Name : G. Nithish
Regno: 19BCS0012
Course : Computer Networks

Test - 2

(1)

Define CSMA:

* CSMA (Carrier Sense Multiple Access) is a network protocol for carrier-transmission that operates in the medium Access Control (MAC) layer.

* It senses or listens whether the shared channel for transmission is busy or not, and transmits if the channel is not busy. Using CMSP protocols, more than one users or nodes send and receive data through a shared medium that may be single cable or optical fiber connecting multiple nodes or a portion of wireless spectrum.

Working Principle :-

↳ When a station has frames to transmit, it attempts to detect Presence of the carrier signal from the other nods connected to the shared Channel.

↳ If a carrier signal is detected it implies that a transmission is in Progress..

↳ the station waits till the ongoing transmission executes to completion and then initiates its own transmission

↳ Generally transmission by the node are received by all other nodes connected to the Channel.

Algorith for CSMA:

Algorith for CSMA are:

- Non Persistant
- 1- Persistant.
- 2 - Persistant

Explaration:

Non Persistant:

If channel is not free then wait for random amount of time then sense the channel, if Free then send data.

1. Transmit if medium is idle
   Otherwise go to 2
2. wait for random amount of time and repeat (1) if medium is busy.

1- Persistant

Continuously sense the channel and when it sees that the channel is

free, it transmit the data.

1:- If medium is idle transmit, otherwise go to 2.

2:- Wait for random amount of time and repeat (1) if medium is busy.

2- Persistant CSMA:

1:- With Probability "P", the station sends its frame.

2:- With Probability 1-P, station waits for the beginning of the next time slot and check the line again.

(i) If lines is idle go to 1

(ii) If line is busy, it acts as Collision has occurred and uses the backoff algorithm.

2) IPV4 Address of class A:-

→ IPV4 address are 32 bit numbers that are typically displayed in dotted decimal notation.

→ A 32 bit address contain 2 Primary Parts

i) Network Prefix.
ii) the host number.

* IPV4 Addressing System is divided into 5 classes of IP Address. All the 5 classes are identified by the 1st Octet of IP Address.

1st octet 2nd octet 3rd octet 4th octet

11000000 . 10101000 . 00000001 . 10011000

192 . 168 . 1 . 152

No. of networks & the no. of host Ports class can be derived by this formula

No. of networks = $2^{network\_bits}$

No. of Hosts/network = $2^{host\_bits} - 2$

When calculating hosts IP address, 2 IP address are decreased because they can't be assigned to hosts, i.e the first IP of a network no. of and the last IP is reserved for Broad cast IP.

Class A Address.

The first bit of the first octet is always set to 0 (zero). Thus First octet ranges from 1-127 i.e.

00000001 - 01111111

1 - 127

Class A addresses only include IP Starting from 1.x.x.x to 126.x.x.x. only. The IP rang 127.x.x.x is reserved for loopback IP address.

Class A addres only indicates IP starting from 1.x.x.x to 126..

the default subnet mask for class A IP Address is 255.0.0.0 which implies that class A addressing can have 126 network ($2^7 - 2$) and 16777214 host ($2^{24} - 2$).

Class A IP addres formatis

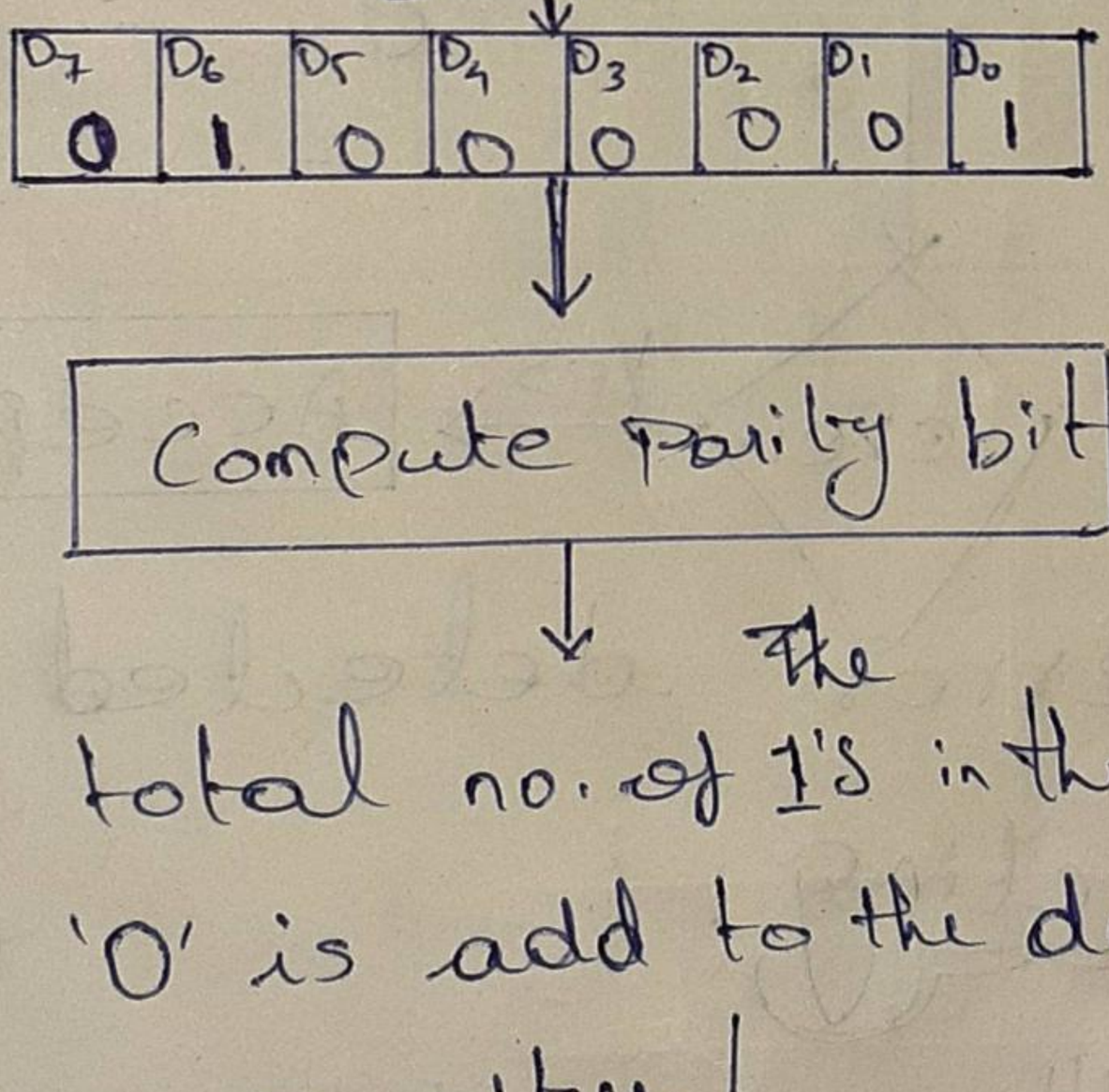
0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

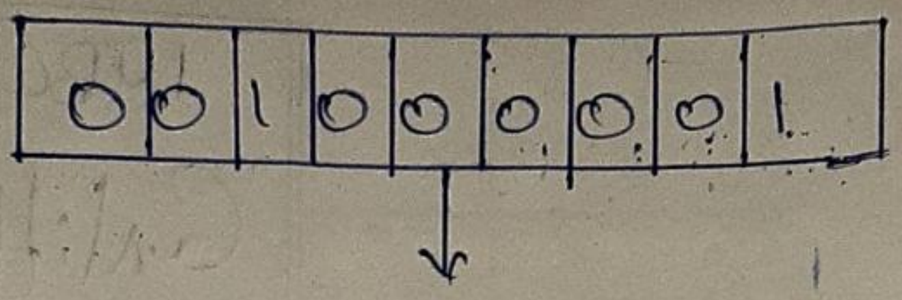
8. The ASCII Value for A is 65 Convert this ASCII value to binary and store them as 8 bit data.

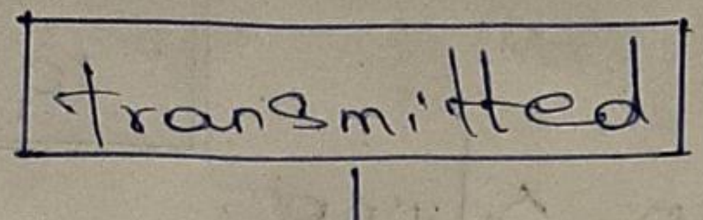
Answer:-

The ASCII value for 'A' is '65'

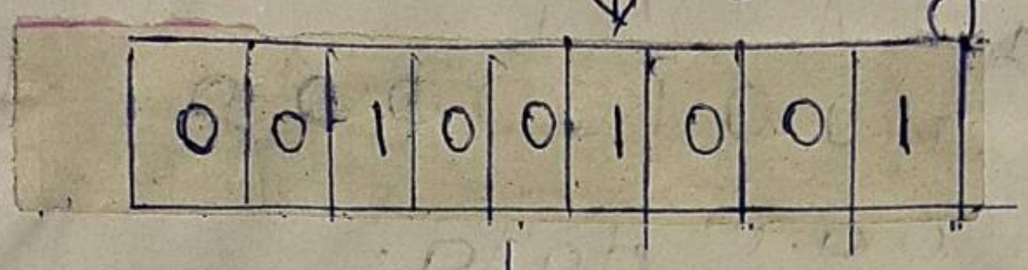
The Binary value for '65' = 11000001

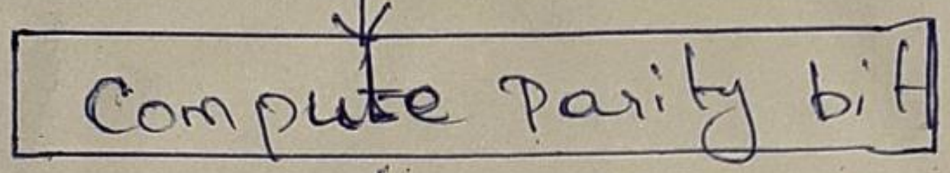






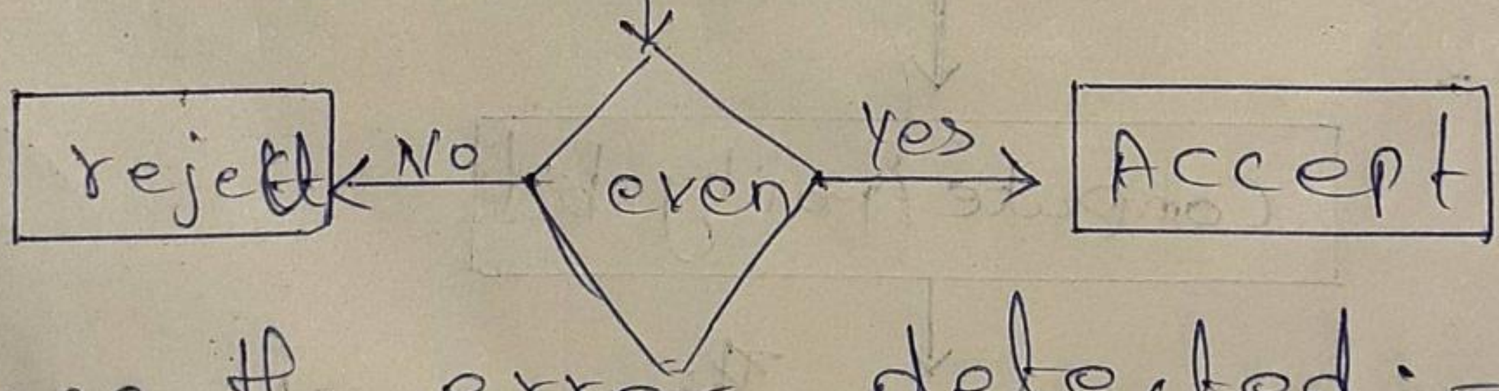
By wrongly the 'D3' location bit is Changed to '1'





So the "error is detect" Becaus of inappropriate Parity Bit".

Now the no. of bit's '1' is 3 bit is odd but it has even Parity



Hence the error detected :-

Error - Correcting :

* Along with error-detecting code, we can also pass some data to figure out the original message.

from the corrupt message that we received.

* In error-correcting, Parity Check has a simple way to detect errors along with a sophisticated mechanism to determin the corrupt bit location.

* Once the corrupt bit is located. its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

→ By the use of error-correcting code it detect the exact location of the corrupt bits here as "D_3"

Chaang it '1' to '0'