CST 303 COMPUTER NETWORKS
MODULE 2

Data link layer - Data link layer design issues, Error detection and correction, Sliding window-protocols, High-Level Data Link Control(HDLC)protocol. **Medium Access Control (MAC) sub layer** –Channel allocation problem, Multiple access protocols, Ethernet, Wireless **LANs** - 802.11, Bridges & switches - Bridges from 802.x to 802.y, Repeaters, Hubs, Bridges, Switches, Routers and Gateways.

DATALINK LAYER

- Data Link Layer is second layer of OSI Layered Model.
- This layer is one of the most complicated layers and has complex functionalities and liabilities.
- Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.
- Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.
- At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

- **Framing**

  Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver’ end, data link layer picks up signals from hardware and assembles them into frames.

- **Addressing**

  Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

- **Synchronization**

  When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **Error Control**

  Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control**

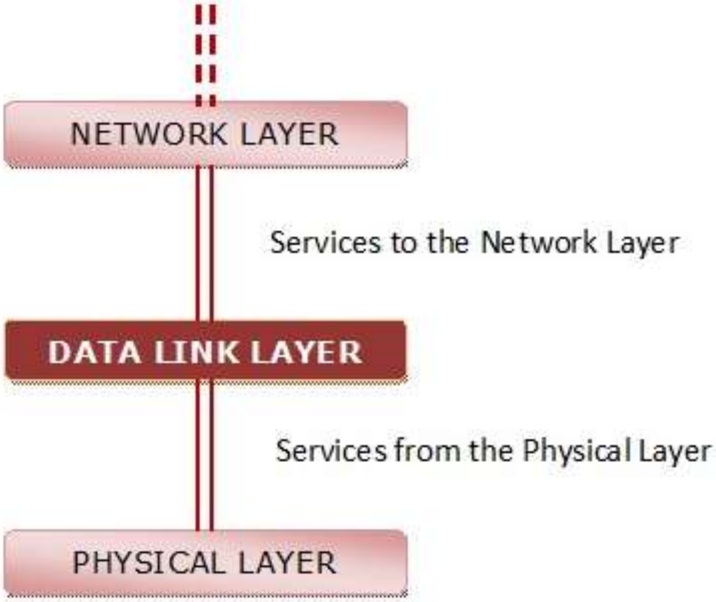
  Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

1. <u>Services to the Network Layer</u>

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer. The primary function of this layer is to provide a well defined service interface to network layer above it


NETWORK LAYER
Services to the Network Layer
DATA LINK LAYER
Services from the Physical Layer
PHYSICAL LAYER

The types of services provided can be of three types −

1. Unacknowledged connectionless service
2. Acknowledged connectionless service
3. Acknowledged connection - oriented service

Unacknowledged and connectionless services.

- Here the sender machine sends the independent frames without any acknowledgement from the sender.
- There is no logical connection established.

Acknowledged and connectionless services.

- There is no logical connection between sender and receiver established.
- Each frame is acknowledged by the receiver.
- If the frame didn’t reach the receiver in a specific time interval it has to be sent again.
- It is very useful in wireless systems.

Acknowledged and connection-oriented services

- A logical connection is established between sender and receiver before data is trimester.
- Each frame is numbered so the receiver can ensure all frames have arrived and exactly once

2. <u>Framing</u>

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer

3. <u>Error Control</u>

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them

- Controlling access to shared channels in case of broadcasting

4. Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

FRAMING

- Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits
- Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.
- Framing is an important aspect of data link layer protocol design because it allows the transmission of data to be organized and controlled, ensuring that the data is delivered accurately and efficiently.

The problems faced in framing are:

1. **Locating at the beginning of the frame**
2. **How will the station notice a frame**
3. **Locating end of frame**

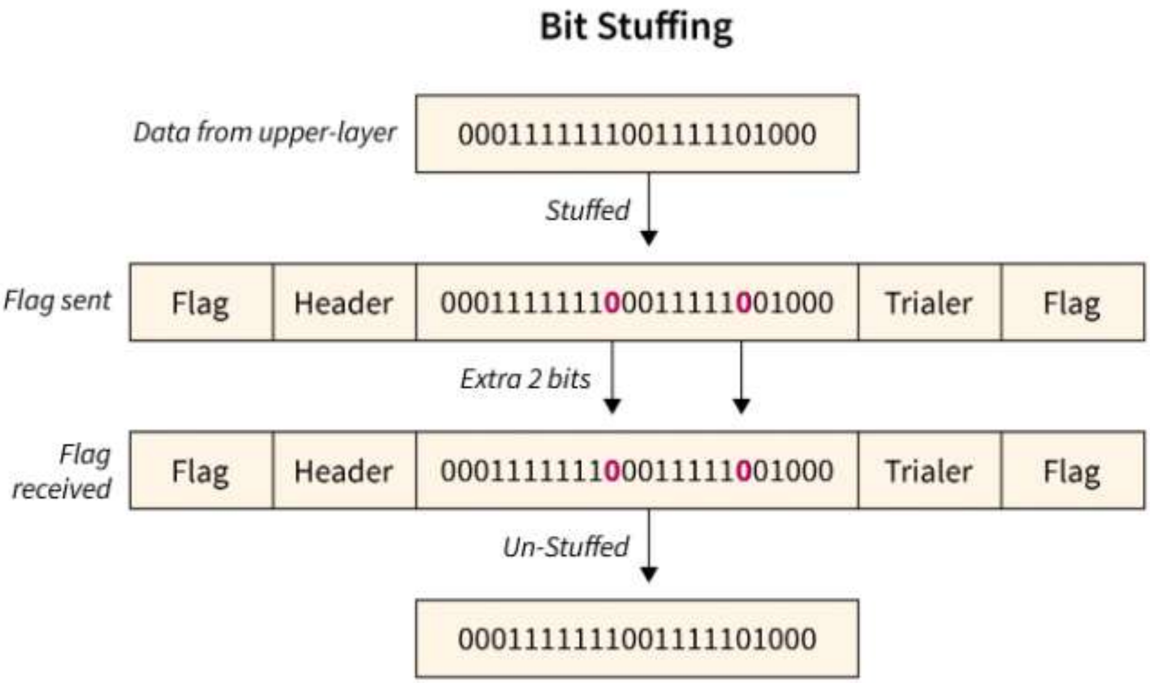
Framing Approaches in Computer Network

Talking about Framing Approaches in computer networking, there are 2-different kind of approaches to Framing in the Data link layer:

Bit-Oriented Framing

Most protocols use a special 8-bit pattern flag 01111110 as a result of the delimiter to stipulate the beginning and so the end of the frame. Bit stuffing is completed at the sender end and bit removal at the receiver end.

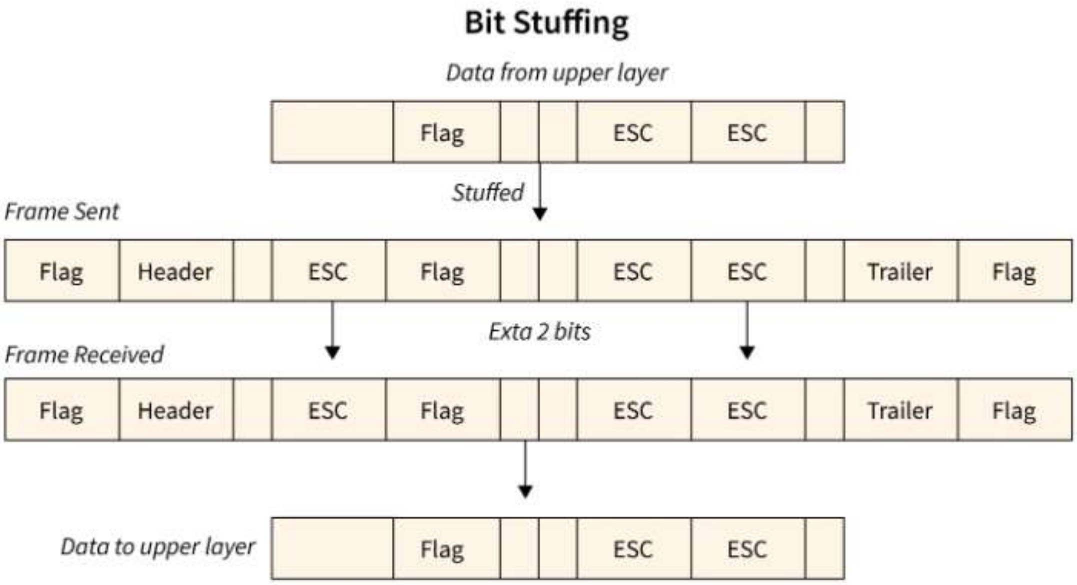
If we have a tendency to get a zero(0) after 5 1s. we have a tendency to tend to still stuff a zero(0). The receiver will remove the zero. Bit stuffing is in addition said as bit stuffing.



Byte-Oriented Framing

Byte stuffing is one of the methods of adding an additional byte once there is a flag or escape character within the text. Take an illustration of byte stuffing as appears in the given diagram.

The sender sends the frame by adding three additional ESC bits and therefore the destination machine receives the frame and it removes the extra bits to convert the frame into an identical message.



Methods of Framing :

There are basically four methods of framing as given below –

1. Character Count

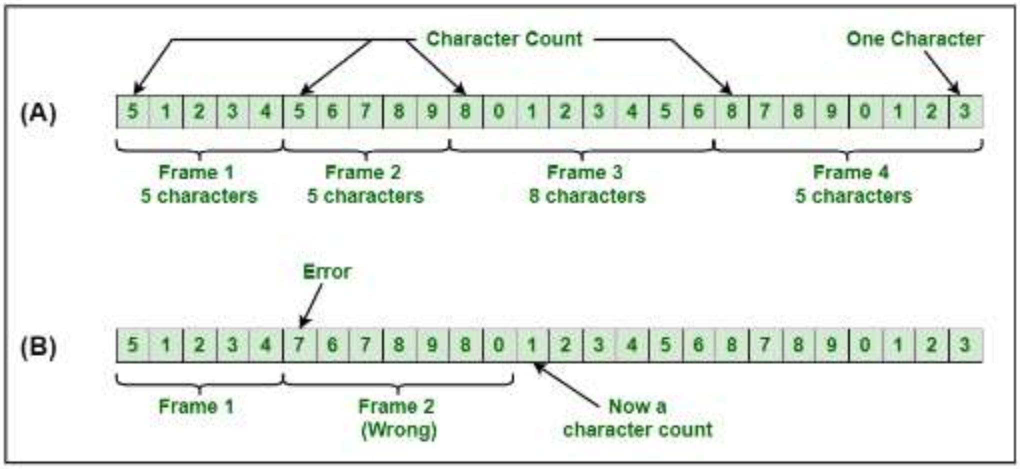
2. Flag Byte with Character Stuffing

3. Starting and Ending Flags, with Bit Stuffing

4. Encoding Violations

CHARACTER COUNT :

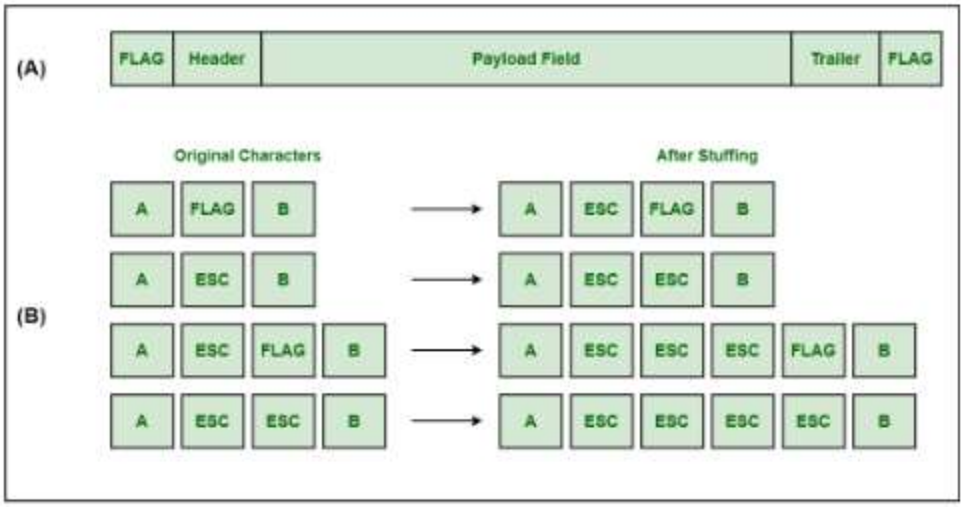
- This method is rarely used and is generally required to count total number of characters that are present in frame.
- This is be done by using field in header. Character count method ensures data link layer at the receiver or destination about total number of characters that follow, and about where the frame ends.
- There is disadvantage also of using this method i.e., if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization.
- The destination or receiver might also be not able to locate or identify beginning of next frame.



CHARACTER STUFFING

- Character stuffing is also known as byte stuffing or character-oriented framing and is same as that of bit stuffing but byte stuffing actually operates on bytes whereas bit stuffing operates on bits.

- In byte stuffing, special byte that is basically known as ESC (Escape Character) that has predefined pattern is generally added to data section of the data stream or frame when there is message or character that has same pattern as that of flag byte.
- But receiver removes this ESC and keeps data part that causes some problems or issues.
- In simple words, we can say that character stuffing is addition of 1 additional byte if there is presence of ESC or flag in text.



BIT STUFFING

Bit stuffing is also known as bit-oriented framing or bit-oriented approach. In bit stuffing, extra bits are being added by network protocol designers to data streams. It is generally insertion or addition of extra bits into transmission unit or message to be transmitted as simple way to provide and give signaling information and data to receiver and to avoid or ignore appearance of unintended or unnecessary control sequences.

It is type of protocol management simply performed to break up bit pattern that results in transmission to go out of synchronization

PHYSICAL LAYER CODING VIOLATIONS :

Encoding violation is method that is used only for network in which encoding on physical medium includes some sort of redundancy i.e., use of more than one graphical or visual structure to simply encode or represent one variable of data.

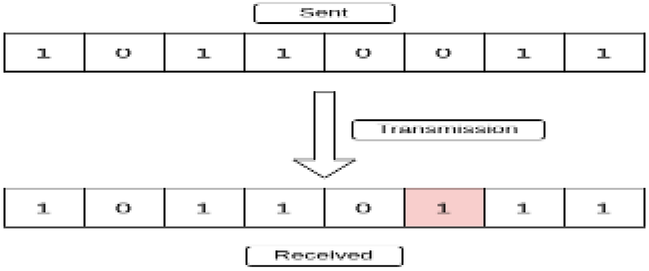
ERROR CORRECTION AND DETECTION IN DATALINK LAYER

The error simply means any flaw or deviation that occurs while the information is transmitted from the source to the destination in a computer network. In other words, if the message or data transmitted by the source is not identical to the one received at the destination, we can say that there is some Error in the Computer Network.

Types of Errors

1. **Single-Bit Error**

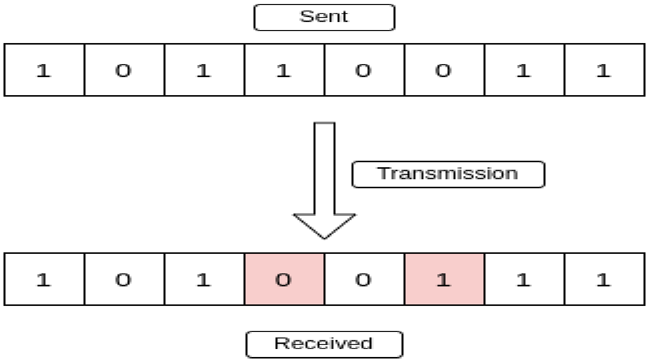
A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.



Single-Bit Error

2. **Multiple-Bit Error**

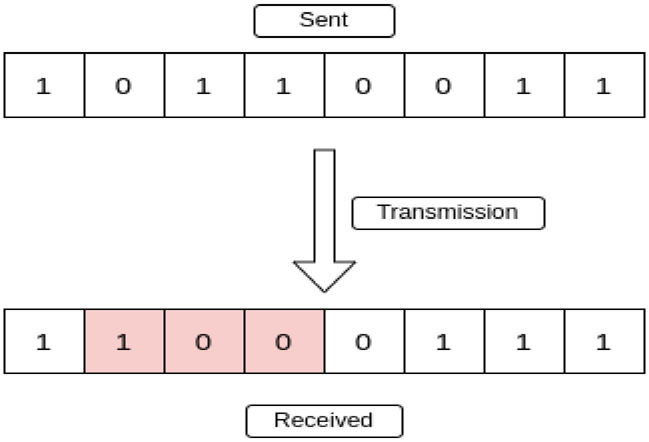
A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected. Although multiple-bit errors are relatively rare when compared to single-bit errors, they can still occur, particularly in high-noise or high-interference digital environments.



Multiple-Bit Error

3. **Burst Error**

When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.



Burst Error

Error Detection Methods

To detect errors, a common technique is to introduce redundancy bits that provide additional information. Various techniques for error detection include:

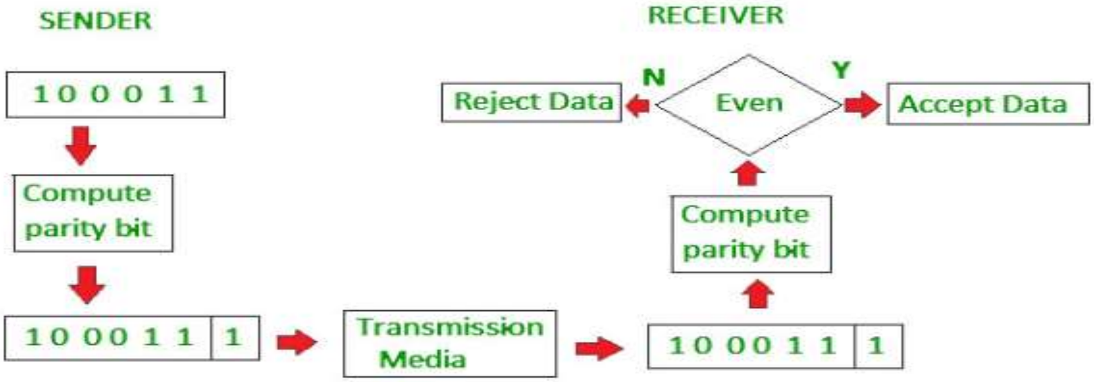
- Simple Parity Check
- Two-Dimensional Parity Check
- Checksum
- Cyclic Redundancy Check (CRC)

<u>Simple Parity Check</u>

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

This scheme makes the total number of 1's even, that is why it is called <u>even parity</u> checking.

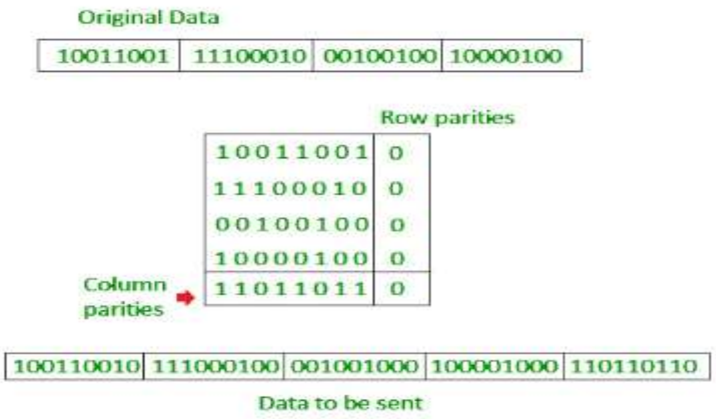


Advantages of Simple Parity Check

- Simple parity check can detect all single bit error.
- Simple parity check can detect an odd number of errors.
- **Single-Bit Error Detection**: It can effectively detect single-bit errors within a data unit, providing a basic level of error detection for relatively low-error environments.

Two-Dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



10011001	11100010	00100100	10000100

1 0 0 1 1 0 0 1	0
1 1 1 0 0 0 1 0	0
0 0 1 0 0 1 0 0	0
1 0 0 0 0 1 0 0	0
1 1 0 1 1 0 1 1	0

100110010	111000100	001001000	100001000	110110110

Advantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can detect and correct all single bit error.
- Two-Dimensional Parity Check can detect two or three bit error that occur any where in the matrix.

Disadvantages of Two-Dimensional Parity Check

- Two-Dimensional Parity Check can not correct two or three bit error. It can only detect two or three bit error.
- If we have a error in the parity bit then this scheme will not work.

Checksum

Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1’s complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver.

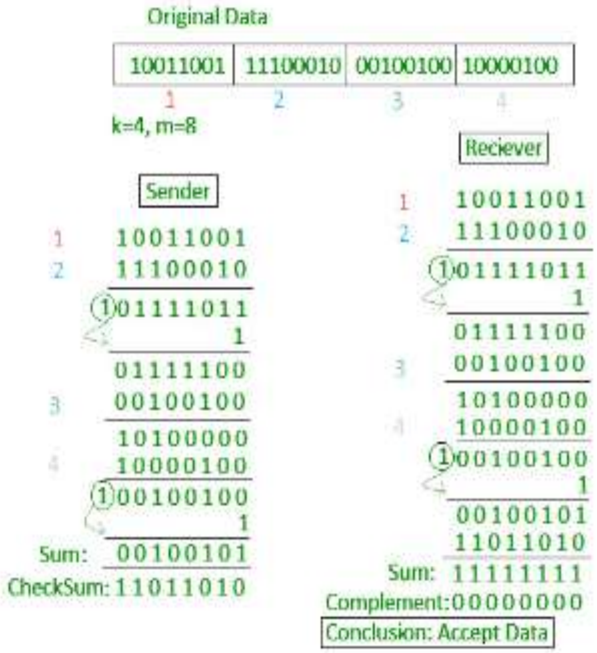
At the receiver’s end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum – Operation at Sender’s Side

- Firstly, the data is divided into k segments each of m bits.
- On the sender’s end, the segments are added using 1’s complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

Checksum – Operation at Receiver’s Side

- At the receiver’s end, all received segments are added using 1’s complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

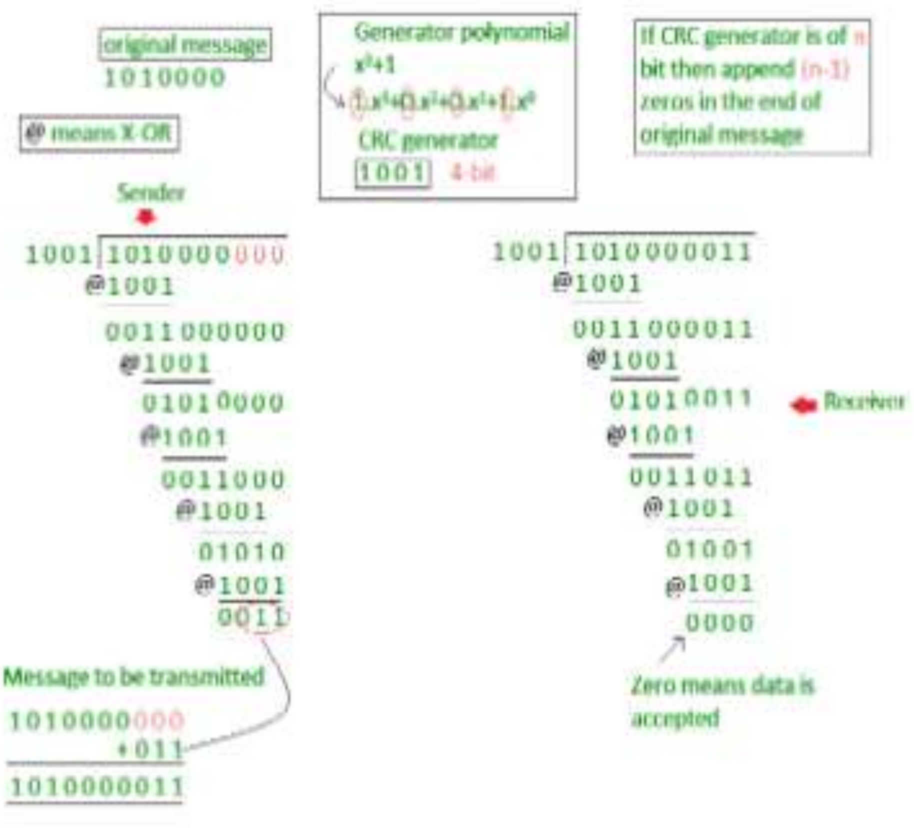


Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.

Example: Let’s data to be send is 1010000 and divisor in the form of polynomial is x3+1. CRC method discussed below.



Error Correction Techniques

We can detect the error using a single additional bit but we cannot use this bit for the correction purpose. It is important to know the exact location of the error if we want to correct that error. For example, for finding out the **single-bit error**, the error detection code checks out that the error is actually in one of the seven bits. Let d represents the number of data bits and r represents the number of redundant bits

Hamming Code

A **hamming code** is a technique developed by R.W Hamming for finding out the position of the error bit. This Hamming code is based on the relationship between the redundant bits and data units and its main advantage is that it can be applied to data units of any length.

Parity bits: The **parity bits** are the special type of bits that are added to the original data of binary bits to make the total 1s either even or odd.

Even parity: For checking the even parity, the following concept is used: The value of the even parity bit will be **0** if the total occurrence of 1s is even and the value of the parity bit can be 1 if the total occurrence of 1s is odd.

Odd Parity: For checking the even parity, the following concept is used: The value of the parity bit will be 1 if the total occurrence of 1s is even and the value of the parity bit can be 0 if the total occurrence of 1s is odd.

Encoding a message by Hamming Code

The procedure used by the sender to encode the message encompasses the following steps −

- **Step 1** − Calculation of the number of redundant bits.
- **Step 2** − Positioning the redundant bits.
- **Step 3** − Calculating the values of each redundant bit.

Calculation of the number of redundant bits.

If the message contains *mm*number of data bits, *rr*number of redundant bits are added to it so that *mr* is able to indicate at least ($m + r$+ 1) different states. Here, ($m + r$) indicates location of an error in each of ($m + r$) bit positions and one additional state indicates no error. Since, *rr* bits can indicate $2^{r}r$ states, $2^{r}r$ must be at least equal to ($m + r$ + 1). Thus the following equation should hold $2^{r} \geq m+r+1$

Positioning the redundant bits.

The *r* redundant bits placed at bit positions of powers of 2, i.e. 1, 2, 4, 8, 16 etc. They are referred in the rest of this text as r_1 (at position 1), r_2 (at position 2), r_3 (at position 4), r_4 (at position 8) and so on.

Calculating the values of each redundant bit.

The redundant bits are parity bits. A parity bit is an extra bit that makes the number of 1s either even or odd. The two types of parity are −

- **Even Parity** − Here the total number of bits in the message is made even.
- **Odd Parity** − Here the total number of bits in the message is made odd.

Each redundant bit, r_i, is calculated as the parity, generally even parity, based upon its bit position. It covers all bit positions whose binary representation includes a 1 in the i^{th} position except the position of r_i. Thus −

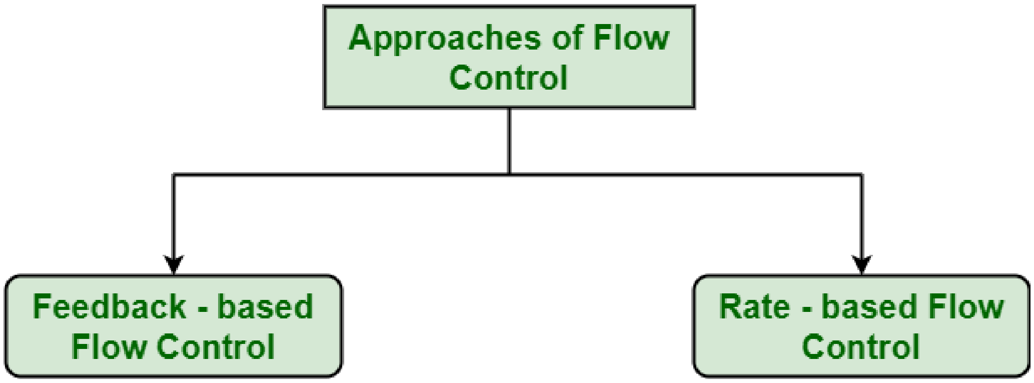
- r_1 is the parity bit for all data bits in positions whose binary representation includes a 1 in the least significant position excluding 1 (3, 5, 7, 9, 11 and so on)
- r_2 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 2 from right except 2 (3, 6, 7, 10, 11 and so on)
- r_3 is the parity bit for all data bits in positions whose binary representation includes a 1 in the position 3 from right except 4 (5-7, 12-15, 20-23 and so on)

FLOW CONTROL IN DATALINK LAYER

- **Flow control** is design issue at Data Link Layer.
- It is a technique that generally observes the proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it.
- This can happen only if receiver has very high load of traffic as compared to sender, or if receiver has power of processing less as compared to sender.
- Flow control is basically a technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another.
- Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver.
- **Flow control** is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver.
- The receiving device also contains only limited amount of speed and memory to store data. This is why receiving device should be able to tell or inform the sender about

stopping the transmission or transferring of data on temporary basis before it reaches limit.

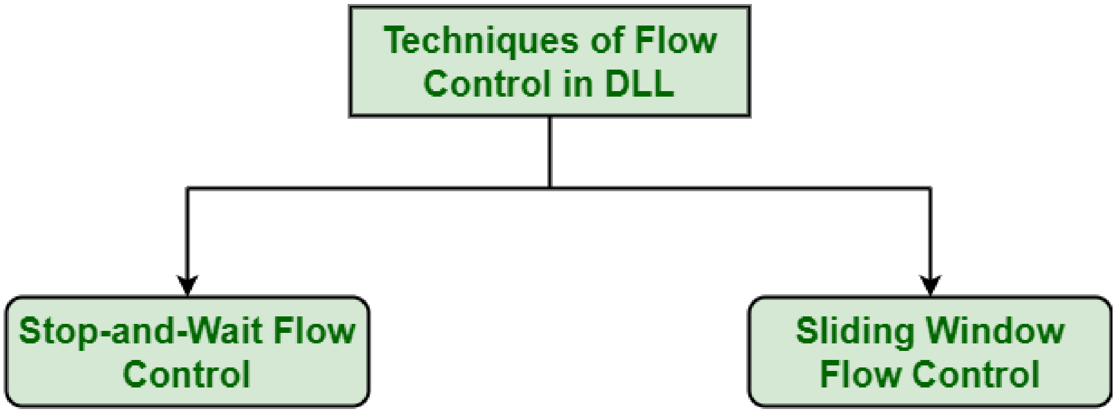
- It also needs buffer, large block of memory for just storing data or frames until they are processed.


Approaches of Flow Control
Feedback - based Flow Control
Rate - based Flow Control

Approaches to Flow Control : Flow Control is classified into two categories:

- **Feedback – based Flow Control :** In this control technique, sender simply transmits data or information or frame to receiver, then receiver transmits data back to sender and also allows sender to transmit more amount of data or tell sender about how receiver is processing or doing. This simply means that sender transmits data or frames after it has received acknowledgements from user.
- **Rate – based Flow Control :** In this control technique, usually when sender sends or transfer data at faster speed to receiver and receiver is not being able to receive data at the speed, then mechanism known as built-in mechanism in protocol will just limit or restricts overall rate at which data or information is being transferred or transmitted by sender without any feedback or acknowledgement from receiver.

Techniques of Flow Control in Data Link Layer : There are basically two types of techniques being developed to control the flow of data


Techniques of Flow Control in DLL
Stop-and-Wait Flow Control
Sliding Window Flow Control

Stop-and-Wait Flow Control : This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgement is received, then only sender will send or transfer the next frame. This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay and Ultimately In this method sender sent single frame and receiver take one frame at a time and sent acknowledgement(which is next frame number only) for new frame.

Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- This method is also very accurate.

Disadvantages –

- This method is fairly slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow.

Sliding Window Flow Control : This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgement. In this method, both the sender and receiver agree upon total number of data frames after which acknowledgement is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet “in-flight” at a time. This increases and improves network throughput. and Ultimately In this method sender sent multiple frame but receiver take one by one and after completing one frame acknowledge(which is next frame number only) for new frame.

Advantages –

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

Disadvantages –

- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.
- The receiver might receive data frames or packets out the sequence.

Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

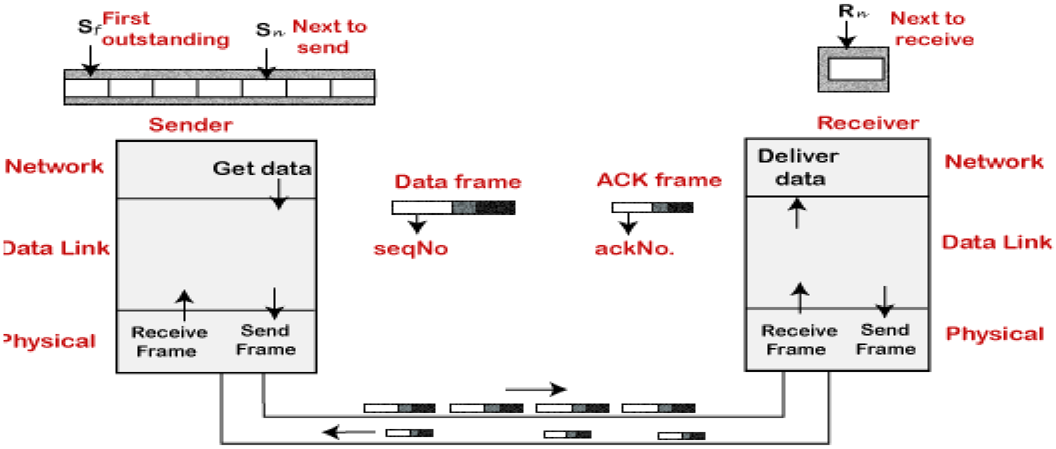
Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.
- The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

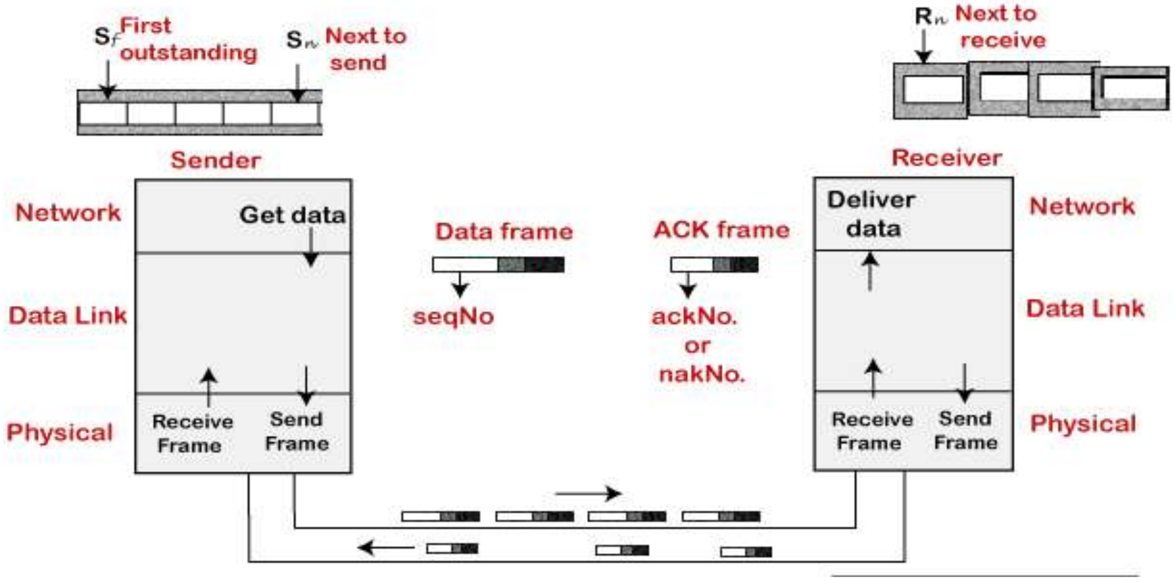
- If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.



Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame.



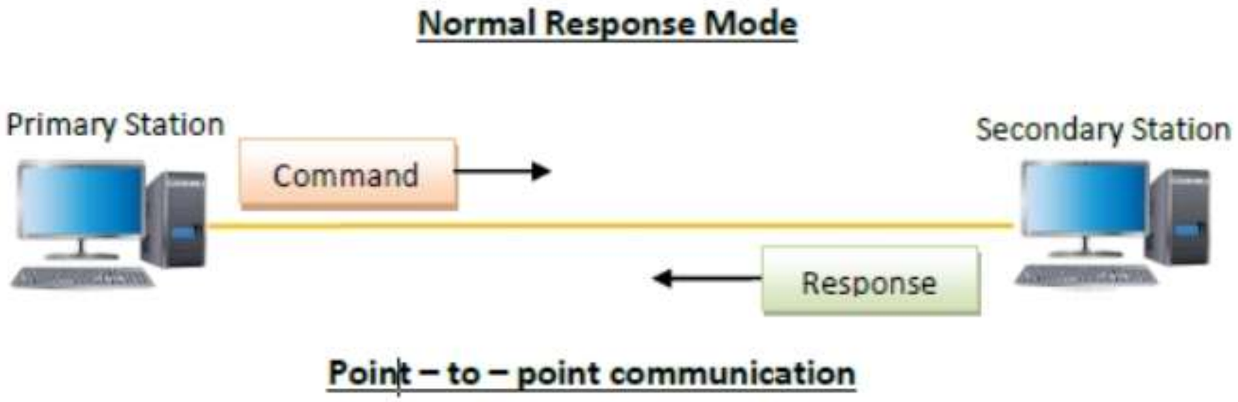
HDLC(HIGH LEVEL DATALINK CONTROL PROTOCOL)

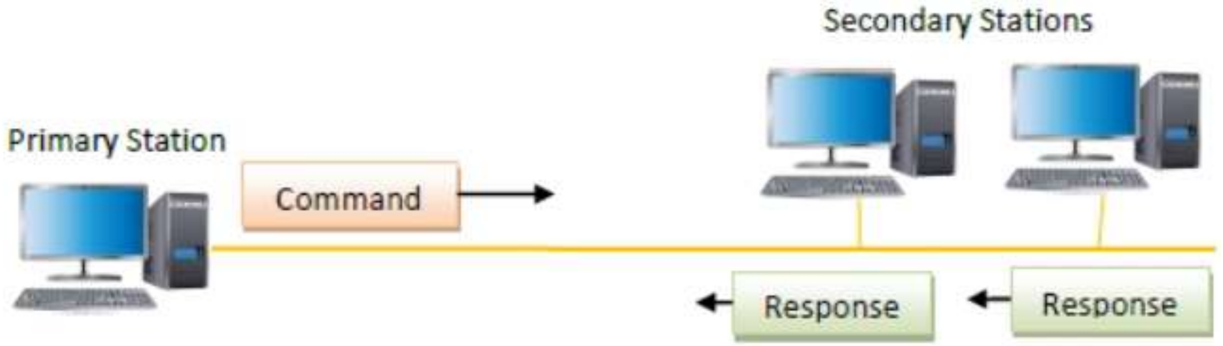
High-level Data Link Control (HDLC) is a group of communication protocols of the **data link layer** for transmitting data between network points or nodes. Since it is a **data link protocol**, data is organized into frames.

Transfer Modes

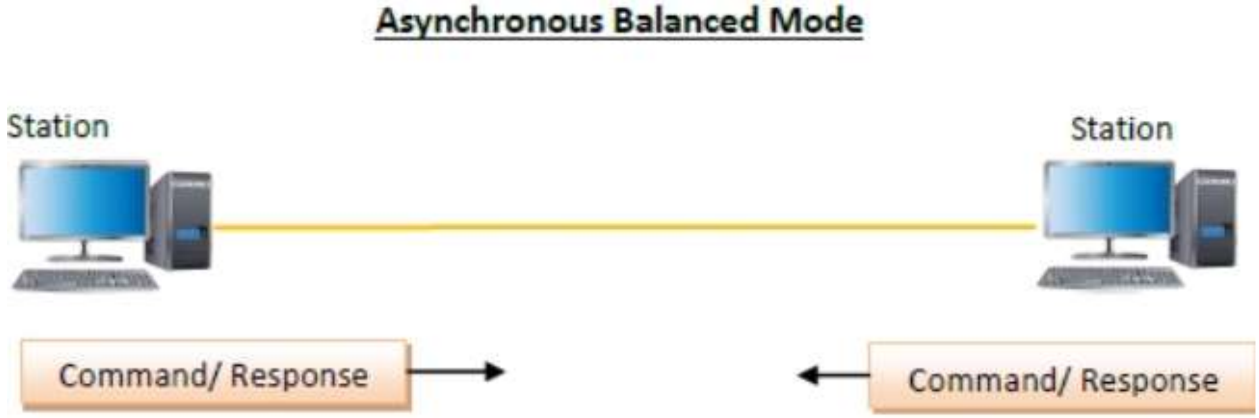
HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.





- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.

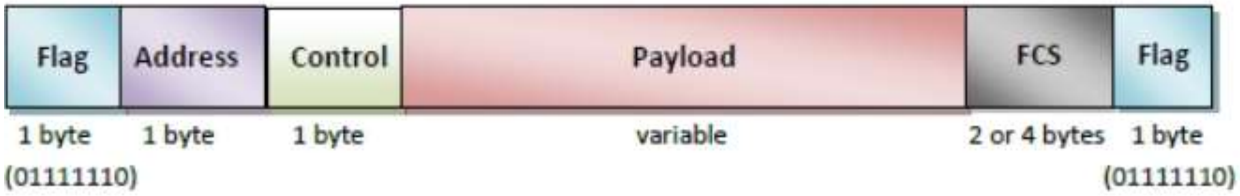


HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)

HDLC Frame



Types of HDLC Frames

There are three types of HDLC frames. The type of frame is determined by the control field of the frame −

- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** − S-frames or Supervisory frames do not contain information field. They are used for flow and error control when piggybacking is not required. The first two bits of control field of S-frame is 10.
- **U-frame** − U-frames or Un-numbered frames are used for myriad miscellaneous functions, like link management. It may contain an information field, if required. The first two bits of control field of U-frame is 11.

MEDIUM ACCESS CONTROL PROTOCOL

Datalink layer is divided into two sublayers. They are

1. Logical link control sublayer
2. Medium access control sublayer

In the case odd Logical link control layer all connections are dedicated. So, there is no problem for sharing channel allocation. But in the case of medium access control sublayer multiple nodes can be connected to the same channel.

Multipoint connections are used in Mac layer so multiple nodes can communicate simultaneously. So it leads to data collision. This data collision can be handled by MAC layer. Actual problem in this scenario is how to determine who got to use the channel next when there is a competition.

CHANNEL ALLOCATION PROBLEM

There are two types of channel allocation methods. They are static channel allocation and dynamic channel allocation.

Static channel allocation

1. **FDM:** Entire bandwidth is divided into N equal sized portions, if there are N users. Each user assigns one portion. then there is no problem for channel allocation. But this method is applicable only for a smaller number of users. If the number of users is large this method is not an efficient method.
2. **TDM:** The entire time is allocated to each use in this method. If the user does not want to send data at the assigned time slot. Then the channel is wasted on that time. No on else can use that channel on that time. So this is not an efficient method.

Dynamic Channel allocation

Some assumptions are taken for channel allocation

1. Stations: the stations are independent. Once the frame is has been generated the station is blocked, does nothing until the frame has been successfully transmitted.
2. Single channel: All stations can transmit on the same channel and all can receive from it.
3. Collisions: when more than one station try to transmit a frame simultaneously both of them are garbled.
4. Continuous/ slotted time: in continuous the frame transmissions can start at any time. But in the case of slotted time, time is divided into slots and each frame can transmit at only on the starting of any time slot.
5. Carrier sense/ No carrier sense: Station would be able to sense the channel to know that whether the channel has already data or busy with data

PROTOCOLS FOR CHANNEL ALLOCATION

Random Access Protocol

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium’s state(idle or busy). It has two features:

- There is no fixed time for sending data

- There is no fixed sequence of stations sending data

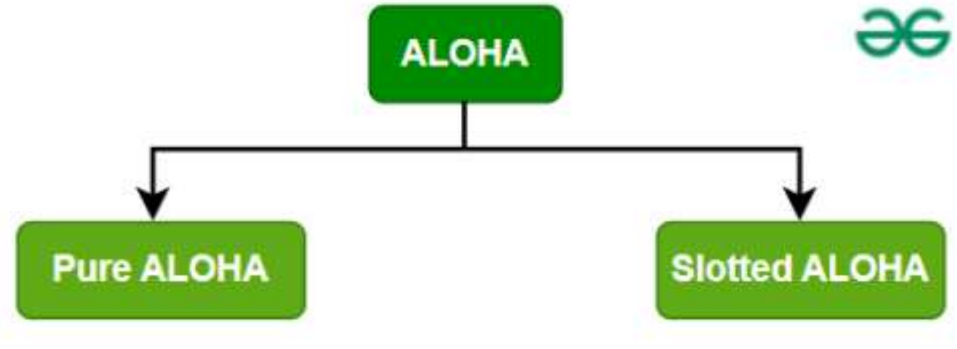
The Random access protocols are further subdivided as:

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

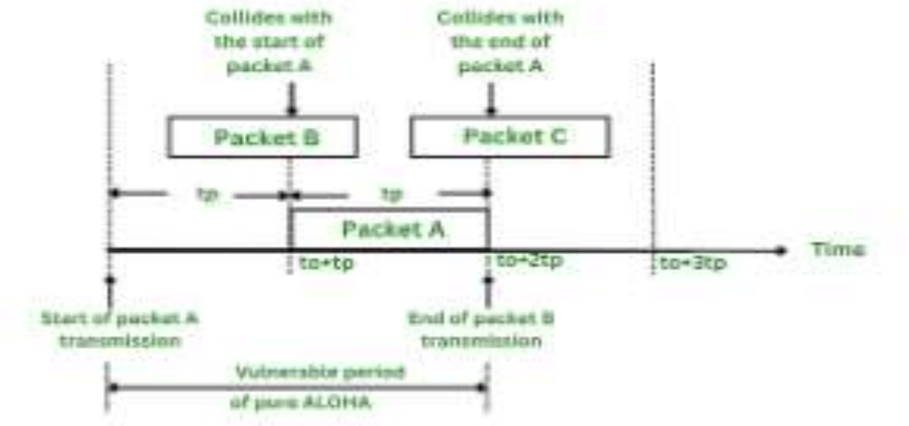


Types of Aloha

Pure ALOHA

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

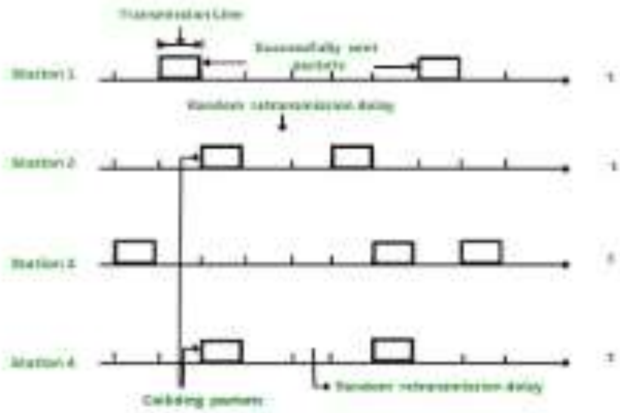
1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.


Collides with the start of packet A
Collides with the end of packet A
Packet B
Packet C
tp
tp
Packet A
Time
to+tp
to+2tp
to+3tp
Start of packet A transmission
End of packet B transmission
Vulnerable period of pure ALOHA

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.


Transmission time
Successfully sent packets
Station 1
t
Random retransmission delay
Station 2
t
Station 3
t
Station 4
t
Colliding packets
Random retransmission delay

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs when there used to be shared Bus Topology and each node (Computers) was connected by Coaxial Cables. Nowadays Ethernet is Full Duplex and Topology is either Star (connected via Switch or Router) or point-to-point (Direct Connection). Hence CSMA/CD is not used but they are still supported though.

- **Step 1:** Check if the sender is ready to transmit data packets.

- **Step 2:** Check if the transmission link is idle.
  The sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. The sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

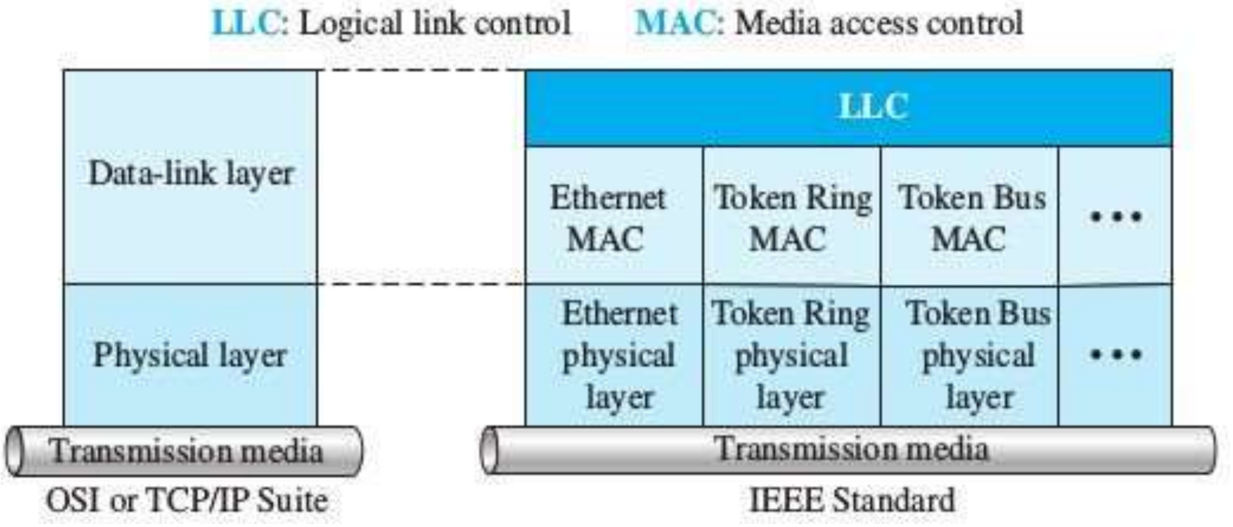
- **Step 3:** Transmit the data & check for collisions.
  The sender transmits its data on the link. CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.

- **Step 4:** If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

IEEE 802 Project

- ▶ **IEEE 802** is a collection of networking **standards** that cover the physical and data-link layer specifications for technologies such as Ethernet and wireless.
- ▶ These specifications apply to local area networks (LAN) and metropolitan area networks (MAN).
- ▶ The IEEE created a Project 802 in 1982 to set standards to enable intercommunication among equipment from a variety of manufacturers.
- ▶ Specifies the functions of Physical layer and Data Link layer of LAN protocols (such as Ethernet, Token Ring, Token Bus, etc).

- The IEEE has subdivided the data-link layer into two sublayers: **Logical Link Control (LLC)** and **Media Access Control (MAC)** sublayers



ETHERNET

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.

- It was first standardized in 1980s by IEEE 802.3 standard.
- IEEE 802.3 defines the Logical link layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.
- Ethernet is classified into two categories: classic Ethernet and switched Ethernet.
- Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps.
- The varieties are commonly referred as **10BASE-X**. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used.
- A switched Ethernet uses switches to connect to the stations in the LAN.
- It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.

There are a number of versions of IEEE 802.3 protocol. The most popular ones are

IEEE 802.3: **(Ethernet)**

- This was the original standard given for **10BASE-5.**
- It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core.
- Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.

IEEE 802.3a: **(Fast Ethernet)**

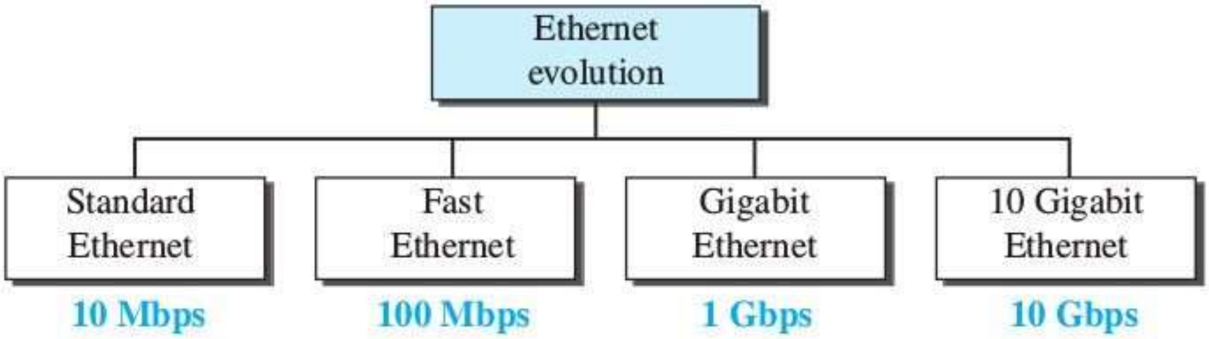
- This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors.
- The 2 refers to the maximum segment length of about 200m (185m to be precise).

IEEE 802.3i: **(Gigabit Ethernet)**

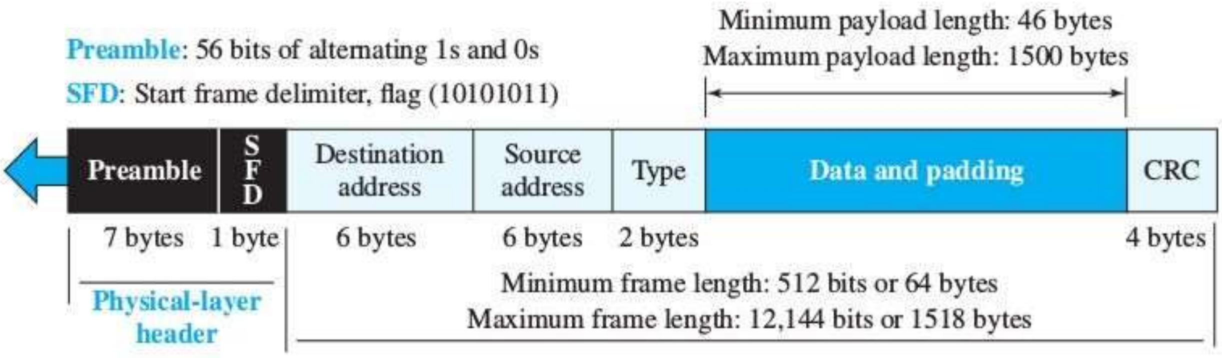
- This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium.
- The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.

IEEE 802.3j: **(10 gigabit Ethernet)**

- This gave the standard for Ethernet over Fiber (**10BASE-F**) that uses fiber optic cables as medium of transmission.



FRAME FORMAT - STANDARD ETHERNET



Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
Type
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

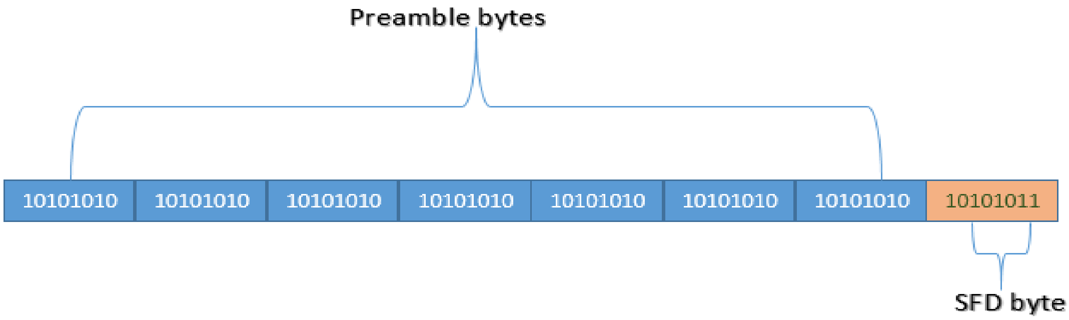
- Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).

Preamble:

- 7 bytes (56 bits), alternate 1s and 0s (ie, **101010101010…..**)
- To indicate that a frame is coming.
- Enables the receiver to synchronize its clock if it’s out of synchronization.
- Not the part of frame, but added by the physical layer.

Start frame delimiter (SFD):

- One byte. It is **10101011**.
- Last chance of synchronization and added by the physical layer
- Indicate that the next field is destination address and the frame is starting.



Destination address (DA):

- Six byte (48 bits) Physical Address (MAC Address or link-layer address or hardware address) of the destination host.
- When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upper-layer.

Source address (SA):

- This field is also six bytes and contains the link-layer address of the sender of the packet.

Type:

- **2** bytes and it stores the information about the upper layer protocol(N/w layer)
- This protocol can be IP, ARP, ICMP, and so on.
- It is used for multiplexing and demultiplexing.
- Now, this field has two purposes. Values of 1500 and below mean that it is used to indicate the size of the payload, while values above indicate that it is used as an Type, to indicate which protocol is encapsulated in the payload of the frame.

Data:

- This field carries data encapsulated from the upper-layer protocols.
- Minimum of 46 bytes and a maximum of 1500 bytes.
- If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame.
- If it is less than 46 bytes, it is to be padded with extra zeros to make it 46.
- A padded data frame is delivered to the upper-layer protocol as it is (without removing the padding), which means that it is the responsibility of the upper layer to remove or to add the padding.

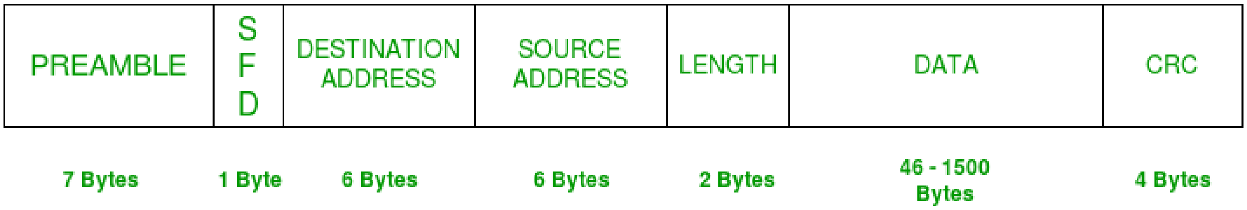
CRC (Cyclic Redundancy Check):

- 4 bytes (32 bits).
- Error detection information, in this case a CRC-32.
- CRC is calculated over the addresses, types, and data field.
- If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame.

Frame Length

Reasons for maximum length:

- ▶ To reduce the buffer size, as memory was expensive at that time.
- ▶ To prevent one device from monopolizing the medium.

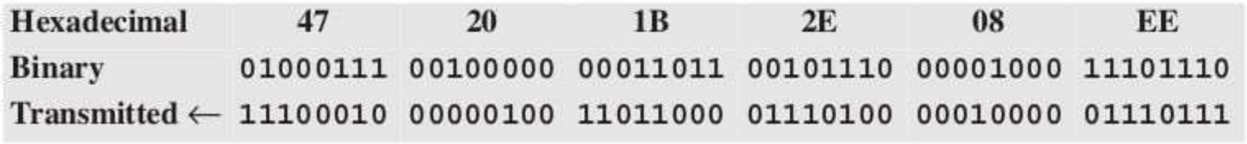


PREAMBLE	SFD	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

Standard Ethernet: Addressing

- Every NIC (Network Interface Card) has a unique 6 bytes (48bits) address.
- This address is called **Physical Address, Hardware Address** or **MAC Address**.
- It is written in hexadecimal notation, with a colon between bytes, like ***47:20:1B:2E:08:EE***.
- Ethernet uses the **MAC address** to transfer the frames from source to destination.
- The transmission is **left to right, byte by byte**; however, **for each byte, the least significant bit is sent first and the most significant bit is sent last**.



Hexadecimal	47	20	1B	2E	08	EE
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast, Multicast, and Broadcast Addresses:

- A source address is always a unicast address.
- The destination address may be unicast, multicast, or broadcast.
- Unicast(one-one), Broadcast(one-all), Multicast(one-many)
- For *unicast address*, the least significant bit of the first byte will be *zero*. It will be *one* for *multicast* and *broadcast* addresses.
- By receiving the *first bit* of the frame, the destination device can understand whether the address is unicast or not.

Eg:

4A:30:10:21:10:1A - The first byte is transmitted as **0**1010010 - Unicast

47:20:1B:2E:08:EE - The first byte is transmitted as **1**1100010 - Multicast

FF:FF:FF:FF:FF:FF - The first byte is transmitted as **1**1111111 - Broadcast

Wireless LAN

- A wired LAN or a wireless LAN operates only in the lower two layers of the TCP/IP protocol suite.
- Suppose we have a wired LAN connected to the Internet through a router or modem.
- If we have to change the network to wireless, change the wired NIC with a wireless NIC and replace the link-layer switch with an access point.

There are several characteristics of wireless LANs that either do not apply to wired LANs or the existence of which is negligible and can be ignored.

- ▶ IEEE 802.11 is the specification for wireless LAN.
- ▶ It covers physical and data link layers.
- ▶ The WiFi (Wireless Fidelity) is a technology for Wireless LAN and is certified by a non-profit organization WiFi Alliance.

Components of Wireless Architecture:

- ▶ Wireless LAN architecture is composed of different components which help in establishing the local area network between different operating systems
- ▶ These components are very essential for WiFi architecture.
  1. Access point
  2. Clients

Access Points -

- ▶ A special type of routing device that is used to transmit the data between wired and wireless networking device is called as AP.
- ▶ It is often connected with the help of wired devices such as Ethernet.

- It only transmits or transfers the data between wireless LAN and wired network by using infra structure mode of network.
- One access point can only support a small group of networks and works more efficiently.
- It is operated less than hundred feet. It is denoted by AP.

Clients-

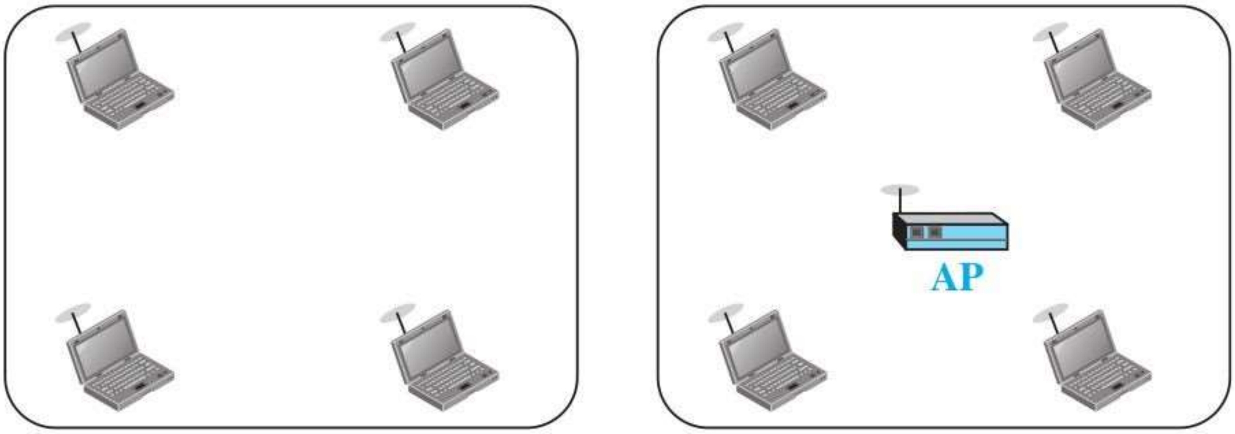
Any kind of device such as personal computers, Note books, or any kind of mobile devices which are inter linked with wireless network area referred as a client of wireless LAN architecture.

Two components are also some time play an important role in Wireless LAN architecture i.e.

- Basic Service Set (BSS)
- Extended Service Set (ESS)

Basic Service Set (BSS)

- Building blocks of a wireless LAN.
- Made of stationary or mobile wireless stations and an optional central base station, known as the Access Point (AP).
- The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture.
- A BSS with an AP is sometimes referred to as an infrastructure BSS.
- Every BSS has an identification (ID) called the BSSID.

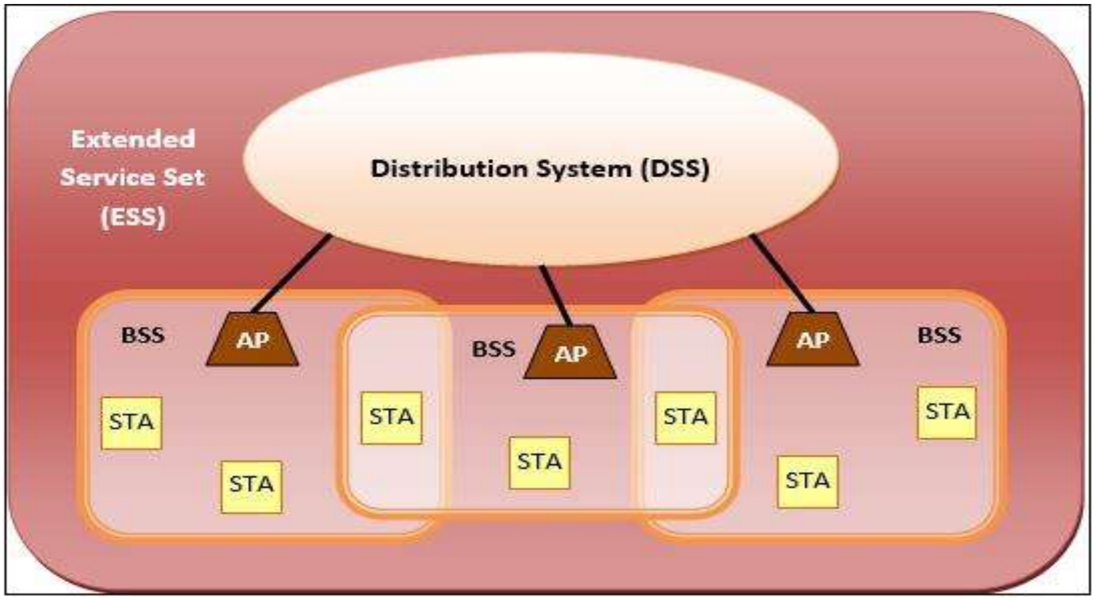


Ad hoc BSS

Infrastructure BSS

Extended Service Set (ESS)

- Made up of two or more BSSs with APs.
- Here the BSSs are connected through a distribution system, which is a wired or a wireless network.
- The distribution system connects the APs in the BSSs. • ESS uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.
- Communication between a station in a BSS and the outside BSS occurs via the AP

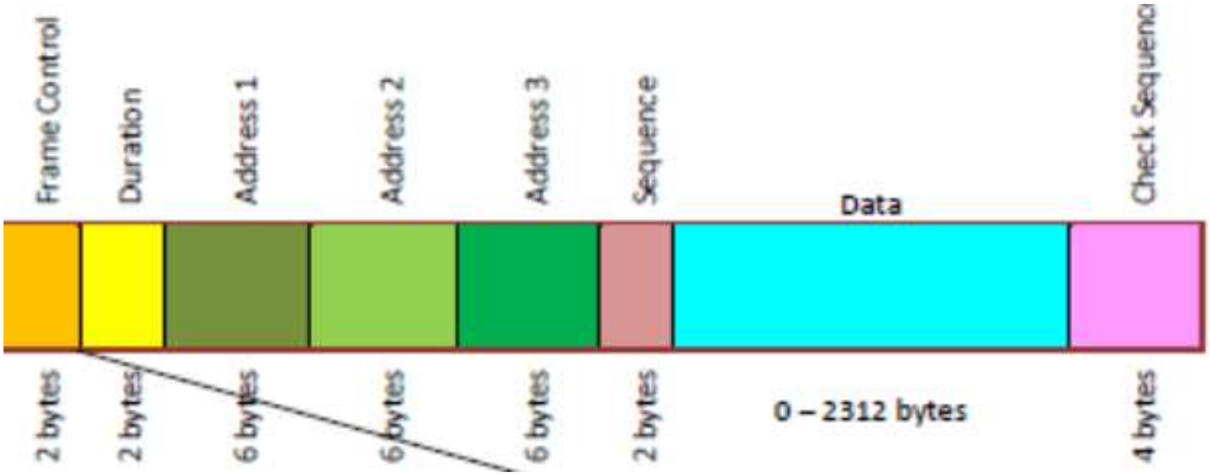


Station Types

- IEEE defines three types of stations based on the station mobility in WLAN.
- A station with **no-transition mobility** is either stationary (not moving) or moving only inside a BSS.
- A station with **BSS-transition mobility** can move from one BSS to another, but inside one ESS.
- A station with **ESS-transition mobility** can move from one ESS to another, but the communication may not be continuous.

802.11 FRAM FORMAT

MAC Frame: The MAC layer frame consists of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



1. **Frame Control(FC) –** It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC such as: Version, Type , Subtype et
2. **Duration/ID –** It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in µs).
3. **Address fields**: There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
4. **SC (Sequence control) –** It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
5. **Data –** It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
6. **CRC (Cyclic redundancy check) –** It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.