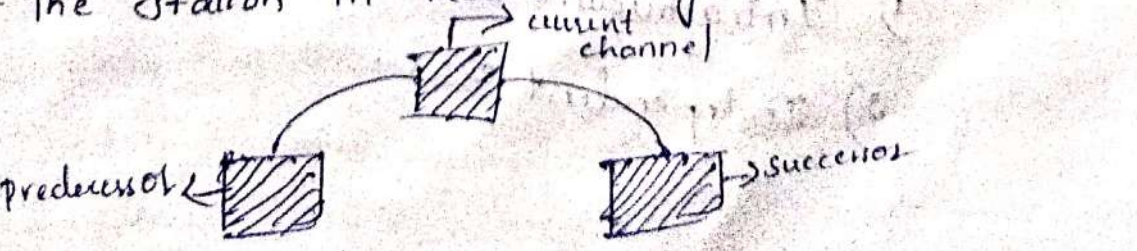
2) Pooling Method:

* It works with the Topology.
* One device is designated as primary station and other device designated as Secondary station.
* Data Exchange Must be made through primary station. pooling Method involves in two functions

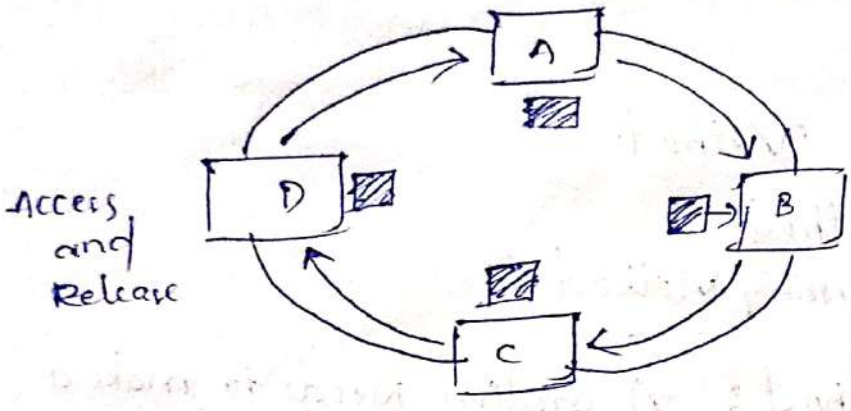
1. Selection Function. ⇒ It uses when primary station wants to send data
2. pooling Function. ⇒ " " " receive data

3) Token passing Method

* The station in Network originate in Logical ring.



* A special packet Token is passing through the Ring.
* The possession of the Token given the station right to Access the channel and send its Data.



* Wireless LANs (WLANs)

=> Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices with in a limited area forming LAN (Local Area Network)

Components of WLANs.

* Stations (STA) ~~=> stations compris.~~
  - two types
    1) Wireless Access point (WAP or AP)
    2) client.

* Basic Service set (BSS)
  - two types
    1) Infrastructure BSS
    2) Independent BSS.

* Extended Service set (ESS) → set of all connected BSS.
* Distribution system (DS) → It connects access points in ESS.

Types of WLANs

↓
two types.

1) Infrastructure Mode.
2) Ad Hoc mode.

Advantages of WLANs

* They provide clutter-free homes, offices and other networked places.
* The system is portable with in the network coverage.
* Access to the network is not bounded by the length of cables.
* Installation and setup are much easier than wired LANs.
* The equipment and setup costs are reduced.

Disadvantages of WLANs

* WLANs are slower than wired LANs.
* Since radiowaves are used for communications, the signals are noisier with more interference from nearby systems.
* Greater care is needed for encrypting information. Also, they are more prone to errors.
* they require greater bandwidth than the wired LANs.

UNIT - III

Network - Layer

* Design Issues :-

* Network Layer is majorly focused on getting packets from the source to the destination, routing error handling and congestion control.

* Before learning about design issues in the Network Layer, the various functions are.

1) Addressing
2) packeting
* Routing
* Inter-networking.

* The network Layer comes with some design issues they are

* store and forward packet switching.
* Services provided to Transport Layer.
* Implementation of connectionless Service.
* Implementation of Connection Oriented Service.

* Comparison of Virtual-circuit and Datagram Subnets.

* Routing algorithms :-

Routing :-

→ Routing should be send to destination, in which path the packet should be transmitted to reach destination.

* The main fundion of the network Layer is routing packets from the source machine to the destination machine.

* Routing Algorithm classified into 2 ways.

1. Non-Adaptive Routing (or) Static Routing.
2. Adaptive Routing (or) Dynamic Routing.

→ Non-Adaptive Routing (or) Static Routing : Routing process should be design in advance and all the Routing process will be store in Routers, when the Booting Computers.

→ It is classified into two types.

1. Flooding : All the incoming packets will be Transmitted to all out going links.
2. Random walk : Incoming packets will be transmitted to the neighbours links randomly.

* Adaptive Routing (or) Dynamic routing : It is using three parameters.
  1. Hop Count
  2. Distance
  3. Transmit time.

* Non-Adaptive Routing (or) Static Routing Algorithms :
  1. Shortest-path Routing.
  2. Flooding
  3. Flow-based Routing.

Shortest-path Routing :

* Travelling packets from source to destination
* Route must be shortest Route.
* Shortest path should identified by using following functions: cost, Distance, Time, Traffic and Bandwidth.

⇒ The idea is to build a graph of the subnet with each node of the graph representing a router and each arc of the graph representing a communication or Link.

* To choose a route between a given pair of routers the algorithm just find the shortest path between them on the graph.

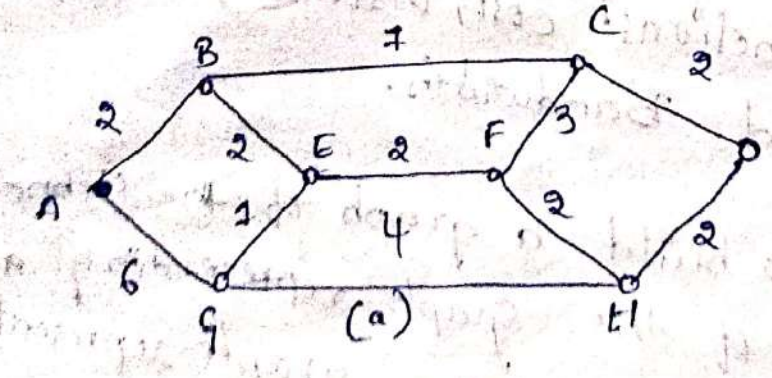
1) Start with the Local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent model.

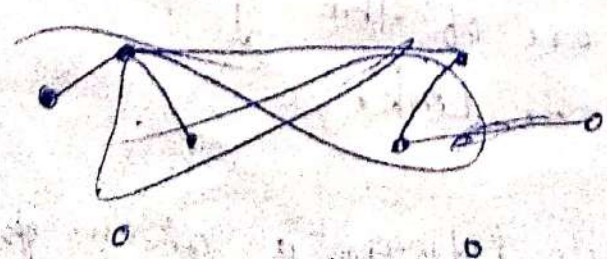
2) Examine each neighbhour of the node that was the Last permanent node.

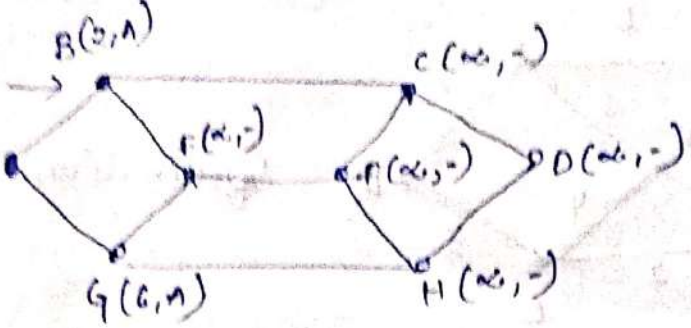
3) Assign a cumulative cost to each node and make it permanent.

4) Among the List of tentative nodes
   a) Find the node with the Smallest cost and make it permanent.
   b) If a node can be reached from more than one route then Select the route with the shortest cumulative cost.

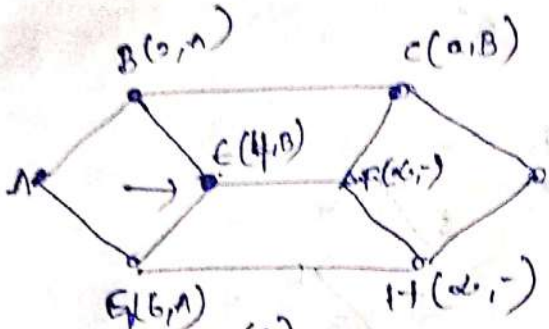
5) Repeat steps 2 to 4 until every node becomes permanent.



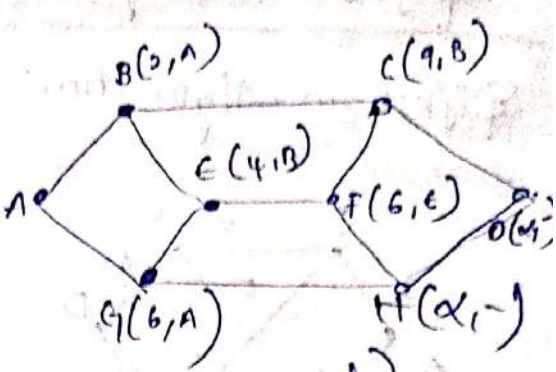




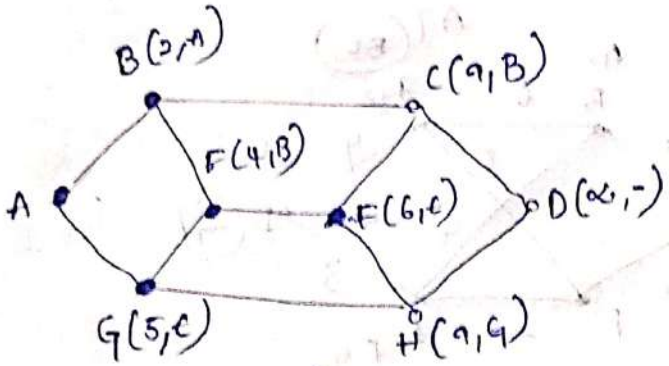
(b)



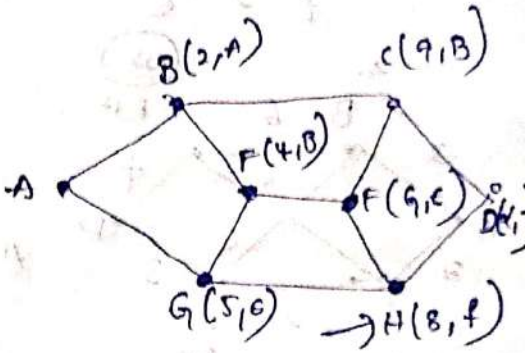
(c)



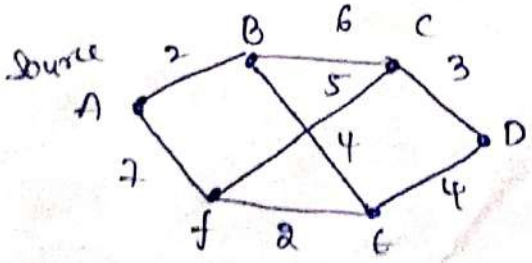
(d)



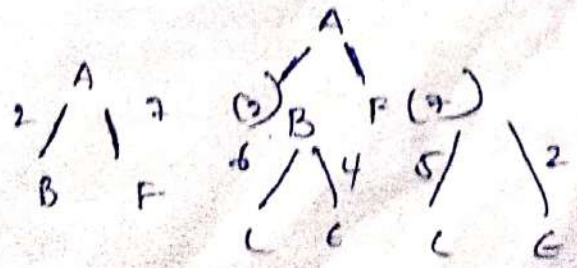
(e)

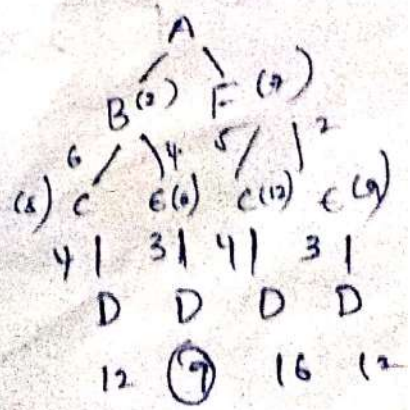


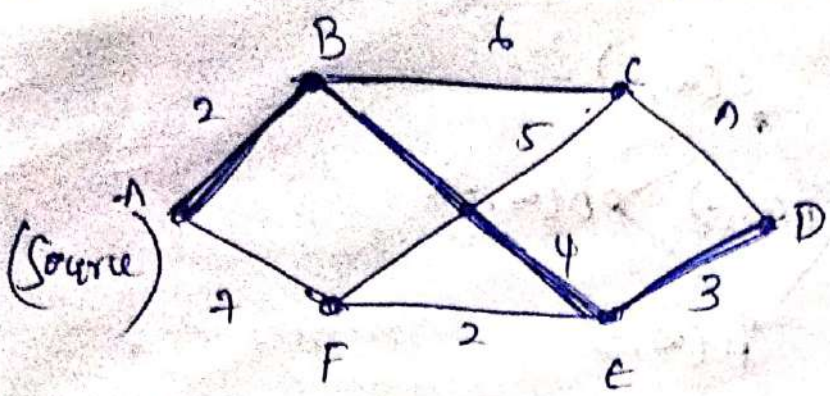
(f)



destination.



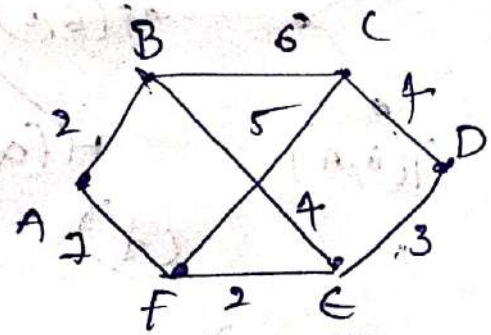


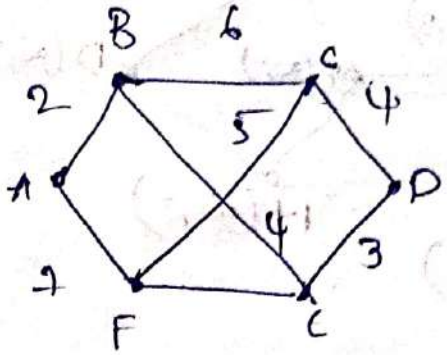


Destination.

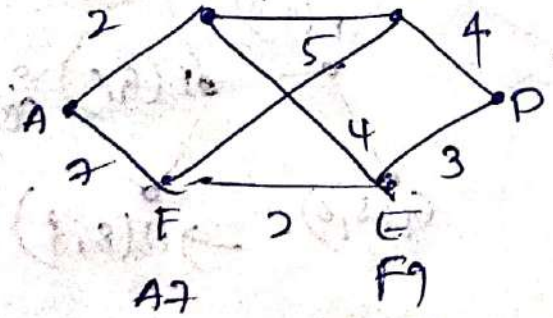
Dijkstra Algorithm

Dijkstraw Algorithm:



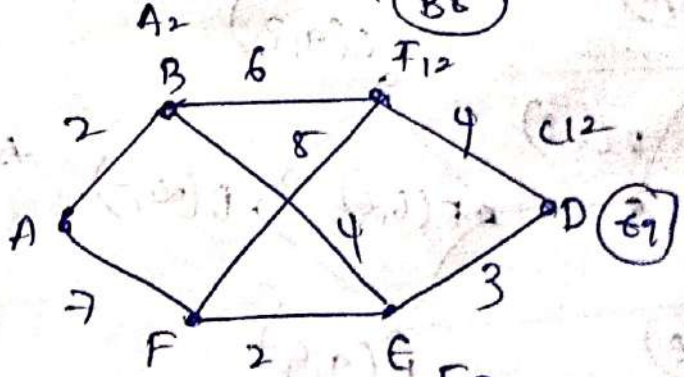


A2 (B8)

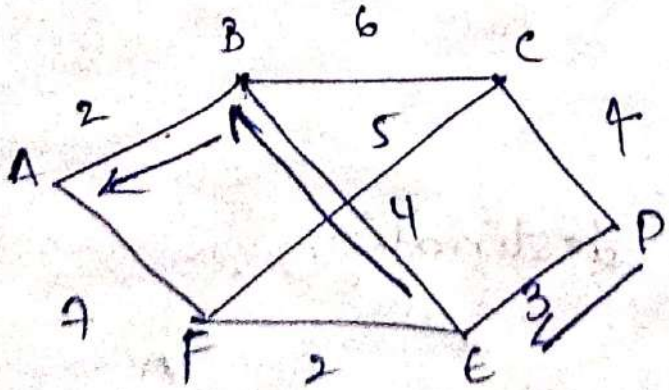


A7 F9 (B6)

A7 (B8)



A7 (B6)



* Flodding

* Broad Cast the packets
* Sending the packets to all out going links except to link from which it was received.

⇒ Flooding is a non-adaptive routing technique ~~follow~~.

⇒ When a data packet arrives at a router, it is

* Distance Vector routing

In distance Vector routing, the Least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a Vector (table) of minimum distances to every node.

Mainly 3 things in this.

Initialization

sharing

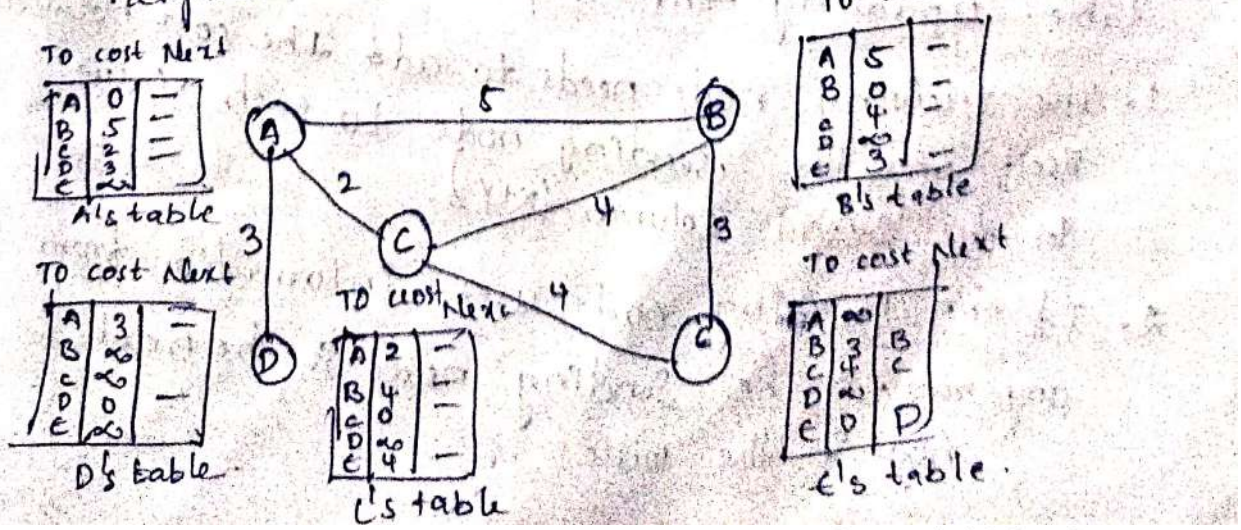
updating.

Initialization:

Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.

⇒ so for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors.

⇒ ~~Below~~ The distance of any entry that is not a neighbor is marked as infinite.



Sharing

The whole idea of distance vector routing is the sharing of information between neighbors.

→ Although node A does not know about node C, node C does. So if node C shares its routing table with A, node A can also know how to reach node C.

→ On the other hand, node C does not know how to reach node D, but node A does.

→ If node A shares its routing table with node C, node C also knows how to reach node D.

⇒ In other words, nodes A and C, as immediate neighbors ~~periodically and when there is a change~~. can improve their routing tables if they help each other.

NOTE : In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

* Updating :

When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating three steps.

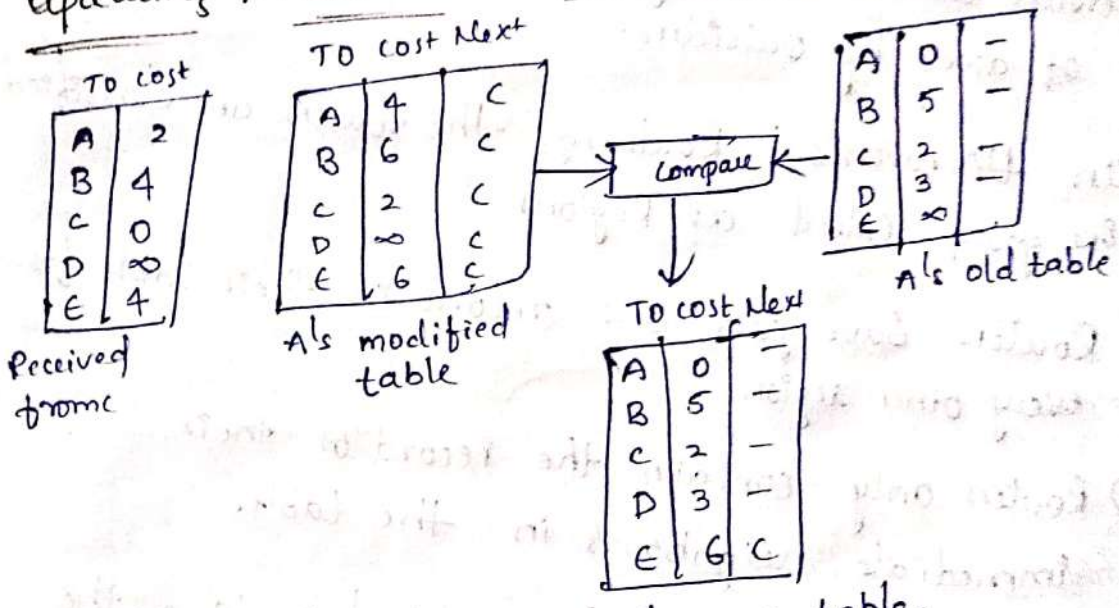
1. The receiving node needs to add the cost between itself and the sending node to each value in the second column. (x+y).
2. If the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

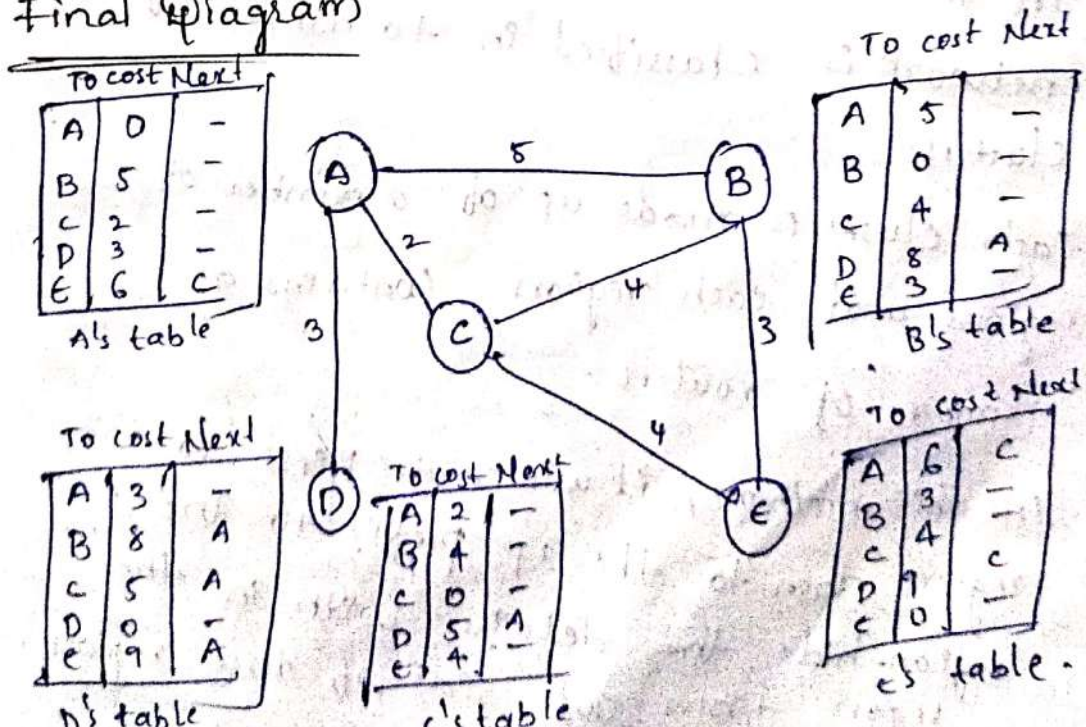
a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

b. If the next-node entry is the same, the receiving node chooses the new row.

Updating in distance vector routing



Final Diagram



Hierarchical routing :-

⇒ Hierarchical routing is the procedure of arranging routers in a hierarchical manner.

→ A good example would be to consider a corporate intranet.

⇒ INTRANET : An intranet is a computer network for sharing information, collaboration tools, operational systems, and other computing services within an organization, usually to the exclusion of access by outsiders.

⇒ In Hierarchical Routing, the routers are classified in groups, called as Regions.

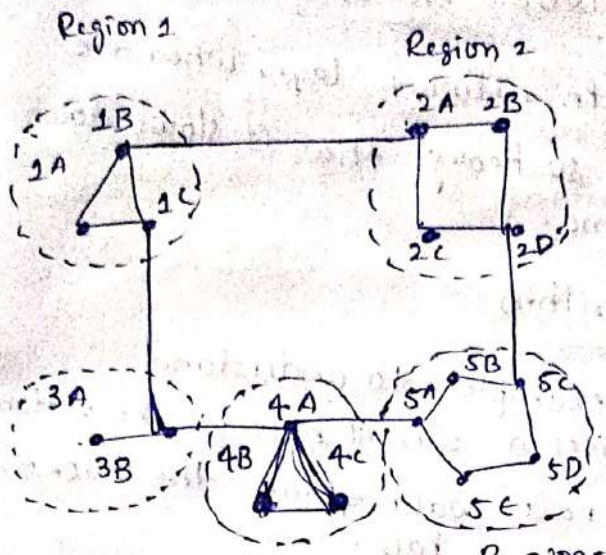
⇒ Routers save just one record in their table for every other region.

⇒ Routers only contain the record of their immediate neighbours in the table.

⇒ In the three Level hierarchical routing, the network is classified in to number of clusters.

→ Each cluster is made up of a number of regions and each region contains a number of routers.

⇒ In this method, it will route first to the region then to the IP prefix to the region-hide the details with in the region from out side of the region.



Full table for 1A Hierarchical table:

Dec1.	line	Hops
1A	-	-
1C	1B	1
2A	1C	1
2B	1B	2
2C	1B	3
2D	1B	3
2A	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
4A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5
1A	-	-
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

* CONGESTION CONTROL ALGORITHMS

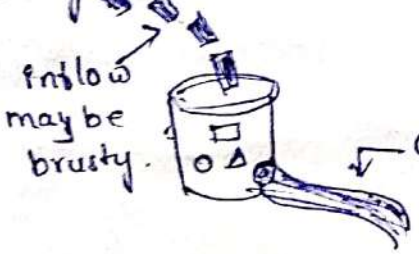
=) A state occuring in network layer when the message traffic is so heavy that it slows down network response time.

* Leaky Bucket Algorithm

Let us consider an example to understand.

=) Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at constant rate.

=) When the bucket is full with water additional water entering spills over the sides and is lost.



Steps:-

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

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

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

=) In practice the bucket is a finite queue that outputs at a finite rate.

* Token Bucket Algorithm

=) Need of token bucket Algorithm:

=) The leaky bucket algorithm enforces output pattern at the average rate, no matter

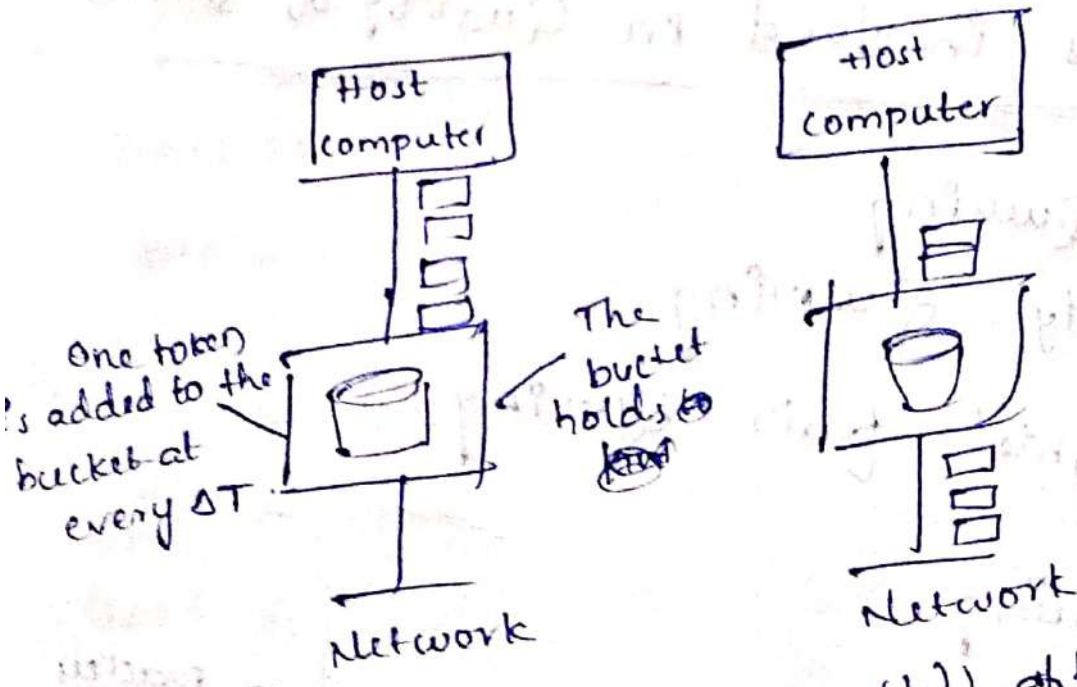
how bursty the traffic is.

→ 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.

⇒ Steps:-

1. In regular intervals tokens are thrown into the bucket.
2. ~~If there is a~~ The bucket has maximum capacity.
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.



* Quality of Service

=> In quality of Service create an appropriate Environment for Traffic.

→ Quality of Service Should be involve in following criterials

1. Relibity : Lack of reliability means loosing a Packet or Ack.
2. Delay : Source to destination delay.
3. Jitter : Variations in delay.
4. Bandwidth.

=> Techniques involved in Quality of Service

1. FIFO Queuing
2. priority Queuing
3. weighted fair Queuing

* FIFO Queuing

The Simplest algorithm is FIFO, where packets are Served in the same order as they arrive in the queue.

=> Scheduling is often linked to queue (buffer) management Schemes.

⇒ A FIFO queue is a queue that operates on a first-in, first-out (FIFO) principle.

* Priority Queuing

* problem with priority Queuing is Starvation.

* Starvation means low priority packets may or may not be processed.

(or)

* The Queue never get chance to processed.

⇒ priority queuing allows you to ensure that important traffic applications, and users take precedence.

* Weighted fair Queuing. (WFQ)

⇒ WFQ is a flow-based queuing algorithm used in Quality of service (QOS). that does two things simultaneously.

⇒ It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows.