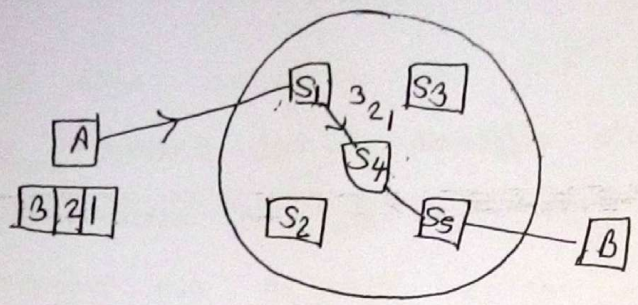
2] VIRTUAL CIRCUIT SWITCHING :-

It is a combination of circuit switching & datagram switching.



Here first each switch will check & establish the connection. Then that connection will get freeze. Now after connection is fixed, message is divided into different packets known as datagram. ~~These message~~ Switch S_1 will transfer all the packets after some duration to the next switch. Now here next intermediate switch S_4 will send the packets to next one.

Acknowledgement of single packet is taken

UNIT 2 :-

DATA LINK LAYER :-

- second last layer of OSI
- last layer of TCP/IP.

Functions are :-

- Data Transfer
- Frame synchronization :- Divides data into frames
- Flow control :- Proper frames are flowing without any errors.
- Error control :- Error detection
- Link Management.

FRAMING :- The bits that are to be transmitted are broken into discrete frames. The process of braking the bits into frames is known as FRAMING.

→ Frame size is decided by Data Link Layer as per channel capacity. Each frame can even have different size even.

→ Now, each frame is given 2 extra bits [for starting & ending]

→ In order to guarantee that bit frame is error free checksum is guaranteed. If order of calculated and observed value is equal then no error else error.

AT RECIEVER END | WHICH WAS CALCULATED AT SENDER END

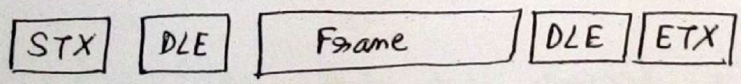
I METHODS OF FRAMING :-

1) CHARACTER COUNT :- No. of characters in a frame is fixed & acc. to that count frame is created.

→ Not a successful method as typing mistake can occur while providing frame size.

2) STARTING & ENDING CHARACTER WITH CHARACTER STUFFING :-

In this method each frame is created in following ways :-



STX → start of text

DLE → Data link escape

ETX → End of text

→ Here since we have to provide extra number of bits due to which bandwidth increases. [As size of frame has Increased].

7) STARTING & ENDING FLAG :-

~~A special bit i.e. flag~~

It is a special single bit applied at starting & ending of frame and tells the boundary of the frame.

- Since here only 1 bits is introduced on both sides.

1 FLOW CONTROL :-

For flow control data link layer uses SLIDING WINDOW PROTOCOL.

V.V. Imp.

SLIDING WINDOW PROTOCOL :-

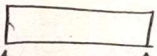
~~It creates a window~~

→ Sender & Reciever creates a window that contains the maximum no. of bits that can be transferred simultaneously.

~~Or~~

→ Then sender has to advertize his window size to receiver before ~~frame synchro~~ flowing data & also draws window size.

→ Each window has 2 walls :-



left wall right wall.

→ Now after receiving sender's window size, receiver also sets his window size.

→ After transmitting first bit to receiver, only left wall ~~is moved~~ will move rightwards by 1.

→ Right wall will only move if any acknowledgement is send by receiver.

- For acknowledgement a technique Piggy Backing is used.
- PIGGY BACKING :- Every packet is not acknowledged by the receiver but receiver will send a combined feedback to sender.

→ In piggy backing the acknowledgement sent ... it means that receiver have acknowledged that ~~received~~ 0, 1, 2 packets, if ~~it~~ now sender has to send 3rd packet number. are received

Sender

Sender window size = 6

0 1 2 3 4 5 6 7 0 1 2 3 4 5

↑ left wall ↑ right wall

Data 0 →

0 1 2 3 4 5 6 7 0 1 2 3 4 5

→ Data 1

0 1 2 3 4 5 6 7 0 1 2 3 4 5

→ Data 2

0 1 2 3 4 5 6 7 0 1 2 3 4 5

~~0~~ 3 4 5 6 7 0 1 2 3 4 5

Receiver

0 1 2 3 4 5 6 7 0 1 2 3

↑ left wall ↑ right wall

0 1 2 3 4 5 6 7 0 1 2 3 4 5

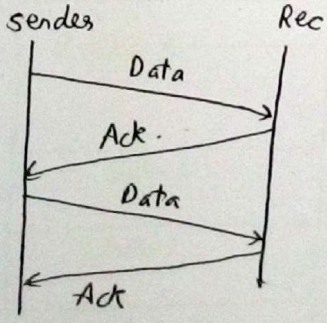
0 1 2 3 4 5

0 1 2 3 4 5

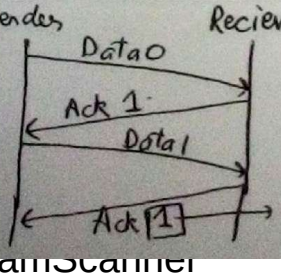
← Ack 3

→ After receiver have send Ack 3, the right wall will shift rightward to make window size = 6 & ~~discards digits~~ sender will permanently discard bits 0, 1, 2.

→ It means that till receiver does not send acknowledge, the previous bits are not discarded to prevent the problem of failure of transmission.



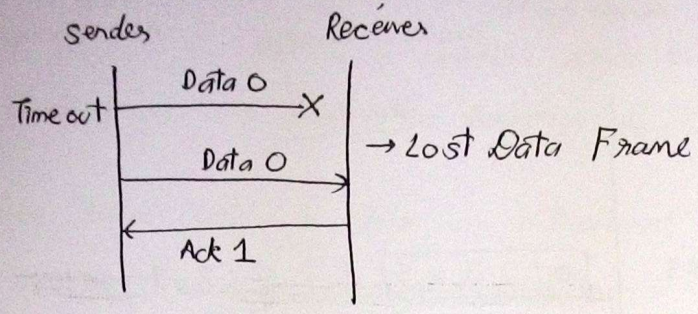
STOP AND WAIT PROTOCOL :-

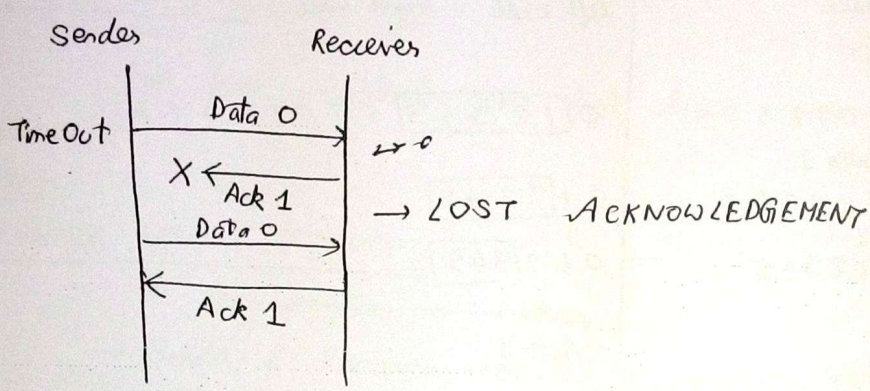


→ DAMAGED FRAME

* Here recievers have to send Ack 2, but here ack 1 is send it means that data 1 is not send successfully.

→ So here receiver is telling damaged frame by the help of acknowledgement.

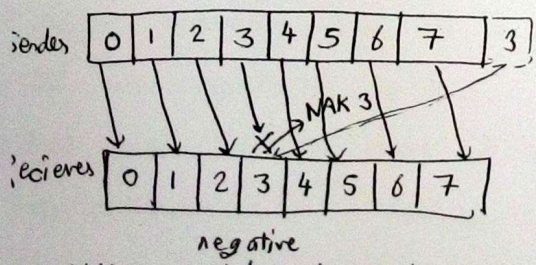




→ Here ~~since~~ if sender is sending the same data again, then receiver will recognize that ack have not received to sender. Thus it discards the previous data & accepts it.

→ DISADVANTAGE :- ~~Since~~ here same data has to be send again & again.

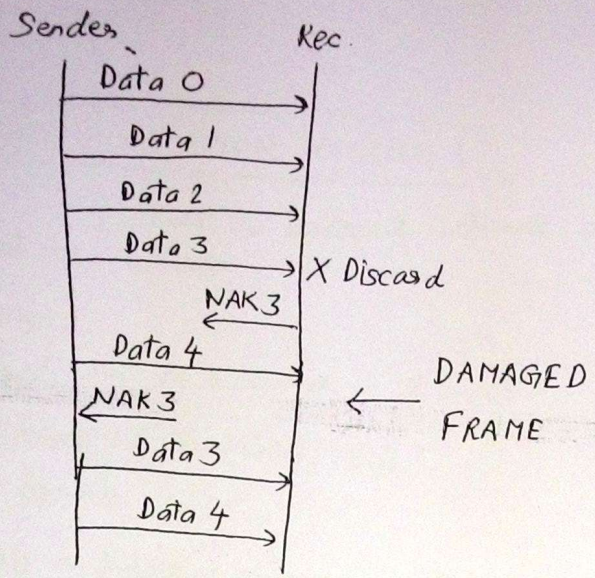
GO BACK N PROTOCOL :-

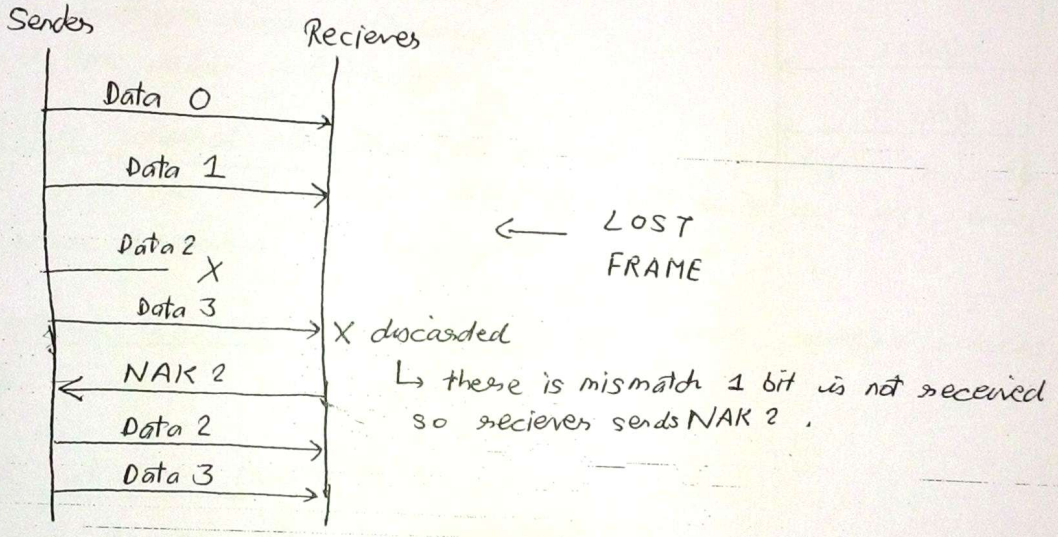


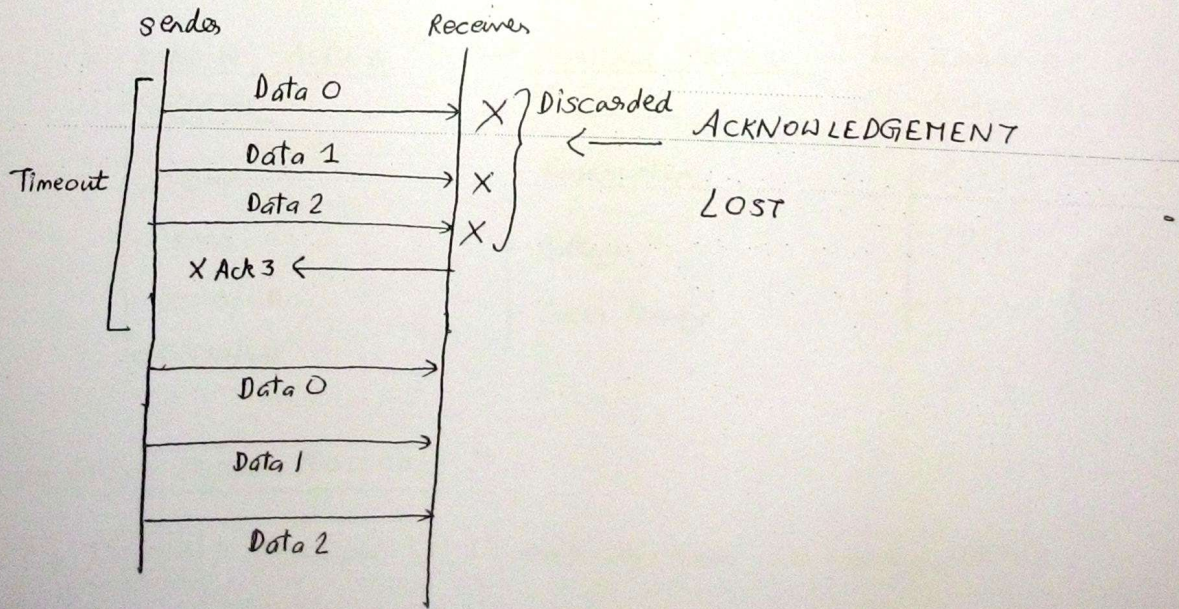
negative

→ NAK 3 → ~~Not~~ acknowledgement 3.

→ Here sender will keep on sending 4, 5, 6. When sender received NAK 3, the sender will resend all the ~~pa~~ bits from that data i.e. 3 ~~to~~ again.

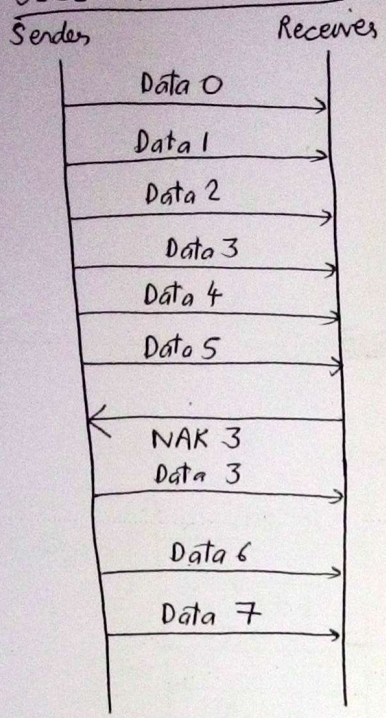






DISADVANTAGE :- Whole data is send again & again in case of failures.

SELECTIVE REPEAT :-



. MAP LAYER :-

CHANNEL ALLOCATION PROBLEM

How to allocate channel simultaneously to multiple users without any collision.

~~2 ways:~~

Channel can be allocated in 2 ways :-

- Static (FDM, WDM, TDM)
- Dynamic

FDM → frequency division multiplexing
WDM → wavelength division multiplexing
TDM → Time division multiplexing

In FIXED channel allocation, all channels are predefined i.e. if ~~user is~~ user is not present ~~that~~ then that slots are left empty. Thus, wastage of spaces is taking place.

For DYNAMIC CHANNEL ALLOCATION we have multiple access protocols.

MULTIPLE ACCESS PROTOCOLS :-

These are divided into 3 categories :-

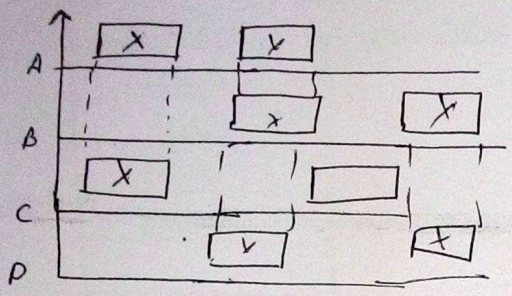
- RANDOM ACCESS PROTOCOL
  - ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA
- CONTROL ACCESS PROTOCOL
  - Reservation
  - Polling
  - Token Passing
- CHANNEL ALLOCATION
  - FDMA
  - TDMA
  - CDMA

→ RANDOM ACCESS PROTOCOLS :-

- ALOHA :- developed by University of Hawai in early 1970s.

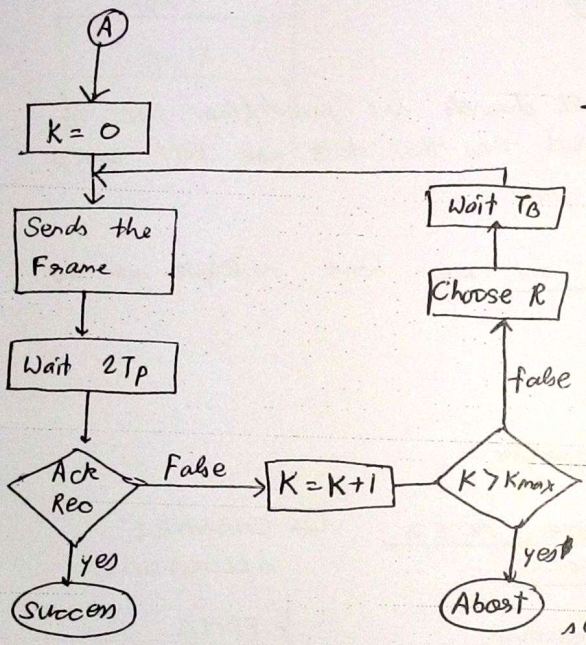
  It is of 2 types :-
  - Pure
  - Slotted.

4 stations A, B, C, D are communicating via same channel. Also each station are sending 2 packets. So now few packets are destroyed due to collision.



To overcome this problem ALOHA is used.

→ PURE ALOHA



→ Here,

In the pure ALOHA the round trip propagation delay is $2T_p$ where T_p is time taken by message to reach from send to receiver. As here, it relies of on acknowledgement, so sender will even wait for acknowledgement after message is reached to reciever hence sender has to wait $2T_p$.

→ Here each station has maximum 15 turns (K_{max}) i.e. no sender can send 15 times (maximum) in case of failure of acknowledgement from receiver.

→ CHOOSE R :- It is a random number.

→ T_B :- backoff Time

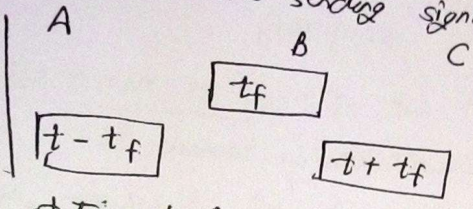
→ Before retransmitting sender is waiting for some random time, known as Backoff Time (T_B).

DISADVANTAGES

→ Time Delay.

LENGTH OF TIME WHERE THERE IS POSSIBILITY OF COLLISION :

If a station B starts sending signal at t_f.



→ So a station should wait for the duration of time to avoid collision i.e. 2 times the transmission time.

→ VULNERABLE TIME :- Time in which there is a possibility of collision i.e. for pure ALOHA the vulnerable time is $2T_f$.

THROUGHPUT OF PURE ALOHA (S) :-

~~$S = 4Xe^{-2G}$~~ $S = (GXe)^{2G}$

G :- average number of frames generated by the system during one frame transmission time.

The maximum throughput of pure ALOHA is :- $S_{max} = 0.184$

Q.) In pure ALOHA a network transmits 200 bit frames on a shared channel of 200 KBPS. What is throughput of the system when 1000 frames/sec are produced.

Ans:) 200 bit frames / 200 KBPS.

Frame transmission time = $\frac{200}{200} = 1ms$

As 1000 frames in 1 sec.
So 1 frame in 1msec.

$S = 4Xe^{-} = 0.135$

FOR 500 FRAMES

$G = \frac{1}{2}$

$S = 4Xe^{-1} = 0.184$

→ So, out of 500 frames, 92 frames are successfully transmitted

→ Now to decrease throughput vulnerable time should be decreased: which is performed by ALOHA slotted ALOHA.

SLOTTED ALOHA

→ Different slots are fixed for all stations.

→ Now if station A is given 5 ms, then if his work here we are not considered for the whether whole information is transmitted or not.

$$S = G \times e^{-G}$$

Here throughput $S_{max} = 0.368$.

Ex:- For 1000 frames,

$$S = 1 \times e^{-1} = 0.368.$$

→ So, even here from 1000 frames only 368 frames are transmitted.

↳ CSMA

– Carry or sense Multiple Access.

→ First sense if channel is free then transmit otherwise leave it.

→ PROBLEM :- When a station B sense that channel is free & in that duration only if station C even sense that channel is free & now these will be collision of B & C.

→ To minimize the collision in CSMA we need :-

Vulnerable Time is the propagation time $T_p + T_t$.

T_t :- time at which station is acquiring channel.

DISADVANTAGE : What a station should do if channel is free or busy?

→ So for this some methods are developed to for allocation of channel
- Non - persistent method
- 1 persistent method
- & p persistent method.

- 1 PERSISTENT METHOD :- In this when channel is busy, it will start transmitting

(MAXIMUM COLLISION)

- NO PERSISTENT METHOD :- In this the station that has a frame to sense, if channel is idle that immediately transmitted otherwise station waits for random amount of time.

→ Here 2 station can have some wait time. → DISADVANTAGE.

- P-PERSISTENT METHODS: Here, channel has time slots that are equal to or greater than propagation time.

(BEST METHOD).

DISADVANTAGE :- It is not telling any technique to avoid or remove collision

↳ CSMA/CD :-

- Carrier sense multiple access with collision detection

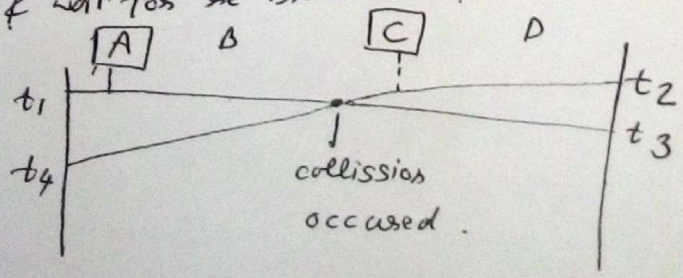
→ First station A, found at time t_1 that channel is empty by persistent method, thus it acquire & transmitted.

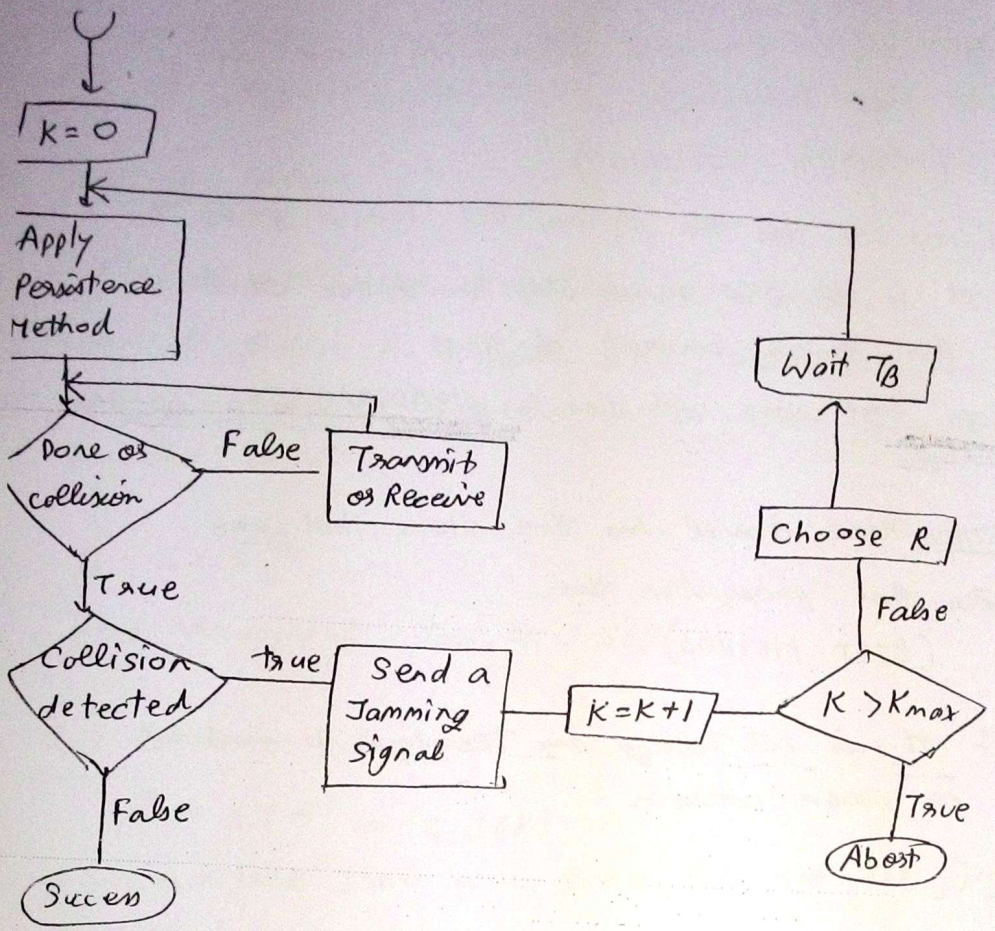
→ At time t_2, station C found that channel is idle by 1-propagation method. [sends info in both the direction].

At time t_3, C found that collision occured & thus C aborted & waits for re-transmission.

At time t_4, when A receive the bits from frame C.

Now at time t_4, A comes to know that collision occured, it would not wait for acknowledgement thus, it will abort A & wait for re-transmission.





Persistense Method :- It will sense the channel.

Jamming signal will advertize all the station that collision have occured & thus no other station should transmit at that time.

- The channel is sensed by measuring the energy level of channel. Energy level can have 3 values :- 0, normal or abnormal.

  0 → idle

  normal → somebody else is using ~~cha~~.

  abnormal → collision.

~~COLLISION AV~~

- **CSMA/CA** :-

  ~~Col~~ Carrier sense multiple access with collision Avoidance.