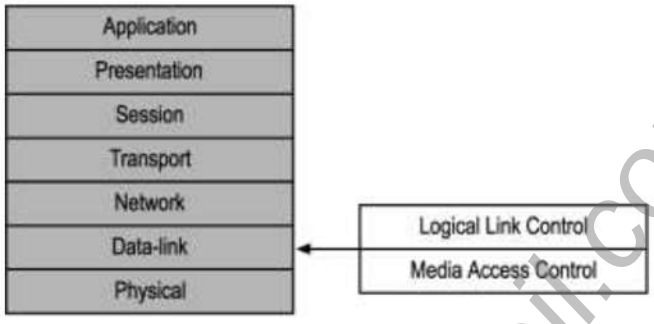
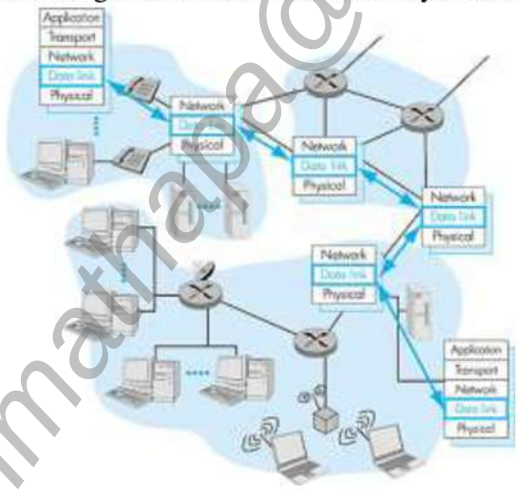
Chapter-3
Data link layer

Introduction

- The data link layer lies between the network layer and the physical layer in the protocol stack.
- It accepts packets from the network layer and arrange them in the form of frames.
- The primary function of data link layer is to provide error free transmission of information between two end stations attached to the same physical media.



- The data link layer is split into two sub layer.
    1. LLC
    2. MAC
- LLC establish and maintains link between the communicating devices. The LCL layer is concerned with managing traffic (flow and error control) over the physical medium It provides service to the network layer above by transferring the data from the network layer on the sending machine to the network layer on receiving machine.



- MAC control the way multiple device shares the same media channel. Since many networks use a shared medium, it is necessary to have rules for managing the medium to avoid conflicts. For example, Ethernet uses CSMA/CD protocol, while token ring uses Token passing protocol. Also MAC performs the function like adding heading and trailing, construction and assembling frames etc.

Functions of Data Link Layer

1. Service provided to network layer: The principle service is to transfer data from the network layer on source machine to the network layer on the destination machine.
2. Frame Synchronization: The source machine sends data in block called frames to the destination machine. The starting and ending on each frame must be recognized by the destination machine. Character count, coding: Manchester encoding etc. technique can be used for frame synchronization.
3. Flow Control: The source machine shouldn't send data frames at the rate faster than the destination machine can accept them.
4. Error detection and handling: The error made in the bits during transmission from source to destination machines must be detected and corrected. For example, CRC is often implemented to allow station receiving data to detect if it was received correctly or not.

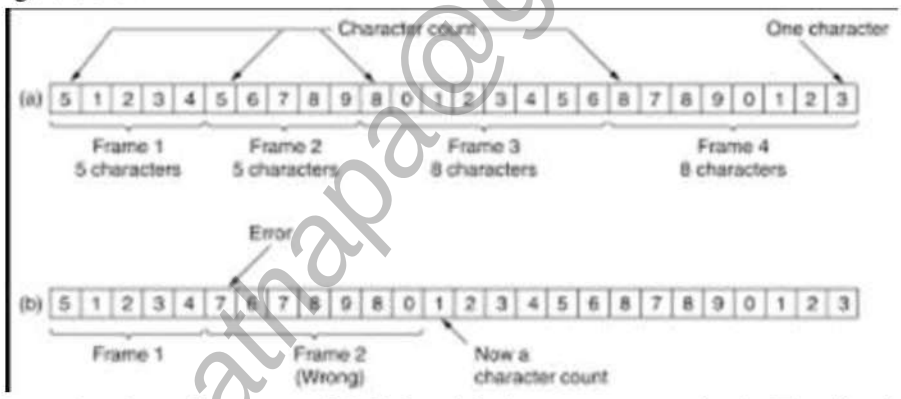
5. Addressing: Each device on a network has a unique number, called MAC address that is used by data link layer protocol to ensure that data intended for a specific machine gets to it properly.

Framing

- The bits to be transmitted is first broken into number of frames at the source data link layer.
- The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.
- Frames can be of fixed or variable size.
- In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.
- In variable-size framing, we need a way to define the end of the frame and the beginning of the next.
- Most data link networks use variable-size framing, which has advantages (more efficient use of the network) and disadvantages (unpredictable traffic flows and the inability to provide quality of service)
- Framing refers to the fact that beginning and end of data are marked so to be recognized and help in synchronization so that each frame is distinguishable.
- For this, there are several methods.

i. Character count:

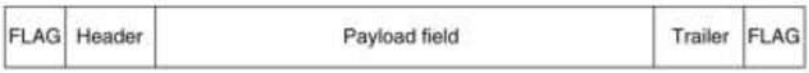
In this method, a field in header is used to specify the number of character in the frame. This number helps the receiver to know the number of characters in the frame following this count. The character count method is illustrated in the figure below



The four frames shown in above figure are of 5, 5, 8 and 8 characters respectively. The disadvantage of this method is that, an error can change the character count. If the wrong character count number is received, then the receiver will get out of synchronization and will be unable to locate start of next frame.

ii. Character Oriented Protocol

It solves the problem of character count method by adding a starting FLAG(8-bit) and ending FLAG(8-bit) at the beginning and end of the frame. Each frame is preceded by the transmission of control character flag. After each frame, same control character flag is transmitted to indicate the end of the frame. Hence if the receiver losses the synchronization, it just has to search for flag character to return back to track. It is because the receiver interprets flag as starting of frame or ending of Frame.



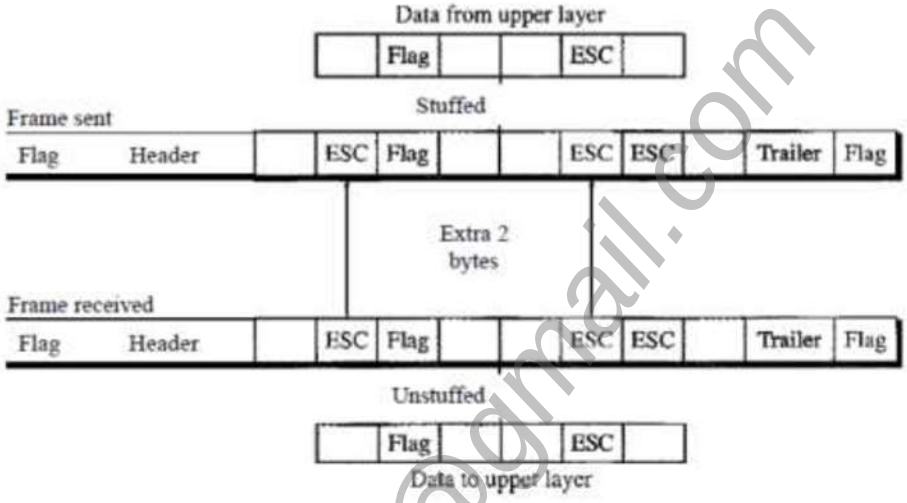
The problem with the above system is that the each 8-bit character used for Flag itself can be part of data. In that case the receiver will misinterpret it as end of frame. This problem is solved by using a technique called **byte stuffing or character stuffing.**

In this technique, the data link at the sender adds additional special 8-bit character ESC (Data Link Escape) character just before each accidental Flag or Esc character in the data. Now whenever the receiver encounters

the ESC character, it removes it from data section and treat the next character as data not as a control information.

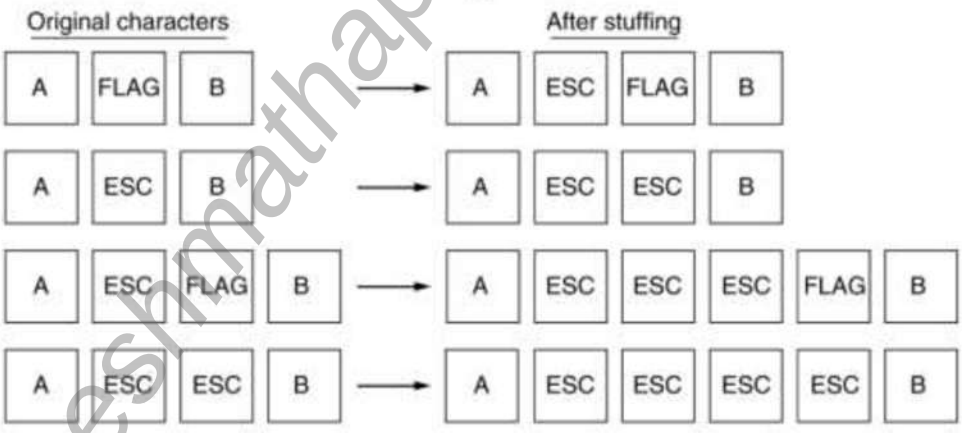
Again the problem arises when the data itself contains ESC character. Here the receiver simply removes the ESC character. So to solve this problem we stuff additional ESC character before each accidental ESC character in data. So, if the escape character is part of the text, an extra one is added to show that the second one is part of the text

The main drawback of this method is that we have to use additional stuffed character(8-bit) in addition to control characters which increases the data size.



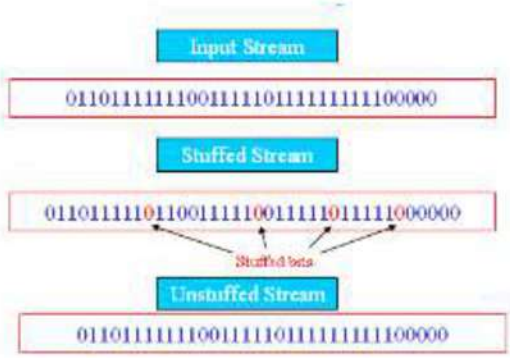
Some Other Example:

The below figure shows how byte stuffing is performed for different combination of character message.



iii. Starting and ending flags with bit stuffing

This technique overcomes the problem associated with the previous framing technique. In this technique, at the beginning and end of each frame, a specific 8-bit pattern 01111110 called flag byte is transmitted. Now whenever a sender data link layer detects the presence of five consecutive ones in the data, it automatically stuffs 0 into the outgoing bit stream. This is called bit stuffing and is illustrated as below.



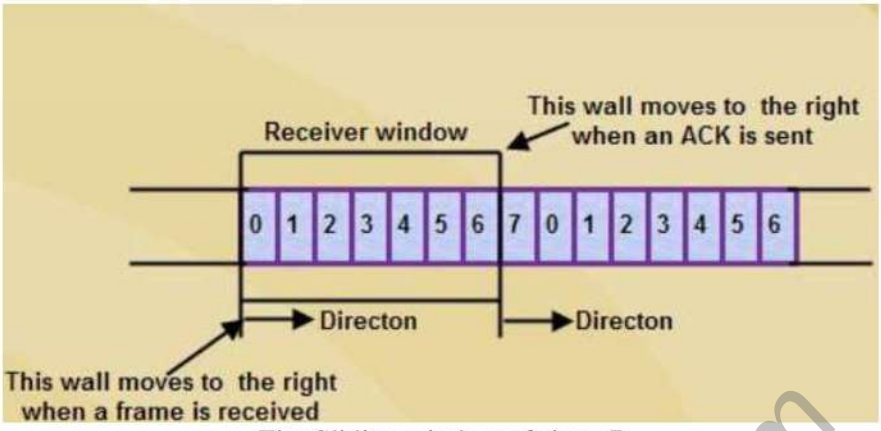
When the receiver detects the presence of five consecutive ones in the received bit stream, it automatically detects the 0 bit following five one. This is called de stuffing. Due to bit stuffing, the possible problem if the data contains the flag byte pattern is eliminated.

Flow Control

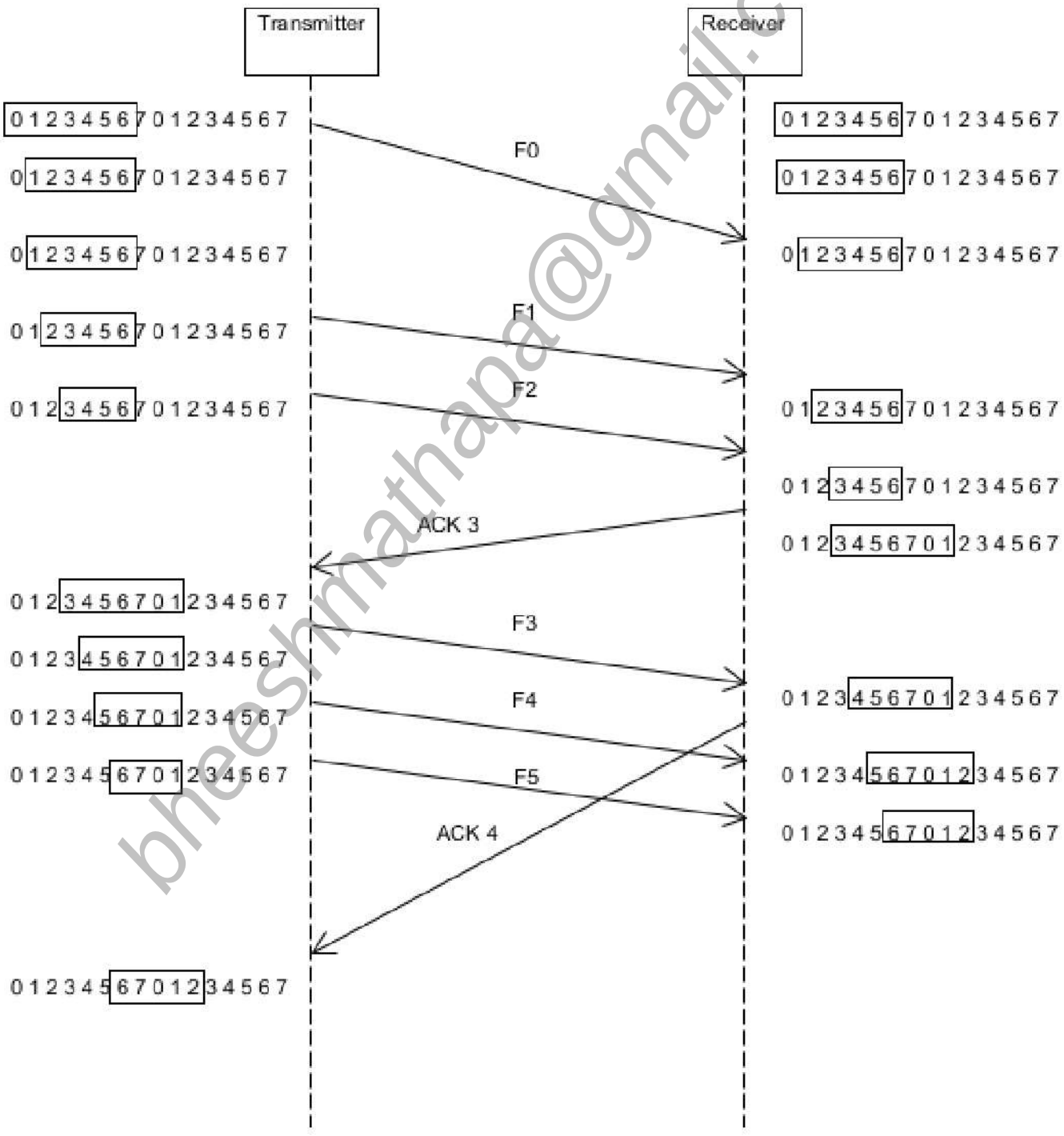
- One of the problems that come in data link layer is that what to do when sender systematically wants to transmits faster than the receiver can accept frame. Such situation arises when, sender is running on fast computer and the receiver is running on a slow computer.
- Even if there is no transmission error, at a certain point the receiver will simply not be able to handle the frames as they arrive and will start to lose some of them.
- The solution to such problem is flow control.
- Flow control is a technique for assuring that the transmitting entity doesn't over load the receiving entity with data.
- Techniques for flow control
    1. Stop and wait flow control
    2. Sliding window flow control

1. Stop and Wait Flow Control
    - The simplest form of flow control technique is stop and wait technique.
    - Here Whenever a source entity transmits a frame and is received by the destination, the destination indicates its willingness to accept another frame by sending back an acknowledgement to the frame just received.
    - The source must wait stop and until it receives acknowledgement before sending next frame.
    - The destination can thus stop the flow of data simply by withholding acknowledgement.
    - This technique is inefficient in today's high speed network.

2. Sliding window flow control
    - This technique allows us to send multiple frames without waiting for acknowledgement.
    - Let us consider two systems A and B connected through full duplex link.
    - Station B allocates buffer space for W frame. Thus B can accept W frames and A is allowed to send W frames without waiting for any acknowledgement.
    - To keep track of which frames have been acknowledged, each is labelled with sequence number.
    - B acknowledges a frame by sending an acknowledgement that includes the sequence number of next frame.
    - This technique can also be used to acknowledge multiple frames.
    - This acknowledgement also indicates that B is ready to receive next W frame, beginning with the number specified.
    - Station A maintains a list of sequence number that is allowed to send, and station B maintains a list of sequence number that is prepared to receive.
    - Each list can be thought as a window of frame. This operation is referred to as sliding-window flow control.



- Fig: Sliding window of size= 7



In the above figure, three bits' sequence number is used so that the frames are sequentially number from 0 to 7. There are 7 frames in window. Each time the frame is sent, the window size shrinks and each time the acknowledgement is received the window size grows.

- Initially A and B have window indication A can transmit 7 frames.
- After transmitting three frames f0, f1 and f2 without acknowledgement, A shrink its window size to four frame.
- When these frames numbered f0, f1 and f2 are received, B then transmit an acknowledgement ack3 indicating it is ready to receive frame number 3 i.e. prepared to receive 7 frames beginning from frame numbered 3.
- When A receives acknowledgement ack3, then now A is permit to transmit next 7 frames beginning from frame3.
- Now B transmits frame f3, f4 and f5.
- B returns ack4 which acknowledges frame f3, which allows transmission of frame f4 through the next instance of f2. But frame f4 and f5 are already transmitted therefore A may only open its window to permit sending 5 frames beginning from frame f6.

Error Detection and Correction

- When transmission of digital signals take place between two system such as computer take place, the signal get contaminated due to addition of noise. This introduces error in the binary bits which results changing of binary value from 0 to 1 and vice versa. Depending upon the number of bits, error can be classified as
  i. Single bit error: In this type of error, only one bit will change from 0 to 1 or 1 to 0.
  ii. Burst error: In this type of error, two or more bits will change from 0 to 1 or 1 to o.
- Transmission error are usually corrected at the data link layer of OSI model.
- Error Detection Method
  1. Check Sum
  2. Parity Checking
  3. CRC
- Error Correction Method
  1. Hamming Code
- Instead of sending a frame as it is , a codeword is sent from source to destination.
- The codeword is the n bit encoded blocks of bits. A codeword contains message bits and a redundant bits (parity bit) that can be used for error handling as shown in the figure below.

Databits	Parity bits

- Drawback of coding
  1. Use of coding make the system complex
  2. An increased transmission bandwidth is required in order to transmit the encoded message due to addition of redundant bet which is added by the encoder.

Parity Check

- In this technique, an additional bit called parity bit is added to each word before transmitting it.
- If the word is 8 bit then, the MSB is generally used as parity bit and remaining 7 bits are used as message/data bit.
- The parity of transmitted bit can be even parity or odd parity depending upon the type of parity required.
- Even parity means number of 1's in the given word including the parity bit should be even.
- Odd parity means number of 1's in the given word including the parity bit should be odd.

0	1001011

1	1001010

Fig: Even Parity

1	1001011

0	1001010

Fig: Odd parity

- The receiver detects an error if the parity of received codeword is different from the expected parity. i.e. if the codeword is transmitted with an even parity, but if the received codeword has an odd parity then the receivers can conclude that the received codeword is not correct. In such case the receiver will ignore the received codeword and request for retransmission of same from transmitter.

0	1001011

Transmitted code with even parity

0	**0**001011

Received code with on error(but now the parity is odd)

- However if the number of errors introduced in the transmitted code is two or any even numbers, then the parity of received code will not change. In this case, this technique will fail to detect error.

0	1001011

Transmitted with even parity

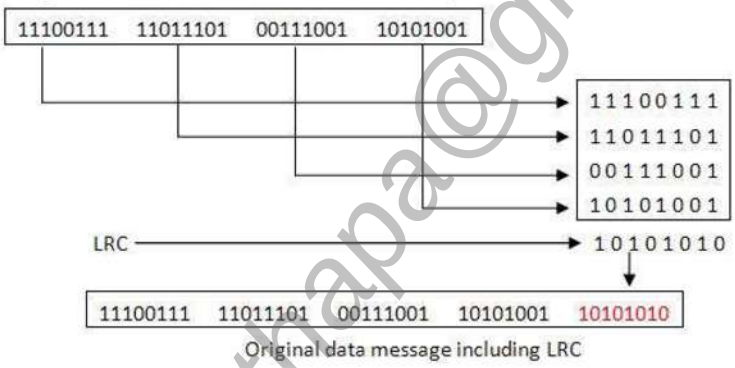
0	**0**001010

Received code with two error(Still the parity is even)

Two Dimensional Parity Check

- One of the way to overcome the problem of simply parity is to use two dimensional parity check.
- In this technique, the parity bits are produced for each row and columns on block of data.
- When large number of binary words are being transmitted or received in succession, the resulting collection of bits is considered as block of data.
- The two set of parity bits so generated are known as
  - i. Longitudinal redundancy checks(LRC) bit

    The LRC indicate the parity of rows. The LRC bits are parity bit associated with the rows of data block. Each LRC bit will make the parity of corresponding row, an even parity. Here a block of bits is organized in the form of a list as rows. If we want to send 32 bits then we arrange them in list of four rows each of 8 bits. Then parity for each columns is calculated and a new row of eight bits is created. These become the parity bits for the whole block. Figure below demonstrate this concept.



  - ii. Vertical redundancy checks(VRC) bit / Simple Parity Check

    A VRC also known as **parity check** is a simple technique which consist of adding a single bit called parity bit to the end of each word before transmitting. The VRC indicate the parity of columns. The VRC bits are parity bit are associated with the columns of data block. Each VCR bit will make the parity of corresponding column, an even parity. It can detect all single bit error as well as burst error if the total number of bits changed is odd.

Example: The following bit stream is encoded using VRC and LRC and even parity. Locate the error and correct the error if present.

11000011 11110011 10110010 00001010 00101010 00101011 10100011 01001011 11100001

Solution: word1 word2…… word9

1	1	0	0	0	0	1	1
1	1	1	1	0	0	1	1
1	0	1	1	0	0	1	0
0	0	0	0	1	0	1	0
0	**0**	**1**	**0**	**1**	**0**	**1**	**0**
0	0	1	0	1	0	1	1
1	0	1	0	0	0	1	1
0	1	0	0	1	0	1	1
1	1	1	0	0	0	0	1

In the above figure, we see that the parity bits corresponding to row 5 and column 1 indicates wrong parity. Therefore, the first bit in the fifth row is incorrect.
However, if two bits in one same data word are damaged, and two bits on exactly positions in another data word are also damaged then. LRC checker will also not be able to detect an error.

Check Sum

- It is a kind of two dimensional parities which can detect two or even number of errors within the same word.
- It provides error detection i.e. flipped bits in transmitted packet.
- It is based on redundancy.
- Many computer network send a check sum along with each packet to help receiver to detect error.
- Is capable of detecting all error, odd as well as most of errors having even no of bits.
- But if one or more bits of a segment and the corresponding bit or bits of opposite value in the second segment are also damaged, the sum of these columns won't change hence the receiver wont detect the problem.

Working principle

- On sending side, data units are divided into equal segments of n bits.
- Segments are added.
- Perform the 1's complement of the sum and appended to the end of the message as redundancy bit in checksum filed.
- Extended data is sent.
- On receiving end, all the segments including checksum value is added.
- Perform the 1's complement of the sum.
- If 1's complement of sum is zero, then the message is said to be error free otherwise erroneous.

Example: Given original message: 1010100100111001.
Dividing the data word into segments of 8bits: 10101001 00111001
Adding the segments

```
  10101001
+ 00111001
----------
  11100010      (Note: if carry discard it)
```

Now 1's complement of the sum is 00011101
Therefore, the message to be sent is 10101001 00111001 00011101

At destination side,
If the message is received error free then, received message =10101001 00111001 00011101
Add the segments including checksum value

```
  10101001
  00111001
+ 00011101
----------
  11111111
```

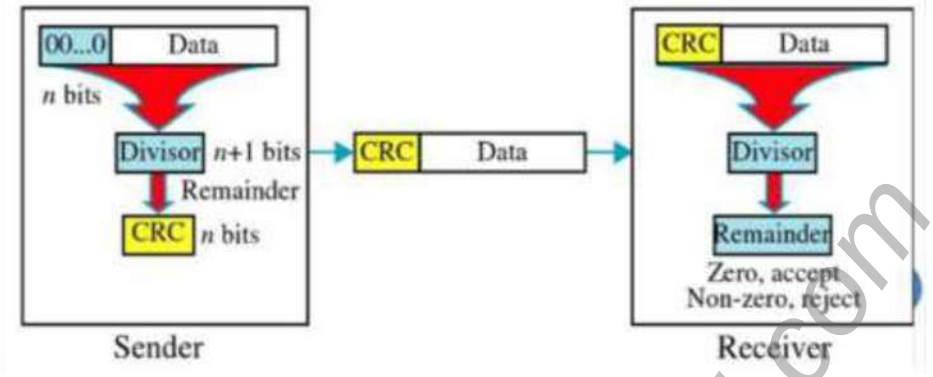
1's complement of the total is 00000000, thus this is error free message.
But, suppose first, second and fourth bit of the received message were flipped. Then received message = 01111001 11101001 00011101
Now, adding the segments

```
  01111001
  11101001
  00011101
----------
 101111111
 ↑
```

Discard

1's complement of the sum is 10000000, so this is erroneous message.

CRC



- One of the most widely used error detection technique is Cyclic redundancy check.
- It is a type of polynomial code in which bit strings is represented in the form of polynomial with coefficient 0 and 1 only.
- Polynomial arithmetic uses modulo-2 arithmetic i.e. and addition and subtraction are identical to EXOR.
- For CRC code, the sender and receiver should agree upon a generator polynomial G(x) which is a divisor.
- CRC is based on binary division. A codeword can be generated for a given data word polynomial M(x) with the help of long division.
- A sequence of redundant bits called CRC remainder is appended at the end of data word.
- A CRC is valid if and only if it is exactly one bit less than divisor and appending the CRC to the end of the data word result in bit sequence which is exactly divisible by divisor.
- The resulting data word unit after adding CRC remainder become exactly divisible by another predetermined binary number.
- At the receiver, this data word is divided by the same binary number.
- There is no error, if this division doesn't yield any remainder but a non-zero remainder indicated presence of errors in the received data word. Such an erroneous data word is then rejected.

Procedure to obtain CRC

i. Divide the data unit by a predetermined divisor.
ii. Obtain the remainder. It is required CRC

CRC generator

i. Append n zeroes to the data unit where n is 1 less than the number of bits in the predefined divisor(n+1) bit.
ii. Divide the newly generated data unit in step I by the divisor. This is a binary division.
iii. The remainder obtained after the division is the n bit CRC.
iv. This CRC will replace the n zeroes to the data unit in step I, to get the codeword to be transmitted.

CRC checker

i. The receiver divides the received code word by same (n+1) bit divisor which was used at transmitter.
ii. If the remainder (also called as syndrome) of this division is zero, then the received codeword is considered as error free otherwise it is considered as presence of error hence it is rejected.

Example:

A message $M(x) = X^7 + X^4 + X^3 + X^2 + 1$ is transmitted using the standard CRC method. The generator polynomial is $x^3 + 1$. Show the actual bit string transmitted. If the received data unit is received without any error, show how this is detected at the receiver. Again suppose the third bit from left is inverted during transmission. Show how this error is detected at the receiver end.

Solution:

Given Message $M(X) = X^7 + X^4 + X^3 + X^2 + 1$ i.e. 10011101

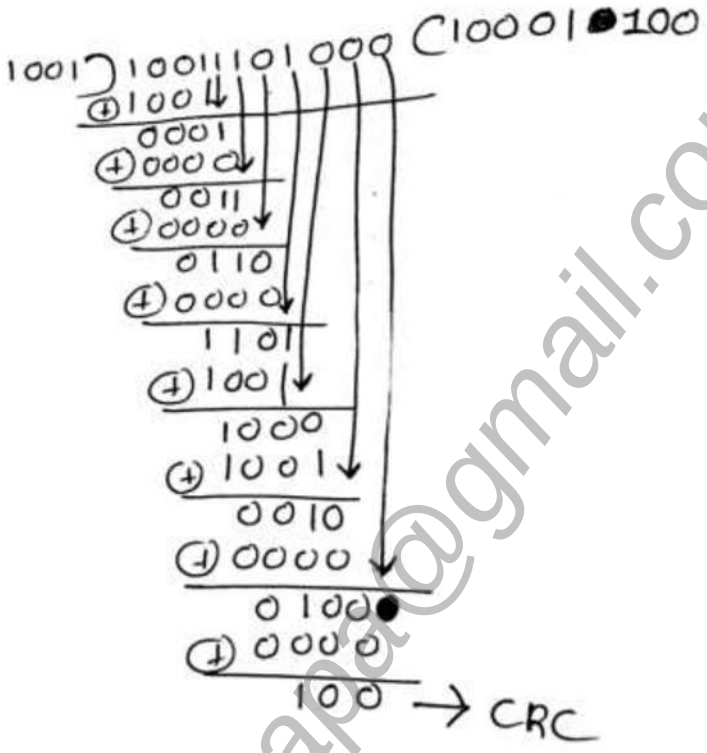
Generator Polynomial $G(X) = X^3 + 1 = 1001$(divisor)

First we obtain the dividend.

Dividend = data word + 3 zeroes

= 10011101000

Then , we carry out the division.



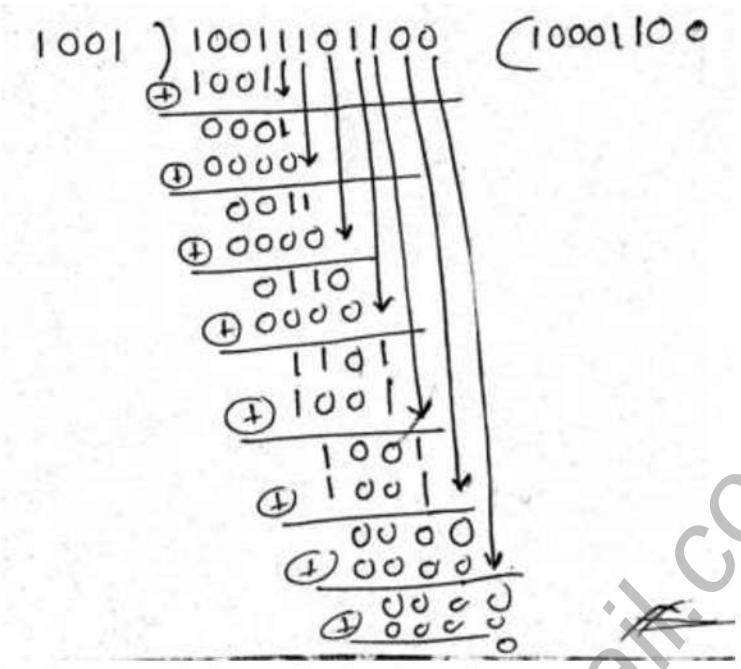
Now we obtain the codeword to be actually transmitted. This is obtained by writing the data word followed by remainder i.e.CRC as given below

Transmitted word = 10011101100

Now if the received word is exactly same as it is transmitted then

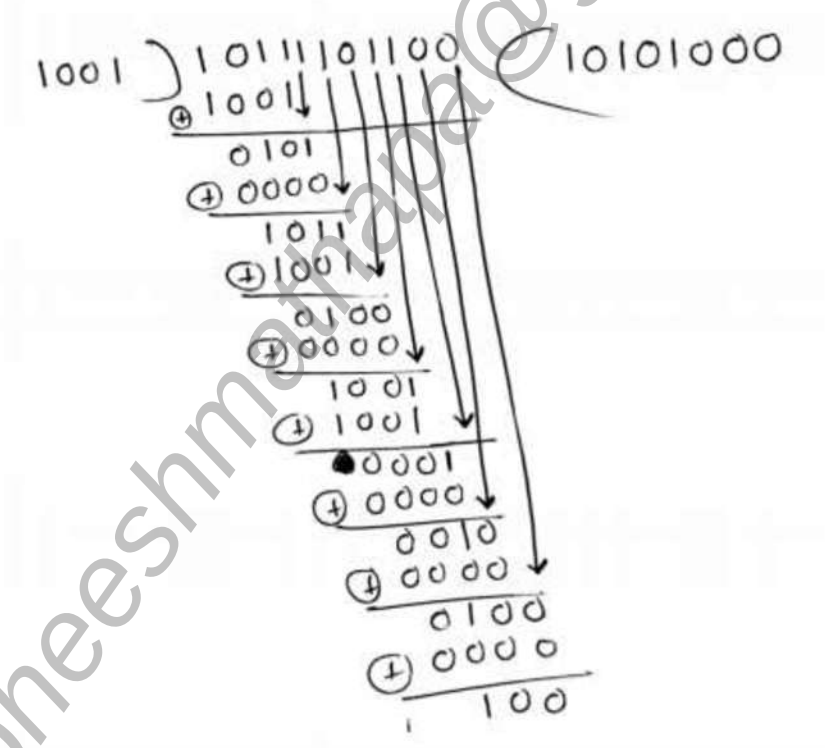
Received word = 10011101100

At the receiver, the received word is divided by the same divider used at transmitter i.e. 1001



A zero reminder indicates that there is no error in the received codeword.
Again, we are supposed to invert the third bit in the received codeword then we get
Received codeword = 10111101100

Now performing, the division by same divisor used at transmitter i.e. 1001 we get



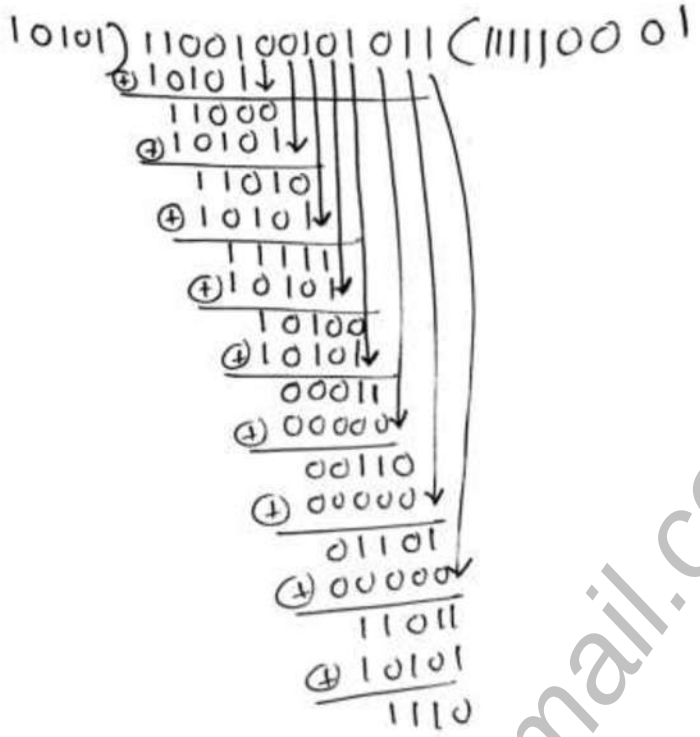
A non-zero remainder indicates that there is error in the received codeword.

A codeword is received as 1100100101011. Check whether there are errors in the received codeword, if the divisor is 10101.

Solution:

Here Data word= **1100100101011**

Divisor = 10101



Since there is a non-zero remainder, it shows that there are errors in the received codeword.

Hamming Code

- Hamming code is linear block code which is a single bit correction method using redundant bit or parity bit.
- For any integer p, there is 2^P -1bit hamming code in which P bits is parity bit and 2^P -1-P bits are data bit.
- Number of parity bit is identified with the following formula

$$2^P \geq D + P + 1$$

Where D is the number of data bits and P is the number of parity bits.

- Consider a message having four data bits (D), then this is transmitted as a 7-bit code word by adding three 3 error control bit or parity bit. This would be called (7,4) hamming code.
- The rule for generating code word in hamming code is
  1. "If we number the bit position from 1 to 2^m -1, the bits 2^k, where $0 \leq k \leq m-1$, are parity bits, and the bits in the remainder position are information bits."
     Example: A 7-bit hamming code is as follows

D	D	D	P	D	P	P
7	6	5	4	3	2	1

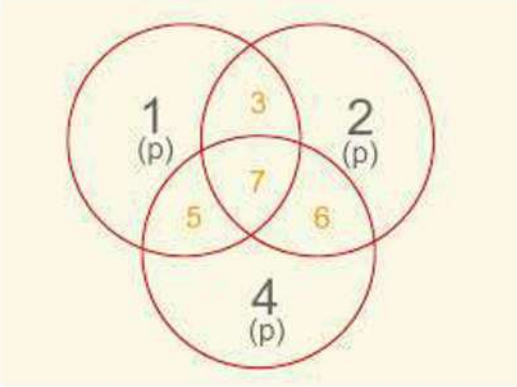
A 15-bit hamming code is as follows

D	D	D	D	D	D	D	P	D	D	D	P	D	P	P
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

D = Data bits
P= Parity bits

  2. P1 sets parity for bits (1,3,5,7) , p2 for bits(2, 3, 6, 7) and p4 for bits (4,5,6,7)
     Note: for p1: check 1 bit, skip 1 bit and so on
     For p2: check 2 bit, skip 2 bit and so on
     For p4: check 4 bit, skip 4 bit and so on.
- For finding and correcting a bad bit:
  1. Check the bits (1,3,5,7, 9, 11,13…), (2,3,6,7, 10, 11…..), (4,5,6,7,12, 13, 14, 15……), (8, 9, 10, 11, 12, 13, 14, 15, 24, 25, 26, 27, 28, 29, 30, 31)…..etc
     Note: for 7 bit hamming code simply check (1, 3, 5, 7), (2, 3, 6, 7) and (4, 5, 6, 7).
  2. If the retrieved group possess even parity, then the received code word is correct but if the parity is not even then received code word is erroneous.

3. This error can be located by forming a three-bit number out of three parity checks.



- The error detection is possible when the number of transmission error in a code word is less than the minimum hammin distance i.e. up to 2 bits' error for because then the erroneous word is not a **valid** code word.

Numerical:

- Write the steps to generate hamming code. Prepare hamming code for the bit pattern 1010. Suppose while transferring, error occurs in 7th bit, write the bit pattern at the receiver. Using hamming code, explain how will you detect and correct the error.

Solution: The 7-bit hamming code word format is

1	0	1	P	0	P	P
D7	D6	D5	P4	D3	P2	P1

Data bit = 1010

Parity bit =?

Now we have to decide p1, p2 and p4

- P1 sets the parity for bits(1,3, 5,7) so p1=0 so as to have even parity in this bit group.
- P2 sets the parity for bits (2,3, 6,7) so p2=1 so as to have even parity in this bit group.
- P4 sets the parity for bits (4,5,6,7) so p4=0 so as to have even parity in this bit group.

So our code word to be transmitted become

1	0	1	0	0	1	0
D7	D6	D5	P4	D3	P2	P1

i.e. **10110010**

if the received code word consists of error in 7th bit, then the received code word becomes **0**0110010

0	0	1	0	0	1	0
D7	D6	D5	P4	D3	P2	P1

so for detecting and correction this error we perform the following task.

- Analyse the bits (4, 5, 6, 7): Here we see odd parity i.e. error exist here so, we set P4=1
- Analyse the bits (2, 3, 6, 7): Here we see odd parity i.e. error exist here so, set p2 = 1
- Analyse the bits (1, 3, 5, 7): Here we see Odd Parity i.e. error exists so, set P1 = 1.

so the error word, E is

P4	P2	P1
1	1	1

The decimal equivalent of error word is $(111)_2 = (7)_{10}$, hence 7th bit in the received code word is in error. So inverting the incorrect bit to obtain the correct code word we get

Correct code word = **10110010**

- A 7-bit hamming code is received as 1110101. What is the correct code?
  Solution:

  The 7-bit hamming code word format is

1	1	1	0	1	0	1
D7	D6	D5	P4	D3	P2	P1

  Data bit=1111
  Parity bit=001

  So for detecting and correction this error we perform the following task.
  - Analyse the bits (4, 5, 6, 7): Here we see odd parity i.e. error exist here so, we set P4=1
  - Analyse the bits (2, 3, 6, 7): Here we see odd parity i.e. error exist here so, set p2 = 1
  - Analyse the bits (1, 3, 5, 7): Here we see even Parity i.e. No error exists so, set P1 = 0

  so the error word is

P4	P2	P1
1	1	0

  The decimal equivalent of error word is $(110)_2 = (6)_{10}$, hence 6th bit in the received code word is in error. So inverting the incorrect bit to obtain the correct code word we get

  Correct code word = 1010101
  Sixth bit inverted

Assignment:
If the 7 bit hamming code word received by a receiver is 1011011. Assuming the even parity, state whether the received codeword is correct or wrong. If wrong, locate and correct the error.

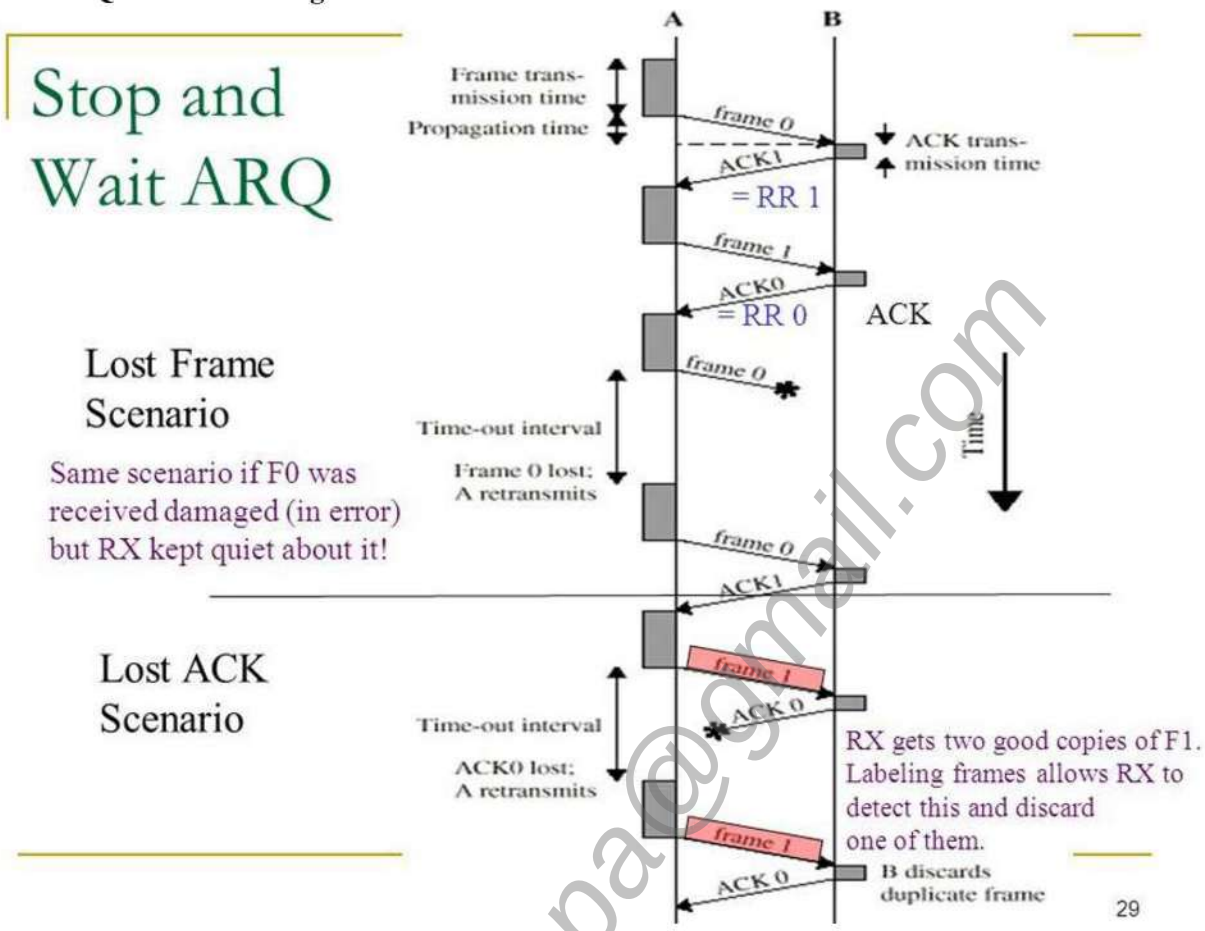
Error Control

- Error control refers to mechanism to detect and correct errors that occur in the transmission of frame.
- There are two types of error.
  1. Lost frame: Transmitted frame doesn't arrive at the destination.
  2. Damaged frame: A recognized frame does arrive, but some of the bits are in error.
- The most common error control are based on the following steps.
  1. Error detection: finding the error during transmission of frames.
  2. Positive acknowledgement: The destination returns positive acknowledgement to successfully received error free frame.
  3. Negative acknowledgement: The destination return a negative acknowledgement to a frame in which an error is detected. The source simply retransmits such frame.
- Collectively, these mechanism is called as automatic repeat request (ARQ).

- Three versions of ARQ have been standardized.
  1. Stop and wait ARQ / one-bit sliding window
  2. Sliding window ARQ
     a. Go- Back-N ARQ

b. Selective Repeat ARQ

1. Stop and Wait ARQ / One-bit sliding window



- This protocol is also called as on bit sliding window protocol because the maximum window size here in 1.
- In this technique, when the source entity transmits a frame it waits for acknowledgement.
- No other data frames can be send until the destination station reply arrives at the source station.

Two problem can occur

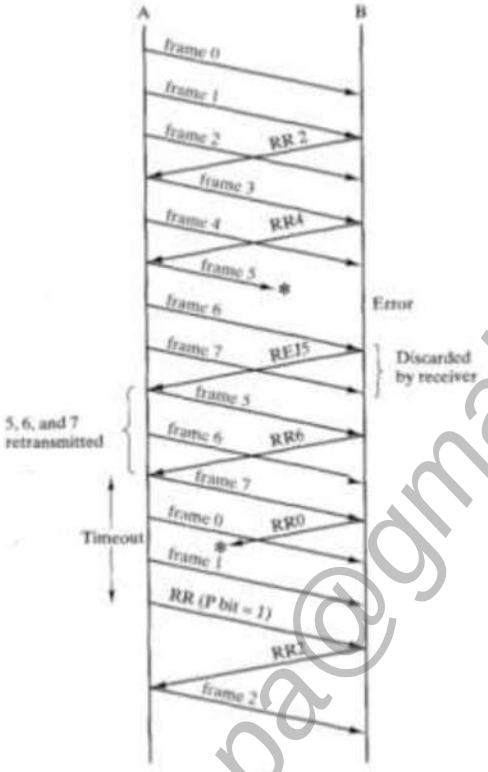
1. Damaged Frame/ lost frame
   - In case of Damaged Frame, a recognized frame does arrive, but some of the bits are in error. The receiver can detect this by using different error detection technique and simply discards such frame.
   - Similarly, if, the frame is lost i.e. receiver doesn't receive transmitted frame, the source is again waiting for an acknowledgement.
   - The source station should have a timer, after the frame is transmitted, the source station waits for an acknowledgement.
   - If no acknowledgement is received by the time the timer expires, then same frame is sent again.
   - In the above figure frame 0 is damaged, /lost so destination station quit it and hence is retransmitted.

2. Damaged or Lost acknowledgement:
   - In this case the frame sent by source station is received correctly by destination station.
   - The destination then responds by sending acknowledgement ack.
   - The acknowledgement ack is damaged and is not recognized by the source station or is Lost, which will therefore timeout and resend the same frame again. For this, the sender sets a timer for every frame it sends. If it doesn't receive and acknowledgement from the receiver before the timer expires, it sends the frame again with new timer.
   - So duplicate frame arrives at the destination station.
   - To preventing the destination station collection, duplicate frames, each frame are alternately labelled with o and 1 and positive acknowledge are of the form ack0 and ack1.

- The main problem with this method is that, since sender must receive each acknowledgement before it can transmit next frame, it makes transmission very slow.

2. Sliding window protocol

i. Go-Back-N ARQ

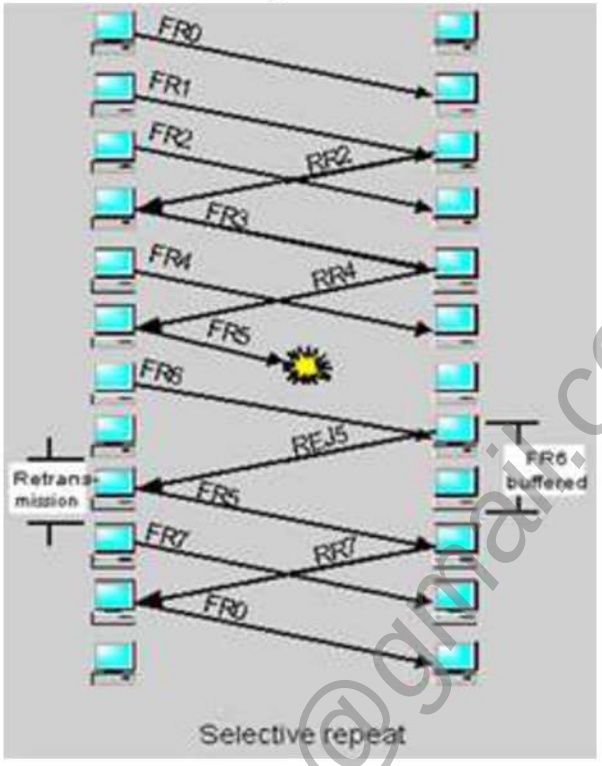


- In this method, source can send a series of frames of some maximum limit i.e. window size without waiting for acknowledgement.
- The numbers of unacknowledged frames are determined by the window size W using sliding window flow control technique.
- Thus destination station can accept W frame and sender is allowed to send W frames without acknowledgement.
- While no error, if a frame with sequence number N is received correctly and is in order, the receiver sends positive acknowledge (RR: Receive Ready) for that frame with next frame sequence number.
- But if the destination station detects an error in a frame
  1. It sends negative acknowledgement (Rej: Reject) for that particular frame.
  2. It discards that frame and the entire future incoming frame until that frame in error is correctly received.
  3. Thus when the source station, receive a negative acknowledgement, it must retransmit the frame in error plus all the succeeding frame that were transmitted before.
- Also, sometime there is a situation that sender has transmitted a frame and waiting for an acknowledgement that might be lost on the way. In this case, the receiver neither send RR nor REJ. Since the sender sets a timer for every frame it sends. If it doesn't receive any acknowledgement from the receiver before the timer expires, it sends the RR frame that includes a bit called P bit which is set to 1. When receiver receive RR frame with P bit set to 1, it acknowledges the sender by RR acknowledge with sequence number i of the frame that it expects. Now upon receiving RR i , the source resends frame starting at i.

ii. Selective Repeat ARQ

- With this technique only that frame from the source station to destination station is again retransmited which has received negative acknowledgement.
- It is more efficient than go back N ARQ because it minimizes the amount of retransmission.

- On the other hand, the receiver must maintain a buffer large enough to save post-REJ frames until the frame in error is retransmitted, and it must contain logic for reinserting that frame in the proper sequence.
- The transmitter, too, requires more complex logic to be able to send a frame out of sequence. Because of such complications, select-reject ARQ is much less used than go-back- N ARQ.



Multiple access protocols

- The upper layer called logical link control of datalink layer is responsible for flow and error control and the lower sublayer of data link layer called media access control is responsible for multiple access resolution.
- Multiple access protocols define how to coordinate the access of multiple sending and receiving node to a shared broadcast channel.
- Multiple access protocols can be classified as **channel partitioning protocols** (FDM and TDM) and **Random access protocols.**
- Random access protocols / Contention is a media access method that is used to share a broadcast medium. in which, any computer in the network can transmit data at any time. This system breaks down when two computers attempt to transmit at the same time. **This is a case of collision. Random access protocol defines mechanism how to recover from this collision.**
- **Some of them random channel access protocols or channel allocation techniques** are

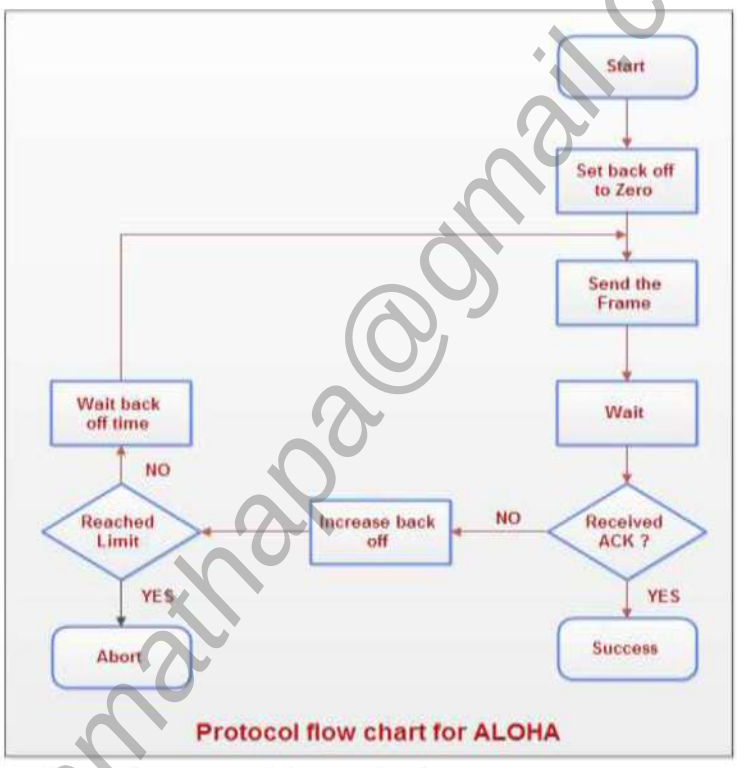
a. ALOHA

1. Pure Aloha

- **Aloha means "Hello".** Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision
- It works on very simple principle. It allows for any station to broadcast at any time. This protocol allows every system to send a frame if it is ready to send. The station then listens for an amount of time equal to the maximum possible RTT (Round Trip Time). RTT is the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgment of that signal to be received.
- If received acknowledgement, then ok otherwise retransmit it. If no acknowledgement after some numbers of repeated transmission, then give up.

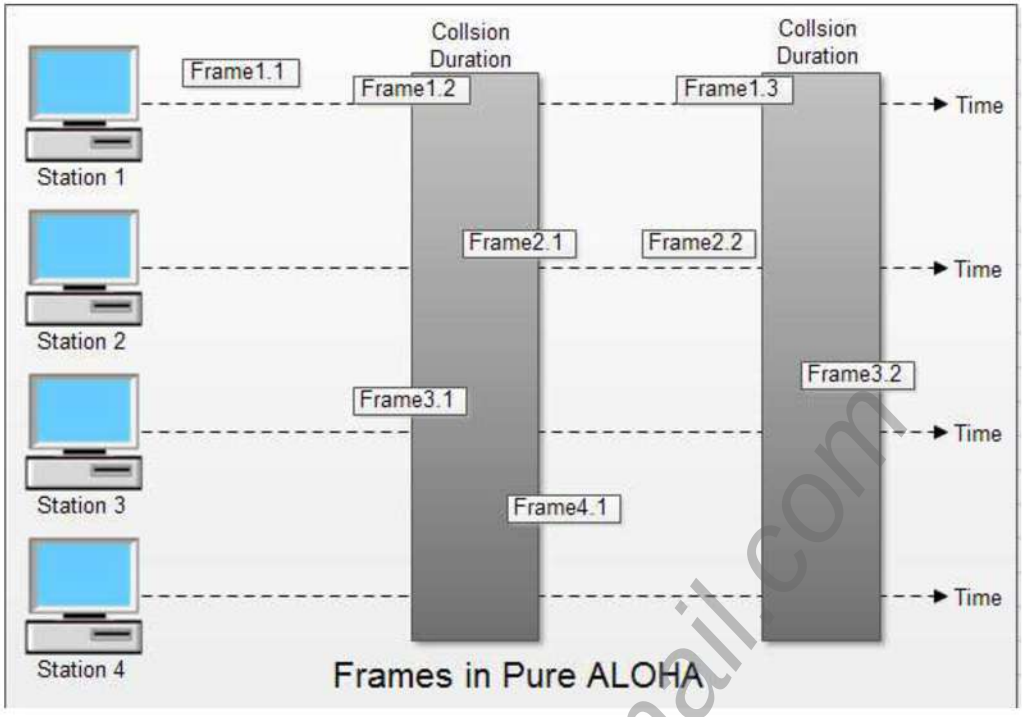
- A receiving station uses a frame check sequence to determine the correctness of an incoming frame. If the frame is valid the station immediately sends an acknowledgement.
- If the frame is damaged by the noise or collision, the receiver determines the frame is invalid and ignores the frame.
- The sender station waits for a random amount of time and then sends the frame again.
- The process continues till the node has send all the frames.
- Since the nodes send their frames without sensing the medium, there is high probability of collisions to occur.
- The maximum success rate can be achieved with aloha protocol is 18% only.

Flow Chart for Aloha



Note: Back off limit determine the number of times the retransmission can be done.

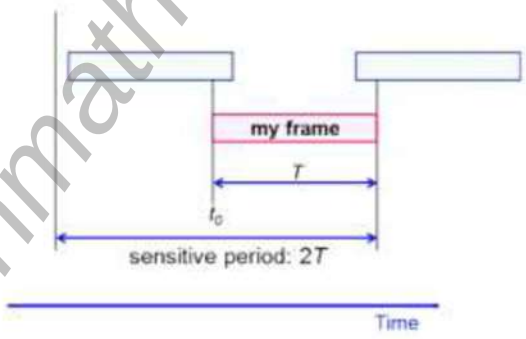
Collision in Aloha



• In above fig, there are four stations that contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 3.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

Efficiency



- For a success, no other transmission should start in twice the frame length period
- Maximum throughput is 18%

2. Slotted Aloha

In ALOHA, a packet transmission can begin at any time. Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high. • In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.

This method requires synchronization between sending nodes where transmission is permitted to begin only at slot boundary to prevent collision. In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time

slot. In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in below figure.

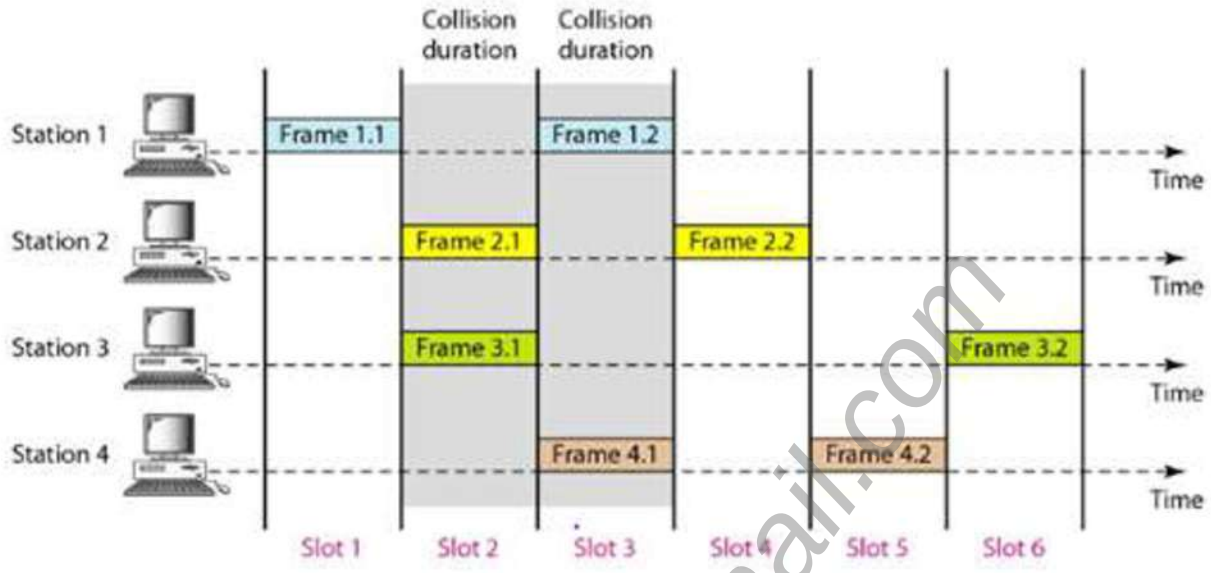
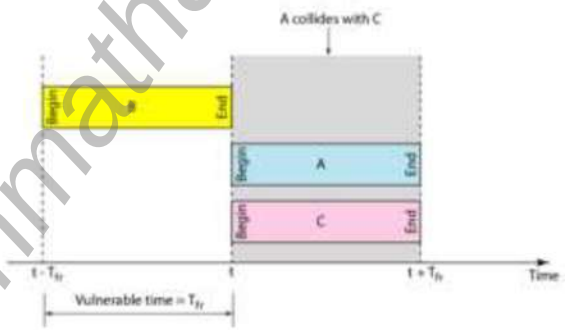


Fig: Frames in Slotted Aloha

In the above figure, only frame 1.1, frame 2.2, frame 4.2 and frame 3.2 survived collision. Remaining frames are destroyed.

Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half. The maximum channel utilization is only 37%.

Efficiency



Sensitive(vulnurable) time decreased from 2T to T thereby increasing the maximum throughput to 36%

b. CSMA (Carrier sense multiple access)

- CSMA is probabilistic media access control in which a node verifies the absence of other traffic before transmitting on a shared transmission medium such as an electronic bus or a band of the electromagnetic spectrum.
- Carrier sense means that a transmitter wishing to transmit listens for clear medium to determine whether another transmission is in progress before initiation a transmission.
- If a carrier is sensed, the transmitter must wait for the transmission in progress to finish before initiating its own transmission.

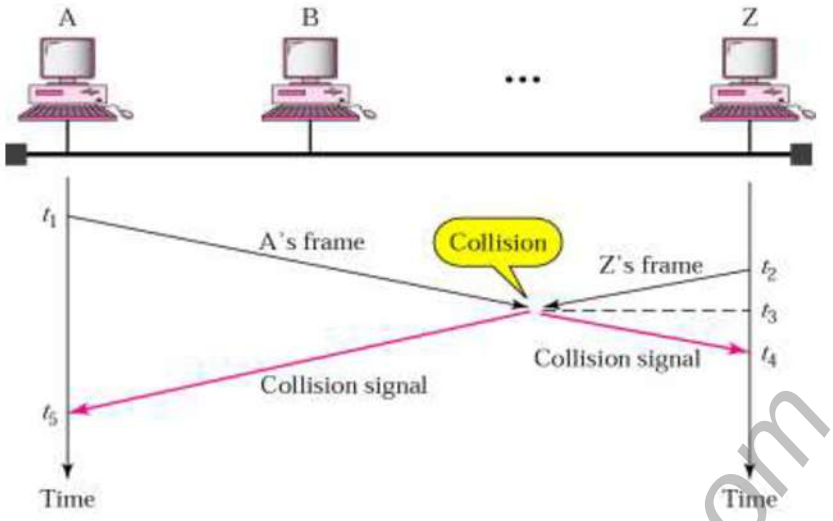
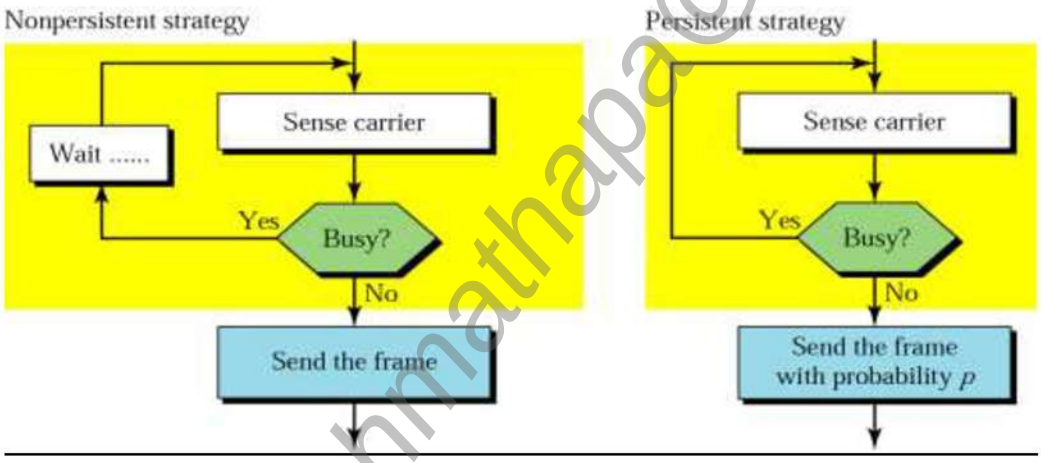


Fig: CSMA collision

- Multiple access means that multiple station sent and receive on the medium.
- CSMA is based on the principle "Sense before transmit". It can reduce the probability of collision but not totally eliminate the collision.

Strategies

1. Persistent and non-persistent



- In non-persistent strategy, a station wishing to transmit listens to the medium and then, if the channel is idle, it starts transmitting the data otherwise if the channel is busy, it waits for random amount of time and repeats the process.=.
-
- In persistent strategy, a station wishing to transmit listens to the channel and then, if the channel is idle, it starts transmitting the data otherwise if the channel is busy, it senses the medium continuously until the channel become idle, then transmit the message. It is used in CSMA/CD system.

c. Carrier Sense Multiple Access/Collision Detection(CSMA/CD)

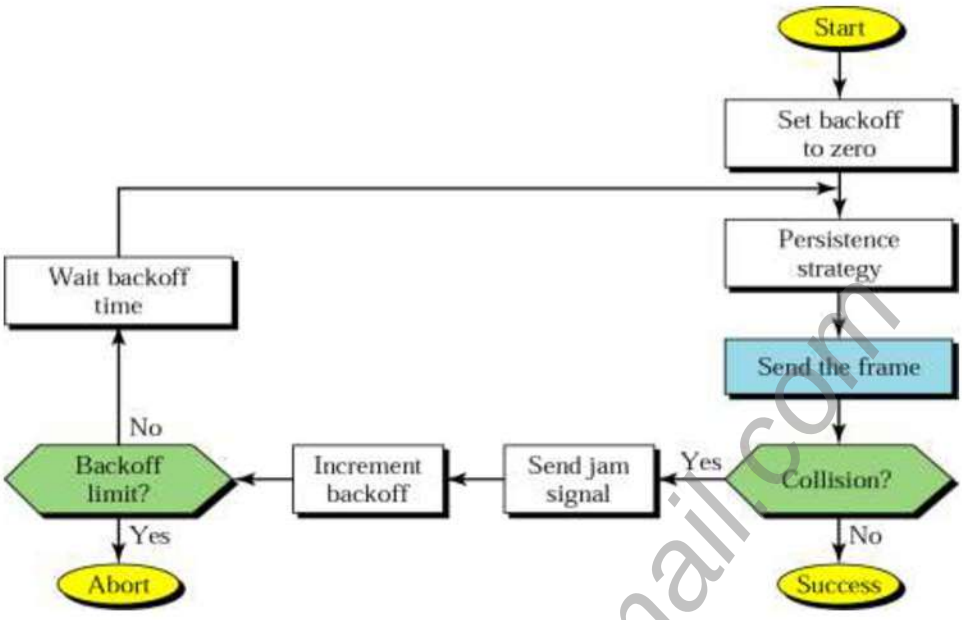


Fig: CSMA/CD

- When the multiple nodes send data at the same time on the shared channel, a collision occurs.
- To avoid this, CSMA/CD forces the nodes to listen to the channel before transmission.
- It is the modification of pure CSMA and used to improve CSMA performance by terminating transmission as soon as collision is detected, thus shorting the time required before a retry can be attempted.
- CSMA/CD adds a procedure to handle a collision as follow.
  1. If the channel is idle, the device that want to send data can do so. The sender then continues to listen to make sure that sending the data didn't cause the collision.
  2. If the channel is busy, continue to listen until the channel is idle and then transmit immediately.
  3. If a collision is detected during the transmission, both the senders will send a Jam signal instead of data frame over the channel. The jam signal indicates to all other devices in the channel that there has been collision and they shouldn't send data on the channel. The indication of collision can be determined by the noise created by the collision itself.
  4. After sending the jam signal, wait for a random amount of time before beginning the entire process over.

d. Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA)

- The performance of pure CSMA is improved by modifying CSMA to be less greedy on the channel, which results CSMA/CA.
- It tries to avoid collisions before they happen rather listen and detect the collisions.
- Carrier sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle".
- When they do transmit, nodes transmit their packet data in its entirety.
- A station wishing to transmit has to listen the channel for a predefined amount of time so as to check for activity in the channel.

When the channel is clear, a station sends a signal telling all other stations not to transmit and then sends its data

IEEE standard 802 for LANs (Ethernet)

i. 802.3(Ethernet):

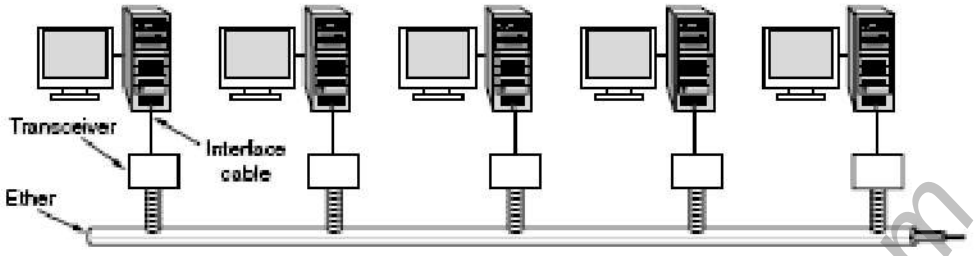


Fig: Architecture of the original Ethernet

- The IEEE 802.3 standard defines a network derived from the Ethernet network.
- This standard defines the characteristics related to MAC sub layer of the data link layer and the OSI physical layer.
- The Ethernet is a popular LAN technology that uses CSMA/CD access method over the variety of cables types.
- In traditional Ethernet the data rate was 10Mbps
- Now fast Ethernet (100Base –T, 100Base-TX, 100Base-FX) operates at 100Mbps and Gigabit Ethernet (1000Base-SX, 1000Base-LX, 1000Base-CX, 1000Base-T) operates at 1Gbps.
- 1000BASE-X is used in industry to refer to Gigabit Ethernet transmission over fiber, where options include 1000BASE-SX, 1000BASE-LX, 1000BASE-CX.
- 1000BASE-T is a standard for Gigabit Ethernet over copper wiring.1000BASE-T network segment can be a maximum length of 100 meters (330 feet), and must use Category 5 cable or better (including Cat 5e and Cat 6).
- 100Base-Tx is simply an extension of 100Base -T.
- We use four types of cable as interface cable which are thick coax (10Base5), thin coax (10Base2), twisted pair(10Base-T) and fiber optics (10Base-F).

Advantage:

- Widely used at present.
- Simple protocol, new computers can be added without bringing the network to down.
- Almost zero delay at low load, no need to wait for token, we can transmit when ready.

Disadvantage:

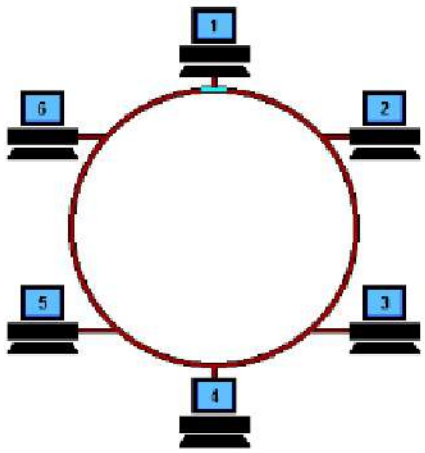
- Addition technique necessary for carrier sense and collision detection.
- Poor performance at high load as there can be lots of collisions.
- Doesn't guarantee the delivery time due to possibility of repeated collisions.

ii. 802.4(Token bus)

- IEEE802.4 standard describes a network with a bus physical topology that controls media access with a token mechanism i.e. Token bus is a network implementing the token ring protocol over a "virtual ring" on a coaxial cable.
- A token is passed around the network nodes and only the node possessing the token may transmit.
- If a node doesn't have anything to send, the token is passed on to the next node on the virtual ring.
- Each node must know the address of its neighbour in the ring, so a special protocol is needed to notify the other nodes of connections to, and disconnections from, the ring.
- This standard was designed to meet the need of industrial automation systems but has gained little popularity.

- Due to difficulties handling device failures and adding new stations to a network, token bus gained a reputation for being unreliable and difficult to upgrade.

iii. 802.5(token ring)

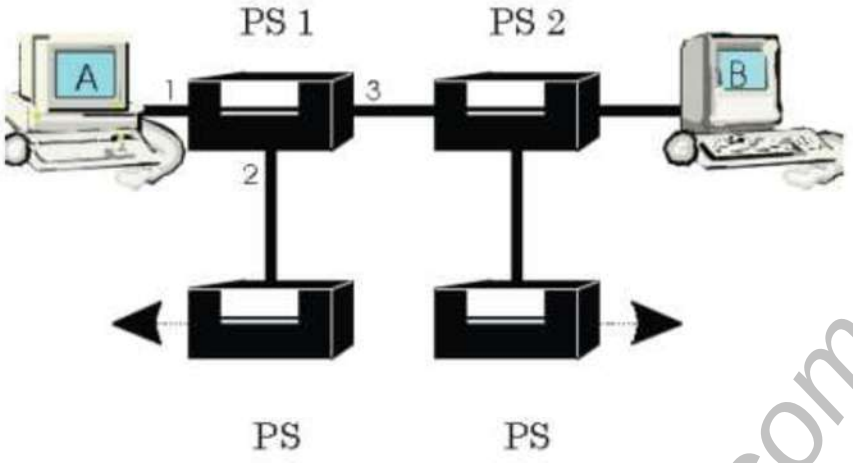


- IEEE802.5 standard describes a network with a **ring topology** and **token** based media access control
- Initially used only in IBM computers, it was eventually standardized with protocol **IEEE 802.5**.
- The data transmission process goes as follows:
  - Empty information frames are continuously circulated on the ring.
  - When a computer has a message to send, it seizes the token. The computer will then be able to send the frame.
  - The frame is then examined by each successive workstation. The workstation that identifies itself to be the destination for the message copies it from the frame and changes the token back to 0.
  - When the frame gets back to the originator, it sees that the token has been changed to 0 and that the message has been copied and received. It removes the message from the frame.
  - The frame continues to circulate as an "empty" frame, ready to be taken by a workstation when it has a message to send.

Virtual Circuit Switching

- A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.
- A virtual circuit (VC) consists of
  1. A path (i.e., a series of links and packet switches) between the source and destination hosts
  2. Virtual circuit numbers, one number for each link along the path
  3. Entries in VC-number translation tables in each packet switch along the path.
- Once a VC is established between source and destination, packets can be sent with appropriate VC number.
- Packets arrive at the destination in the correct sequence, and it is guaranteed that essentially there will not be errors.
- This approach is slower than Circuit Switching, since different virtual circuits may compete over the same resources, and an initial setup phase is needed to initiate the circuit.
- As in Circuit Switching, if an intermediate node fails, all virtual circuits that pass through it are lost.
- If a network employs virtual circuits, then the network's switches must maintain state information for the ongoing connections.
- Virtual circuits can be either permanent, called Permanent virtual Circuits (PVC), or temporary, called Switched Virtual Circuits (SVCs).
- A Permanent Virtual Circuit (PVC) is a virtual circuit that is permanently available to the user. A PVC is defined in advance by a network manager. A PVC is used on a circuit that includes routers that must maintain a constant connection in order to transfer routing information in a dynamic network environment.
- A switched virtual circuit (SVC) is a virtual circuit in which a connection session is set up dynamically between individual nodes temporarily only for the duration of a session. Once a communication session is complete, the virtual circuit is disabled.

- The most common implementation of Virtual Circuit networks are **X.25, Frame Relay and ATM.**



- In the above figure, suppose A request that the network establish VC between itself and node B. Supposes the network chooses the paths A-PS1-PS2-B and assigns VC number 12, 22, 32 to three link in a path. Then when a packet as a part of this VC leaves host A, the value of the VC number field is 12, when it leaves the PS1, the value is 22 and when it leaves PS2, the value is 32. The number next to the link of PS1 are the interface number. Each packet switch has a VC number translation table. The VC number translation table in PS1 can be like in below figure . The PS must maintain VC number and each time a connection is released, the entry is removed from the table.

Incoming Interface	Incoming VC#	Outgoing Interface	Outgoing VC#
1	12	3	22
2	63	1	18
3	7	2	17
1	97	3	87
...	...	...	...

Datagram Packet Switching Vs Virtual-circuit Packet Switching:

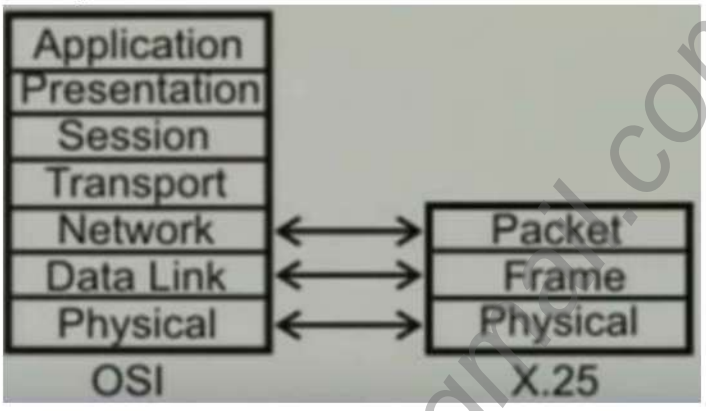
sno	Datagram Packet Switching	Virtual-circuit Packet Switching
1	Two packets of the same user pair can travel along different routes.	All packets of the same virtual circuit travel along the same path.
2	The packets can arrive out of sequence.	Packet sequencing is guaranteed.
3	Packets contain full Src, Dst addresses	Packets contain short VC Id. (VCI).
4	Each host occupies routine table entries.	Each VC occupies routing table entries.
5	Requires no connection setup.	Requires VC setup. First packet has large delay.
6	Also called Connection less	Also called connection oriented.
7	Examples: X.25 and Frame Relay	Eg. Internet which uses IP Network protocol.

Virtual Circuit Network

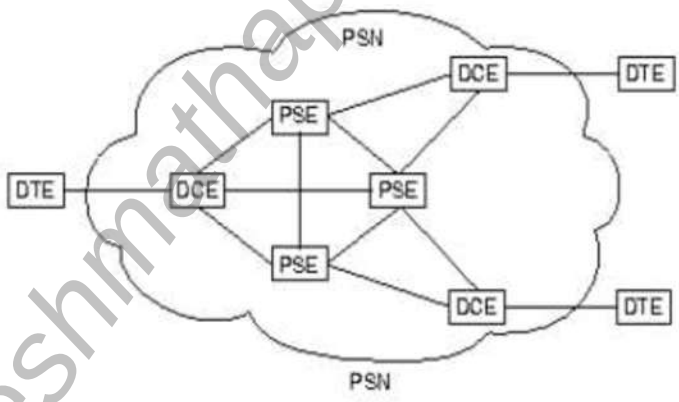
- The most common implementation of virtual circuit network are X25, Frame relay and ATM

1. X.25

- TheX.25 is a connection oriented packet switched WAN protocol.
- This means to use X.25, a computer first establishes connection to the remote computer called virtual circuit.
- The resulting virtual circuit is identified by the channel number.
- Data packets labelled with the channel number are delivered to the corresponding destination address.
- Data packets were very simple consisting of three-byte header (because it consists of three layer named physical, datalink and packet) and up to 128 bytes of data.



- The header consists of 12-bit connection number and a packet sequence number and acknowledgement number and a few miscellaneous bits.
- X25 provided low data transmission rate of 64kbps. Because X25 has extensive error control and flow control in both data link layer and packet layer. This was so because X.25 was designed in the 1970s, when the available transmission media were more prone to errors.



- DTE is Data Terminal Equipment such as computers and terminals at the customer premises and DCE is data communications equipment, such as X.25 packet switches.
- X.25 define three layers of protocol. The physical layer protocol specifies electrical interface. The data link layer protocol is designed to deal with transmission errors, flow control, establishing and termination connection etc. The packet layer protocol deals with addressing and packet switching.
- The X.25 support both switched virtual circuit(SVC) as well as Private virtual circuit(PVC).
- Presently, it is used for networks for ATMs and credit card verification.

Frame Relay

- Frame Relay is a virtual-circuit wide-area network that was designed in response to demands for a new type of WAN in the late 1980s and early 1990s.
- Frame Relay operates at a higher speed (1.544 Mbps and recently 44.376 Mbps).
- Frame Relay is a high-performance WAN protocol that operates at the **physical and Data Link layers** of the OSI reference model.

- This means it can easily be used as a backbone network to provide services to protocols that already have a network layer protocol, such as the Internet.
- Frame Relay has error detection at the data link layer only. There is no flow control or error control. There is not even a retransmission policy if a frame is damaged; it is silently dropped. Frame Relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers.

The frame relay operation can be explained as below

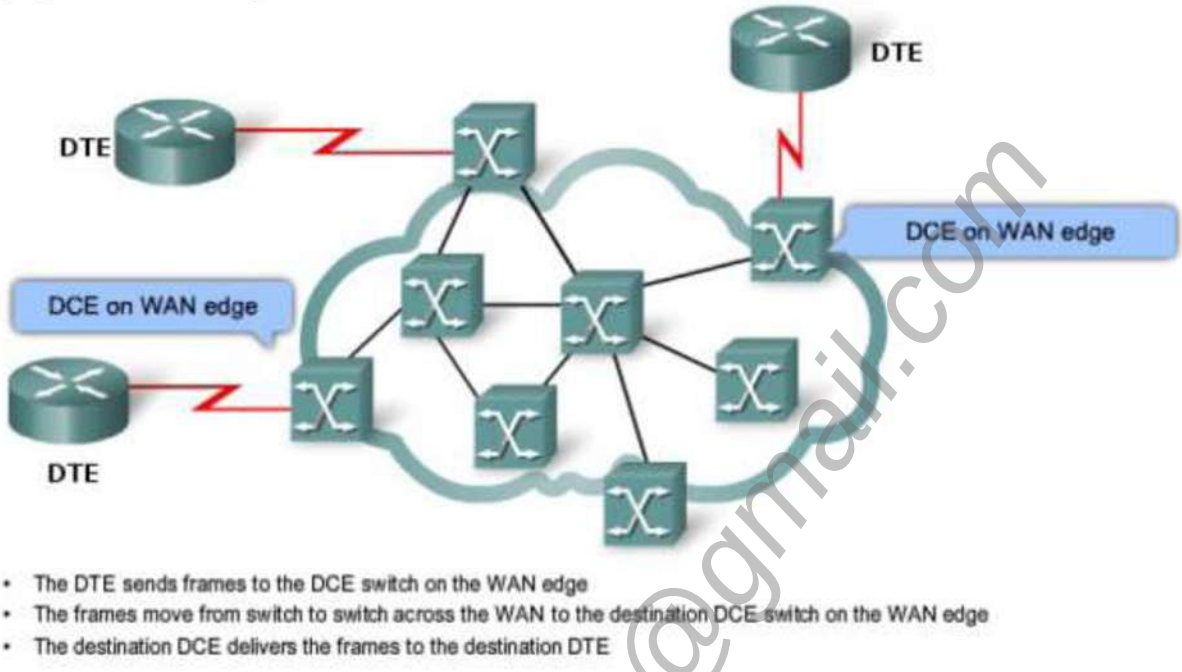
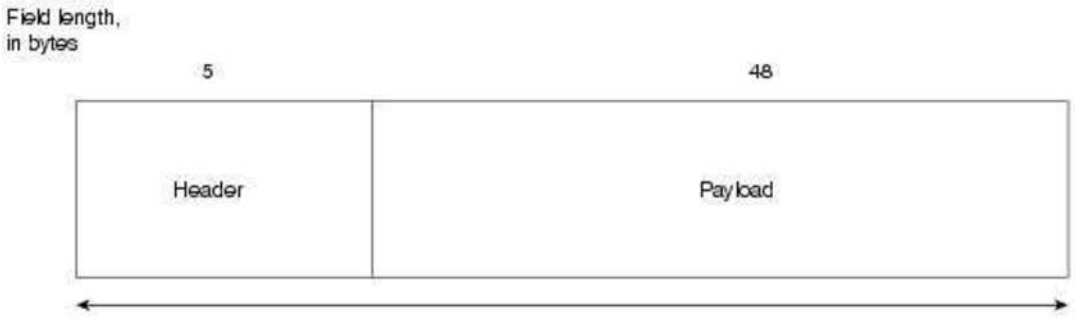


Fig: Frame Relay Operation

Frame Relay	X.25
Offers higher performance and grater transmission efficiency	Lower than frame relay
Frame relay is a Layer 2 protocol suite	X.25 provides services at Layer 3
No error detection hence it provides greater speeds.	Error detection hence it provides error free delivery. It contains fields which are used for error and flow control.
It has Physical layer and data link layer. Hence higher performance and greater transmission rate is achieved.	It has physical, data link and network layers
It prepares and sends frames.	It prepares and sends packets.
It can dynamically allocate bandwidth.	Fixed bandwidth is available in X.25 network

Asynchronous Transfer Mode (ATM)

- Before ATM, data communications at the data link layer had been based on frame switching and frame networks.
- As networks become more complex, the information that must be carried in the header becomes more extensive. The result is larger and larger headers relative to the size of the data unit.
- The result is larger and larger headers relative to the size of the data unit. In response, some protocols have enlarged the size of the data unit to make header use more efficient (sending more data with the same size header).
- Unfortunately, large data fields create waste. If there is not much information to transmit, much of the field goes unused. To improve utilization, some protocols provide variable frame sizes to users.



- ATM is built on a **cell based architecture rather than on frame based architecture**.
- **ATM eliminates the varying delay times associated with different-size frames.**
- ATM cell are always 53 bytes fixed length cell.
- It contains five-byte ATM header followed by 48 bytes' payload.
- Small fixed length cell is well suited for carrying voice and video traffic.
- ATM technology is capable of transferring voice, video and data through private and public network.

- ATM provides functionality that is similar to both circuit switching and packet switching networks:
- ATM uses asynchronous time-division multiplexing and encodes data into small, fixed-sized packets called cells.
- ATM uses a connection-oriented model in which a virtual circuit must be established between two end points before the actual data exchange begins.
- **ATM was designed to be extremely scalable and can support link speed up to 622mbps and higher.**
- Although fixed length cell is well suited for voice and video, it is less efficient. A 5-byte header for every 58-byte payload is really a waste of bandwidth for large network layer packets. ATM offers connection oriented but unreliable transmission service. The responsibility for transmission reliability is taken over by a higher order protocol such as TCP.
- Use of ATM technology was eventually largely superseded by Internet Protocol (IP)-only technology.

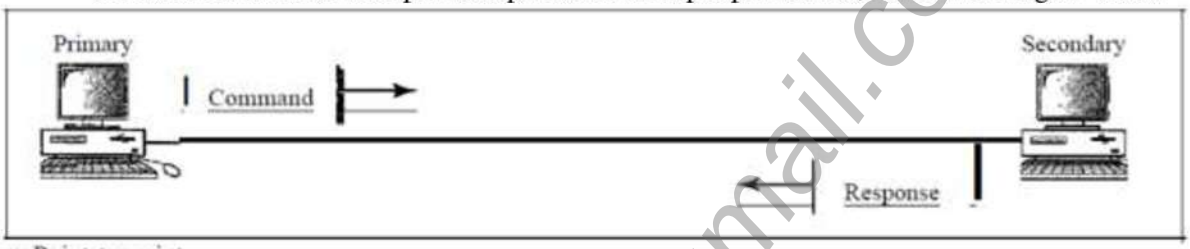
Data Link Layer Protocol

1. **Point to point protocol(PPP)**
   - One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP).
   - Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP.
   - The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer.
   - But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data link layer.
   - PPP provides several services:
     1. PPP defines the format of the frame to be exchanged between devices.
     2. PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
     3. PPP defines how network layer data are encapsulated in the data link frame.

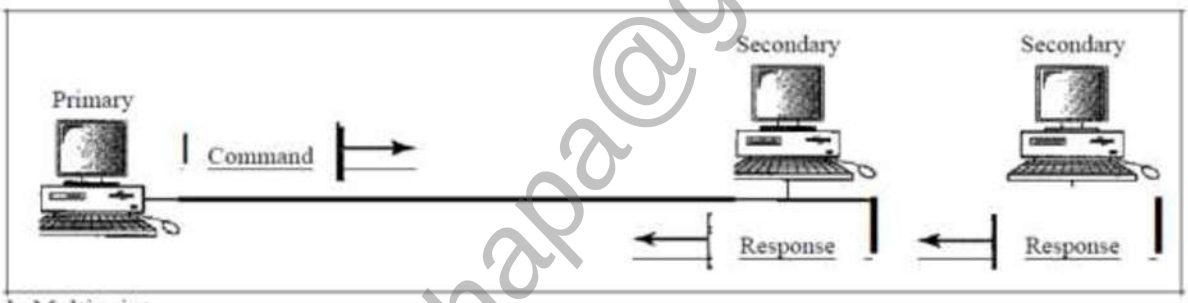
4. PPP defines how two devices can authenticate each other.
5. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

2. HDLC (High-level data link control)

- High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links.
- However, the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP), which is a byte-oriented protocol.
- HDLC provides two common transfer modes that can be used in different configurations:
  1. Normal response mode (NRM)
     - In normal response mode (NRM), the station configuration is unbalanced.
     - We have one primary station and multiple secondary stations.
     - A primary station can send commands; a secondary station can only respond.
     - The NRM is used for both point-to-point and multiple-point links, as shown in figure below

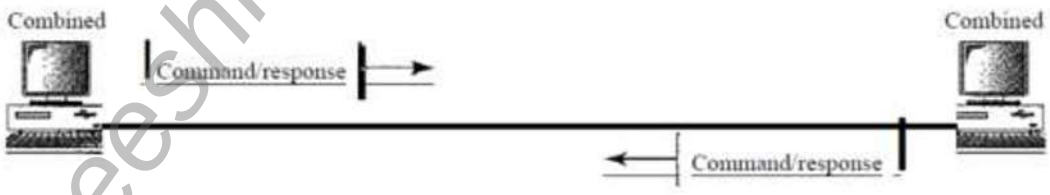


a. Point-to-point



b. Multipoint

  2. Asynchronous balanced mode (ABM).
     - In asynchronous balanced mode (ABM), the configuration is balanced.
     - The link is point-to-point, and each station can function as a primary and a secondary (acting as
     - peers), as shown in figure below.
     - This is the common mode today.



HDLC Frame Format

- HDLC defines three types of frames: information frames (I-frames), supervisory frames (S-frames), and unnumbered frames (V-frames).
- Each type of frame serves as an envelope for the transmission of a different type of message.
- I-frames are used to transport user data and control information relating to user data
- S-frames are used only to transport control information.
- V-frames are reserved for system management. Information carried by V-frames is intended for managingthe link itself.
- Each frame in HDLC may contain up to six fields, as shown in figure below: a beginning flag field, an address field, a control field, an information field, a frame check sequence (FCS) field, and an ending flag field.

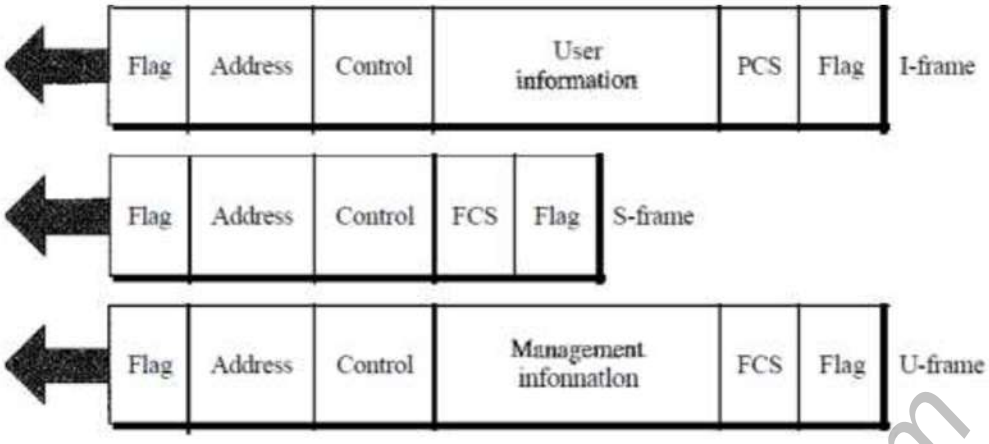


Fig: HDLC Frame

- Different fields and their use in different frame types is explained below
  1. Flag field. The flag field of an HDLC frame is an 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver.
  2. Address field. The second field of an HDLC frame contains the address of the secondary station. If a primary station created the frame, it contains a to address. If a secondary creates the frame, it contains a from address. An address field can be 1 byte or several bytes long, depending on the needs of the network.
  3. Control field. The control field is a 1- or 2-byte segment of the frame used for flow and error control.
  4. FCS field. The frame check sequence (FCS) is the HDLC error detection field. It can contain either a 2- or 4-byte CRC.