

O.L.O.L.
Data Link Layer

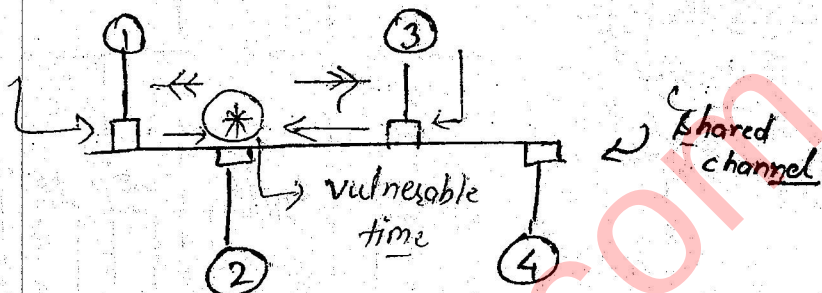
(Shared channel)
MAC Layer
(medium access control)

forming.

* "MAC Layer"

to overcome collisions,
Internet with NIC card.

⇒ "Pure ALOHA"



Rules:-

1) Any system is having data, it can transmit immediately.

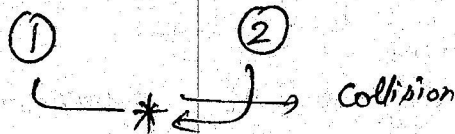
* If two or more systems transmit the data at the same time, then there is a possibility of collision.

* The Time at which the collision occurs is known as vulnerable time.

* Once there is a collision, system has to wait a random amount of time known as, Back-off time.

* Back-off time is given by Exponential back-off algorithm?

Exponential Back-off algorithm:-



k = Collision No

$$\therefore W.T._1 = (0 \text{ to } 2^{k-1}) * P.T.$$

$$= (0, 1) * P.T.$$

$$W.T._2 = (0 \text{ to } 2^{k-1}) * P.T.$$

$$= (0, 1) * P.T.$$

is waiting time
89

- 1) Systems 1 & 2 have transmitted their data for first time, collided and waited a random amount of time, then what is the probability that system 1 will retransmit before system 2.

$$\frac{W.T._1}{0 \text{ P.T.}} \quad \frac{W.T._2}{0 \text{ P.T.}} \Rightarrow \frac{1}{4} \text{ Ans}$$

} → 4 possibilities
required

* If ① * ② → Collision 2nd time
 $K=2$

$$W.T._1 = (0 \text{ to } 2^{K-1}) * P.T. \quad W.T._2 = (0 \text{ to } 2^{K-1}) * P.T.$$

$$= (0 \text{ to } 2^{2-1}) * P.T.$$

$$= (0, 1, 2, 3) * P.T. \quad W.T._2 = (0, 1, 2, 3) * P.T.$$

- 2) Systems 1 & 2 have transmitted their data for 2nd time, collided and waited a random amount of time then what is the probability that system 1 will retransmit before system 2.

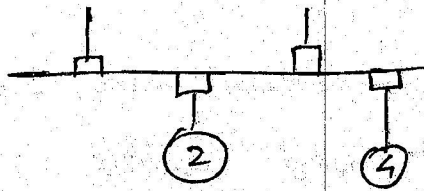
$$\begin{array}{c} W.T._1 \\ 3 \leftarrow 0 \\ 2 \leftarrow P.T. \\ 1 \leftarrow 2 P.T. \\ \quad 3 P.T. \end{array} \quad \begin{array}{c} W.T._2 \\ 0 \\ P.T. \\ 2 P.T. \\ 3 P.T. \end{array}$$

= 6

Total Possibilities = 16

$$\Rightarrow \frac{6}{16} \Rightarrow \frac{3+2+1}{16} \Rightarrow \frac{6}{16}$$

* As the K value increases, the chance of collision decreases. (The chance of data reaching safely will increase)



No of Stations	Stations ready	Collisions	Data reaching safely
100	50 50/100	30	20
100	50 50/100	10	40
100	100 100/100	50	50

Non-deterministic $\rightarrow G_L$

G_L (channel load) :-

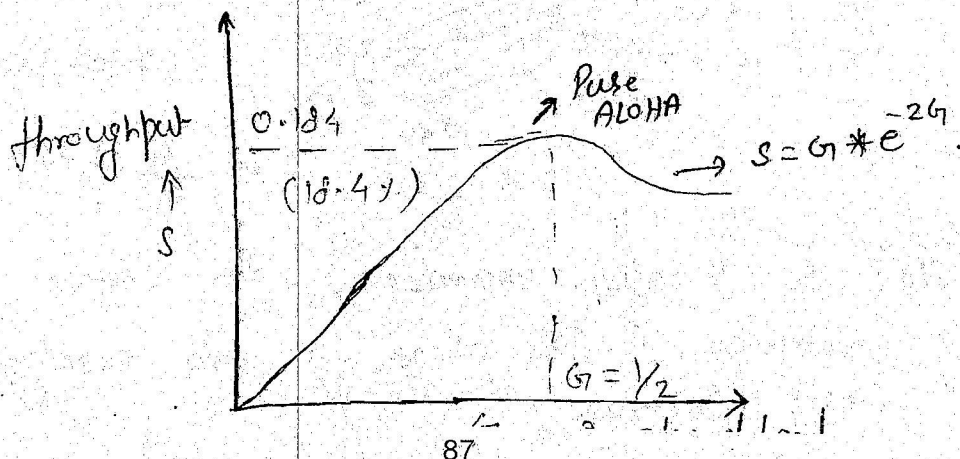
capacity ≤ 100 $\Rightarrow G_L = 50/100 = 1/2$ ($G_L < 1$) $\rightarrow$ under loaded

$\Rightarrow G_L = 100/100 = 1$ ($G_L = 1$) $\rightarrow$ critically Loaded

$\Rightarrow G_L = \frac{200}{100} = 2$ ($G_L > 1$) $\rightarrow$ overloaded

Throughput :-
in MAC sublayer

The Rate at which user transmits the data and the data should reach safely is known as throughput.



$$S = G * e$$

(51)

for $S_{max} \Rightarrow \frac{\partial S}{\partial G} = 0 \quad \leftarrow \text{for max value}$

$$G * (-2) * e^{-2G} + 1 * e^{-2G} = 0$$

$$e^{-2G} [-2G + 1] = 0$$

$$\Rightarrow G = \frac{1}{2}, \quad \underline{S_{max}}$$

$$\Rightarrow S = \frac{1}{2} * e^{-2 * \frac{1}{2}}$$

$$= \frac{1}{2e} = 0.184 \quad (18.4\%) \quad \leftarrow \underline{S_{max}} \text{ (throughput)}$$

Note:-

* out of 100 frames that are transmitted, maximum 'only 18.4% frames' will safely reach the destination in Pure ALOHA.

(1) B.W. = 50 Mbps
max throughput of pure ALOHA.

$\Rightarrow$ Pure ALOHA :- 18.4% of Bandwidth.

$$= \frac{18.4}{100} * 50 \text{ Mbps}$$

$$= 9.2 \text{ Mbps.}$$

(2) calculate the throughput of Pure ALOHA at $G = 1$

$$S = G * e^{-2G}$$

$$S = 1 * e^{-2}$$

$$= \frac{1}{e^2} = 0.135 = 13.5\%$$

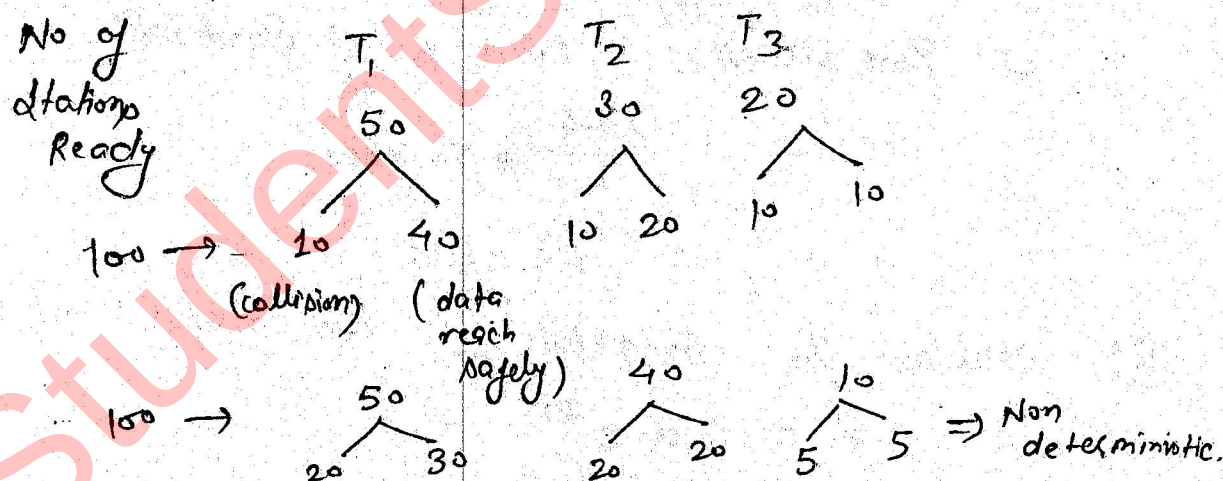
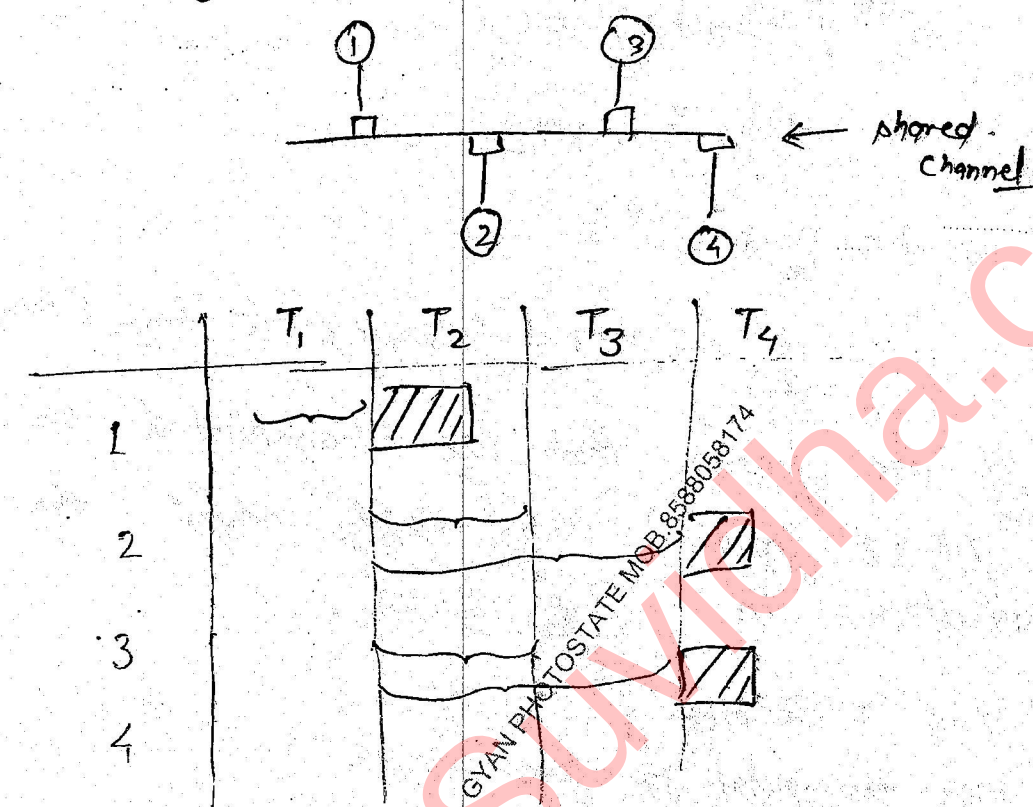
$\Rightarrow$ 13.5% of Bandwidth

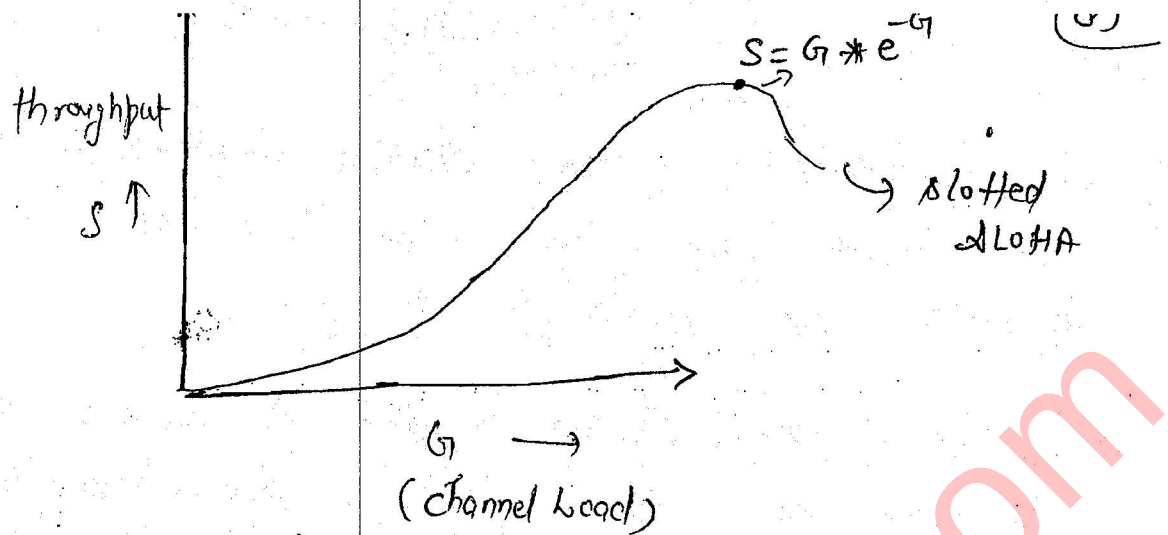
$$= \frac{13.5}{100} * 50 \text{ Mbps}$$

$$= \frac{13.5}{2} \text{ Mbps} = 6.75 \text{ Mbps.}$$

* In Slotted ALOHA the Total time is divided into time-slots

* Any system is ready with the data, it can start transmitting only at the starting of time slot.





$$S_{\max} = G * e^{-G}$$

$$S_{\max} \Rightarrow \frac{\partial S}{\partial G} = 0$$

$$G * (-1) * e^{-G} + 1 * e^{-G} = 0$$

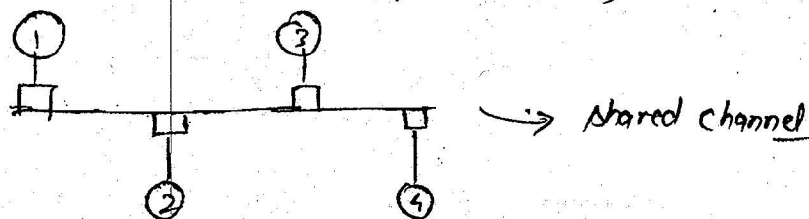
$$\Rightarrow e^{-G} (-G + 1) = 0$$

$$\Rightarrow G = 1$$

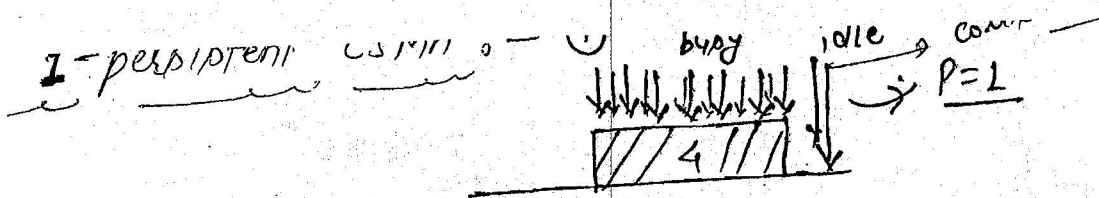
$$S_{\max} = 1 * e^{-1} = \frac{1}{e} = 0.368 = 36.8\%$$

* The Throughput of Slotted ALOHA is double that of Pure ALOHA that is out of 100 frames, maximum 36.8 frames will reach safely. Remaining all frames will suffer from collisions.

:- "CSMA" :- (Carrier sense multiple access)

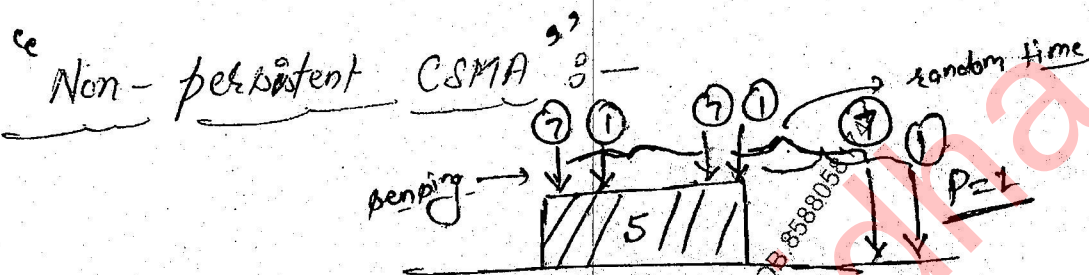


- * When the energy is low, channel is idle.
- * When the energy is moderate, channel is busy.
- * When the energy is High, then there is a collision in the Network.



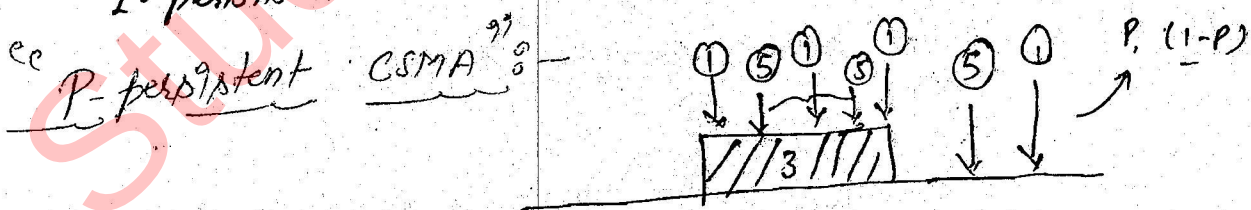
* In 1-persistent CSMA, stations continuously sense the channel, once the channel is idle, it will transmit with probability $P = 1$

* If two or more systems find the channel idle at the same time then there is a possibility of collision.



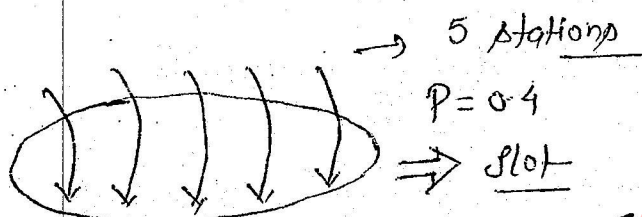
* In Non-persistent CSMA, once the channel is busy then the system will wait a random amount of time and again senses the channel.

* In this, finding the channel idle at the same time by different stations is minimum, so possibility of collision will be less compared to 1-persistent CSMA.



* In P-persistent CSMA, once the channel is idle it may transmit with probability 'P' or it may not transmit with probability '(1-P)'.

① there are five stations, probability of transmitting the data is 0.4. Only one station should transmit. then what is the probability that only one station will transmit in the given slot.



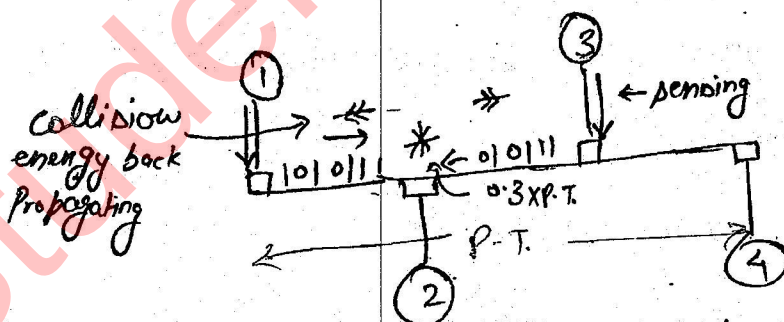
$$1 * (0.4)^1 * (1-0.4)^{5-1} + 1 * (0.4)^1 * (1-0.4)^{5-1} \dots 5 \text{ times}$$

$$= 5C_1 * (0.4)^1 * (1-0.4)^{5-1}$$

$$\Rightarrow nC_1 * p^1 * (1-p)^{n-1}$$

** CSMA/CD $\rightarrow$ wired LAN (Bus topology).
 $\rightarrow$ carrier sense multiple Access / collision detection.

Every station (two process) $\rightarrow$ one program is to transmit data
 $\rightarrow$ other program is to sense for collision.



Collision occurrence	collision detection
$0.3 * P.T.$	$0.6 * P.T.$

* when collision happens somewhere in the network, then the collision energy will retrieve back to the source, then collision can be detected.

* once collision detected station will stop transmitting the data and applies exponential back-off algorithm.

- The Range of collision occurrence is 0 - 2 P.T.
- * The Range of collision detection is 0 - 2 P.T.

* Note:-

- * If collision is detected at $< 2 P.T.$ or at $= 2 P.T.$ then station will stop transmitting then applies exponential back-off algorithm. (wrong statement)

- * If collision is not detected at $< 2 P.T.$ or at $= 2 P.T.$ then the station has captured the channel or get control over the channel, then station will start transmitting the original data.
- * The Maximum time to detect a collision is 2 P.T.
- * The minimum time to acquire (capture) the shared channel is 2 P.T.

① B.W. = 100 Mbps
 $l = 230 \text{ m}$
 $v = 2.3 \times 10^8 \text{ m/sec}$

calculate min frame size to acquire the channel in CSMA/CD or Ethernet?

$$T.T. = 2 * P.T.$$

$$P.T. = \frac{l}{v} = \frac{230}{2.3 \times 10^8} = 10^{-6} \text{ sec} = 1 \mu\text{sec}$$

$$T.T. = 2 \times 1 \mu\text{sec} = 2 \mu\text{sec}$$

$$\frac{\text{frame size}}{\text{B.W.}} = 2 \mu\text{sec}$$

$$\frac{\text{frame size}}{10^8} = 2 \times 10^{-6} \Rightarrow 200 \text{ bits} \leq \text{frame size}$$

(2) $B.W. = 10 \text{ Mbps}$
 $d = 280 \text{ m}$
 $v = 2.8 \times 10^8 \text{ m/sec.}$

calculate the max frame size to detect a collision in ethernet?

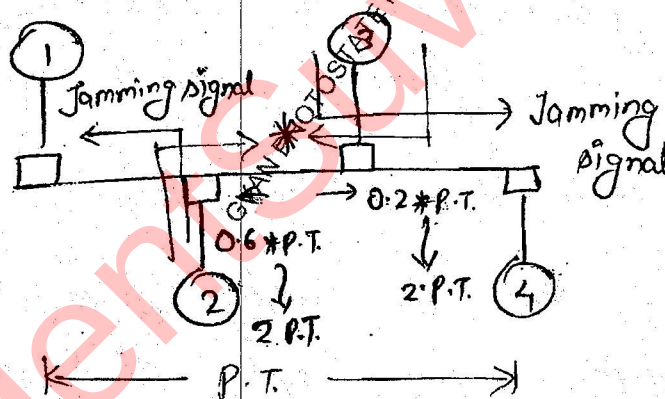
$T.T. = 2 P.T.$

$\Rightarrow$ To detect collision max time = $\frac{2 P.T.}{\text{frame size}}$

$\frac{\text{frame size}}{B.W.} = 2 \times \frac{d}{v}$

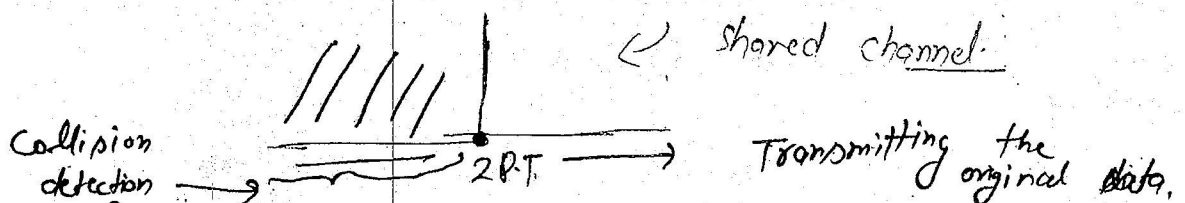
$\frac{\text{frame size}}{10^7} = 2 \times \frac{280}{2.8 \times 10^8}$

frame size = 20 bits



** Note:- when collision is detected at $< 2 P.T.$ then up to $2 P.T.$ 'Jamm signal' is transmitted then at $2 P.T.$ exponential back-off algorithm is applied.

* The purpose of jamm signal is to inform the unknown stations about the collision.



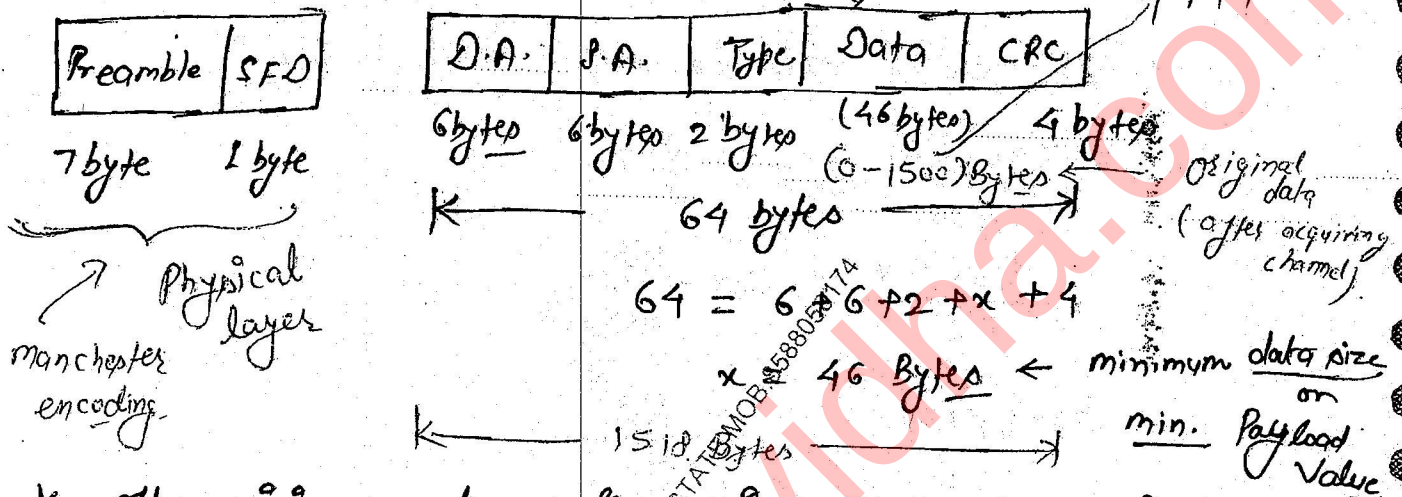
* In a shared channel only one system can transmit the data, that is after acquiring the channel.

IEEE 802.3 :-

(Bus Topology)

Logical

↳ Frame format :-



* The minimum frame-size in IEEE 802.3 is 64 Bytes to support CSMA/CD protocol.

* The minimum data in IEEE 802.3 is 46 Bytes.

* If the data, that is coming from Network layer is < 46 Bytes then upto 46 Bytes padding bits will be added.

* The maximum frame-size in IEEE 802.3 is 1518 Bytes or the maximum data in IEEE 802.3 is 1500 Bytes.

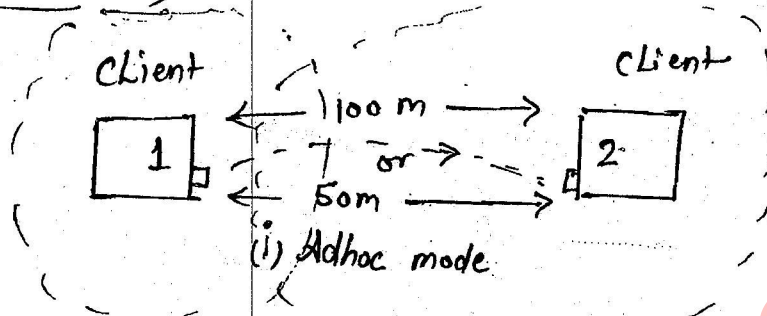
* This restriction is to give fair and equal chance to all systems in the Network.

Note 3:- CRC can detect the error easily when the data-size is small.
(CRC-32) standard

that the data is coming.

"Wireless Network LAN" :-

(IEEE 802.11)

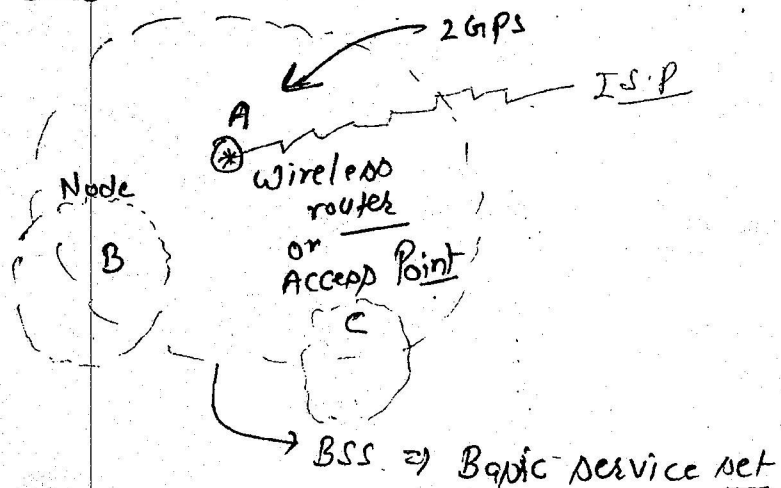


* The effect of Noise is more in wireless, compared to wired Network. So loss of data will be high in wireless compared to wired Network (LAN).

* A Node can transmit the data to the other node when they are in-range to each-other, this mode of transmission is called Adhoc mode transmission.

* In the wired Bus topology, all Nodes have same shared channel whereas in wireless LAN every Node has its own shared channel.

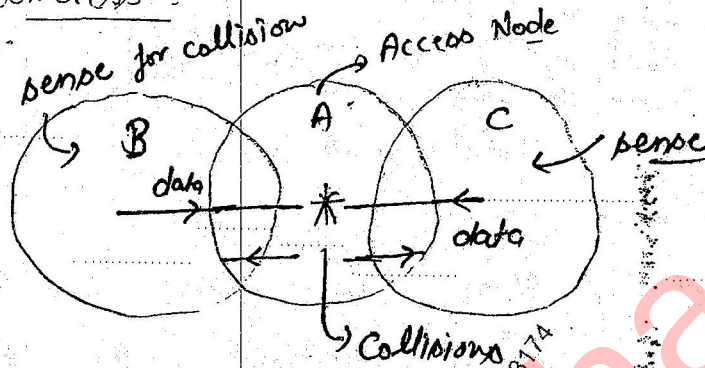
(ii) Infrastructure Mode :-



will be communicating to access Node for getting the Internet service.

* Nodes and the access Node combinedly is known as the Basic service set (BSS).

CSMA/CD in wireless :-



* Node B, A, C are in the plane region, when Node B is transmitting the data to A and parallelly, Node C is transmitting the data to A then there is a collision at Node A.

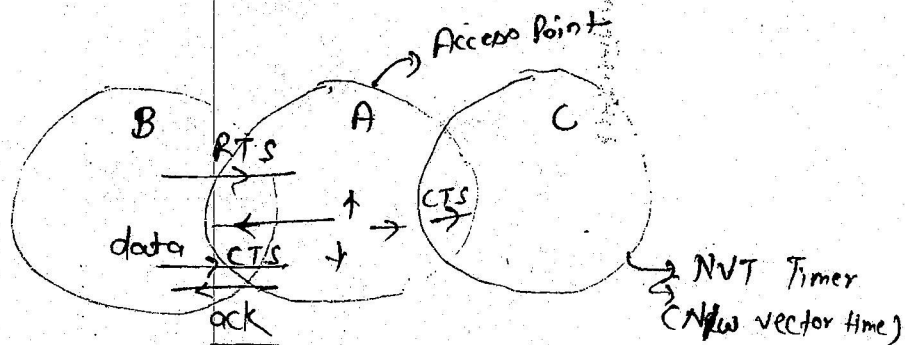
* This collision energy may not reach to node B & C so collisions can not be detected, because for Node B, Node C is hidden and for Node C Node B is hidden.

So CSMA/CD can not be applied, because 'Hidden Node' problem.

CSMA/CA :- carrier sense multiple access / collision avoidance

RTS :- Request to send

CTS :- clear to send



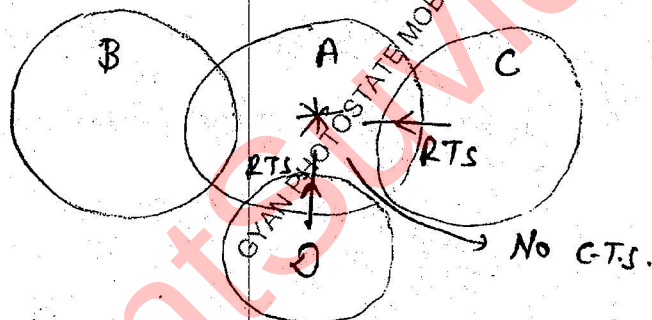
CSMA/CA by allowing one station to transmit the data.

* CSMA/CA applies 4-way Handshaking for transmitting the data.

* When Node B transmits RTS to Node A then, Node A will reply with C.T.S.

* So parallelly Node B will transmit the data and Node C will start NVT Timer.

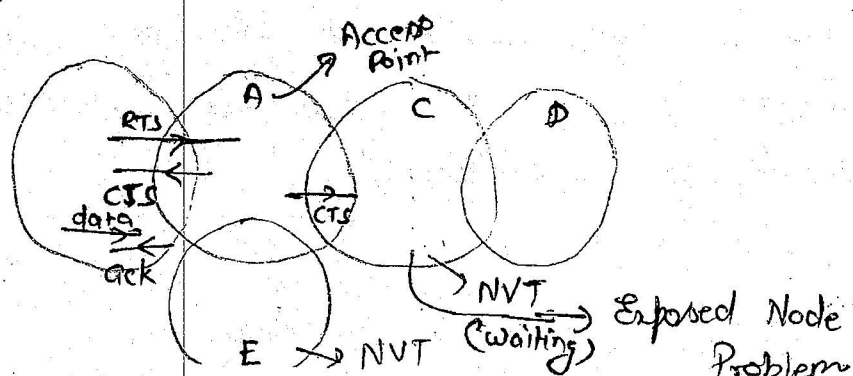
* By the time transmission of Node B is completed, NVT Timer of Node C will expire.



* When Node C & D send RTS at the same time then there is a collision, at Node A.

* Not getting the C.T.S. is a confirmation that there is a collision. Then Nodes C & D will apply exponential back-off algorithm.

Exposed Node Problem in CSMA/CA :-



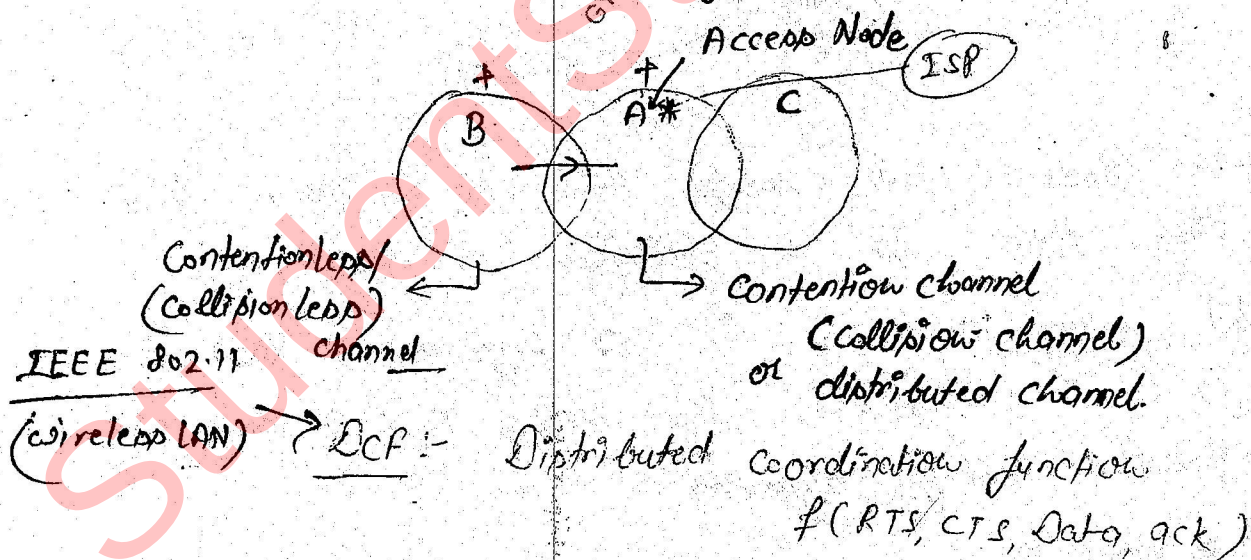
★ At the cost of Solving, the hidden Node problem using CSMA/CA, then an Exposed Node problem will occur that is in the above diagram:

→ Even 'D' is visible to 'C' at that time C can't transmit the data to 'D' this problem is known as Exposed Node problem.

Note -

★ In CSMA/CD there is No separate acknowledgement but collision detection itself will act as an ack. whereas in CSMA/CA, there is a separate acknowledgement.

★ More Number of retransmissions in CSMA/CA, whereas Less Number of retransmissions in CSMA/CD.



★ When a Node wants to transmit the data to the Access Node, it uses "DCF" function that is the channel is distributed.

PCF - Point Coordination Function

$f(\text{Data}, \text{ack})$

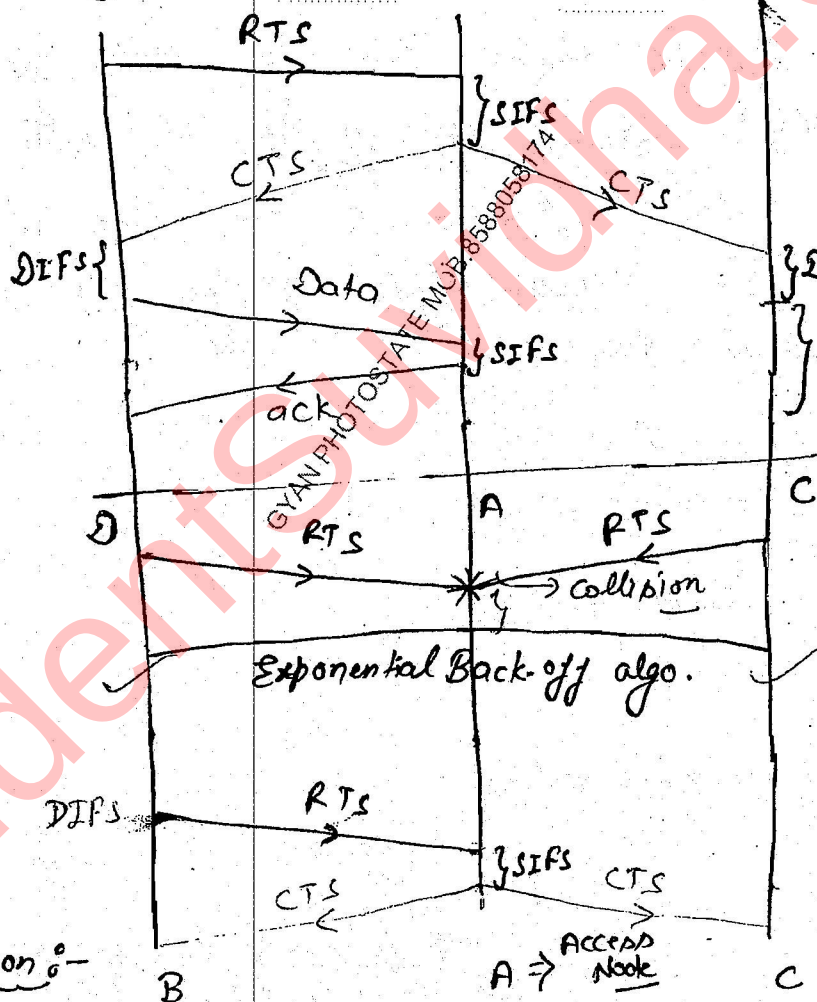
↑ Contentionless or collisionless channel.

★ When a Node wants to transmit the data to the Access Node, It will use "PCF" function.
 { It will be a contentionless channel. }

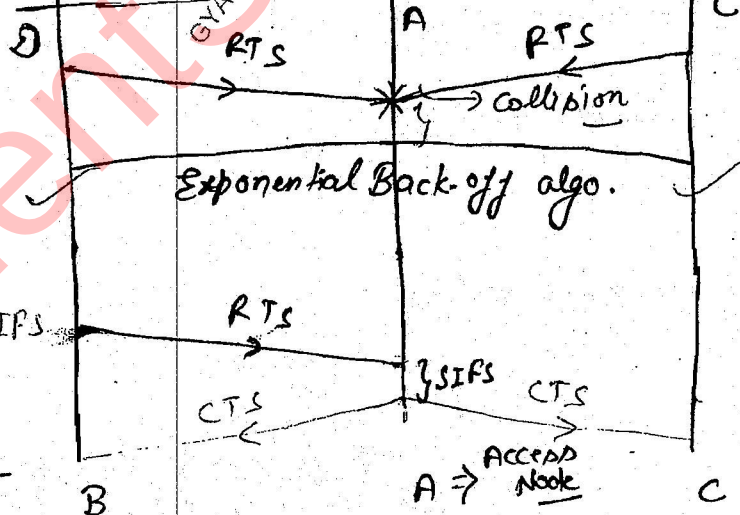
DCF Function

Timing diagram:-

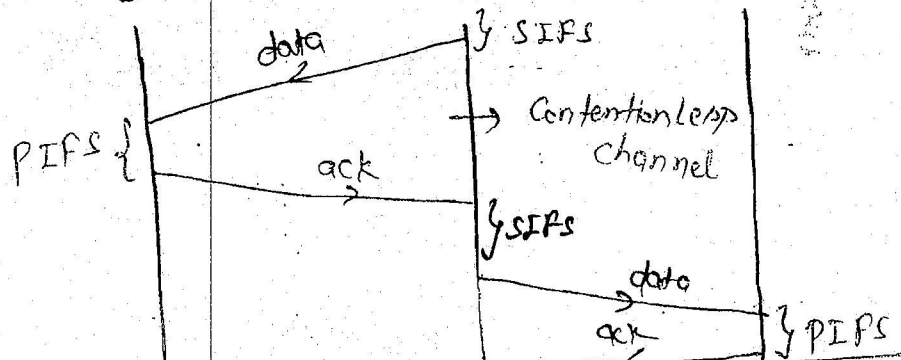
Case(i):-



Case(ii):-



PCF function:-



IFS ⇒

Inter frame space

DIFS:-

Distributed IFS

PIFS Point IFS

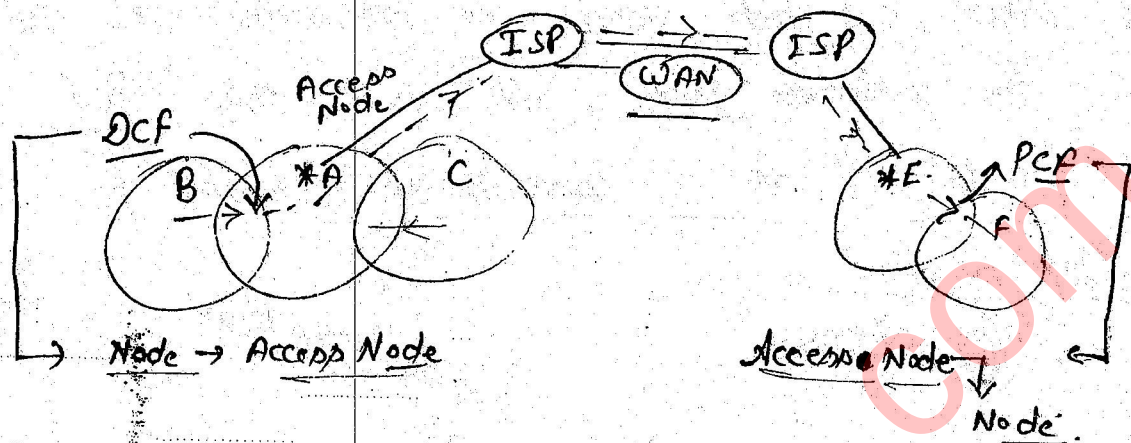
SIFS:-

NVT Short IFS
 timer waiting expires

* PCF is having high priority compared to NCF.

$$\therefore \underline{PIFS} < \underline{DIFS}$$

* In IEEE 802.11 total 4 addresses are used

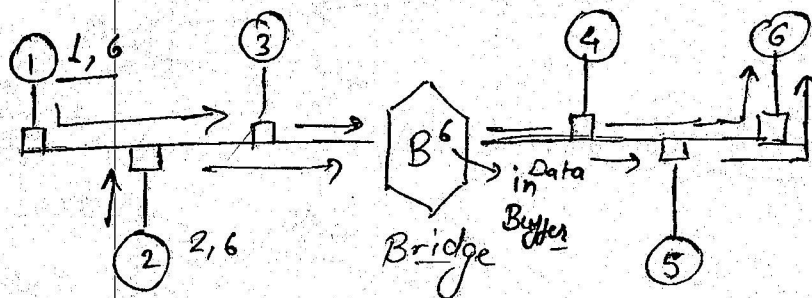


“Polling” :-

Access Node has to elect one of the Node from the group to transmit the data using PCF function. The time that is spent by the Access Node during that election is called polling time.

* “Networking Devices” :-

- 1) Repeater
 - 2) Hub
 - 3) Bridge
 - 4) Router
 - 5) Gateway
- “Bridge” :-



Bridge :- Bridge is a LAN device and its operation is based on MAC address.

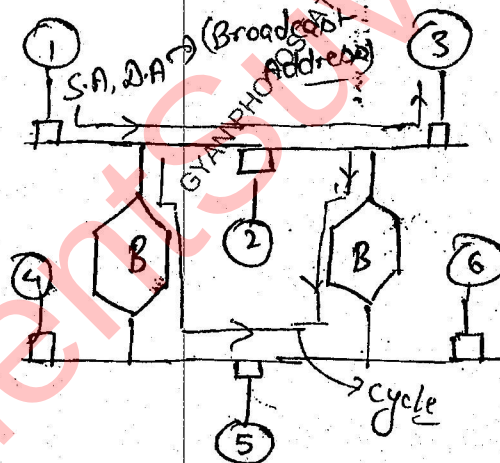
Bridge is used to connect 'similar' LAN Networks.

* Initially the bridge table of the bridge is empty.

* once bridge knows the complete information of the Network then Bridge is treated as converge and stable.

* The functionalities of a Bridge are :-
'Blocking', 'Learning' & 'forwarding'.

* once Bridge knows the complete information then only Blocking & forwarding will be there.

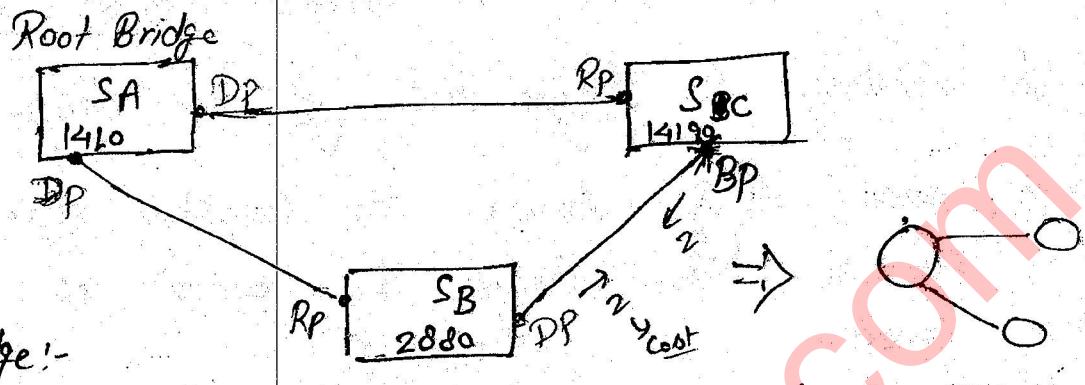


* We connect more than one Bridge b/w two LAN N/w to support fault tolerance i.e. If suddenly one Bridge fails then the data can be diverted via other paths.

* Whenever we connect more than one Bridge between the similar LAN Networks then there is a possibility of cycles or loop problems between the Bridges.

tree protocol' then cycles can be eliminated.

Spanning Tree Protocol :-



Root Bridge:-

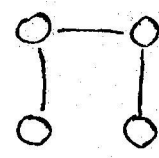
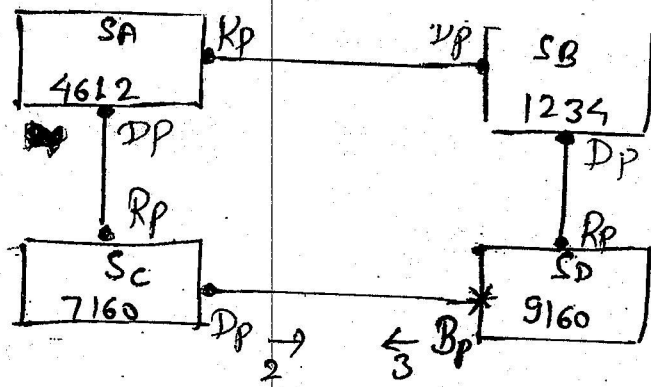
* The Bridge which is having the least MAC address is known as the Root Bridge.

(ii) Root port :- Root port is a port which is having (identifying) least cost path from Non-root Bridge to Root Bridge. These ports are for sending data). (Rp).

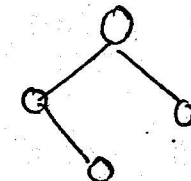
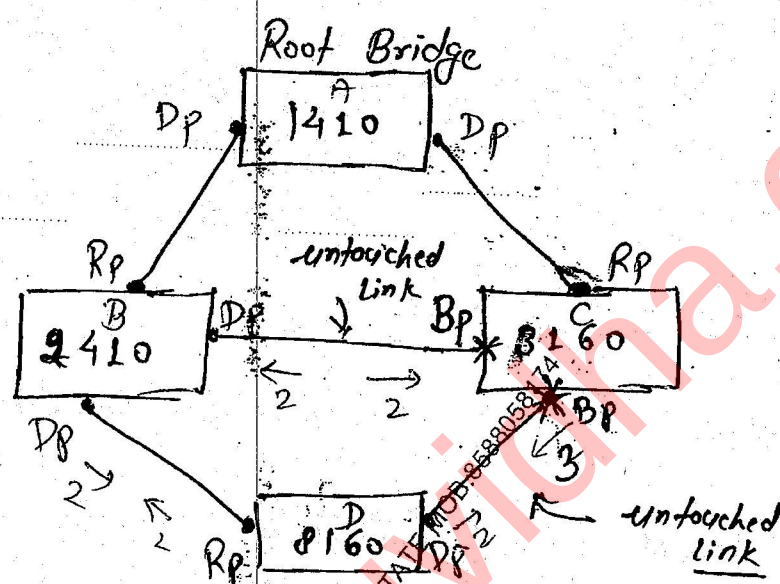
(iii) Designated port :- Designated port is a port which is having least cost path from Root Bridge to Non-Root Bridge. (DP) (These ports are for sending configuration files).

(iv) Blocked Port :- Block port is a port, which is having highest cost path from Non-Root Bridge to Root Bridge. If two Non-Root Bridges having the same cost path, then by comparing their MAC addresses, we identify the Block-port, which on the side of highest MAC Address Bridge. Opposite to Bp is Dp (Designation Address).

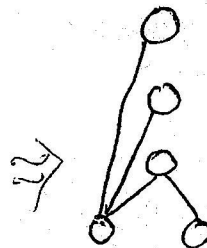
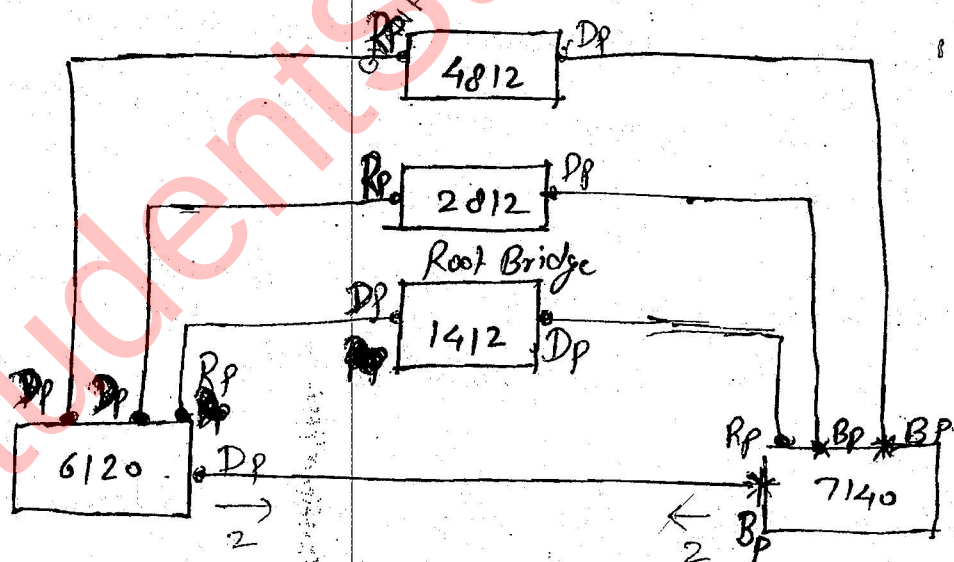
(2)



(3)

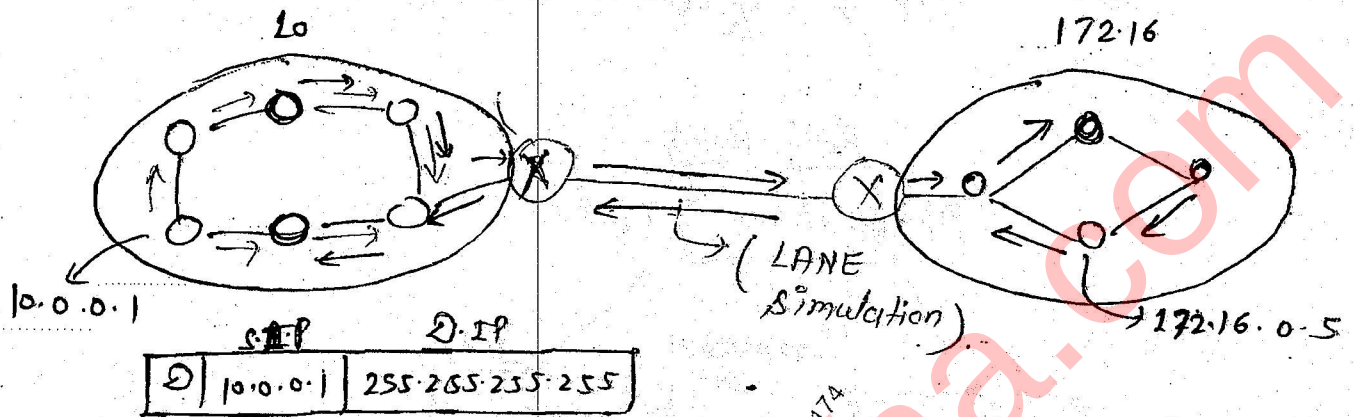


(4)



* Router :- Router is a device which operation is based on IP address."

"Router is used for connecting different classes of Networks (dissimilar Networks)."



"By default Router is a broadcast domain separator."

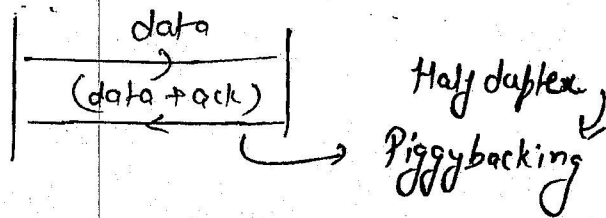
* By default Router is a collision domain separator.

* By default Router is not a multi-protocol converter, but gateway is a multi-protocol converter because the gateway can convert one model of packet into another model.

Note :- window size is the logical quantity or parameter in the flow control policies.

Piggybacking :- sending data along with acknowledgement is known as Piggybacking.

* The advantage of Piggybacking is effective channel utilization.



Dated
15/06/2014

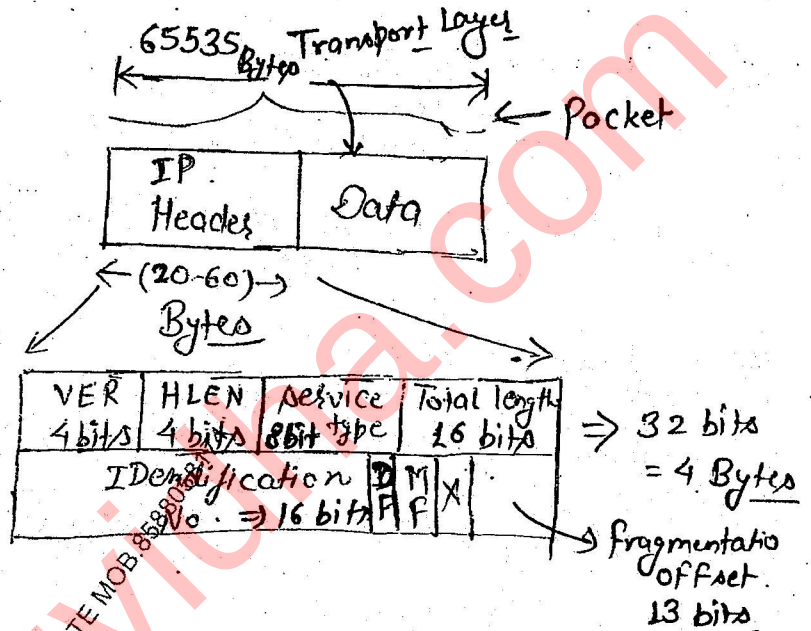
Network Layer

⇒ IP Protocol

'version':-

0100 ⇒ IPv4

0110 ⇒ IPv6



* The starting 4 bits of the IP packet decides whether the packet is IPv4 or IPv6.

* other than these two possibilities, if the packet come to the router the packet will be discarded.

0000 }
 0001 } X (Don't care)
 0010 }
 0011 }
 0100 } ⇒ 4 rows * 4 = 16 Bytes
 0101 } ⇒ 5 rows * 4 = 20 Bytes
 0110 } ⇒ 6 rows

(20-60) Bytes ← Range

1111 } 15 rows ⇒ 15 * 4 Bytes = 60 Bytes

(1) HLEN = 1010

Size of Header = 10 * 4 = 40 Bytes ← Header size