PART-1

Medium Access Sub Layer – Channel Allocations.

CONCEPT OUTLINE

- Two different schemes used for channel allocation are :
  i. Static channel allocation
  ii. Dynamic channel allocation
- Types of CSMA are :
  i. Non-persistent CSMA
  ii. 1-persistent CSMA
  iii. P-persistent CSMA

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.1. Explain medium access control sublayer.

Answer

1. The MAC sublayer is very important in LANs because it is a broadcast network. Fig. 2.1.1, show the position of MAC sublayer.

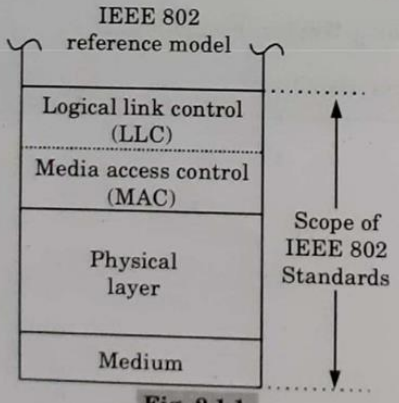


Fig. 2.1.1.

2. It is called as IEEE 802 reference model.

Functions of Media Access Control (MAC) sublayer :

1. To perform the control of access to media.
2. It performs the unique addressing to stations directly connected to LAN.

3. Detection of errors.

Functions of Logical

1. Error recovery.
2. It performs the flow
3. User addressing.

Que 2.2. Explain ch
schemes used for cha

Answer

1. In a broadcast netw allocated to one tran to this medium shoul
2. There are two differ
   - **a. Static channel**
     - i. The traditio users is by
     - ii. In these me slot is allott bandwidth
     - iii. The Frequen Multiplexing
   - **b. Dynamic chan**
     - i. In this meth allotted to th their require
     - ii. Following as this method :
       1. **Station** stations frames f
       2. **Single** commun
       3. **Collisio** two or m resulting
       4. **Continu** used to d can begi For a slo slots.

3. Detection of errors.

Functions of Logical Link Control (LLC) sublayer :

1. Error recovery.
2. It performs the flow control operations.
3. User addressing.

Que 2.2. Explain channel allocation. What are the two different schemes used for channel allocation ?

Answer

1. In a broadcast network, the single communication channel is to be allocated to one transmitting user at a time. The other users connected to this medium should wait. This is called as channel allocation.
2. There are two different schemes used for channel allocation :

a. Static channel allocation :

i. The traditional way of allocating a single channel, among many users is by means of Frequency Division Multiplexing (FDM).

ii. In these methods either a fixed frequency band or a fixed time slot is allotted to each user. Thus either the entire available bandwidth or entire time is shared.

iii. The Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) are the example of static channel allocation.

b. Dynamic channel allocation :

i. In this method neither a fixed frequency nor fixed time is allotted to the user. The user can use the single channel as per their requirements.

ii. Following assumptions are made for the implementation of this method :

1. **Station model :** This model consists of N independent stations such as a PC, computer etc. which can generate frames for transmission.
2. **Single channel :** A single channel is available for all communication.
3. **Collision :** If frames are transmitted at the same time by two or more stations, there is an overlap in time and the resulting signal is disconnected. This is called as collision.
4. **Continuous or slotted time :** There is no master clock used to divide time into discrete time intervals. So, frames can begin at any random instant. This is continuous time. For a slotted time, the time is divided into discrete time slots.

5. **Carrier or no carrier sense :** Stations sense the channel before transmission or they directly transmit without sensing the channel.

Que 2.3. **Write a short note on random access.**

Answer

1. In the random access technique, there is no control station.
2. Each station will have the right to use the common medium without any control over it.
3. With increase in number of stations, there is an increased probability of collision or access conflict.
4. The collisions will occur when more than one user tries to access the common medium simultaneously.
5. As a result of such collisions some frames can be either modified (due to errors) or destroyed.
6. In order to avoid collisions, we have to set up a procedure like CSMA/CD and CSMA/CA.

Que 2.4. **Explain Carrier Sense Multiple Access (CSMA) protocol.**

OR

Discuss different carrier sense protocols. How are they different than collision protocols ? **AKTU 2014-15, Marks 05**

AKTU 2017-18, Marks 10

Answer

The CSMA protocol operates on the principle of carrier sensing. In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

Different carrier sense protocols are :

1. **CSMA/CA :**
   a. Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a network contention protocol used for carrier transmission in networks using the 802.11 standard.
   b. CSMA/CA works to avoid collisions prior to their occurrence.
2. **CSMA/CD :**
   a. Carrier Sense Multiple Access / Collision Detection is a set of rules which determine how network devices respond when two devices attempt to use a data channel simultaneously.
   b. CSMA/CD protocol works to handles transmissions only after a collision has taken place.

CSMA is different from collisio
for the channel without any
performance.

Que 2.5. **Explain the con**

Answer

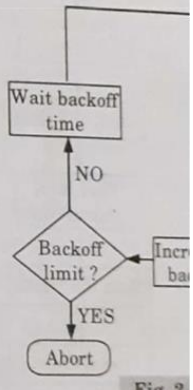


Fig. 2.

Explanation :

1. The station having read
2. Then it senses the line u
3. It then sends the frame, i to one complete frame, t
4. Otherwise (in the event inform the other station
5. The station then increm backoff time and sends t
6. If the backoff has rea transmission.
7. CSMA/CD is used for th

Que 2.6. **Discribe CSM**

Write a short note on coll

CSMA is different from collision free protocol as it resolves the contention for the channel without any collision and does not affect the system performance.

Que 2.5. Explain the concept of CSMA/CD.

Answer

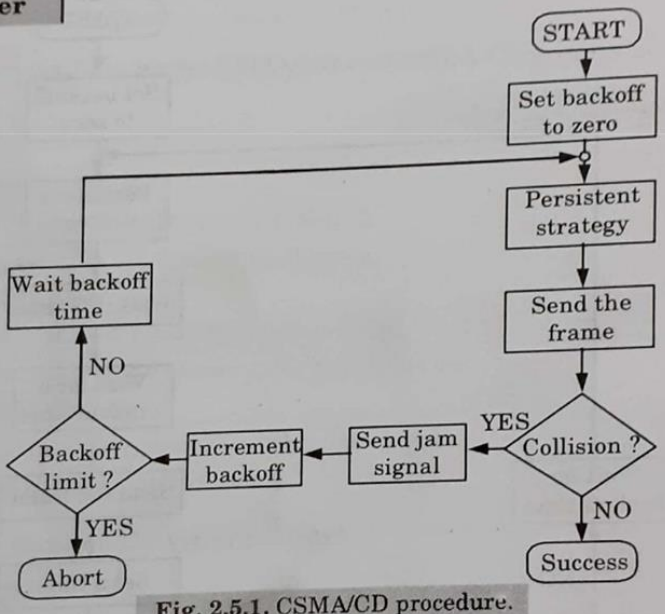


Fig. 2.5.1. CSMA/CD procedure.

Explanation :

1. The station having ready frame sets the backoff parameter to zero.
2. Then it senses the line using one of the persistent strategies.
3. It then sends the frame, if there is no collision for a period corresponding to one complete frame, then the transmission is successful.
4. Otherwise (in the event of collision) the station sends the jam signal to inform the other stations about the collision.
5. The station then increments the backoff time and waits for a random backoff time and sends the frame again.
6. If the backoff has reached its limit then the station aborts the transmission.
7. CSMA/CD is used for the traditional Ethernet.

Que 2.6. Discribe CSMA / CA in brief.

OR

Write a short note on collision avoidance.

AKTU 2014-15, Marks 2.5

Answer

1. The long form of CSMA / CA is CSMA protocol with collision avoidance. Fig. 2.6.1 shows the flow chart explaining the principle of CSMA / CA.

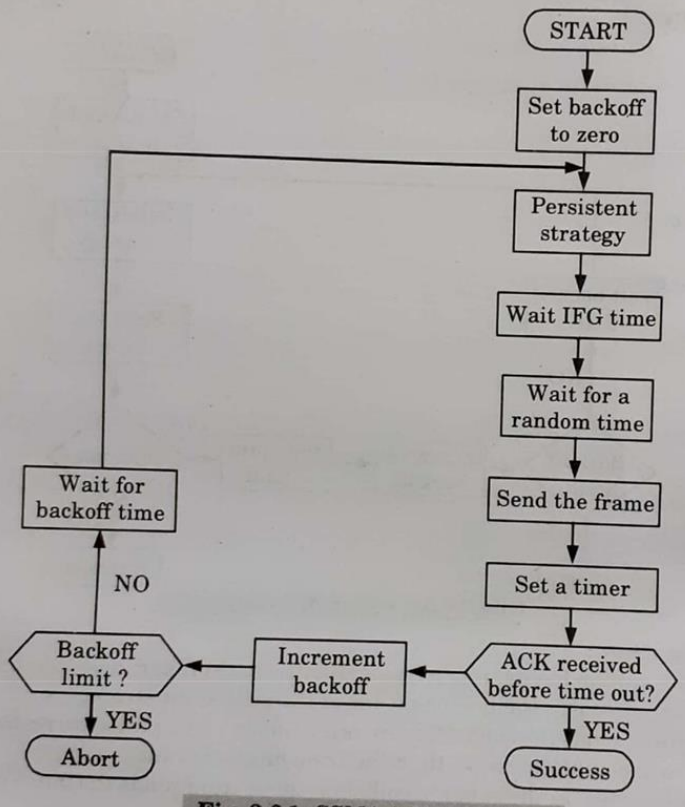


Fig. 2.6.1. CSMA / CA procedure.

2. The station ready to transmit, senses the line by using one of the persistent strategies.
3. As soon as it finds the line to be idle, the station waits for a time equal to an Interframe Gap (IFG).
4. It then waits for some more random time and sends the frame.
5. After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.

6. If the acknowledgem transmission is succe
7. But if the transmi acknowledgement bef parameter, waits fo CSMA / CA completel

Que 2.7. **Explain abo**

Answer

CSMA/CD : Refer Q. 2.5, P

CSMA/CA : Refer Q. 2.6, P

Uses of CSMA/CD :

1. CSMA/CD is used for t
2. It uses MAC protocol t

Uses of CSMA/CA :

1. It is used to avoid collis
2. It is used in channel uti

Que 2.8. **Explain the t**

Answer

Types of CSMA :

a. **Non-persistent CSMA**
   1. In this scheme, if a that the channel is b will wait for fixed ir
   2. After this time, it a channel is free it wi

b. **1-persistent CSMA :** In continuously monitors t immediately.

c. **P-persistent CSMA :**
   1. The possibility of suc the p-persistent CSM
   2. In this scheme, all th simultaneously as so

6. If the acknowledgement is received before expiry of the time, then the transmission is successful.
7. But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the backoff parameter, waits for the backoff time and senses the line again, CSMA / CA completely avoids the collision.

Que 2.7. Explain about CSMA/CD and CSMA/CA and its uses.

AKTU 2013-14, Marks 05

Answer

CSMA/CD : Refer Q. 2.5, Page 2–5A, Unit-2.

CSMA/CA : Refer Q. 2.6, Page 2–5A, Unit-2.

Uses of CSMA/CD :

1. CSMA/CD is used for traditional Ethernet.
2. It uses MAC protocol to encounter data collision.

Uses of CSMA/CA :

1. It is used to avoid collision between data frames.
2. It is used in channel utilization.

Que 2.8. Explain the types of CSMA.

Answer

Types of CSMA :

a. Non-persistent CSMA :

1. In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
2. After this time, it again checks the status of the channel and if the channel is free it will transmit.

b. 1-persistent CSMA : In this scheme the station which wants to transmit, continuously monitors the channel until it is idle and then transmits immediately.

c. P-persistent CSMA :

1. The possibility of such collisions and retransmissions is reduced in the p-persistent CSMA.
2. In this scheme, all the waiting stations are not allowed to transmit simultaneously as soon as the channel becomes idle.

PART-2

LAN Protocols – ALOHA Protocols.

CONCEPT OUTLINE

- ALOHA system has two versions :
  i. **Pure ALOHA :** It does not require global time synchronization
  ii. **Slotted ALOHA :** It require time synchronization.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.9. Write a short note on pure ALOHA.

Answer

1. In pure ALOHA, the stations transmit frames whenever they have data to send.
2. When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
3. In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
4. If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
5. If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.
6. Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help to avoid more collisions.

Assumption for analysis :

1. All frames are of the same size/length to maximize the output.
2. Packet transmission time is the unit time.
3. The number of packets successfully transmitted per unit time is 'S'.
4. Load for channel offered is 'G' for transmission, which is Poisson's distribution (arrival).
   a. If $S < G$ then at high load, there will be frames from most of the users and hence many collisions.

b. If $G < S$ then at low load, there will be few or no collision, hence fewer retransmissions.

c. If $S > 1$, then the number of frames generated are more than the channels can handle, and every time probability of collision is 1.

d. If $G \approx S$, throughput is just the offered load, G times the probability of transmission being successful *i.e.*, $S = GP_0$

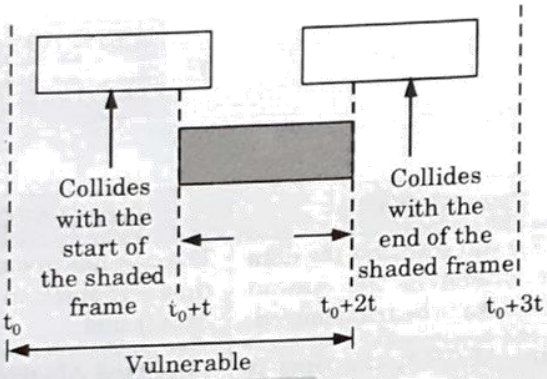


Fig. 2.9.1.

where P_0 is the probability, when the frames do not suffer from collision.

Que 2.10. Discuss slotted ALOHA.

Answer

1. It follows a synchronous transmission system, with time divided into slots.
2. Each slot size is equal to a fixed packet transmission time.
3. When the packet is ready for transmission, it needs to wait until the previous slot is over.
4. It uses the common clock at each station and satellite.
5. Fig. 2.10.1 shows packets completely or without any overlap.

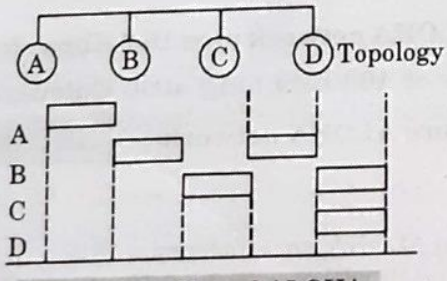


Fig. 2.10.1. Slotted ALOHA.

Performance of slotted ALOHA :

$S = G \times$ probability of no other transmission/overlap/arrival in previous slot

$\therefore S = Ge^{-G}$

Its peak at $G = 1$ with a throughput 0.368 (twice that of pure ALOHA). Operation at higher G reduces the number of empty slots but increases collision.

Que 2.11. How can you compare pure ALOHA and slotted ALOHA ?

AKTU 2013-14, Marks 05

AKTU 2014-15, Marks 2.5

Answer

S. No.	Pure ALOHA	Slotted ALOHA
1.	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
2.	In pure ALOHA, the time is continuous.	In slotted ALOHA, the time is discrete.
3.	The time is not globally synchronized.	The time is globally synchronized.

Que 2.12. A pure ALOHA network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all station together) produces 250 frames per second ?

AKTU 2014-15, Marks 2.5

Answer

If the system creates 250 frames per second, that is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$

This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Que 2.13. An ALOHA network uses 19.2 Kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network. **AKTU 2015-16, Marks 05**

Answer

The network is pure ALOHA, so, efficiency = 18 %

Usable bandwidth for 19.2 Kbps = $19.2 \times 0.18 = 3.456$ Kbps

Therefore, the maximum throughput of pure ALOHA

$$= \frac{1}{2e} \times 3.456 = \frac{18.4 \times 3.456}{100} = 0.635\ \%$$

PART-3

Overview of IEEE Standard – FDDI.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.14. Explain the IEEE 802.3 MAC sublayer frame format.

Answer

IEEE 802.3 specifies one type of frame containing seven fields : preamble, SFD, DA, SA, length/type of PDU, 802.2 frame and the CRC. The format of the MAC frame in CSMA/CD is shown in Fig. 2.14.1.

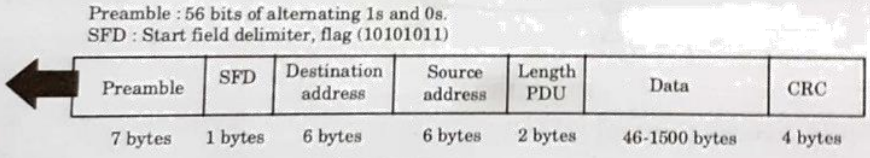


Fig. 2.14.1.

1. **Preamble :** The first field of the 802.3 frame, the preamble, contains seven bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enable it to synchronize its input timing.
2. **Start Frame Delimiter (SFD) :** The second field (one byte : 10101011) of the 802.3 frame signals at the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.
3. **Destination Address (DA) :** The Destination Address (DA) field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its Network Interface Card (NIC).
4. **Source Address (SA) :** The source address (SA) field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.

Performance of slotted ALOHA :

$S = G \times$ probability of no other transmission/overlap/arrival in previous slot

$\therefore S = Ge^{-G}$

Its peak at $G = 1$ with a throughput 0.368 (twice that of pure ALOHA). Operation at higher G reduces the number of empty slots but increases collision.

Que 2.11. **How can you compare pure ALOHA and slotted ALOHA ?**

AKTU 2013-14, Marks 05

AKTU 2014-15, Marks 2.5

Answer

S. No.	Pure ALOHA	Slotted ALOHA
1.	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
2.	In pure ALOHA, the time is continuous.	In slotted ALOHA, the time is discrete.
3.	The time is not globally synchronized.	The time is globally synchronized.

Que 2.12. **A pure ALOHA network transmits 200 bit frames on shared channel of 200 kbps. What is the throughput if the system (all station together) produces 250 frames per second ?**

AKTU 2014-15, Marks 2.5

Answer

If the system creates 250 frames per second, that is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$

This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

Que 2.13. **An ALOHA network uses 19.2 Kbps channel for sending message packets of 100 bits long size. Calculate the maximum throughput for pure ALOHA network.** **AKTU 2015-16, Marks 05**

Answer

The network is pure ALOHA, so, efficiency = 18 %

Usable bandwidth for 19.2 Kbps = $19.2 \times 0.18 = 3.456$ Kbps

Therefore, the maximum throughput of pure ALOHA

$$= \frac{1}{2e} \times 3.456 = \frac{18.4 \times 3.456}{100} = 0.635\ \%$$

PART-3

Overview of IEEE Standard – FDDI.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.14. Explain the IEEE 802.3 MAC sublayer frame format.

Answer

IEEE 802.3 specifies one type of frame containing seven fields : preamble, SFD, DA, SA, length/type of PDU, 802.2 frame and the CRC. The format of the MAC frame in CSMA/CD is shown in Fig. 2.14.1.

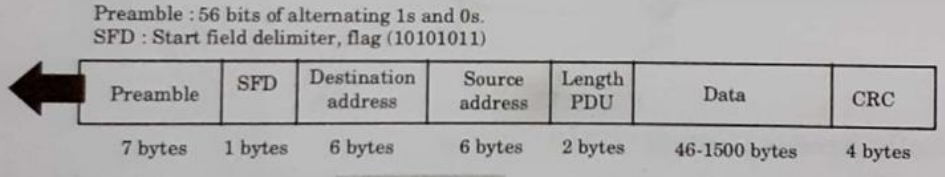


Fig. 2.14.1.

1. **Preamble :** The first field of the 802.3 frame, the preamble, contains seven bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enable it to synchronize its input timing.
2. **Start Frame Delimiter (SFD) :** The second field (one byte : 10101011) of the 802.3 frame signals at the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.
3. **Destination Address (DA) :** The Destination Address (DA) field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its Network Interface Card (NIC).
4. **Source Address (SA) :** The source address (SA) field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router to receive and forward the packet.

5. **Length/Type of Protocol Data Unit (PDU) :** These next two bytes indicate the number of bytes in the coming PDU. If the length of the PDU is fixed, this field can be used to indicate type, or as a base for other protocols.
6. **Data :** This field can be split up into two parts Data (0-1500 bytes) and padding (0-46 bytes).
7. **CRC :** The last field in the 802.3 frame contains the error detection information, in this case a CRC-32.

Que 2.15. How does in IEEE standard 802.5 LAN operates ? Discuss.

Answer

1. IEEE standard 802.5 LAN is a token ring system which is as shown in Fig. 2.15.1. It consists of a number of stations connected to the ring through a Ring Interface Unit (RIU).
2. The RIU is basically a repeater, therefore it regenerates the received data frames and sends them to the next station after some delay.

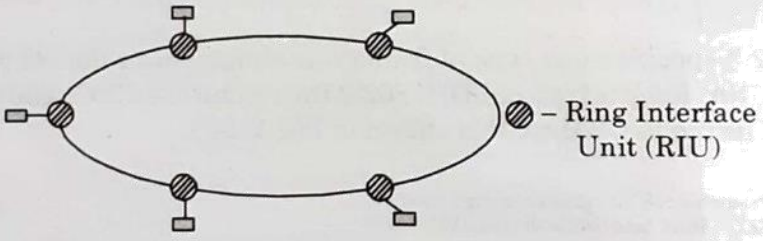


Fig. 2.15.1.

Media Access Control (MAC) :

1. The access to the medium (*i.e.*, who will transmit) is controlled by the special control frame called token.
2. The token is passed from one station to the other round the ring. The sequence of token passing is dependent on the physical location of the stations connected to the ring. It is not dependent on logical number as in case of token bus system.
3. A station which is in possession of the token only can transmit the frames. It may transmit one or more data frames but before the expiry of Token Holding Time (THT). Thus every station gets a fixed time to transmit its data.
4. Typically this time is of 10 msec. After the THT, the token frame must be handed over to some other station.

Que 2.16. How does IEEE standard 802.4 LAN operates ?

Answer

1. The IEEE 802.4 standard for Media Access Control (MAC) is known as token bus.

2. Logically the interconnected stations form a ring as shown in Fig. 2.16.1. The physical topology is bus topology as shown in Fig. 2.16.1.

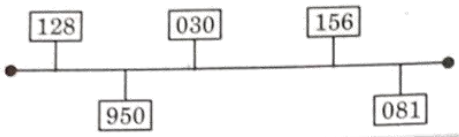


Fig. 2.16.1. Physical topology in token passing.

Media access control :

The operation of token bus taken place as follows :

1. At any time, the station which holds the token only can transmit its data frames on the bus. Every frame contains source and destination address.
2. All the other stations are ready to receive these data frames.
3. As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence. That station is allowed to transmit its data now.
4. In one cycle of operation, each station will get an opportunity to transmit once. The same station can get more number of chances to transmit in one cycle if more than one address is assigned to it.

Que 2.17. Differentiate between 802.3, 802.4, and 802.5 IEEE standards.

AKTU 2013-14, Marks 05

Answer

S. No.	Parameters	802.3 Ethernet Bus	802.4 Token Bus	802.5 Token Ring
1.	Physical topology	Linear	Linear	Ring
2.	Logical topology	None	Ring	Ring
3.	Contention	Random chance	By token	By token
4.	Maintenance	No central maintenance	Distributed algorithm provides maintenance.	A designated monitor station performs maintenance.
5.	Cable used	Twisted pair, co-axial fiber optic	Co-axial	Twisted pair and fiber optic.
6.	Cable length	50 m to 2000 m	200 m to 500 m	50 m to 1000 m
7.	Frequency	10 Mbps to 100 Mbps	10 Mbps	4 to 100 Mbps
8.	Frame structure	1500 bytes	8191 bytes	5000 bytes

Que 2.18. Define Fiber Distributed Data Interface (FDDI) in detail with the help of its frame format.

Answer

FDDI :

1. Fiber Distributed Data Interface (FDDI) is a local area network protocol.
2. It supports data rates of 100 Mbps and provides a high speed alternative to Ethernet and token ring.
3. The copper version of FDDI is known as CDDI.
4. In FDDI, access is limited by time.
5. A station may send as many frames as it can within its allotted access period, with the provision that real time data be sent first.

Frame format :

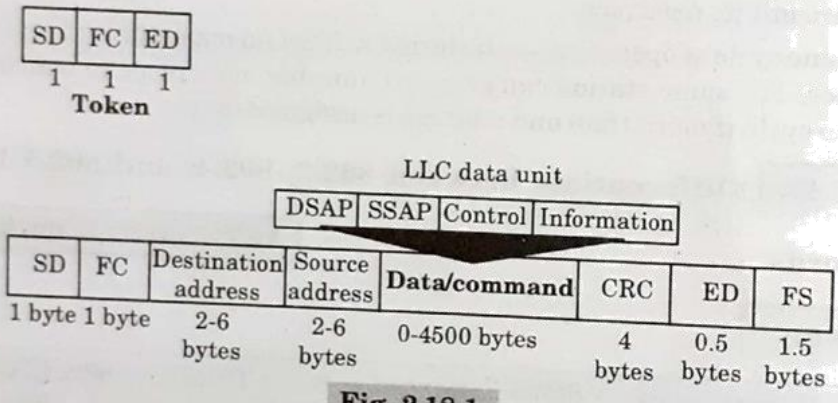


Fig. 2.18.1.

Frame fields :

1. **Start Delimiter (SD) :** The first byte of the field is the frame's starting flag.
2. **Frame Control (FC) :** The second byte of the frame identifies the frame type.
3. **Addresses :** The next two fields are the destination and source addresses. Each address consists of two to six bytes.
4. **Data :** Each data frame can carry up to 4500 bytes of data.
5. **Cyclic Redundancy Check (CRC) :** The field consists of 4 bytes.
6. **End Delimiter (ED) :** This field consists of half a byte in the data frame or a full byte in the token frame. It is changed in the physical layer with one *T* violation symbol in the data/command frame or two *T* symbols in the token frame.
7. **Frame Status (FS) :** The FDDI FS field is similar to that of token ring. It is included only in the data/command frame and consists of 1.5 bytes.

Que 2.19. **Brief about how line coding implemented in FDDI and describe its format.** **AKTU 2016-17, Marks 10**

Answer

Line coding implementation :

1. FDDI line coding use NRZI scheme in transition of data.
2. In this scheme, 4B/5B method is used in group encoding strategy.
3. The 4B/5B encoding scheme takes data in four bits codes and maps them to corresponding five bit codes.
4. For example, the four bit data code for the letter F (1111) corresponding to the five bit encoding 11101. These five bit codes are then transmitted using NRZI. By transmitting five bit codes using NRZI, a logical 1 bit is transmitted at least once every five sequential data bits, resulting in a signal transition.

Frame format for FDDI : Refer Q. 2.18, Page 2–14A, Unit-2.

PART-4

Data Link Layer – Elementary Data Link Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.20. **Discuss the issues in the data link layer and about its protocol on the basis of layering principle.** **AKTU 2016-17, 2017-18; Marks 10**

Answer

Data link layer issues are :

1. **Services provided to the network layer :**
   a. The data link layer act as a service interface to the network layer.
   b. The principle service is transferring data from the network layer on sending machine to the network layer on destination machine. This transfer always takes place via DLL (Dynamic Link Library).
2. **Frame synchronization :**
   a. The source machine sends data in the form of blocks called frames to the destination machine.

b. The starting and ending of each frame should be identified so that the frames can be recognized by the destination machine.

3. **Flow control :**
   a. Flow control is done to prevent the flow of data frame at the receiver end.
   b. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

4. **Error control :**
   a. Error control is done to prevent duplication of frames.
   b. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

Data link layer protocol on the basis of layering principle :

1. **Serial Line Internet Protocol (SLIP) :**
   a. This protocol is used to connect a workstation to the internet over a dial-up line using a modem.
   b. It is connection-oriented protocol.
   c. The protocol is very simple. The workstation sends raw IP packets over the line with a flag byte at the end for framing purpose.

2. **Point-to-Point Protocol (PPP) :**
   a. This protocol is used by a lot of internet users to connect their home computers to the server of an Internet Service Provider (ISP).
   b. Most of these users have a traditional modem and they are connected to the internet through a telephone line or a TV cable.
   c. The PPP is used for controlling and managing the data transfer.

3. **High Level Data Link Control (HDLC) Protocol :**
   a. HDLC is a bit oriented data link control protocol, and it is designed to satisfy many of data control requirements.
   b. For the HDLC protocol the following three types of stations have been defined :
      i. **Primary station :** A primary station takes care of the data link management.
      ii. **Secondary station :** A secondary station operates under the control of a primary station.
      iii. **Combined station :** A combined station can act as both primary and secondary stations.

4. **Ethernet :**
   a. Ethernet supports nearly every protocol, and can operate with any networking equipment that adheres to the IEEE standard.

b. This openness, combined with the ease of use, has made Ethernet dominant in the local area network.
c. The Ethernet system consists of three basic elements :
   i. The physical medium used to carry Ethernet signals between computers.
   ii. A set of medium access control rules embedded in each Ethernet interface that allow multiple computers to fairly access to the shared Ethernet channel.
   iii. An Ethernet frame that consists of a standardized set of bits used to carry data over the system.

PART-5

Sliding Window Protocols.

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.21. Explain sliding window protocol.

OR

Write short note on sliding window protocol.

AKTU 2014-15, Marks 2.5

AKTU 2017-18, Marks 05

Answer

1. Sliding window protocol is a feature of packet based data transmission protocols.
2. Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.
3. In sliding window method, multiple frames are sent by sender at a time before an acknowledgement is needed.
4. To keep track of which frames have been transmitted and which received, sliding window introduces an identification scheme based on the size of the window.
5. The frames are numbered modulo-n, which means they are numbered from 0 to $n - 1$. For example, if $n = 8$, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, ... The size of the window is $n - 1$ (*i.e.*, 7).
6. When the receiver sends an ACK, it includes the number of the next frame it expects to receive. In other words, to acknowledge the receipt of a string of frames ending in frame 4, the receiver sends an ACK containing the number 5.

7. When the sender sees an ACK with the number 5, it knows that all frames up to number 4 have been received.
8. The window can hold $n-1$ frames at either end; therefore, a maximum of $n-1$ frames may be sent before an acknowledgement is required.

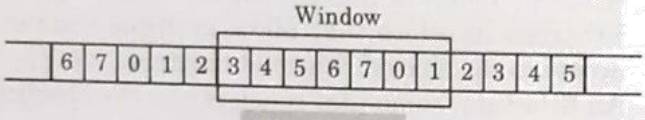


Fig. 2.21.1.

Sender window : At the beginning of a transmission, the sender's window contains $n-1$ frames. As frames are sent out, the left boundary of the window moves inward, shrinking the size of the window.

1. Given a window of size w, if three frames have been transmitted since the last acknowledgement, then the number of frames left in the window is $w-3$.
2. Once an ACK arrives, the window expands to allow in a number of new frames equal to the number of frames acknowledged by that ACK. Fig. 2.21.2 shows a sender sliding window of size 7.

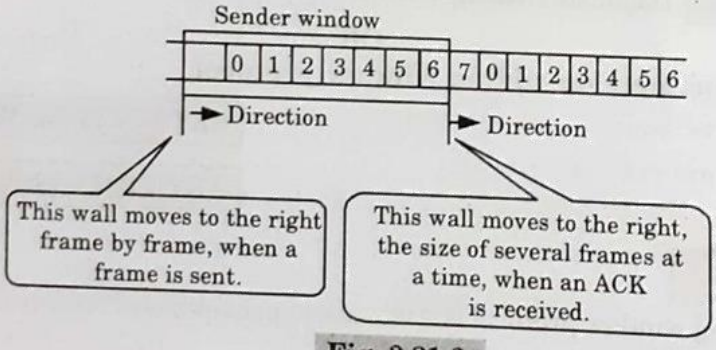


Fig. 2.21.2.

Receiver window : At the beginning of transmission, the receiver window contains not $n-1$ frames but $n-1$ spaces for frames.

1. As new frames come in, the size of the receiver window shrinks. The receiver window therefore represents not the number of frames received but the number of frames that may still be received before an ACK must be sent.
2. Given a window of size w, if three frames are received without an acknowledgement being returned, the number of spaces in the window is $w-3$.
3. As soon as an acknowledgement is sent, the window expands to include places for a number of frames equal to the number of frames acknowledged. Fig. 2.21.3 shows a receiving window of size 7.

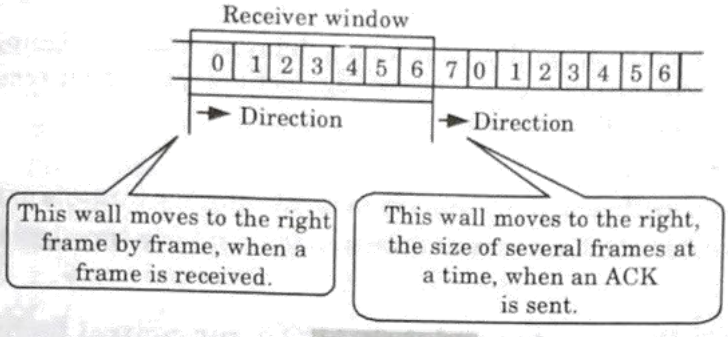


Fig. 2.21.3.

Que 2.22. Discuss stop and wait technique for flow control.

Answer

1. Stop and wait technique is the simplest form of flow control where a sender transmits a data frame.
2. After receiving the frame, the receiver indicates its willingness to accept another frame by sending back an ACK frame acknowledging the frame just received.
3. The sender must wait until it receives the ACK frame before sending the next data frame.
4. This technique is simple to understand and easy to implement, but not very efficient.
5. Fig. 2.22.1 illustrates the operation of the stop and wait protocol.

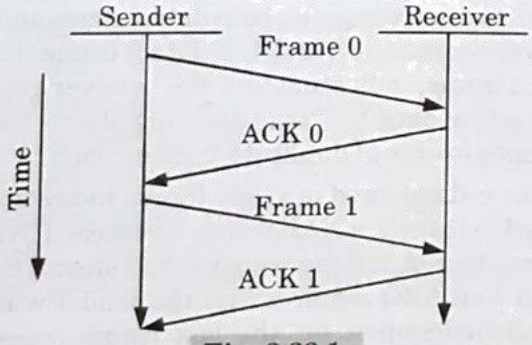


Fig. 2.22.1.

Que 2.23. State drawbacks of stop and wait protocols.

AKTU 2013-14, Marks 05

Answer

Drawbacks of stop and wait protocols are :

1. Data is lost due to processing or storage that occurs between the last backup and the subsequent disk crash, system crash, or some other such disaster.

2. After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet in stop and wait protocols.
3. No pipelining.
4. It is very inefficient as at any one moment, only one frame is in transition.
5. The sender will have to wait at least one round trip time before sending next.

Que 2.24. Discuss stop and wait ARQ error control technique.

OR

Write a short note on stop and wait ARQ. **AKTU 2014-15, Marks 2.5**

AKTU 2017-18, Marks 05

Answer

1. Stop and wait ARQ is a form of stop and wait flow control extended to include retransmission of data in case of lost or damaged frames.
2. For retransmission to work, four features are added to the basic flow control mechanism :

   The sending device keeps a copy of the last frame transmitted until it receives an acknowledgement for that frame. Keeping a copy allows the sender to retransmit lost or damaged frames until they are received correctly.

   b. For identification purposes, both data frames and ACK frames are numbered alternately 0 and 1. A data 0 frame is acknowledged by an ACK 1 frame, indicating that the receiver got the data 0 and is now expecting data 1. This numbering allows for identification of data frames in case of duplicate transmission.

   c. If an error is discovered in a data frame, indicating that it has been corrupted in transit, a NAK frame is returned. NAK frames, which are not numbered, tell the sender to retransmit the last frame sent. Stop and wait ARQ requires that the sender wait until it receives an acknowledgement for the last frame transmitted before it transmits the next one. When the sending device receives a NAK, it resends the frame transmitted after the last acknowledgement regardless of number.

   d. The sending device is equipped with a timer. If an expected acknowledgement is not received within an allotted time period, the sender assumes that the last data frame was lost in transit and sends it again.

Following are the operations of protocol under certain conditions :

a. Operation in case of damaged frames :

1. When a frame is discovered by the receiver to contain an error, it returns a NAK frame and the sender retransmits the last frame.

2. For example, the sender transmits a data frame : data 0. The receiver returns an ACK 1, indicating the data 0 arrived undamaged and it is now expecting data 1.
3. The sender transmits its next frame : data 1. It arrives undamaged, and the receiver returns ACK 0.
4. The sender transmits its next frame : data 0. The receiver discovers an error in data 0 and returns a NAK.
5. The sender retransmits data 0. This time data 0 arrives intact, and the receiver returns ACK 1.

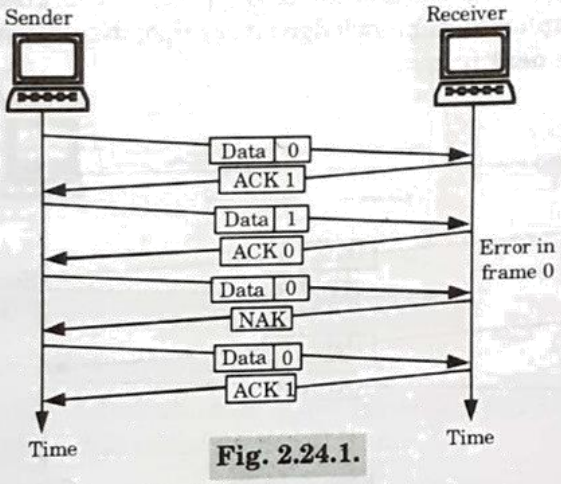


Fig. 2.24.1.

b. Operation in case of lost frame :

1. Any of the three frame types can be lost in transit. Fig. 2.24.2 shows how stop and wait ARQ handles the loss of a data frame.
2. The sender is provided with a timer that starts every time when a data frame is transmitted. If the frame never makes it to the receiver, the receiver can never acknowledge it, positively or negatively.
3. The sending device waits for an ACK or NAK frame until its timer goes off, at which point it tries again. It retransmits the lost data frame, restarts its timer, and waits for an acknowledgement.

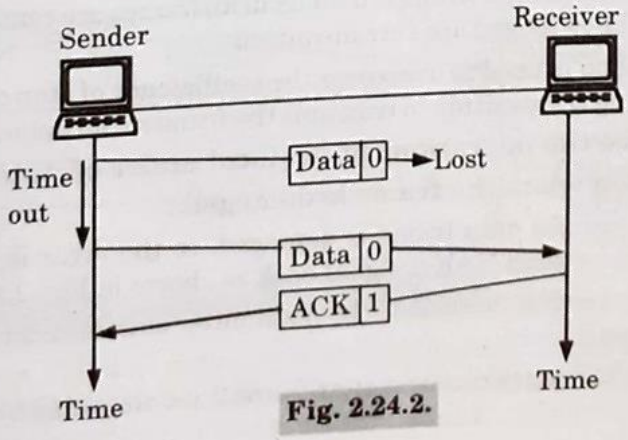


Fig. 2.24.2.

c. Operation in case of lost acknowledgement :

1. In this case, the data frame has made it to the receiver and has been found to be either acceptable or not acceptable. But the ACK or NAK frame returned by the receiver is lost in transit.
2. The sending device waits until its timer goes off, then retransmits the data frame.
3. The receiver checks the number of the new data frame. If the lost frame was a NAK, the receiver accepts the new copy and returns the appropriate ACK.
4. If the lost frame was an ACK, the receiver recognizes the new copy as a duplicate, acknowledges it receipt, then discards it and waits for the next frame.

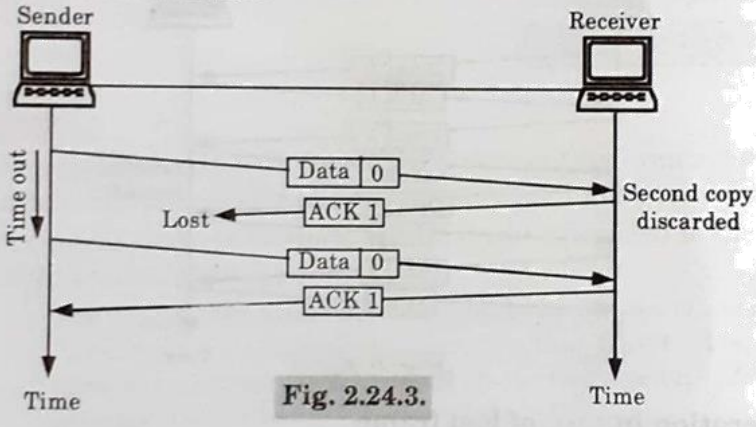


Fig. 2.24.3.

Que 2.25. Describe the Go-back-N ARQ protocol.

OR

Write a short note on Go-back-N ARQ. **AKTU 2014-15, Marks 2.5**

AKTU 2017-18, Marks 05

Answer

1. In this method if one frame is damaged, all frames are sent since the last frame acknowledged are retransmitted.
2. This method is used to overcome the inefficiency of stop and wait ARQ by allowing transmitter to transmit the frames continuously.

Following are the operations of protocol under certain condition :

1. Operation when the frame is damaged :

a. The second data frame is damaged, so the error is detected and receiver send NAK-2 signal back as shown in Fig. 2.25.1.

b. On receiving this signal, the transmitter starts retransmission from frame 2.

c. All the frames received after frame 2 are discarded by the receiver.

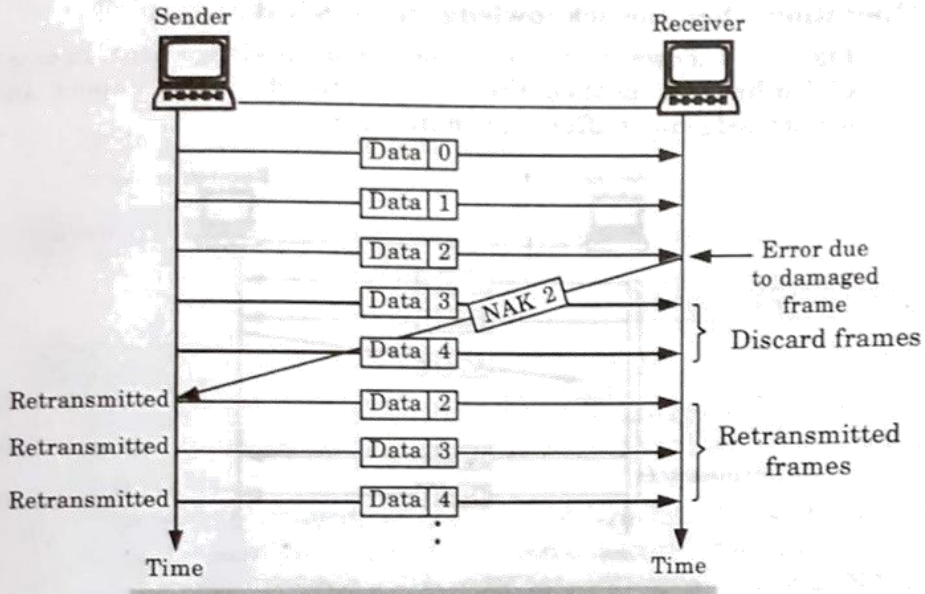


Fig. 2.25.1. Go-back-N, damaged data frame.

2. Operation when a frame is lost :

a. As shown in Fig. 2.25.2, the case of lost frame is also treated in the same manner as that of the damaged frame.

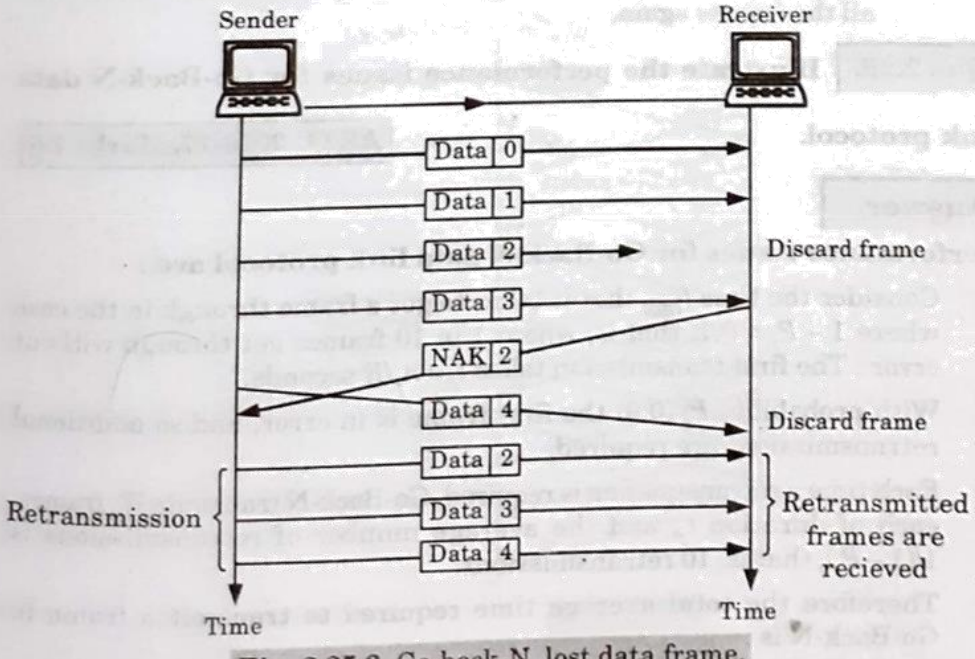


Fig. 2.25.2. Go-back-N, lost data frame.

b. The receiver, if it does not receive a particular data frame it sends a NAK to the transmitter and the transmitter retransmits all the frames sent since the last frame acknowledged.

3. Operation when the acknowledgement is lost :

a. Fig. 2.25.3 shows the condition for lost acknowledgement. In case of Go-back-N method the transmitter does not expect an acknowledgement after every data frame.

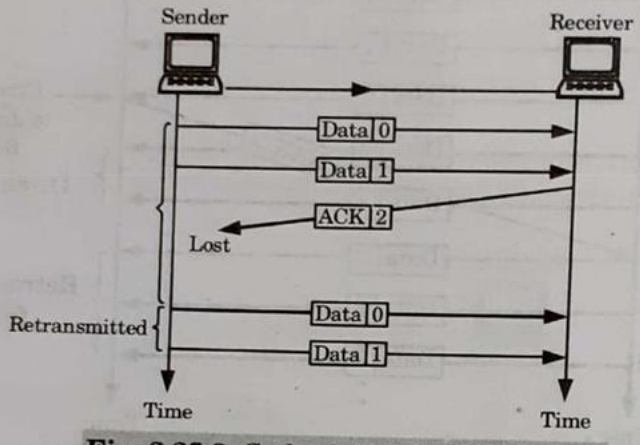


Fig. 2.25.3. Go-back-N, lost ACK frame.

b. The transmitter can send as many frames as the window allows before waiting for an acknowledgement.

c. Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the frames again.

Que 2.26. Illustrate the performance issues for Go-Back-N data link protocol.

AKTU 2016-17, Marks 7.5

Answer

Performance issues for Go-Back-N data link protocol are :

1. Consider the time t_{GBN} that it takes to get a frame through in the case where $1 - P_f = 0.1$, that is, where 1 in 10 frames get through without error : The first transmission takes $t_f = n_f/R$ seconds.
2. With probability P_f (0.9) the first frame is in error, and so additional retransmissions are required.
3. Each time a retransmission is required, Go-Back-N transmits W_s frames, each of duration t_f, and the average number of retransmissions is $1/(1-P_f)$, that is, 10 retransmissions.
4. Therefore the total average time required to transmit a frame in Go-Back-N is :

$$t_{GBN} = t_f + P_f \frac{W_s t_f}{1 - P_f}$$

Thus for the example, we have $t_{GBN} = t_f + 9W_s t_f$.

5. The efficiency for Go-Back-N is given by :

$$\eta_{GBN} = \frac{\frac{n_f - n_0}{t_{GBN}}}{R} = \frac{1 - \frac{n_0}{n_f}}{1 + (W_s - 1)P_f}(1 - P_f)$$

If the channel is error-free, that is $P_f = 0$, then Go-Back-N attains the best possible efficiency, namely, $1 - n_0/n_f$.

Que 2.27. **Write a short note on selective repeat ARQ.**

AKTU 2014-15, Marks 2.5

Answer

1. The selective repetitive ARQ scheme retransmits only those for which NAKs are received or for which timer has expired, this is shown in the Fig. 2.27.1.
2. This is the most efficient among the ARQ schemes, but the sender must be more complex so that it can send out-of-order frames.
3. The receiver also must have storage space to store the post NAK frames and processing power to reinsert frames in proper sequence.
4. In selective repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NAK for only frame which is missing or damaged.

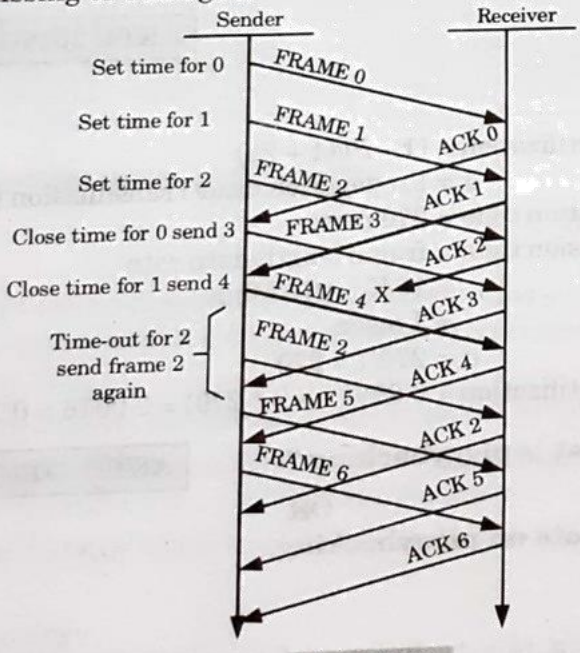


Fig. 2.27.1.

Que 2.28. **Compare two data link layer protocols : Go-back-N and selective repeat in terms of flow control, error recovery and packet loss.**

Answer

S. No.	Criteria	Go-back-N	Selective repeat
1.	Flow control	Flow control is done by storing frame of window size (N) in buffer at receiver end.	Flow control is done by storing continuous occurring frame in buffer at receiver end.
2.	Error recovery	It detects and controls the error during transmission of packets.	It detects and corrects the error during transmission of packets.
3.	Packet loss	If packet is lost during transmission then it discards all the packets after receiving NAK acknowledgement for the lost packet.	If packet is lost during transmission then it discards only the packet which is lost and continues to send other packets.

Que 2.29. Consider the use of 10 K-bit size frames on a 10 Mbps satellite channel with 270 ms delay. What is the link utilization for stop-and-wait ARQ technique assuming $P = 10^{-3}$?

AKTU 2016-17, Marks 10

Answer

Link utilization = $(1 - P)/(1 + 2a)$

where, a = Propagation time/Transmission time

Propagation time = 270 msec

Transmission time = frame length/data rate

= 10 K-bit/10 Mbps

= 1 msec

Hence, $a = 270/1 = 270$

Link utilization = $0.999/(1 + 2 * 270) = 0.0018 = 0.18\%$

Que 2.30. What is piggybacking ?

AKTU 2013-14, Marks 05

OR

Write a short note on piggybacking.

Answer

1. Piggybacking is a technique of temporarily delaying outgoing acknowledgments. So, that they can be hooked into the next outgoing data frame.
2. A better solution would be to use each channel (forward and reverse) to transmit frames both ways, with both channels having the same capacity.

3. Let A and B be the users. Then the data frames from A to B are intermixed with the acknowledgements from A to B. By checking the kind field in the header of the received frame, the received frame can be identified as either data frame or acknowledgement.
4. When a data frame arrives, the receiver waits, does not send the control frame (acknowledgement) back immediately.
5. The receiver waits until its network layer passes in the next data packet.
6. The acknowledgement is then attached to this outgoing data frame. Thus the acknowledgement travels along with next data frame.

PART-6

Error Handling.

CONCEPT OUTLINE

- Three error detecting methods :
  i. Parity checking
  ii. Checksum error detection
  iii. Cyclic redundancy check

Questions-Answers

Long Answer Type and Medium Answer Type Questions

Que 2.31. Discuss error and its types.

Answer

1. Whenever an electromagnetic signal flows from one point to another, it is subject to unpredictable interference from heat, magnetism, and other forms of electricity.
2. This interference can change the shape or timing of the signal.
3. If the signal is carrying encoded binary data, such changes can alter the meanings of the data. This condition results in error.

Depending on the number of bits in error we can classify the errors into two types as :

1. **Single bit error :**
   a. The term single bit error suggests that only one bit in the given data unit such as byte is in error.
   b. That means only one bit in a transmitted byte will change from 1 to 0 or 0 to 1, as shown in Fig. 2.31.1.

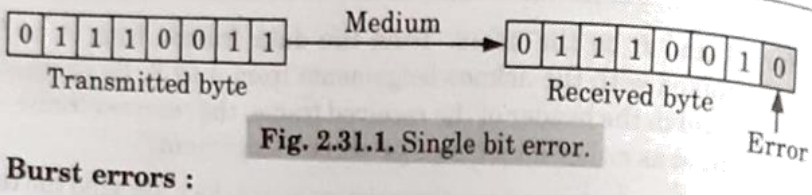


Fig. 2.31.1. Single bit error.

2. **Burst errors :**

   a. If two or more bits from a data unit such as a byte change from 1 to 0 or from 0 to 1 then burst errors are said to have occurred.

   b. The length of the burst error extends from the first erroneous bit to the last erroneous bit. Even though some of the bits in between have not been corrupted the length of the burst error is shown to be 5 bits.

   c. Burst errors are illustrated in Fig. 2.31.2.

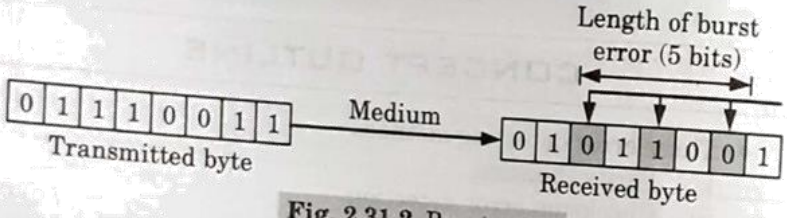


Fig. 2.31.2. Burst error.

Que 2.32. How does parity checking is helpful in error detection ?

Answer

1. The parity checking at the receiver can detect the presence of an error if the parity of the received signal is different from the expected parity.
2. That means if it is known that the parity of the transmitted signal is always going to be "even" and the received signal has an odd parity then the receiver can conclude that the received signal is not correct. This is as shown in Fig. 2.32.1.

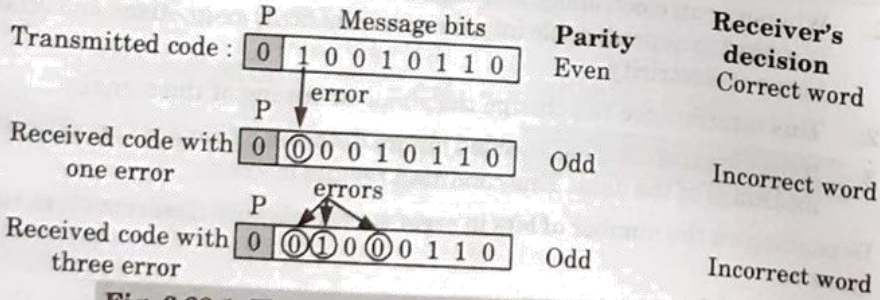


Fig. 2.32.1. The receiver detects the presence of error if the number of errors is odd *i.e.*, 1, 3, 5.

3. If a single error or an odd number of bits change due to errors introduced during transmission the parity of the codeword will change.
4. Parity of the received codeword is checked at the receiver and if there is change in parity then it is understood that error is present in the received word. This is as shown in Fig. 2.32.1.
5. If presence of error is detected then the receiver will ignore the received byte and request for the retransmission of the same byte to the transmitter.

Que 2.33. Explain the concept of checksum. How error is detected using the checksum byte ?

Answer

1. A checksum is a value used to verify the integrity of a file or a data transfer.
2. It is a sum that checks the validity of data.
3. A checksum is a simple type of redundancy check that is used to detect errors in data.
4. Checksums are typically used to compare two sets of data to make sure they are the same.
5. At the receiver end, the checksum function is applied to the message frame to retrieve the numerical value.
6. If the received checksum value matches the sent value, the transmission is considered to be successful and error free.

Error detection using checksum byte :

1. In checksum error detection scheme, the data is divided into k segments each of m bits.
2. In the sender's end the segments are added using 1's complement arithmetic to get the sum.
3. The sum is complemented to get the checksum.
4. The checksum segment is sent along with the data segments.
5. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
6. If the result is zero, the received data is accepted otherwise discarded.

Let consider following data

10011001111000100010010010000100

Original data

10011001	11100010	00100100	10000100
1	2	3	4

k = 4, m = 8

Sender

1 10011001

2 11100010

(1)01111011

1

01111100

3 00100100

10100000

4 10000100

(1)00100100

1

Sum : 00100101

Checksum : 11011010

Receiver

1 10011001

2 11100010

(1)01111011

1

01111100

3 00100100

10100000

4 10000100

(1)00100100

1

00100101

11011010

Sum : 11111111

Complement : 00000000

Conclusion : Accept data

Que 2.34. Write a short note on CRC.

Answer

1. CRC is a type of polynomial code in which a bit string is represented in the form of polynomials with coefficients of 0 and 1 only.
2. Polynomial arithmetic uses a modulo-2 arithmetic *i.e.*, addition and subtraction are identical to EX-OR.
3. For CRC code the sender and receiver should agree upon a generator polynomial $G(x)$. A codeword can be generated for a given dataword (message) polynomial $M(x)$ with the help of long division.
4. CRC works on the principle of binary division. A sequence of redundant bits called CRC or CRC remainder is appended at the end of the message. This word is called appended message word.
5. The appended word thus obtained becomes exactly divisible by the generator word corresponding to $G(x)$.

CRC generator :

1. The CRC generator is shown in Fig. 2.34.1.

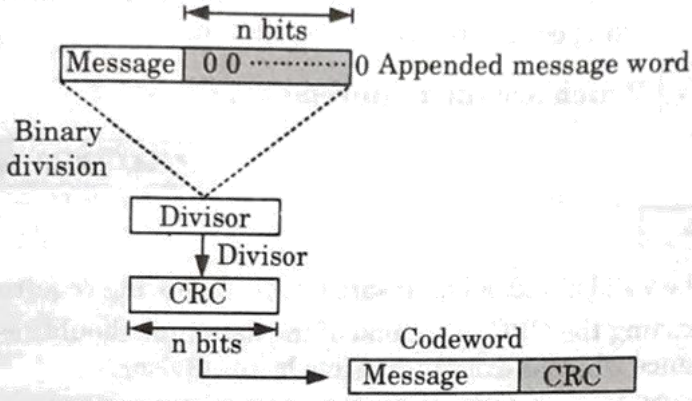


Fig. 2.34.1. CRC generator.

2. The stepwise procedure in CRC generation is as follows :

   Step 1 : Append a train of n 0s to the message word where n is 1 less than the number of bits in the predecided divisor (*i.e.*, generator word). If the divisor is 5-bit long then we have to append 4-zeros to the message.

   Step 2 : Divide the newly generated data unit in step 1 by the divisor (generator). This is a binary division.

   Step 3 : The remainder obtained after the division in step 2 is the n bit CRC.

   Step 4 : This CRC will replace the n 0s appended to the data unit in step 1, to get the codeword to be transmitted as shown in Fig. 2.34.1.

CRC checker :

1. Fig. 2.34.2 shows the CRC checker.

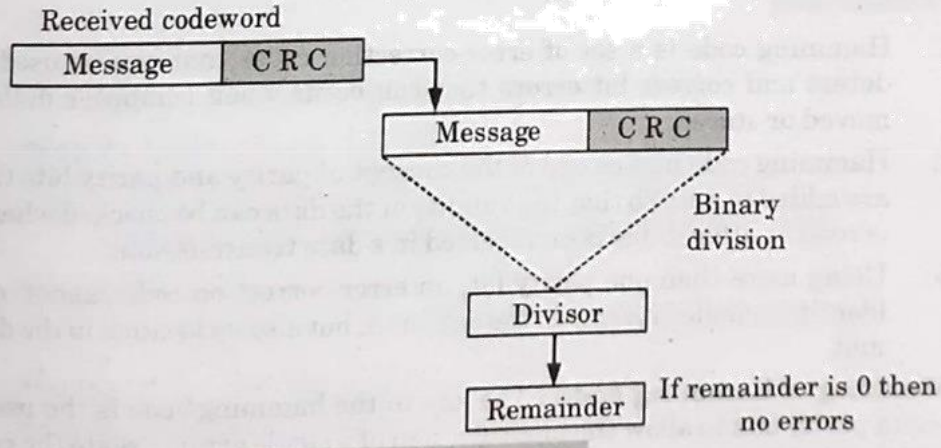


Fig. 2.34.2. CRC checker.

2. The codeword received at the receiver consists of message and CRC.
3. The receiver treats it as one unit and divides it by the same $(n + 1)$ bit divisor (generator word) which was used at the transmitter.
4. The remainder of this division is then checked.

5. If the remainder is zero, then the received codeword is error free and hence should be accepted.
6. But a non-zero remainder indicates presence of errors hence the corresponding codeword should be rejected.

Que 2.35. Which are the requirements of CRC ?

AKTU 2013-14, Marks 05

Answer

CRC will be valid if and only if it satisfies the following requirements:

1. Appending the CRC to the end of the data unit should result in the bit sequence which is exactly divisible by the divisor.
2. The CRC has one bit less than the divisor. It means that if CRC is of n bits, divisor is of $n + 1$ bit.
3. At the destination, the incoming data unit *i.e.*, data + CRC should be divided by the same number (predetermined binary divisor).
4. If the remainder after division is zero then there should be no error in the data unit and receiver accepts it.

Que 2.36. Describe hamming code. How it is used for error detection and correction ? Illustrate with the help of suitable example.

OR

What is hamming code ? Explain its working with suitable example.

AKTU 2015-16, Marks 7.5

Answer

1. Hamming code is a set of error-correction codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored.
2. Hamming code makes use of the concept of parity and parity bits that are added to data so that the validity of the data can be checked when it is read or after it has been received in a data transmission.
3. Using more than one parity bit, an error-correction code cannot only identify a single bit error in the data unit, but also its location in the data unit.

Working of hamming code : The key to the hamming code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows :

1. Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)
2. All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)

3. Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.

   Position 1 : Check 1 bits, skip 1 bits, check 1 bits, skip 1 bits, etc. (1,3,5,7,9,11,13,15,...)

   Position 2 : Check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)

   Position 4 : Check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)

   Position 8 : Check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)

   Position 16 : Check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc., (16-31,48-63,80-95,...)

   Position 32 : Check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc., (32-63,96-127,160-191,...)

4. Set a parity bit to 1 if the total number of ones in the positions it checks is odd.

5. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

For example : If the 7-bit hamming codeword received by a receiver is 1 0 1 1 0 1 1. Assuming the even parity state whether the received codeword is correct or wrong. If wrong, locate the bit in error.

	D_7	D_6	D_5	P_4	D_3	P_2	P_1
Received codeword :	1	0	1	1	0	1	1

Step 1 : Analyze bits 4, 5, 6 and 7 :

$$P_4\, D_5\, D_6\, D_7 = 1\,1\,0\,1 \rightarrow \text{Odd parity.}$$

$\therefore$ Error exists here.

$\therefore$ Put $P_4 = 1$ in the 4's position of the error word.

Step 2 : Analyze bits 2, 3, 6 and 7 :

$\therefore$ $P_2\, D_3\, D_6\, D_7 = 1\,0\,0\,1 \rightarrow$ Even parity so no error.

Hence put $P_2 = 0$ in the 2's position of the error word.

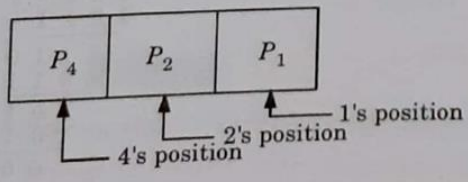
Step 3 : Check the bits 1, 3, 5, 7 :

$\therefore$ $P_1 D_3 D_5 D_7 = 1\,0\,1\,1 \rightarrow$ Odd parity so error exists.

Hence put $P_1 = 1$ in the 1's position of the error word.

Step 4 : Write the error word :

Error word E =



Substituting the values of P_4, P_2 and P_1 obtained in steps 1, 2 and 3 we get

$E =$ | 1 | 0 | 1 |

$= (5)_{10}$

Hence, bit 5 of the transmitted codeword is in error.

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

Incorrect bit

Step 5 : Correct the error :

Invert the incorrect bit to obtain the correct codeword as follows :
Correct codeword = [1 0 0 1 0 1 1]

Que 2.37. **Given a 10-bit sequence 1010011110 and a divisor of 1011. Find the CRC. Check your answer.** **AKTU 2014-15, Marks 05**

Answer

```
                1 0 0 1 0 0 0 1 1 1
          ┌─────────────────────────
1 0 1 1   │ 1 0 1 1 0 0 1 1 1 1 0 0 0 0
          │ 1 0 1 1
          │ ---------
          │   0 0 1 0
          │   0 0 0 0
          │   -------
          │     0 1 0 1
          │     0 0 0 0
          │     -------
          │       1 0 1 1
          │       1 0 1 1
          │       -------
          │         0 0 0 1
          │         0 0 0 0
          │         -------
          │           0 0 1 1
          │           0 0 0 0
          │           -------
          │             0 1 1 0
          │             0 0 0 0
          │             -------
          │               1 1 0 0
          │               1 0 1 1
          │               -------
          │                 1 1 1 0
          │                 1 0 1 1
          │                 -------
          │                   1 0 1 0
          │                   1 0 1 1
          │                   -------
          │                     0 0 1
```

Here, since remainder is 001. So, CRC will be 001.
We will add CRC to data and send it over network. At destination we have to check it if remainder is 000 then the data is right.

```
                1 0 0 1 0 0 0 1 1 1
          ┌─────────────────────────
1 0 1 1   │ 1 0 1 1 0 0 1 1 1 1 0 0 0 1
          │ 1 0 1 1
          │ ---------
          │   0 0 1 0
          │   0 0 0 0
          │   -------
          │     0 1 0 1
          │     0 0 0 0
          │     -------
          │       1 0 1 1
          │       1 0 1 1
          │       -------
          │         0 0 0 1
          │         0 0 0 0
          │         -------
          │           0 0 1 1
          │           0 0 0 0
          │           -------
          │             0 1 1 0
          │             0 0 0 0
          │             -------
          │               1 1 0 0
          │               1 0 1 1
          │               -------
          │                 1 1 1 0
          │                 1 0 1 1
          │                 -------
          │                   1 0 1 1
          │                   1 0 1 1
          │                   -------
          │                   0 0 0 0
```

Que 2.38. **Sketch the Manchester and differential Manchester encoding for the bit stream: 0001110101.** **AKTU 2014-15, Marks 05**

Answer

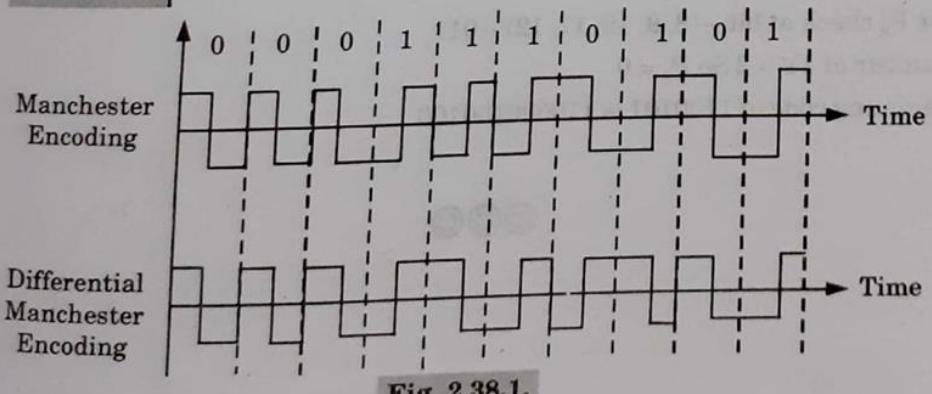


Fig. 2.38.1.

Que 2.39. **What is hamming code ? Calculate the hamming code for following message string : 1100101 with each and every step explained clearly.**

Answer

Hamming code : Refer Q. 2.36, Page 2–32A, Unit-2.

Numerical :

First check the number of parity bit used by using

$$2^x \geq k + x + 1$$

Number of data bit (k) = 7

$$2^x \geq 7 + x + 1$$

if $x = 4$

$$2^4 > 13$$

Number of parity bit = 4

Data/Parity	D_{11}	D_{10}	D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1
Data code	1	1	0		0	1	0		1		
Parity code				0				0		0	0
Code received	1	1	0	0	0	1	0	0	1	0	0

For P_1 check at bit – (1, 3, 5, 7, 9, 11) – 10001

Number of 1's = 2 So $P_1 = 0$

For P_2 check at bit – (2, 3, 6, 7, 10, 11) – 11011

Number of 1's = 4 So $P_2 = 0$

For P_4 check at bit – (4, 5, 6, 7, 12) – 011

Number of 1's = 2 So $P_4 = 0$

For P_8 check at bit – (8, 9, 10, 11, 12) – 011

Number of 1's = 2 So $P_8 = 0$

Hamming code of 1100101 is 110000100100.

☺☺☺