DATA LINK LAYER →

① Services (Data link provides to network layer)
② Framing
③ Flow control
④ Error Control
⑤ Access Control.

Services →

1. Unacknowledged connectionless Service

→① It is appropriate when error rate is very low

② It is suitable for real time traffic such as voice.

2. Acknowleged connectionless Service

→ It is useful over unreliable channel such as wireless systems.

3. Acknowledged connection Oriented Service

→ It is the most sophisticated service provided by DLL to network layer.

→ It gaurantees two important points
① Every frame will be recieved exactly once
② Frame is recieved in the right order

Application ⇒ WAN's

- **Framing** → It is a process of separating messages from one sender to another or from one destination to another.

Framing
- Fixed sized
- Variable sized

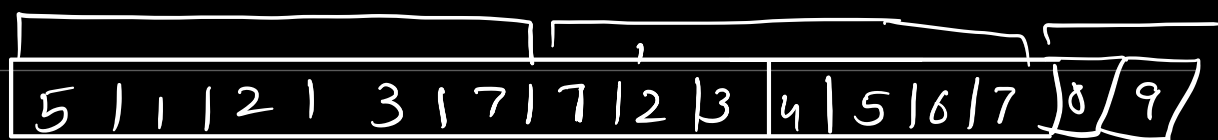
- An application of fixed size framing is in ATM's in WAN
- Appl^{n} of Variable sized is LAN

Delimiter → It is a character that marks the beginning or (and) end of the unit of Data.

- Variable sized framing is categorized into
  → ① Character oriented protocol
  ② Bit " "

These utilizes 4 diff. ways →

① Character count.



Limitation → ① The count can be garbled during transmission.

② The problem with resynchronization is eminent b'coz of which it is barely used.

② Flag Bytes with Byte Stuffing →

- In this mechanism each frame starts

and end with special bytes.

- It helps in removal of resynchronization

Flag	H	Payload field	T	Flag

- **Issues** → ① A | FLAG | B → A | ESC | Flag | B

  ② A | ESC | B → A | ESC | ESC | B

  ③ A | ESC | FLAG | B → A | E | E | F | E | B

Limitations → ① The use of 8 bit characters is not always possible in every machine

- Utilised in PPP protocol (point to point)

③ Starting/end flag with bit stuffing

→ Each frame starts & end with same pattern.

→ whenever sender's DLL encounters 5 consecutive 1's in data. It automatically stuffs 0 bits into outgoing bit stream.

→ This bit stuffing is analogus to byte stuffing in which an escape byte is stuffed into the ongoing character scheme before the flag byte in Data.

→ When reciever recieves 5 consecutive 1 bits followed by 0 bit. It automatically destuffs the zero bit.

0 111111 0
0

0110 1111111111111111 0010

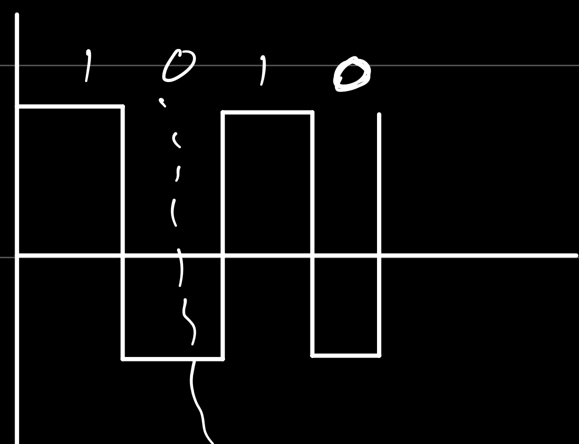
↓

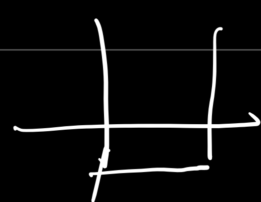
0110 11111 $\boxed{0}$ 11111 $\boxed{0}$ 11111 $\boxed{0}$ 0010

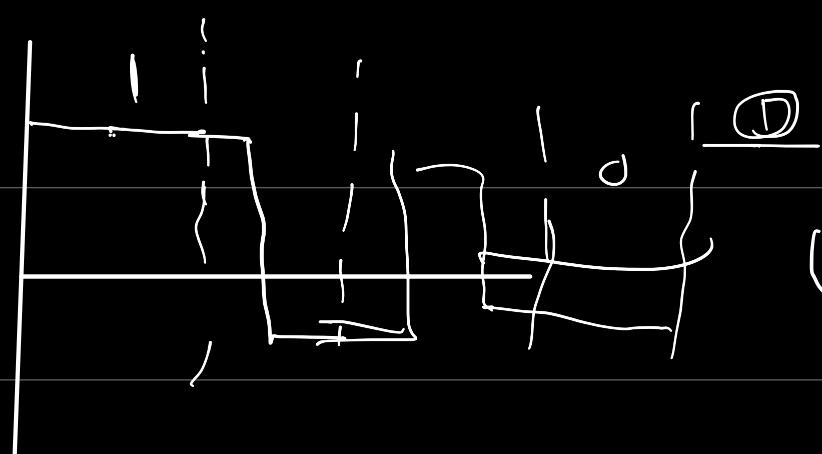
Stuffed bits.

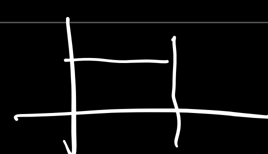
4. Physical Layer Coding voilations ⇒ It is only applicable to networks in which the encoding on physical medium contains some redundancy.

• We can apply diff. set of rules to solve the problem of data extraction from a frame. ex. enforcing a high/Low pair as 1 and low/high pair as zero and proving a neccessity for the transition to occur only in middle will help in identifying the data as the transition in middle ensures to locate the bit boundaries. In such a case the delimiter can be set as either a high-high pair or a low/low pair.









(1,0) (0,1)

• Types of Delays →

① Queing Delay ⇒ It is the amount of time a message is waiting in the queue before being taken out for processing. Varies from 0 – ∞. It depends on the processing speed and buffer capacity.

② Processing ⇒ Amount of time taken by the machines to process a packet or frame or message i.e looking at destination ip, extracting network id searching in the routing table and identifying the destination route. Depends on processing speed of machine.

③ Tx. Delay → Amount of time taken by machine to transfer the message to the outgoing link

$$TD = \frac{L}{B}$$

$L \rightarrow$ size of packet

$B \rightarrow$ Bandwidth of channel.

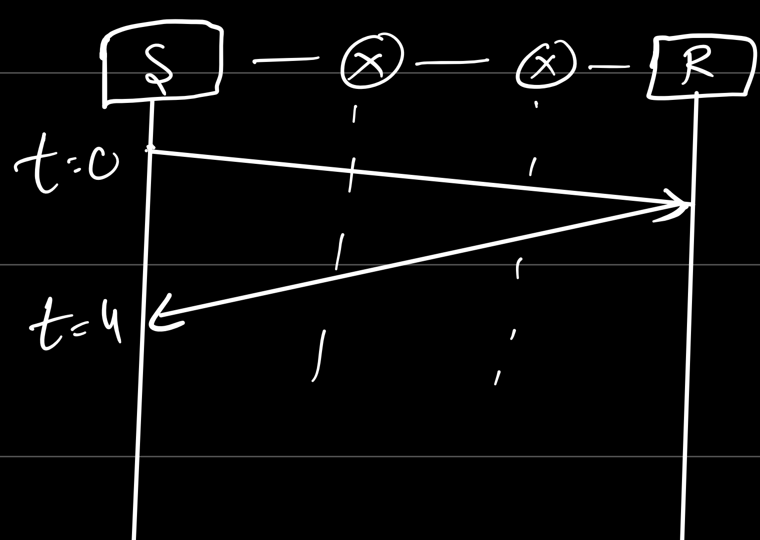
(4) **Propagation Delay** $\rightarrow$ Amount of time taken by the message to make a physical journey from one machine to another.

$$\left(PD = \frac{d}{v} \right)$$

$d \rightarrow$ distance b/w these two machine

(5) **Link-to-Link Delay** $\rightarrow$ Assuming that there are 2 devices in the network d_1 & d_2.

Round Trip Time (RTT)



$$RTT = PD(D_1 \rightarrow D_2) + PrD(D_2) + TD(D_2) + PD(D_2 \rightarrow D_1) + QD(D_2)$$

(6) End-to-End Delay →

$$RTT = 2\left[PD[(D_1 \rightarrow D_2)] + N(QD + PrD + TD)\right]$$

$N \Rightarrow$ intermediate router / machines.

$$\boxed{\text{Time Out, T.O.} = 2 \times RTT}$$

- **NOTE** → In networked enviornment 3 types of packets are possible
  → (1) Data
  (2) Control
  (3) Acknowledgement
  - +ve
  - −ve

If n is the no. of messages to be sent
for +ve $= n+1$
−ve $= n$.

ACK

Independent

For every message recieved you have to send ack.

Cummulative

The reciever send Ack after some set of messages.

- Piggy Backing →

DATA.

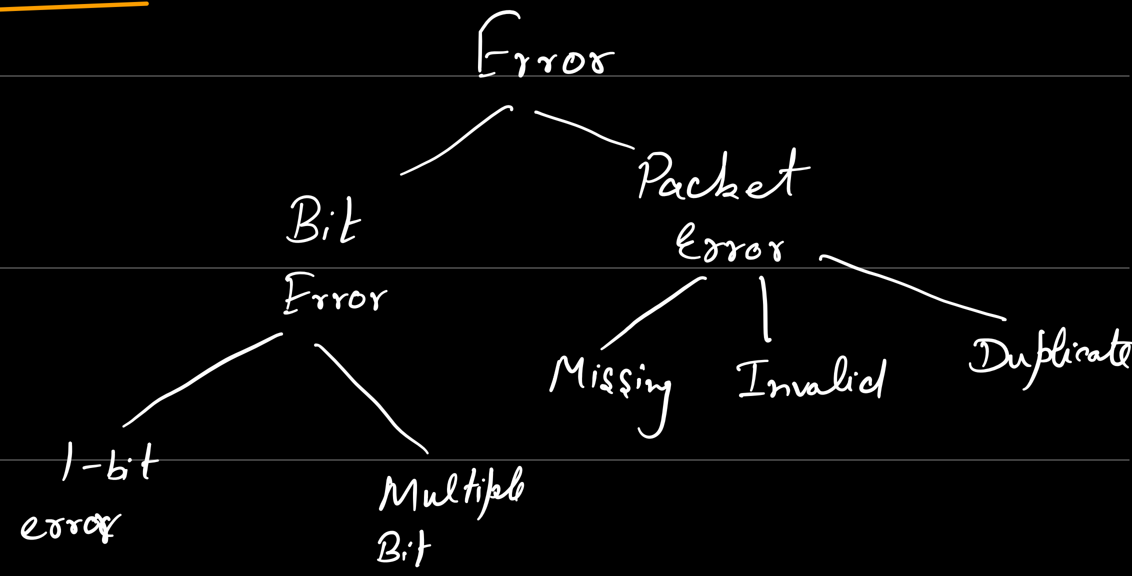
- NOTE → ① Network traffic is low in cummulative Ack.

② In independent Ack. if the Ack. no. is n then the nth packet is assumed to be recieved.

③ In independent Ack high traffic is accepted.

④ Reliability is higher in independent Ack.

- **Error Control** →



- Multiple Bit error is also called burst error

- **NOTE** → Single bit error occurs in parallel transmission while multi bit errors occurs in serial transmission usually.

- **Reason for Bit error** → (1) Noise

- Usually the serial communication takes place when length of communication is long otherwis parallel transmission is used.

- Burst length is calculated from extreme end of error.

Example => Burst length of an OS depends on the no. of bits that OS posseses.

- Error Detection → Error detecting codes include redundancy to allow the reciever to deduce that error has occured but not which error and no request for retransmission is initiated.

- Error Correction → ECC includes enough redundant info along with each block of data sent to enable the reciever to deduce what the transmitted data must have been.

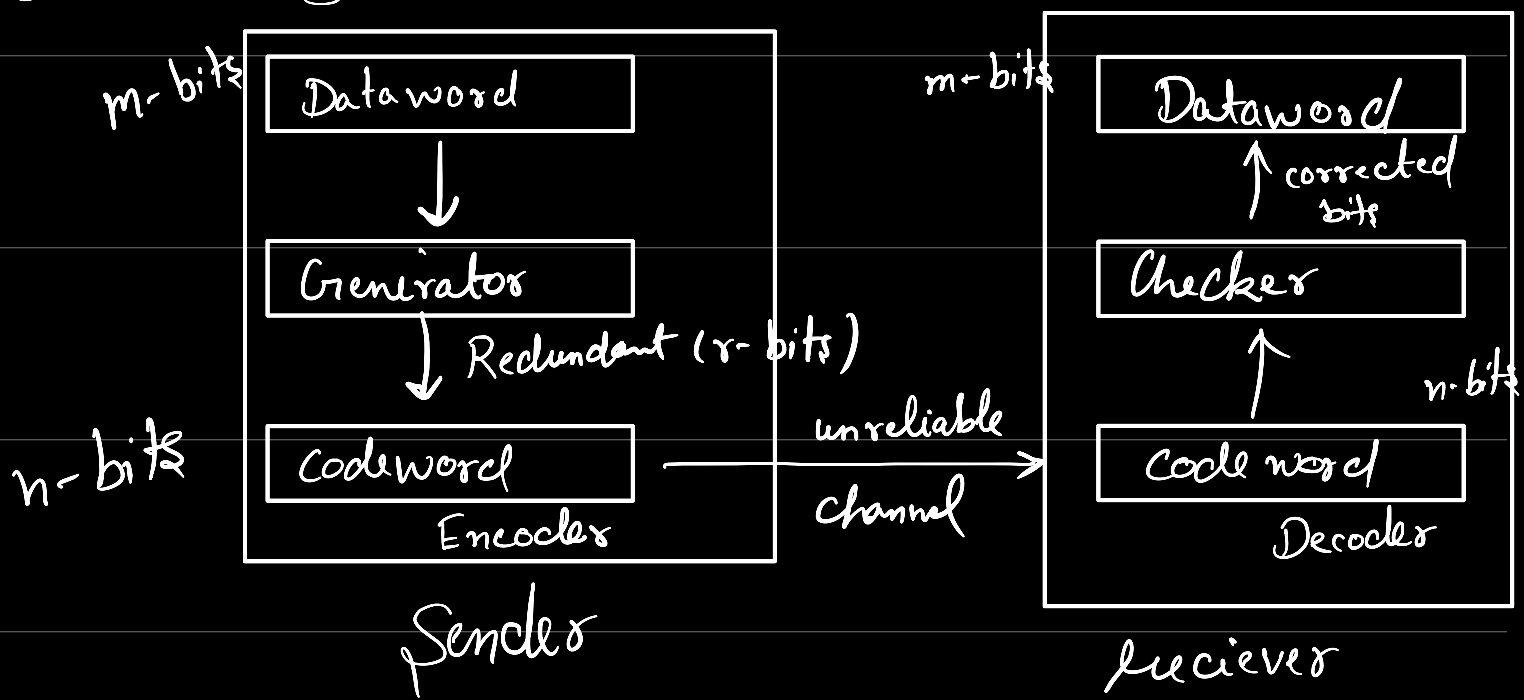
- Consider that m represents data bits.

  r → redundant bits

  $n = m + r$

  ↳ codeword

here the redundant bit is the additional number of bits added to already existing data word or data bit for the purpose of checking the error in the bits transmitted.



- **Hamming Distance** → Given two codewords X & Y Hamming distance provides the no. of bit position in which two code words differ.

Q Find min. Hamming distance

Data Word	Codeword
00	00000 - f_1
01	01011 - f_2
10	10101 - f_3
11	11110 - f_4

$d(f_1, f_2) = 3$ $\qquad$ $d(f_2, f_3) = 4$

$d(f_1, f_3) = 3$

$d(f_1, f_4) = 4$

Min = 3.

• NOTE → ① To garuntee the detection of upto s errors the min. Hamming distance in a code must be $s+1$.

② To garuntee the correction of upto s errors the min. hamming distance must be $2s+1$.

Techniques of Error detection →

The codes can be of two types

① Linear block code

② Cyclic Code

• In case of linear block code the XOR of any two code word gives another valid codeword.

- In cyclic code the code word is cyclically shifted or rotated to obtain a result which is another code word.

① Simple Parity check →

odd   even.

01100100	10001111	10011001
f_1	f_2	f_3

f_1 01100100 $\boxed{1}$ → trailer.

f_2 10001111 $\boxed{1}$

f_3 10011001 $\boxed{0}$

- CRC → Cyclic Redundancy Check

⇒ It is based on binary division

→ It consists of seq. of redundant bits called cyclic redundancy check bits which are appended to the end of data unit so that the resulting data unit becomes exactly divible by second binary numbers which is predetermined.

→ At destination it is divided by same determined number.

→ If at this step there is no reminder data unit is assumed to be correct and accept.

→ A reminder indicate the data unit has been damaged during transmission therefore must be rejected.

Algorithm ⇒

① Let r be the degree of $G(x)$ where $G(x)$ is called generator polyⁿ.

// Append r_0 bits to the low order end of the frame so that it now contains $(m+r)$ bits. (where $m \Rightarrow$ no. of bits in data) and corresponds to the polyᵐ $x^r M(x)$.

② Divide the bit string corresponding to $x^r M(x)$ using modulo 2 division

③ Subtract the reminder which is always r or fewer bits from the bit string corresponding to $x^r M(x)$ using modulo 2

The result is Checksummed frame to be transmitted. Assume it to be polyᵐ $T(x)$.

• NOTE → If $G(x)$ has n bits then append $(n-1)$ zeros in the data word

$m: 11011$

$x^r M(x) = x^4 + x^3 + x + 1$

$G(x) = x^2 + x + 1$

Example → Frame : 1101011011

$G(x) = x^4 + x + 1$

$= 10011$

1101

1+4+8 = 13

1011

3

11

10011) 11010110110000

10011

10011

10011

1011

Append (n-1) zeros

1110 ⇒ reminder.

1101011011 $\boxed{1110}$ ⇒ new append kardia. 0000 ki jagah.

- Adv. ⇒ ① Good performance in detecting single bit and burst errors
  ② It can be implemented efficiently in hardware and software.

- **CheckSum** ⟶ In checksum error detection scheme the data is divided into n- segments each of m bits.

In the sender's end the segments are added using 1's complement to get the sum.

This sum is complemented to get the checksum.

⟶ The checksum segment is sent along the data unit.

⟶ At the reciever's end all recieved segments are added using 1's complement arithmetic sum to get the sum.

→ The sum is complemented and if that is zero then it is accepted.

n, m

3, 10, 8, 9, 11, 41

$\boxed{-41}$

$\boxed{10}1001$

→ 10

11 1011

1's complement 0100

4 (checksum)

Reciever par ye be add hoga with the given data.

Sender

3
10
8
9
11

41

Reciever

3
10
8
9

$\boxed{10}$1101
$\hookrightarrow$ 10

1111
$\Downarrow$
complent is Zero.

11
41
+4
45

Example 2 → | 10011001 | 11100010 | 00100100 | 10000100 |

f_1 f_2 f_3 f_4.

$n = 4$
$m = 8$

f_1 10011001
f_2 11100010

1 01111011
1

01111100
f_3 00100100

10100000
f_4 10000100

00100101

1's comp 11011010 ← checksum.

- Internet CheckSum →

  - Sender → ① Message is divided into 16 bits words.
    ② Value of checksum word is said to 0.
    ③ All words including checksum are added using 1's complement addition.
    ④ Sum is complemented and considered as checksum for the whole data.
    ⑤ Checksum is sent with the data.

  - Reciever → ① Message is divided into 16 bit words.
    ② All words are added using 1's complement addition

3. Sum is complemented and becomes the new checksum.

4. If value of checksum is zero then it is accepted otherwise it is rejected.

65, 97
A a

Ex. Forouzan

FO → 111 ASCII

ASCII 70

ro → 6F

uz

an

0
1
2
3
4
5
6
7
8
9
A 10
B 11
C 12
D
E
F

$16 \overline{)70} (4$
64
6

46

97 → a

$16 \overline{)111} (4$
96

F → 46] → B5
O → 6F

r → 72] → E1
o → 6F

u → 75] → EF
z → 7A

a → 61]
n → 6E

4 6 6 F   Fo

7 2 6 F   ro

7 5 7 A   uz

6 1 6 E   an

8 F C 6

1

8 F C 7

1's → 7038

Reciever End ⇒

8 F C 7
7 0 3 8

F F F F

↓ 1's complement

0000.

- **Error Correction Techniques** ⇒ There are two ways with which error correction is performed

① Backward error correction

↳ It is done by the virtue

of ~~ee~~ transmission

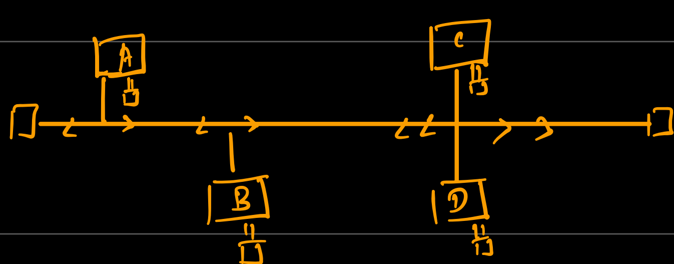
② Forward Error Correction

① It uses error correcting codes to generate actual frames.
Some of the methods utilized are
① hamming code
② Binary con~~v~~volation code.
③ Read-soloman code
④ Low density parity check code.

- Self paced assignment → What is the Int. std. in IEEE 802 to detect errors

Note → x^{32} means it can detect ≤ 32 burst errors.

- Access Control →

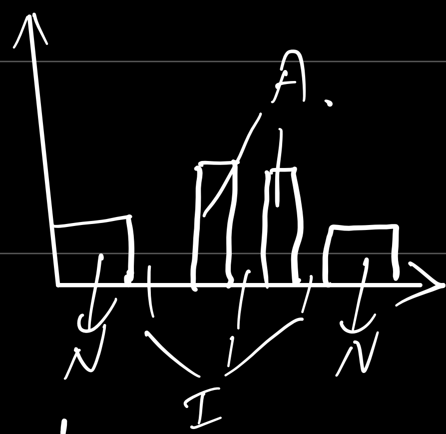


Levels (of signals)

Zero — Idle

Normal —

Abnormal - collision



DLL

LLC → Logical link control

Error control

MAC → Media access control

multiple

(SLIDES) Access.

- Pure Aloha relies on Ack. from reciever thus two imp. parameter affect the efficiency of Aloha protocol

① Max^m attempts. of retransmission

② Backoff time → pure Aloha dictates that when time out period passes each station waits a random amount of time before resending its frames.

Randomness will help to avoid more collisions. This time is known as backoff time.

Q The stations on a wireless Aloha Network are a max^m of 600 Km apart. If we assume that signals propagate at 3×10^8 m/s find the value of backoff time T_B. for k = 1, 2, 3, ...

→ $T_p = 2$ ms (d/v)

$k = 1$ $[2^{k-1}$ combination$)$

$\{0, 1\}$

$\left.\begin{array}{l} 0 \times 1 = 0 \\ 1 \times 2 = 2 \end{array}\right] \rightarrow$ choice for T_B

$k = 2$

$\{0, 1, 2, 3\}$

Q A pure Aloha network transmit 200 bit frame. on a channel 200 kbps. What is the req. to make it collision free.

Soln =>

$$T_{fr} = \frac{200}{200 \text{ kbps}} = 1 \text{ ms}$$

vulnerable time = 2ms.

No station should transmit later than 1ms before the station starts transmission and ~~an~~ no other station should start sending during the 1 ms period while this station is transmitting or sending.

Q A pure Aloha network transmit 200 bit frames on the shared channel of 200 kbps. What is the throughput if system produce 1000 frame/sec.

→

$$T_{fr} = 1 \text{ms}$$

$G = 1$ frame / ms

Throughput $= G * e^{-2G}$
$= 0.135$

CSMA ⇒ slides se padhna.

Q A network using CSMA cd has a B.w of 10 Mbps. If maxm propagation time (two way propagation) is 25.6 μs what is the min. size of frame.

Soln ->

$T_{fr} = 2 \times 25.6$
$= 51.2\ \mu s.$

$512/8$

$2^9/2^3 = 2^6$
$= 64$

frame size $= T_{fr} \times B.w$
$= 512$ bits
$= 64$ bytes

• NOTE -> The value of T_{fr} implies that the station needs to transmit for

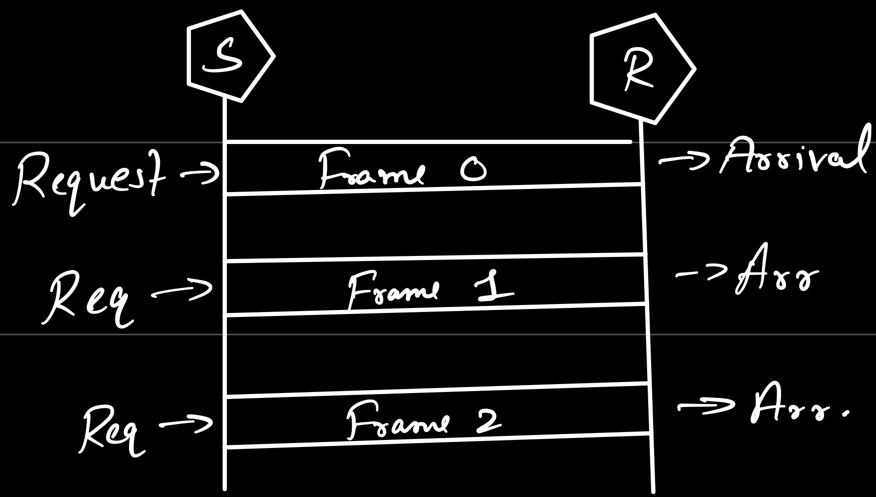
51.2 μs to detect the collision.

- **Flow Control** →
  - Noiseless channel
    - Simplex protocol
    - Stop & wait protocol
  - Noisy
    - Stop & wait (ARQ)
    - GBN (ARQ)
    - SR (ARQ)
      ↓
      Automatic repeat request.

- **Note** → Theoretical protocols of flow control considers unidirecn flow of data whereas irl the data flow is bidirecn which sometimes utilizes piggy backing.

- **Simplex Protocol** → It is a unidirecn protocol in which data frames travel only in one direcn.

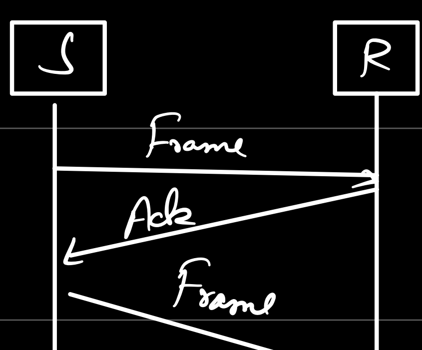
It has no error control & no flow control.



Limitations

1. If a sender sends data frame at much higher speed then that can processed at reciever end with storage limitations then this model will not be a suitable one.
2. The denial of Services.

- **Stop & Wait Protocol** → This mechanism suppoot flow control but doesn't support error control.



- **Problems** → ① No error control.

(in real time) ② Lost data (frame)

③ Lost Ack.

④ Delayed Ack.

SOLUTIONS → ① Time out mechanism

② Seq. no. of data transmitted

③ Seq. no. of Ack.

SW + TO + seq(F) + seq(Ack)

↓

SWARQ

- **SLIDING WINDOW Protocol** → Used in connection oriented communication.

Offers flow control and packet level

error control.

Used in both transport and DLL.

It is a theoretical concept which is practically implemented as stop & wait go back N and selective repeat.

- Stop & Wait ARQ → It adds simple error control mechanism in the existing stop & wait protocol.

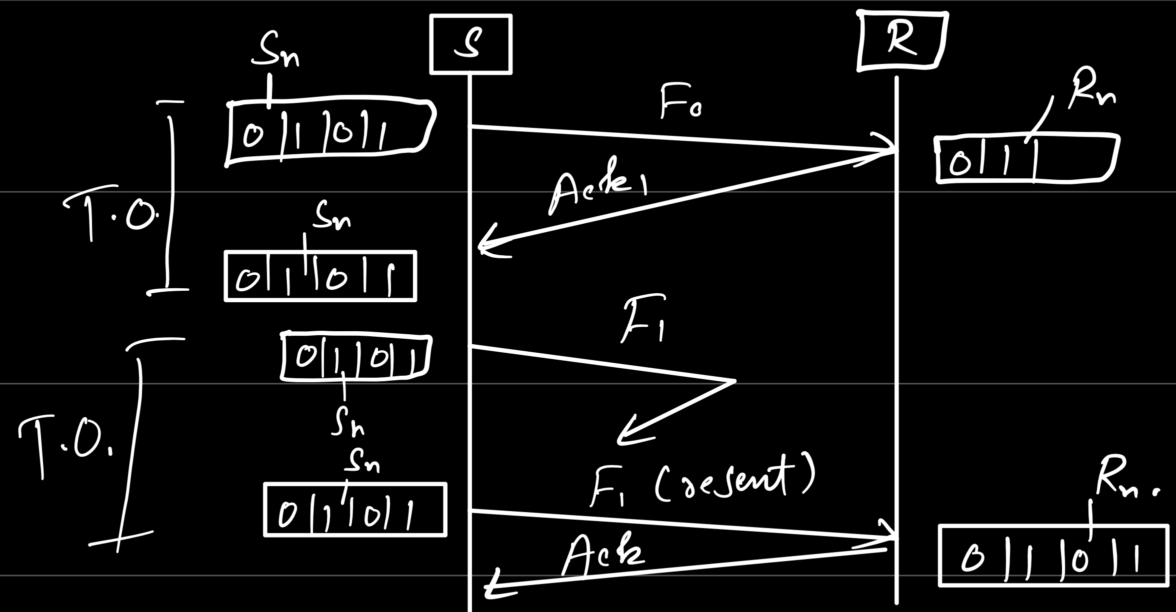
Error correction is done by keeping a copy of sent frame and retransmitting when timer expire.

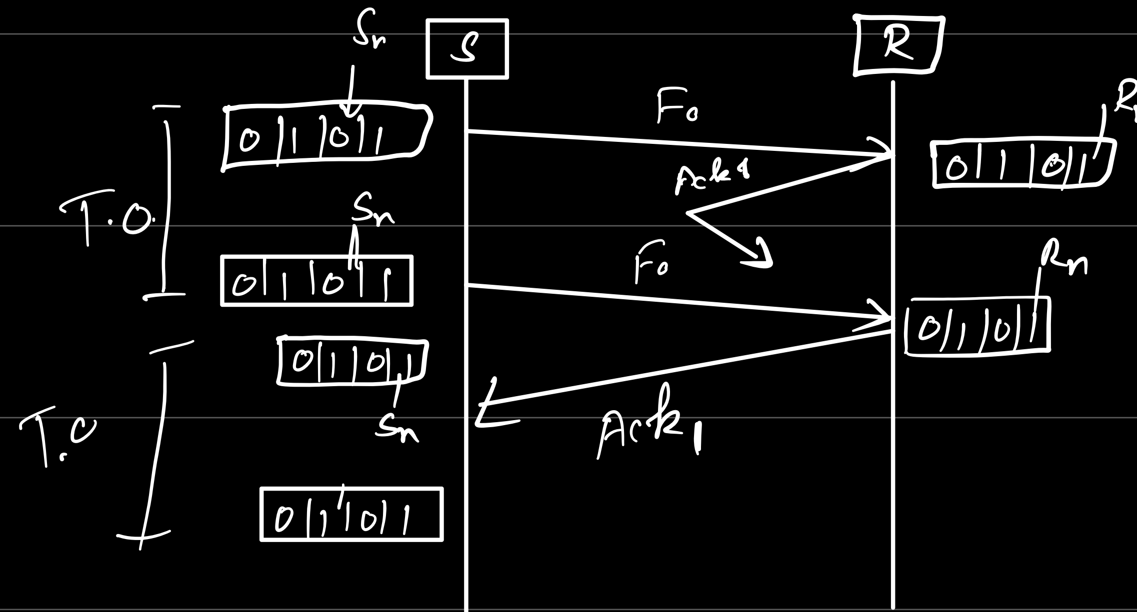
The Seq. no. is used to provide the numbering to the frames being sent.

The no. scheme specifies the fact that if x^{th} frame is sent then next will be $(x+1)^{th}$.

The control variables utilized in Stop & wait ARQ are S_n and R_n

when S_n is the n^{th} frame to be sent and R_n is the n^{th} frame recieved. The seq. no. utilized modulo 2 arithmetic.





Numerical → If B.w of a link is 1.5 Mbps. Round trip is 45 ms and packet size = 1 Kilo bytes. Then find Link utilization in stop & wait protocol.

$$\frac{2^{10} \times 8}{1.5 \times 45 \times 10^{-3} \times 10^{6}}$$

B.W = 1.5 Mbps

Size = 1 KB

RTT = 45 ms.

$$\text{Throughput} = \frac{1 \text{ data}}{RTT} = \frac{1024 \times 8}{45 \times 10^{-3}}$$

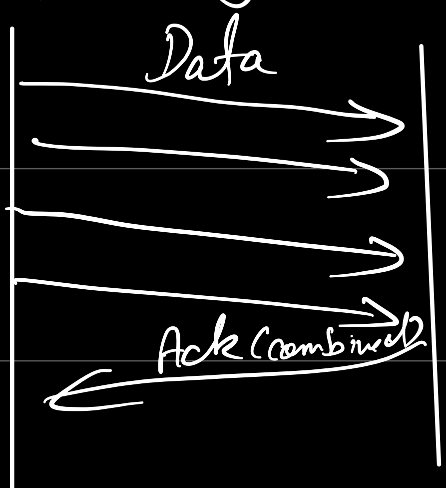
$$= 182 \text{ Kbps}$$

$$\eta = \frac{\text{Throughput}}{B.W} \times 100$$

$$= \frac{182}{1500} \times 100$$

$$= 12.13\%$$

Pipelining



- Problems with pipelining →

1. It requires more seq. numbers
2. In terms of hardware it req. more buffer space.

- IEEE 802 Standards →

LLC
MAC

IEEE 802 standard	Name of standard
802.1	higher layer LAN protocol working group.
802.2	Standardization of LLC
802.3	Ethernet
802.4	Token bus
802.5	Token Ring
802.6	Standardization of MAN
802.7	Broadband LAN using coaxial cable.
802.8	Fibre optic Tag
802.9	Integrated Services LAN

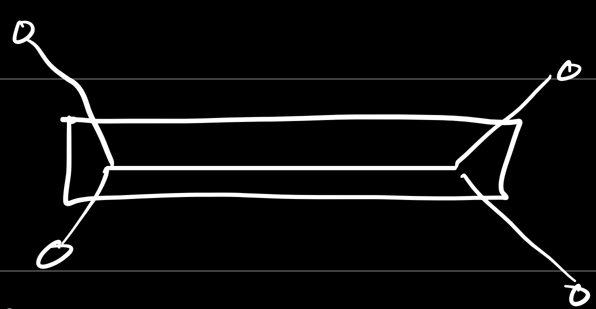
802.10	Interoperable LAN Security.
802.11	wireless LAN
802.12	100 base VG
802.13	unused.
802.14	Cable modems
802.15	wirless PAN
802.15.1	Bluetooth.
802.15.2	Co-existence of
802.15.3	Ultrawide band.
" 15.4	Zigbee
" 15.5	wireless PAN (Mesh network
" 15.6	BAN (body Area Network)
15.7	Visible Light communication
802.16	Wi Max → Broadband wireless Access.
⋮	
802.24.	

- **Ethernet →** • Characteristics

→ Ethernet offer connectionless communication

→ No flow control and packet level error control.

→ No acknoledgement
→ Uses bus topology as a logical topology and star as the physical topology.



It uses CSMSCD as an access control Method.

- **Evolution of Ethernet →**

① Std. Ethernet → some times known as basic ethernet.

2. **Fast Ethernet** → 100 Mbps

3. **Gigabit Ethernet** → 1 Gbps

4. **10 Gigabit Ethernet** → 10 Gbps.

- **Frame Format** →

7 Byte	1 Byte	6 Byte	6 Byte	2 Byte	46-1500 Byte	4 Byte
Preamble	SFD	SA	DA	Data Length	Data	CRC
Header					Actual Data	Trailer

- **Preamble** → It consists of 1's and zeros for 7 Bytes.
  - Used for synchronization purpose

  - SFD → Start of Frame Delimiter
    ↳ consists of 1s and zeros but Last two bits will always be 11.

  - **SA & DA** → They are 48 bit physical address representing

Source & destination

- **DATA** → The min. frame in ethernet is 46 Bytes Long so that we can make out 72 Bytes frames wherein Maxm size of data is 1500 Bytes.

- **Data length** → Since data is varying from 46 - 1500 Bytes to keep track of correct size of data this field is needed.

- **CRC** → It is added as part of trailer to identify bit errors.

- **NOTE** → ① Data rate supported by ethernet are 10 Mbps, 100 Mbps, 1 Gbps

  ② It utilizes 48 bit physical addressing scheme.

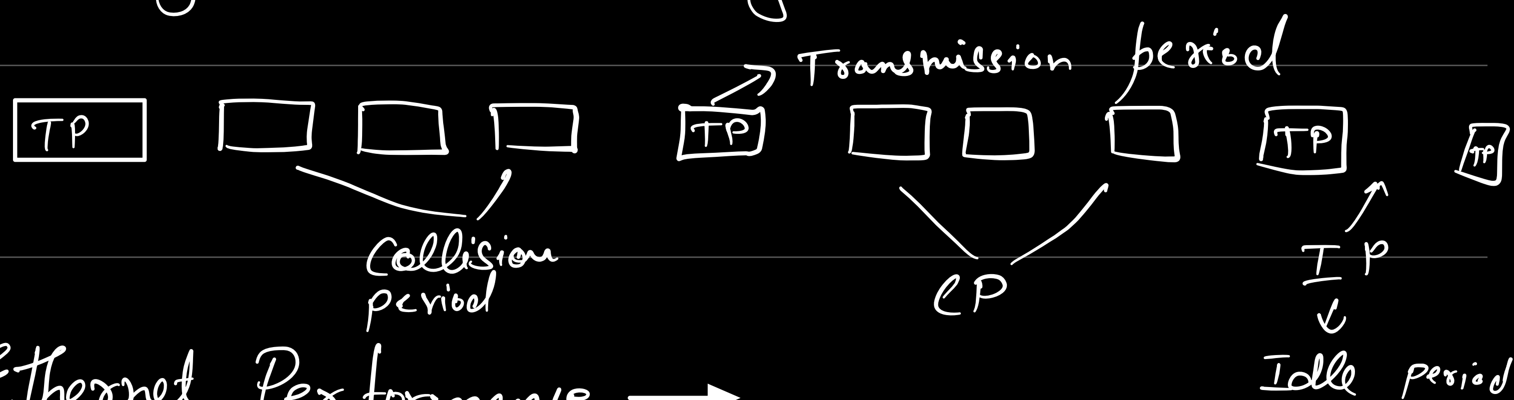
  ③ Signaling used is Manchester encoding.

Min		Max		
46	–	1500	→	Data
72	–	1526	→	frame.

- **Efficiency →**

NOTE → ① In worst case scenario it takes 51.2 μs to detect a collision in ethernet protocol.

② The min. size of frame supported by ethernet is of 512 bits.



Ethernet Performance →

Let N is total number of systems in the network, P_s is probability of a station to transfer data, $1-P_s$ probability of station not to transfer data.

$(1-P_s)^{N-1} \Rightarrow$ Probability for remaining $N-1$ stations not to transfer data

$P_s(1-P_s)^{N-1} \Rightarrow$ Probability of success of a single station.

$$\boxed{\underbrace{\eta}_{\text{Efficiency}} = \frac{TP}{TP + CP + IP}}$$

Assume IP is negligible

$$\eta = \frac{TP}{TP + CP} \quad — ①$$

$NP_s(1-P_s)^{N-1} = A = 1/e$ — ② $\Rightarrow$ probability of success of any arbitrary station among N stations.

- Number of contention slots will be equal to $1/A = e$.

From equation ② when $N \to \infty$

then $A = 1/e$

Contention period is the sum of no. of contention slot and slot duration.

$$\eta = \frac{1}{1 + \frac{2 d B e}{L V}}$$

d → Distance

B → Bandwidth

V → velocity

L → Length of tx./size of packet

$$\eta = \frac{TP}{TP + CP}$$

$$= \frac{t_{trans}}{t_{trans} + 2 \times t_{prop} \times e} = \frac{TP}{TP + CP + t_{prop}}$$

$$= \frac{1}{1 + 2ae} = \frac{1}{1 + 6.44a}$$

$$= \frac{1}{1 + 5.44a}$$

where $a = \frac{t_{prop}}{t_{trans}}$.

Q Consider an 802.3 LAN with 500 stations connected to 5 500 m segments.
The data rate is 10Mbps. Slot time = 51.2 μs.
If all stations transmit with equal probability. What is the channel utilization for frame size of 512 Bytes
Assume no. of contention slot = 1.716

Given →

$B.W = 10 \text{ Mbps}$

$N = 500$

slot time = 51.2 μs

$L = 512 \text{ Bytes}$

$$T_x \text{ period} = \frac{L}{B} = \frac{512 \times 8}{10 \times 10^6}$$

$$= \frac{2^{12}}{10^7}$$

$$= 0.4096 \text{ ms}$$

$$C_p = \text{no. of contention slots} \times 51.2 \times 10^{-6}$$

$$= 1.716 \times 51.2 \times 10^{-6}$$

$= 8.78 \times 10^{-5}\, s$

$$\eta = \frac{TP}{TP + CP}$$

$$= \frac{0.4096}{0.4096 + 878 \text{ ms}}$$

$$\eta = 0.82$$

Utilization $= 82\%$.

Q A channel has bit rate of 4 kbps and Propagation delay $= 20$ ms

1 sec me 20m propagate hora h!

For what range of frame sizes The stop and wait protocol gives efficiency of 50%

$$\eta = \frac{T_D}{T_D + \underbrace{2 \times P_D}_{RTT}} = \frac{1}{1 + 2 \cdot \frac{P_D}{T_D}}$$

$$= \frac{1}{1+2a}$$

where, $a = \frac{P_D}{T_D}$

$$\eta = \frac{L/B}{L/B + R}$$

$$= \frac{L}{L + BR}$$

- NOTE → (1) If $L = BR$ $\eta = 50\%$

(2) If $L > BR$ $\eta > 50\%$

(3) " $L < BR$ $\eta < 50\%$

$B = 4$ Kbps

$L = BR$

$$L = 4 \times 10^3 \times 40 \times 10^{-3}$$
$$= 160 \text{ bits}$$

Q. Consider a MAN with avg. src & dst 20 Km apart and one way delay of 100 μs. At what data rate does the Round trip delay = T_x delay for a 1 KB frame.

$$RTT = T_D$$

$$2 \times P_D = \frac{L}{B}$$

$$2 \times 100 \times 10^{-6} = \frac{1 \times 8 \times 1024}{B}$$

$$BW \rightarrow 10^3$$

$$\text{size} \rightarrow 1024.$$

Steps to solve Problems in Stop & wait Protocol →

① Calculate RTT

② Based on the given B.W & RTT or either of them (whichever is suitable for the problem at hand.)

Calculate no. of bits we are able to transfer within RTT & equate it as w bits

↳ sliding window

③ $W_p = \frac{W_{bits}}{PS_{bits}}$ where PS is the packet size in bits.

④ Seq. no. req. = W_p

⑤ Equate $2^k = W_p$ where k = no. of bits in seq. no. which is fixed.

Q Suppose that you are designing 10Mbps sliding window protocol for P2P link to the moon. which has one way latency of 1.25 sec. Assume that each frame carries 1 KB of data what is the min. no. of bits you need for seq. number.

Soln

① RTT = 2.5 second

② 1 sec − 10^6 bits

$W_{bits} = 2.5 \times 10^6$ bits

③ $w_p = \dfrac{2.5 \times 10^6}{1024 \times 8}$

$= 305.17$

④ $2^k = 305.17$

$k = 9$