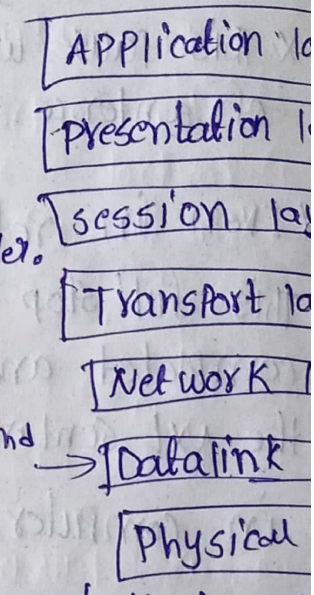
unit-2 Datalink layer

Link layer services

Data link layer is layer 2 in the osI reference model. we have 7 layer in osI model. Data link is 2nd layer. we can also called as link layer

* The role of data link layer when the Network layer creates the packet it gives that packet to th data link layer. in order to add header and trailer.
* after adding the header and trailer the Network layer pdu will call this as a Frame
* Data link layer Deals with Frames and it is th responsibility of data link layer is Moving data (fi from one node to another node.
* we know the physical layer converts the data in bits or signals. data link layer encapsulates such o The information such as physical adress of the source and physical adress of destination
* They only it enables node to node communicati
* we will see what are the various services offere by data link layer.



Services provided by Data link layer

1) Framing
2) Physical Adressing
3) Flow control
4) Error control
5) Access control

Framing

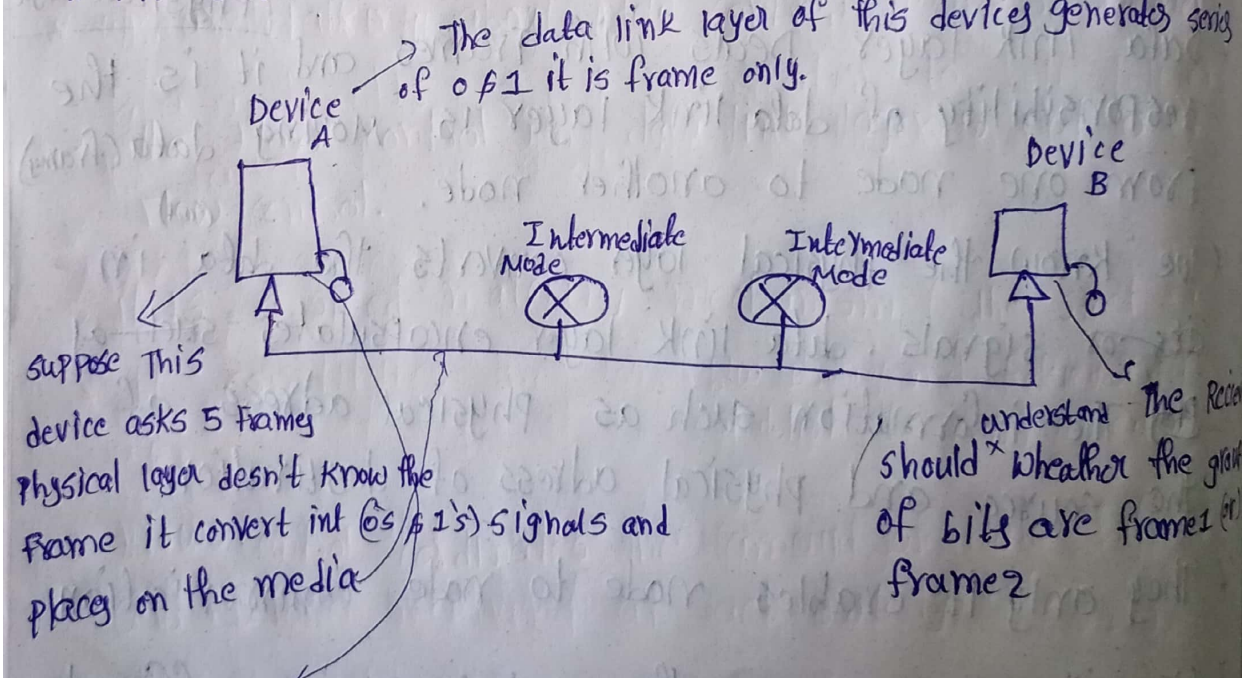
The data link layer needs to pack bits into frames so that each frame is distinguishable from another.

Ex: if i want to deliver 5 sentences in my speech after ~~sending~~ delivering Each i will give a pause

* This pause will helps the listener to know the end of sentence

* Even in return communication also we use full stop This full stop will help ~~reader~~ know the current sentence has completed and whatever follows after the full stop the next sentance

* in computer Network also data link layer of this device



* Then only the communication is sucessful. framing is a important task in Data link layer

ex: our postal system practices a types of framing. → frame
the simple act of inserting a letter into an envelop
seperates one piece of information from another, the
envelope serves as the delimeter.

* likewise in CN also we need some techniques inorder to distingush one frame to another. This what we called as Framing.

* The first service of the data link layer is framing

physical adressing

we know whatever Recieved from the Network layer

* A Frame is the encapsulation of the header and trailer information with the packet.

* in the header, is contains the source and the destination of MAC adress are dealt.

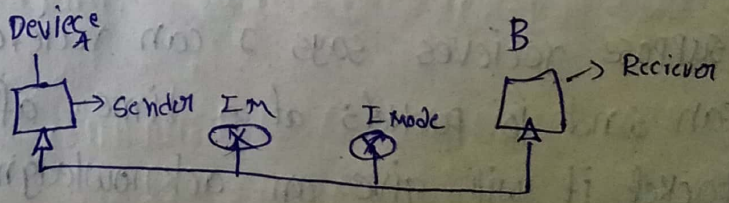
* observe After adding the ip adress information in the Network layer

* The data link layer add the source & destination of MAC adress.

Flow control :

* if the sender is slow sender. He is the Fast Recieve

* it sendes slowly and it Recieves No problem in this Approach



* He is the Fast Sender. He can send 100 packets at a time but this Reciever Recieves 10 packets at a time so it becomes overloaded and fine Point He can't handle the situation.

The packets will be lost.

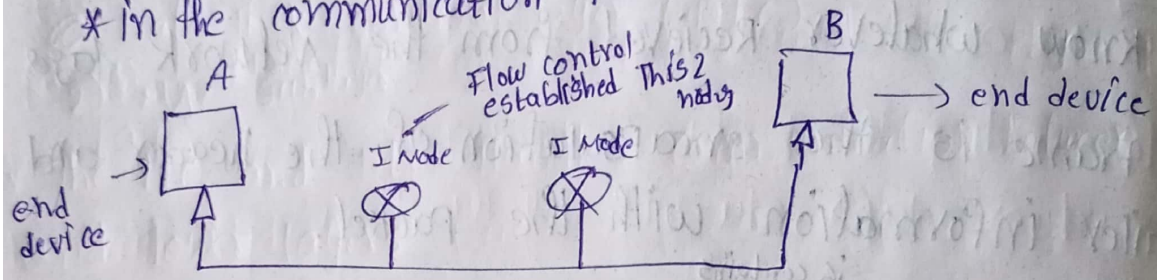
* To solve this problem we need to establish a flow control

→ Flow control is one of the duties of data link control sublayer → talk about in future

* The sublayer deals with the sub control.

* Flow control means it deals with end to end Flow control.

* in the communication pattern device A and device B



* we are talking about flow control b/w these 2 nodes A & B

→ The Flow control in data link layer is end to end Flow control.

→ it is a speed matching mechanism. (The speed matching b/w sender and Reciever should establish the communication with loss

→ Flow control cordinates the amount of data that can be sent before recriving an acknowledgment.

* suppose recieves says I can recieve 10 packets sender can send 10 packets at a time. after Recieving a packet it will give an acknowledgment

* This acknowledgment will send an indication to the sender to send nxt 10 packets.

Acess control

The Acess control dealing about media Acess control

suppose the common media where n devices wants to send the data in a common media

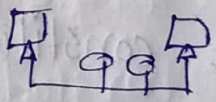
* How All these going to use this common media inorder to send Their data without collosion.

→ That is deal by the media Acess control → talk about future

Error Control

suppose if the device sending the frame we expect The frame should reach the Reciever (destination). without any transmission error

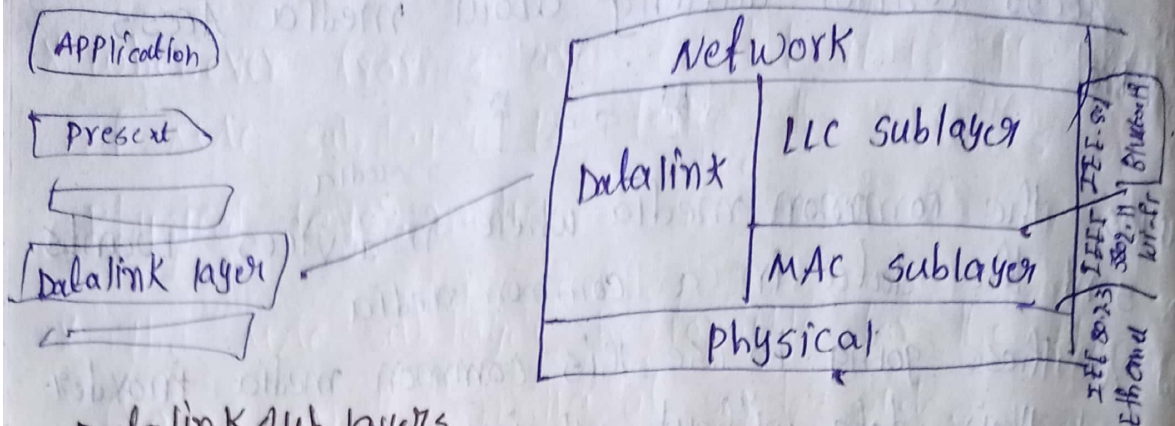
* when the frame leaves the computer on device A. Then not, it hands on the device A to protect the frame. Whereas no. of transmission errors for effect Frame
* So it is the responsibility of data link layer to protect take the frame and we have 2 approaches in error control



1) Error Detection
2) Error Correction

* This is the simple scheme the Reciever detects the error in a Frame it can discard that Frame (or) it can correct the errors also
* while Error Detection is easily. The Error-correction is complex task.

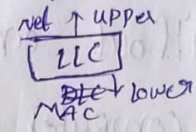
Sub layers of data link layer



Datalink sub layers

1) Logical link control sublayer (LLC) (or)
2) Data link control sub layer (DLC)
3) MAC sublayer

* The LLC and DLC Handles communication between upper and lower layers



* The role of (LLC) (or) (DLC) is takes the Network pa data and adds control information to help deliver the packet to the destination (Flow control)

MAC sub layer

* it constitutes the lower sub layer of the data lin layer
* it is normally implemented by hardware, typically in the computer Network Interface card (NIC).
* The physical layer have interact with only MAC sub
* Two primary responsibilities
  * Data encapsulation
  * Media Acess control.

Data encapsulation

* Frame assembly before transmission and frame disassembly upon reception of a frame.
* after collecting the data from network layer all the control information are added. after adding the control information of sub layer
* it starts collecting all the bits of information and finally constructs the frame.
* before transmission frame Assembly should be done upon reception frame reception should be done.

→ This MAC layer only adds a header and trailer to the network layer PDU.

* After adding the header and trailer of network PDU frames are created.

primary functions of MAC sublayer

* Framing
* Physical Adressing (or) MAC Adressian
* Error control

→ in Data link layer 5 services are there 1 service are done by LLC sublayer.

* The remaining 4 services done by MAC sublayer.

The MAC are name itself are Media access control

media

* whenever frames are created it is the responsi of MAc sub layer to ~~take~~ place the frames on the Physical ~~layer~~ media.

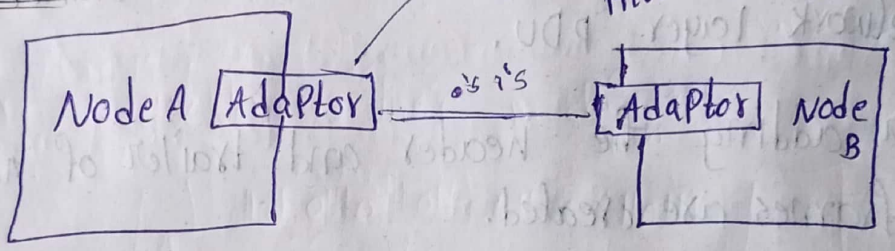
* The MAc sub layer Responsible for the placement frames on the media at sender side.

* and removal frames ~~frames~~ from media ~~the~~ Reciever si

→ and directly communicates with the physical layer.

Framing — I one of service of DL layer

This adaptor only sending the data it recieves from the data link layer into signal. The signals Recieved,



Problem i's

* Application layer creates the data which set of 0 and 1's Then it goes to the transport layer.

* in transport layer it is going to add set of 0's. it is over the Network layer.

* The Network layer going to add Network header it is called as Packet. again set of 0's & 1's are add and it goes to the data link layer

* In the Data link layer set of 0's and 1's a in header part and set of 0's & 1's are in the trailer part.

we have a complete set of 0's & 1's we called as a frame.

* The set of 0's and 1's are packed into frame. And this frames understandable only by the data link layer

* as per physical layer is concern a frame set of 0's and 1's. The physical layer takes every individual bits it 1's or 0's converts into equivalent signals and sends it.

* In physical layer it doesn't know anything about the frame but they data link layer only deals with the Frame.

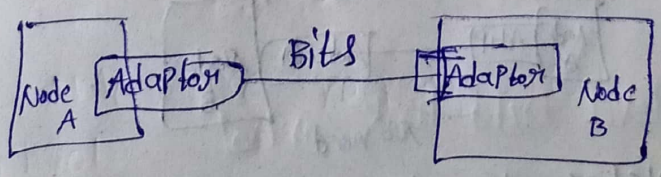
* whenever the 0's & 1's sent to the Reciever The Reciever collects all the zeros and 1's so that physical layer of that Reciever collects 0's & 1's and construct the frame

→ problem is how do the Reciever know this is the frame

* suppose Node A sends 500 bits of data. where 50 bits belongs to frame 1. 50 bits are sent all the 50 bits are Recieved These signals.

* Reciever adapotor Recieves all the 50 signals and How These Reciever knows that 50 signals are Frame 1

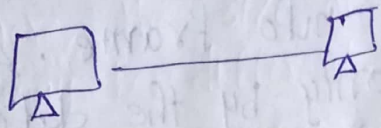
* Here This the problem with the solution



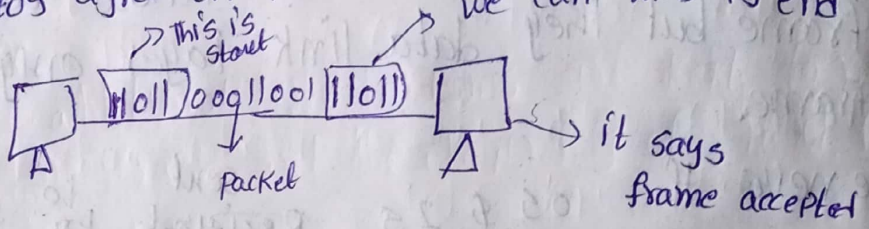
Bits flow between adaptors, frames between hosts

Ex:

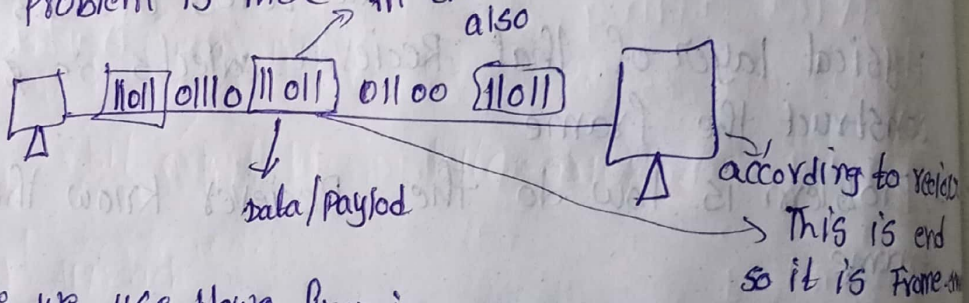
There 2 computers



* They are deal up with Sending and Recieving information
* it follows protocol & the protocol: let the start a frame and end of frame be 11011
* when the sender computer Recievse Packet from layer it ads 11011 on header and trailer part as 11011.
* both computers agree on protocol.



* Here 1 problem is there in data part also

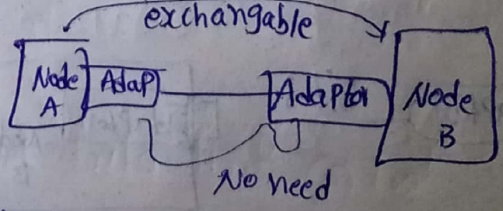


* in future we use How a framing-error are handled

Frame = Header + Network layer PDU + Trailer.

Pack switched Networks

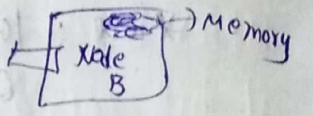
* in packet switched networks, the block of data called frames are exchanged between nodes, not bits streams.



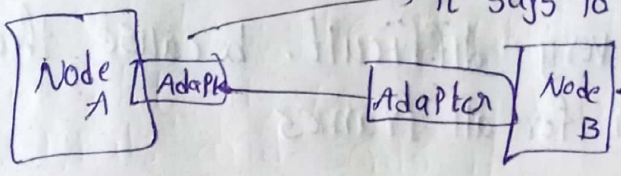
* when node A wishes to transmit a frame to node B it tells its adapter to transmit a frame from node A memory.

* This results in a sequence of bits being sent over the link.

* The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B's memory



→ challenge: what set of bits constitute a frame?



* if the Frame size is fixed it is easy.

→ * what about the variable size

Types of Framing

1. Fixed size Framing
2. Variable-size Framing

1. Fixed size Framing

The sender and Reciever know the size of frame. So it is easy for sender & Reciever to construct a Frame

* Here size of frame is fixed so the Frame length acts as delimeter of the frame → 10 is 1 Frame another 10 → Frame 2

* consequently, it does not require additional boundary bits to identify the start and end of frame

if size is fixed

2. Variable - size framing

Here, the size of each frame to be transmitted may be different.

* ex : 100 bits may constitute Frame 1.
  60 bits constitute Frame 2.
  80 bits " Frame 3

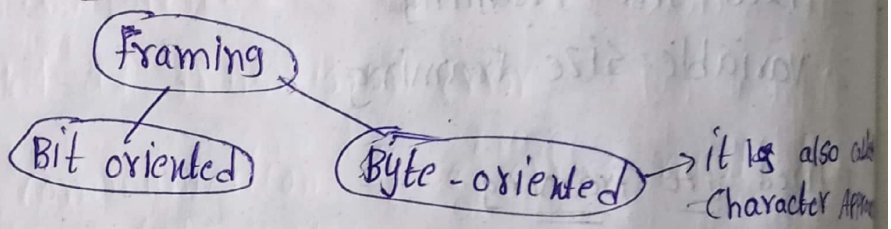
* in this case it is very difficult. because the length is not uniform for all frames

* so must it maints start of the frame end of the frame.

So, additional mechanisms are kept to mark the end of one frame and the begining of next frame.

Various Framing Approaches

* 2 Approaches



Bit oriented Approach

* The name itself it concerns with bits.
* it simply views the frame as a collection of bits.
* in bit - oriented framing, data is transmited as a sequence of bits that can be interpreted in the upper layers both as text as well as multimedia data (audio video)

Bit - oriented protocol

HDLC — High - level Data link control

Byte oriented Approach

* it is concern with bytes
* it is one of the oldest approaches to framing
* Here each fram is viewed as a collection of bytes (characters) rather than bits. so it is called a.k.a character oriented approach

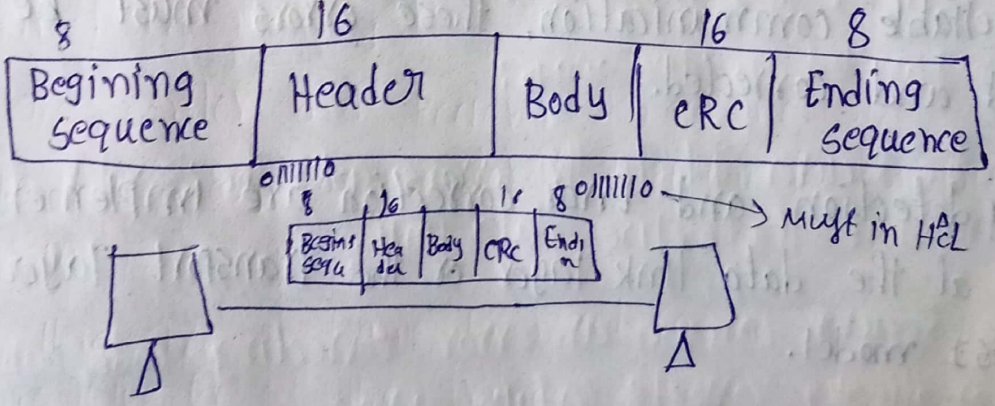
Byte oriented protocols

BISYNC — Binary synchronus communication protocol
DDCMP — Digital Data communication Message Protocol
PPP — Point-to-Point protocol.

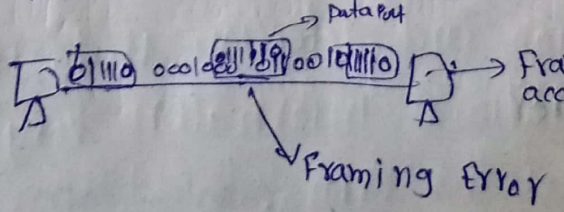
3. clock based Framing

* The third approach to framing is the clock based framing. it is used for optical networks.
* EX: SONET → synchronus optical network

HDLC - Frame Format



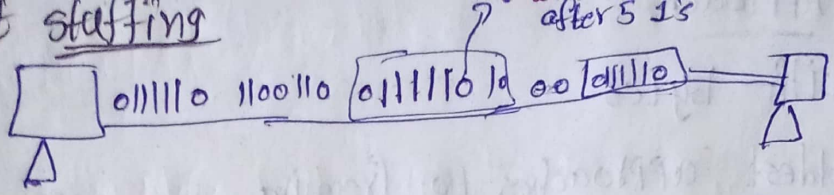
HDLc protocol : Beging and ending sequence is 01111110



The are only added Header and trailx the data Parts also same it is Framing error. but we don't what the upper layer generates (Network layer).

* To rectify this issue. Solution is Bit stuffing

Bit stuffing



* Suppose if the sender Recieving the data from the upper layer and sender sees that there are 5 consecutive it will going stuff a zero after 5 1's
* And reciever undo this remove the zero and Recieved. Problem solved

Error Detection

Error

Data are transmitted in the Network. we don't Know what happen's to the data has left the node.

* The data can be corrupted during transmission.
* This are called as transmission error
* For reliable communication, these errors must be detected and corrected.
* Error detection and Error correction are implemented either at the data link layer or the transport layer the OSI model.

Types of Error

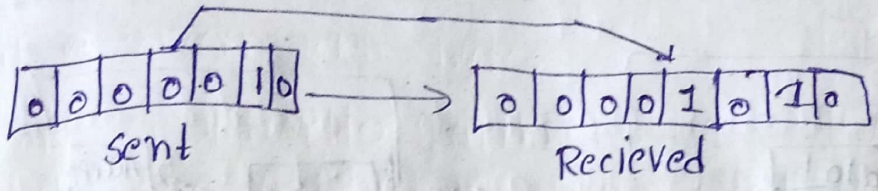
1) single Bit Error
2) Burst error

Single Bit-error

only single bit has to bee changed

* it is also known as single bit error, only 1 bit in the

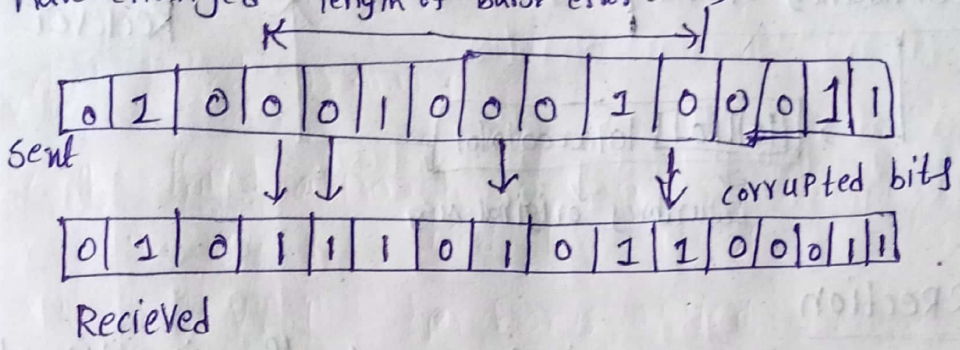
data unit has been changed.



* the sender send information Reciever Recieved it but only 1 bit is changed so it is called single bit error.

Burst ERRor

* in burst error, 2 or more bits in the data unit have changed

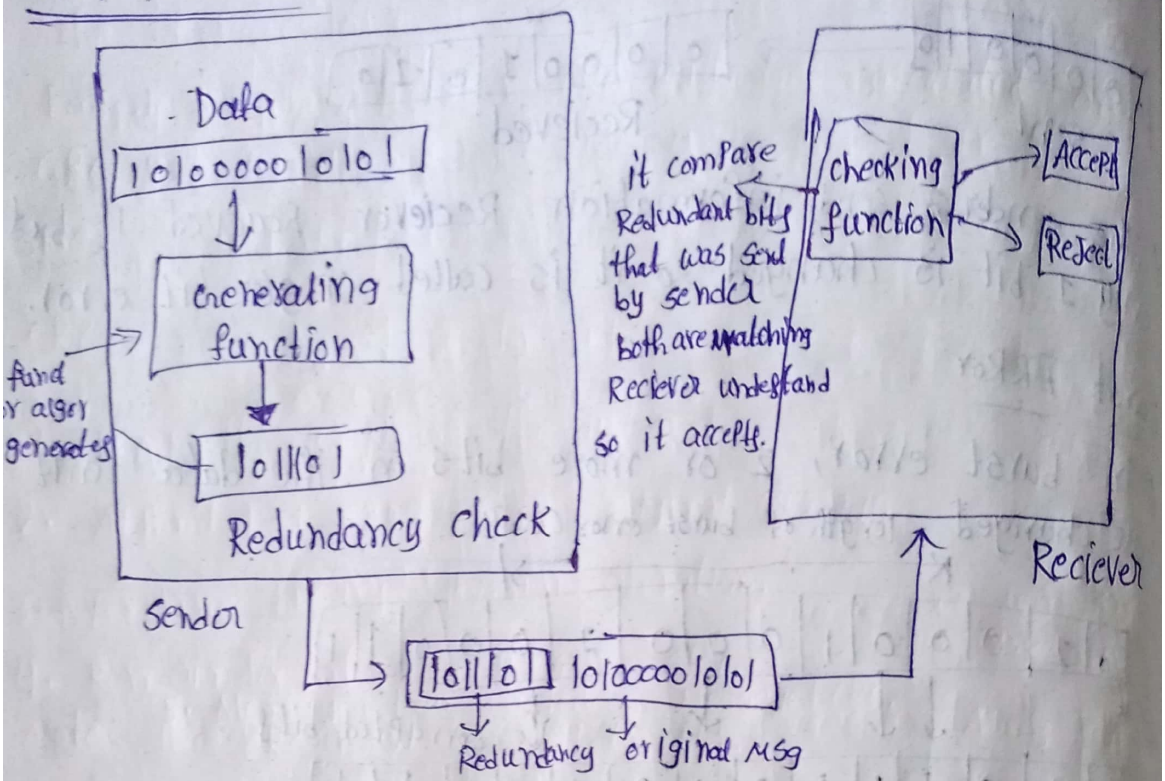


Detect the ERRors

Error Detection means to decide wheather the recieved data is correct or not without having a copy of the original message.

* The original message itself corrupted by transmission erro know How to detect errors
* so with the message the addition information also send by the sender.
* These additional information will help the reciever to find out wheather there is a Error or not in the data is transmitted
* To detect erros (or) correct error, we need to send some ex bits. with the data.
* These extra bits are called as redundant bits.

REDUNDANCY



ERROR CORRECTION

ERROR Detection is easy. it is correct otherwise discard

* But ERROR Detection is not easy
* The Reciever has to correct the Error

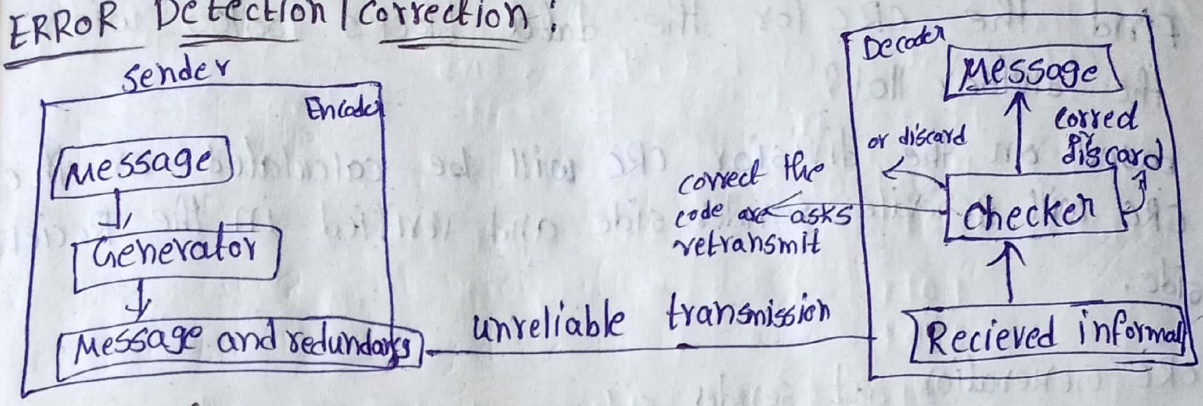
It can handled in two ways;

1) if the Reciever detects the errors asks the sender to retransmit the entire data unit.

2) The Reciever can use an error-correcting code, which automatically corrects certain errors.

> Both Error correction and detection needs Redundancy. because without additional information very difficult to correct or detect the errors.

ERROR Detection / correction :



ERROR Detection Techniques

Four types of redundancy checks are used in data communications. They are :

1. Vertical Redundancy check (VRC)
2. Longitudinal Redundancy check (LRC)
3. checksum
4. cyclic Redundancy check (CRC)

checksum

cylic Redundancy check (CRC)

* we know that any error detection technique we append the redundant bits with the message
* because this redundant bits will enable the reciever t detect wheather there is a Error or not.
* likewise CRC also going to generate some redundant bits. And these bits are called as the redundant bits
* In this technique these redundant bits are specifically called as CRC

let solve a problem now.

Find the CRC for the data blocks 100100 with the divisor 1101?

based on the division CRC will be calculated on the CRC will generate sender side and verified in the Reciev side.

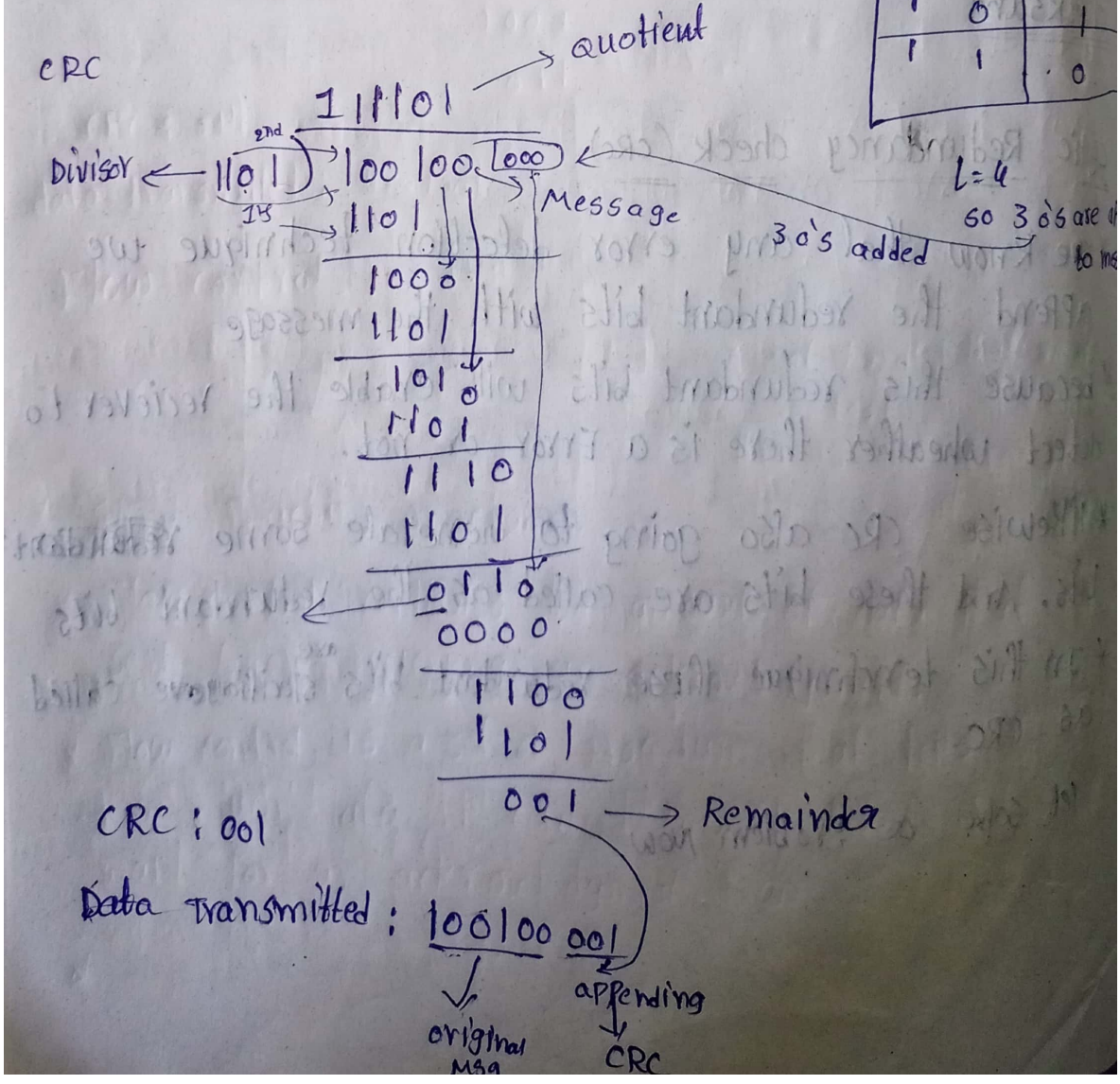
CRC Generation at sender side

1. Find the length of the divisor 'L'.
2. Append 'L-1' bits to the original Message.
3. Perform binary division operation.
4. Remainder of the division = CRC
5. Message transmitted = Message + CRC.

Note: The CRC must be of L-1 bits.

we must know
or XOR operation

A	B	A XOR
0	0	0
0	1	1
1	0	1
1	1	0



→ Polynomial

Hint $x^7+x^5+x^2+x+1$

$x^6\ x^5\ x^4\ x^3\ x^2\ x\ 1$

1 0 1 0 0 1 1 1 → Divisor

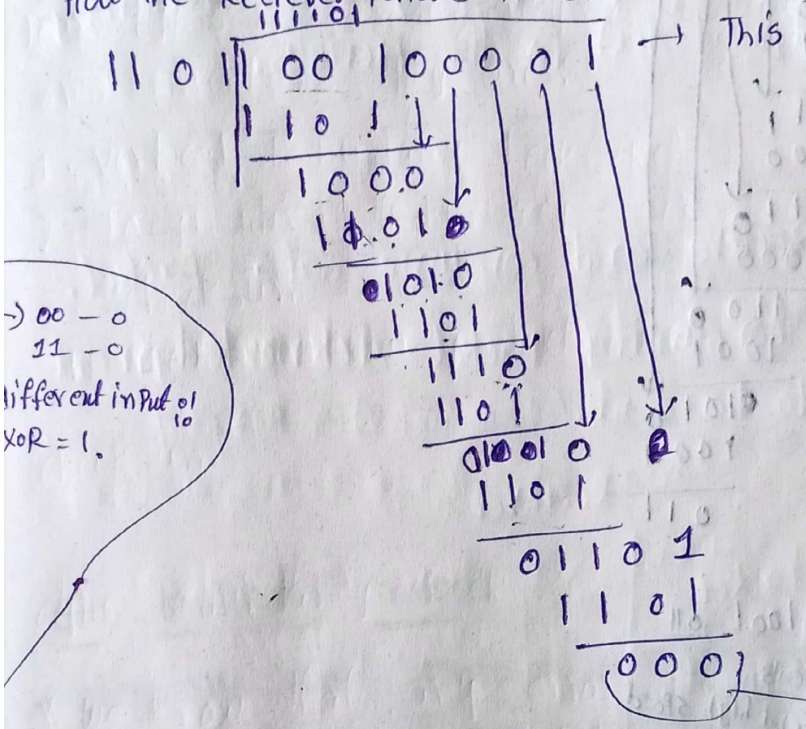
How the Recieved detect the error using CRC.

CRC : 001

Dat transmitted : 100100 001

Data Recieved by the reciever : 10010000 1

How the Rccieved Knows No error in the data. The data



→ This is recieved

→ 00 − 0
11 − 0
different input 01 / 10
XOR = 1.

→ where the Recieved Recieves all zeroes as Remainder. Receiver understand crct and it accepted.

The Message 1100101 is to be transmitted using CRC polynomial X^3+1 to protect it from errors. The message that should be transmitted is.

The Remainder are appended the data (or) Message

Sender side

x3 1

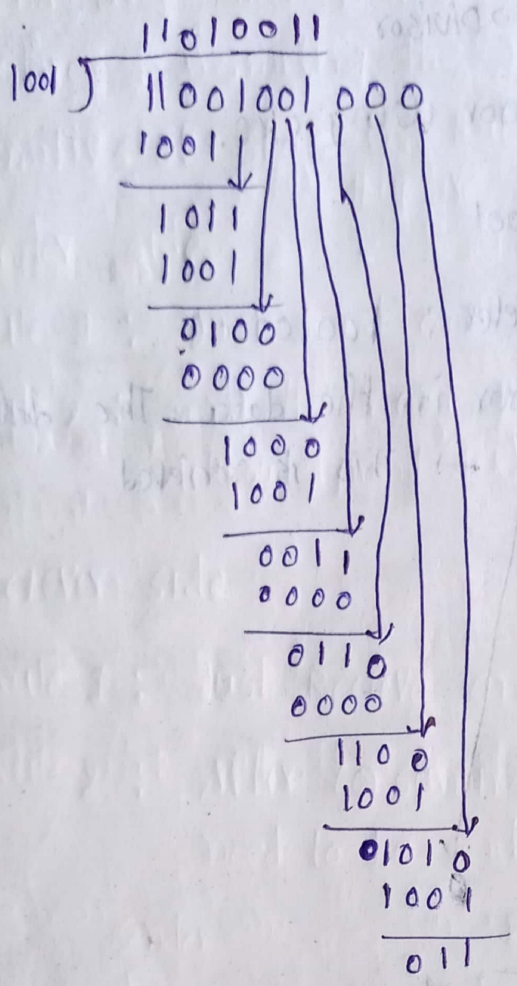
$= x^3+1 = 1x^3+0x^2+0x^1+1$

$= 1001$

1. length of divisor = 4 (1001)
2. Append 4-1 bits to orginal message
3. binary division operation
4. Remainder = CRC
5. Message transmitted = Messg

Note

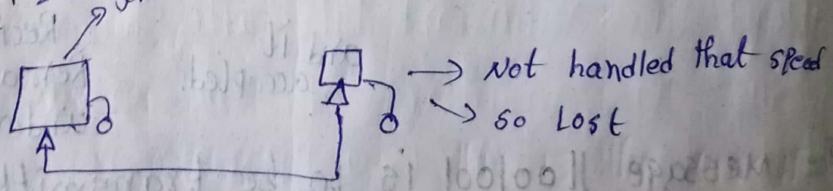
The CRC Must be of 1-1, 4-1 = 3 bits



CRC : 011

data transmitted : 11001001 011

Flow control — Protocols

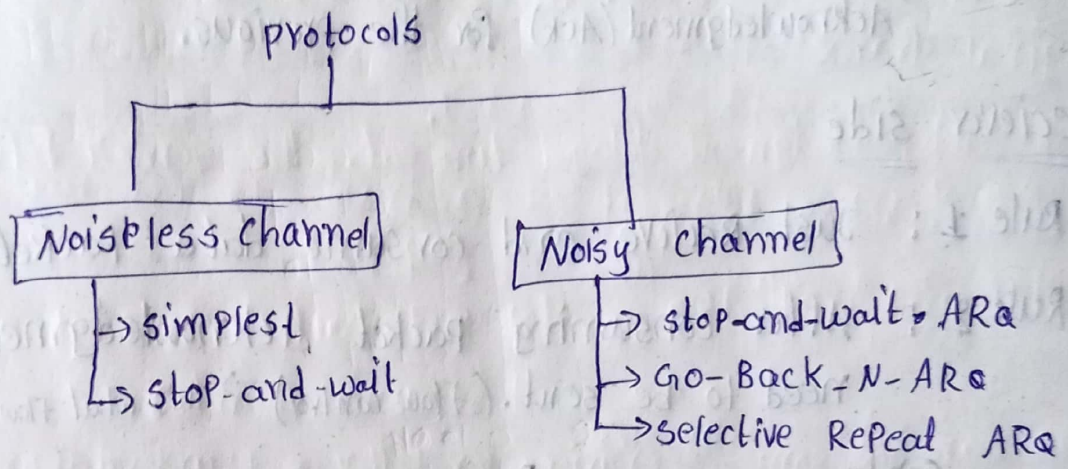


* Speed maching mechanism
* Flow control cordinates the amount of data that can be sent before recieving an acknowledgment.
* Flow control is a set of procedure that tells the sender how much data it can transmit before it must wait for an acknowledgment from the reciever.
*

* Reciever has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.

* Reciever must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.

Flow control - protocols



stop-and-wait protocol

* stop-and-wait protocol is data link layer protocol for transmission of frames over noiseless channels.

* it provides unidirectional data transmission with flow control facilities. but it not focus on error control facilities.

* unidirection means sending or Recieving take place at a time both sending and Recieving Not happen at the same time.

* That is why stop-And-wait protocol is - anidirectional data transmission.

* The idea behind stop and wait protocol is very straight forward.

* After sending one frame, the sender will not send any other frame it waits for an Acknowle before transmiting the next frame.

primitives of stop And wait Protocol rules

They are very simple for sender and reciev

Sender side

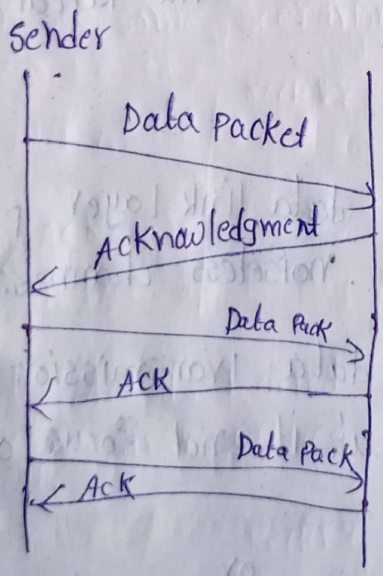
Rule 1 : Just send one data packet at a time.

Rule 2 : Send the next packet only after recieving Acknowledgment (Ack) for the previous.

Reciever side

Rule 1 : Just Recieve and consume data packet.

Rule 2 : After consuming packet Acknowledgment need to be sent. (Flow control) → This what flow co



→ This is the process of stop and wait Protocol.

Advantage

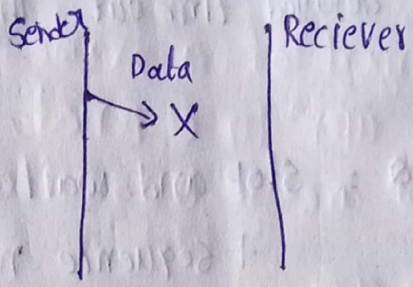
Main Advantage is simplicity

disadvantage is that if asks 1000 data packets all the 1000 data packets can not transmited at the same time one by one sending.

problems of stop and wait protocol

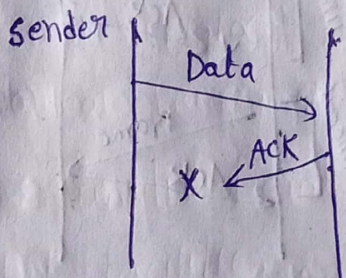
1. problems due to last data
   * senders sends the data This data is lost.
   * what happens the Reciever waiting for a long period of time for the data.
   * since the Reciever not recieve the data it not sends Ack. The Reciever not sends Ack it won't send the Nxt Packet.

→ Sender waits for Ack for infinite amount of time
→ Reciever waits for data an infinite amount of time

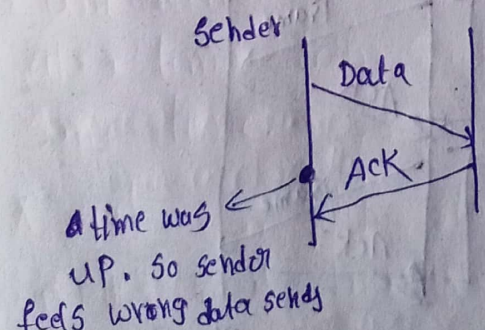


2. Problems due to lost Ack

* The sender send the data The Reciever Recieves and sends Ack. but Ack lost due to some problem.



3. problem due to delayed Ack/data.
   * The sender send the data, a delayed Ack might be wrongly considered as Ack of some other data Packet



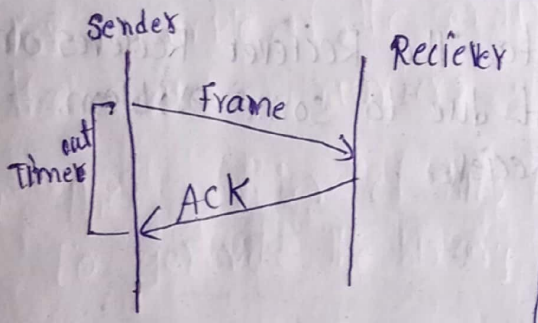
Stop-and-wait ARQ Protocols

it is very simple protocol

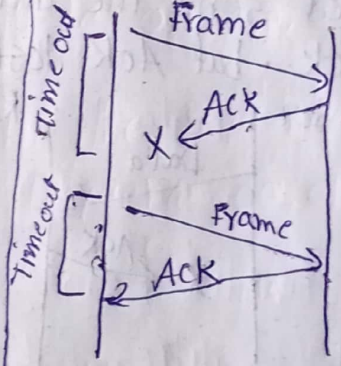
* The idea of stop and wait protocol is straight forwa
* The idea is After transmiting one frame, the sender waits for an Ack befor transmiting the nxt frame
* if the Acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the orginal frame

The Acknowledgment delayed time out. The sender retrans orginal frame

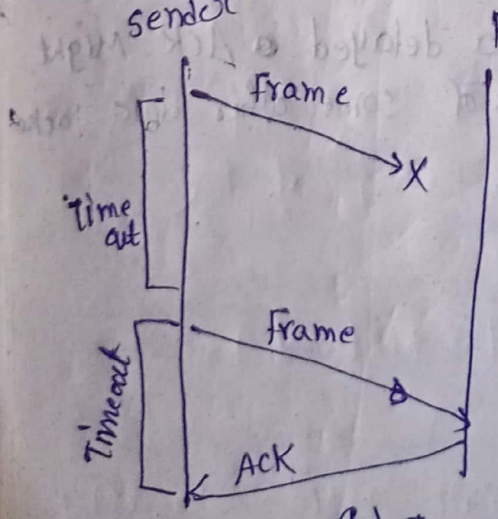
* Stop-and-wait ARQ = stop and wait + Timeout Time + sequence number.
* we can see some scenarioes for ~~better~~ ~~exp~~ understanding



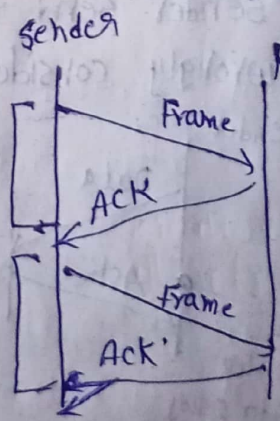
(a) The Ack is recieved before timer expires so it is perfect.



(c) The Ack is lost



(b) The original frame is

(d) 

(d) The timeout fires to so

~~Sliding window Protocol~~

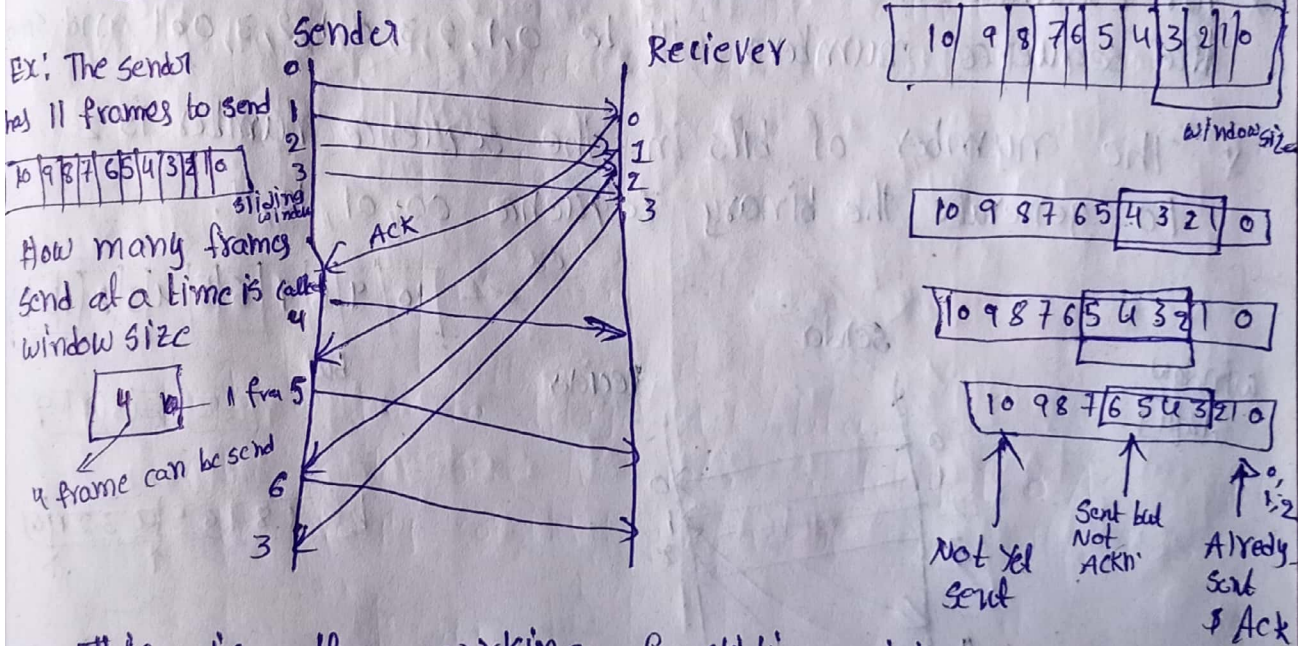
Stop-and-wait ARQ - Drawbacks

* one frame at a time
* Poor utilization of bandwidth.

Sliding window Protocol

* in stop-and-wait Ack we can send one frame at a time but sliding window protocol ~~frames~~ send multiple frames at a time.
* send multiple frames at a time.
* Number of frames to be based on parameter called window size.
* Each frame is number called as sequence number.

working of sliding window protocol



→ This is the working of sliding window protocol.

Go-Back-N ARQ

N is the sender window size

Go Back-5 → 5 frames sent by sender before recieveing ACK

* Go-Back-N ARQ uses the concept of protocol pipelining i.e the sender can send multiple frames befor recieving the acknowledgment for the first frame.

* There are finite number of frames and the frames are numbered in a sequential manner.

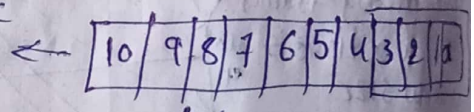
* The number of frames that can be sent depends on the window size of the sender.

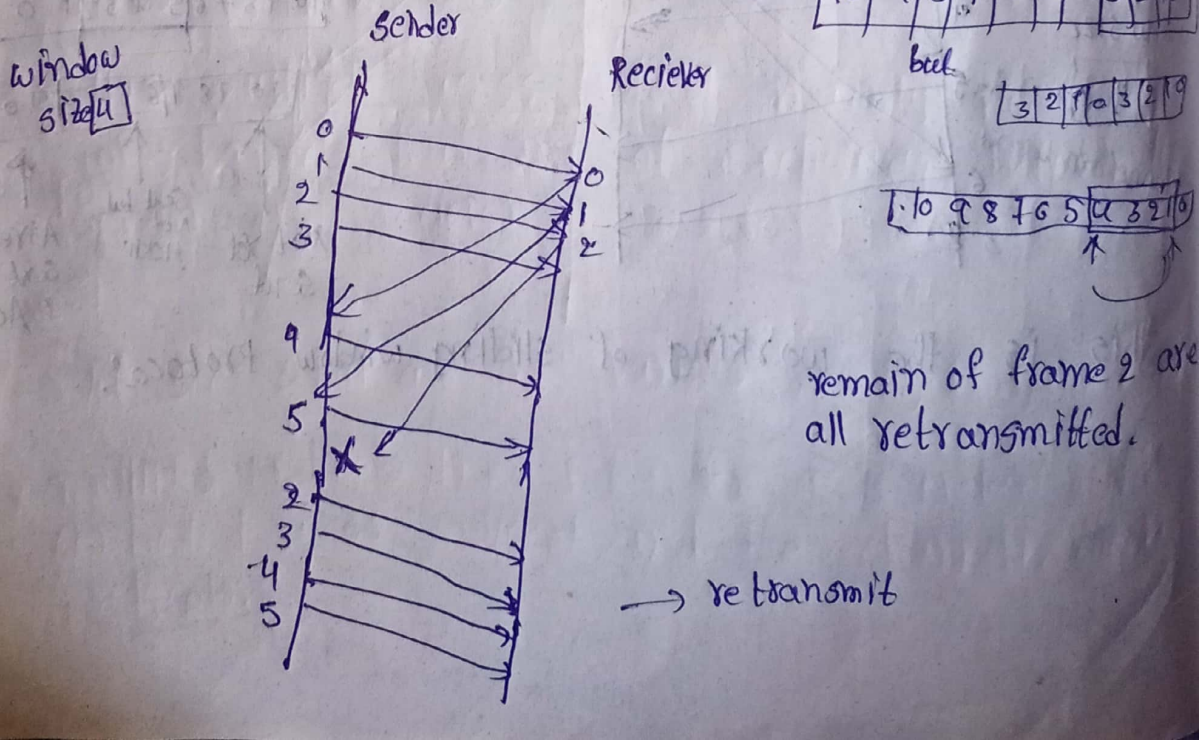
* if the acknowledgment of a frame is not recieved within an agreed upon time period, all frames in the current window are re-transmitted.

---

* N - is sender window size.
* For example, if the sending window size is 4 (2^2), then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0 0 1 and so.
* The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

ex





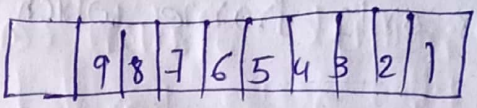
remain of frame 2 are all retransmitted.

→ retransmit

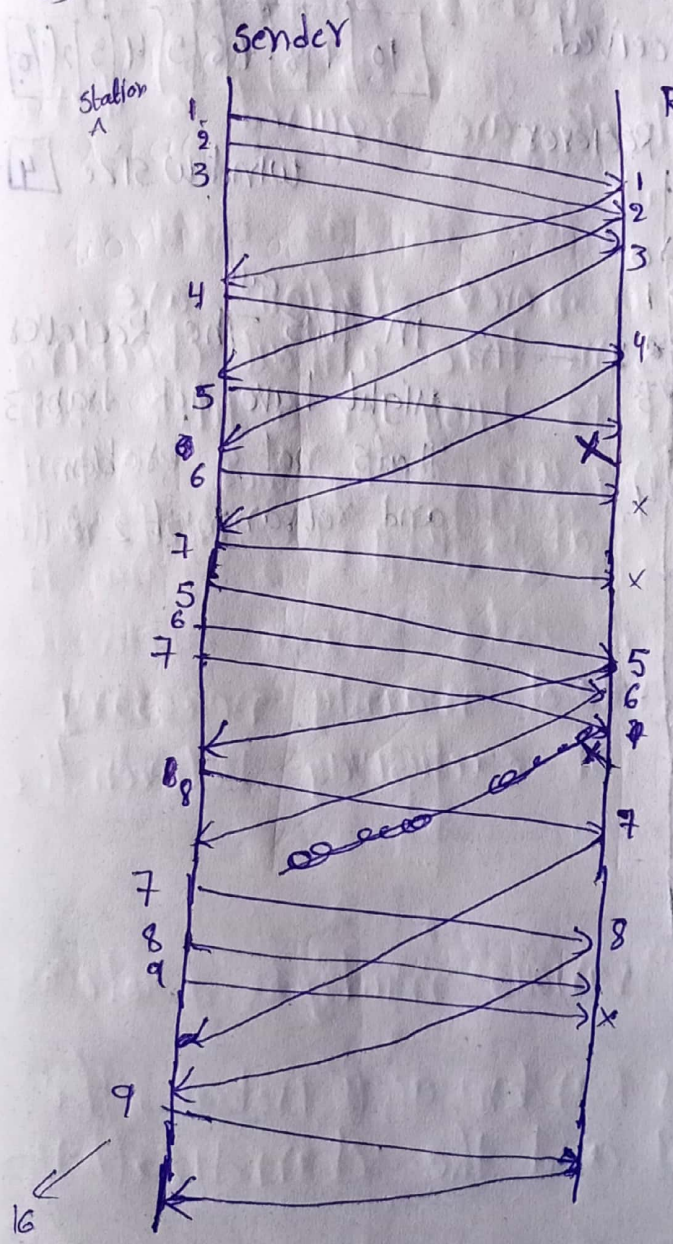
Question

Station A needs to send a message consisting of 9 packets to station B using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. if every 5th packet that A transmits gets lost (but no Acks from B ever get lost), then what is the number of packets that A will transmit for sending the message to B?

A) 12
B) 14
C) 16 ← Answer
D) 18



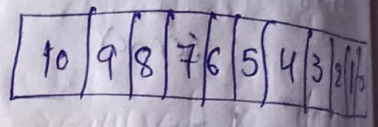
window size 3



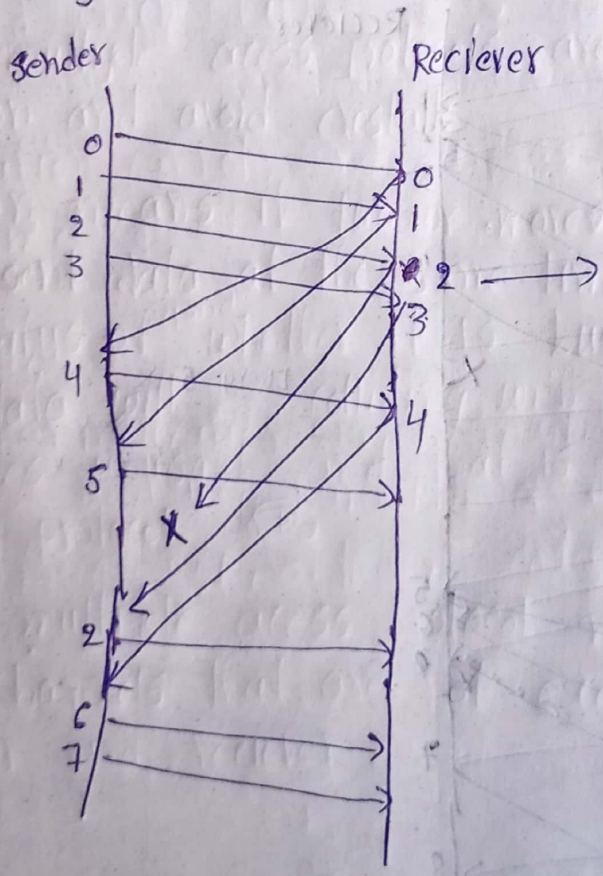
Every 5 X
10 also X
15 also X

Selective Repeat ARQ

* in selective Repeat ARQ, only the erroneous or lost frames are retransmitted, while correct frames are recieved and buffered.
* But in go-back-N all they retransmited : selective Repeat only losted are retransmitted
* The reciever while Keeping track of sequence numbers buffers the frames in memory and sends NACK for only frame which is missing or damaged
* The sender will send/retransmit packet for only which Negelive Ack is received.



window size 4



in this case The Reciever Might have Ack from 3 thats not a problem and retranmist 2

Question

in SR protocol, suppose frames through 0 to 4 have been transmitted. Now, imagine that 0 times out. 5 (a new frame) is transmitted, 1 times out, 2 times out and 6 (another new frame) is transmitted. At this point, what will be the outstanding packets in sender's window?

a. 3 4 1 5 2 6

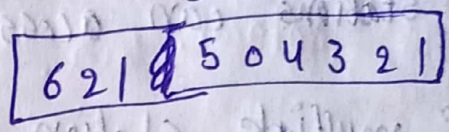
b. 3 4 0 5 1 2 6

c. 0 1 2 3 4 5 6

d. 6 5 4 3 2 1 0

e. None of

sender's window



multiple Access protocols

in compater Network we have a exclusive channel (or) medium blw the sender and reciever Then No worries

* but if the channel (or) medium is shared among many stations or nodes Just like that we can not send the data
* because the channel may already be involved in data transmission blw any other two nodes if any station (or) node wants to send data without Knowing the status of channel (or) medium.
* that is whether the channel (or) the medium is busy or idle then the data can be lost or the data can be corrupted (or) the data can be overlapped.

Chaos

ex: in class teacher resolves all students are giving answers

* in computer Network the multiple acess protocols resolves this chaos. let's see why do we need multiple acess protocols in detail

→ if there is a dedicated link between the sender and the reciever. the data link control lay is sufficient that is since the channel is exclusively between the sender and the reciever we need not worry about it.

* → however if there is no dedicated link present blw the sender and Reciever the multiple stations can access the channel simultaneously

→ if multiple station can access the channel simulta it has to be handled because there is a serious problem called collision.

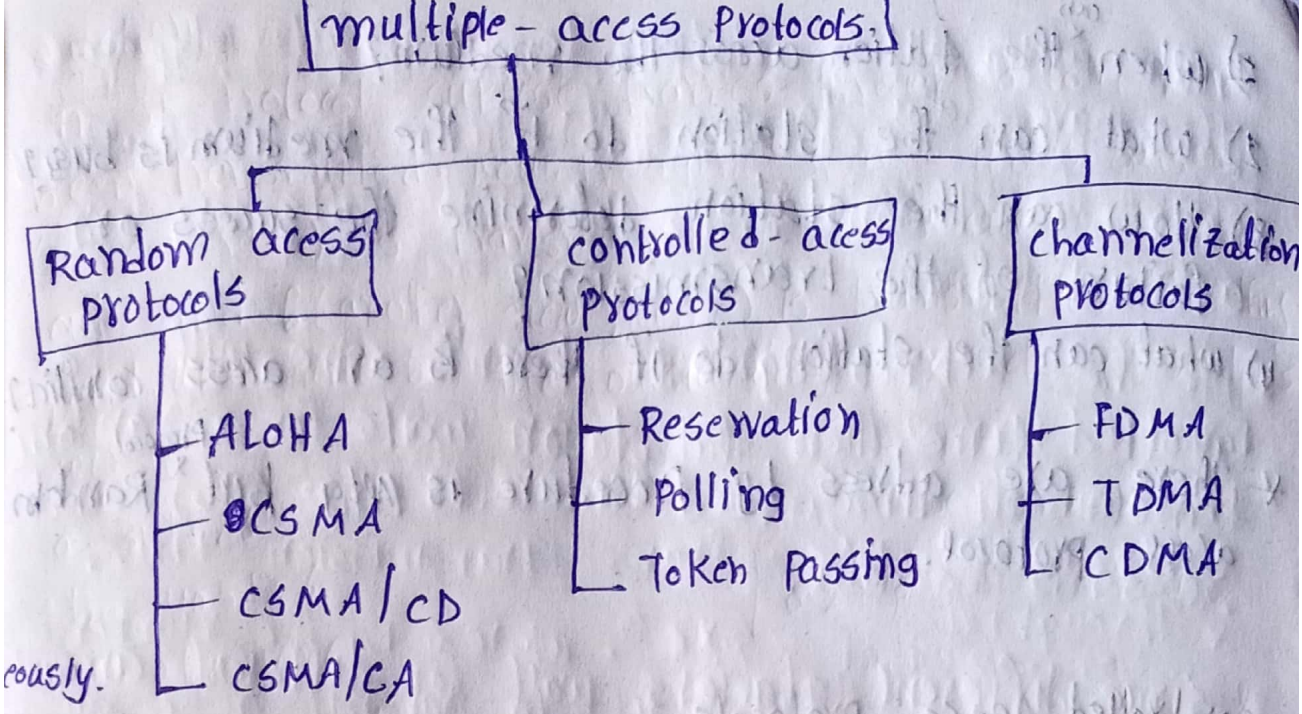
* Hence multiple access protocols are required to decrease collosion and avoid crostalk

* collosion means if two or more station are node sent data at the same time without checking the status of channel whether it is busy or a little then the data will be colliding with each other and it becomes unusable and that is why we need multiple access protocol

→ This multiple access protocol mainly necessary for channels that are not exclusively between the sender and reciever

→ let see what are the various multiple protocols

* multiples protocols involves Random accs protocal, the controlled access protocol and the channelization protocols.



eously.

Random Access protocols

The name itself says that random acess protocols where any station can send the data in any time but obviously there are chances for collosion.

* in this, all station have same superiority (priority) that is no station more priority than another station. Any station can send data depending on medium's state (idle or busy).
* in a Random acess method, each station hay the right to the medium without being controlled by any other station.
* if more than one station tries to send, there is an acess conflict (collision) and the frames will be either destroyed or modified.

→ To avoid acess conflict (collision), each station follows a procedure (protocols)

1) when can the station acess the medium?
2) what can the station do if the medium is busy?
3) How can the station determine the success or failure of the transmission?
4) what can the station do if there is an acess conflict?

* These are advess by Procedure is Ntg but Random acess protocol.

Controlled Acess protocols

* in controlled acess, the stations consult one another to find which station has the right to send.
* A station cannot send unless it has been authorized by other stations.

Channelization protocols

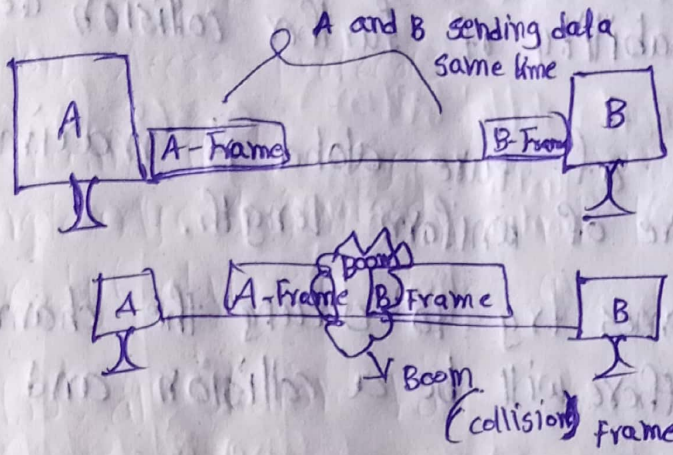
Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through codes, between different stations.

Pure Aloha :-

* Aloha is random access protocol (a station can send data any time)
* it was actually designed for wireless LAN but it 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 (Not usable data)

collosion

station A & B. and common shared medium

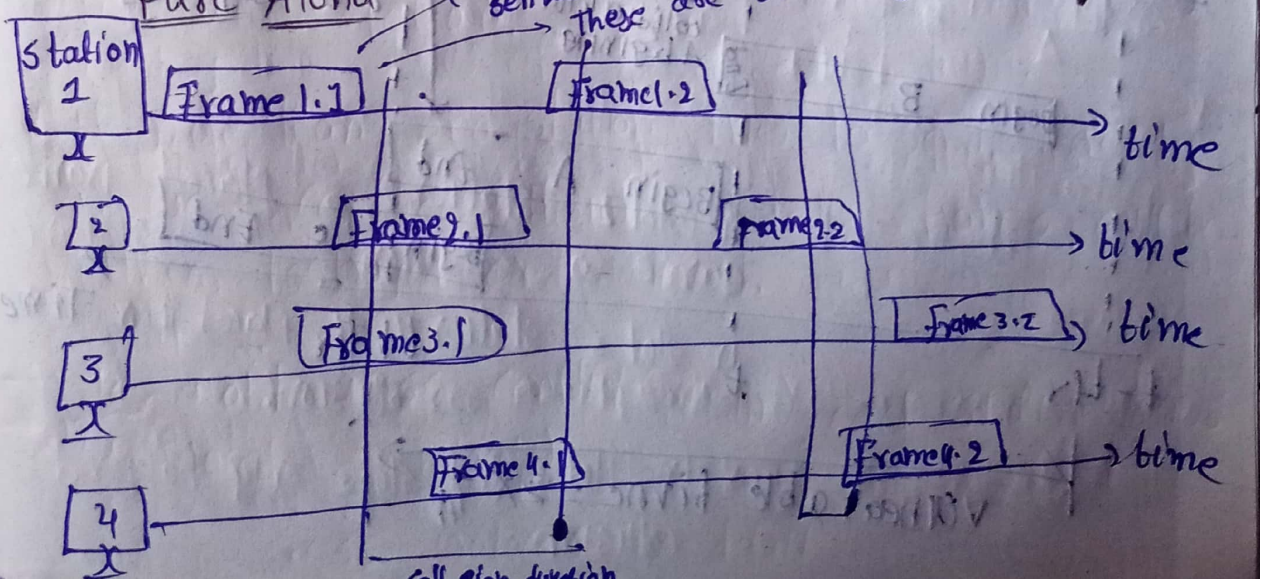


let see how Aloha protocol handle this collision in shortly !

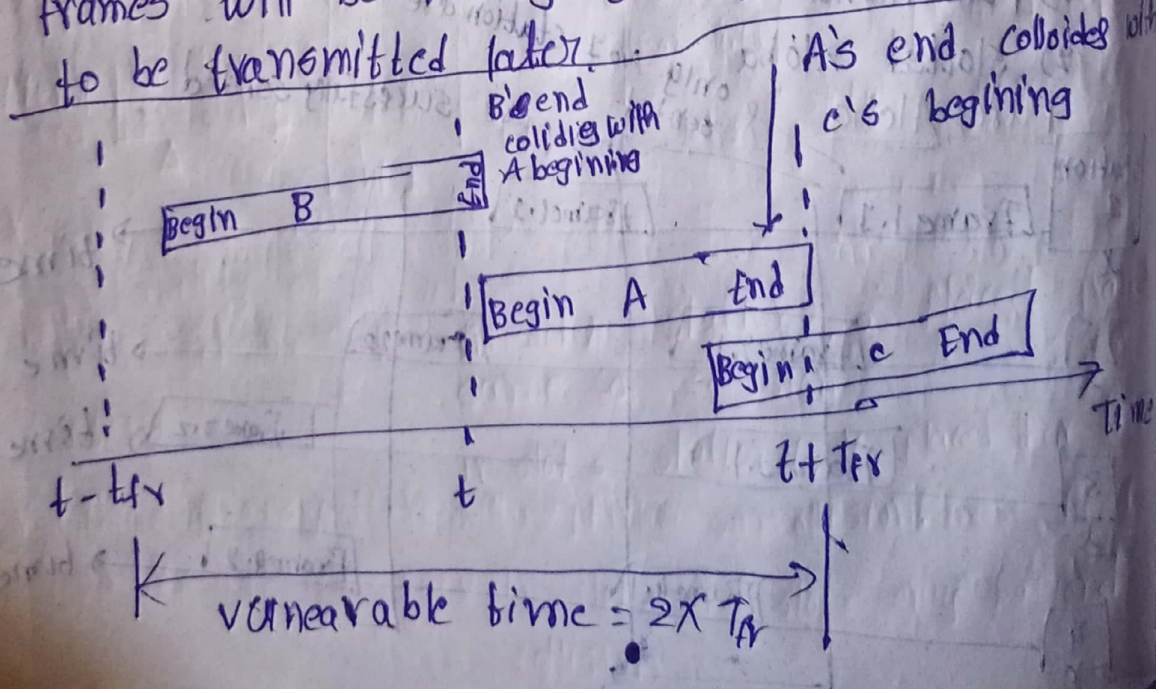
Then we see types of Aloha

1) Pure Aloha
2) slotted Aloha

Pure Aloha

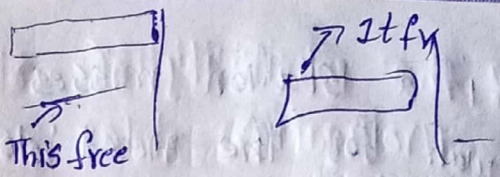


* Pure aloha allows stations to transmit whenever they have data to be sent.
* when a station sends data it waits for an acknowledgment.
* if the acknowledgment doesn't come with the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data.
* since different stations wait for different amount of time, the probability of further collision decreases
* The throughput of pure aloha is maximized when frames are of uniform length.
* whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
* if the first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be transmitted later.



* Vulnerable time - $2 * T_{fr}$

* Throughput = $G \times e^{-2G}$



Then only it is $2T_{fr}$

Maximum throughput = 0.184 for $G = 0.5 (1/2)$

Slotted Aloha :

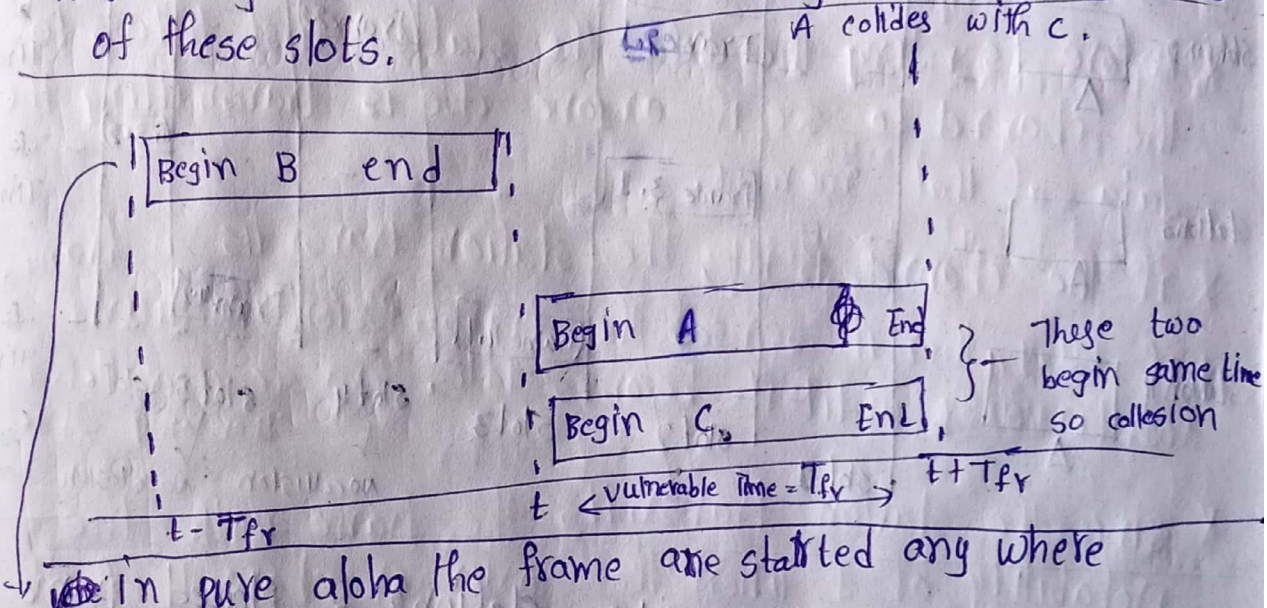
Slotted Aloha was developed just to improve the efficiency of pure aloha as the chances for collision in pure aloha are high.

* Pure aloha throughput = 0.184 it is improved efficiency by help of slotted aloha.

* The time of the shared channel is divided into discrete time intervals called slots.

why do we need time slots?

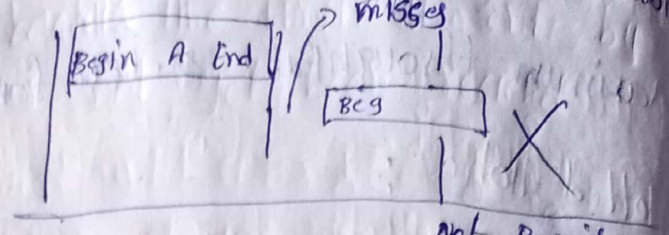
* sending of data is allowed only at the beginning of these slots.



* In pure aloha the frame are started any where

* but in slotted aloha the placement of frames happend in only at begining of the time slot.

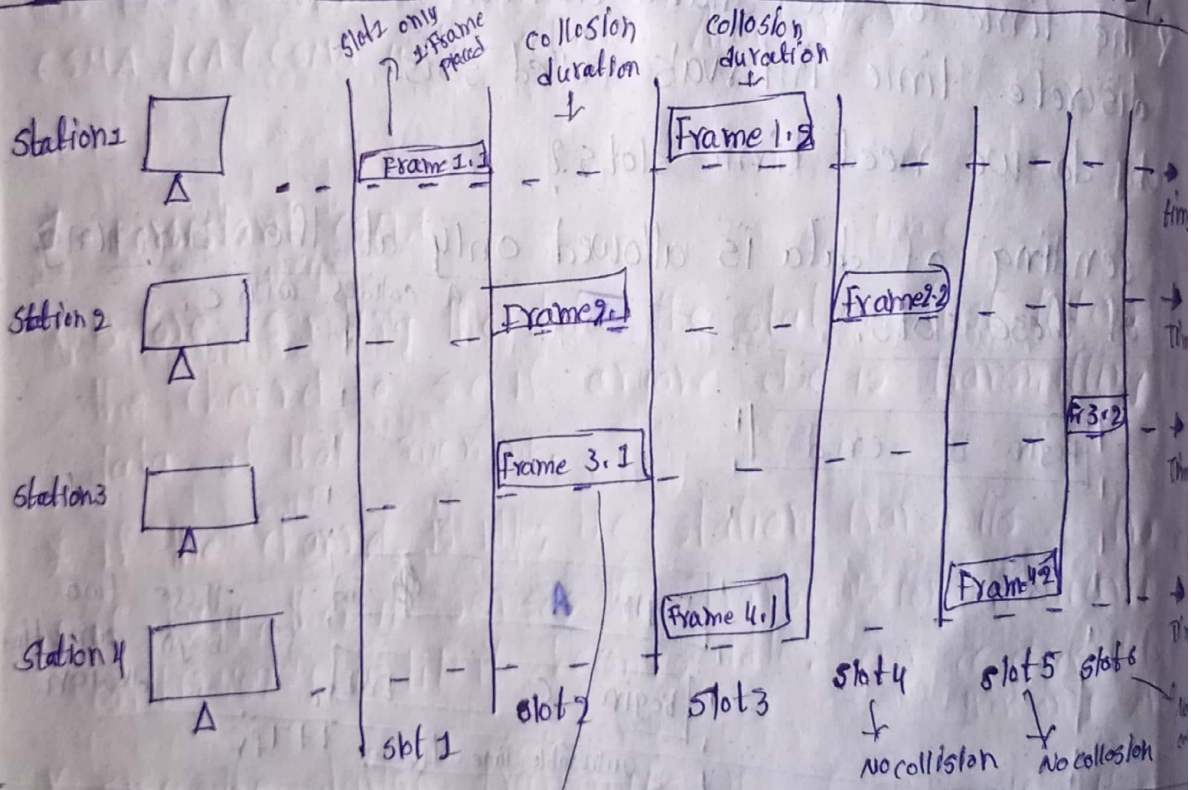
* if a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.



Formulas for slotted Aloha

* Vulnerable Time = Frame Transmission Time.
* Throughput = $G \times e^{-G}$. where G is the number of stations wish to transmit in the same

* Maximum throughput of (Slotted Aloha) = 0.368 for G = 1.



in slot 2 station 2, 3 placed frame same so collision

in slot 3 station 1, 4 placed their frame same time so collision.

* in slot 2 and slot 3 only happend collision

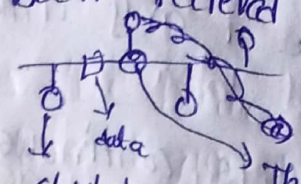
Slotted Aloha

Pure Aloha	Slotted Aloha
1) Any station can transmit the data at any time.	1) Any station can transmit the data at the beginning of any time slot.
2) The time is continous and not globally synchronized	2) The time is discrete and globally synchronized
3) Vulnerable time in which collision may occur = $2 \times T_{fr}$	3) Vulnerable time in which collosion may occur = T_{FR}.
4) Probability of sucessful transmission of data packet = $G \times e^{-2G}$	4) Probability of sucessful transmission of data packet = $G \times e^{-G}$
5) Maximum efficiency = 18.4%. (occurs at $G = 1/2$)	Maximum efficiency = 36.8%. (occurs at $G = 1$)
6) Main advantage: simplicity in implementation	Main advantage: it reduce the number of collisions to half and double the efficiency of Pure Aloha.

carrier sense multiple Access (CSMA)

* carrier means channel (or) medium.
* To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
* principle of CSMA: sense befor transmit (or) "listen before talk".
* carrier busy = Transmission is taking place.
* carrier idle = No transmission currently taking place.

propagation delay; a station may sense medium and find it idle, only because the first bit sent by another station has not yet been recieved



Types of CSMA

1. 1- persistent CSMA
2. P- Persistent CSMA
3. Non-persistent CSMA
4. 0- Persistent CSMA

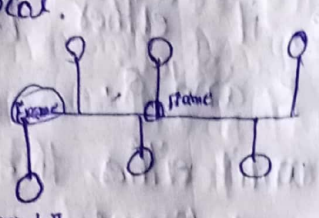
CSMA/CD (CSMA with collision Detection)
CSMA/CA (CSMA with collision Avoidance)

1- Persistant CSMA

* Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
* if the channel is idle, the station transmits a frame
* if busy, then it senses the transmission medium continuously until it becomes idle. (ever sec check it free Then only send)
* since the station transmits the frame with the probability of 1 when the carrier or channel is idle this scheme of CSMA is called as 1- persistant CSMA
* The propogation delay has an important effect on the performance of the protocol.

* The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.

ex:



2. NON-Persistant CSMA

busy or free

* Before sending, a station senses the channel. if no one else is sending the station begins doing so itself.
* ~~if the channel is idle, the station transmits a frame.~~
* ~~if busy, then it senses the transmission medium medium continously until it becomes idle.~~
* However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission. (Randomly checking so it highly delay)

Randomly checking

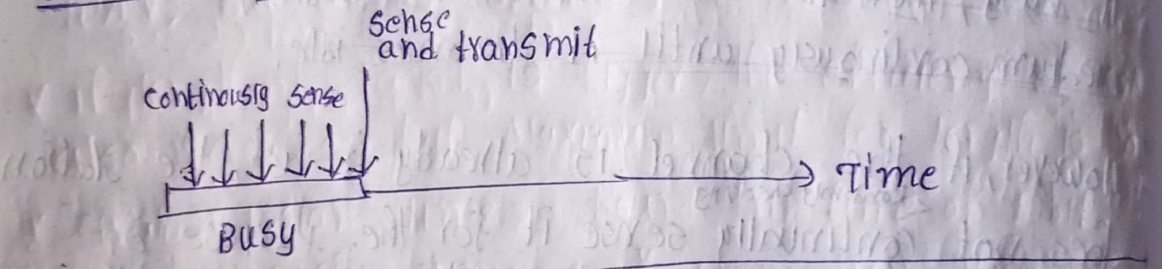
* instead, it waits a random period of time and then repeats the algorithm. consequently, this algorithm leads to better channel utilization but longa delay than 1-Persistent CSMA.

P-persistent CSMA

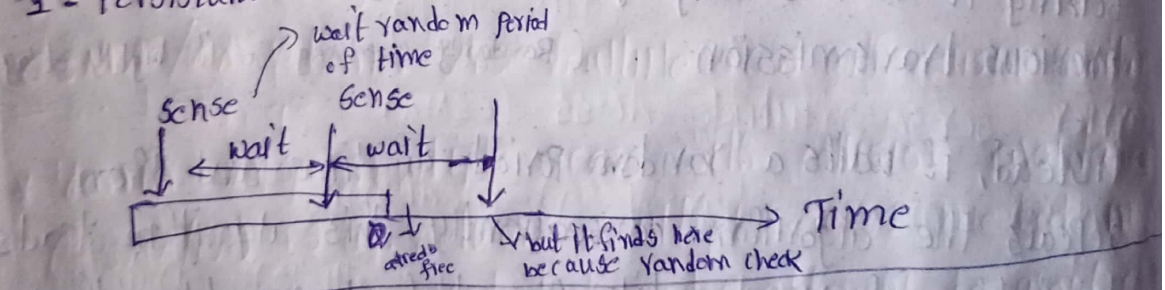
* it applies to slotted channels (in slotted channels each node send it only its time slot).
* When a station becomes ready to send, it senses the channel
* if it is idle, it transmit with a probability P.

* with a probability $q = 1-p$, it defers until the next slot.
* if that slot is also idle, it either transmits or defers again, with probabilities p and q.
* This process is repeated until either the frame has been transmitted or another station has begun transmitting.
* in the latter case, the unlucky station acts as if there had been a collision (i.e, it waits a random time and starts again).
* if the station initially senses the channel busy, it waits until the next slot and applies the above algorithm.

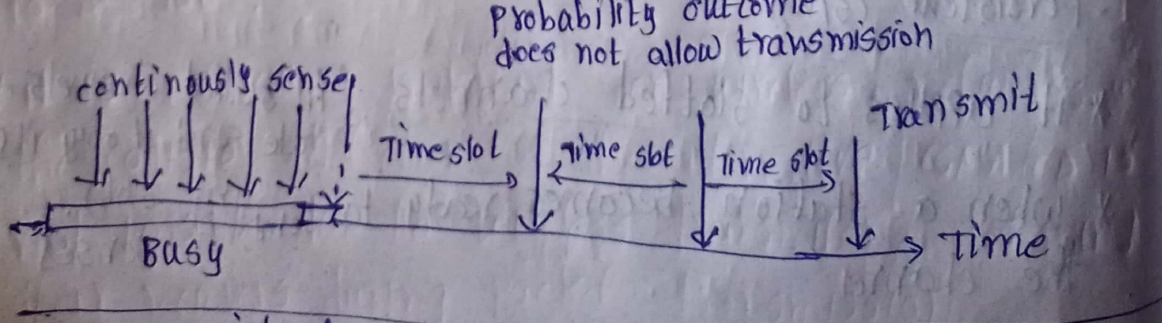
Behaviour of Three persistent Methods



1 - Persistant



Non - Persistant



P - Persistant

0- Persistent CSMA

* Each node is assigned a transmission order by a supervisory node.

Carrier Sense Mulliple Acess (CSMA/CD)

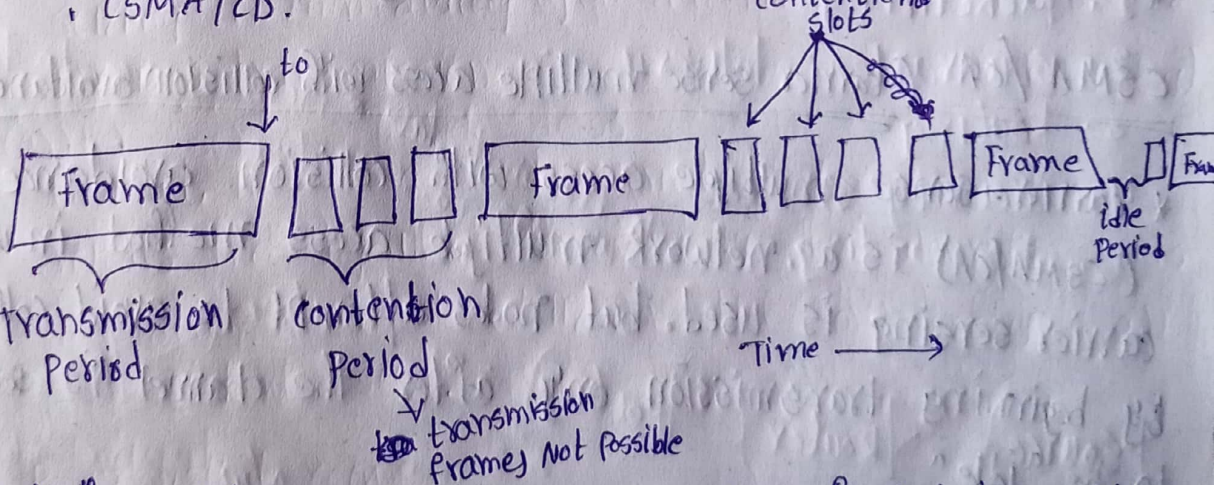
* if the two stations sense the channel to be idle and begin transmitting simultaneously they will both detect the collision almost immedialely.

* as soon as the collision detected the stations should stop transmitting because these corrupted frames becomes useless.

* quickly terminating damaged frames saves time and bandwidth.

* This protocol, Known as CSMA/CD (CSMA with collision Detection) is widely used on LANS in the MAC sublayer.

* The most widely used wired LAN technology The Ethernet : CSMA/CD.



* At the point marked to, a station has finished transmitting its frame.

* Any other station having a frame to send may now attempt to do so. if two or more stations decide to transmit simultaneously, there will be a collision.

* Collision can be detected by looking at the power or pulse width of the recieved signal and comparing it to transmitted signal

* After a station detects a collision, it aborts its transmis
waits a random period of time, and then tries again, assu
that no other station has started transmitting in the
mean time.
* Therefore, model for CSMA/CD will consist of alternati
contention and transmission periods, with idle periods
occurring when all stations are quiet.

* CSMA/CD -

$$\text{efficiency} = \frac{1}{1+6.44 \times a}$$

$$a = \frac{Tp}{Tt}$$

* if distance increases, efficiency of CSMA decreases.
* CSMA is not suitable for long distance networks like WAN; but works optimally for LAN
* if length of packet is bigger, the efficiency of CSMA also increases; but Maximum limit for length is 1500
* Transmission Time >= Round Trip time of 1 bit.
* Transmission Time >= 2* propagation Time.

CSMA/CA (carrier sense multiple access with collision avoidance)

* carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used. but nodes attempt to avoid collis by beginning transmission only after the channel is sense to be "idle".
* it is particulary important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmiters desensing their recievers during packet transmission.

* CSMA/CA is unreliable due to the hidden node problem and exposed terminal problem.

* Solution : RTS/CTS exchange.

* CSMA/CA is a protocol that operates in the Data link layer (layer 2) of the OSI model.

* The Access method used by IEEE 802.11 wi-fi is CSMA/CA.

Multiple Access Methods used by
Ethernet : CSMA/CD
wi-fi : CSMA/CA