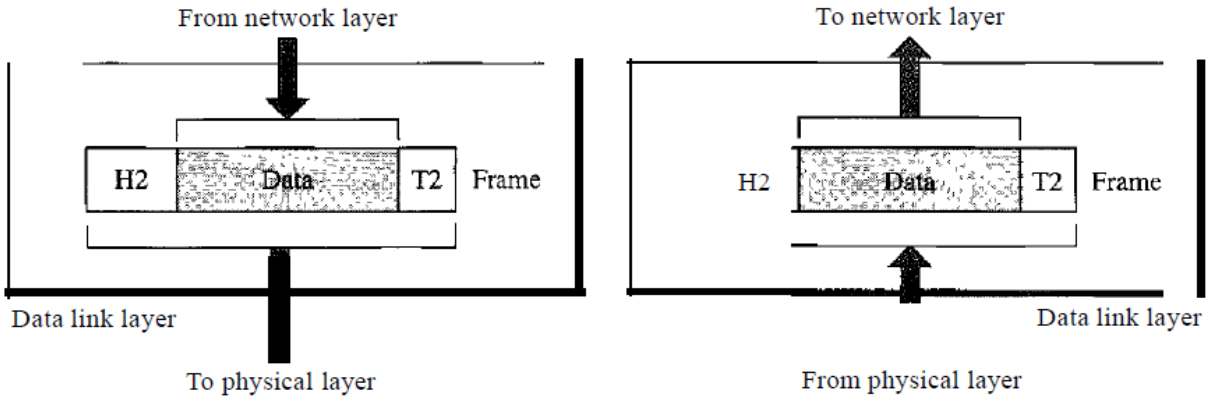
Unit – II

Data Link Layer – Design Issues:

The data link layer transforms the physical layer, and raw information's is transmitted to a reliable link. It make physical layer appear error – free to the upper layer i.e. network layer.



Above figure shows that relationship between the data link layer to n/w layer and physical layer.

The responsibility of the data link layer is to move frames one hop (node) to the next hop.

The data link layer uses the services of the physical layer to send and receive bits over the communication channel.

1. It has to provide well – defined service interface to network layer.
2. Dealing with transmission errors
3. Regulating the flow of data so that slow receiver are not swamped by the fast senders.

Framing

The data link layer divides the stream of bits received from the n/w layer into manageable data units called frames.

Each frame contains a head, a pay load field for holding the packet a frame trainer.

Physical Addressing

If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and or receiver of the frame.

Flow control

When a sender systematically wants to send frames faster than the receiver can accept them.

The rate at which the data are absorbed by the receiver less than the rate at which the data are produced in the sender

The data link layer imposes a flow control mechanism to avoid over whelming the receiver.

Error Control

The data link layer adds reliability to the physical layer by adding mechanism to defect and retransmit damaged or lost frames.

It also uses a mechanism to recognize duplicate frames

Error control is normally achieved through a trailer adder to the end of the frame.

Access Control

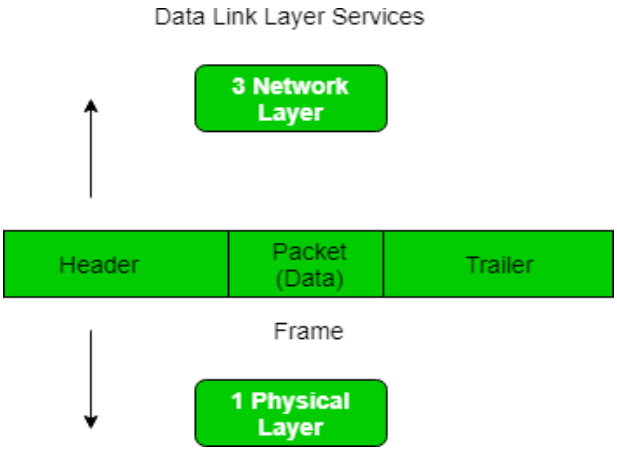
When two or more devices are connected to the same link, the data link layer protocols are necessary to determine which device has control over the link at any given time.

Design Issues

1. Services to Network layer

2. Framing in Data Link Layer

Frames are the units of digital transmission particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in case of light energy. Frame is continuously used in Time Division Multiplexing process. Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. 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. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.



At data link layer, it extracts message from sender and provide it to receiver by providing sender's and receiver's address. The advantage of using frames is that data is broken up

into recoverable chunks that can easily be checked for corruption.

Problems in Framing –

- **Detecting start of the frame:** When a frame is transmitted, every station must be able to detect it. Station detect frames by looking out for special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).
- **How do station detect a frame:** Every station listen to link for SFD pattern through a sequential circuit. If SFD is detected, sequential circuit alerts station. Station checks destination address to accept or reject frame.
- **Detecting end of frame:** When to stop reading the frame.

Types of framing – There are two types of framing:

1. Fixed size – The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.

- **Drawback:** It suffers from internal fragmentation if data size is less than framesize
- **Solution:** Padding

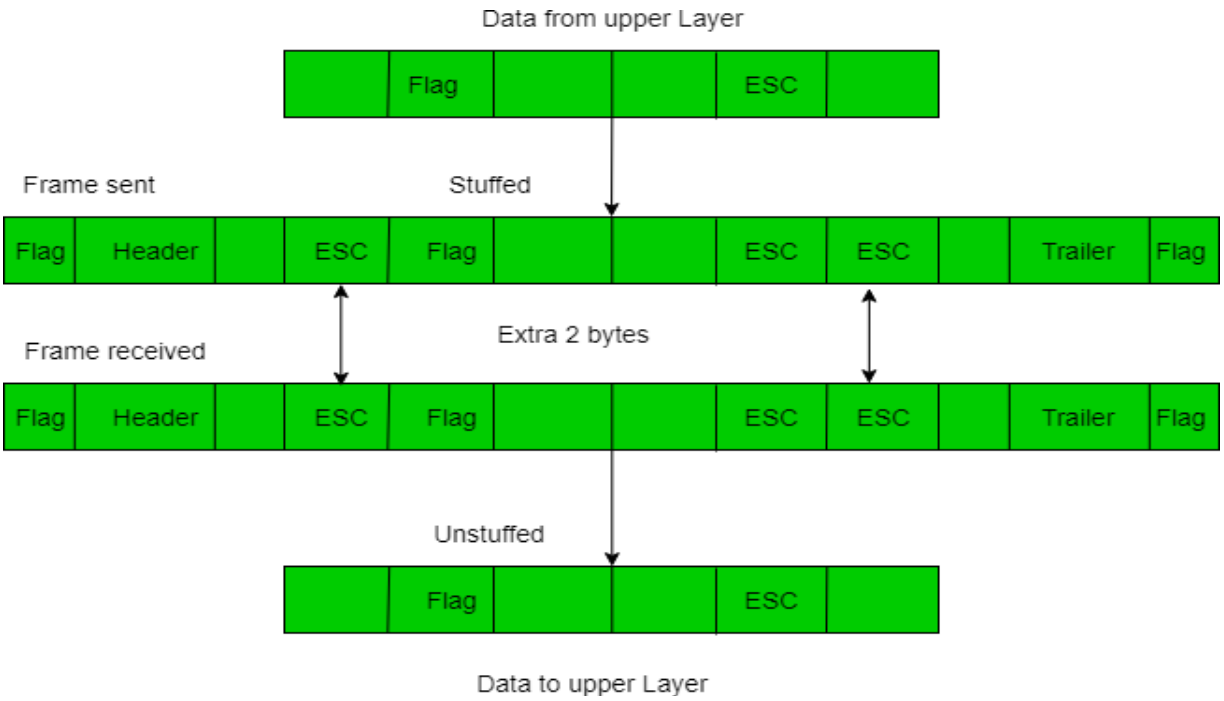
2. Variable size – In this there is need to define end of frame as well as beginning of next frame to distinguish. This can be done in two ways:

1. **Length field (Character Count) –** We can introduce a length field in the frame to indicate the length of the frame. Used in **Ethernet(802.3)**. The problem with this is that sometimes the length field might get corrupted.
2. **End Delimiter (ED) –** We can introduce an ED(pattern) to indicate the end of the frame. The problem with this is that ED can occur in the data. This can be solved by:

   1. Character/Byte Stuffing: Used when frames consist of character. If data contains ED then, byte is stuffed into data to differentiate it from ED.

   Let ED = "$" –> if data contains '$' anywhere, it can be escaped using '\O' character.

   –> if data contains '\O$' then, use '\O\O\O$'($ is escaped using \O and \O isescaped using \O).



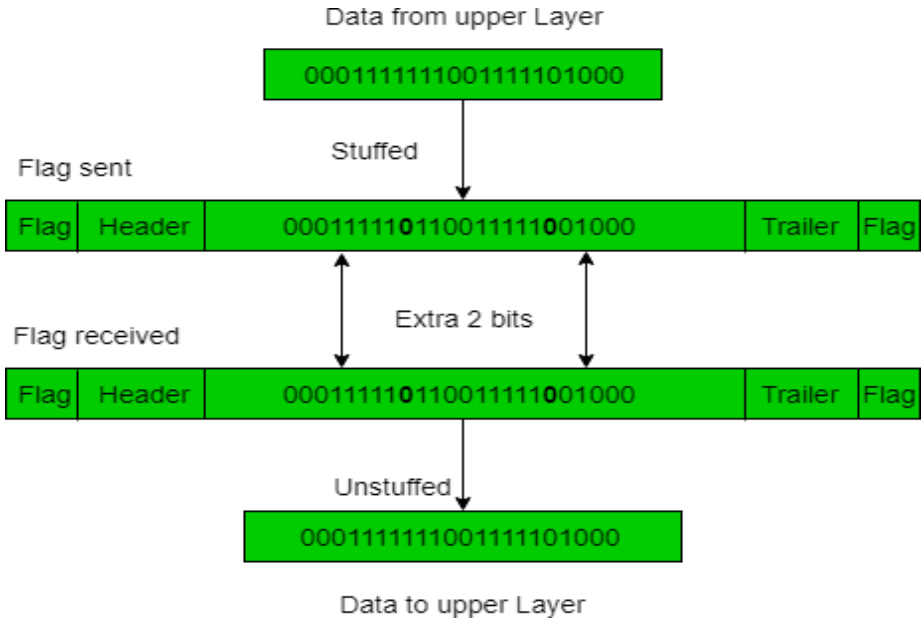
Disadvantage – It is very costly and obsolete method.

2. Bit Stuffing: Let ED = 01111 and if data = 01111

–> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data =0111**0**1.

–> Receiver receives the frame.

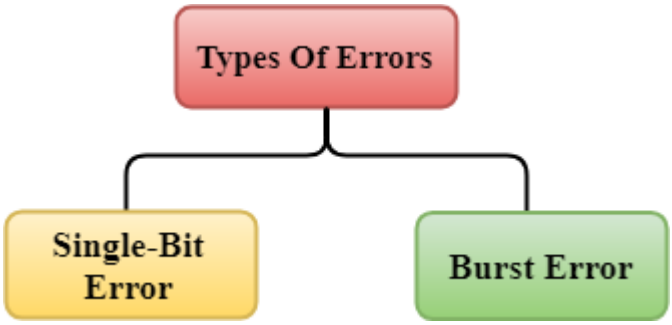
–> If data contains 01101, receiver removes the 0 and reads the data.



3. Error Detection & Correction

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Types of Errors:



Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.

Burst Error:

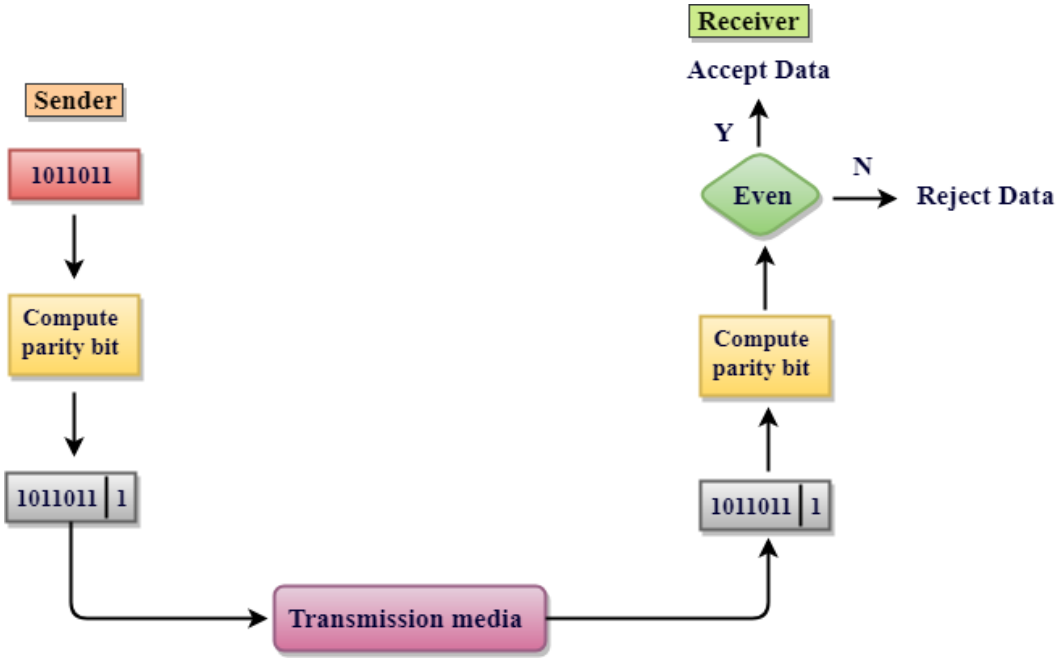
The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

Error Detection Techniques:

i) Parity check

- Parity checking is the simple mechanism and inexpensive to detect the errors.
- In this technique, a redundant bit is also known as a parity bit which is appended at the end of the data unit so that the number of 1s becomes even. Therefore, the total number of transmitted bits would be 9 bits.
- If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

- At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.
- This technique generates the total number of 1s even, so it is known as even-parity checking.



Drawbacks of Single Parity Checking

- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.

ii) Checksum:

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data. When the receiver gets this data, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error.

Error Detection by Checksum

For error detection by checksum, data is divided into fixed sized frames or segments.

- **Sender's End** − The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.

- **Receiver's End** − The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

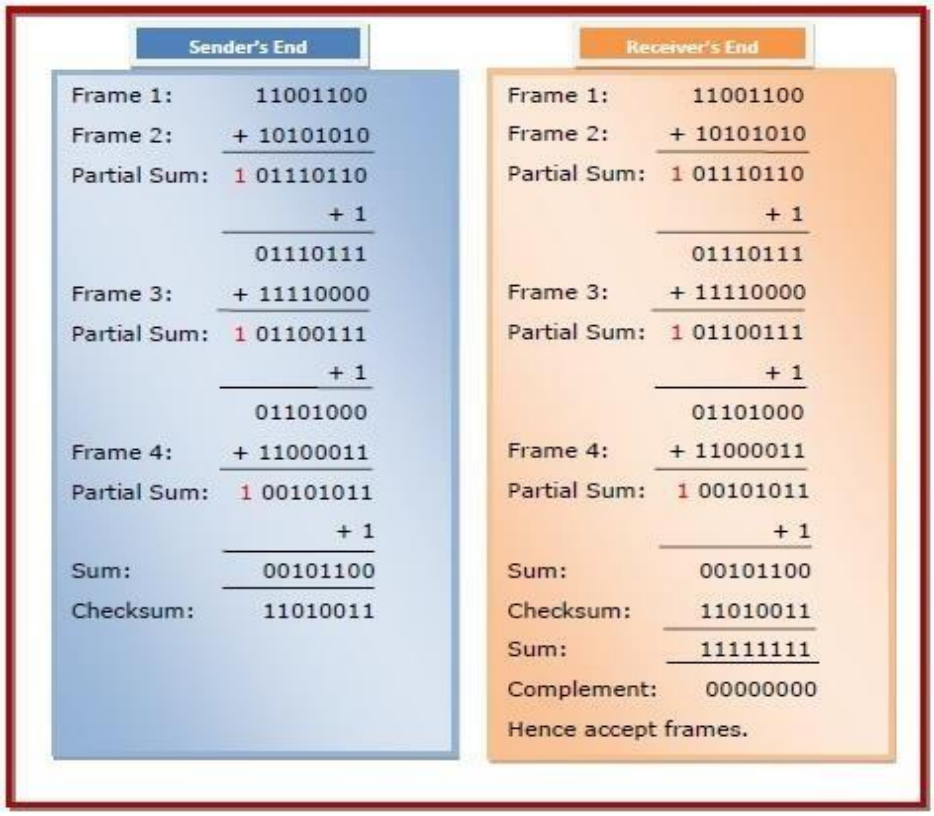
If the result is zero, the received frames are accepted; otherwise they are discarded.

Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.

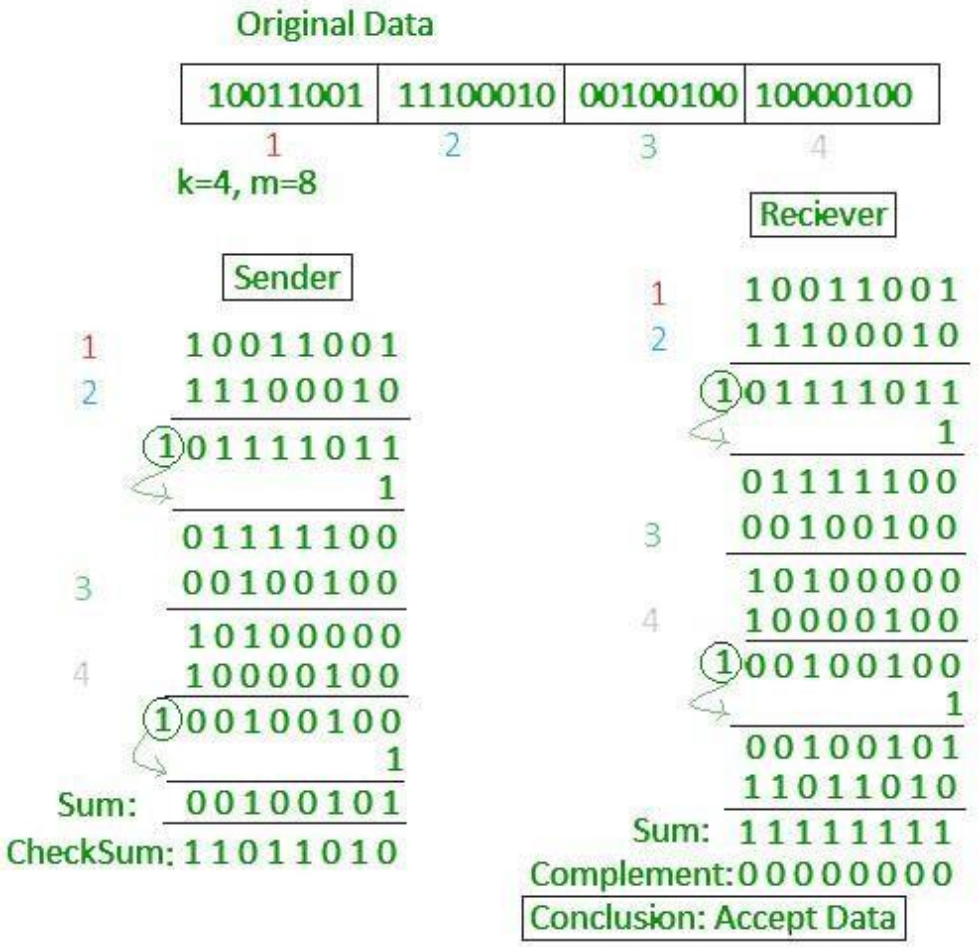
The sender adds the bits using 1s complement arithmetic. While adding two numbers using 1s complement arithmetic, if there is a carry over, it is added to the sum.

After adding all the 4 frames, the sender complements the sum to get the checksum, 11010011, and sends it along with the data frames.

The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.



- In checksum error detection scheme, the data is divided into k segments each ofm bits.
- In the sender's end the segments are added using 1's complement arithmetic toget the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- 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.



iii) Cyclic Redundancy Check Codes:

In order to send the data from sender to receiver, the data must be checked and preceded with zero errors to receiver.

CRC (cyclic redundancy check) is also called as polynomial code.

Polynomial codes are based on the treating bit string as representations of polynomials with co – efficient of 0 and 1 only.

It is used in networks such as LANS and WANS.

In sender or encoder, the generator has k bits (4 – bits) the code word has n bits (7 – bits) are given by as per the structure.

Generator is : 1 1 0 1

Data word is : 1 0 1 1 0 1 1

The size of the data word is appended by n – k (bits) 0s to the right hand side of the code word.

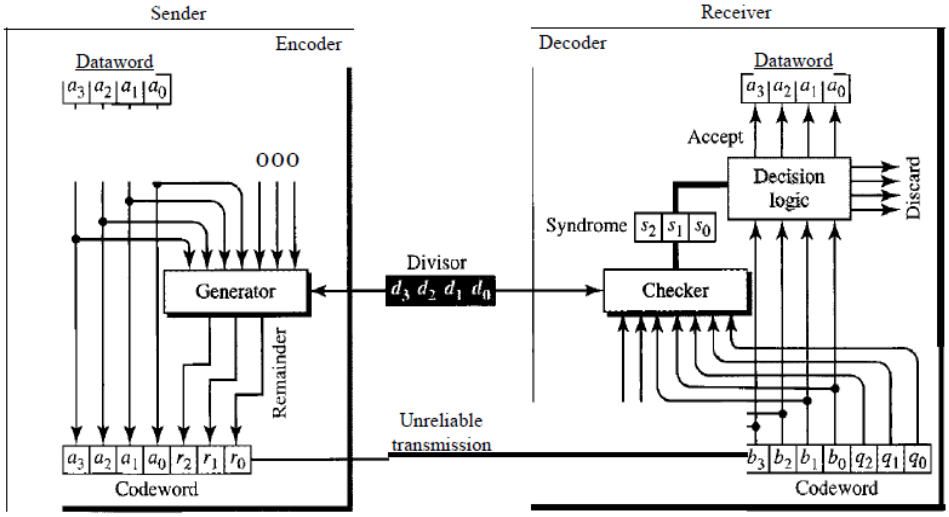
The CRC generator has 4 – bits, so (4-1) three zeros has to be added to data word. Therefore, the code word is given by: 1 0 1 1 0 1 1 0 0 0

The generator divides the augmented data word by divisor (modulo – 2 divisions), the quotient of the division is discarded.

The reminder is appended to the data word to create the code word.

A copy of all n – bits is fed to the checker which is replica of the generator.

The remainder produced by the checker is a syndrome of n – k (3 – bits) which is fed to decision logic analyzer.



The analyzer has to perform simple function like if the syndrome bits are all 0s, the 4 left most bits of the code word are accepted as the data word (interpreted as no error) otherwise the bits are non – zero mean (interpreted as error) and are discarded.

Example:

Perform CRC check for error force data transmission to receiver. generator is: 1 1 0 1 and data word is given by: 1 0 1 1 0 1 1.

Solution:

Generator : 1 1 0 1 (k – bits)

Dataword : 1 0 1 1 0 1 1 (n – bits)

Cyclic redundancy generators is: (k-1) = 0 0 0 (3 – bits)

The 3 – bits are append to the data word to check CRC

Perform a division operation with code word.

i.e., by modulo – 2 division it also represents EX – OR like operation

```
          1 1 1
      ------------------
1 1 0 1) 1 0 1 1 0 1 1 0 0 0  (
         1 1 0 1
      ------------------
         0 1 1 0 0 1 1 0 0 0
           1 1 0 1
      ------------------
         0 0 0 1 1 1 0 0 0
               1 1 0 1
         ---------------
             0 0 1 1 0 0
                 1 1 0 1
             -----------
               0 0 0 1   → CRC – bit
```

Case 1:

In the above operation last bit is ‘1’ the CRC both is append to the code word to check error free transmission.

Checking at the receiver side

```
          1 1 1 1
      ------------------
1 1 0 1) 1 0 1 1 0 1 1 0 0 1  (
         1 1 0 1
      ------------------
         0 1 1 0 0 1 1 0 0 1
           1 1 0 1
```

~~0 0 0~~ 1 1 1 0 0 1
1 1 0 1

~~0 0~~ 1 1 0 1
1 1 0 1
0 0 0 0 → Syndrome is ‘0’.

If code word have a corrupted bit, for such cases single error may occur, which will be discarded.

Case 2:

1 1 0 1) 1 0 [1] 1 0 1 1 0 0 1 (
0 → Corrupted bit – replaced as ‘0’

1 1
1 1 0 1) 1 0 0 1 0 1 1 0 0 1 (
1 1 0 1

~~0~~ 1 0 0 0 1 1 0 0 1
1 1 0 1

~~0~~ 1 0 1 1 1 0 0 1
1 1 0 1

~~0~~ 1 1 0 1 0 0 1
1 1 0 1
~~0 0 0 0~~ 0 0 1 → Syndrome is ‘1’→ Error Bit

In this case data word not accepted, discarded due to non – zero CRC – bit occur.

For an successful transmission of data is selected by the checking of CRC must done with above manner.

Error Correction Code

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is a technique developed by R.W. Hamming for error correction.

The number of redundant bits can be calculated using the following formula:

$$2^r \geq m + r + 1$$

where, r = redundant bit, m = data bit

General Algorithm of Hamming code: Hamming Code is simply the use of extra parity bits to allow the identification of an error.

1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form. **a.** Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc). **b.** Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc). **c.** Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc). **d.** Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc). **e.** In general, each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

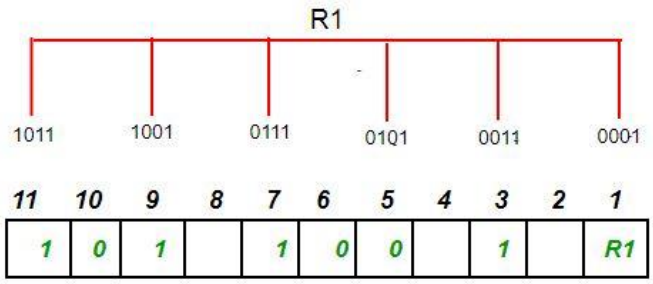
Determining the position of redundant bits – These redundancy bits are placed at positions that correspond to the power of 2.

- Suppose the data to be transmitted is 1011001, the bits will be placed as follows:

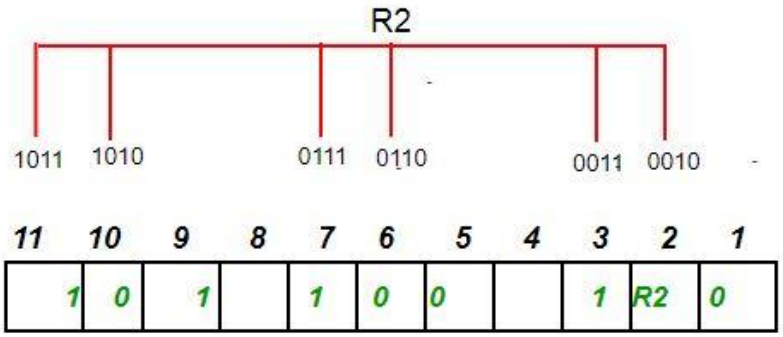
11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	R4	1	R2	R1

Determining the Parity bits:

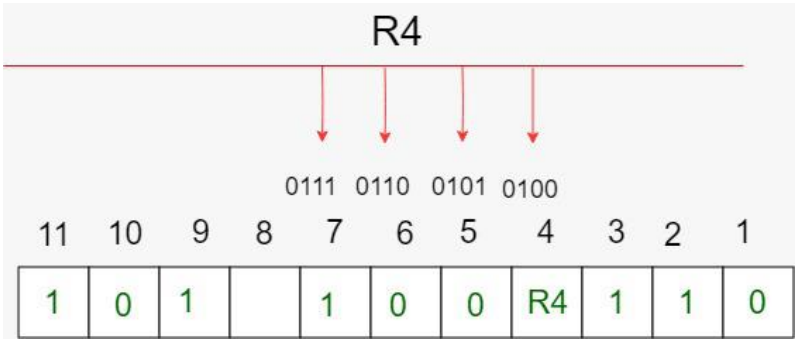
- R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position. R1: bits 1, 3, 5, 7, 9, 11



- To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0
- R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit. R2: bits 2,3,6,7,10,11

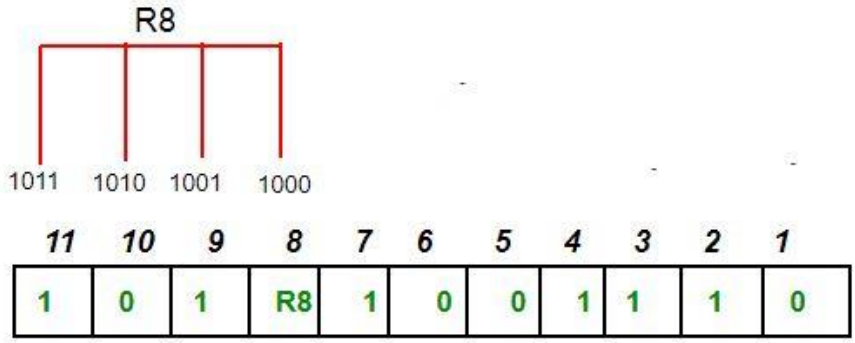


- To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1
- R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit. R4: bits 4, 5, 6, 7

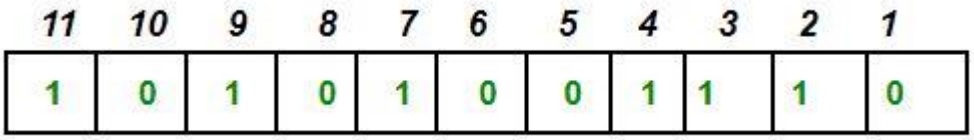


- To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1
- R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit. R8:

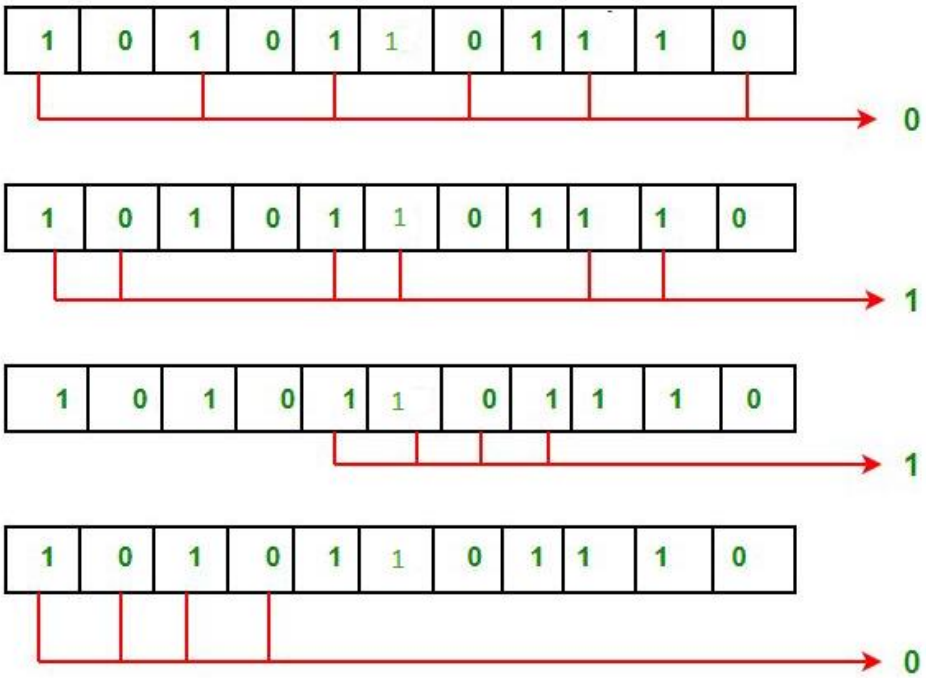
8,9,10,11. bit



- To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0. Thus, the data transferred is:



Error detection and correction: Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:

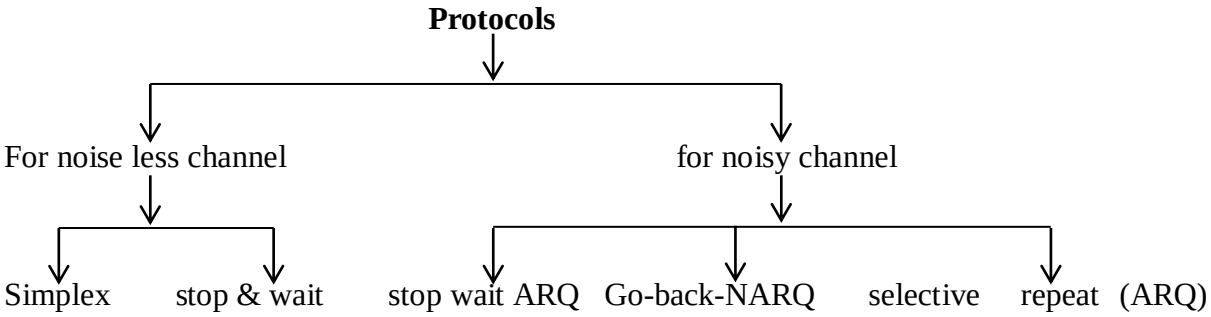


The bits give the binary number 0110 whose decimal representation is 6. Thus, bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

Elementary Data Link Layer Protocols:

A protocol is a set of rules that govern data communications and it represents an agreement between the communicating devices.

The protocols that can be used for noiseless (error – free) channels and those that can be used for noisy (error – creating) channels.



At the protocols that are Uni-directional in the sense that the data frames travel from one node called sender to another node called receiver.

The special frames are called acknowledgement (ACK). Negative acknowledgement (NAK) can flow in the opposite direction for flow and error control purposes, data flow in only one direction.

Simplex Protocol:

The simple protocol is one that has no flow (or) error control.

It is a unidirectional protocol n which data frames are travelling in only one directional from the sender to receiver.

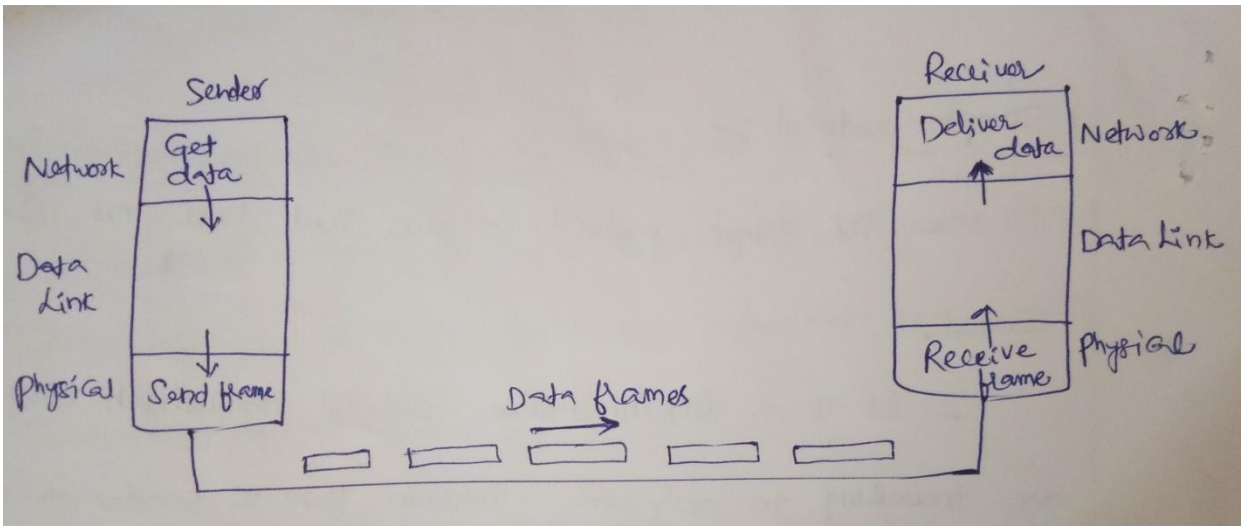
Assume that the receiver can immediately handle any frame it receives with a processing time that is small enough and negligible.

The data link layer of the receiver immediately removes the header from the frames and takes the data packet to its network layer.

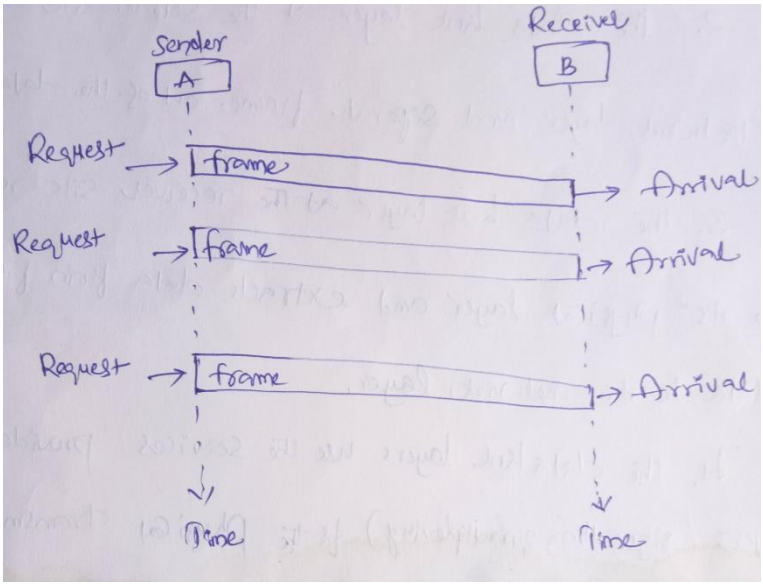
The design issues are given by for simple protocol is

1. There is no need for flow control process.
2. The data link layer at the sender site gets data from its network layer and separate frame out of the data and send it
3. The data link layer at the receiver site receives a frame from its physical layer and extracts data from frame and delivers the data to its network layer.

4. The data link layers use the services provided by their physical layers (signaling and multiplexing) for the physical transmission of bits.



5. The sender site cannot send a frame until its network layer has a data packets to send and the receiver site cannot deliver a data packet to its network layer until a frame arrives.
6. Suppose, if the protocol is implemented as a procedure, introduce an event in the protocol. The procedure at the sender site is also constantly running there is no action until a request from the network layer.
7. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives.



From above figure, the sender sends a sequence of frames without even thinking about the receiver.

In order to send three frames, three events occur at the sender site and three events at the receiver site.

Stop – And – Wait Protocol:

If the data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use.

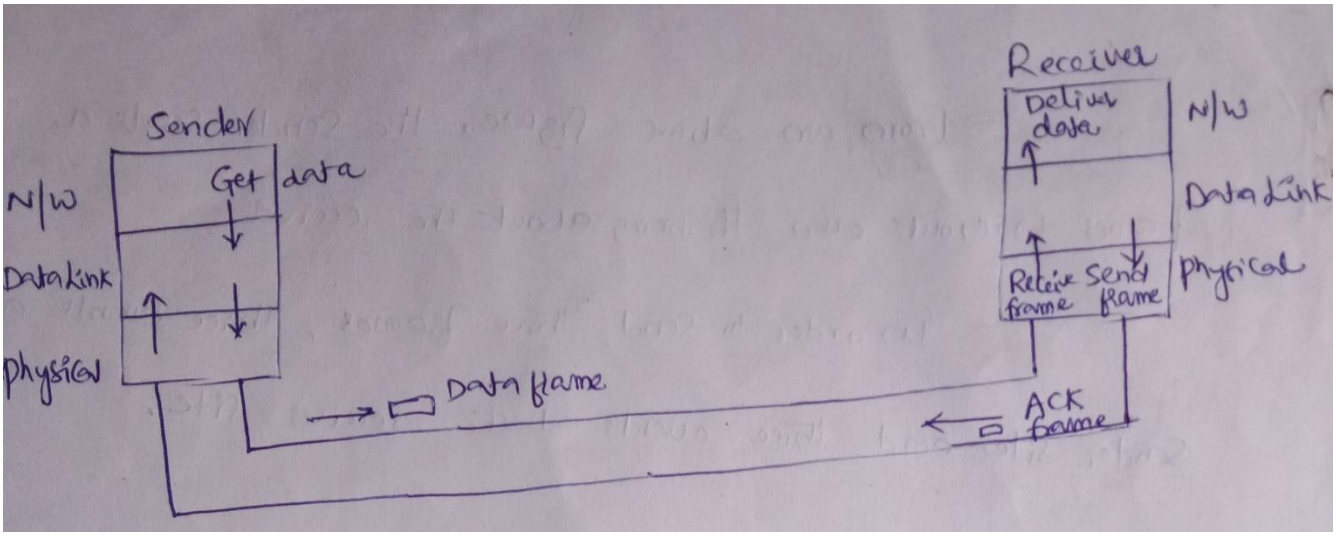
The receiver does not have enough storage space, especially it is receiving data from many sources, which may result in either the discarding of frames or denied the service.

In order to discarding of frames we need to tell the sender to slowdown.

In a stop – and – wait protocol, the sender sends one frame stops until it receives confirmation from the receiver and then sends the next frame.

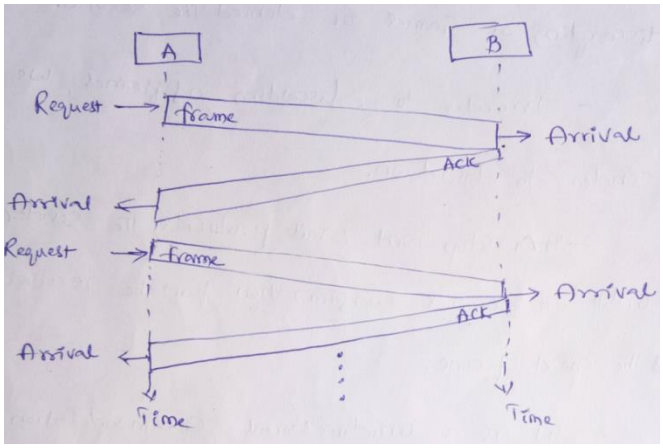
It is a unidirectional communication for data frames, but auxiliary ACK frames (acknowledgment) travel from other direction.

We add flow control to this protocol.



From an above figure, at any time there is either one data frame on the forward channel or one ACK frame on the reverse channel.

The link is like a half-duplex



The sender sends one frame and waits for feedback from the receiver. When acknowledgement arrives, the sender sends the next frame.

Note: sending two frames in the protocol involves the sender in four events and receiver in two events.

Noisy Channel Protocols

Sliding Window Protocol:

Sliding window is one of the method of error correction. To increase the data rate, this method allows the sender to transmit a specific number of packets in continuous mode. i.e., at the maximum possible rate.

The no. of packets that can be transmitted in such a way that i.e. window size.

Window size can be constant parameter, which means that it is chosen at connection setup and does not change entire session.

If the destination receives the packet with corrupted data, it might send a negative acknowledgement (NAKK), specifying that the packet needs to be retransmitted.

When a data frame arrives, instead of immediately sending a separate control frame, the receiver restrains itself and waits until the network layer passes it the next packet.

Sender Window Size

It is a list of consecutive frame sequence numbers that can be sent by the sender or that have been sent and acknowledgment are waited for.

When an ACK arrives and all previous frames have already been acknowledged the window can be transmitted with next highest available sequence number

Receiver Window Size

It is a list of sequence numbers for frames that can be accepts by the receiver.

When a valid frame arrives and previous frames have already arrived the window is advanced. If a frame arrive that is not with in the ‘window’ is discarded.

Advantages

1. Sliding window is simpler, having only one set of parameters to manage.
2. Simultaneous communication in both direction is possible
3. Better utilization if n/w band width especially if there are large transmission delays.
4. Traffic flow with reverse traffic data, known as piggy backing.

Stop & Wait ARQ:

This is the simplex protocol with sequence numbers and with ACK frame indicating the sequence number of the next frame expected.

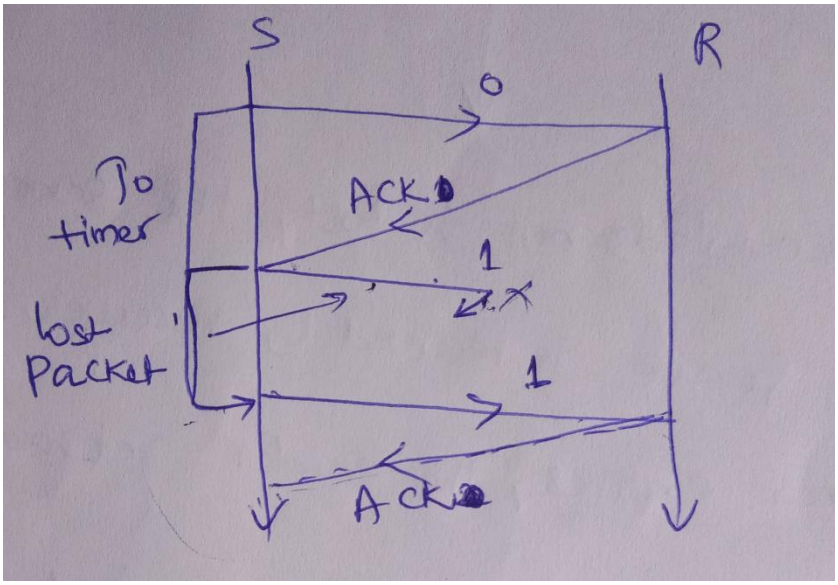
In this sliding protocol, the maximum window size of 1. Such protocol uses stop & wail protocol since the sender transmits a frame and waits for its acknowledgements before sending to the next one.

One – bit sliding window protocol is also called stop wait – ARQ.

The following issues, which may occur in stop and wait protocol are

1. Data packet lost
2. Acknowledgement lost
3. Delayed acknowledgement

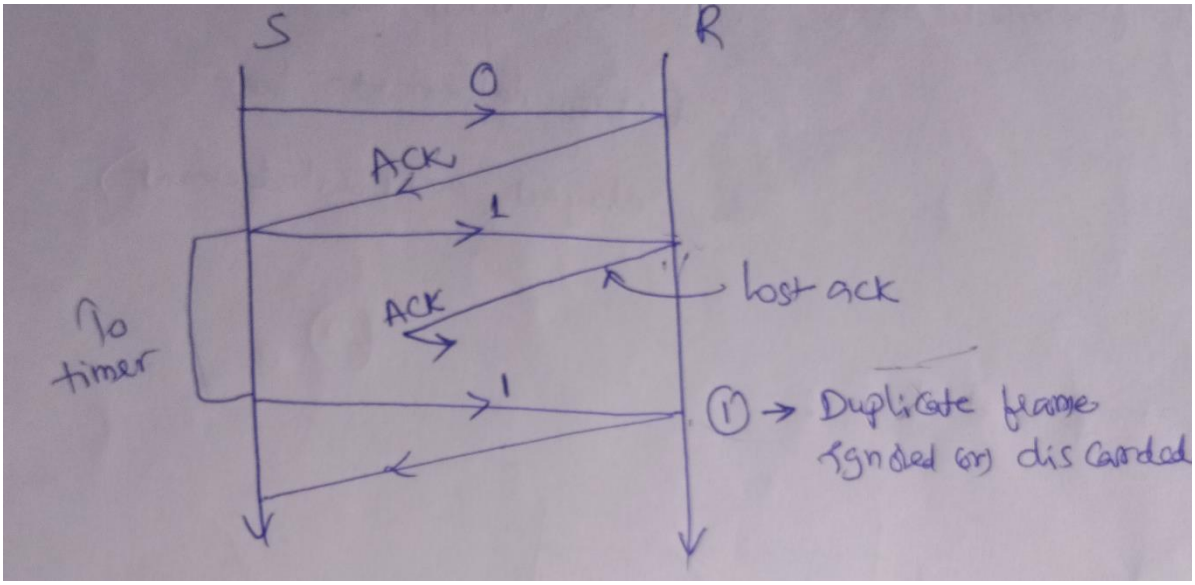
Data Packet Lost



In a above data packet lost, when a receiver receivers the frame and found it damaged or lost, it is discarded but retains its number, when sender does not receive its acknowledgement it retransmits the same frame, when timer expires. ("To → Time out times for retransmitting of packets).

Usually a timer is set by sender after each frame is transmitted, its acknowledgement must be received before timer expires.

Acknowledgement Lost



When an acknowledgement is lost the sender does not know whether the frame is received by receiver.

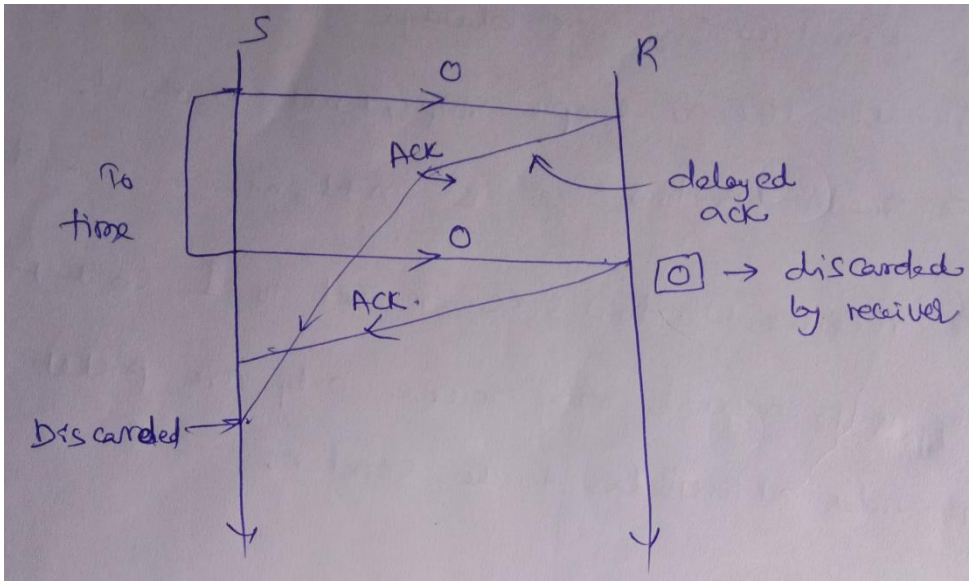
As for the timer expires, the sender retransmitted the same frame. On the other hand, receiver has already received this frame earlier hence sender copy of the frame is discarded.

So the sender will think about sending the data packets in frames by providing sequence numbers.

Delayed Acknowledgement

The ACK frame may be delayed due to some link problem. The ACK is received after the time r is elapsed.

While the sender has already transmitted the same frame Again second ACK is initiated by receiver for the transmitted frame, hence the second ACK is discarded.



In order to avoid duplication the acknowledgment numbered. (S & W + To + sequence number to acknowledgements).

Go Back N (GBN) Protocol:

Go back N uses the sliding window flow control protocol. If no errors occurs the operations are identical to sliding window.

A station may send multiple frames as allowed by the window size.

The Go Back N follows the methods to approach error force transmission with frames /packet.

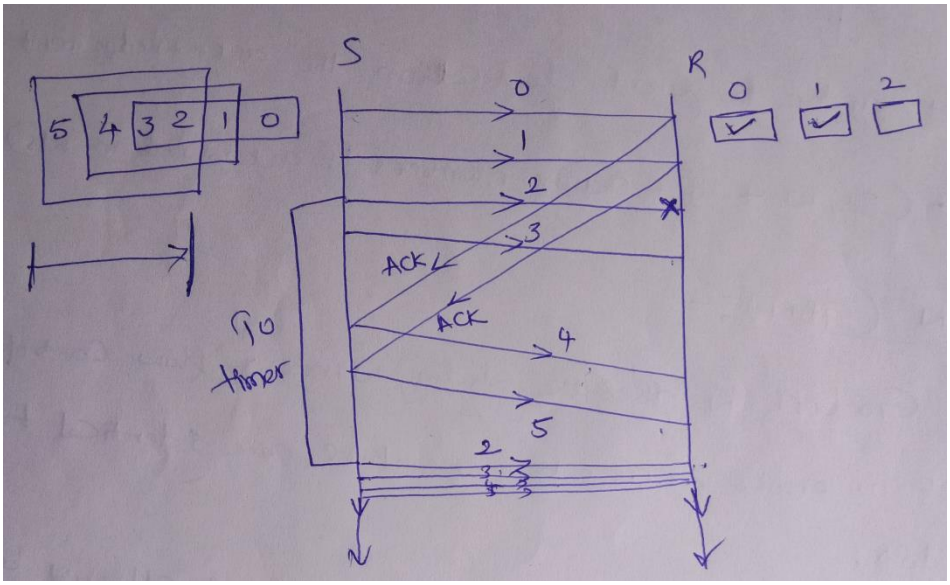
1. Sender window size ($W_S > 1$)
2. Receiver window size ($W_R = 1$)
3. Acknowledgements (cumulative & independent acknowledgements)

Sender Window Size

The sender window is always greater than one, otherwise it acts like a simple stop & wait protocol.

The sender window size is n+1, n+2 . ……etc

Receiver window size: is set to 1 so that the capability of the receiver may receive only one packet at a time provides acknowledgment to the sender.



From an above fig if any one of the packet may lost, the receiver cannot accepted the lost packet and could not send acknowledgement.

The sender may transmit next frames to the receiver (3,4 &5) receiver simply discard the frames because those are the out of order packets/frames the receiver tightly which may receiver only in order packets.

When the timer expires, the sender retransmits the frame (2), and simultaneously which transmits remaining packets same time.

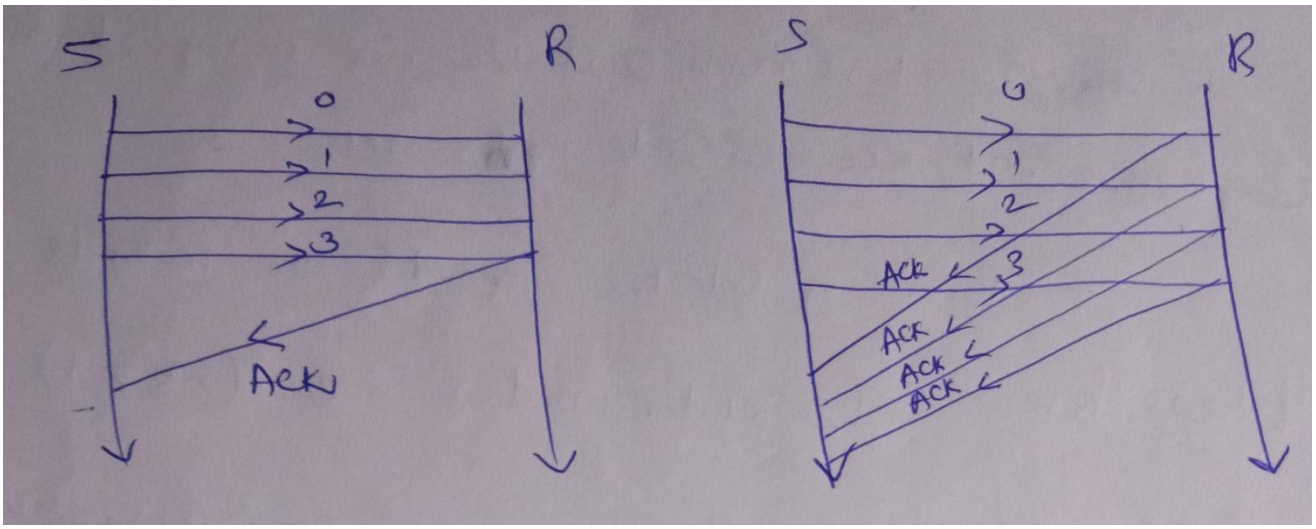
Acknowledgements

Acknowledgements are provided in the go back N are

1. Cumulative acknowledgement
2. Independent acknowledgement

Go Back N always use cumulative acknowledgement

Cumulative Acknowledgments & Independent Acknowledgment:



In cumulative acknowledgements, the sender may send more packets in a slot the receiver only and one particular acknowledgement to the sender.

The advantage of this cumulative acknowledgement is less traffic.

The drawback of this less reliable, be causes any one packet must be lost whole transmission from sender is collapsed.

In independent acknowledgement, for every packet there is an acknowledgement.

The advantage of this independent acknowledgement is more reliable, because any of the packets may lost, the sender sends remaining packets without any discrepancy

The drawback of this model is high traffic.

Selective Repeat (SR) Protocol:

The selective repeat ARQ is the model in which retransmits only the damaged packets instead of sending multiple frames.

The selective retransmission increases the efficiency of transmission and is more suitable for noisy channel. The Circuit complexities at receiver side increses.

By using selective repeat the methods which may follows here.

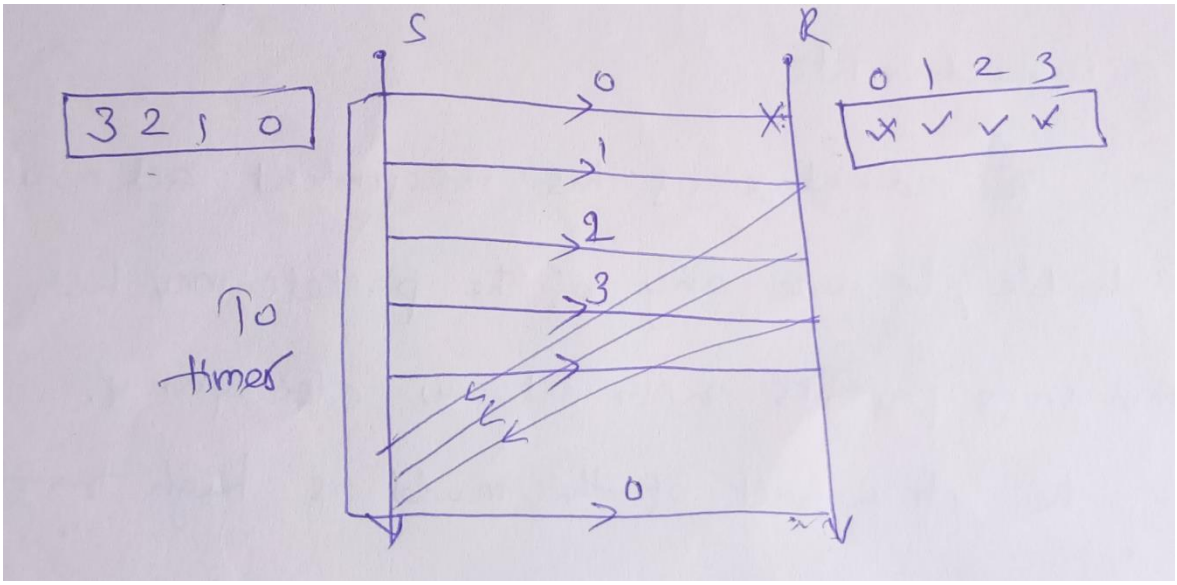
1. Sender window size ($W_S > 1$)
2. Receiver window size ($W_R = W_S$)
3. Acknowledgements (Negative acknowledgements)

Sender Window Size:

The sender window size is always greater than that of the selective repeat. In order to transmit more packets in a sender side.

Receiver Window Size:

The receiver window is equal to the sender window size is that the receiver is simply follows the sender to acknowledge the incoming packets.

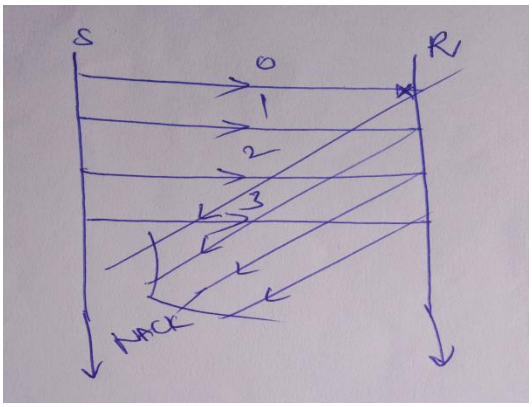


From an above figure, if the packet (0) is lost while sending receiver could not accept the packet and its accepts the packets (1,2,3) in the receiver window reference.

The lost packet is retransmitted when timer expire, during this event we transmit only the lost packet selectively. So this is called selective repeat (SR).

Acknowledgements:

So that the receiver which may provide negative acknowledgement for lost packet for retransmission.



In this negative acknowledgement the sender will assume that packet may lost and retransmit again.

In any stop & wait protocol, the transmit time is more that the acknowledgment time for successful packets delivery in order to improves the efficiency.

Example Data Link protocols

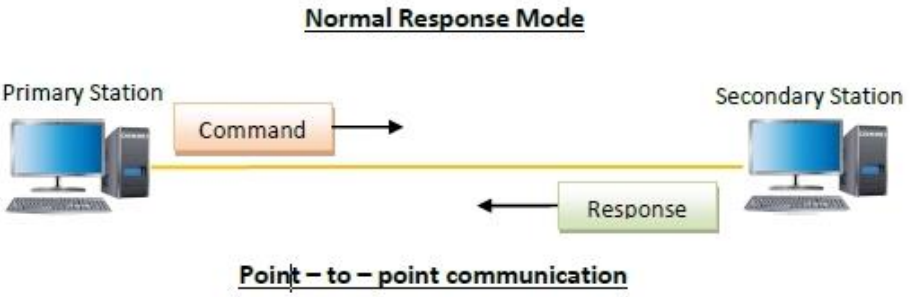
HDLC (High-level Data Link Control)

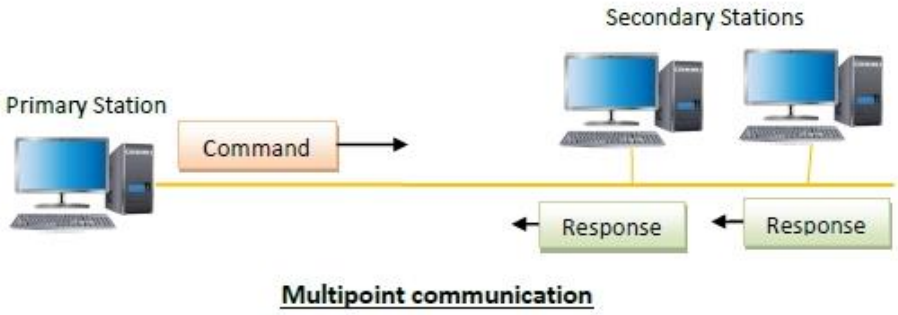
High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

Transfer Modes

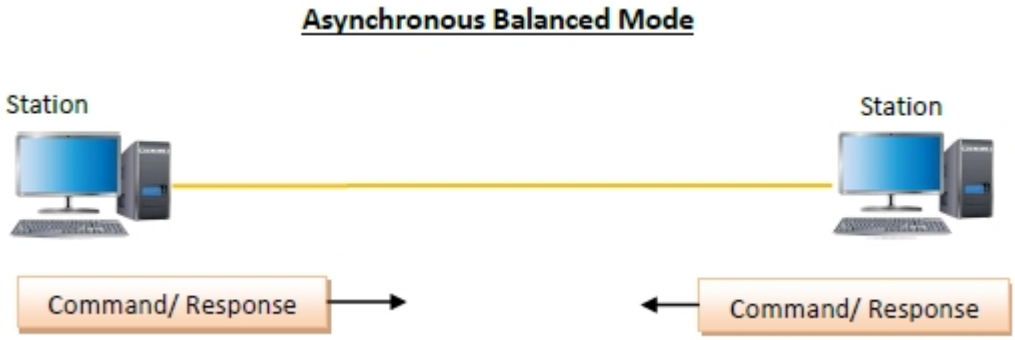
HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **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.





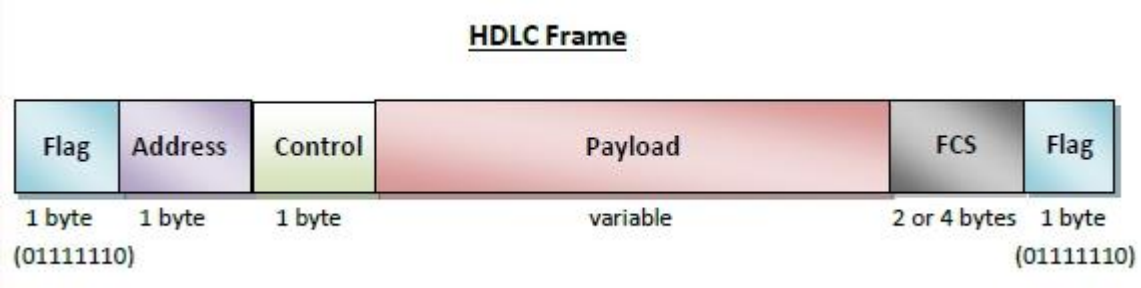
- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



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)

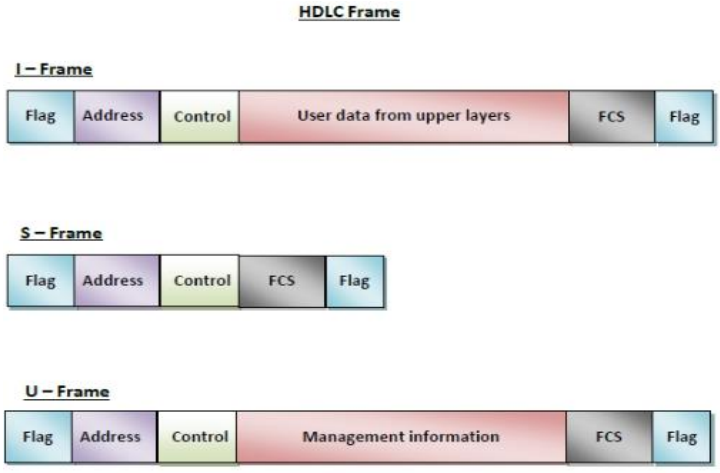


Types of HDLC Frames

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.



PPP (Point - to - Point Protocol)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range OS services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
    - Password Authentication Protocol (PAP)

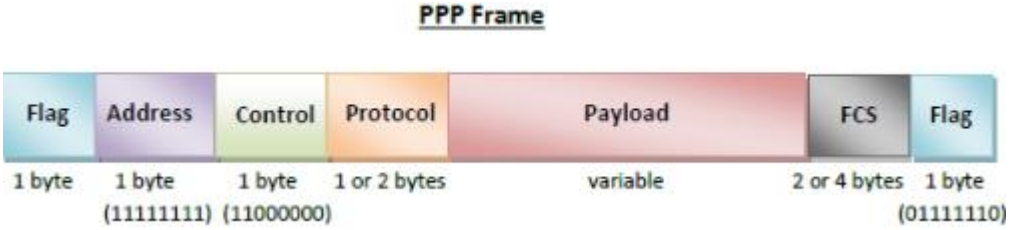
- Challenge Handshake Authentication Protocol (CHAP)

- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)
  - IPv6 Control Protocol (IPV6CP)

PPP Frame

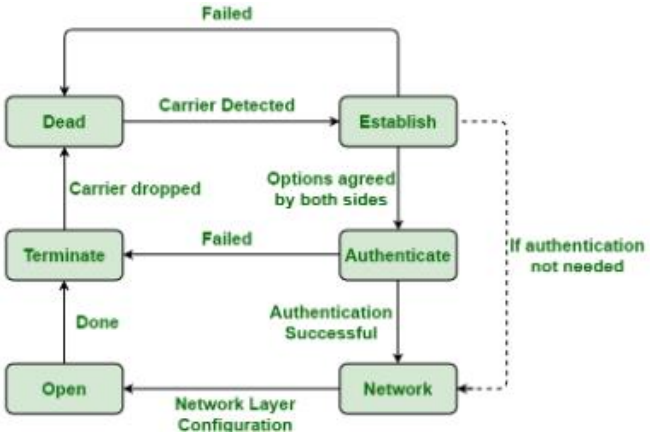
PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Byte Stuffing in PPP Frame − Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

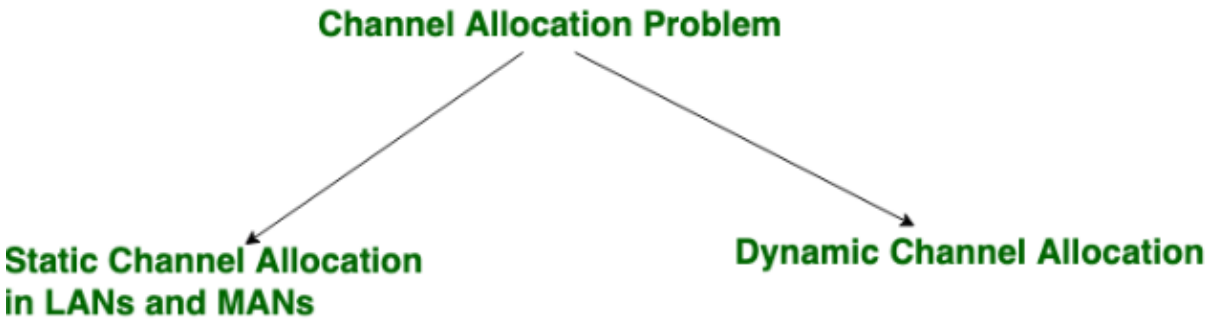
PPP Transition Phases



Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, then Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). if there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. since each user has a private frequency band, there is no interface between users.
It is not efficient to divide into fixed number of chunks

2. Dynamic Channel Allocation:
Possible assumptions include:

1. **Station Model:**
   Assumes that each of N stations independently produce frames. The probability of

producing a packet in the interval of length Δt is $I\Delta t$ where I is the constant arrival rate of new frames.

2. **Single Channel Assumption:**
   In this allocation all stations are equivalent and can send and receive on that channel.

3. **Collision Assumption:**
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must retransmitted. Collisions are only possible error.

4. **Time** can be divided into Slotted or Continuous.

5. **Stations** can sense a channel is busy before they try it.

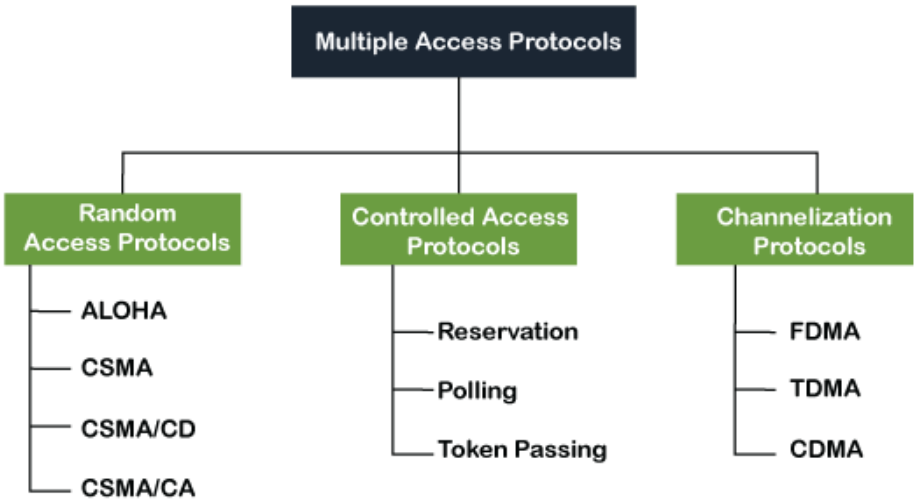
Protocol Assumption:

- N independent stations.
- A station is blocked until its generated frame is transmitted.
- Probability of a frame being generated in a period of length Δt is $I\Delta t$ where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

Multiple Access Protocol:

In LAN's the back bone is a street channel (or) transmission link, which provides all users to access the transmission facility. It may be possible that two (or) more stations transmitting simultaneously, causing their signals to interfere and becomes garbled.

In order to resolve this conflict no. of different control mechanism or access protocols have been given. Access the medium from many entry prints is called contention. It is controlled with in contention protocol. In a random access method, each station has the right to the medium without being controlled by other station. However if more than one station tries to send, there is an access conflict. i.e. collision and the frames will be either destroyed (or) modified.



The random access techniques are given by

1. ALOHA
2. Carrier sense multiple access (CSMA)
3. CSMA/CD (CD – collision detection)

1. ALOHA:

The ALOHA protocol was developed at the university of Hawaii in the earth 1970's

ALOHA was developed for packet radio networks it is used in any shared transmission medium.

In this multiple users try to send messages to other stations through a common broad cast medium i.e., random access or contention technique.

When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and becomes garbled

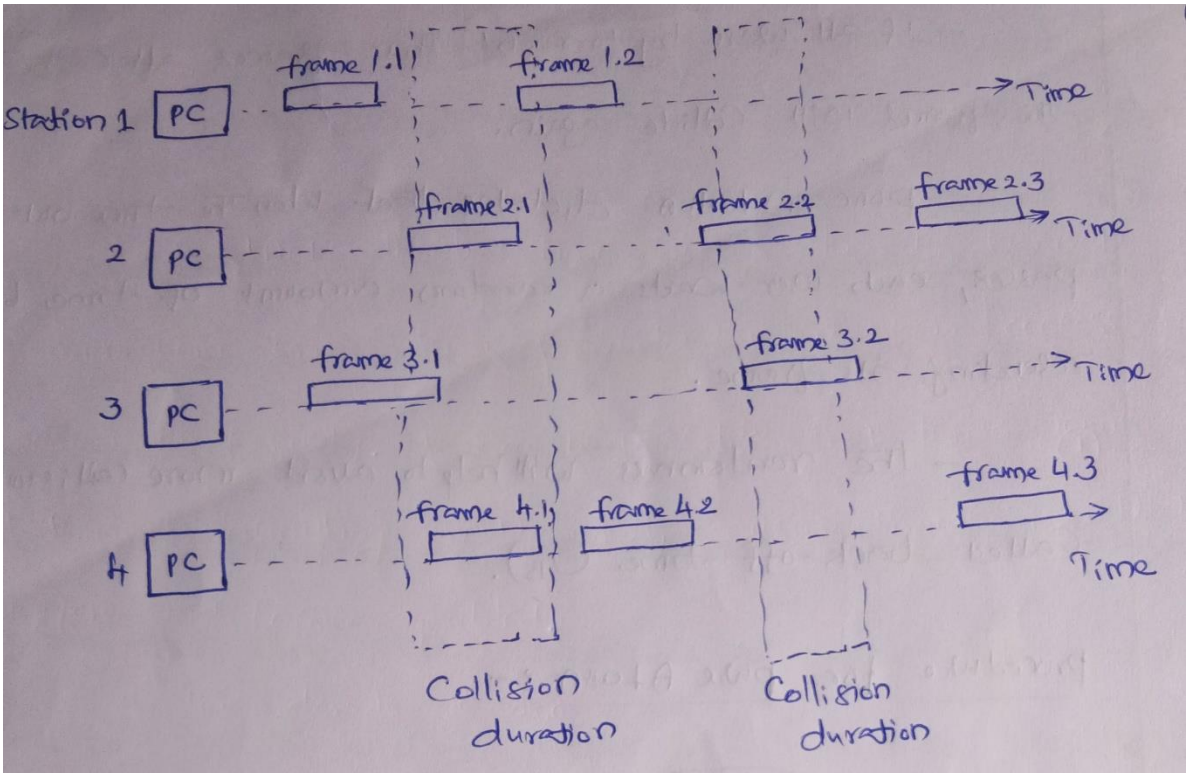
If two signals collided so, each station would simply wait a random time and try again.

PURE ALOHA:

The original ALOHA protocol is called pure ALOHA. it is a simple protocol, the idea given by the each station sends a frame wherever it has a frame to send.

Since there is only one channel to share, there is possibility of collision between frames from different stations

The below figure shows that frame collisions in pure ALOHA



The pure ALOHA relies on acknowledgements from the receiver. When a user sends a frame, it expects the receiver to send an acknowledgment.

If acknowledgement does not arrive after a time out period, the station assumes that the frame has been destroyed and resends the frames.

Whenever two frames try to occupy the channel at the same time, there will be collision and both will be garbled,

If the first bit of a new frame over laps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will be transmitted again.

If all users try to send their frames after the time out the frames will collide again.

Pure ALOHA dictates that when the time out period passes, each user waits a random amount of time before resending its frames.

The randomness will help to avoid more collisions. This is called back – off time (T_B)

Procedure For Pure ALOHA:

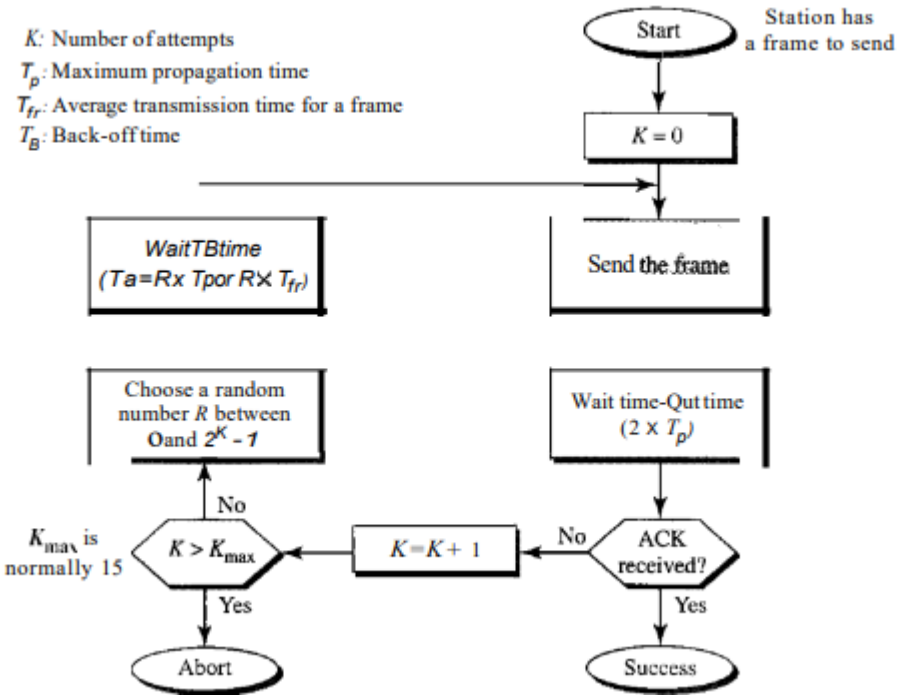
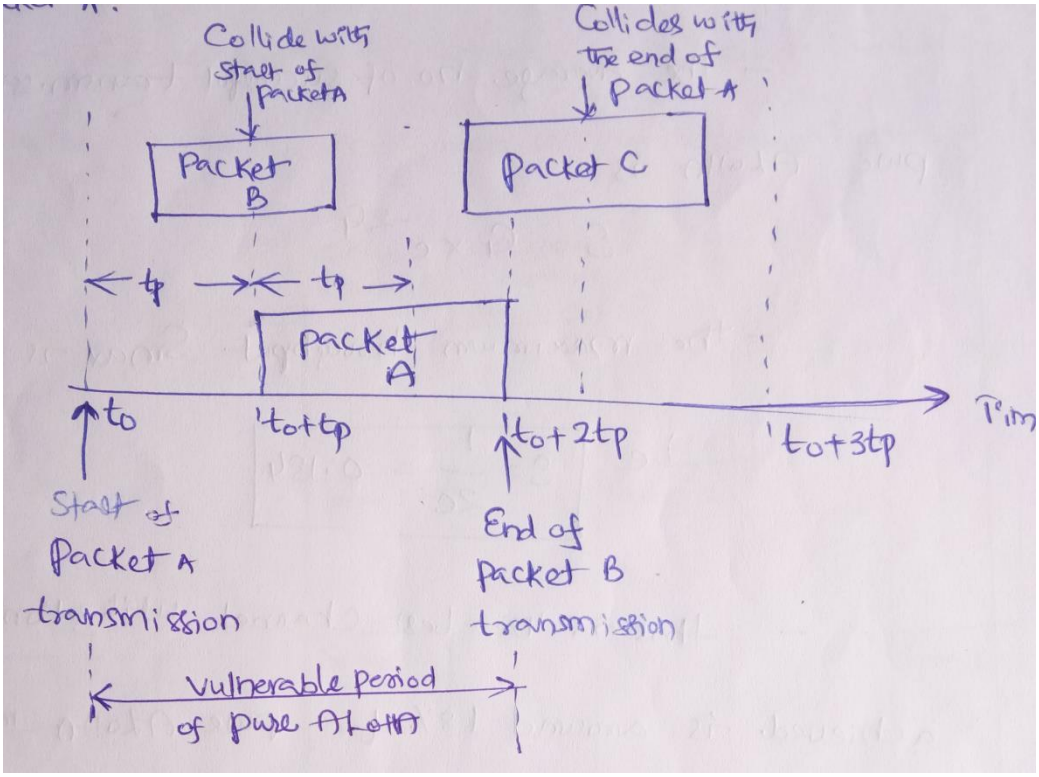


Figure: working for pure ALOHA

From an above flow chart, the time out period is equal to the maximum possible round trip propagation delay, which is twice the amount of time required to send a frame between the two moist widely separated stations$(2 \times J_p)$.

Let all the packets have same length and each required one time unit for transmission (t_p).

Consider any user to send a packet A at time to if any other user B has generated a packet between time to and $t_0 + t_p$, the end of packet B will collide with the beginning of packet A.



Since in pure ALOHA packet, a station does not listen to the channel before transmitting it has no way of knowing that above frames was already under way.

Similarly if another user wants to transmit between (t_0+t_p) and (t_0+2t_p) i.e, packet C, the beginning of packet C will collide with the end of packet A.

Thus if two packets overlap by even the smallest amount in the vulnerable period both packets will be corrupted and need to be retransmitted.

Through Put: the through put is defined as average successful traffic transmitted between stations per unit time.

The unit of time is slot – time, which is the time required to transmit a frame

The average no. Successful transmission time for pure ALOHA is

$$S = G \times e^{-2G}$$

The maximum throughput S_{max} is 0.184, for G = ½

$$\text{i.e.,} S = \frac{1}{2e} = 0.184$$

This is the best channel utilization that can be achieved is around 18% for pure ALOHA method.

Advantages: it is a simple protocol which can result in low cost stations since no synchronization is required between stations in the each system.

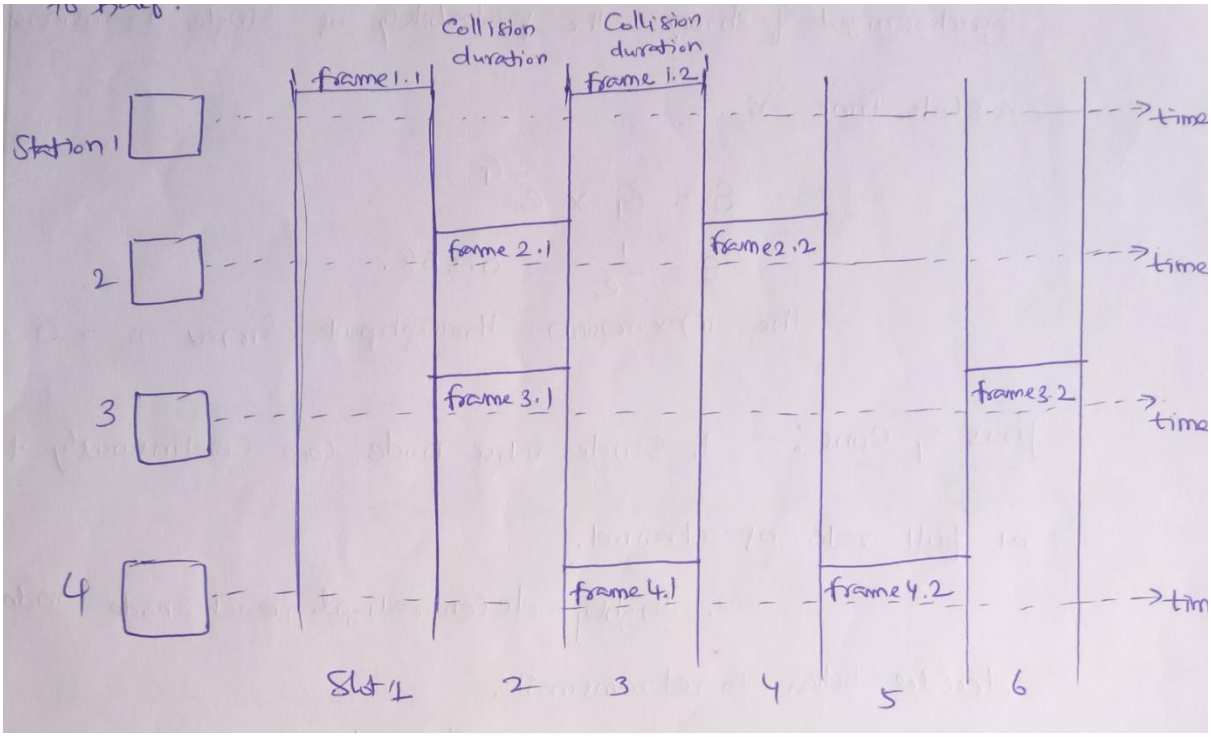
Slotted ALOHA:

It was invented for improve the efficiency of pure ALOHA.

In slotted ALOHA the synchronized to these time slots and the stations are allowed to transmit at specific instance of time.

All users are then synchronized to these time slots, so that whenever a user generates a packet it must synchronize exactly with the next possible channel slot.

Consequently the wasted time due to collision can be reduced to one packet time or vulnerable period is reduced to half.



Transmission attempts for four network user and random retransmission delays for colliding packets in slotted ALOHA.

Assumptions:

1. All frames are of same size.
2. Time is divided into equal size slots, a slot equals the time to transmit one frame.
3. Nodes start to transmit frames only at beginning of slots.
4. Nodes are synchronized
5. If two or more nodes transmit in a slot, all nodes detects collision before the slot ends.

Through of Slotted ALOHA:

In slotted ALOHA, the packets arrive in a synchronized fashion. The probability of single transmission during a slot time is

$$S = G \times e^{-G}$$

$$S = \frac{1}{e} = 0.368$$

The maximum through put S_{max} is = 0.368 $\therefore G = 1$

Pros & Cons:

1. Single active node can continuously transmit at full rate of channel.
2. Highly decentralized, each node independently divides when to retransmit.
3. Simple to implement

Cons:

1. Collisions waste slots
2. Idle slots.

2.Carrier Sense Multiple Accesses (CSMA)

In order to minimize the chance of collision and therefore increase the performance, CSMA was developed.

The low maximum through of the ALOHA schemes is due to the wastage of transmission band width because of frame collisions.

This wastage can be reduced by avoiding transmissions that are certain to cause collisions. By sending the medium for the presence of a carrier signal from other stations, a station can determine whether there is an ongoing transmission.

CSMA requires that each station first listen to the medium before sending.

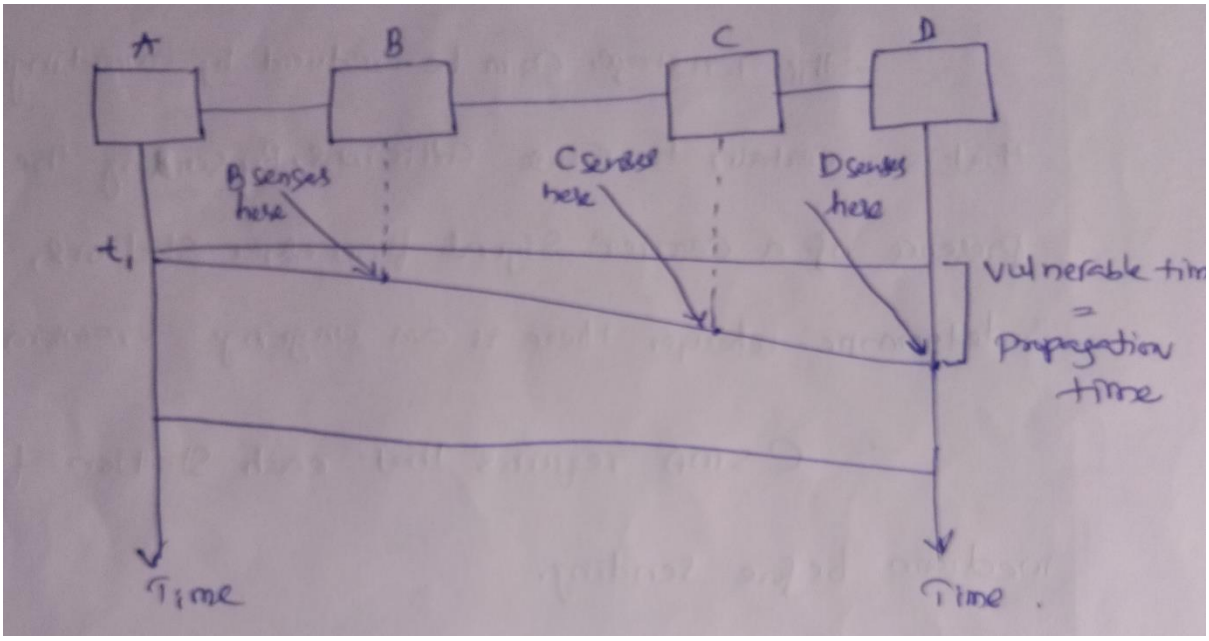
In other words, CSMA is based on the principle “sense before transmit” or “ listen before talk”

CSMA can reduce the possibility of collision but it cannot eliminate it.

The possibility of collision still exists because of propagation delay. A station may sense the medium and find it idle, only because the first bit sent by another station has not yet between received.

Vulnerable Time: The vulnerable time for CSMA is the propagation time (TP) this is the time needed for a signal to propagate from one end of the medium to the other.

When a station A sends a frame at time t_1 which reaches the right most station D at time $t_1 + T_p$



Persistence Methods: There are the three protocols

1. Non persistent CSMA
2. 1- persistent CSMA
3. P – persistent CSMA

1. Non – Persistent Method:

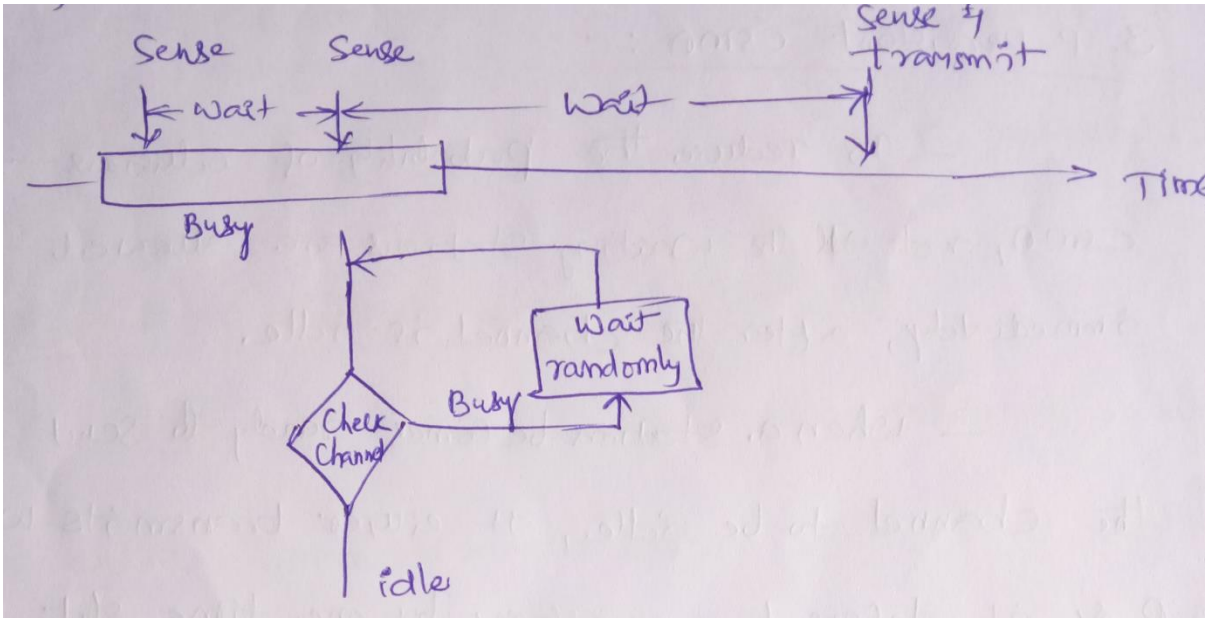
In non-persistent CSMA, when a station having a packet (frame) to transmit and finds that the channel is busy, it backs off a fixed interval of time

It then checks the channel again and if the channel is free tehn it transmits.

The back – off delay is determined by the transmission time of a frame, propagation time and other system parameters.

If the channel already in use, the stations does not continuously sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission

But it waits a random period of time and again checks for activity.

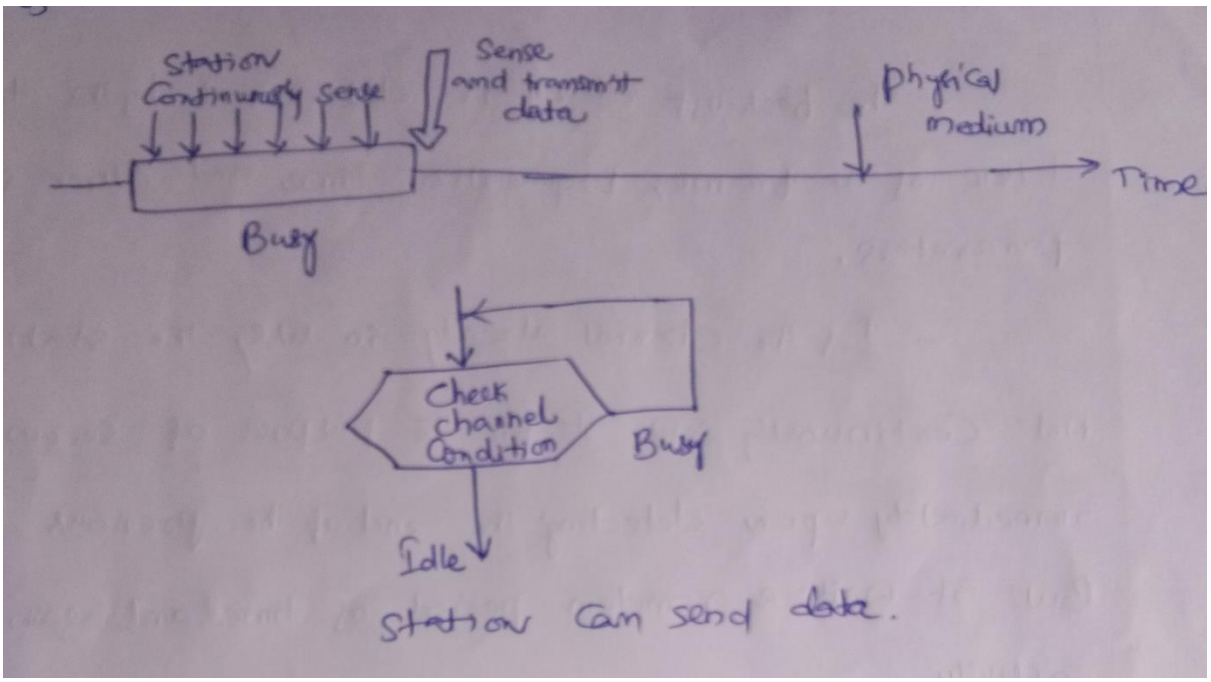


2. 1- Persistent:

Any station wishing to transmits, monitor the channel continuously until the channel is ideal and then transmits immediately with probability one, hence the name called 1 – persistent.

When two or more stations are waiting to transmit a collision is guaranteed. Since each station will transmit immediately at the end of busy period.

In this case each will wait a random amount of time and will then reattempt to transmit.



3. P – Persistent CSMA:

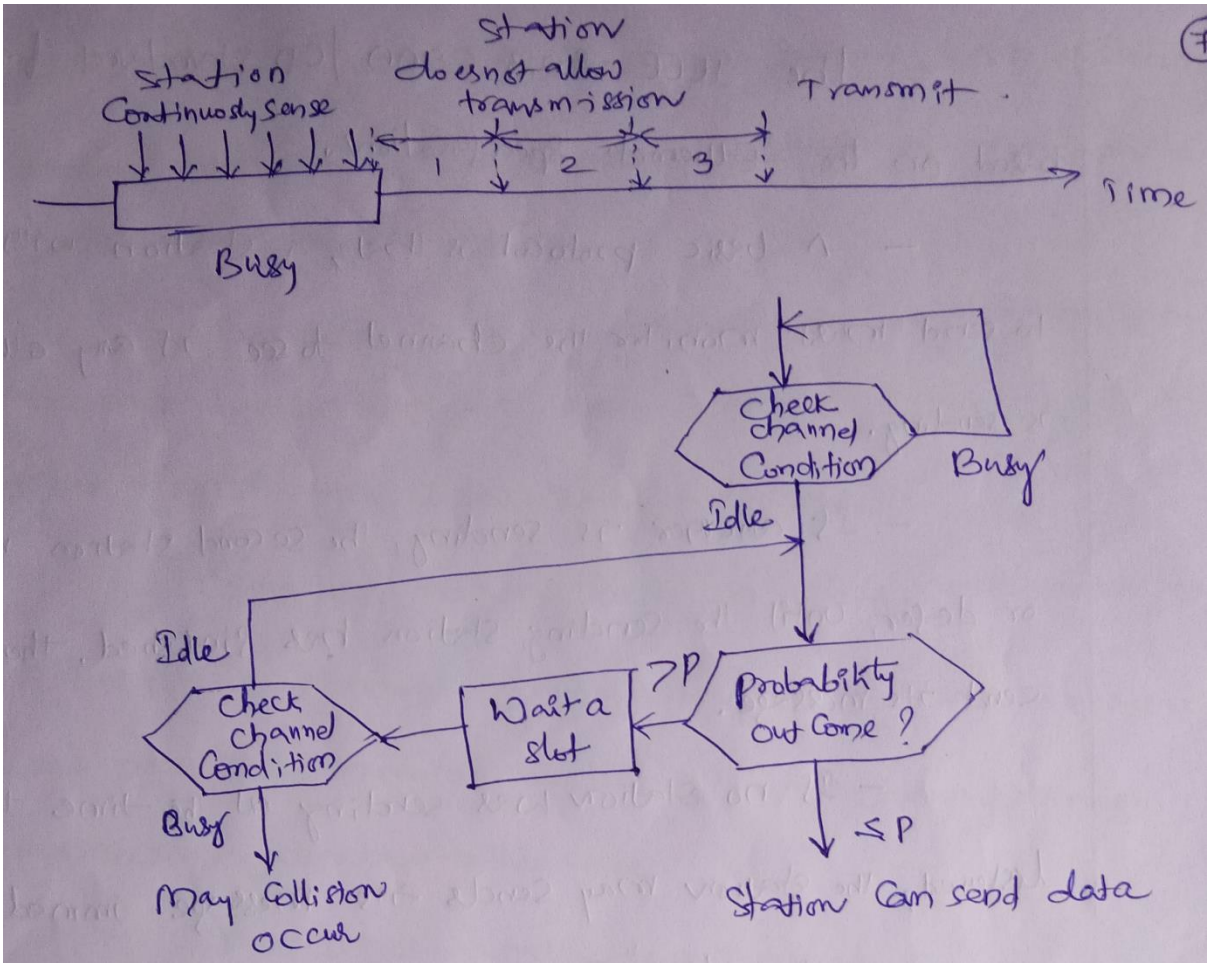
To reduce the probability of collisions in 1- persistent CSMA, not all the waiting stations are allowed to transmit immediately, after the channel is idle.

When a station becomes ready to send and it sense the channel to be idle, it either transmits with a probability p or it defers transmission by one time slot with a probability

$$q = 1 - p$$

If deferred slot is idle, the station either transmits with probability p or defers again with a probability q.

This process is repeated until either packets are transmitted or the channel becomes busy.



3.CSMA/CD (Collision Detection):

In both CSMA and ALOHA schemes, collisions involve entire frame transmission. If a station can determine whether a collision is taking place, then the amount of wasted bandwidth can be reduce by aborting the transmission when a collision is detected.

CSMA/CD is the most commonly used protocol for LANS.

It was developed jointly by digital equipment corporation (DEC), Intel and Xerox

This network is called as Ethernet. The IEEE 802.3 CSMA /CD standard for LAN based on the Ethernet specification.

A basic protocol is that, a station with a message to send must monitor the channel to see if any other station is sending.

If another is sending the second station must wait or defer, until the sending station has finished. Then it may send its messages.

If no station was sending at the time that it first listened, the station may sends its message immediately.

The term “carried sense” indicates “listening before transmitting” behaviour

If two or more stations have messages to send at the same time and they are separated by significant distance on the bus / channel, each may begin transmitting at roughly the same time without being a wave of the other station.

The signals from each station will super impose on the channel and is garbled beyond the decoding ability of the receiving station. This is called “collision”

A protocol is required for transmitting station to monitor the channel while sending each of bits message and to detect such “collisions”

When a collision has been detected, each of sending stations must cease transmitting wait for a random length of time, and then try again.

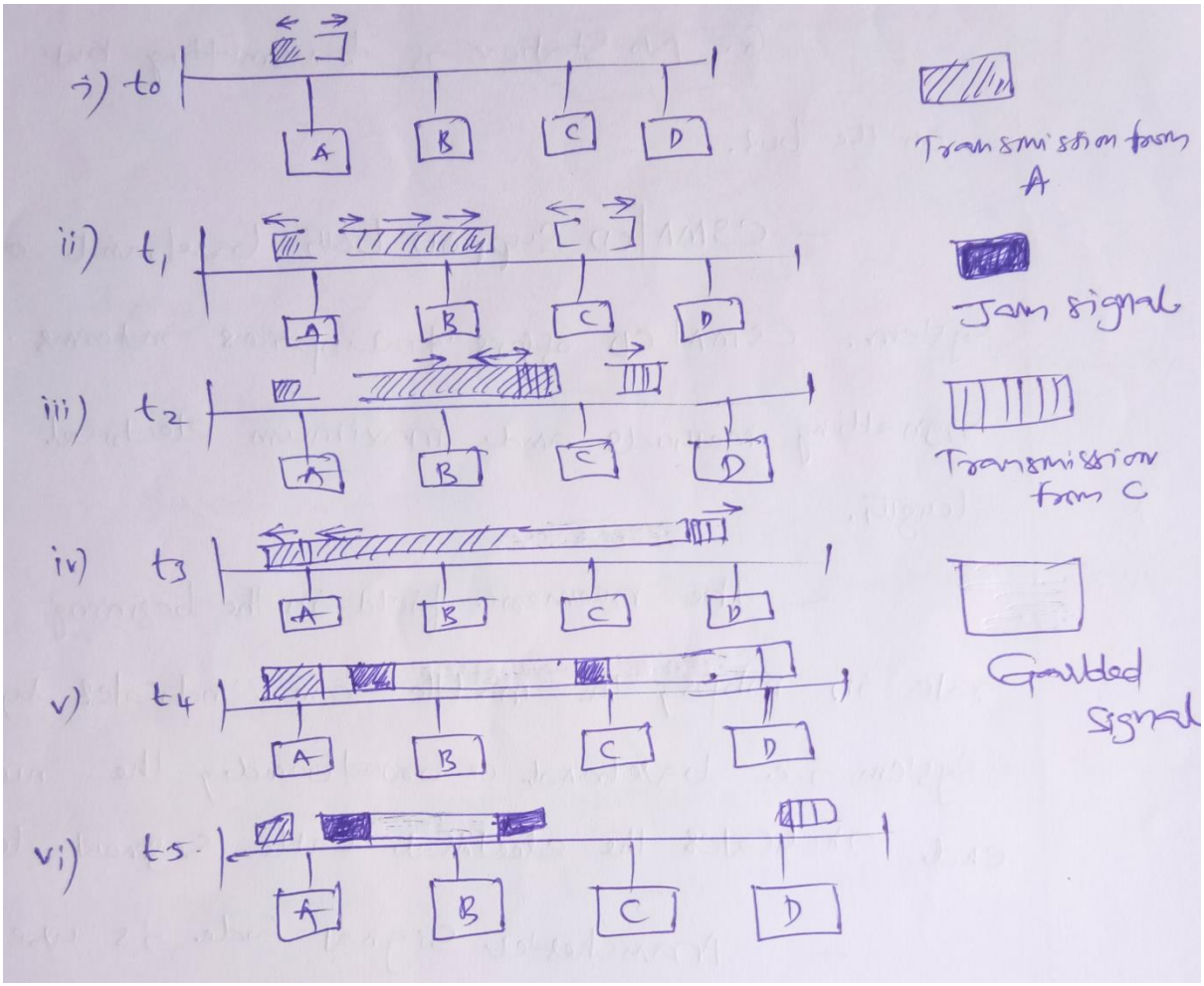
Because of quick termination of transmission time and bandwidth is saved. Therefore CSMA/CD is more efficient then ALOHA, slotted ALOHA and CSMA.

CSMA/ CD network best on a bus, multipoint topology with bursty asynchronous transmission. All stations are attached to one path and monitor the signal on the channel through transreceiver attached to the cable.

CSMA/CD has totally decentralized control and is based on contention access.

From an above figure, station A and station D are the extreme ends of a bus structure

1. Station A listens channel starts transmitting a packet addressing D.
2. Station B and C all ready for transmission. B senses a transmission on channel so defers. C is unaware of transmission and begins its own transmission.
3. Station A transmission reaches C. C detects collision and crass transmission sends jam signal.
4. Effect of collision propagates back to A, A stops its transmission.
5. A sends jam signal.
6. No station is transmitting but there still signals on the bus.



CSMA/CD supports both base band and broad band system CSMA/CD offers four options in terms of bit rate signaling methods and maximum electrical cable segment length.

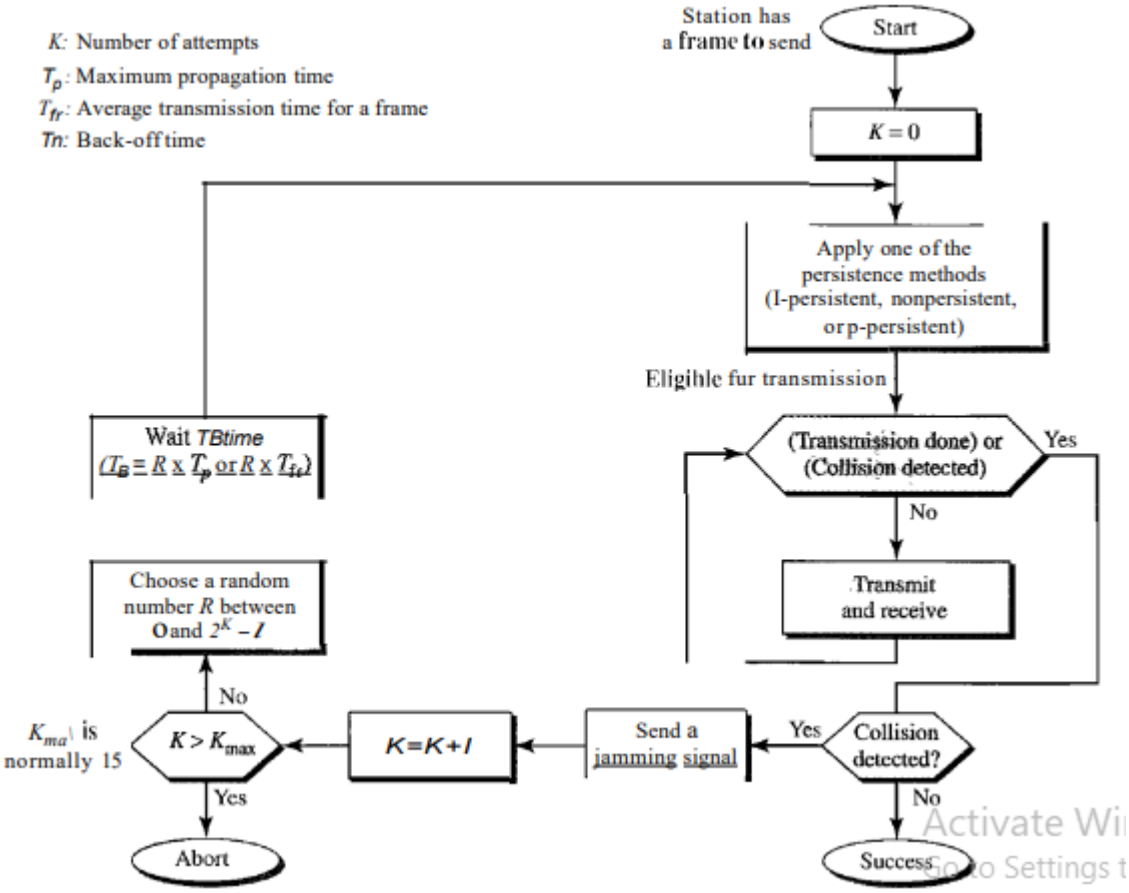
The numeric field in the beginning indicates the bit rate in mbps, the middle terms indicates type of signaling system i.e. back band or broad band, the numeric field in the end indicates the electrical cable segment length in × 100 meters

Manchester signal code is used at the baseband level of transmission.

CSMA/CD Throughput:

1. The throughput of CSMA/CD is greater than that of pure or slotted ALOHA
2. For 1- persistent method, the maximum throughput is around 50% when G = 1
3. For non-persistent method, the maximum throughput can go up to 90% when G is between 3 and 8.

CSMA/CD Flow Graph:



4.CSMA/CA: (collision Avoidance): In wireless n/w's cannot use CSMA/CD in the MAC sub layer, this requires the ability to receive and transmit at the same time.

In a wireless n/w's, much of the sent energy is lost transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy.

This is not useful for effective collision detection; we need to avoid collision on wireless networks because they cannot be detected. Since, CSMA/CA was invented for the networks.

Collision avoidance using in three models

1. Inter frame space
2. Contention window
3. Acknowledgement

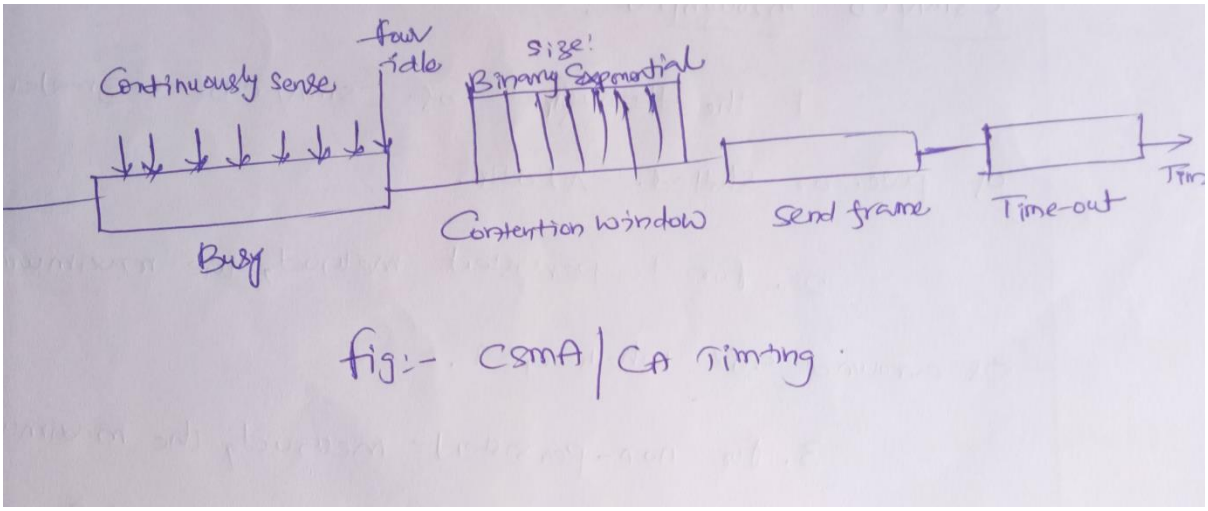


fig:- CSMA/CA Timing

Inter Frames Space:

1. Collisions are avoided by deterring transmission even if the channel is found idle.
2. When an idle channel is found, the station does not send immediately. It waits for a period of time called the inter frame space.(IFS)
3. In CSMA/CA, the IFS can also be used to define the priority of a station of a frame. A station that is assigned shorter it's has a higher priority.

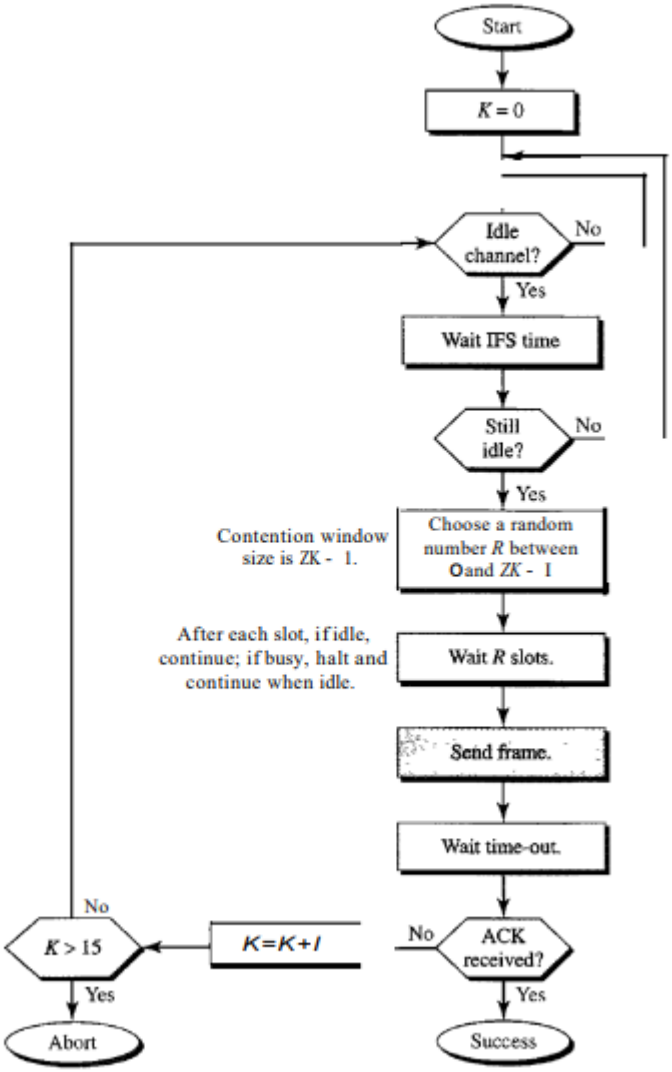
Contention Window:

1. Contention windows are an amount of time divided into slots. A station that is ready to send chooses a random no. of slots as its wait time.
2. Station set one slot for the first time and then double each time station cannot detect an idle channel after the IFS time.
3. In this method, the station needs to sense the channel after each time slot
4. If the station finds channel busy, it does not restart the process, it just stops the timer and restarts it when the channel is sensed as idle.
5. This method gives the priority to the station with the longest waiting time.

Acknowledgement:

The data may be corrupted during the transmission. The positive acknowledgement and the time out can help guarantee that the receiver has received the frame.

Flow Chart for CSMA/CA:



Collision Free Protocols:

Almost collisions can be avoided in **CSMA/CD**, they can still occur during the contention period. The collision during contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network come into use. Here we shall discuss some protocols that resolve the collision during the contention period.

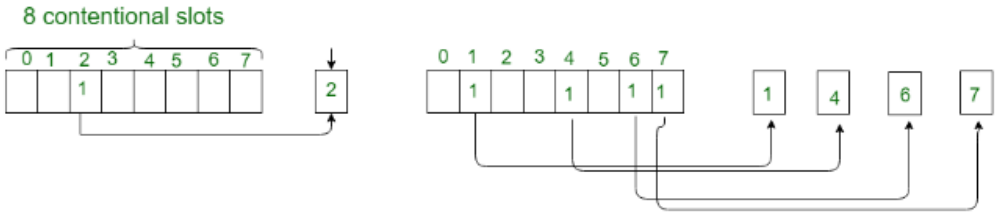
- Bit-map Protocol
- Binary Countdown

Bit-map Protocol:

Bit map protocol is collision free Protocol in In bitmap protocol method, each contention period consists of exactly N slots. if any station has to send frame, then it transmits a 1 bit in the respective slot. For example if station 2 has a frame to send, it transmits a 1 bit during the second slot.

In general Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next.

Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called *Reservation Protocols*.



For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of *d* time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

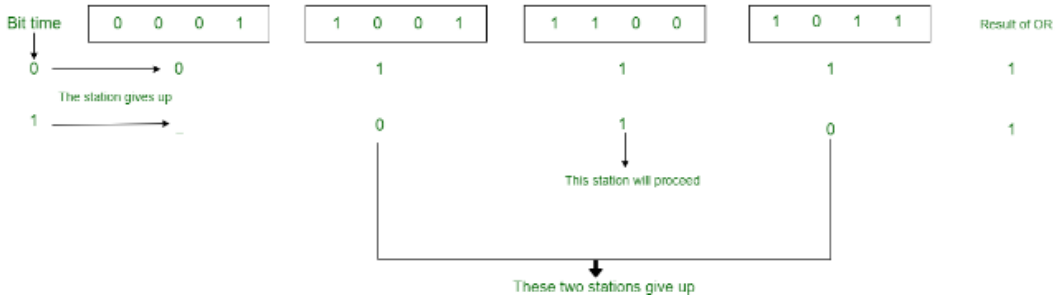
Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

Binary Countdown:

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are ORed together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are ORed together. Station 0001 see the 1MSB in another station addresses and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next bit is 1 at station 1100, swiss station 1011 and 1001 give up. Then station 110 starts transmitting a frame, after which another bidding cycle starts.



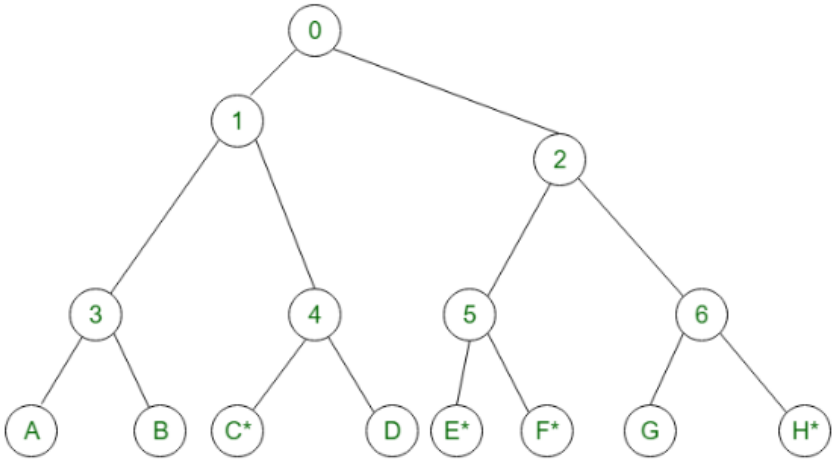
Limited Contention Protocols:

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.

- How about combining their advantages
    1. Behave like the ALOHA scheme under light load
    2. Behave like the bitmap scheme under heavy load.

Adaptive Tree Walk Protocol:

- partition the group of station and limit the contention for each slot.
- Under light load, everyone can try for each slot like aloha
- Under heavy load, only a group can try for each slot
- **How do we do it:**
    - treat every stations as the leaf of a binary tree
    - first slot (after successful transmission), all stations can try to get the slot(under the root node).
    - if no conflict, fine
    - in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



- **Slot-0:** C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
- **Slot-1:** C* (all nodes under node 1can try}, C sends
- **Slot-2:** E*, F*, H*(all nodes under node 2 can try}, conflict
- **Slot-3:** E*, F* (all nodes under node 5 can try to send), conflict
- **Slot-4:** E* (all nodes under E can try), E sends
- **Slot-5:** F* (all nodes under F can try), F sends
- **Slot-6:** H* (all nodes under node 6 can try to send), H sends.

Wireless LAN's (WLAN's):

Wireless LANs are increasingly popular, and homes, offices, cafes, libraries, airports, zoos, and other public places are being outfitted with them to connect computers, PDAs, and smart phones to the Internet. Wireless LANs can also be used to let two or more nearby computers communicate without using the Internet. The main wireless LAN standard is 802.11

802.11 Architecture and protocol stack

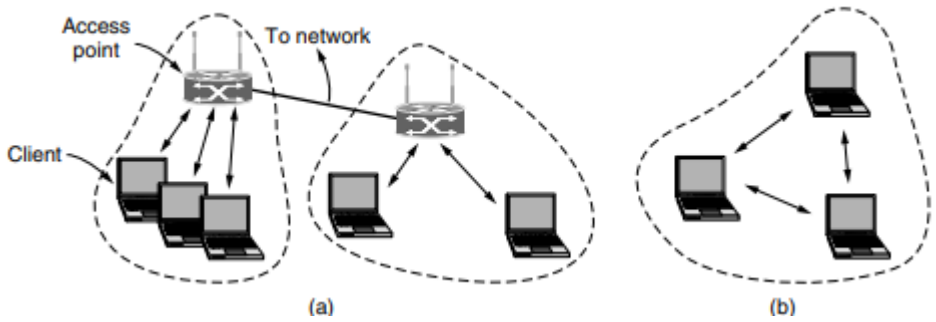


Fig. 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode

WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.

- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion.

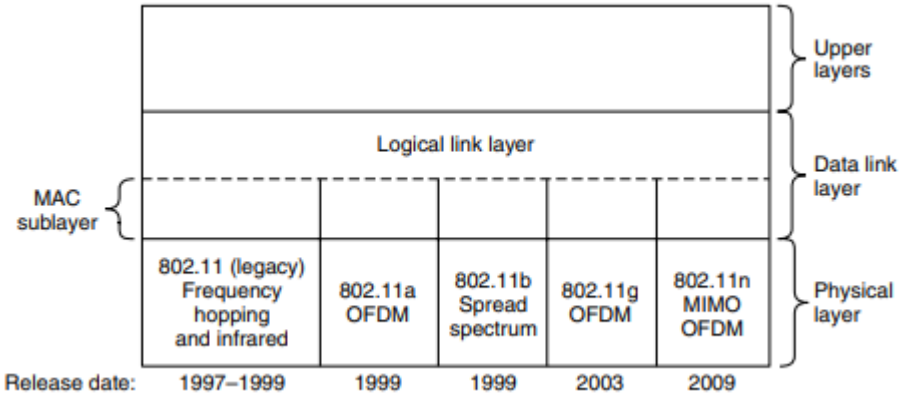


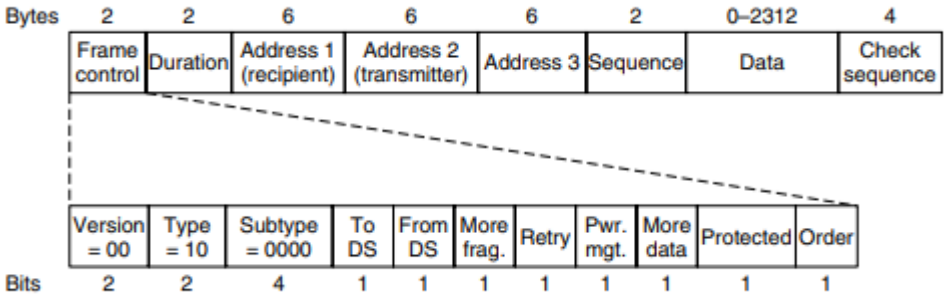
Fig. Protocol stack of 802.11

Components of WLANs

The components of WLAN architecture as laid down in IEEE 802.11 are −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −
  - Wireless Access Point (WAP or AP)
  - Client
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −
  - Infrastructure BSS
  - Independent BSS
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.

802.11 Frame structure



Advantages of WLANs

- They provide clutter-free homes, offices and other networked places.
- The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.
- The system is portable within the network coverage. Access to the network is not bounded by the length of the cables.
- Installation and setup are much easier than wired counterparts.
- The equipment and setup costs are reduced.

Disadvantages of WLANs

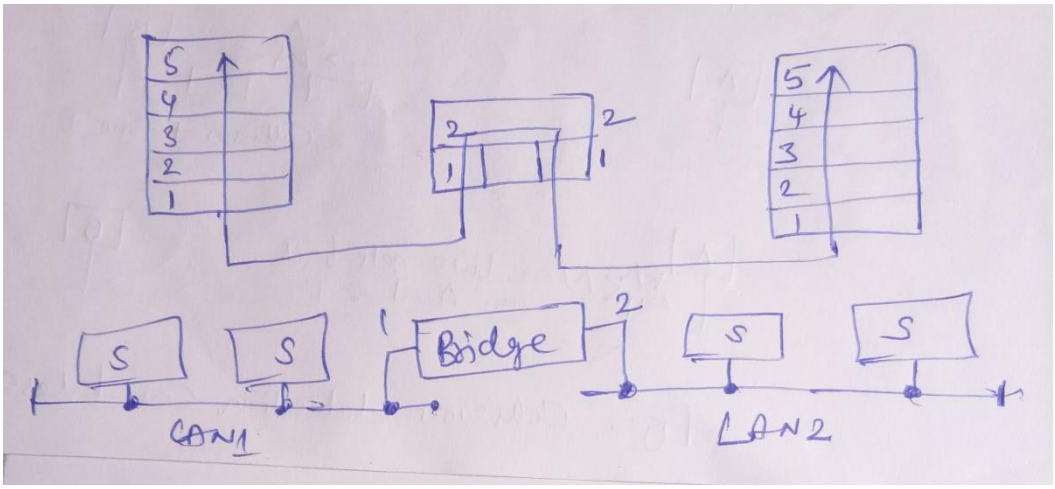
- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

Data link layer switching

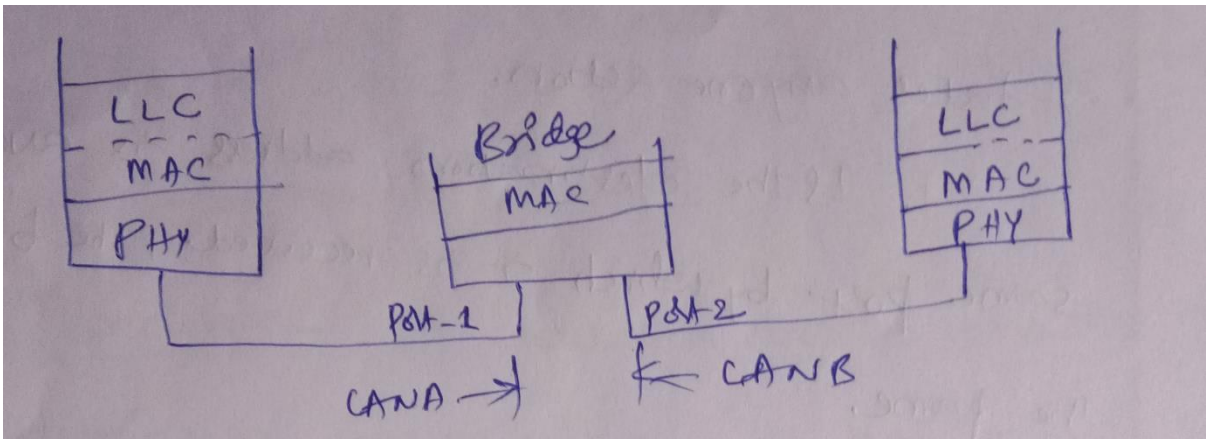
Bridges: A bridge operates in both the physical and data link layer. A bridge extends the maximum distance of network by connecting separate network segment.

A bridge simply passes on all the signals it receives. It reads the address of the entire signal it receivers.

Bridges performs data link functions such as error detection, frame formatting and frame routing.



Bridge Architecture:



The layered architecture of two Port bridge as shown in fig.

At each port of bridge, it has physical layer and MAC sub layer

The physical layer and MAC layer protocols at each port of bridge match with the protocols of the respective LAN.

The MAC sub layers have relay and routing function between them. When MAC frame is received by it examine the destination address, it reformats the frame as required by the other LAN.

Function of bridge: The following functions of bridges are

1. Frames filtering and forwarding.
2. Learning address
3. Routing

Frames filtering and forwarding: when the bridge receive a frame at any of its ports it takes any one action.

1. if the destination address is available on the same port by which it is received, the bridge discards the frame.
2. If the destination address is on different physical ports, it forwards the frame onto that port
3. If the bridge does not find the destination address it forwards the frames over all its physical ports except from which it is received.

Learning the Address: when a frame received at a bridge and if source address is not available in the database, it updates the database.

This entry consists of the address, port on which address was received and a timer value when the address was arrived.

Routing: When multiple LANs and multiple interconnecting bridges are configured, the bridges need to have routing capability. The bridge must know the alternative in terms of number of hops.

Alternative and duplicate routes must be distinguished.

In the networks duplicates routes interfere in the self-address learning mechanism. The process of deciding which frames to forward and where is called bridge routing.

Learning bridges:

A learning bridge has all the capabilities of a basic bridge, it has reduces the amount of broad cast traffic on the LANS.

A learning bridge listen to all frames in the two LAN segments just as basic bridge doesn't and where each physical address located.

The learning bridges make a list of the physical address and which port they are connected so. Because it stores each frames as it receives it, it then forwards frames selectively based on the LAN to which that physical address located.

Whenever the learning bridge encounters a frame contacting a physical address doesn't know if forwards that frame out all other ports to the other LANs.

Spanning Tree Bridge:

In this bridge mechanism, bridges automatically develop a routing table and update table in response to changing topology.

It consists of three techniques:

1. Frames forwarding
2. Address learning
3. Loop resolution.

Frames forwarding:

When a frame arrives on a bridge port, a bridge must decide whether to discard or forward it to which LAN.

This decision is made by looking up the destination address in a big database in the bridge. This data base contains station addresses to which frames should be forwarded through that port.

This information pertains to both source & destination address. If the destination address is not in the forwarding database, it is send tout on all ports of the bridge except the one on which frame was received is called flooding.

When the destination address exists in forwarding database, the port identifier of stored address is compared with identifier of the port on which the address was received.

Address learning: it is also called back ward learning, it takes care about destination address.

When a frame is received at a bridge, its source address is compared with the address in forward database.

If the source address is not found there, the bridge makes a new entry to the database.

Loop resolution (or) spanning tree:

The process of frame forwarding and address learning process to operate properly there must be only one path of bridges and LAN'S between any two segments in the entire bridge LAN. Such topology is known as spanning tree and the methodology for setting up is called spanning tree algorithm.

1. Roof Bridge: each bridge has a unique identifier the bridge with the lowest identifier is called the root bridge.

2. Root Path Cost: each port of a bridge has an associated cost parameter which is the cost of transmitting a frame through the particular port.

When a frame transverse a path through several bridges, the path cost is the sum of all the inserting port cost parameters

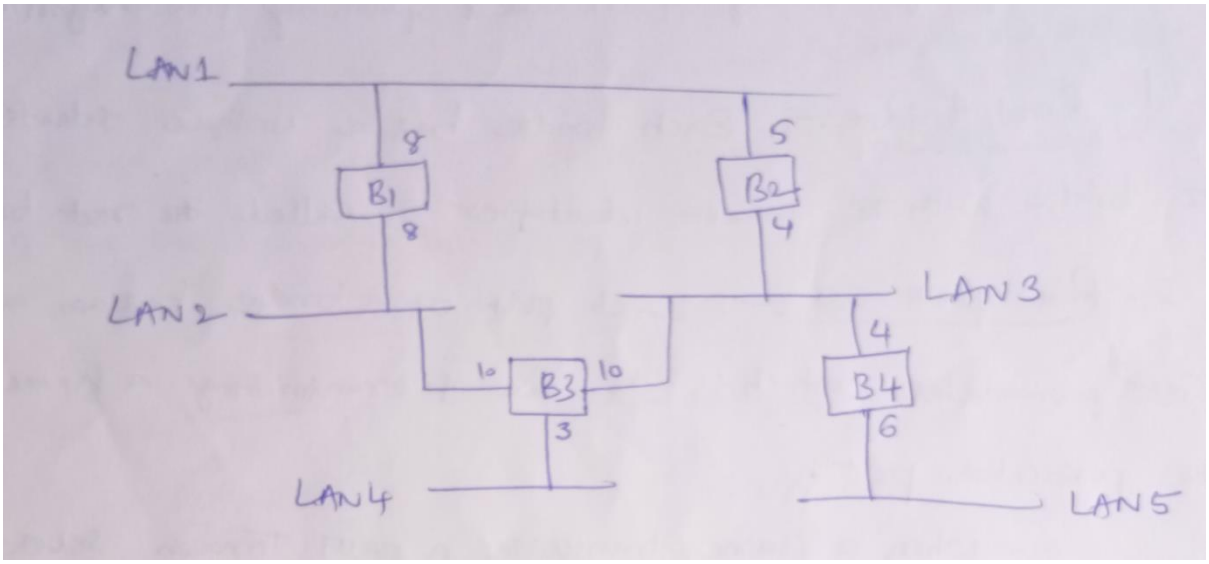
Root path cost is the minimum path cost from a bridge to the root bridge.

3. Root port: each bridge determines its port through which if a frame transmitted, it will reach the root bridge incurring the roof path cost. This port of the bridge is called root port.

4. Designated Bridge And Designated Port:

If a LAN has several brides connecting it to the root bridge, one of the bridge is called the designated bridge and all the frames from the LAN are transmitted through the designated bridge. The corresponding port of the bridge is called designated port.

Construction of Spanning Tree:



For spanning tree algorithm to work properly, each bridge must have unique identifier. Each port with in a bridge must have distinct identity.

First a root bridge is selected, then each bridge selects a port through which the least cost path to the root bridge is found. Then a specific designated bridge is selected for each LAN. Lastly each bridge puts its root port and all bridges ports to LAN for which it is designated into a forwarding state. The other bridge ports are said to be in a blocked state.

When the n/w is in operation, the spanning tree algorithm exchanges status information between bridges via messages called bridge protocol data units.

Consider the configuration shown in above figure.

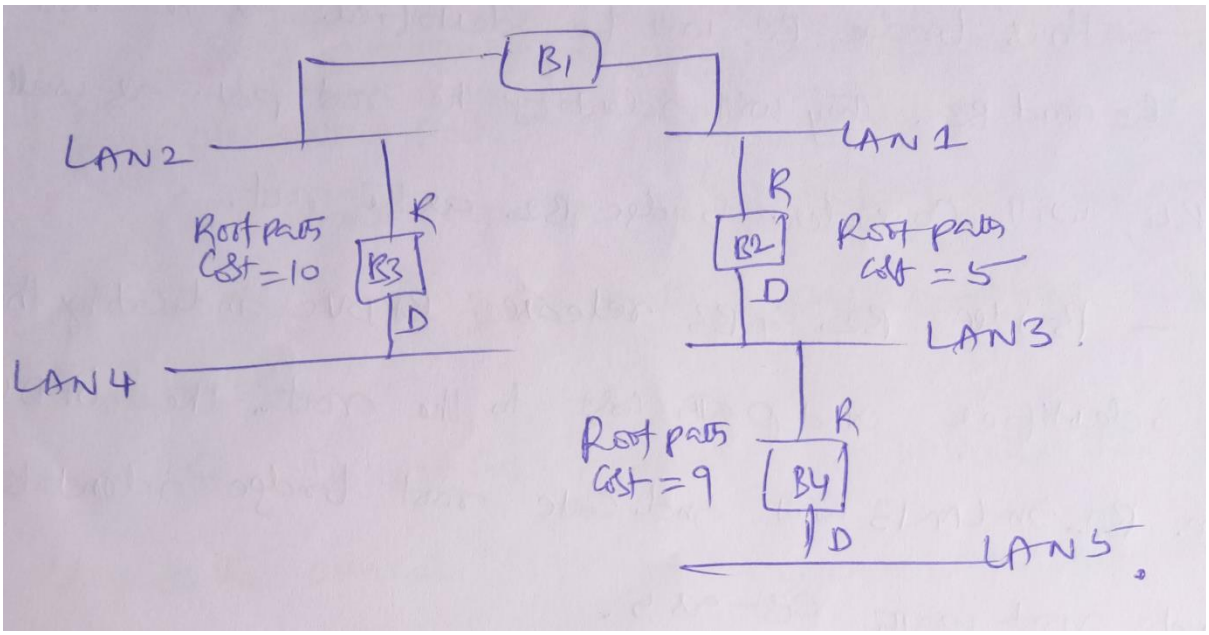
All bridges consider themselves to be the root bridge by broadcasting a BPDV on each of its LANS. Only one clamant will have the lowest bridge identifier and will maintain this believe. The other will accept this fact by comparing the bridge identifier in the BPDUs they receiver. Thus bridge B1 will be identified as the root by brides B2 and B3. They will identify the root port as well. Bridge B4, will consider bridge B2 as the root.

Bridge B2 and B3 release BPDUs indicating the root bridge identifier and path cost to the root. The BPDU released by bridge B2 in LAN 3 will indicate root bridge identifier as B1 and root path cost as 5. Similarly, the BPDU released by bridge B3 in LAN3 and LAN4 will indicate the root bridge identifier as R1 and root path cost as 10.

When bridge B4 receivers these BPDV's it will realize that the root identifier is B1 and the root is accessible through bridge B2 at a lower path cost of 5. Therefore, bridge B2 is the designated bridge for LAN3 and port of bridge B2 connected to LAN3 is chosen as the designated port for transmission of frames to the root.

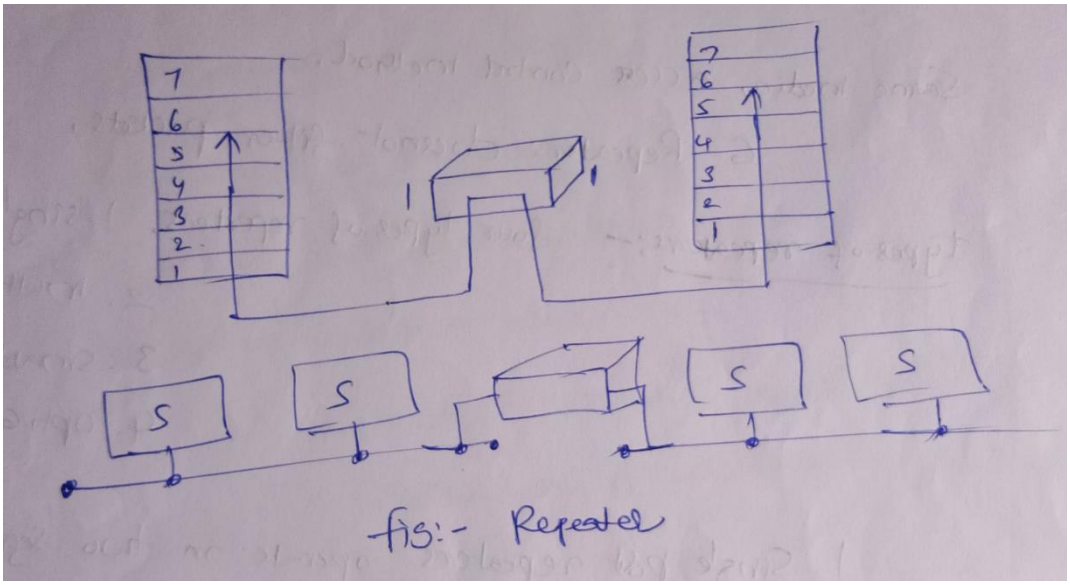
The port of bridge B3 connected to LAN3 is put in the blocked state. Bridge B4 will further propagation this information to the other bridges connected to LAN5. It will indicate the root

identifier as B1 and the root path cost is 9. This process continue and finally we have spanning tree with no loops.



Repeaters: It is a device, which operates only in the physical layer. The purpose of the repeater is to extend the distance of LAN.

A repeater receives a signal and before it becomes too weak or corrupted, generates the original bit pattern. The repeaters then send the refreshed signal.



A repeater does not actually connect two LANs it connects two segments of the same LAN. A repeater is not a device that can connect two LANs of different protocols.

A repeater doesn't amplify signal; it generates signal. When it receives a weak or corrupted signal, it creates a copy, bit for bit, at the original strength.

Characteristics of Repeater:

1. Repeaters are used to regenerate an existing base band signal.
2. Repeater will pass a broad cast.
3. Repeater issued primarily in a co – axial bus topology
4. Repeater operates at physical layer of OSI model.
5. Segments connected by a repeated must use the same media access control method.
6. Repeater doesn't filter packets.

Types of Repeaters: Four types of repeaters

1. Single port repeater
2. Multiport repeater
3. Smart repeaters
4. Optical repeaters.

1. Single port repeater

1. Single port repeater operate in two segment's; one type has a signal taken it to boost and pass to the next segment
2. In multiport repeater has one input port and multiple output port
3. Smart repeater is a hybrid device and very similar to a bridge in functionality. Packet filter is done by smart repeaters.
4. In optical repeaters, in which the repeater repeats the optical signals. Repeaters are implemented in all cables.

Switches: switch operates at the data link layer (DLL) of the OSI model. It can interpret address information.

Switch reassembles bridges and can be considered as multiport bridges. With these the limited band width utilization and prove more cost – effective than bridge.

Switches divided a network into several isolated channels. Packets sending from one channel will not go to another is not specify

Each channel has its own capacity and need not be shared with other channels.

Advantages of Switches:

1. Switches divide a network into several isolated channels or collision domains.
2. Reduce the possibility of collision.
    i. Collision only occurs when two devices try to get access to one channel.
    ii. It can be solved by buffering one of them for later access.

3. Each channel has its own network capacity and it is suitable for real time application. E.g. video conference

Layer 2 switch:

It performs at the physical and data link layer.

It is a bridge with many ports and a design that allows better performance. It operates using physical network addresses, identify individual devices.

Layer 3 switches:

The layer 3 switch use network or IP address that identifies location on the network. They read network address more closely then layer 2 switches.

They identify network location as well as the physical device. A location can be a LAN work station, a location in computer memory or even a different packet of data travelling through a network.

Layer 4 Switches:

This layer 4 switch of the OSI model communicate and co – ordinate between the systems. Layer 4 switch are capable of identifying which application protocol (HTTP, SNMP, FTP) are included with each packet and they use this information to hand off the packet to the appropriate higher layer software.

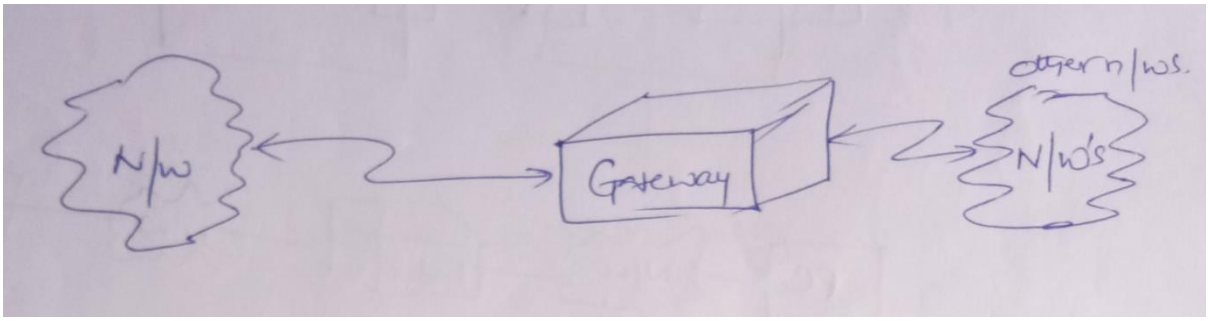
Layer 4 switches make packet forwarding decisions based on not only on the MAC address and IP address, but also on the application to which a packet belongs.

Gate Ways:

Gate way connects two independent networks a gate way is a protocol converter.

A gateway can accept a packet formatted for one protocol (Ex: TCP/IP) and converts it to a packet formatted for another protocol before forwarding it.

The gate way must adjust the data rate, size and data format. Gateway is generally software installed within a router.



Hubs: all the networks (except those using co – axial cable) require a central location to bridge media segment together, these central locations are called hubs.

Hubs are special repeaters that overcome the electromechanical limitations of a media signal path.

Function of Hub:

1. Facilitate adding, deleting or moving work stations.

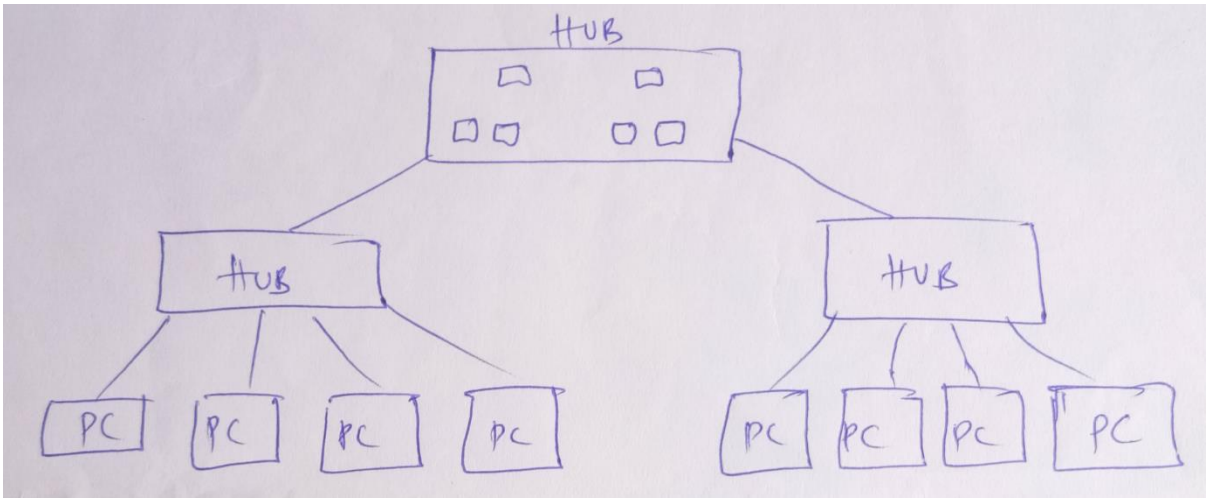
2. Extend the length of the network
3. Provided flexibility by supporting multiple inter face.
4. If offers fault tolerance feather.
5. Provide centralize management services.

Types of Hubs: There are three types of hubs

1. Passive hub
2. Active hub
3. Intelligent hub.

Passive hub: A passive hub is just a connector. It simply combines the signals of network segments. There is no regeneration of signal. It is a part of transmission media

Active Hub: An active hub is actually a multipoint repeater. An active hub that regenerates or amplifies the signals. By using active hubs the distance between the devices can be increased. It is very expensive than passive hub.



The drawback of the active hub is that they amplify noise along with signal.

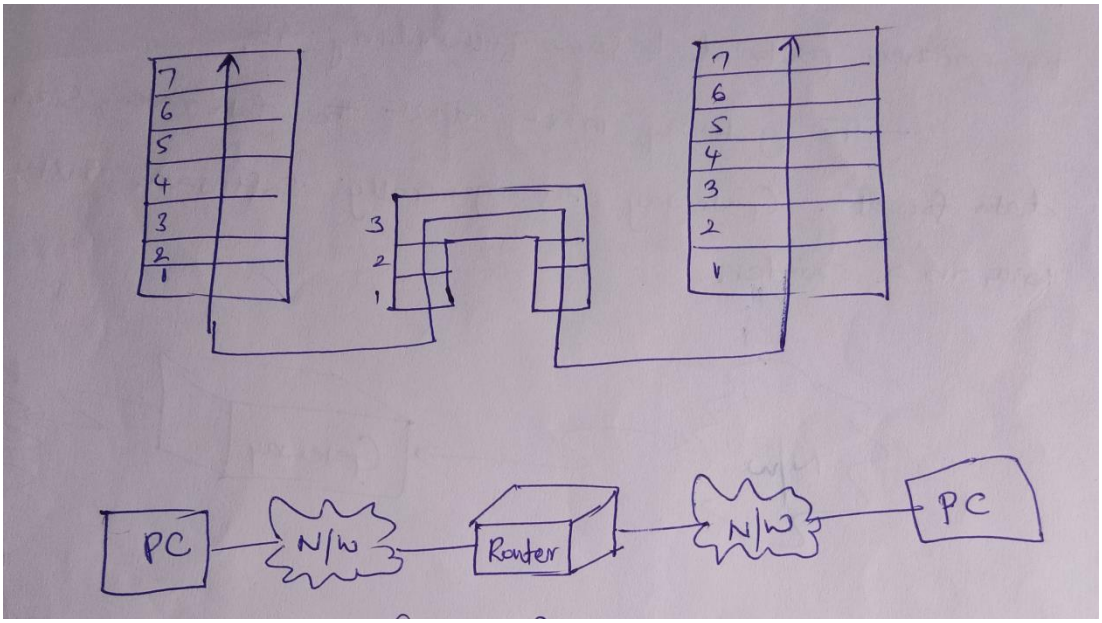
Intelligent hub regenerates the signal and performs some network management and intelligent path selection. It indicates that alternate path, will be the quickest and send the signal that way. Permanently connecting to the hub because each segment will be used only when a signal is sent to a device using that segment.

Routers:

A router is a three layer device that routes packet based on their logical address. Router connects two (or) more networks. It consists of combination of the hardware and software.

A router normally connects LANs & WANs in the internet and has a routing table that is used for making decision about the route.

Router connects dissimilar networks together and have access to information from physical, data link and network layer.



The key factor of a router is to determine a shortest path to destination. A router forwards packet by examining protocol address at network layer, look up the address in the routing table, then forward the packet to the next hop.