UNIT NO. 2 DATA LINK LAYER

2.1 Introduction to Data Link Layer

The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decode and organizing the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

Sub-layers of the Data Link Layer
The data link layer is further divided into two sub-layers, which are as follows:

Logical Link Control (LLC)
This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC)
MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access.

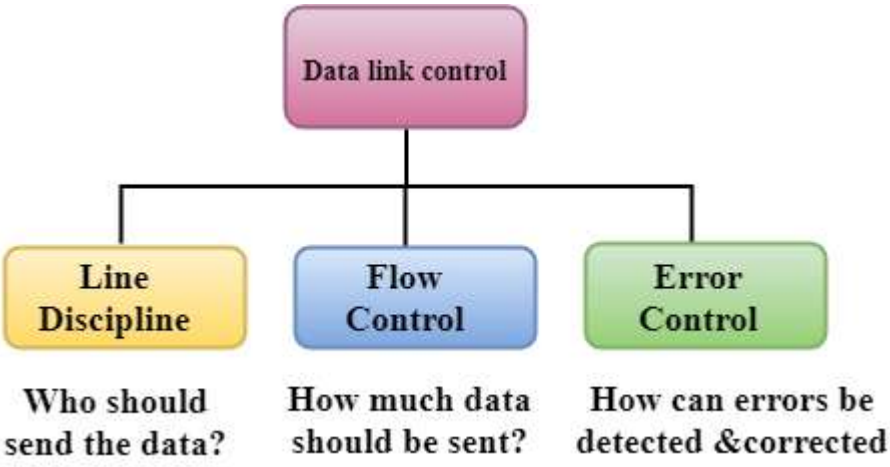
2.2 DLC Services

Data Link Controls

Data Link Control is the service provided by the Data Link Layer to provide reliable data transfer over the physical medium. For example, In the half-duplex transmission mode, one device can only transmit the data at a time. If both the devices at the end of the links transmit the data simultaneously, they will collide and leads to the loss of the information. The Data link layer provides the coordination among the devices so that no collision occurs.

The Data link layer provides three functions:

- Line discipline
- Flow Control
- Error Control



Line Discipline

- Line Discipline is a functionality of the Data link layer that provides the coordination among the link systems. It determines which device can send, and when it can send the data.

Line Discipline can be achieved in two ways:

- ENQ/ACK
- Poll/select

END/ACK

END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.

END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

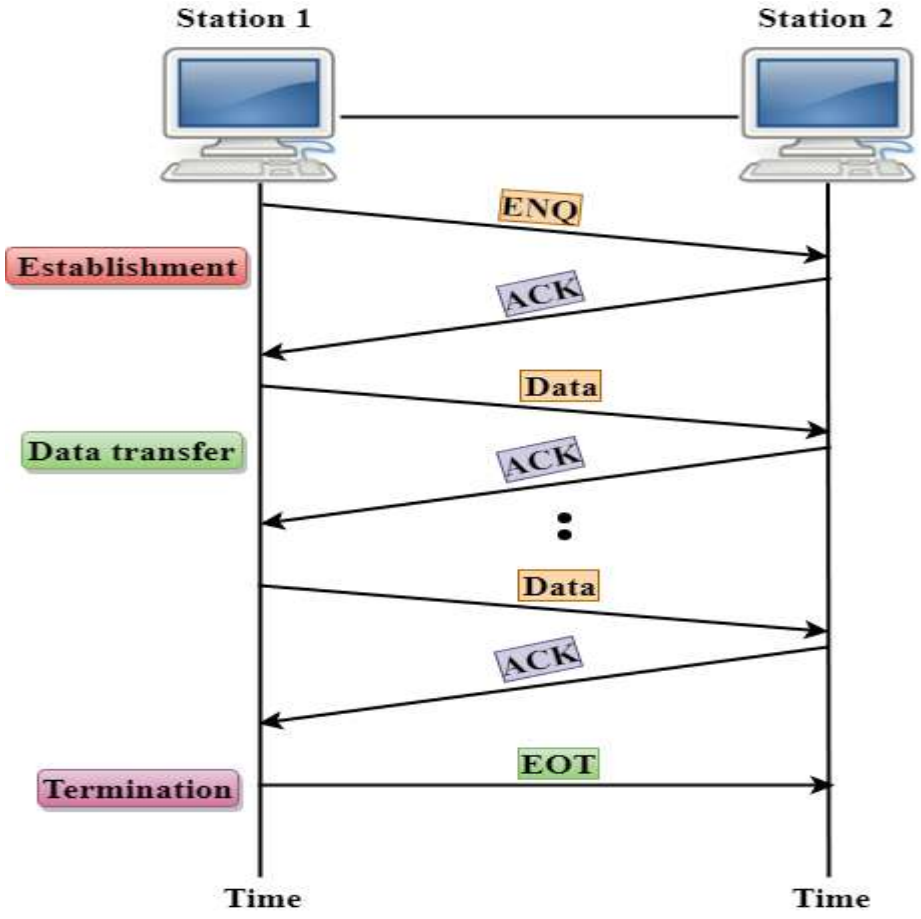
Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.

The receiver responses either with the positive acknowledgement (ACK) or with the negative acknowledgement (NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

- If the response to the ENQ is positive, the sender will transmit its data, and once all of its data has been transmitted, the device finishes its transmission with an EOT (END-of-Transmission) frame.
- If the response to the ENQ is negative, then the sender disconnects and restarts the transmission at another time.
- If the response is neither negative nor positive, the sender assumes that the ENQ frame was lost during the transmission and makes three attempts to establish a link before giving up.



Poll/Select

The Poll/Select method of line discipline works with those topologies where one device is designated as a primary station, and other devices are secondary stations.

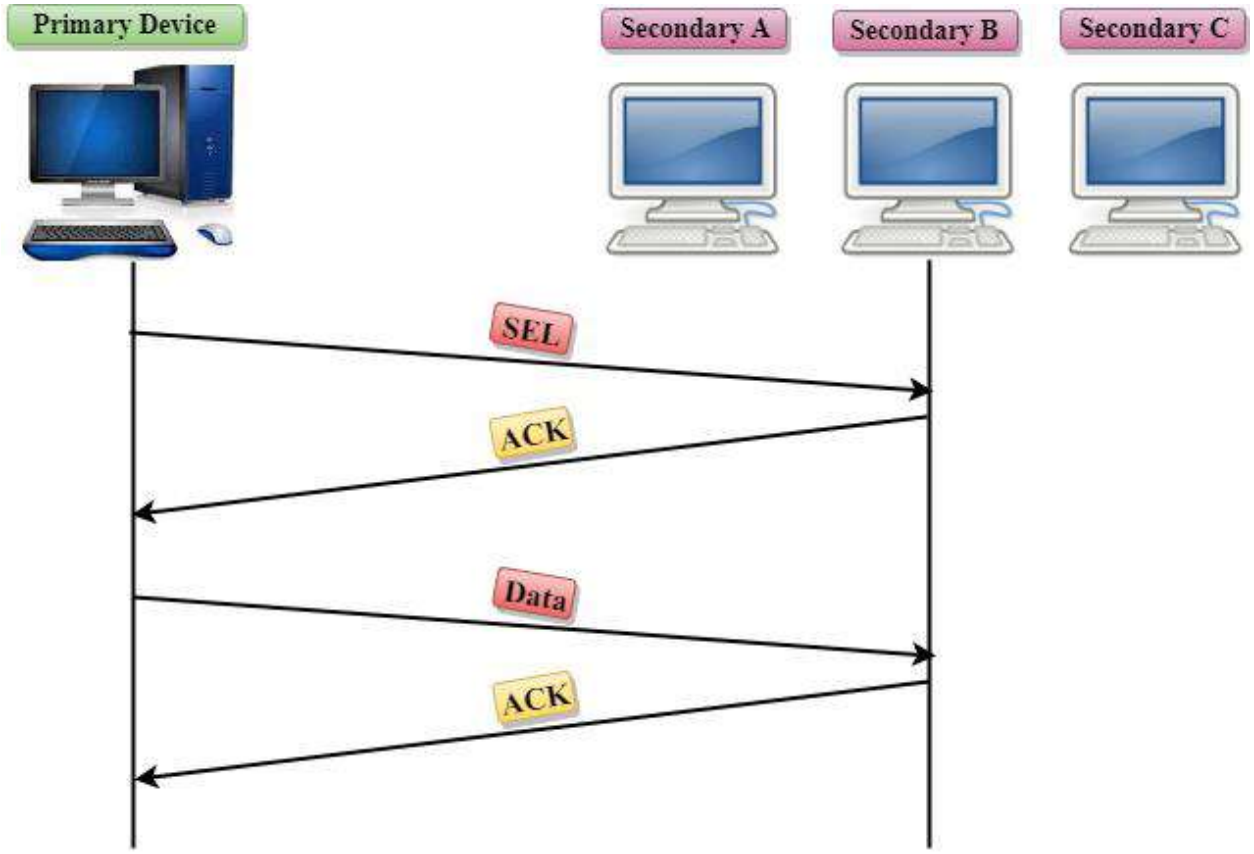
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.

- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.
- The primary device determines which device is allowed to use the communication channel. Therefore, we can say that it is an initiator of the session.
- If the primary device wants to receive the data from the secondary device, it asks the secondary device that they anything to send, this process is known as polling.
- If the primary device wants to send some data to the secondary device, then it tells the target secondary to get ready to receive the data, this process is known as selecting.

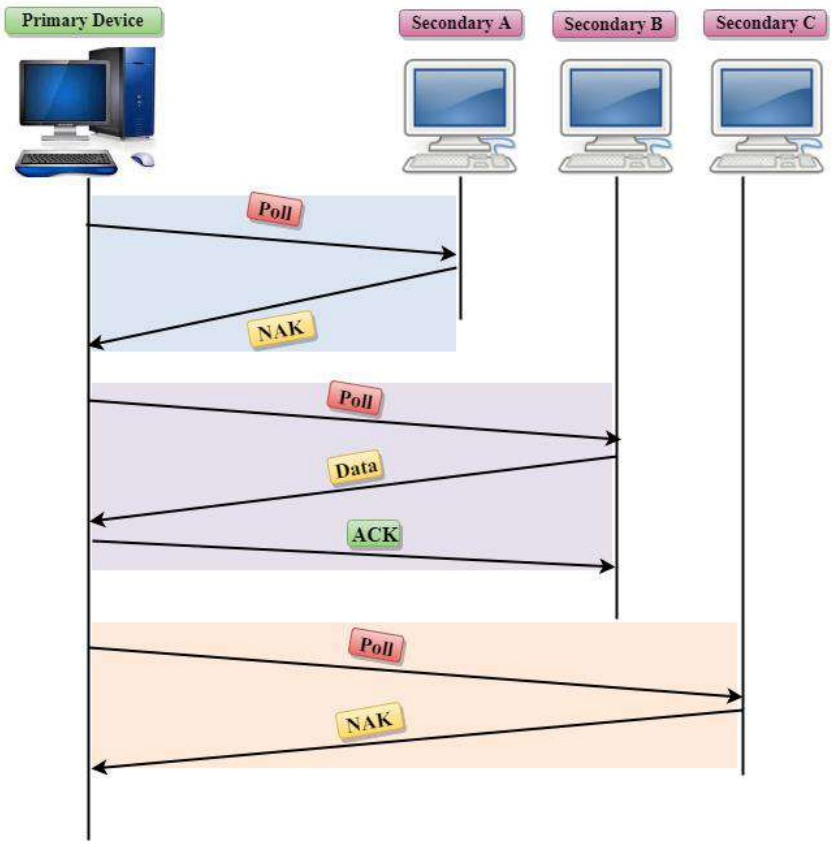
Select

- The select mode is used when the primary device has something to send.
- When the primary device wants to send some data, then it alerts the secondary device for the upcoming transmission by transmitting a Select (SEL) frame, one field of the frame includes the address of the intended secondary device.
- When the secondary device receives the SEL frame, it sends an acknowledgement that indicates the secondary ready status.
- If the secondary device is ready to accept the data, then the primary device sends two or more data frames to the intended secondary device. Once the data has been transmitted, the secondary sends an acknowledgement specifies that the data has been received.



Poll

- The Poll mode is used when the primary device wants to receive some data from the secondary device.
- When a primary device wants to receive the data, then it asks each device whether it has anything to send.
- Firstly, the primary asks (poll) the first secondary device, if it responds with the NACK (Negative Acknowledgement) means that it has nothing to send. Now, it approaches the second secondary device, it responds with the ACK means that it has the data to send. The secondary device can send more than one frame one after another or sometimes it may be required to send ACK before sending each one, depending on the type of the protocol being used.



Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver.
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.

- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantage of Stop-and-wait

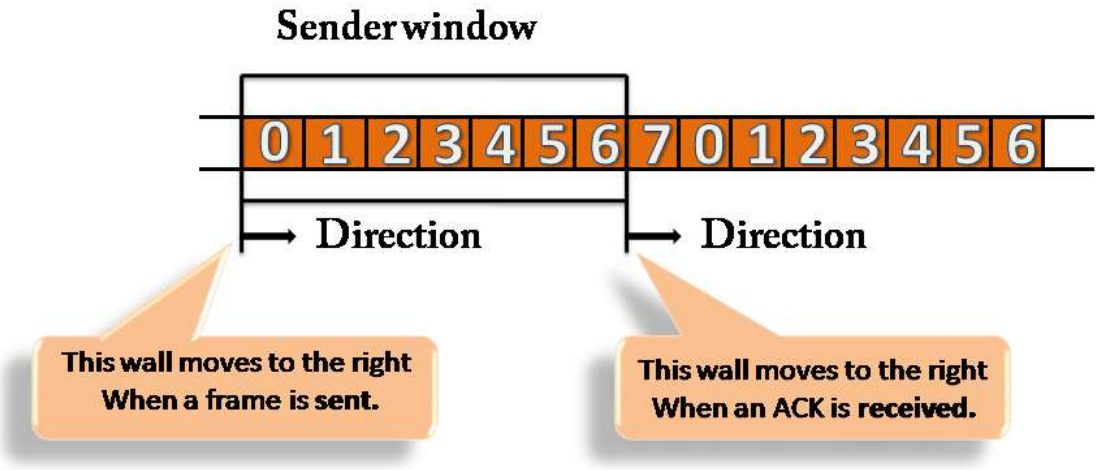
Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement.
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently.
- A single ACK acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement.
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window

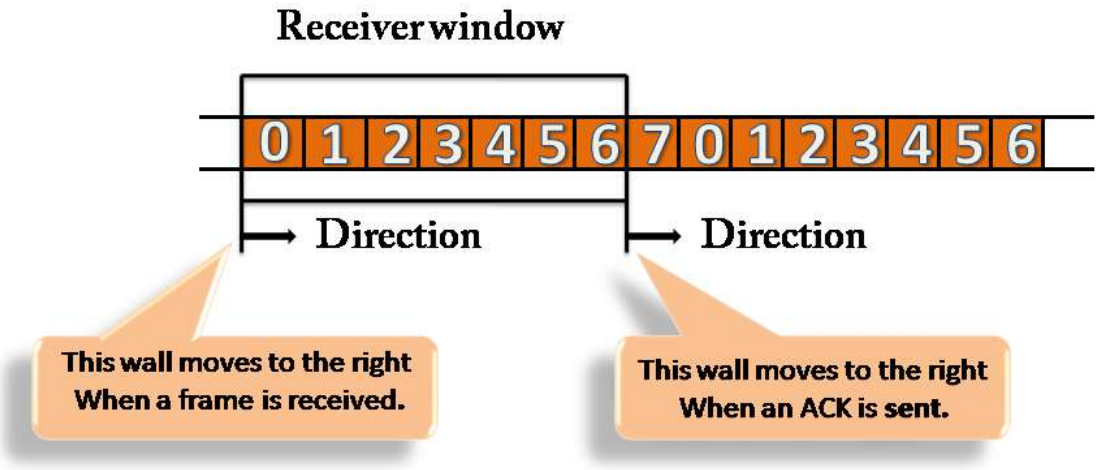
- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.
- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2).



Receiver Window

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.

- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1. In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent.



Error Control

Error Control is a technique of error detection and retransmission.

Categories of Error Control:

Stop-and-wait ARQ

Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames.

This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame.

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0

frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.

- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

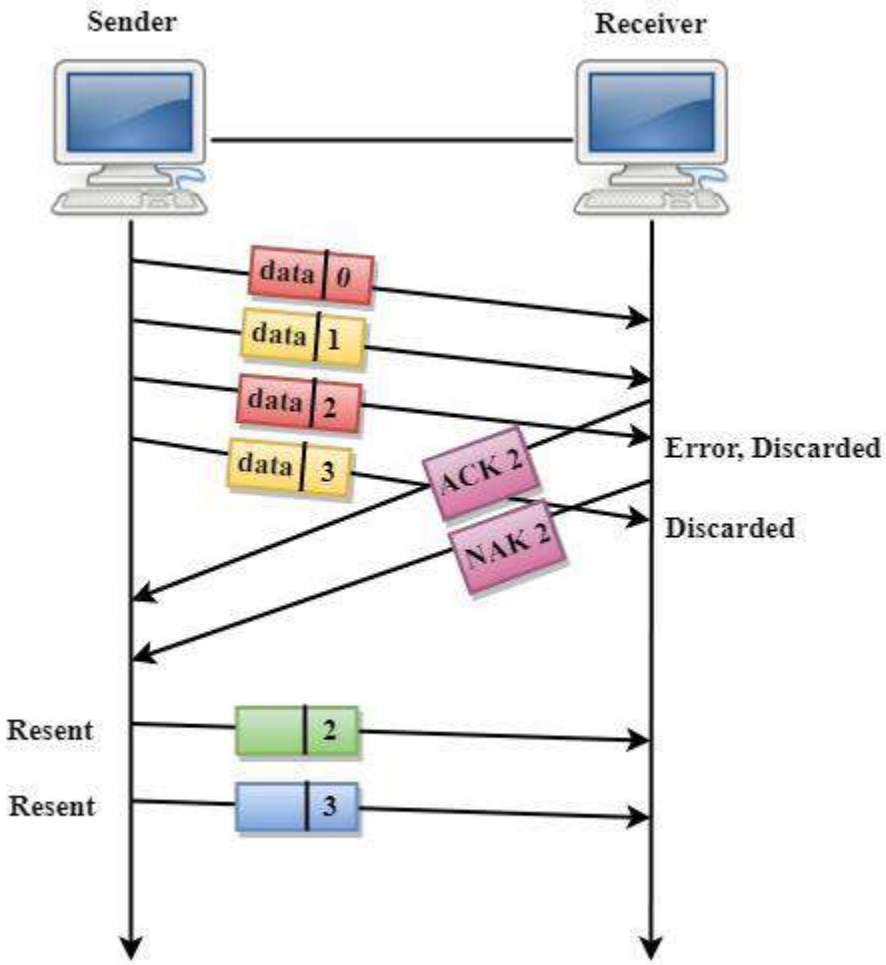
- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame.
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used.

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK.

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame.



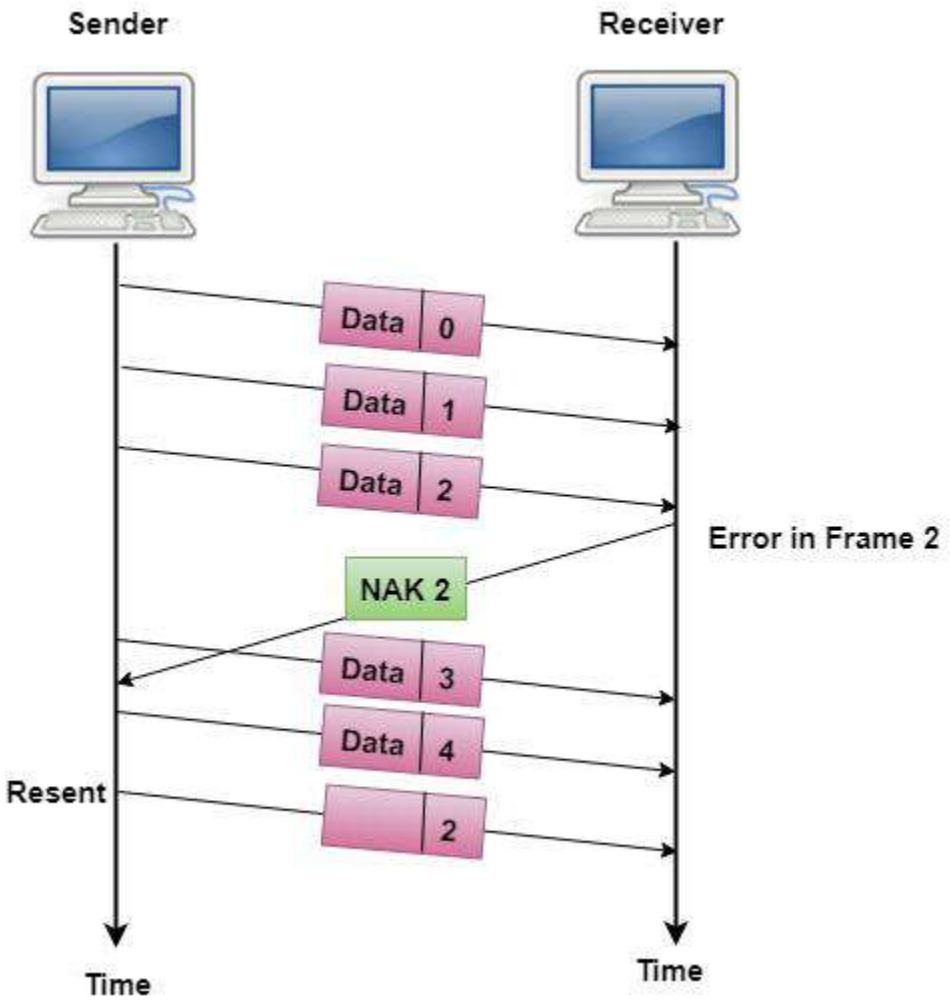
In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3.

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.

- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

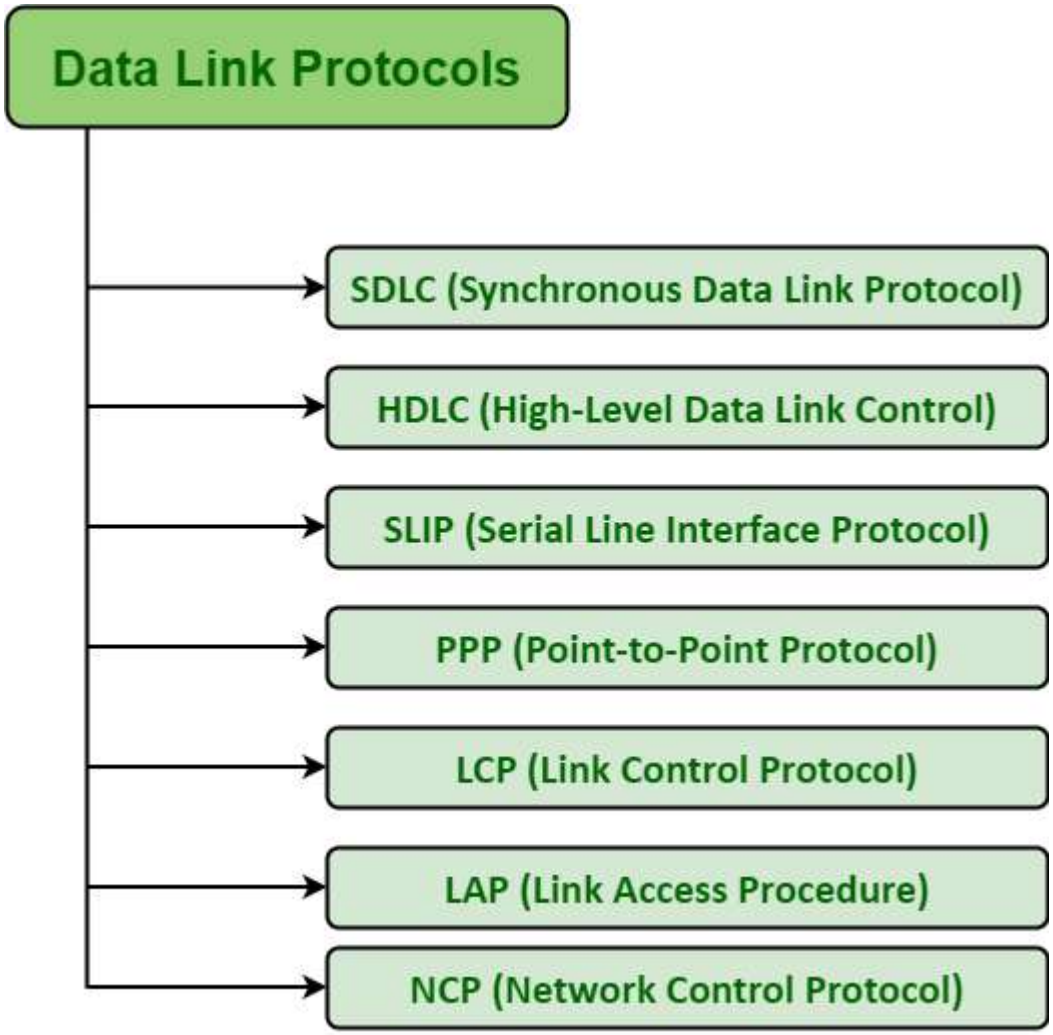
Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.
- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.



2.3 DLL Protocols

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the Open System Interconnections (OSI) Model. **Some Common Data Link Protocols:** There are various data link protocols that are required for Wide Area Network (WAN) and modem connections. Logical Link Control (LLC) is a data link protocol of Local Area Network (LAN). Some of data link protocols are given below:



SDLC:

SDLC stands for synchronous data link control protocol, is a communication protocol of a computer. It is usually used to carry system network architecture traffic. synchronous data link protocol connects all the remote devices to the mainframe computer at the Central location. This connection is done in two formats, point to point format i.e. one to one connection, and point to multipoint format, i.e. one to many connections. SDLC support one to many connections even in case of error detection or error recovery. SDLC ensures that all the received data units are correct and flow is right from one network point to the next network point.

HDLC:

HDLC stands for High-level data link control protocol, is a bit-orientated code transparent synchronous protocol developed by ISO (International organization for

standardization) in1979. It provides both connection-orientated and connectionless services. HDLC protocol contains various wide-area protocols. It is based on the SDLC protocol that supports both point-to-point and multipoint communication. HDLC frames are transferred over synchronous or asynchronous serial communication links. HDLC uses various modes such as normal response mode, asynchronous response mode, asynchronous balanced mode. Normal response mode is used to share the secondary to primary link without contention. asynchronous response mode is used for full-duplex links. asynchronous balanced mode, support combined terminal which can act as both primary and secondary

SLIP:

SLIP stands for Serial line interface protocol which is used to add framing byte at the end of the IP Packet. SLIP is a data link layer protocol That transforms the IP packets among ISP (Internet Service Providers) and home user over dial-up links. SLIp is designed to work with ports and router connections. SLIP does not provide error detection, being reliant on upper-layer protocols for this. Therefore, SLIP on its own is not satisfactory over an error-prone dial-up connection.

PPP:

PPP stands for Point to point protocol. PPP is a data link layer protocol that provides the same services as the Serial line interface protocol. It is a robust protocol that transfers the other types of pockets also with the IP packets. It provides two protocols – LCP and NCP, that we will discuss in the next section. Point to point protocol uses framing methods that describe the frames. Point to point protocol is also called character orientated protocol which is used to detect errors. PPC provides Connection authentication, data compression, encryption, and transmission. It is used over various networks such as phone lines, cellular telephones, serial cables, trunk lines, ISDNs, Specialized radio links, etc.

LCP:

LCP stands for Link control protocol, is a part of point-to-point control protocol. LCP packets determine the standards of data transmission. LCP protocol is used to determine the identity of the linked devices, if the device is correct it accepts it otherwise it rejects the device. It also determines whether the size of the packet is accepted or not. If requirements exceed the parameters, then the link control protocol terminates that link.

LAP:

LAP stands for Link access procedure is a data link layer protocol that is used for framing and transfer the data across point-to-point links. There are three types of Link access procedure – LAPB (Link Access procedure balanced), LAPF (Link Access Procedure Frame-Mode Bearer Services), and LAPD (Link Access Procedure D-Channel. LAP was originally derived from HDLC (High-Level Data Link Control), but was later updated and renamed LAPB (LAP Balanced).

NCP:

NCP stands for Network control protocol, is a part of the point-to-point protocol. The network control protocol is used to negotiate the parameter and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. IPCP (Internet Protocol control protocol), DNCP (DECnet Phase IV Control Protocol), OSINLCP (OSI Network Layer Control Protocol), IPXCP (Internetwork Packet Exchange Control Protocol), NBFCP (NetBIOS Frames Control Protocol), IPV6CP (IPv6 Control Protocol) are some of the NCPs.

2.4 High-level Data Link Control (HDLC)

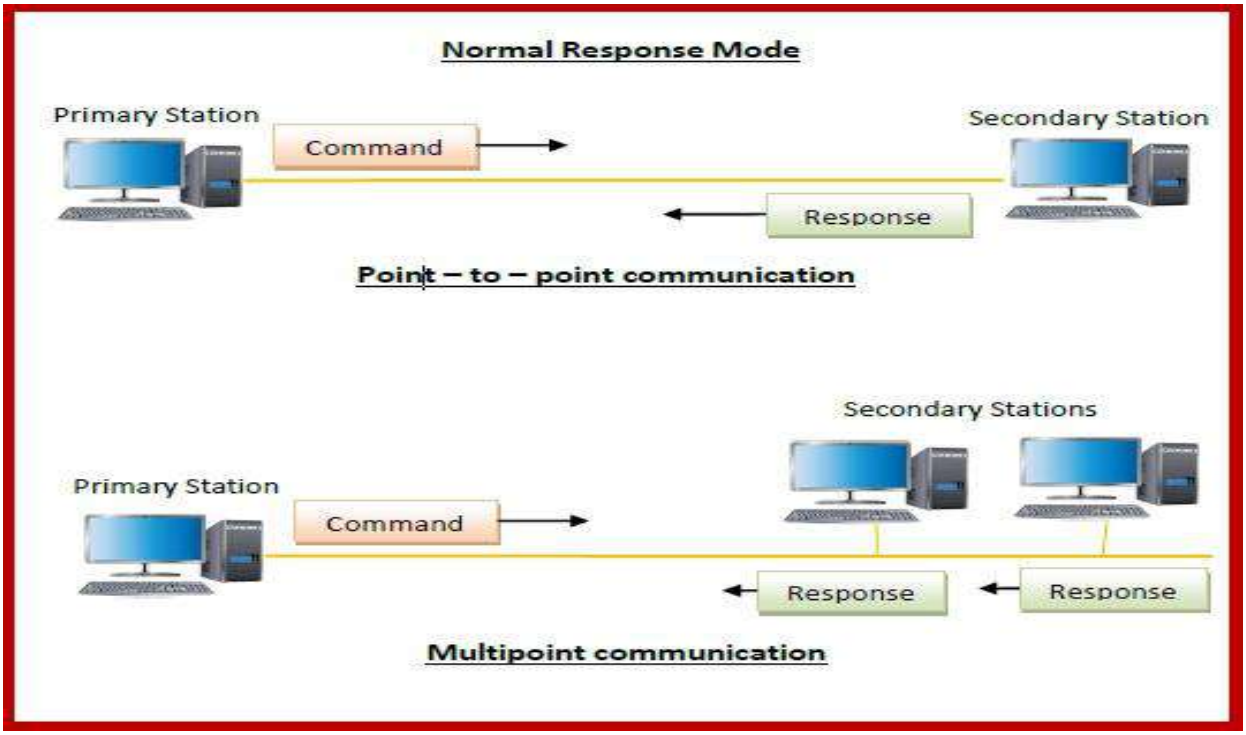
High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful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

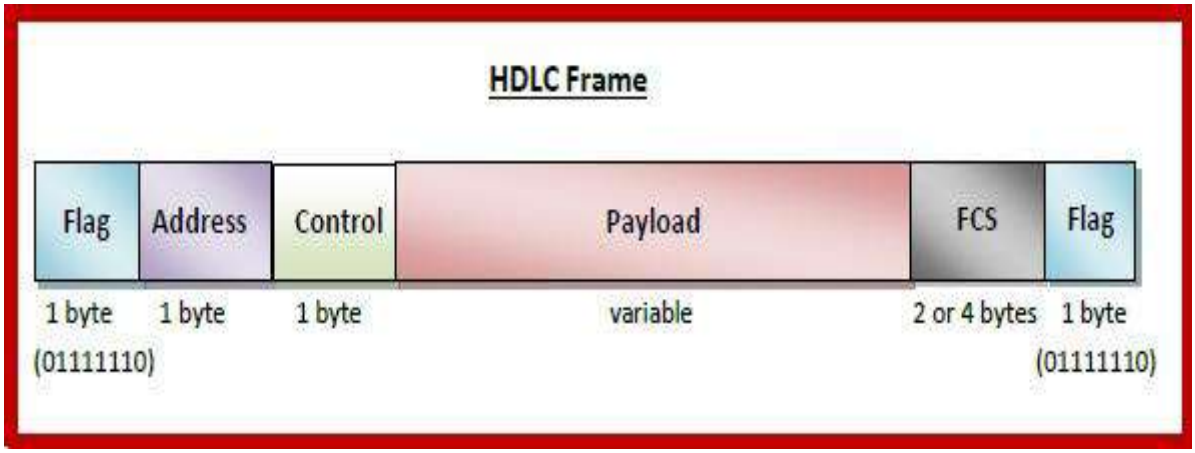


HDLC Frame

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.



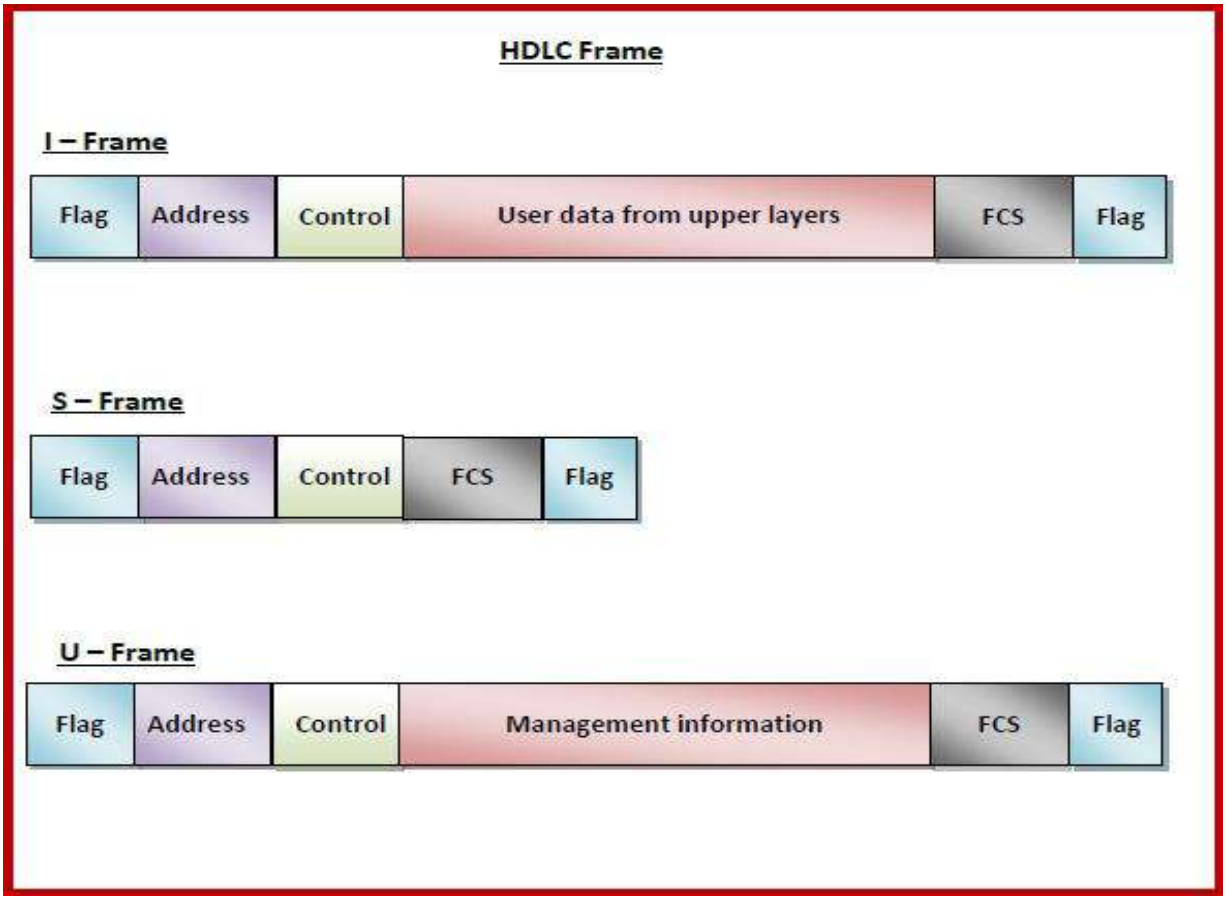
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.

- **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 bit 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 bit of control field of U-frame is 11.



2.5 PPP Protocol

The PPP stands for Point-to-Point protocol. It is the most commonly used protocol for point-to-point access. Suppose the user wants to access the internet from the home, the PPP protocol will be used.

It is a data link layer protocol that resides in the layer 2 of the OSI model. It is used to encapsulate the layer 3 protocols and all the information available in the payload in order to be transmitted across the serial links. The PPP protocol can be used on synchronous link like ISDN as well as asynchronous link like dial-up. It is mainly used for the communication between the two devices.

It can be used over many types of physical networks such as serial cable, phone line, trunk line, cellular telephone, fiber optic links such as SONET. As the data link layer protocol is used to identify from where the transmission starts and ends, so ISP (Internet Service Provider) use the PPP protocol to provide the dial-up access to the internet.

- It defines the format of frames through which the transmission occurs.

- It defines the link establishment process. If user establishes a link with a server, then "how this link establishes" is done by the PPP protocol.
- It defines data exchange process, i.e., how data will be exchanged, the rate of the exchange.
- The main feature of the PPP protocol is the encapsulation. It defines how network layer data and information in the payload are encapsulated in the data link frame.
- It defines the authentication process between the two devices. The authentication between the two devices, handshaking and how the password will be exchanged between two devices are decided by the PPP protocol.

Services Not provided by the PPP protocol

- It does not support flow control mechanism.
- It has a very simple error control mechanism.
- As PPP provides point-to-point communication, so it lacks addressing mechanism to handle frames in multipoint configuration.

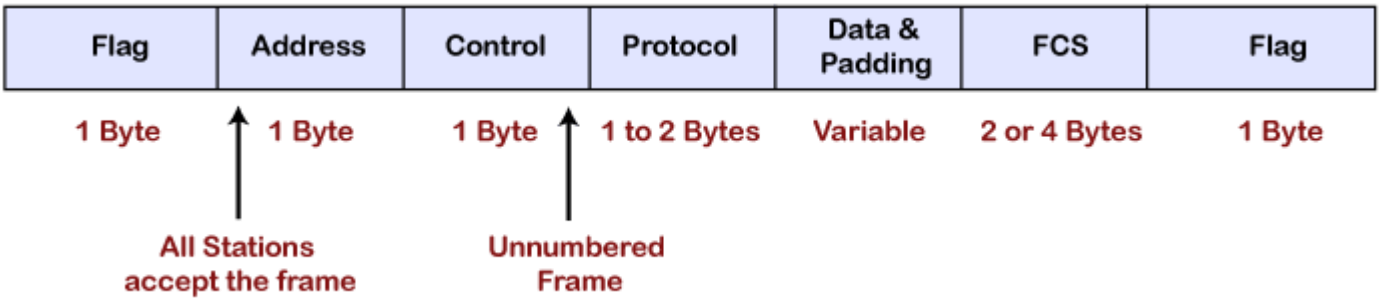
It is a byte-oriented protocol as it provides the frames as a collection of bytes or characters. It is a WAN (Wide Area Network) protocol as it runs over the internet link which means between two routers, internet is widely used.

PPP has two main uses which are given below:

- It is widely used in broadband communications having heavy loads and high speed. For example, an internet operates on heavy load and high speed.
- It is used to transmit the multiprotocol data between the two connected (point-to-point) computers. It is mainly used in point-to-point devices, for example, routers are point-to-point devices where PPP protocol is widely used as it is a WAN protocol not a simple LAN ethernet protocol.

Frame format of PPP protocol

The frame format of PPP protocol contains the following fields:



- **Flag:** The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.
- **Address:** It is a 1-byte field that contains the constant value which is 11111111. These 8 ones represent a broadcast message.
- **Control:** It is a 1-byte field which is set through the constant value, i.e., 11000000. It is not a required field as PPP does not support the flow control and a very limited error control mechanism. The control field is a mandatory field where protocol supports flow and error control mechanism.
- **Protocol:** It is a 1 or 2 bytes field that defines what is to be carried in the data field. The data can be a user data or other information.
- **Payload:** The payload field carries either user data or other information. The maximum length of the payload field is 1500 bytes.
- **Checksum:** It is a 16-bit field which is generally used for error detection.

2.6 MAC (Media Access Control)

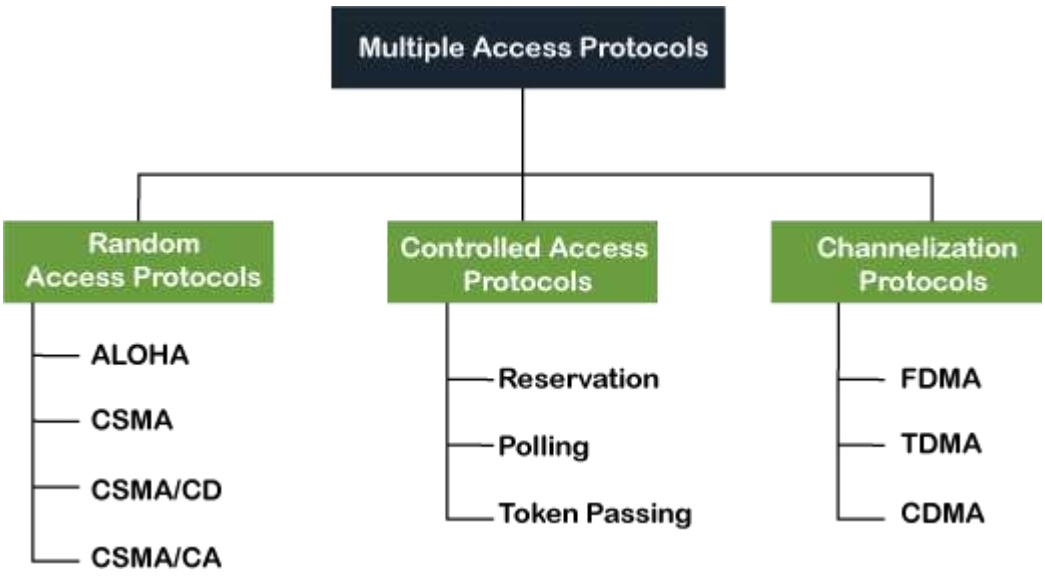
What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmit the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start

answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station or any station control. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

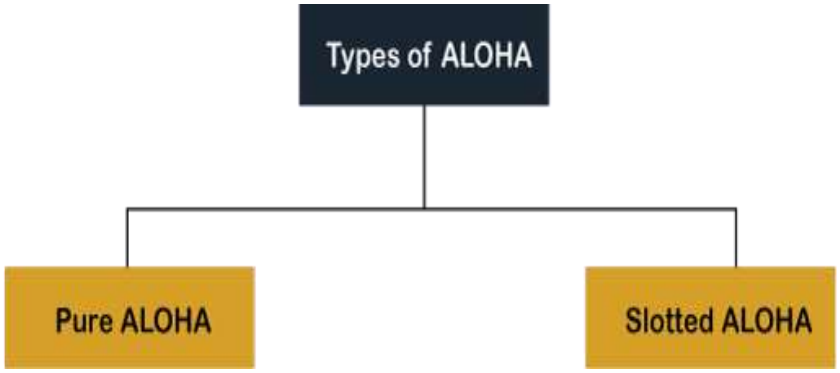
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

1. ALOHA(Advocates OF Linux Open Source HawaiiAssociation) Random Access Protocol

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

Aloha Rules

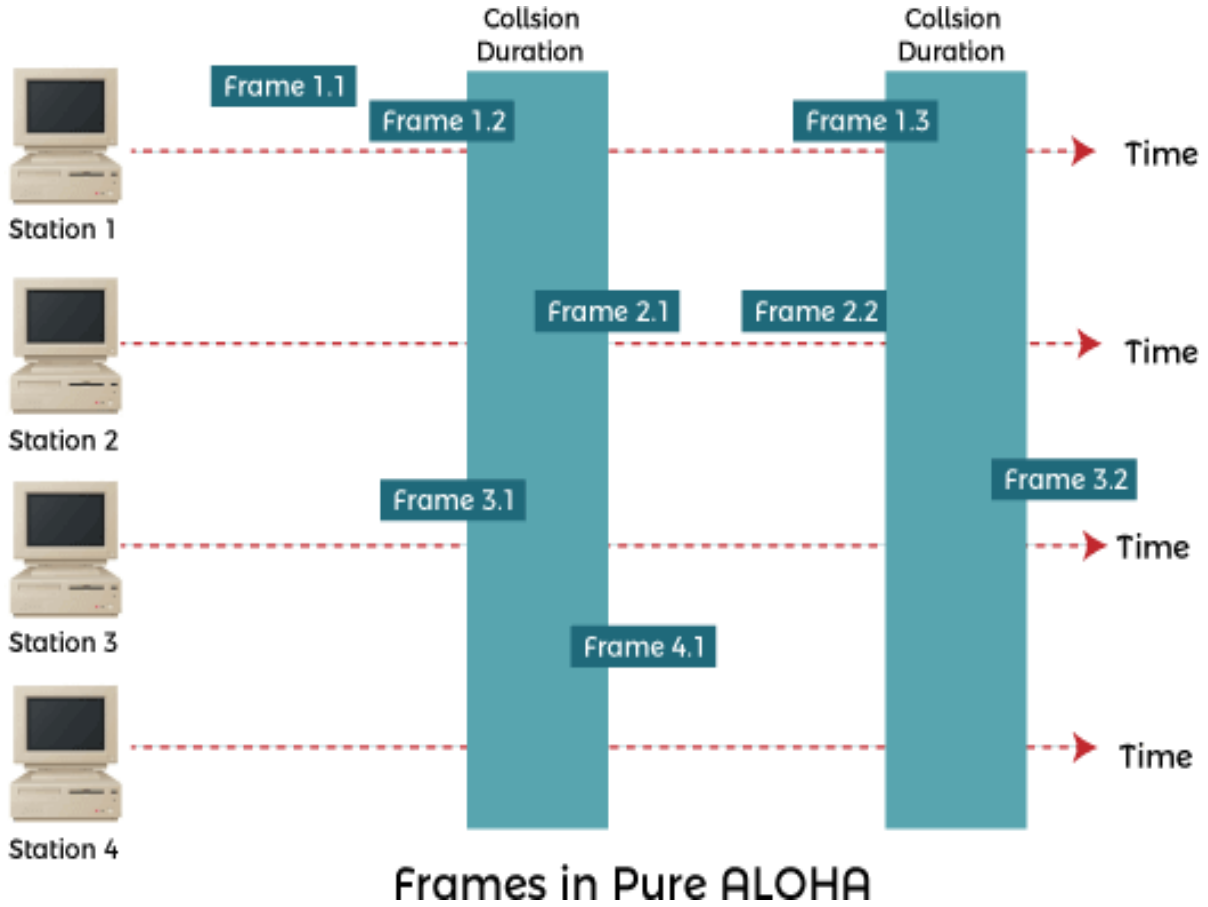
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires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



Pure Aloha

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

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



Frames in Pure ALOHA

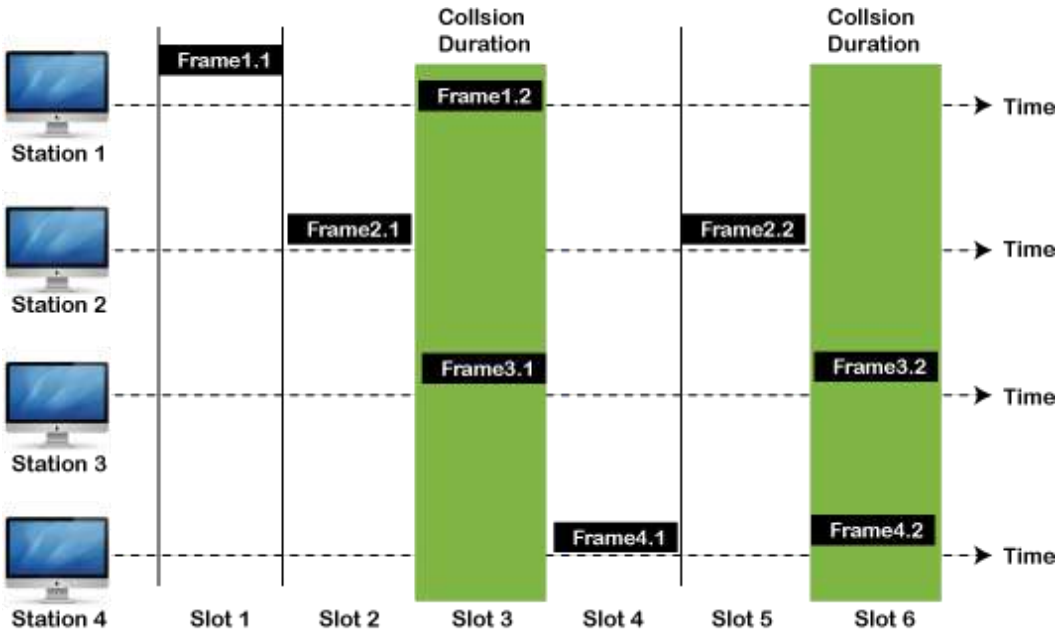
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide

because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

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

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



Frames in Slotted ALOHA

What is carrier sense multiple accessprotocols?

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. In others words, CSMA is based on the principle "sense before transmit" or "listen before talk".

Carrier Sense Multiple Access (CSMA) Protocols

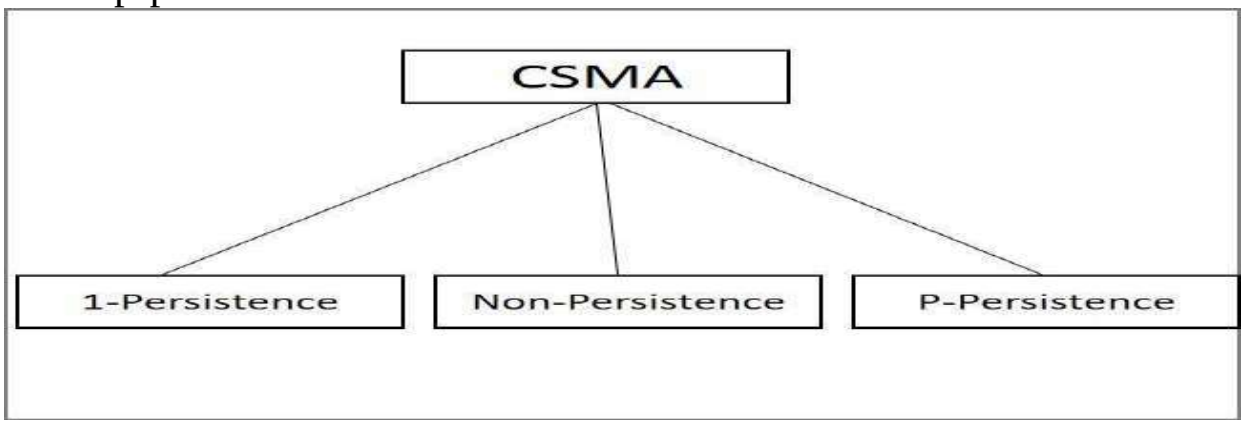
Persistence Method

What should a station do if the channel is busy? What should a station do if the channel is idle?

The three protocols that discuss the various implementations are as

follows −

- 1-persistent CSMA
- Non- Persistent CSMA
- p-persistent CSMA



1-persistent CSMA

The 1-Persistent CSMA is explained below in a stepwise manner.

Step 1 − When a node has data to send, it first listens to the channel to see if anyone is transmitting.

Step 2 − If the channel is busy, the station waits until it becomes idle.

Step 3 − When the station identifies an idle channel, it transmits a frame.

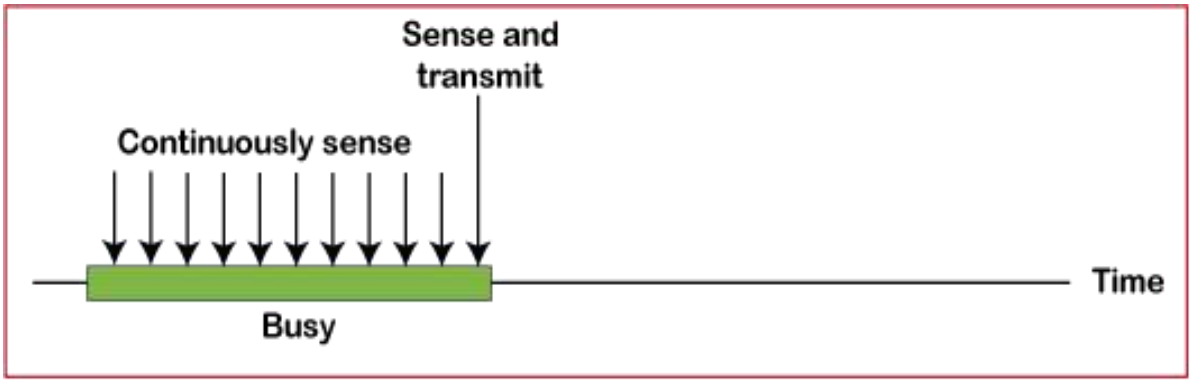
Step 4 − If a collision occurs, the station waits a random amount of time and starts retransmission.

The only drawback is that the propagation delay time affects the 1-persistent CSMA protocol.

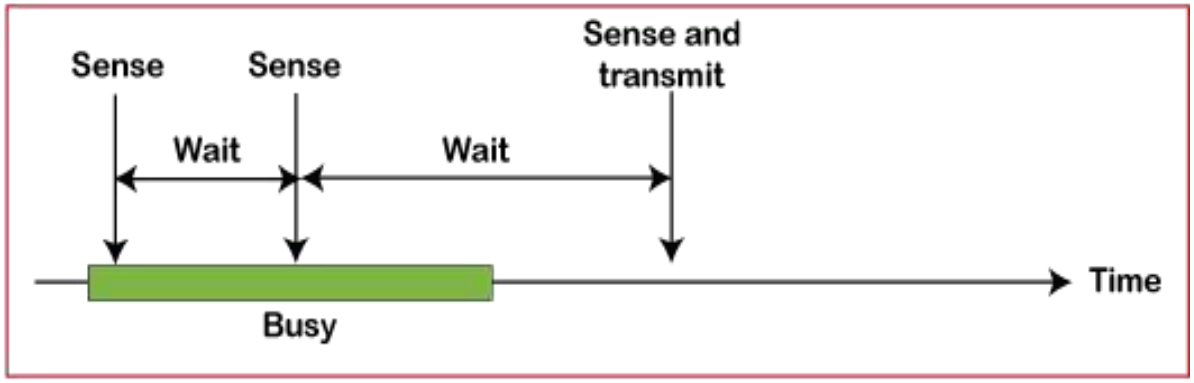
Example

Let us consider an example, just after station A begins its transmission, station B also becomes ready to send its data and senses the channel. If the station A signal has not yet reached station B, station B will sense the channel to be idle and will begin its transmission. This will result in a collision.

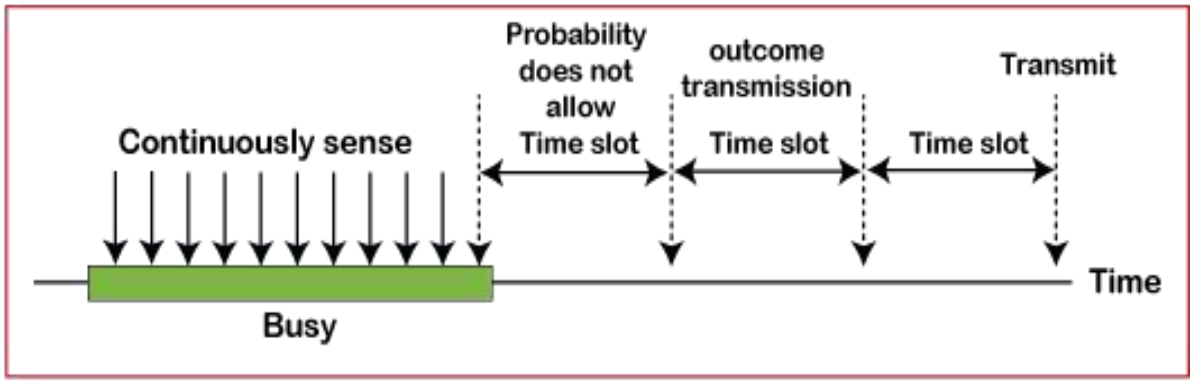
Even if propagation delay time is zero, then also collision occurs. If two stations become ready in the middle of the third station's transmission, both stations will wait until the transmission of the first station ends and then both will begin their transmission exactly simultaneously. This will also result in collision.



a. 1-persistent

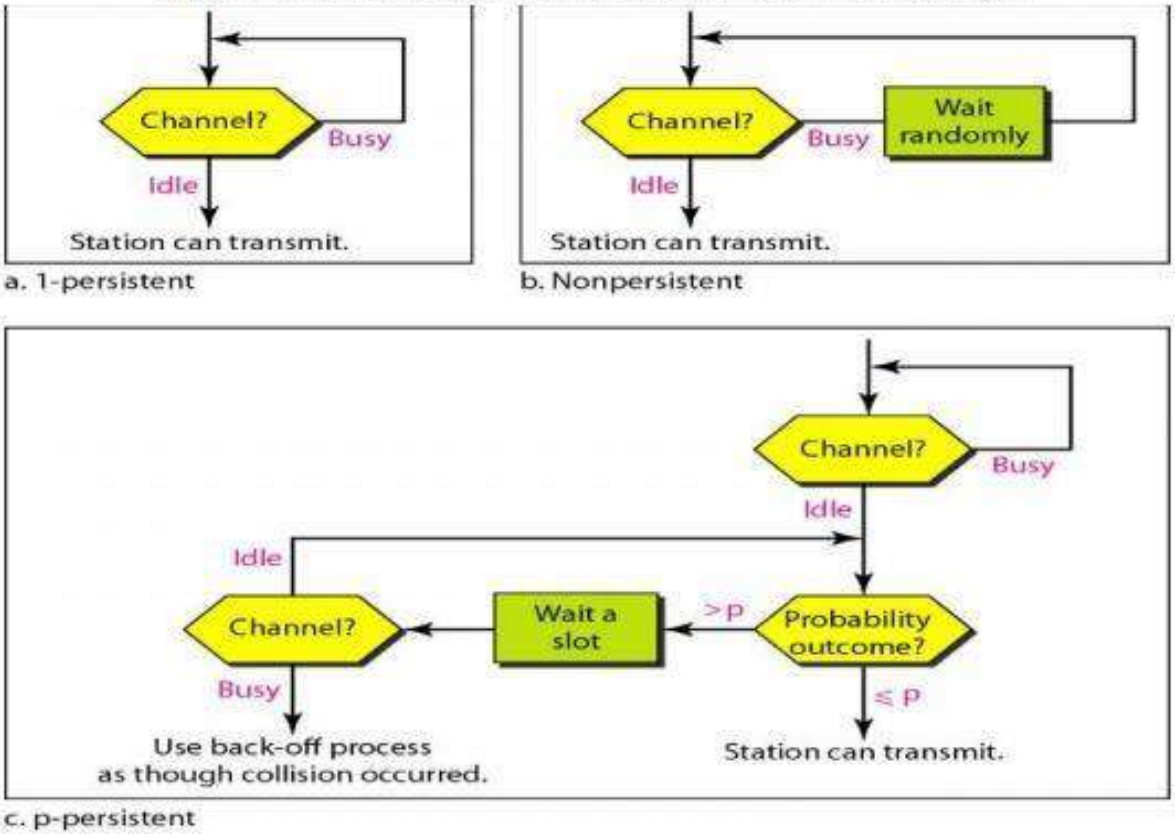


b. Nonpersistent



c. p-persistent

Figure 2.39 shows the flow diagrams for these methods.



Non-persistence CSMA

The Non-Persistence CSMA is explained below in a stepwise manner.

Step 1 − An attempt is made to be less greedy than persistence.

Step 2 − A node that has a frame to send first senses the channel. If the channel is idle, then it senses immediately.

Step 3 − If the channel is busy, then it waits for a random amount of time and then senses the channel again.

Step 4 − In non-persistence CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Step 5 − Consequently this Non persistence leads to better channel utilization but longer delays than 1-persistence CSMA. Here, the number of collisions is reduced.

The **advantage** is that it reduces the chances of collision because the nodes wait for a random amount of time before transmitting.

The **disadvantage** is that it reduces the efficiency of the network because the channel remains idle when there may be stations with frames to send. This is because the nodes are waiting a random amount of time before transmitting.

P-Persistence

The P-Persistence CSMA is explained below in a stepwise manner.

Step 1 − It applies to slotted channels so that the time slot duration is equal to or greater than maximum propagation delay time.

Step 2 − When a station becomes ready to send, it senses the channel.

Step 3 − If it is idle, it transmits with a probability p. with probability q=1-p, it defers until the next slot.

Step 4 − If that slot is idle it either transmits or defers again, with probability p and q. This process is repeated until either the frame has been transmitted or another node has begun transmitting.

Step 5 − In the latter case, the node acts as if there had been a collision

Step 6 − If the station initially senses that the channel is busy, it waits until the next slot and applies the above algorithm.

Step 7 − IEEE 802.11 uses refinement of p-persistence CSMA.

The **advantages** are that the P-Persistence reduces the chances of collision and improves the efficiency of the network.

Let’s see the comparison of the channel utilization versus load for various random-access protocols

CSMA/CD-CSMA Collision Detection

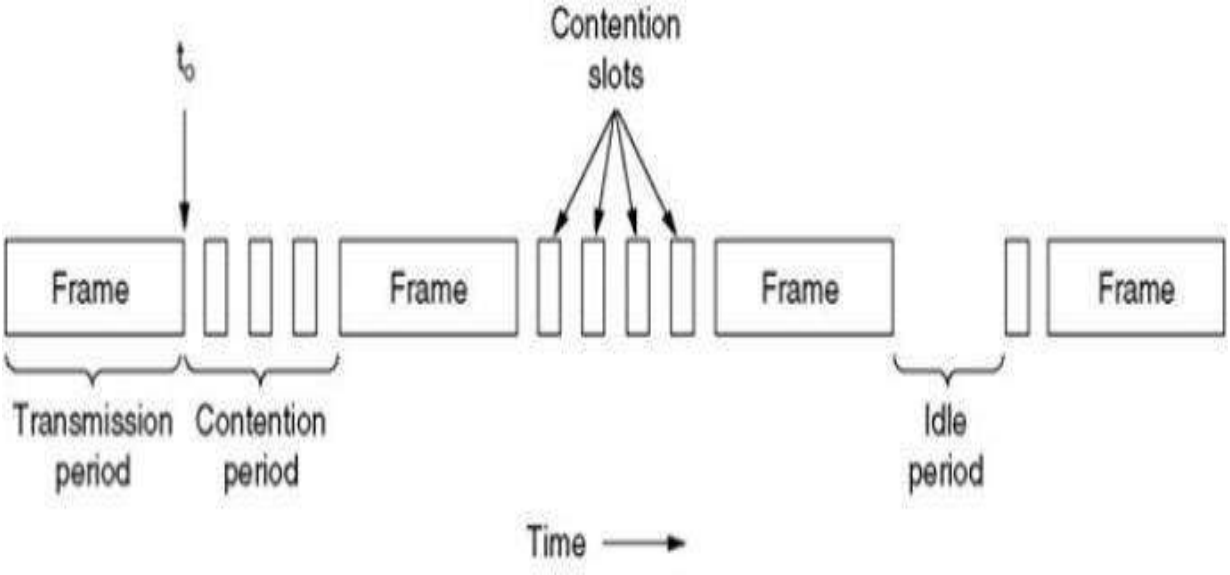
The concept of Collision Detection (CSMA/CD) is explained below in stepwise manner:

Step 1 − If two stations sense the channel to be ideal and they begin transmitting simultaneously and collision occurs, rather than finish transmitting the frames should just stop transmitting the frames as soon as collision dictated.

Step 2 − By terminating frames it would save time and bandwidth. This is called CSMA/CD.

Step 3 − It is mainly used LAN in the MAC sub player (part of data linklayer network) and Ethernet.

CSMA/CD can be in contention, transmission, or idle state. Let us see the below diagram to understand the concept −



Here,

- At the time to transition period ends and at the next frame sentbetween there is the condensation period.
- This period is the minimum time a host must transmit such that itcan be sure that no other host packet it has been transmitting.

- It will be a minimum period. By this way we can avoid collisions.
- Collision can be detected by looking at the power or pulse width of the received signal and compared with the transmitted signal.
- Power signal is better than the transmitted signal. The ideal periodis when all stations are quiet.
- So at consecutive transmission and condensation periods the framecan check if a collision is found.
- The main disadvantage is that it is not suitable for long distance transmission and it cannot be used in wireless technologies.

Controlled Access Protocols

In the Controlled access technique, all stations need to consult with one another in order to find out which station has the right to send the data.

- The controlled access protocols mainly grant permission to send only one node at a time; thus in order to avoid the collisions among the shared mediums.
- No station can send the data unless it has been authorized by the other stations.

The protocols lies under the category of Controlled access are as follows:

1. Reservation
2. Polling
3. Token Passing

Let us discuss each protocol one by one:

1. Reservation

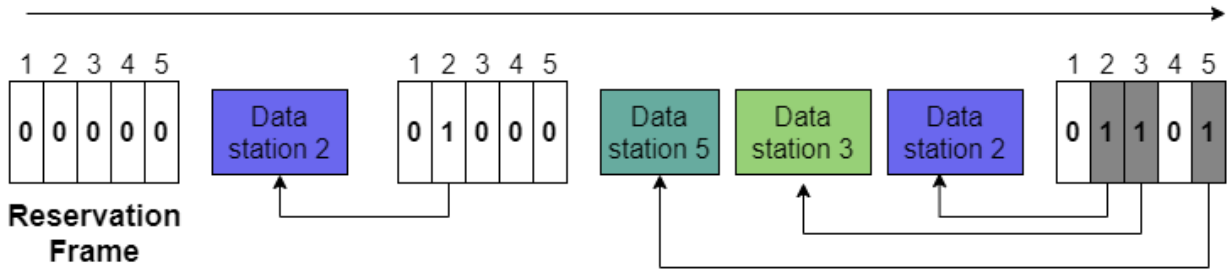
In this method, a station needs to make a reservation before sending the data.

- Time is mainly divided into intervals.
- Also, in each interval, a reservation frame precedes the data frame that is sent in that interval.

- Suppose if there are **'N'** stations in the system in that case there are exactly **'N'** reservation mini slots in the reservation frame; where each mini slot belongs to a station.
- Whenever a station needs to send the data frame, then the station makes a reservation in its own mini slot.
- Then the stations that have made reservations can send their data after the reservation frame.

Example

Let us take an example of 5 stations and a 5-mini slot reservation frame. In the first interval, the station 2, 3 and 5 have made the reservations. While in the second interval only station 2 has made the reservations.



2. Polling

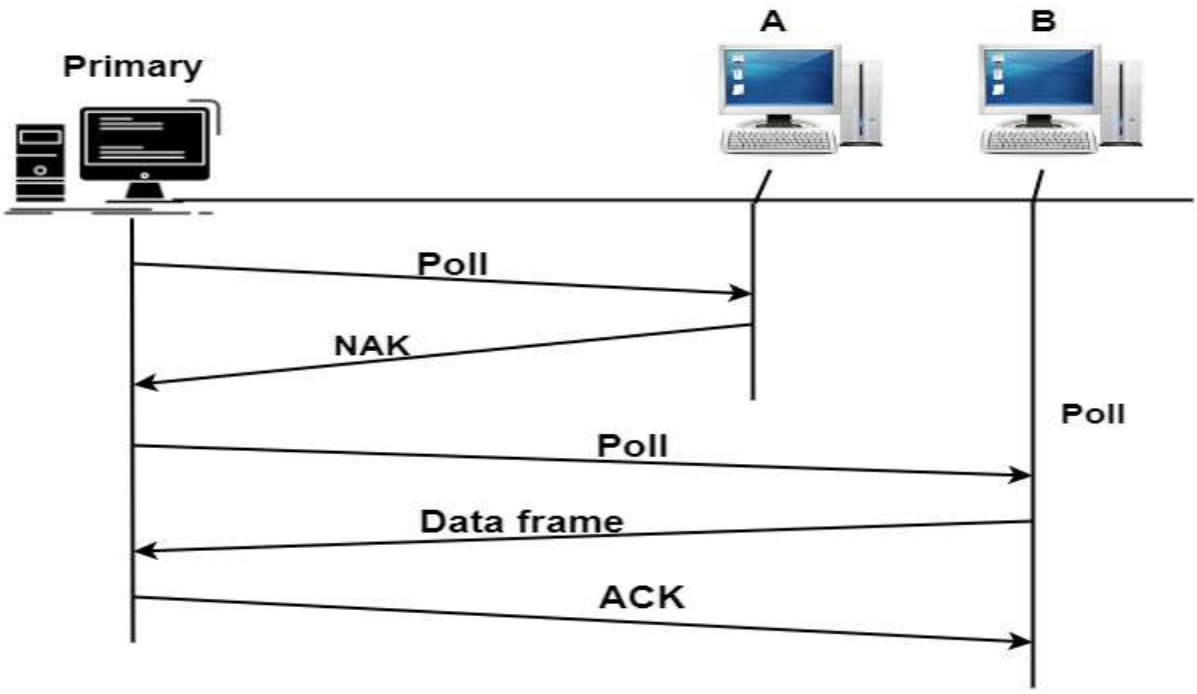
The polling method mainly works with those topologies where one device is designated as the primary station and the other device is designated as the secondary station.

- All the exchange of data must be made through the primary device even though the final destination is the secondary device.
- Thus to impose order on a network that is of independent users, and in order to establish one station in the network that will act as a controller and periodically polls all other stations is simply referred to as **polling**.
- The Primary device mainly controls the link while the secondary device follows the instructions of the primary device.
- The responsibility is on the primary device in order to determine which device is allowed to use the channel at a given time.
- Therefore the primary device is always an initiator of the session.

Poll Function

In case if primary devices want to receive the data, then it usually asks the secondary devices if they have anything to send. This is commonly known as **Poll Function**.

- There is a **poll function** that is mainly used by the primary devices in order to solicit transmissions from the secondary devices.
- When the primary device is ready to receive the data then it must **ask (poll)** each secondary device in turn if it has anything to send.
- If the secondary device has data to transmit then it sends the data frame, otherwise, it sends a **negative acknowledgment (NAK)**.
- After that in case of the negative response, the primary then polls the next secondary, in the same manner until it finds the one with the data to send. When the primary device received a positive response that means (a data frame), then the primary devices reads the frame and then returns an acknowledgment **(ACK)**frame,



Select Function

In case, if the primary device wants to send the data then it tells the secondary devices in order to get ready to receive the data. This is commonly known as the **Select function**.

- Thus the **select function** is used by the primary device when it has something to send.
- We had already told you that the **primary device** always **controls the link.**
- Before sending the data frame, a select **(SEL) frame is** created and transmitted by the primary device, and one field of the SEL frame includes the address of the intended secondary.
- The primary device alerts the secondary devices for the upcoming transmission and after that wait for an acknowledgment (ACK) of the secondary devices.

3. Token Passing

In the token passing methods, all the stations are organized in the form of a logical ring. We can also say that for each station there is a predecessor and a successor.

- The predecessor is the station that is logically before the station in the ring; while the successor is the station that is after the station in the ring. The station that is accessing the channel now is the **current station**.
- Basically, a special bit pattern or a small message that circulates from one station to the next station in some predefined order is commonly known as a **token**.
- Possessing the token mainly gives the station the right to access the channel and to send its data.
- When any station has some data to send, then it waits until it receives a token from its predecessor. After receiving the token, it holds it and then sends its data. When any station has no more data in order to send then it releases the token and then passes the token to the next logical station in the ring.
- Also, the station cannot send the data until it receives the token again in the next round.
- In Token passing, when a station receives the token and has no data to send then it just passes the token to the next station.
- The problem that occurs due to the Token passing technique is the duplication of tokens or loss of tokens. The insertion of the new station, removal of a station, also needs to be tackled for correct and reliable operation of the token passing technique.

The performance of a token ring is governed by 2 parameters, which are delay and throughput.

Delay is a measure of the time; it is the time difference between a packet ready for transmission and when it is transmitted. Hence, the average time required to send a token to the next station is a/N.

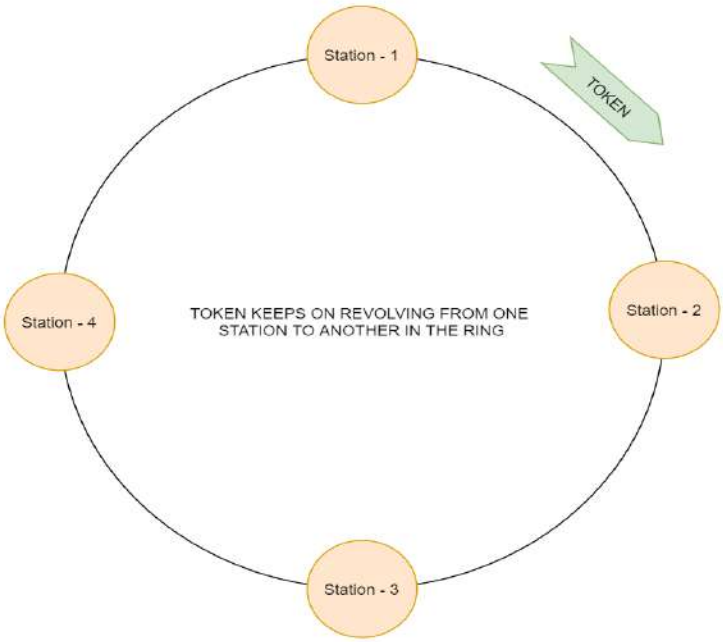
Throughput is a measure of the successful traffic in the communication channel.

Throughput, S = 1/ (1 + a/N) for a<1

S = 1/[a(1+1/N)] for a>1, here N = number of stations & a = Tp/Tt

Tp = propagation delay &Tt = transmission delay

In the diagram below when station-1 posses the token, it starts transmitting all the data-frames which are in its queue. now after transmission, station-1 passes the token to station-2 and so on. Station-1 can now transmit data again, only when all the stations in the network have transmitted their data and passed the token.

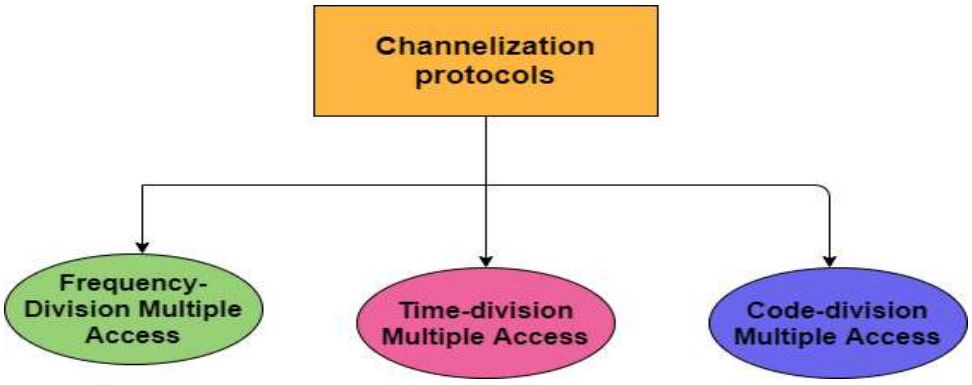


Channelization Protocols

Channelization is basically a method that provides the multiple-access and in this, the available bandwidth of the link is shared in time, frequency, or through the code in between the different stations.
Channelization Protocols are broadly classified as follows:

- FDMA(Frequency-Division Multiple Access)

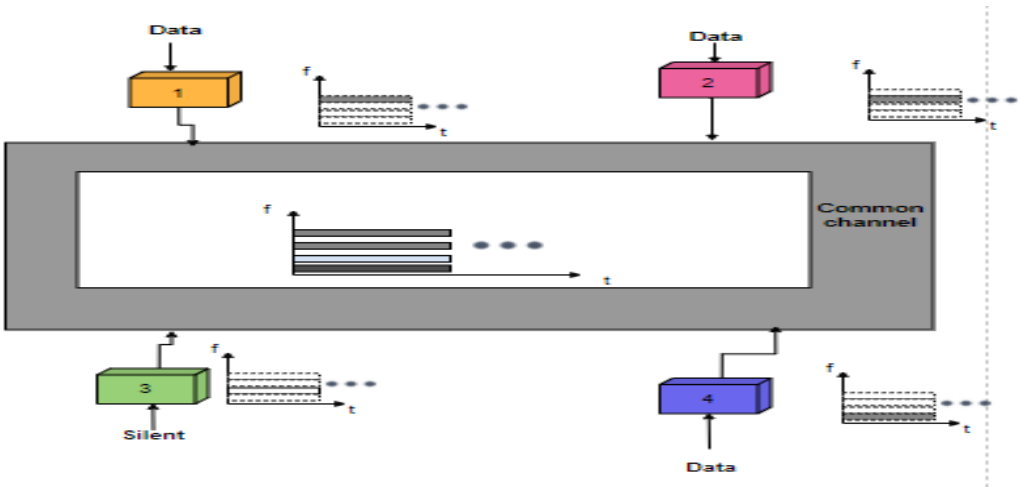
- TDMA(Time-Division Multiple Access)
- CDMA(Code-Division Multiple Access)



1. Frequency-Division Multiple Access

With the help of this technique, the available bandwidth is divided into frequency bands. Each station is allocated a band in order to send its data. Or in other words, we can say that each band is reserved for a specific station and it belongs to the station all the time.

- Each station makes use of the **bandpass filter** in order to confine the **frequencies of the transmitter.**
- In order to prevent station interferences, the allocated bands are separated from one another with the help of small **guard bands.**
- The Frequency-division multiple access mainly specifies a predetermined frequency for the entire period of communication.
- Stream of data can be easily used with the help of FDMA.



2. Time-Division Multiple Access

Time-Division Multiple access is another method to access the channel for shared medium networks.

- With the help of this technique, the stations share the bandwidth of the channel in time.
- A time slot is allocated to each station during which it can send the data.
- Data is transmitted by each station in the assigned time slot.
- There is a problem in using TDMA and it is due to TDMA the synchronization cannot be achieved between the different stations.
- When using the TDMA technique then each station needs to know the beginning of its slot and the location of its slot.
- If the stations are spread over a large area, then there occur propagation delays; in order to compensate this guard, times are used.
- The data link layer in each station mainly tells its physical layer to use the allocated time slot.

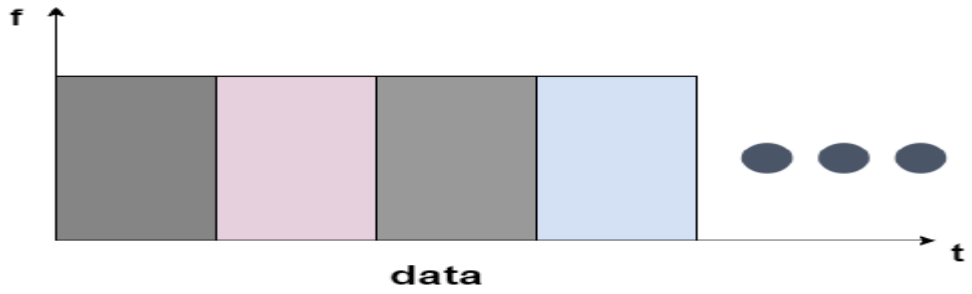


Figure: Time-Division media access.

3. Code-Division Multiple Access

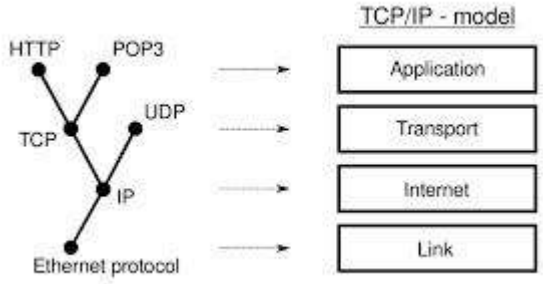
CDMA(code-division multiple access) is another technique used for channelization.

- CDMA technique differs from the FDMA because only one channel occupies the entire bandwidth of the link.
- The CDMA technique differs from the TDMA because all the stations can send data simultaneously as there is no timesharing.
- The CDMA technique simply means communication with different codes.
- In the CDMA technique, there is only one channel that carries all the transmission simultaneously.

- CDMA is mainly based upon the coding theory; where each station is assigned a code, Code is a sequence of numbers called chips.
- The data from the different stations can be transmitted simultaneously but using different code languages.

2.7 What is an Ethernet Protocol?

Ethernet protocol definition: The most popular and oldest LAN technology is Ethernet Protocol, so it is more frequently used in LAN environments which is used in almost all networks like offices, homes, public places, enterprises, and universities. Ethernet has gained huge popularity because of its maximum rates over longer distances using optical media.

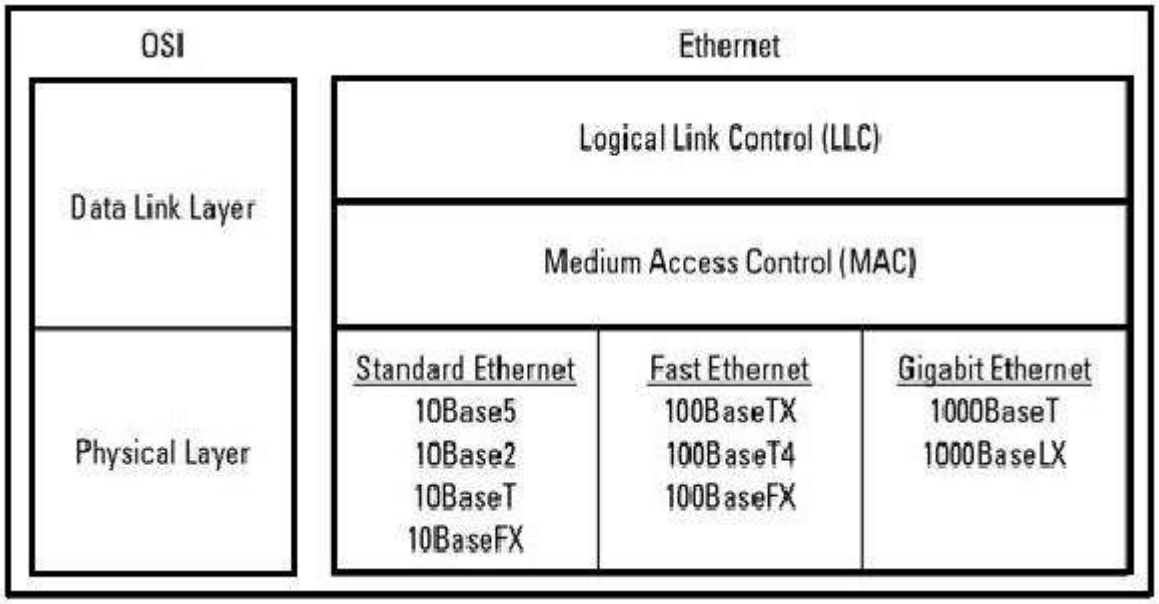


The Ethernet protocol uses a star topology or linear bus which is the foundation of the IEEE 802.3 standard. The main reason to use Ethernet widely is, simple to understand, maintain, implement, provides flexibility, and permits less cost network implementation.

Ethernet Protocol Architecture

In the OSI network model, Ethernet protocol operates at the first two layers like the Physical & the Data Link layers but, Ethernet separates the Data Link layer into two different layers called the Logical Link Control layer & the Medium Access Control layer.

The physical layer in the network mainly focuses on the elements of hardware like repeaters, cables & network interface cards (NIC). For instance, an Ethernet network like 100BaseTX or 10BaseT indicates the cables type that can be used, the length of cables, and the optimal topology.



The data link layer in the network system mainly addresses the way that data packets are transmitted from one type of node to another. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where every computer listens to the cable before transmitting anything throughout the network.

The two layers in the above Ethernet protocol block diagram deal with the physical network structure where the network devices can transmit data from one device to another on a network. Certainly, the most popular set of protocols used for both the Physical & Data Link layers is known as Ethernet. Ethernet is available in different forms where the current Ethernet can be defined through the IEEE 802.3 standard.

Ethernet protocols are available in different flavors and operate at various speeds by using different types of media. But, all the Ethernet versions are well-matched through each other. These versions can mix & match on a similar network with the help of different network devices like hubs, switches, bridges to connect the segments of the network that utilize different types of media.
The Ethernet protocol's actual transmission speed can be measured in Mbps (millions of bits for each second), The speed versions of Ethernet are available in three different types 10 Mbps, called Standard Ethernet; 100 Mbps called Fast Ethernet & 1,000 Mbps, called as Gigabit Ethernet. The transmission speed of the network is the maximum speed that can be attained over the network in ideal conditions. The output of the Ethernet network rarely achieves this highest speed.