Chapter 3
Data Link Layer

Dr. Nilesh Madhukar Patil

Associate Professor, DJSCE

Unit	Description	Duration	CO	Marks
III	**Data Link Layer:** Design Issues: Framing Error Control: Error Detection and Correction (Hamming Code, CRC, Checksum), Flow Control: Stop and Wait, Sliding Window (Go Back N, Selective Repeat), Elementary Data Link protocols, HDLC, PPP. **Medium Access Control Sublayer:** Channel Allocation problem, Multiple Access Protocol (Aloha, Carrier Sense Multiple Access (CSMA/CA, CSMA/CD) **Wired LANS**: Ethernet, Ethernet Standards, Virtual LANs.	10	CO3	25

Data Link Layer Design Issues/ Functions of Data Link Layer

1. **Providing Services to the Network Layer**
2. **Error Control**
3. **Flow Control**
4. **Framing**

Providing Services to the Network Layer

(a) Unacknowledged Connectionless Service:

No acknowledgements are used. It is a connectionless service.
Example: VoIP.

(b) **Acknowledged Connectionless Service**:

Acknowledgments are used. It is a connectionless service.
Example: Wi-Fi.

(c) **Acknowledged Connection-oriented Service**:

Acknowledgments are used. It is a connection-oriented service.
Example: Telephone.

Error Control

To achieve error control, following techniques are used:

(a) Acknowledgments:

When the receiver correctly receives the data, it sends an acknowledgement to the sender. (Used in Stop-and-wait protocol)

(b) Timer:

The sender maintains a timer which is set to a time which is enough for the data to reach the receiver and for the acknowledgement from the receiver to reach back to the sender.

(c) Sequence Numbers:

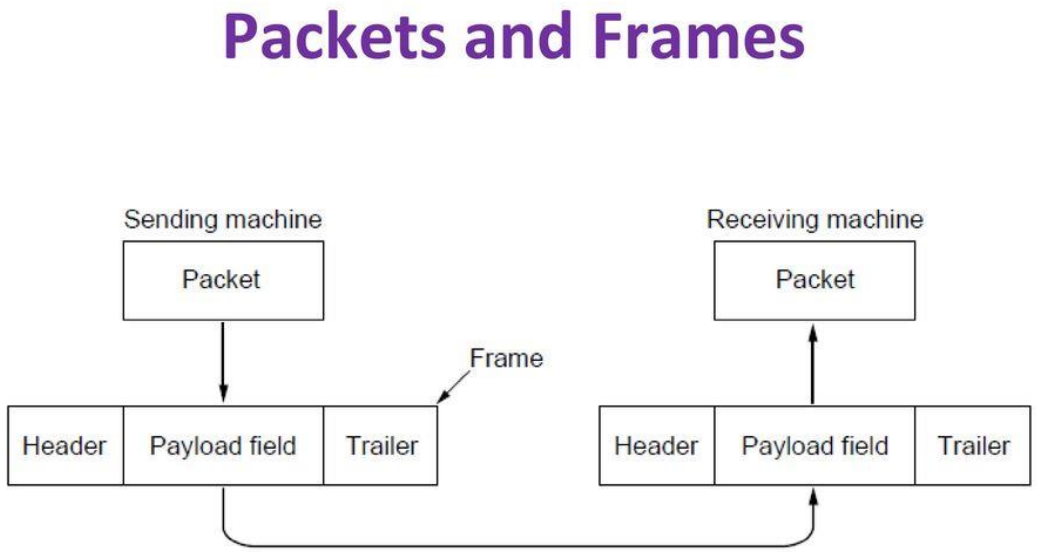
Sequence numbers are used by the receiver to decide if they are receiving the new frames or the duplicate frames.

Flow Control

- A receiving node can receive the frames at a faster rate than it can process the frame.
- Without flow control, the receiver's buffer can overflow, and frames can get lost.
- DLL regulates the flow of data so that receivers are not swamped by the fast senders.

Framing

- The data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
- Each frame contains a frame header, a payload field for holding the packet, and a frame trailer as shown in Fig.
- Frame management forms the heart of what the data link layer does.

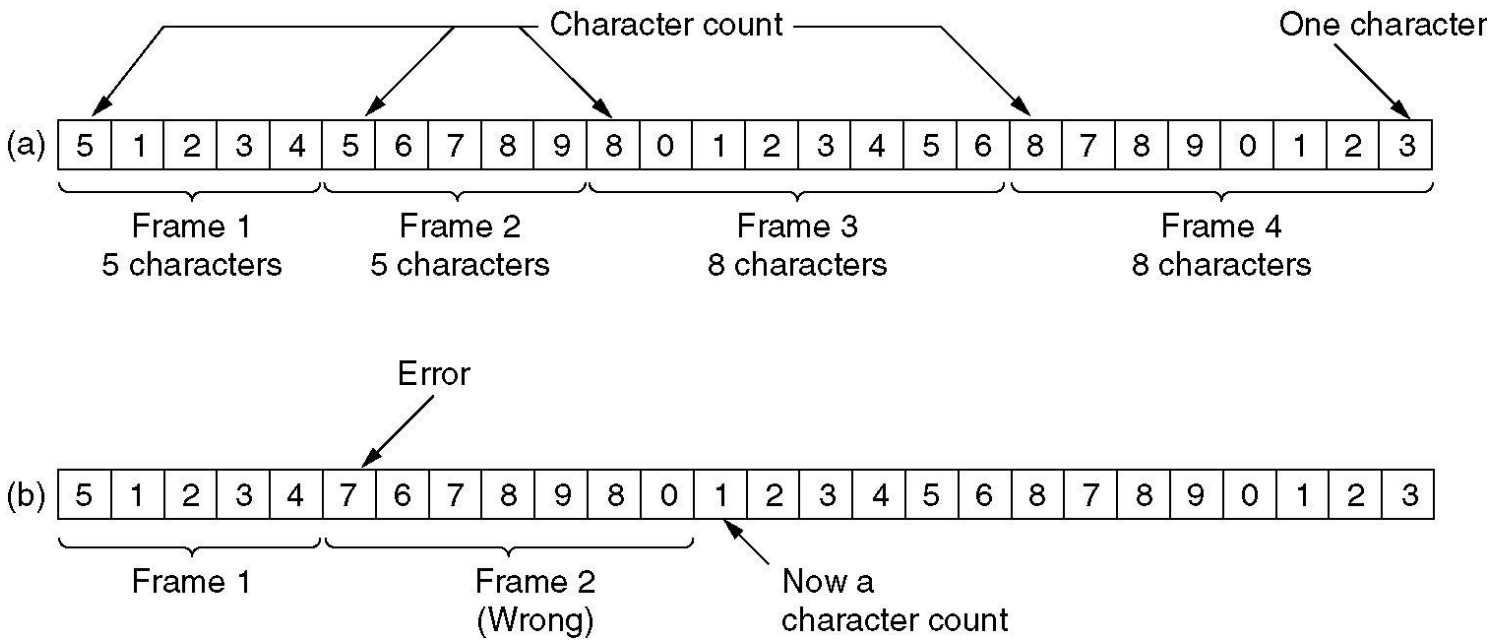


Relationship between packets and frames.

Methods of Framing

- Character count
- Byte/char stuffing
- Bit stuffing
- Violating the Physical encoding scheme.

Framing – Character count

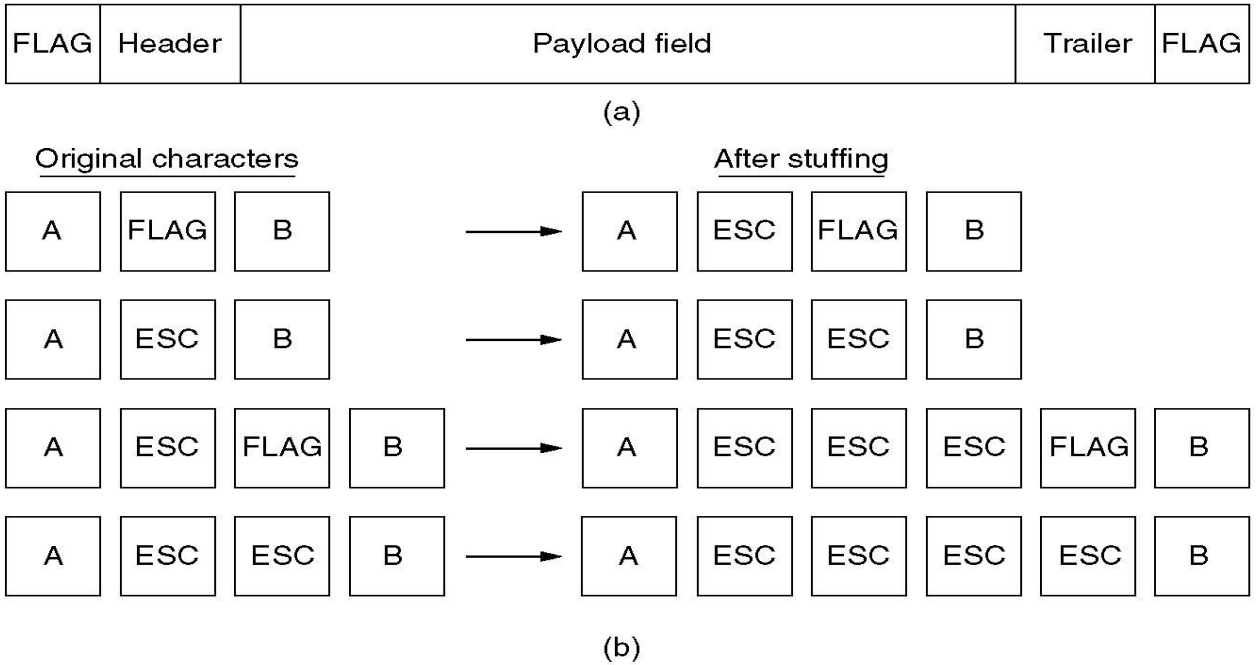


A character stream. (a) Without errors. (b) With one error.

- The first field in the header specifies the number of characters in the frame.
- When the data link layer at the destination sees the character count, it knows how many characters follow and hence where the end of frame is.

Problem: If the count is garbled by the transmission error then the receiver will get out of the synchronization

Framing – Byte/Char stuffing



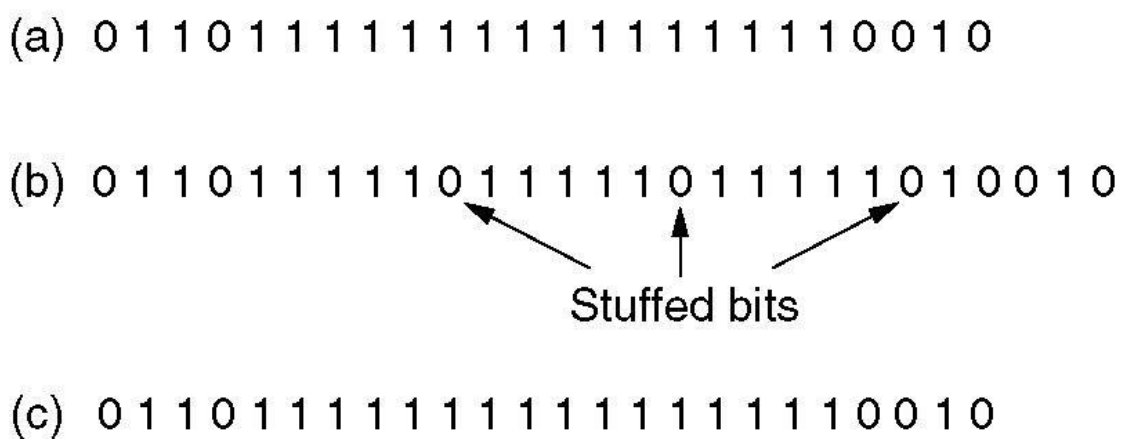
(a) A frame delimited by flag bytes.

(b) Four examples of byte sequences before and after stuffing.

- Each frame starts with a special start and end bytes (flag bytes).
- If flag byte is already present in the data, insert special escape byte (ESC) before each FLAG in data. Remove it at receiver end. This is called **byte stuffing** or **character stuffing**.
- Probably it won't happen for text data, but could easily happen with binary data.
- If ESC is itself in the data, insert another ESC before it.
- De-stuffing recovers original characters.

Problem: Closely tied to the use of 8-bit characters. Not all character code use 8-bits. For e.g. UNICODED uses 16-bit.

Framing (3) Bit stuffing



Bit stuffing

(a) The original data.

(b) The data as they appear on the line.

(c) The data as they are stored in receiver's memory after de-stuffing.

- Each frame begins and ends with a special bit pattern 01111110
- When ever the sender's data link layer identifies five consecutive 1's it stuffs bit 0 into the outgoing stream.
- Whenever receiver sees five consecutive 1's followed by 0 it de-stuffs the 0 bit.

Flow Control Techniques

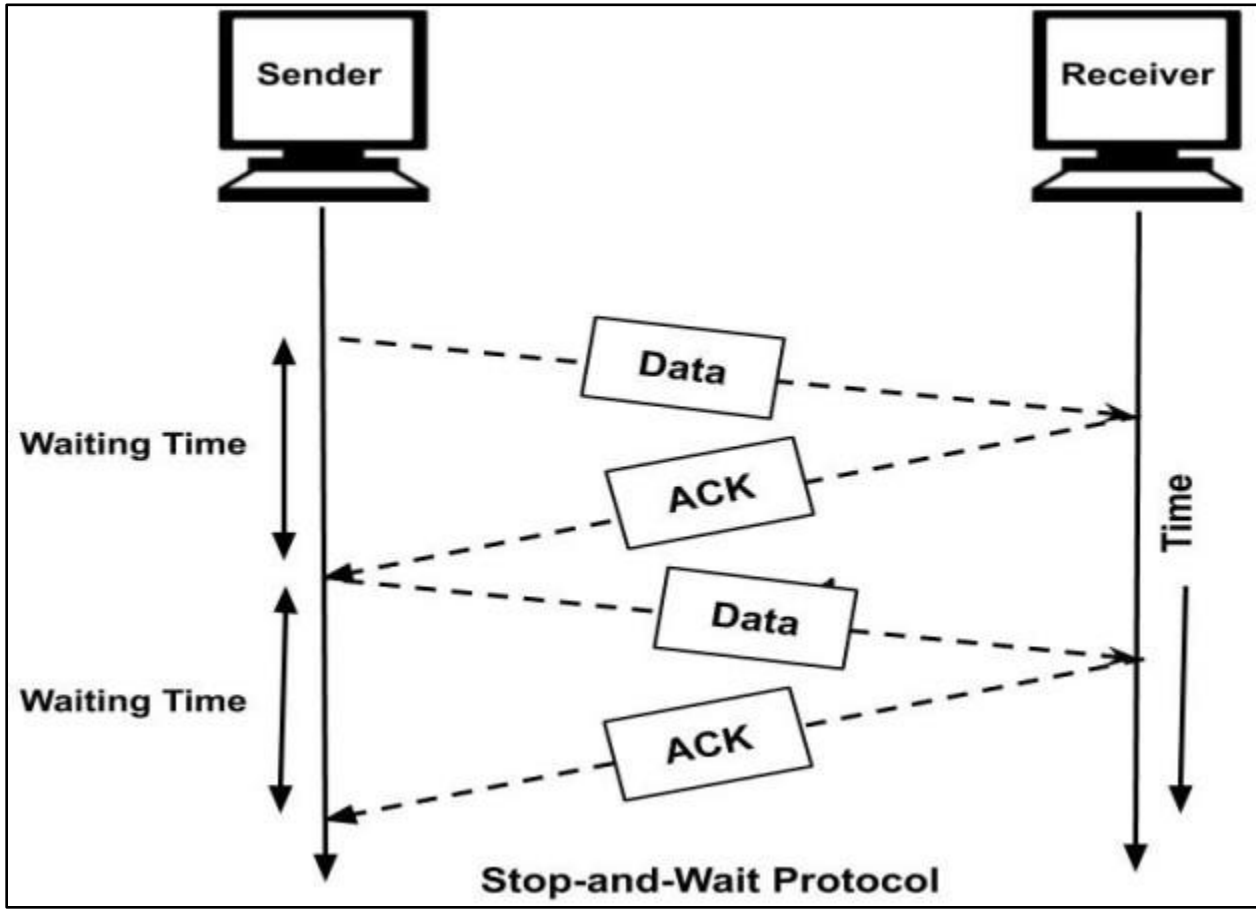
1. Stop-and-wait Flow Control
2. Sliding Window Flow Control

Stop-and-Wait Flow Control

- The sender waits for an acknowledgement from the receiver after every frame, which is transmitted by the sender.
- It indicates the willingness of the receiver to accept another frame by sending back an acknowledgement to the sender.
- The sender must wait until it receives the acknowledgement before sending next frame.
- The receiver thus can stop the flow of data simply by withholding acknowledgement.

Advantage: Simplicity. Each frame is checked and acknowledged before the next frame is sent.

Disadvantage: Inefficiency. Stop-and-wait is slow. Each frame must travel all the way to the receiver and the acknowledgement must travel all the way back to the sender before the next frame can be sent.

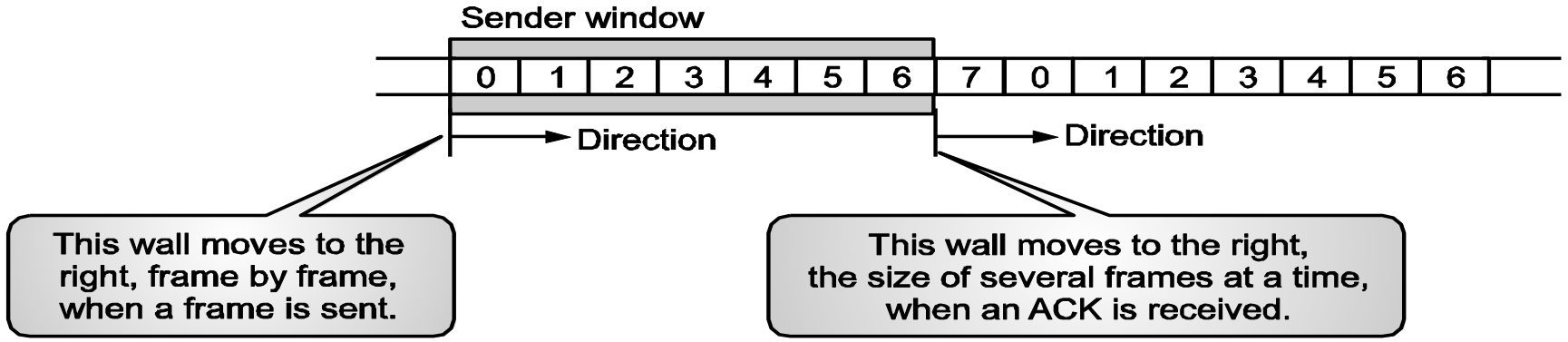


Sliding Window Flow Control

- In sliding window method of flow control, the sender can transmit several frames before getting the acknowledgement.
- The link can carry several frames at one time and its capacity can be used efficiently.
- The sliding window refers to imaginary boxes at both the sender and the receiver end.
- The window can hold frames at either end and these may be acknowledged at any point without waiting for the window to fill up.
- To keep track of which frames have been transmitted and received, sliding window introduces an identification scheme based on size of the window.
- The frames are numbered from 0 to n − 1 and the size of window is also n − 1.
- Example: If n=8, the frames are numbered 0, 1, 2, 3, 4, 5, 6, 7 and size of window = 7.
- Thus, the receiver sends an acknowledgment which includes the number of next frame it expects to receive.

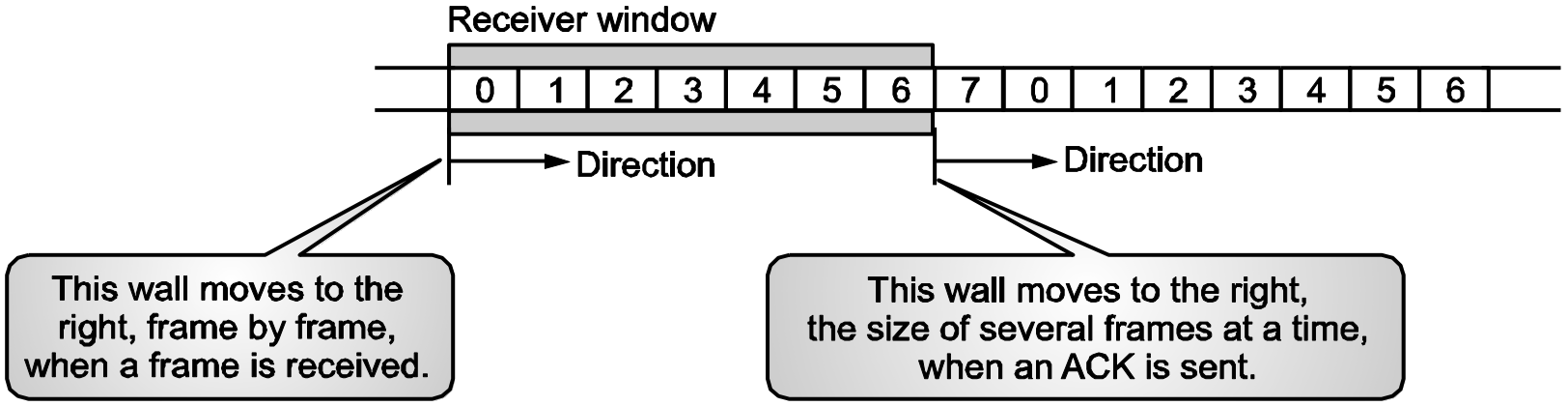
Sender's Window

- At the beginning of transmission, the sender's window contains n-1 frames.
- As the frames are sent out, the left boundary of the window moves inwards shrinking the size of the window.
- Once an acknowledgement arrives, the window expands to allow in a number of new frames equal to number of frames acknowledged by the receiver.

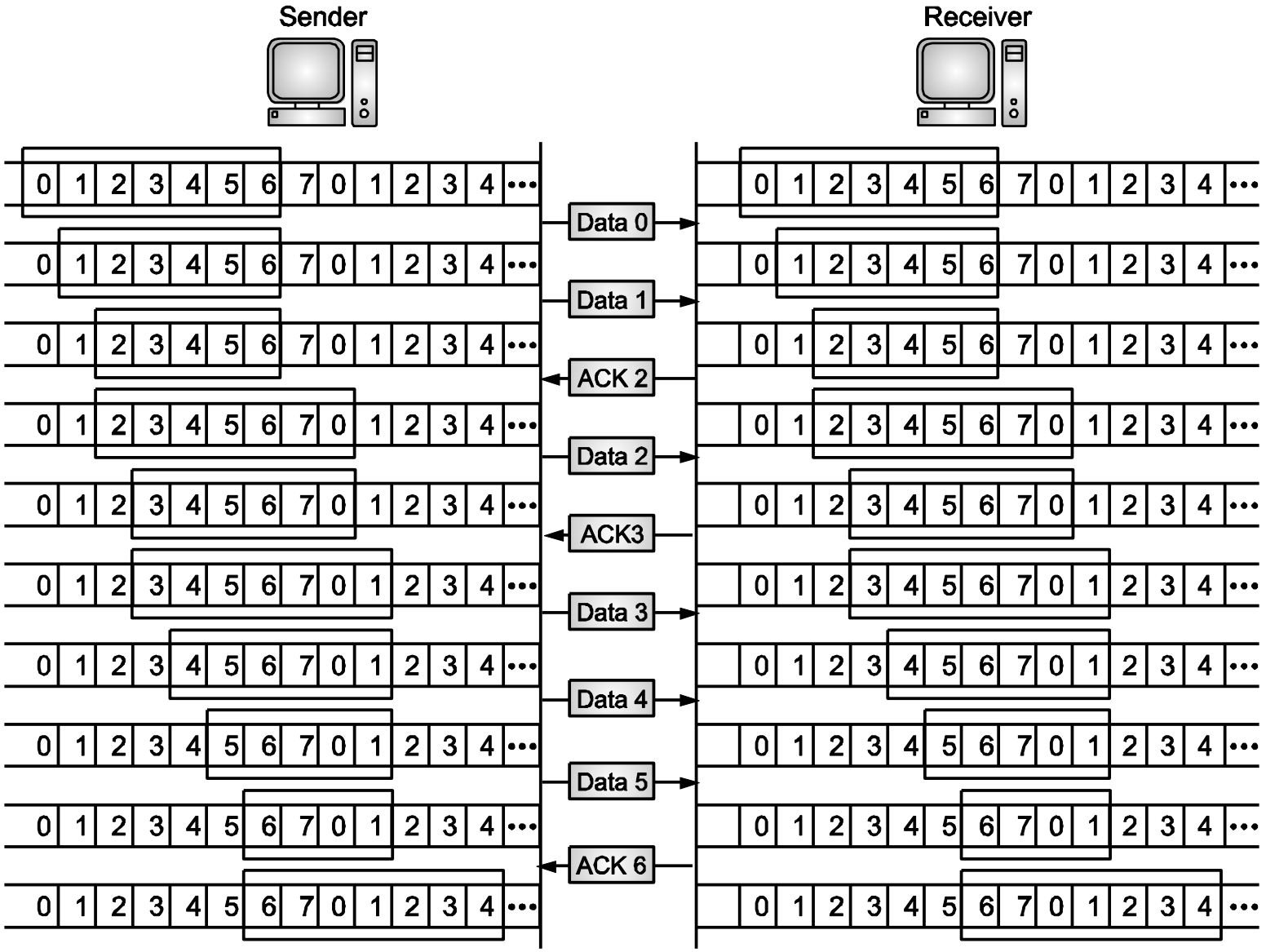


Receiver's Window

- At the beginning of transmission, the receiver's window contains n-1 spaces for frames.
- As new frames come in, the size of the receiver window shrinks as soon as the acknowledgement is sent.
- The window expands to include spaces for a number of frames equal to the number of frames acknowledged.



Sliding Window Flow Control Example



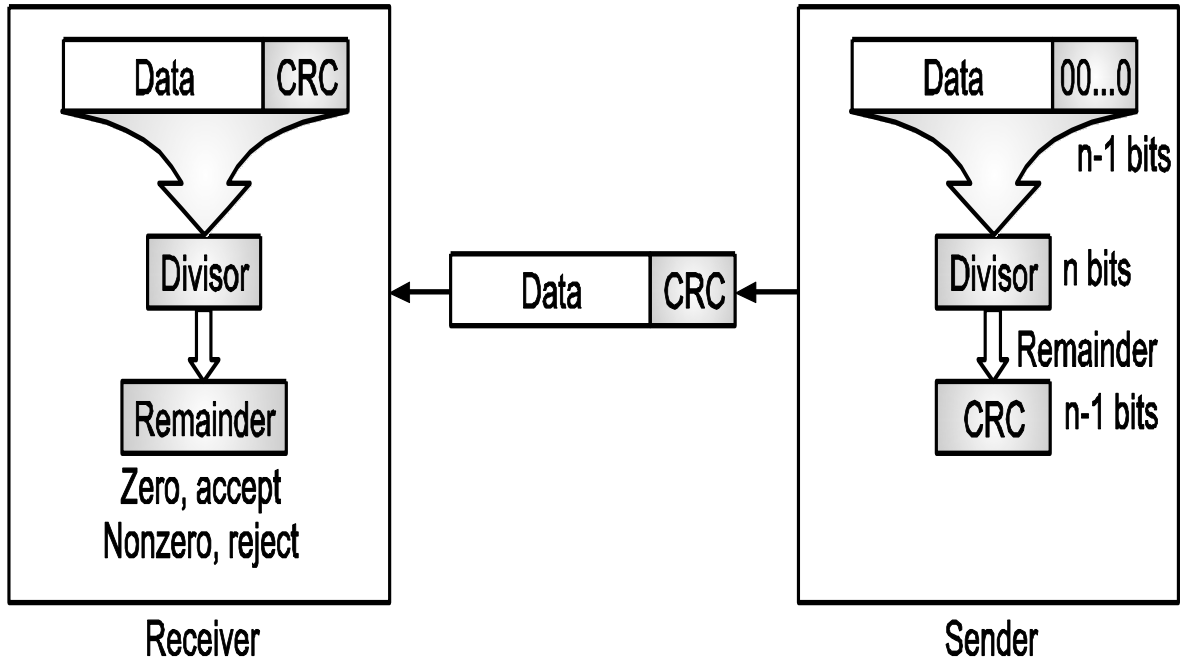
Error Detection

- Data can be corrupted during transmission.
- For reliable communication, errors must be detected and corrected.
- Errors are of two types.
    1. Single Bit Error: Only one bit in the data unit is changed.
    2. Burst Error: 2 or more bits in the data unit are changed.
- Cyclic Redundancy Check (CRC) is one of the methods used for error detection.

Cyclic Redundancy Check (CRC)

The basic steps involved in CRC are:

1. A string of n − 1 zero's is appended to the data unit.
2. The number 'n' is the number of bits in the predetermined divisor.
3. The newly elongated data unit is divided by the divisor using a process called Binary Division (or XOR division or Modulo-2 division).
4. The remainder resulting from the division is called CRC.
5. The CRC of n − 1 bits derived replaces the zeroes at the end of the data.
6. The data unit followed by the CRC arrives at the receiver end.
7. The receiver treats the whole string as a unit and divides it by the same divisor that was used to find the CRC remainder.
8. If the string arrives without error, the CRC checker yields a remainder of zero and the data unit passes.
9. If the string has been changed in the transit, the division gives a non-zero remainder and the data unit does not pass.

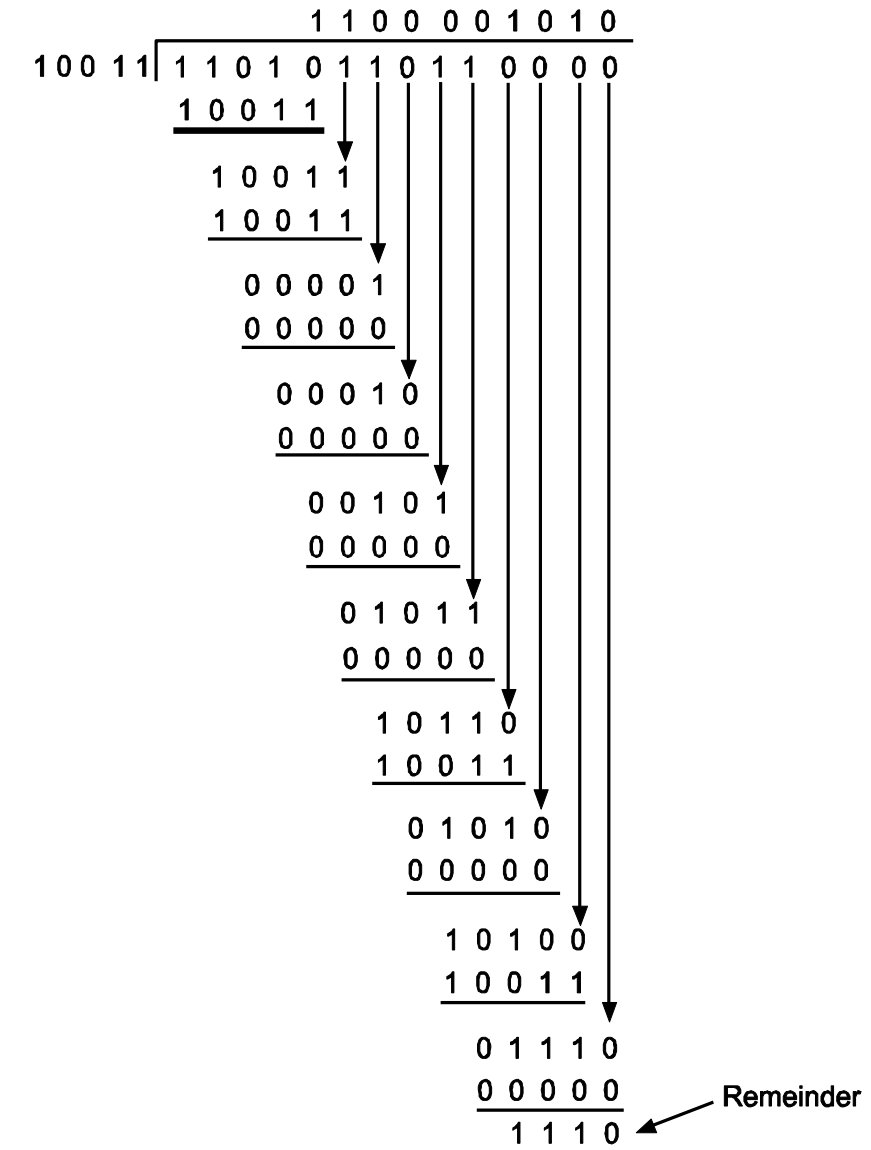


A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

Solution:

- The generator polynomial $G(x) = x^4 + x + 1$ is encoded as 10011.
- Clearly, the generator polynomial consists of 5 bits.
- So, a string of 4 zeroes is appended to the bit stream to be transmitted.
- The resulting bit stream is 1101011011**0000**.

Now, the binary division is performed as:



From here, CRC = 1110.

Now,

- The code word to be transmitted is obtained by replacing the last 4 zeroes of 1101011011**0000** with the CRC.
- Thus, the code word transmitted to the receiver = 1101011011**1110**.

Generate the CRC code for a dataword 110010101. The divisor 10101. Check whether there are errors in the received codeword.

Solution:

Given, M(x) = 110010101

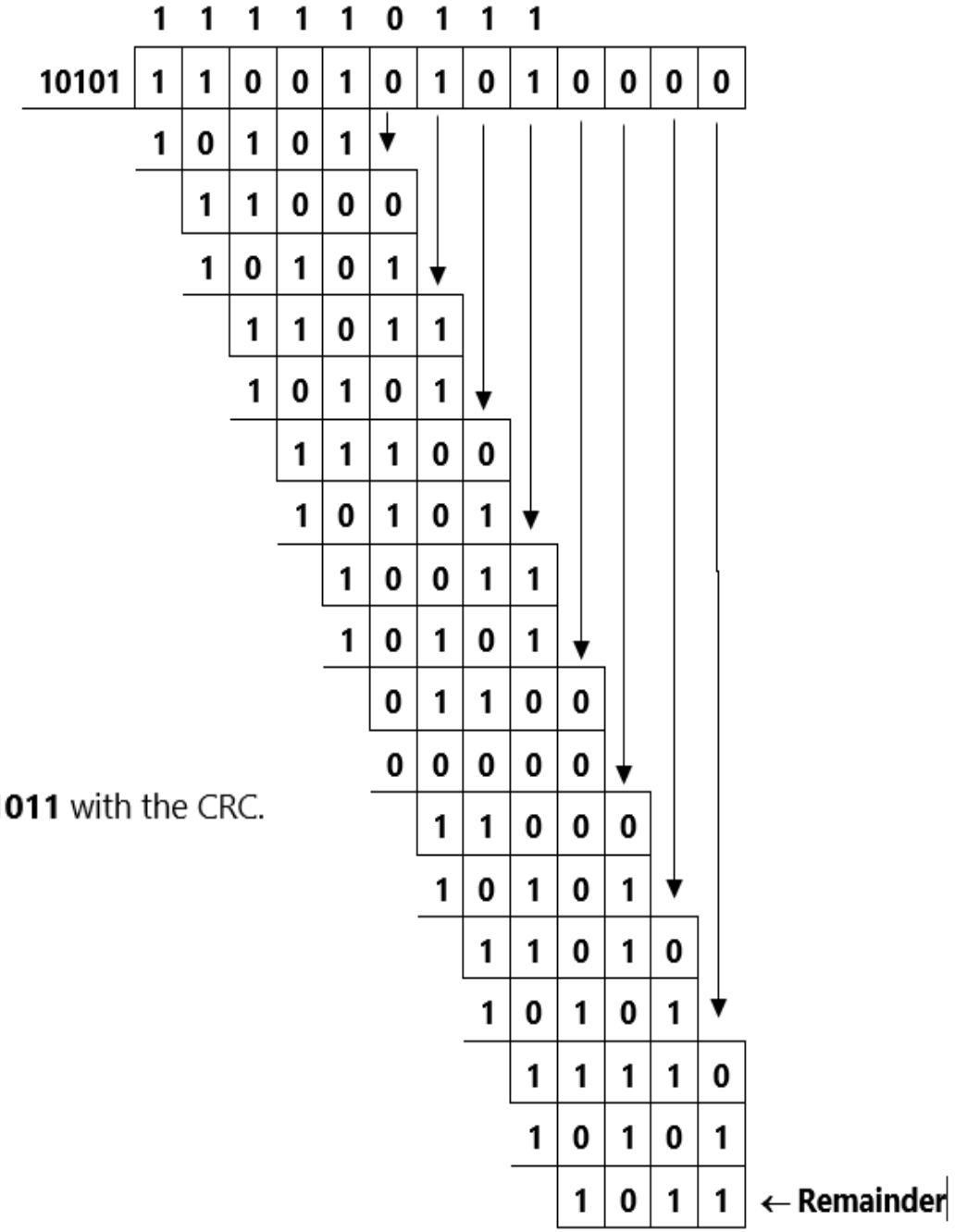
G(x) = 10101

∴ n = |G(x)| = 5

So, a string of 4 zeroes is appended to the bit stream to be transmitted.

The resulting bit stream is 110010101**0000**.

Now, the binary division is performed as:



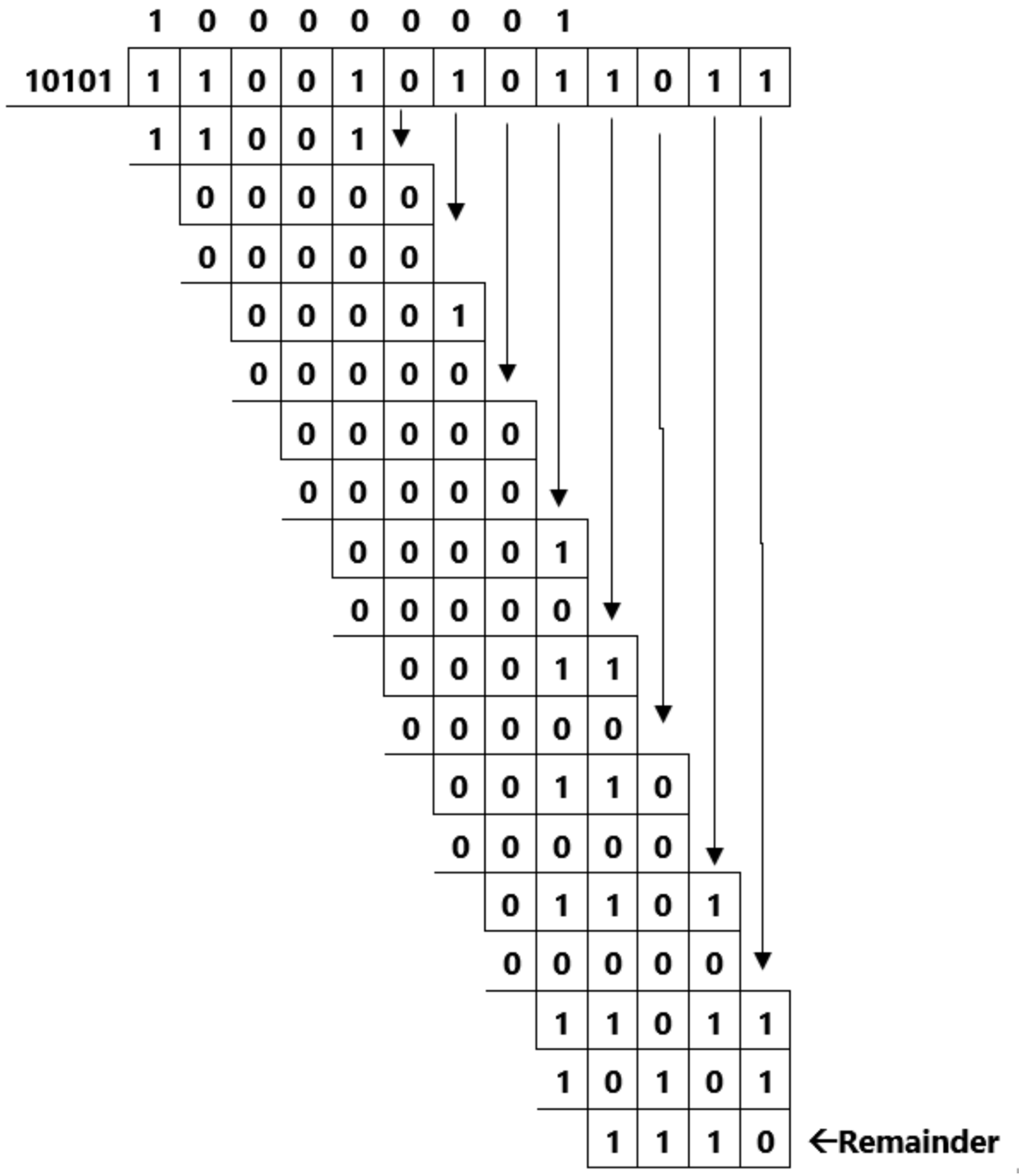
From here, CRC = 1011.

Now,

- The code word to be transmitted is obtained by replacing the last 4 zeroes of 110010101**1011** with the CRC.
- Thus, the code word transmitted to the receiver = 110010101**1011**.

Next,

- Receiver receives the bit stream = 1100101011011.
- Receiver performs the binary division with the same generator polynomial as:



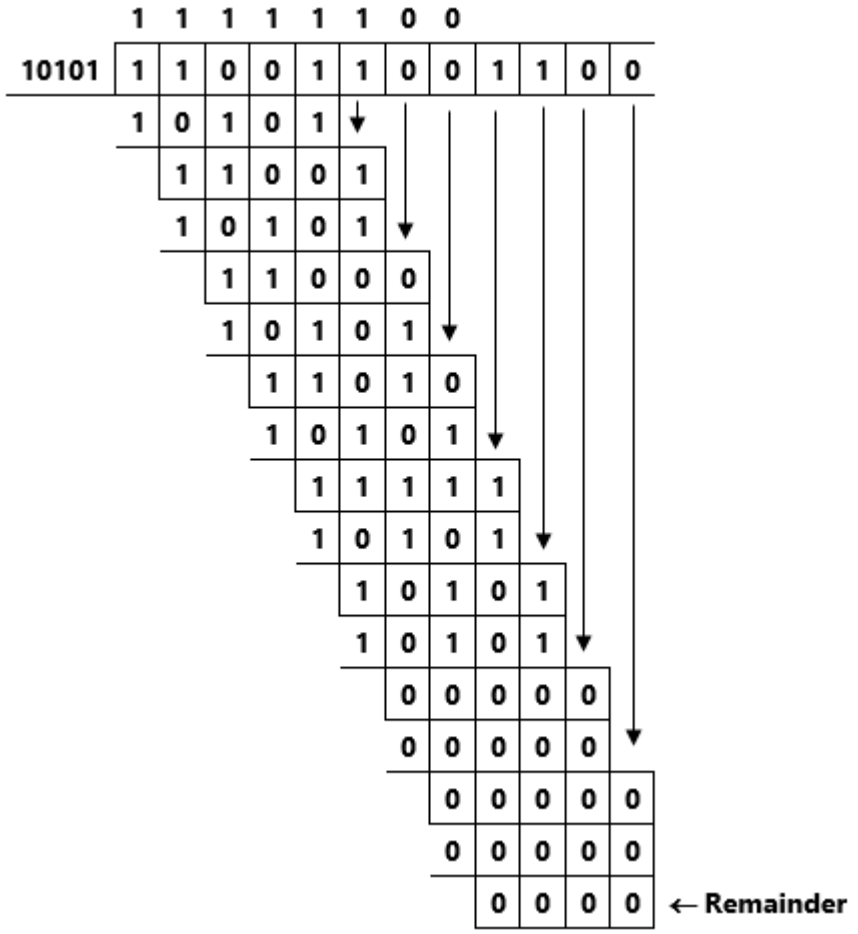
Since the remainder is not zero, there are errors in the received codeword.

The received string of bits is 1100011001100. Is it acceptable? If so, what is the data bit sequence? Consider the divisor is 10101.

Solution: Given, received string of bits = 110011001100

G(x) = 10101. Therefore, n = |G(x)| = 5

Receiver performs the binary division with 10101



Since the remainder is zero, the received bit string is accepted. To get the data bit sequence, we remove n − 1 bits from end of received bit string. Hence, the data bit sequence is 11001100.

Error Correction

- Hamming code is an error correcting code.
- Hamming codes are linear block codes.
- Parity bits are used here.
- They are inserted in between the data bits.
- The most commonly used is a 7-bit Hamming code.
- Structure of a 7-bit Hamming code:

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

(D → Data bits, P → Parity bits)

- Parity bits are in position 2^m; where m = 0, 1, 2, ….
- Computing the values of parity bits:

7	6	5	4	3	2	1	← Position
D7	D6	D5	P4	D3	P2	P1	
111	110	101	100	011	010	001	3-bit binary of position no.

- To find P1, select positions that has first bit as 1 from LSB i.e., positions 1,3,5,7.
- To find P2, select positions that has second bit as 1 from LSB i.e., positions 2,3,6,7.
- To find P4, select positions that has third bit as 1 from LSB i.e., positions 4, 5, 6, 7.
- Parity can be even or odd.

  If we want to find even parity, then number of 1's excluding parity bit has to be even. If yes, then the parity bit becomes 0; otherwise, the parity bit becomes 1.

  If we want to find odd parity, then number of 1's excluding parity bit has to be odd. If yes, then the parity bit becomes 0; otherwise, the parity bit becomes 1.

Q. A bit word 1011 is to be transmitted. Construct the even parity 7-bit Hamming code for the data.

Solution:

7	6	5	4	3	2	1	← Position
D7	D6	D5	P4	D3	P2	P1	
1	0	1	P4	1	P2	P1	Bits

To find P1, take bits in the position 1, 3, 5, 7. They are P1, 1, 1, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P1 = 1.

To find P2, take bits in the position 2, 3, 6, 7. They are P2, 1, 0, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P2 = 0.

To find P4, take bits in the position 4, 5, 6, 7. They are P4, 1, 0, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P4 = 0.

So, the even parity 7-bit Hamming code for data 1011 is **1010101**.

Q. Determine which bit is in error in the even parity. Hamming code character is 1100111.

Solution:

7	6	5	4	3	2	1	← Position
D7	D6	D5	P4	D3	P2	P1	
1	1	0	0	1	1	1	Bits

To find P1, take bits in the position 1, 3, 5, 7. They are 1, 1, 0, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P1 = 0. But here P1 =1 is given. Therefore, **P1 bit is in error**.

To find P2, take bits in the position 2, 3, 6, 7. They are 1, 1, 1, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P2 = 1. Therefore, P2 is not in error.

To find P4, take bits in the position 4, 5, 6, 7. They are 0, 0, 1, 1 respectively.

Given even parity. Therefore, number of 1's needs to be even.

Hence, P4 = 0. Therefore, P4 is not in error.

So only P1 bit is in error.

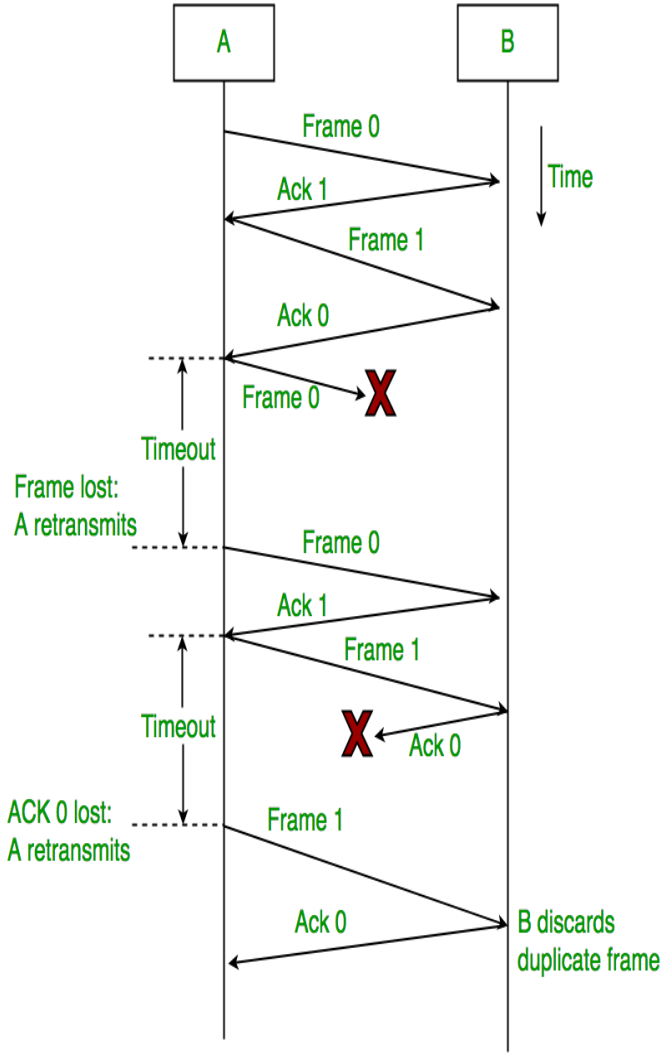
Corrected Hamming code character is **1100110**.

ERROR CONTROL

- When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted.
- In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.
- In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame.
- Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.
- Requirements for error control mechanism:
- **Error detection:** The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK:** When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK:** When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

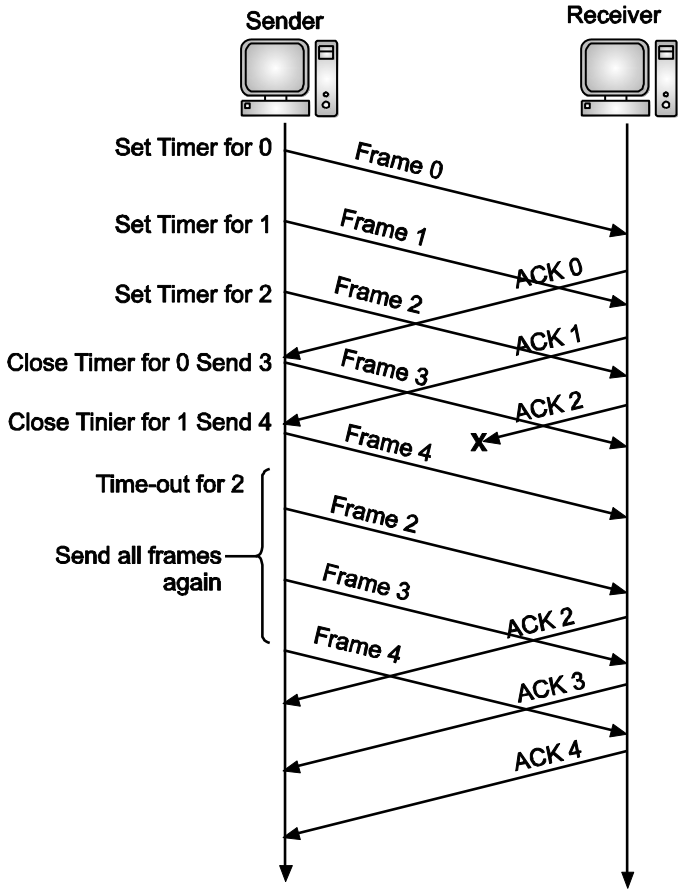
Stop-and-Wait ARQ

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.



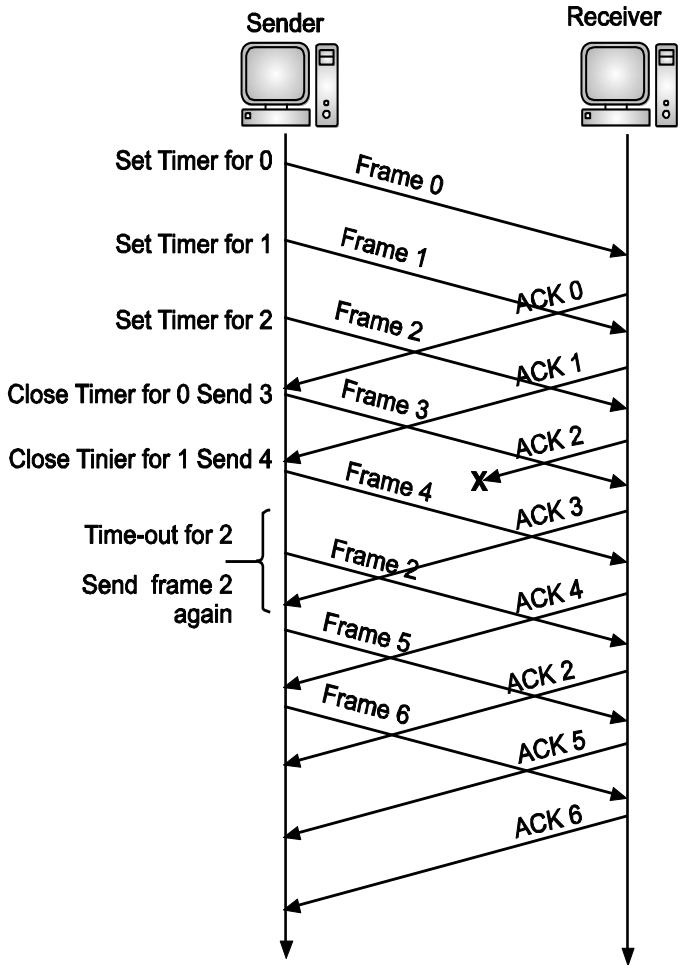
Go-Back-N ARQ

- In Go-Back-N ARQ method, both sender and receiver maintain a window.
- The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones.
- The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.
- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement.
- If all frames are positively acknowledged, the sender sends next set of frames.
- If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.



Selective Repeat ARQ

- In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.
- The sender in this case, sends only packet for which NACK is received.



High Level Data Link Protocol (HDLC)

- **HDLC** (High-Level Data Link Control) is a bit-oriented protocol.
- Used for communication over the **point-to-point and multipoint links**.
- Implements the mechanism of ARQ(Automatic Repeat Request).
- Full-duplex communication is possible.
- Widely used protocol and offers reliability, efficiency, and a high level of flexibility.

Three types of stations in HDLC

- **Primary Station:** This station mainly looks after data management. In the case of the communication between the primary and secondary station, it is the responsibility of the primary station to connect and disconnect the data link. The frames issued by the primary station are commonly known as commands.
- **Secondary Station:** The secondary station operates under the control of the primary station. The frames issued by the secondary stations are commonly known as responses.
- **Combined Station:** The combined station acts as both Primary stations as well as Secondary stations. The combined station issues both commands as well as responses.

Transfer Modes in HDLC

- The HDLC protocol offers two modes of transfer that mainly can be used in different configurations. These are as follows:

1. Normal Response Mode(NRM)
2. Asynchronous Response Mode (ARM)
3. Asynchronous Balance Mode(ABM)

Normal Response Mode(NRM)

- In this mode, the configuration of the station is unbalanced.
- There are one primary station and multiple secondary stations.
- Where the primary station can send the commands and the secondary station can only respond.
- This mode is used for both **point-to-point** as well as **multiple-point links.**

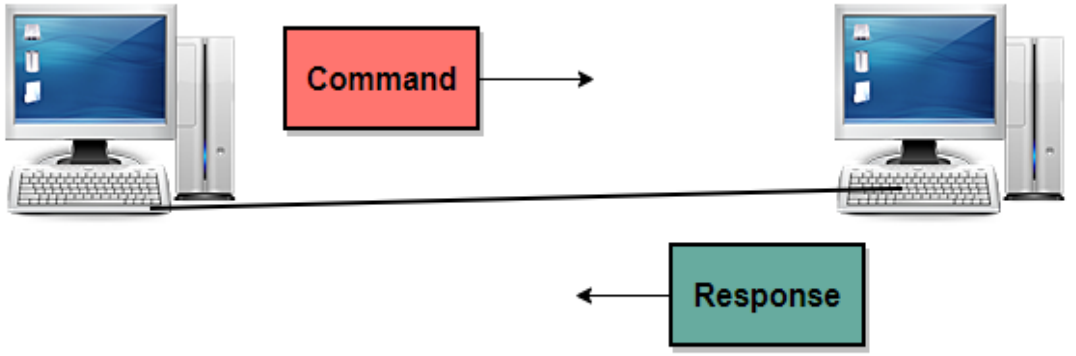


Figure: Point-to-Point

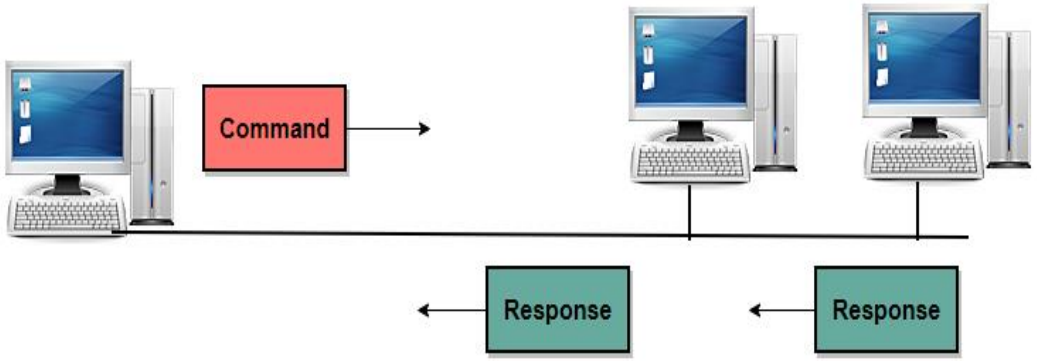


Figure: Multipoint

Asynchronous Response Mode (ARM)

- Asynchronous Response Mode (ARM) is **an unbalanced configuration in which secondary terminals may transmit without permission from the primary terminal**.
- However, there is still a distinguished primary terminal which retains responsibility for line initialization, error recovery, and logical disconnect.

Asynchronous Balance Mode(ABM)

- In this mode, the configuration of the station is balanced.
- In this mode, the link is point-to-point, and each station can function as a primary and as secondary.
- Asynchronous Balance mode(ABM) is a commonly used mode today.

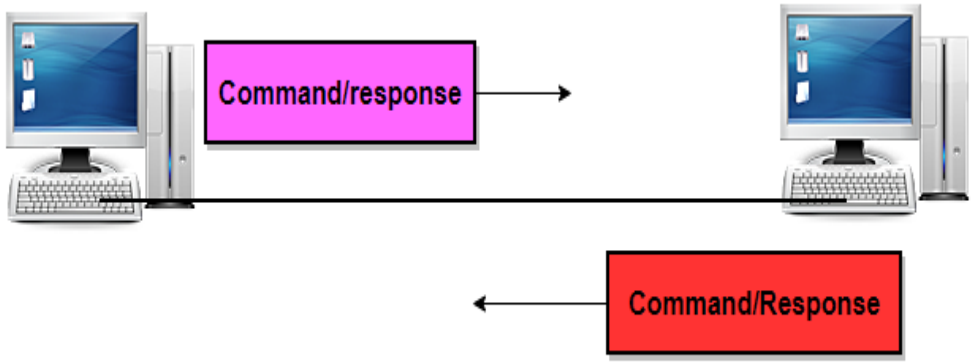
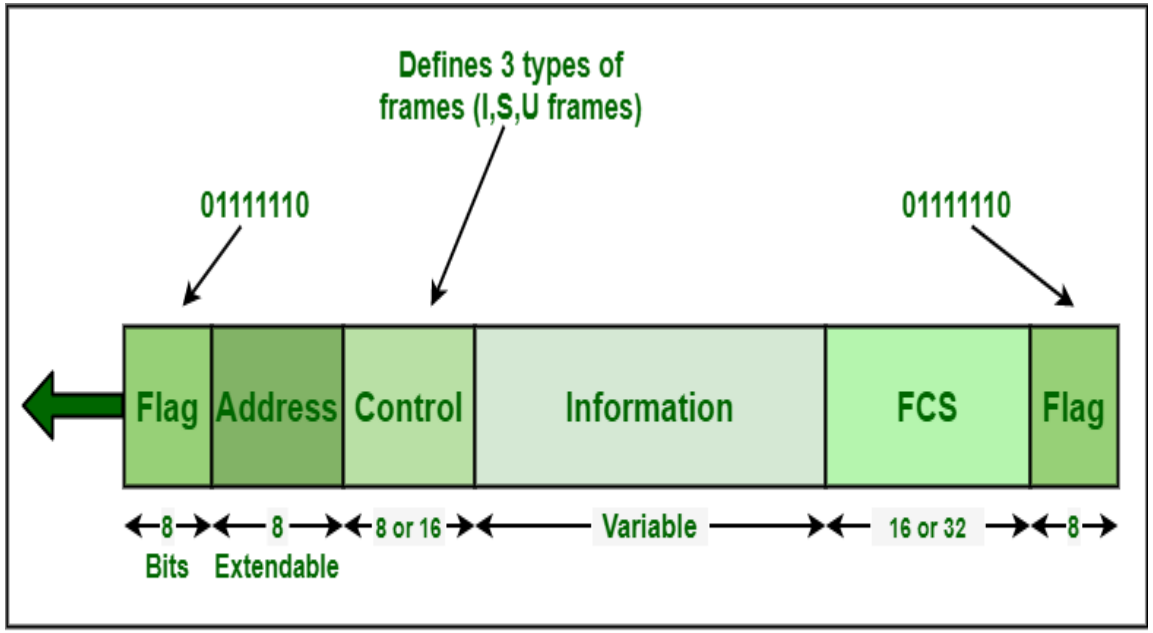


Figure: Asynchronous Balance Mode

HDLC Frames

- There are three types of frames defined in the HDLC:
- **Information Frames(I-frames):** These frames are used to transport the user data and the control information that is related to the user data. If the first bit of the control field is 0 then it is identified as I-frame.
- **Supervisory Frames(S-frames)** These frames are only used to transport the control information. If the first two bits of the control field are 1 and 0 then the frame is identified as S-frame.
- **Unnumbered Frames(U-Frames)** These frames are mainly reserved for system management. These frames are used for exchanging control information between the communicating devices. If the first two bits of the control field are 1 and 1 then the frame is identified as U-frame.

HDLC Frame Structure



Basic Frame Structure

1. Flag Field

This field of the HDLC frame is mainly a sequence of 8-bit having the bit pattern 01111110 and it is used to identify the beginning and end of the frame. The flag field mainly serves as a synchronization pattern for the receiver.

2. Address Field

It is the second field of the HDLC frame and it mainly contains the address of the secondary station. This field can be 1 byte or several bytes long which mainly depends upon the need of the network. In case if the frame is sent by the primary station, then this field contains the address(es) of the secondary stations. If the frame is sent by the secondary station, then this field contains the address of the primary station.

3. Control Field

This is the third field of the HDLC frame and it is a 1 or 2-byte segment of the frame and is mainly used for flow control and error control. Bits interpretation in this field mainly depends upon the type of the frame.

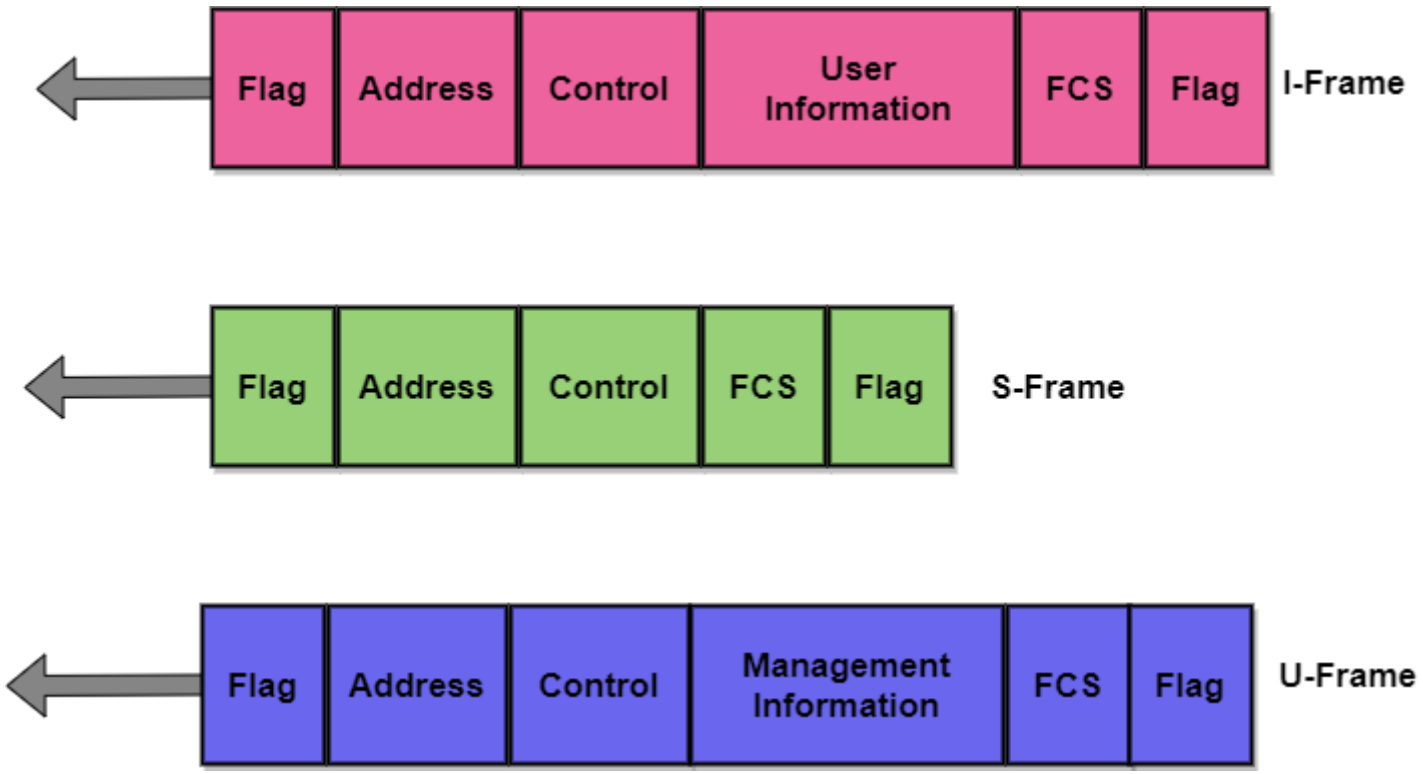
4. Information Field

This field of the HDLC frame contains the user's data from the network layer or the management information. The length of this field varies from one network to another.

5. FCS Field

FCS means Frame check sequence and it is the error detection field in the HDLC protocol. There is a 16 bit CRC code for error detection.

Frame Format



Point-to-Point Protocol

- PPP protocol is a byte-oriented protocol.
- The PPP protocol is mainly used to establish a direct connection between two nodes.
- The PPP protocol mainly provides connections over multiple links.
- This protocol defines how two devices can authenticate with each other.
- PPP protocol also defines the format of the frames that are to be exchanged between the devices.
- This protocol also defines how the data of the network layer are encapsulated in the data link frame.
- The PPP protocol defines how the two devices can negotiate the establishment of the link and then can exchange the data.

PPP Frame Format

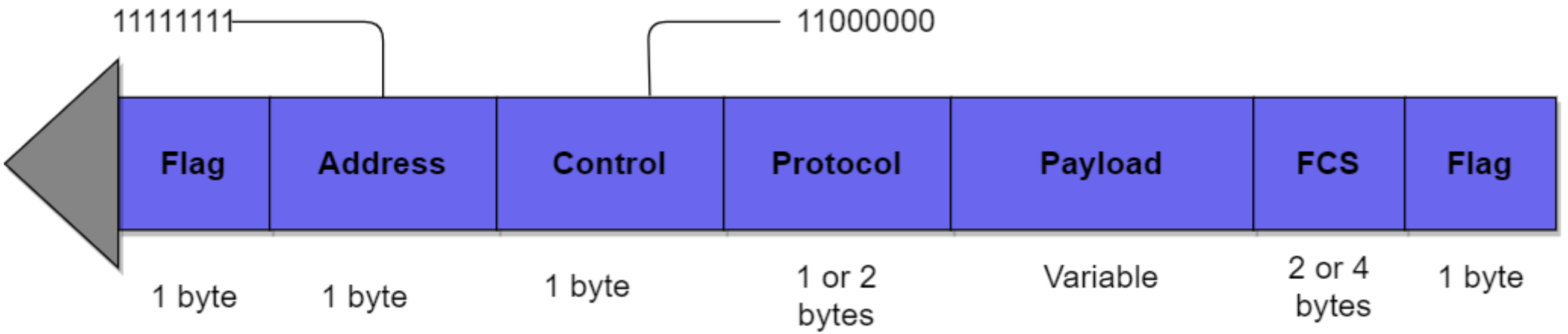


Figure: PPP Frame Format

1. Flag

The PPP frame mainly starts and ends with a 1-byte flag field that has the bit pattern: 01111110. It is important to note that this pattern is the same as the flag pattern used in HDLC. But there is a difference too and that is PPP is a byte-oriented protocol whereas the HDLC is a bit-oriented protocol.

2. Address

The value of this field in PPP protocol is constant and it is set to 11111111 which is a broadcast address. The two parties can negotiate and can omit this byte.

3. Control

The value of this field is also a constant value of 11000000. We have already told you that PPP does not provide any flow control and also error control is limited to error detection. The two parties can negotiate and can omit this byte.

4. Protocol

This field defines what is being carried in the data field. It can either be user information or other information. By default, this field is 2 bytes long.

5. Payload field

This field carries the data from the network layer. The maximum length of this field is 1500 bytes. This can also be negotiated between the endpoints of communication.

6. FCS

It is simply a 2-byte or 4-byte standard CRC(Cyclic redundancy check).

Transition Phases in the PPP Protocol

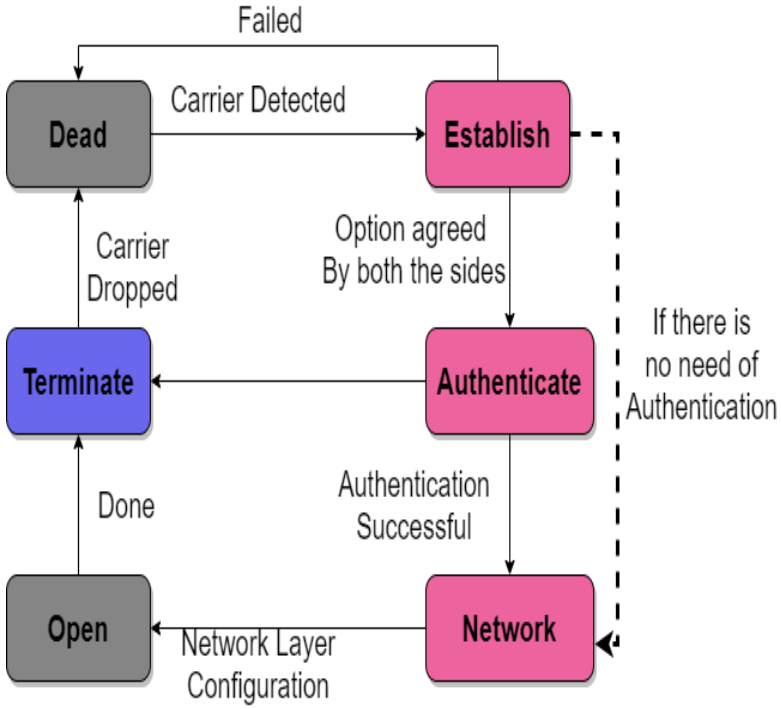


Figure: Transition Phases

Dead

In this phase, the link is not being used. No active carrier is there at the physical layer and the line is simply quiet.

Establish

If one of the nodes starts the communication then the connection goes into the established phase. In this phase, options are negotiated between the two parties. In case if the negotiation is done successfully then the system goes into the Authenticate phase (in case if there is the requirement of authentication otherwise goes into the network phase.)

Several packets are exchanged here.

Authenticate

This is an optional phase. During the establishment phase, the two nodes may decide not to skip this phase. If the two nodes decide to proceed with the authentication then they send several authentication packets.

If the result of this is successful then the connection goes into the networking phase otherwise goes into the termination phase.

Network

In this phase, the negotiation of the protocols of the network layer takes place. The PPP protocol specifies that the two nodes establish an agreement of the network layer before the data at the network layer can be exchanged. The reason behind this is PPP supports multiple protocols at the network layer.

In case if any node is running multiple protocols at the network layer simultaneously then the receiving node needs to know that which protocol will receive the data.

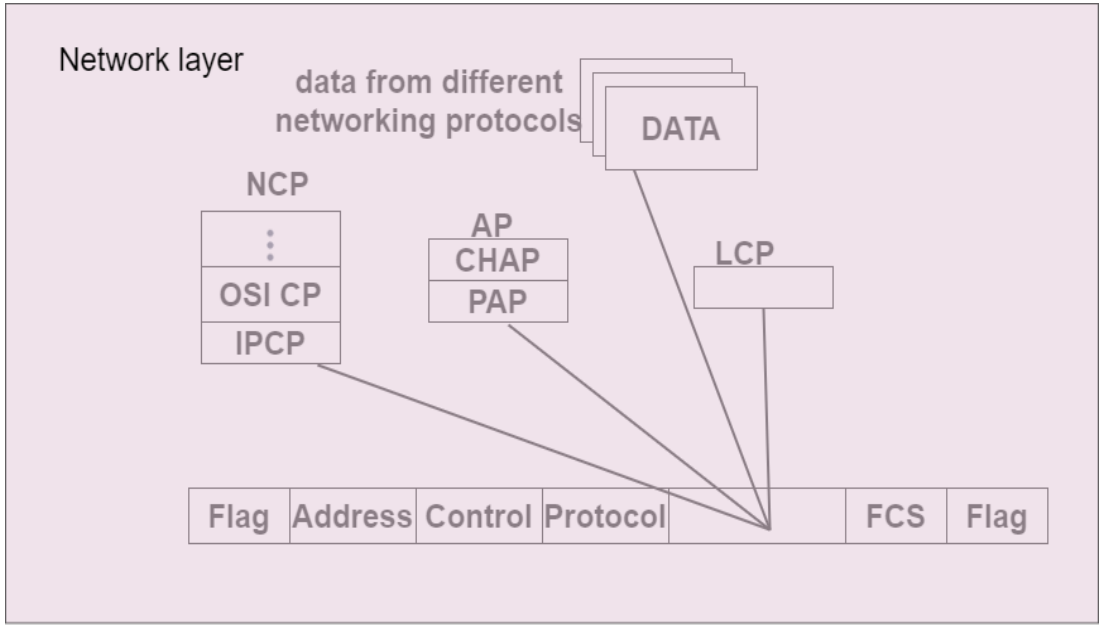
Open

In this phase the transfer of the data takes place. Whenever a connection reaches this phase, then the exchange of data packets can be started. The connection remains in this phase until one of the endpoints in the communication terminates the connection.

Terminate

In this phase, the connection is terminated. There is an exchange of several packets between two ends for house cleaning and then closing the link.

Components of PPP/ PPP stack



LCP:0xC021
AP: 0xC023 and 0xC223
NCP:0x8021

LCP: Link Control Protocol
AP: Authentication Protocol
NCP: Network Control Protocol

Basically, PPP is a layered protocol. There are three components of the PPP protocol and these are as follows:

- Link Control Protocol
- Authentication Protocol
- Network Control Protocol

Link Control protocol

This protocol is mainly responsible for establishing, maintaining, configuring, and terminating the links. Both endpoints of the link must need to reach an agreement about the options before the link can be established.

Authentication protocol

This protocol is mainly used to authenticate the endpoints for the use of other services. There are two protocols for authentication:

1. Password Authentication Protocol
2. Challenge handshake authentication Protocol

Network Control Protocol

The Network Control Protocol is mainly used for negotiating the parameters and facilities for the network layer.

Some of the Network Control protocol of the PPP are as follows;

1. Internet Protocol Control Protocol (IPCP)
2. Internetwork Packet Exchange Control Protocol (IPXCP)
3. DECnet Phase IV Control Protocol (DNCP)
4. NetBIOS Frames Control Protocol (NBFCP)
5. IPv6 Control Protocol (IPV6CP)

HDLC Vs PPP

BASIS FOR COMPARISON	HDLC	PPP
Expands to	High-level Data Link Layer Protocol	Point-to-Point Protocol
Type of protocols	Bit-oriented protocol	Byte oriented protocol
Used in	Only synchronous media	Synchronous as well as asynchronous media
Authentication	No provision of authentication	Provides authentication
Dynamic addressing	Does not offer dynamic addressing.	Dynamic addressing is used.
Implemented in	Point-to-point and multipoint configurations.	Only point-to-point configurations.
Compatibility with other protocols	Can not be operated with non-Cisco devices.	Interoperable with non-Cisco devices also.

Medium Access Control

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of the source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiates retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

Channel Allocation Problem

- When there is more than one user who desires access to a shared network channel, an algorithm is deployed for channel allocation among the competing users.
- The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.
- Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.

Channel Allocation Schemes

- Channel Allocation may be done using two schemes −

1. Static Channel Allocation
2. Dynamic Channel Allocation

Static Channel Allocation

- In a static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred to as fixed channel allocation or fixed channel assignment.
- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel.
- However, it is not suitable in the case of a large number of users with variable bandwidth requirements.

Dynamic Channel Allocation

- In a dynamic channel allocation scheme, frequency bands are not permanently assigned to the users.
- Instead, channels are allotted to users dynamically as needed, from a central pool.
- The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimizes bandwidth usage and results in faster transmissions.
- Dynamic channel allocation is further divided into centralized and distributed allocation.
- Possible assumptions include:

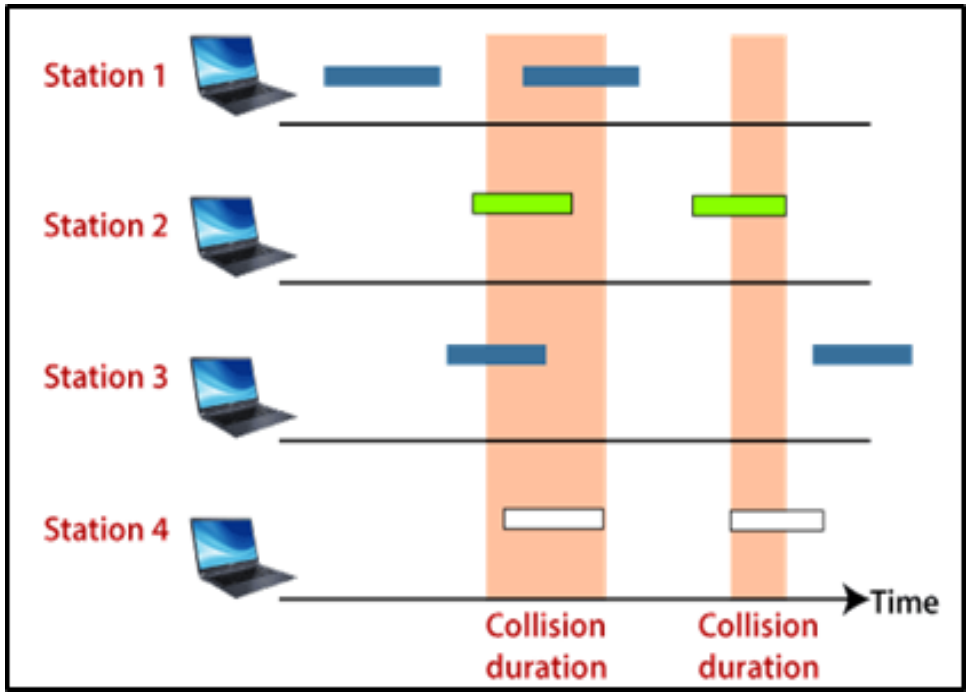
1. **Station Model**: Assumes that each of N stations independently produces frames. Once the frame is generated at the station, the station does nothing until the frame has been successfully transmitted.
2. **Single Channel Assumption**: In this allocation, all stations are equivalent and can send and receive on that channel.
3. **Collision Assumption**: If two frames overlap time-wise, then that's a collision. Any collision is an error, and both frames must be retransmitted. Collisions are the only possible error.
4. **Time** can be divided into Slotted or Continuous.
5. **Stations** can sense a channel if it is busy before they try it.

ALOHA

- ALOHA is a multiple-access protocol for the transmission of data via a shared network channel.
- It operates in the medium access control sublayer (MAC sublayer).
- In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy.
- If the channel is idle, then the frames will be successfully transmitted.
- If two frames attempt to occupy the channel simultaneously, the collision of frames will occur and the frames will be discarded.
- These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

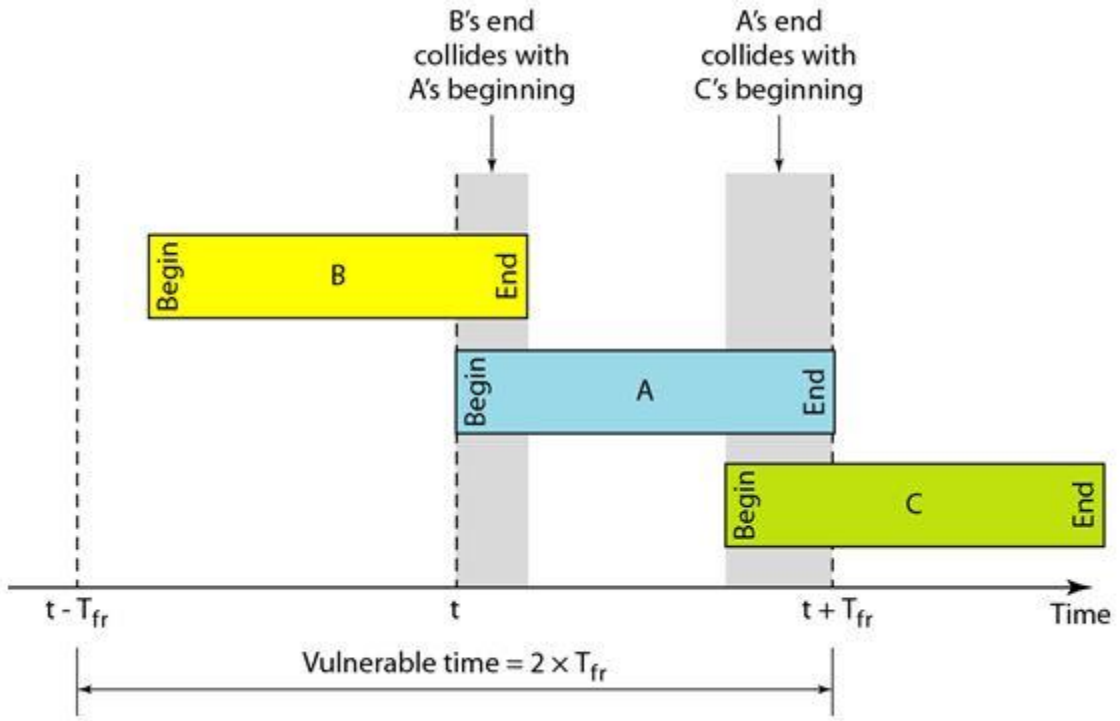
Pure ALOHA

- In pure ALOHA, the time of transmission is continuous.
- Time is not slotted and stations can transmit whenever they want.
- There is a high possibility of collision and the colliding frames will be destroyed.
- If frames collide and get destroyed, then the sender waits for a random amount of time and resends the frame.



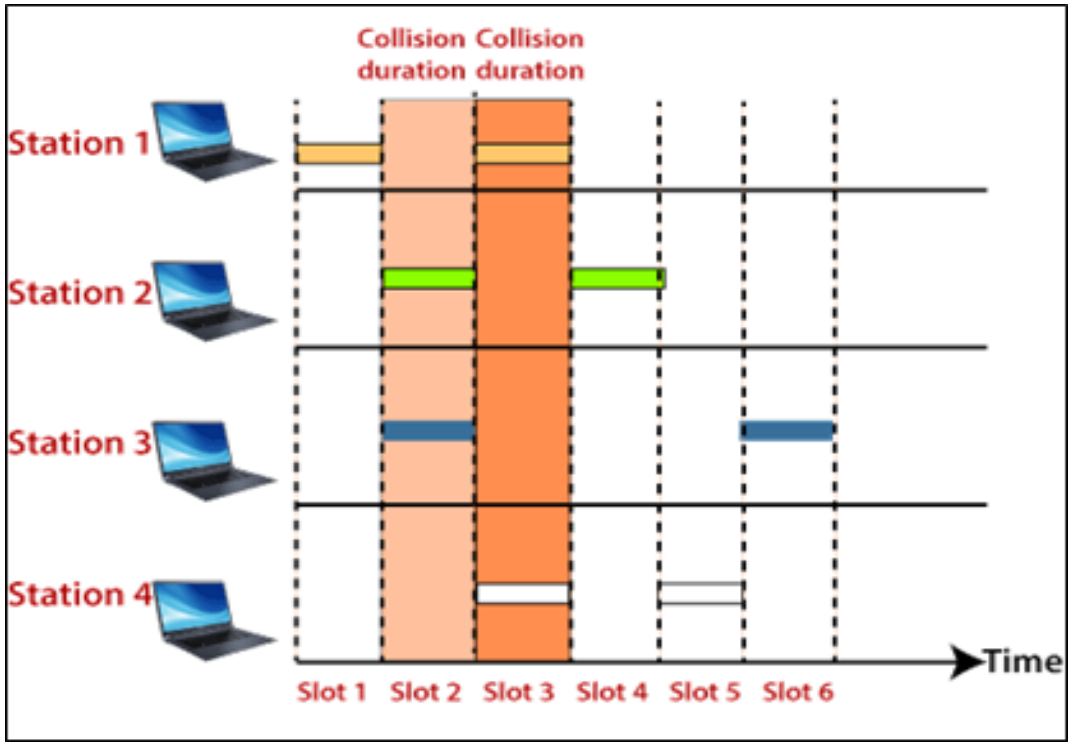
Vulnerable time for Pure ALOHA

- The vulnerable time is in which there is a possibility of collision.
- We assume that the stations send fixed-length frames with each frame taking T_{fr} Sec to send.
- The following figure shows the vulnerable time for station A.
- Station A sends a frame at time t.
- Now imagine station B has already sent a frame between $(t - T_{fr})$ and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame.
- On the other hand, suppose that station C sends a frame between t and $(t + T_{fr})$. Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

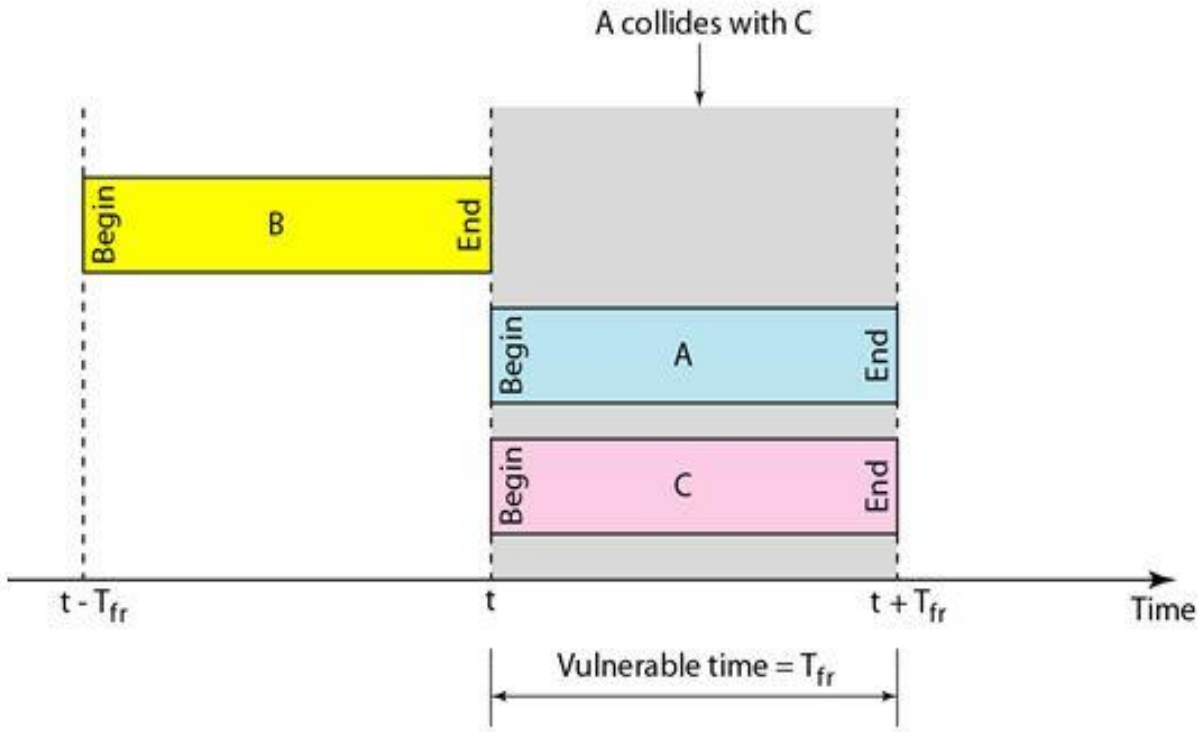


Slotted ALOHA

- Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA.
- The shared channel is divided into a number of discrete time intervals called slots.
- A station can transmit only at the beginning of each slot.
- However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.



Vulnerable time for Slotted ALOHA



Efficiency of ALOHA

Terms Used

- Frame Time: Time required to transmit a frame
- G: Average number of new + old frames generated per frame time.
  (Old frames are the frames which have to be retransmitted due to collision)
- S: Average number of new frames generated per frame time
- P_0: Probability that the frame does not suffer collision.
- VP (Vulnerable Period): Time for which a station should not transmit anything to avoid collision with the shaded frame.
- For pure ALOHA, vulnerable period = 2 time slots.
- For slotted ALOHA, vulnerable period = 1 time slot.

Derivation:

At low load, $S \approx 0$ and $G \approx 0$.

$\therefore S = G$

At high load, $S = G.P_0$ .....(I)

According to Poisson distribution formula

$P_k = \frac{e^{-m} m^k}{k!}$, where m is the mean and k is the random variable

For $k = 0$, $P_0 = e^{-m}$

$\therefore S = G.\ e^{-m}$ ..... (II)

For pure ALOHA,

VP = 2 time slots

$\therefore m = 2G$

Putting m = 2G in equation (II), we get

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

Differentiating w.r.t G and equate it to zero

$\frac{dS}{dG} = \frac{d}{dG}(G.\ e^{-2G}) = 0$

$G\ e^{-2G}(-2) + e^{-2G}(1) = 0$

$e^{-2G}(1 - 2G) = 0$

$\therefore (1-2G) = 0$

$\therefore G = 0.5$

At $G = 0.5$, $S_{max} = G.\ e^{-2G} = 0.5\ e^{-2x0.5}$

$\therefore S_{max} = 0.184$

$\therefore \boldsymbol{\eta_{max} = 0.184 \times 100 = 18.4\%}$

For slotted ALOHA,

VP = 1 time slot

$\therefore m = G$

Putting m = G in equation (II), we get

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

Differentiating w.r.t G and equate it to zero

$\frac{dS}{dG} = \frac{d}{dG}(G.\ e^{-G}) = 0$

$G\ e^{-G}(-1) + e^{-G}(1) = 0$

$e^{-2G}(1 - G) = 0$

$\therefore (1-G) = 0$

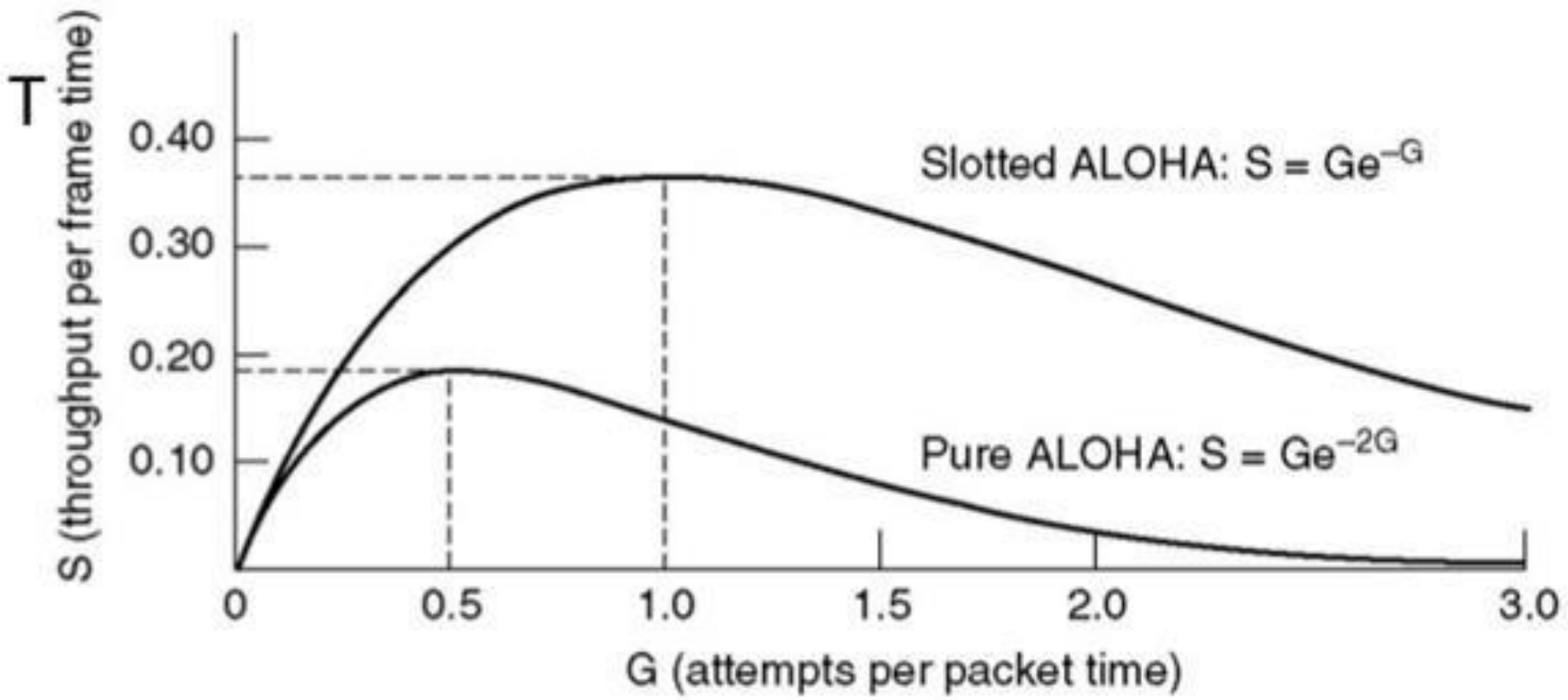
$\therefore G = 1$

At $G = 1$, $S_{max} = G.\ e^{-G} = 1e^{-1}$

$\therefore S_{max} = 0.368$

$\therefore \boldsymbol{\eta_{max} = 0.368 \times 100 = 36.8\%}$

Performance of Pure and Slotted ALOHA



Pure ALOHA Vs Slotted ALOHA

Pure ALOHA	Slotted ALOHA
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur = 2 x T	Vulnerable time in which collision may occur = T
Probability of successful transmission of data packet = $G \times e^{-2G}$	Probability of successful transmission of data packet = $G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)
The main advantage of pure ALOHA is its simplicity in implementation.	The main advantage of slotted ALOHA is that it reduces the number of collisions to half and doubles the efficiency of pure aloha.

Q1. A group of N stations share 100 Kbps slotted ALOHA channel. Each station output a 500 bits frame on an average of 5000ms even if previous one has not been sent. What is the required value of N?

Solution:

Throughput of One Station

Throughput of each station

= Number of bits sent per second

= 500 bits / 5000ms

= 500 bits / (5000 x 10^{-3} sec)

= 100 bits/sec

Throughput of Slotted ALOHA

Throughput of slotted ALOHA

= Efficiency x Bandwidth

= 0.368 x 100 Kbps

= 36.8 Kbps

Total Number of Stations

Throughput of slotted aloha = Total number of stations x Throughput of each station

Substituting the values, we get-

36.8 Kbps = N x 100 bits/sec

∴ N = 368

Thus, required value of **N = 368**.

Q2. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:

a. 1000 frames per second

b. 500 frames per second

c. 250 frames per second

Solution:

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-2G}$ or $S = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-2G}$ or $S = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ frames. Only 92 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-2G}$ or $S = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$ frames. Only 38 frames out of 250 will probably survive.

Q3. A slotted ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces:

a. 1000 frames per second

b. 500 frames per second

c. 250 frames per second.

Solution:

The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, this is 1 frame per millisecond. The load is 1. In this case $S = G \times e^{-G}$ or $S = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.368 = 368$ frames. Only 368 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, this is (1/2) frame per millisecond. The load is (1/2). In this case $S = G \times e^{-G}$ or $S = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.303 = 151$ frames. Only 151 frames out of 500 will probably survive.

c. If the system creates 250 frames per second, this is (1/4) frame per millisecond. The load is (1/4). In this case $S = G \times e^{-G}$ or $S = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$ frames. Only 49 frames out of 250 will probably survive.

Carrier Sense Multiple Access (CSMA) Protocol

- Carrier Sense: A station can sense the channel to see if anyone is using it. If the channel is being used, then the station will not attempt to use the channel.
- CSMA works on the principle of "Listen before Talking" or "Sense before Transmit".
- Types:

(a) 1-Persistent CSMA

(b) Non-persistent CSMA

(c) p- Persistent CSMA

(d) CSMA/CD

1-Persistent CSMA

- When a station needs to send data, it first listens to the channel.
- If the channel is busy, the station waits till the channel becomes free.
- When the channel becomes free, a station can transmit a frame.
- A collision occurs when two stations detect an idle channel at the same time and simultaneously send frames.
- If a collision occurs, the station waits a random amount of time and starts all over again.
- It is called 1-persistent as the station will transmit with a probability of 1, when it finds the channel idle.

Advantage

- Due to carrier sense property, 1-persistent CSMA gives better performance than the ALOHA systems.

Drawbacks

- Propagation Delay: It is possible that just after a station begins transmitting, another station becomes ready to send and it will sense the channel. If the first station's signal has not yet reached the 2nd station, the 2nd station will sense an idle channel and will begin sending its data. This will lead to a collision.
- Assume that station 2 and station 3 are waiting for station 1 to finish its transmission. Immediately after station 1 finishes transmitting, both station 2 and station 3 begin transmitting at the same time thus leading to a collision.

Non-persistent CSMA

- A station senses the channel when it wants to send data.
- If the channel is idle, the station begins sending the data.
- However, if the channel is busy, the station does not continually sense the channel like 1-persistent CSMA. Instead, it waits a random period of time and then checks the channel again.

- **Disadvantage**

This leads to longer delays than 1-persistent CSMA.

- **Advantage**

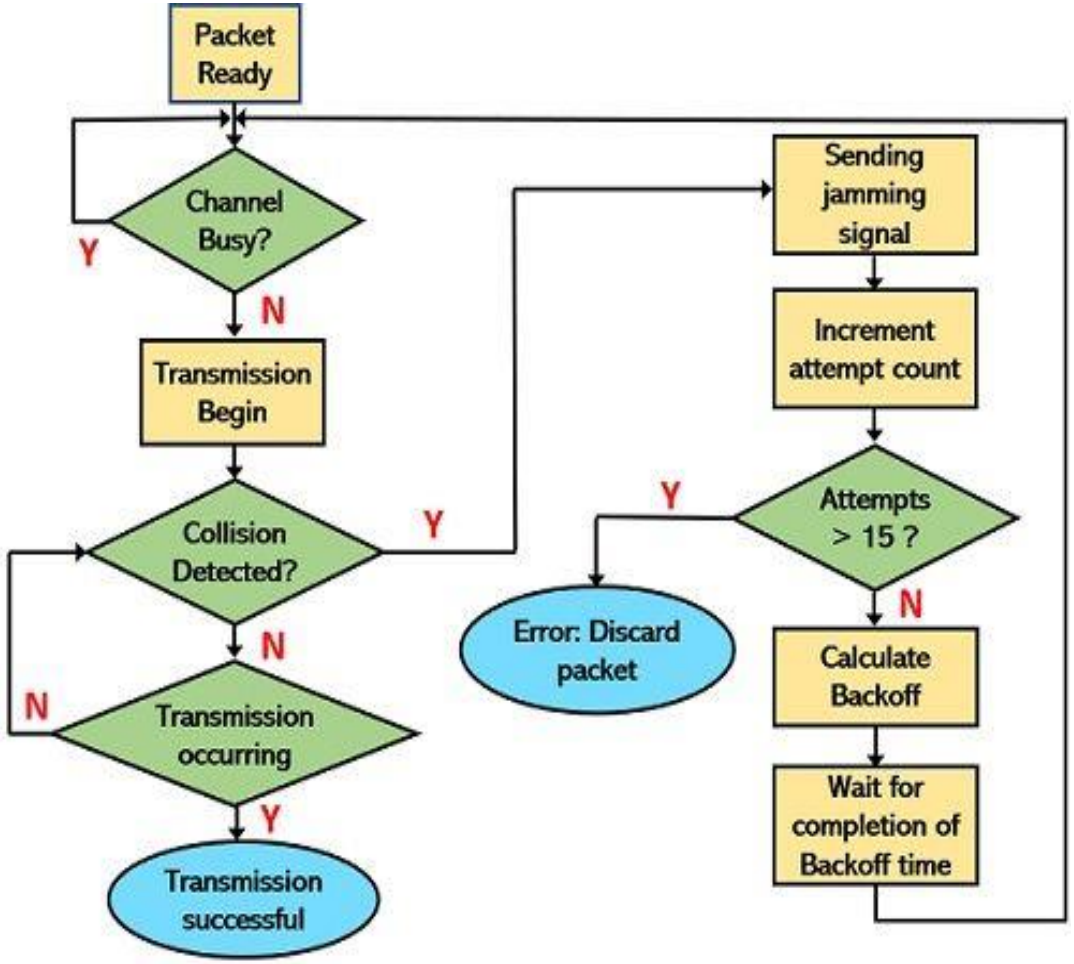
This algorithm leads to better channel utilization.

p-persistent CSMA

- It is used for slotted channels.
- When a station becomes ready to send, it senses the channel.
- If channel is idle, station transmits within that slot with a probability p and defers from sending with a probability q = 1- p.
- If p > q, then the station transmits, else if p < q, then the station does not transmit and waits till the next slot and again checks if p > q or p < q.
- This process is repeated until either the frame has been transmitted or another station has started transmitting.

CSMA/CD (Carrier Sense Multiple Access with Collison Detection)

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.
- It senses or listens to whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free.
- The collision detection technology detects collisions by sensing transmissions from other stations.
- On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.
- The maximum permissible attempts to transmit a packet after detecting collision for a node is 15.
- If after incrementing, the attempts get more than 15 in the count then the packet gets discarded due to excessive collision. However, in case the count for the same is less than 15 then the respective node will prepare to retransmit the data packet over the channel again.
- For this, it will calculate the back-off time and will wait for the completion of that time duration. Once this is done, the node will again go for checking the availability of the channel and whether it is free or not in order to resume the transmission.



CSMA/CD Frame Format

Frame format of IEEE 802.3 CSMA/CD frame

1. **Preamble**: It is seven bytes (56 bits) that provides bit synchronization. It consists of alternating 0s and 1s. The purpose is to provide alert and timing pulse.
2. **Start Frame Delimiter (SFD)**: It is one-byte field with unique pattern: 10 10 1011. It marks the beginning of frame.
3. **Destination Address (DA)**: It is six-byte field that contains physical address of packet's destination.
4. **Source Address (SA)**: It is also a six-byte field and contains the physical address of source or last device to forward the packet (most recent router to receiver).
5. **Length**: This two-byte field specifies the length or number of bytes in data field.
6. **Data**: It can be of 46 to 1500 bytes, depending upon the type of frame and the length of the information field.
7. **Frame Check Sequence (FCS)**: This four-byte field contains CRC for error detection.

Q1. A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including (including the delays in the devices and ignoring the time needed to send a jamming) is 25.6 μs, what is the minimum size of the frame?

Solution:

Propagation delay $T_p = 25.6$ μs

Bandwidth = 10 Mbps

Frame transmission time $T_{fr} = 2 \times T_p = 2 \times 25.6$ μs $= 51.2$ μs

Minimum frame size = Bandwidth x T_{fr} = 10 Mbps x 51.2 μs

= **512 bits = 64 bytes**

Q2. Consider a CSMA/CD network that transmits data at a rate of 100 Mbps over a 1km cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

Solution:

Bandwidth = 100 Mbps

Distance = 1 km

Minimum frame size = 1250 bytes

Minimum frame size = Bandwidth x T_{fr} = 100 Mbps x T_{fr}

$$\therefore 1250 \times 8 = 100 \times 10^6 \times T_{fr}$$

$$\therefore T_{fr} = \frac{1250 \times 8}{10^8} = \mathbf{1 \times 10^{-4} sec}$$

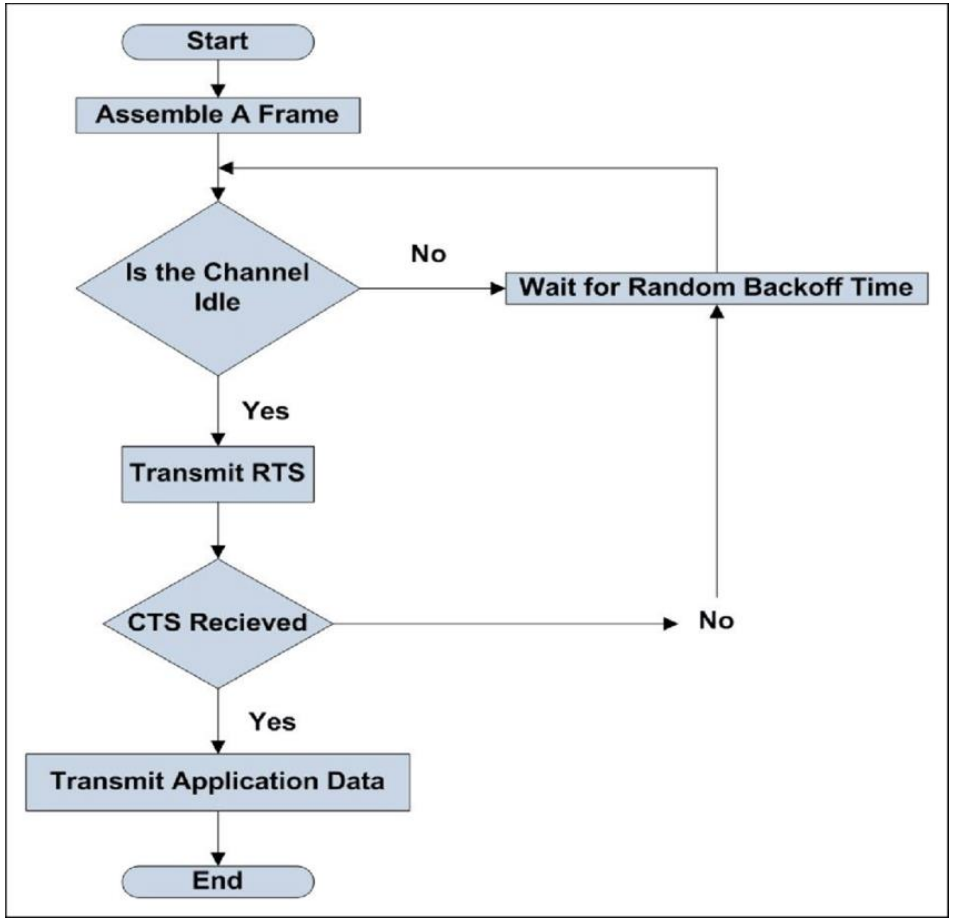
Frame transmission time T_{fr} = 2 x T_p

$$T_p = \frac{T_{fr}}{2} = \frac{1 \times 10^{-4}}{2} = \mathbf{5 \times 10^{-5}\ sec}$$

$$\text{Speed} = \frac{\text{Distance}}{\text{Time}} = \frac{1\ \text{km}}{5 \times 10^{-5}\ \text{sec}} = \mathbf{20000\ km/sec}$$

CSMA/ CA (Carrier Sense Multiple Access with Collison Avoidance)

- CSMA/CA stands for **Carrier Sense Multiple Access** with **Collision Avoidance**.
- It means that it is a network protocol that uses to avoid a collision rather than allowing it to occur, and it does not deal with the recovery of packets after a collision.
- In CSMA/CA, whenever a station wants to send a data frame to a channel, it checks whether it is in use.
- If the shared channel is busy, the station waits until the channel enters idle mode.
- Hence, we can say that it reduces the chances of collisions and makes better use of the medium to send data packets more efficiently.



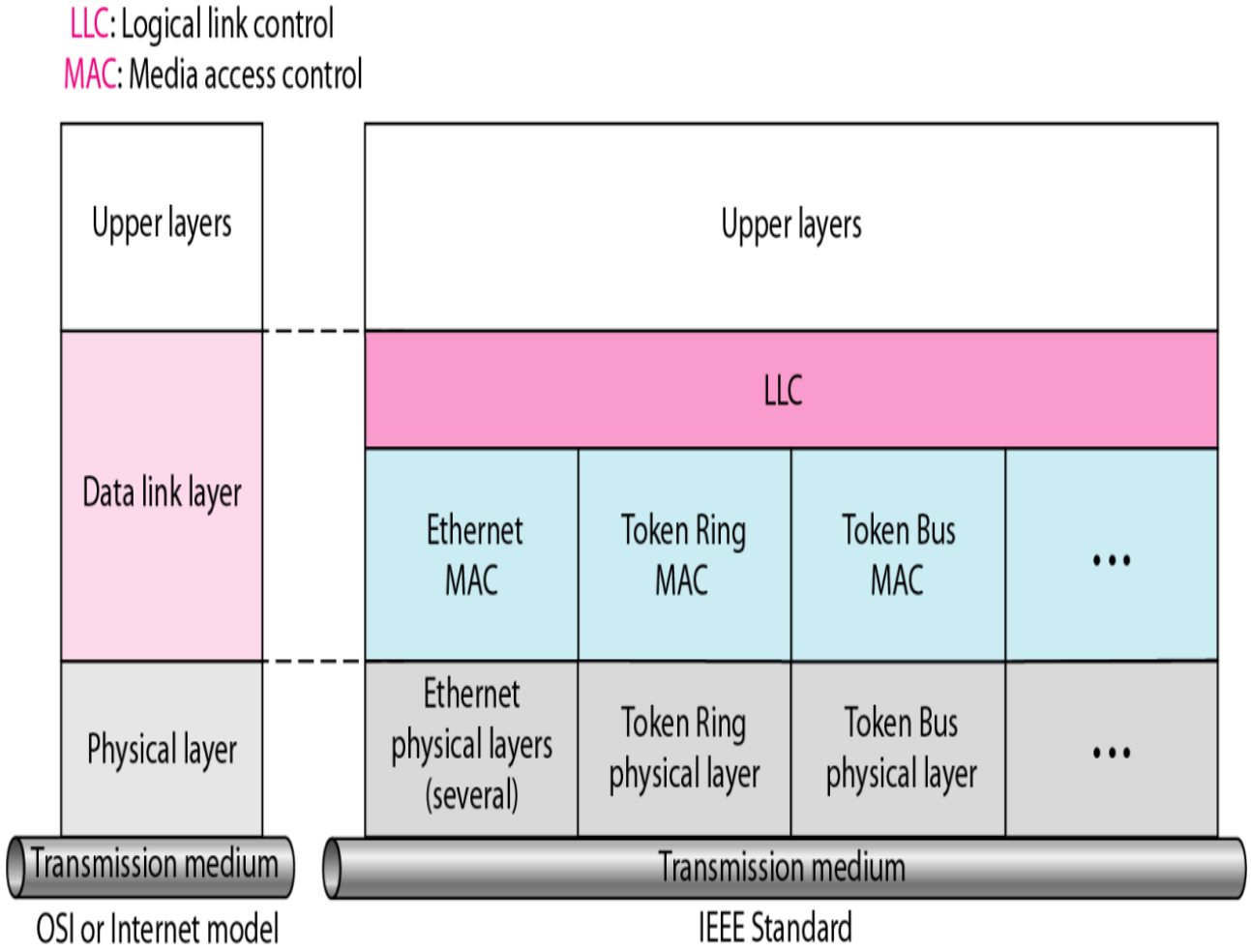
- RTS : Request to Send
- CTS : Clear to Send

CSMA/CD Vs CSMA/CA

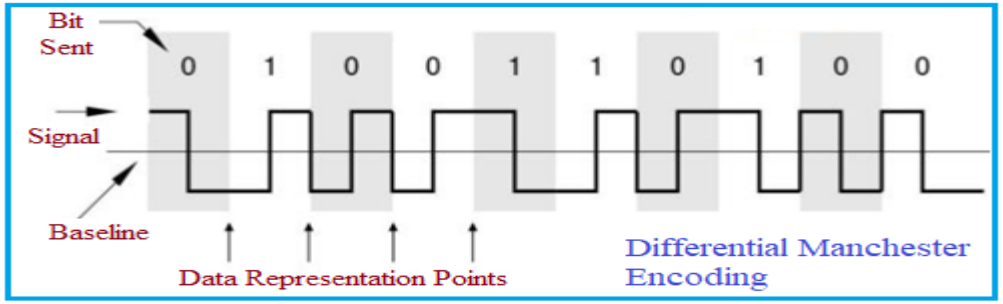
CSMA/CD	**CSMA/CA**
It is the CSMA type used to detect a collision on a shared channel.	It is a form of CSMA that is used to avoid collisions on a shared channel.
The collision detection methodology is what it is.	It is a collision avoidance protocol.
CSMA/CD found in 802.3 Ethernet network cables.	CSMA/CA is used in the Ethernet 802.11 network.
It is compatible with wired networks.	It is compatible with wireless networks.
This is effective after a network's collision detection.	This is useful prior to collision detection on a network.
When a data packet clashes on a shared channel, the data frame is resent.	The CSMA/CA, on the other hand, waits until the channel is congested and does not recover after a collision.
It cuts down on recovery time.	It reduces the possibility of a collision.
When compared to CSMA, CSMA/CD has a higher efficiency.	The efficiency of CSMA/CA is comparable to that of CSMA.
It is more widely used than the CSMA/CA protocol.	It is less well-known than CSMA/CD.

Wired LANs (Ethernet)

- **A local area network (LAN) is a computer network** that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet.
- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 does not seek to replace any part of the OSI or the Internet model.
- The relationship of the 802 Standard to the traditional OSI model is shown in the below figure
- The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.
- In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. **Framing is handled in both the LLC sublayer and the MAC sublayer**.
- The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer, which provides **different protocols for different LANs**.



Ethernet 802.3



- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet generally uses Bus Topology.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.
- Manchester Encoding Technique is used in Ethernet where 0 is expressed by a high-to-low transition, a 1 by the low-to-high transition and Baud rate = 2 x Bit rate.
- Ethernet LANs consist of network nodes and interconnecting media or link.
- The network nodes can be of two types: Data Terminal Equipment (DTE) and Data Communication Equipment (DCE).

DTE Vs DCE

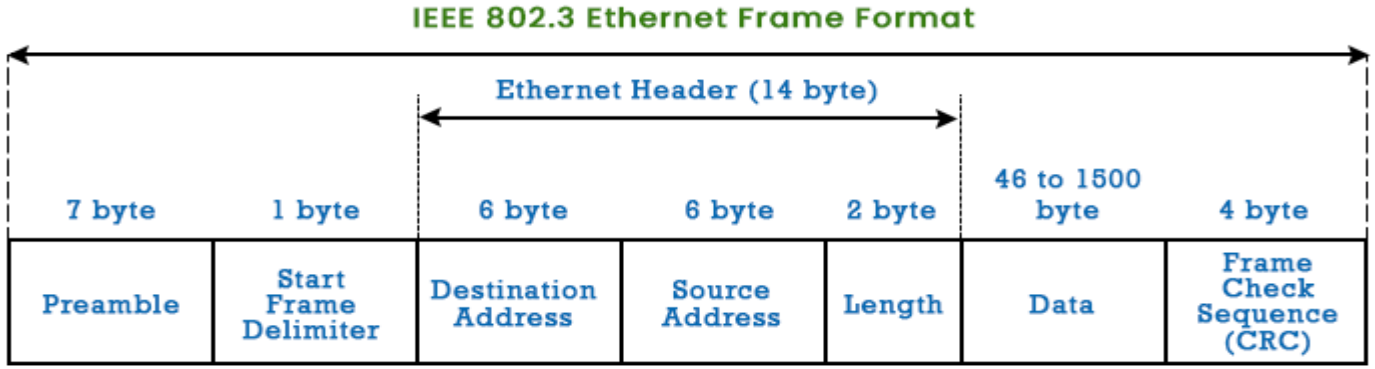
Data Terminal Equipment (DTE):

- Generally, DTEs are the end devices that convert the user information into signals or reconvert the received signals.
- DTEs devices are: personal computers, workstations, file servers or print servers also referred to as end stations.
- These devices are either the source or the destination of data frames.

Data Communication Equipment (DCE):

- DCEs are the intermediate network devices that receive and forward frames across the network.
- They may be either standalone devices such as repeaters, network switches, routers or maybe communications interface units such as interface cards and modems.
- The DCE performs functions such as signal conversion, coding and may be a part of the DTE or intermediate equipment.

IEEE 802.3 Frame Format



- **Preamble**: It is the starting field that provides alert and timing pulse for transmission. It is of 7 bytes. It consists of alternating 0s and 1s.
- **Start of Frame Delimiter**: It is a 1-byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones (**10101011**)
- **Destination Address**: It is a 6-byte field containing physical address of destination stations.
- **Source Address**: It is a 6-byte field containing the physical address of the sending station.
- **Length**: Length is a 2-byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between 0 to 65534, but length cannot be larger than 1500 because of some own limitations of Ethernet.
- **Data**: This is a variable sized field that carries the data from the upper layers. The maximum size of data field is 1500 bytes. **Padding of 0's is done** to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC is 4-byte field. CRC stands for cyclic redundancy check. It contains the error detection information.

Addressing in Ethernet

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC).
- The NIC fits inside the station and provides the station with a 6-byte physical address.
- As shown in Figure above, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.
- **Unicast, Multicast, and Broadcast Addresses**
- A source address is always a unicast address as the frame comes from only one station.
- The destination address, however, can be unicast, multicast, or broadcast.
- Figure below shows how to distinguish a unicast address from a multicast address.
- If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.
- The broadcast destination address is a special case of the multicast address in which all bits are 1s.

Q. Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A
b. 47:20:1B:2E:08:EE
c. FF:FF:FF:FF:FF:FF

Solution:

To find the type of the address, we need to look at the second hexadecimal digit from the left.

- If it is even, the address is unicast.
- If it is odd, the address is multicast.
- If all digits are F's, the address is broadcast.

Therefore, we have the following:

a. This is a unicast address because A in binary is 1010.
b. This is a multicast address because 7 in binary is 0111.
c. This is a broadcast address because all digits are F's.

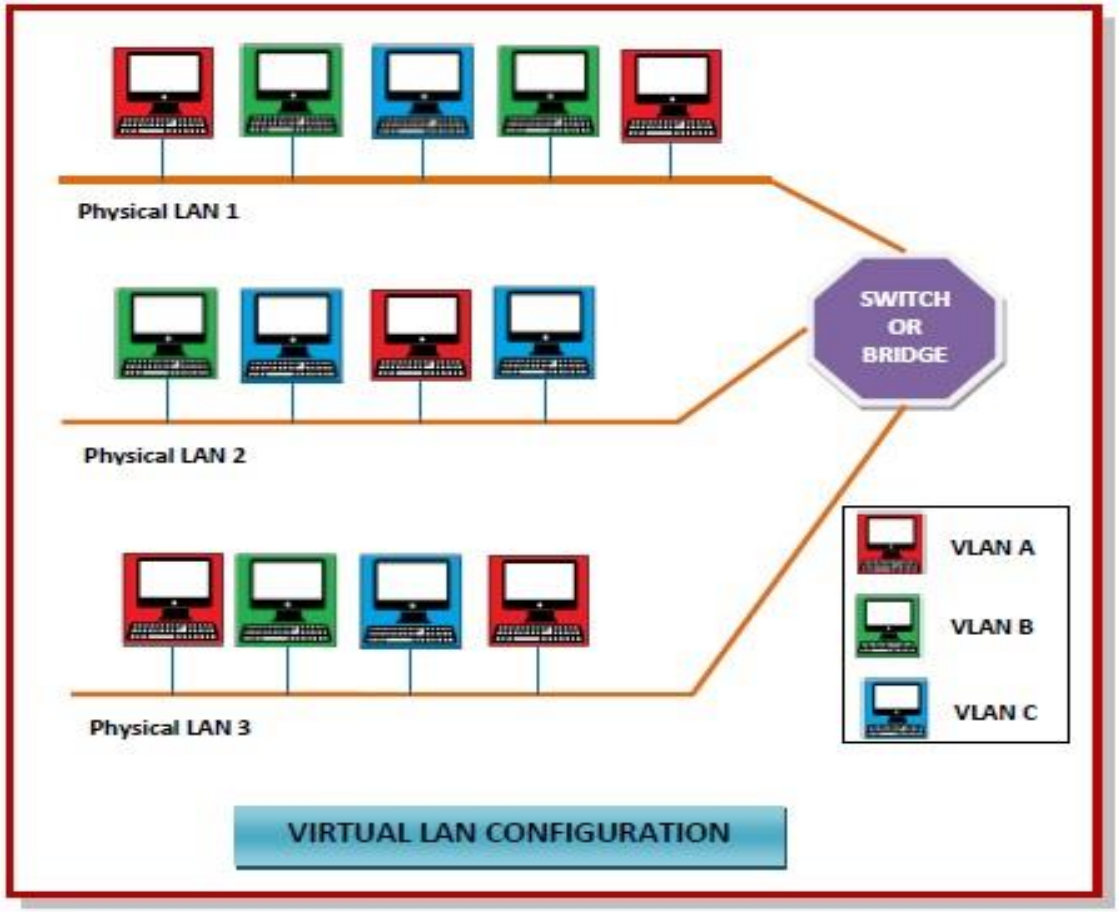
Ethernet Standards

- Ethernet is defined in a series of IEEE 802.3 standards.
- These standards define the physical layer and data link specifications for Ethernet.
- The most important 802.3 standards are:

Original IEEE	IEEE Shorthand Name	Informal Name(s)	Speed	Typical Cabling
802.3i	10BASE-T	Ethernet	10 Mbps	UTP
802.3u	100BASE-T	Fast Ethernet (Fast E)	100 Mbps	UTP
802.3z	1000BASE-X	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	Fiber
802.3ab	1000BASE-T	Gigabit Ethernet (Gig E, GbE)	1000 Mbps	UTP
802.3ae	10GBASE-X	10 GbE	10 Gbps	Fiber
802.3an	10GBASE-T	10 GbE	10 Gbps	UTP
802.3ba	40GBASE-X	40GbE (40 GigE)	40 Gbps	Fiber
802.3ba	100GBASE-X	100GbE (100 GigE)	100 Gbps	Fiber

Virtual LAN

- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.
- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprises of a subset of ports on single or multiple switches or bridges.
- This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

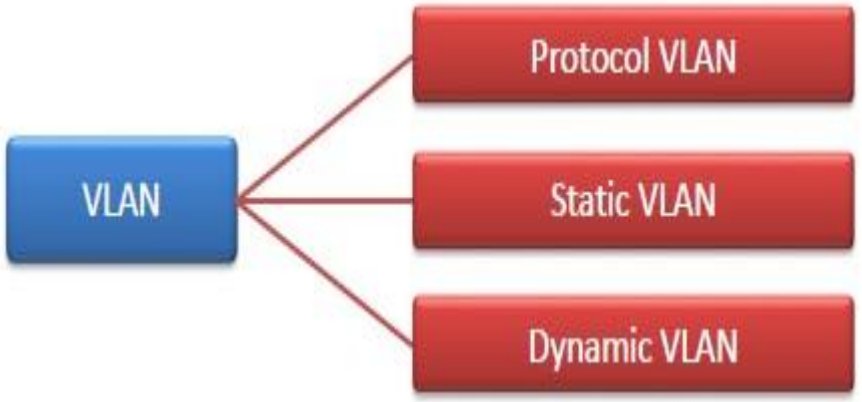


Features of VLANs

- A VLAN forms a sub-network grouping together devices on separate physical LANs.
- VLANs help the network manager segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e., Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- VLANs help large organizations to re-partition devices aiming for improved traffic management.
- VLANs also provide better security management allowing the partitioning of devices according to their security criteria and also ensuring a higher degree of control of connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections.

Types of VLANs

- **Protocol VLAN** – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards, or discards frames that come to it, based on the traffic protocol.
- **Port-based VLAN** – This is also called static VLAN. Here, the network administrator assigns the ports on the switch/bridge to form a virtual network.
- **Dynamic VLAN** – Here, the network administrator simply defines network membership according to device characteristics.



Difference between LAN and VLAN

LAN	VLAN
LAN stands for Local Area Network	VLAN stands for Virtual Local Area Network
A local area network (LAN) is a collection of computer and peripheral devices linked in a specific geographic area.	A VLAN is a custom network that is built from one or more local area networks.
The network packet is advertised to each and every device in a LAN.	The network packet is only transmitted to a specific broadcast domain in a VLAN.
The LAN has a high latency.	VLAN has a lower latency.
It employs a ring and the FDDI (Fiber Distributed Data Interface) protocol.	It employs Internet Service Provider (ISP) and VLAN Trunking Protocol (VTP) as protocols.
Overall cost in LAN is generally high as compared to VLAN	Overall cost is less as compared to LAN