UNIT 3:
Data Link Layer

Design Issues in Data Link Layer

Data-link layer is the second layer after the physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes. Before going through the design issues in the data link layer. Some of its sub-layers and their functions are as following below.

The data link layer is divided into two sub-layers :

1. **Logical Link Control Sub-layer (LLC) –**
   Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –
   - **(i)** Error Recovery.
   - **(ii)** It performs the flow control operations.
   - **(iii)** User addressing.

2. **Media Access Control Sub-layer (MAC) –**
   It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card.
   Functions are –
   - **(i)** To perform the control of access to media.
   - **(ii)** It performs the unique addressing to stations directly connected to LAN.
   - **(iii)** Detection of errors.

Design issues with data link layer are :

1. **Services provided to the network layer –**
   The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Data link-layer).

2. **Frame synchronization –**
   The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.
3. **Flow control –**
   Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.
4. **Error control –**
   Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

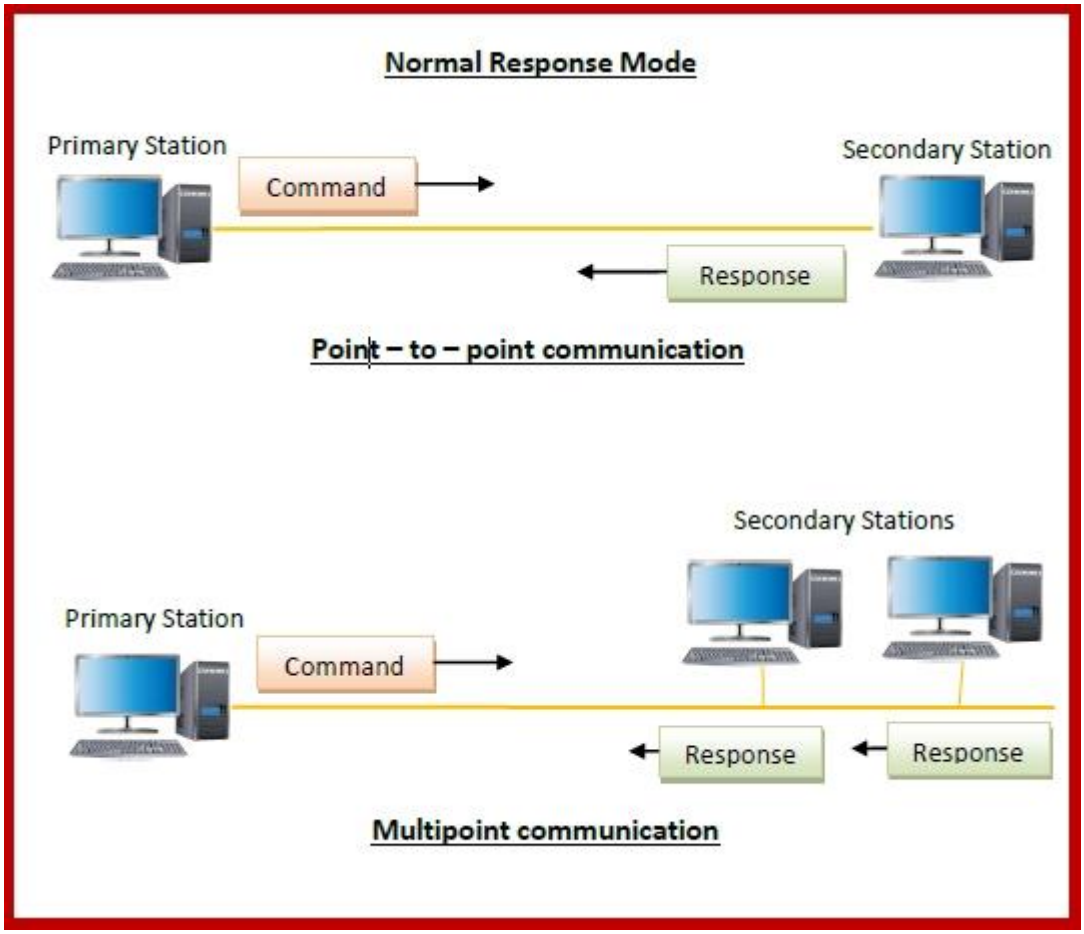
High-level Data Link Control (HDLC)

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 point - to - point and multipoint communications.

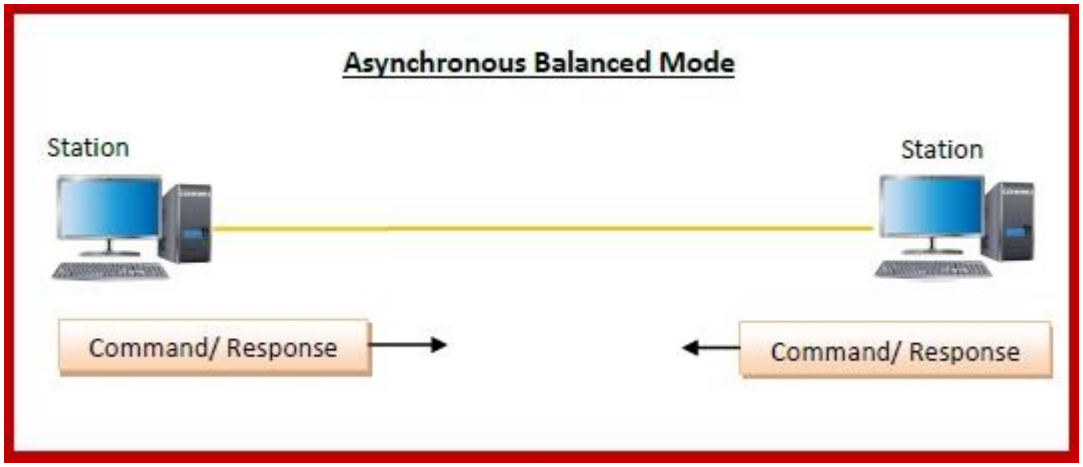
Transfer Modes

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

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



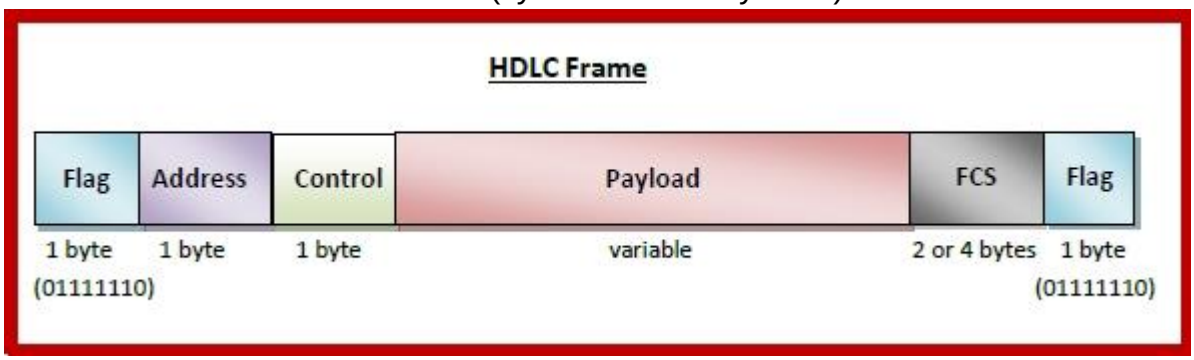
- **Asynchronous Balanced Mode (ABM)** − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

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

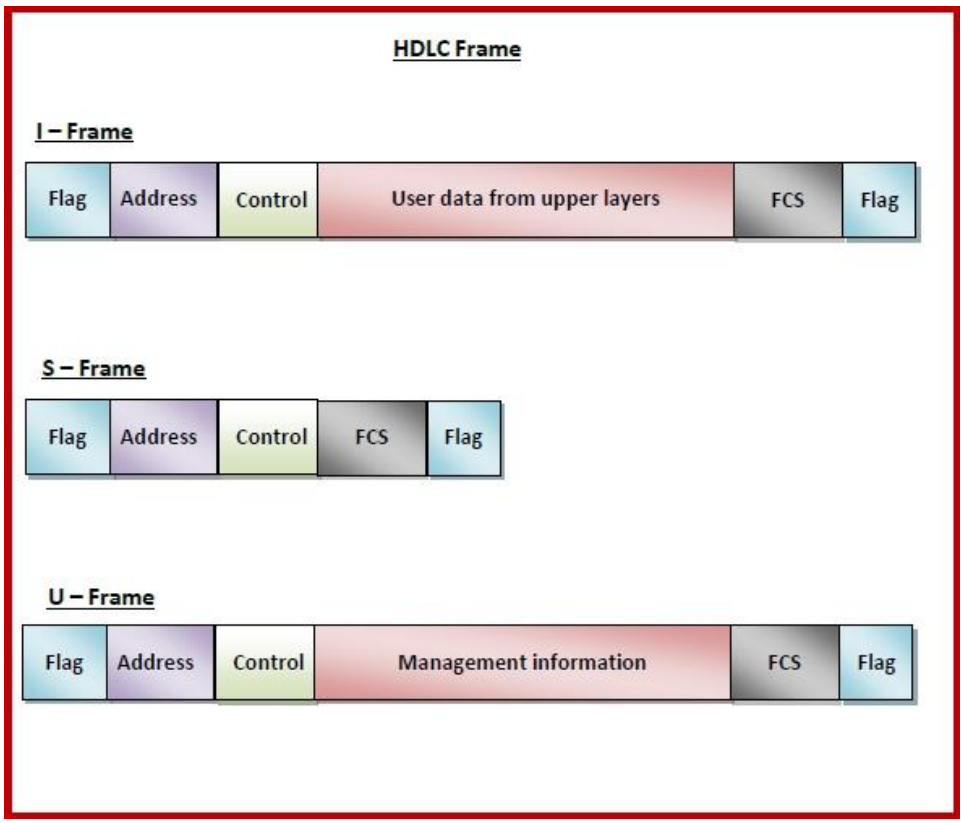
- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent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



Types of HDLC Frames

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

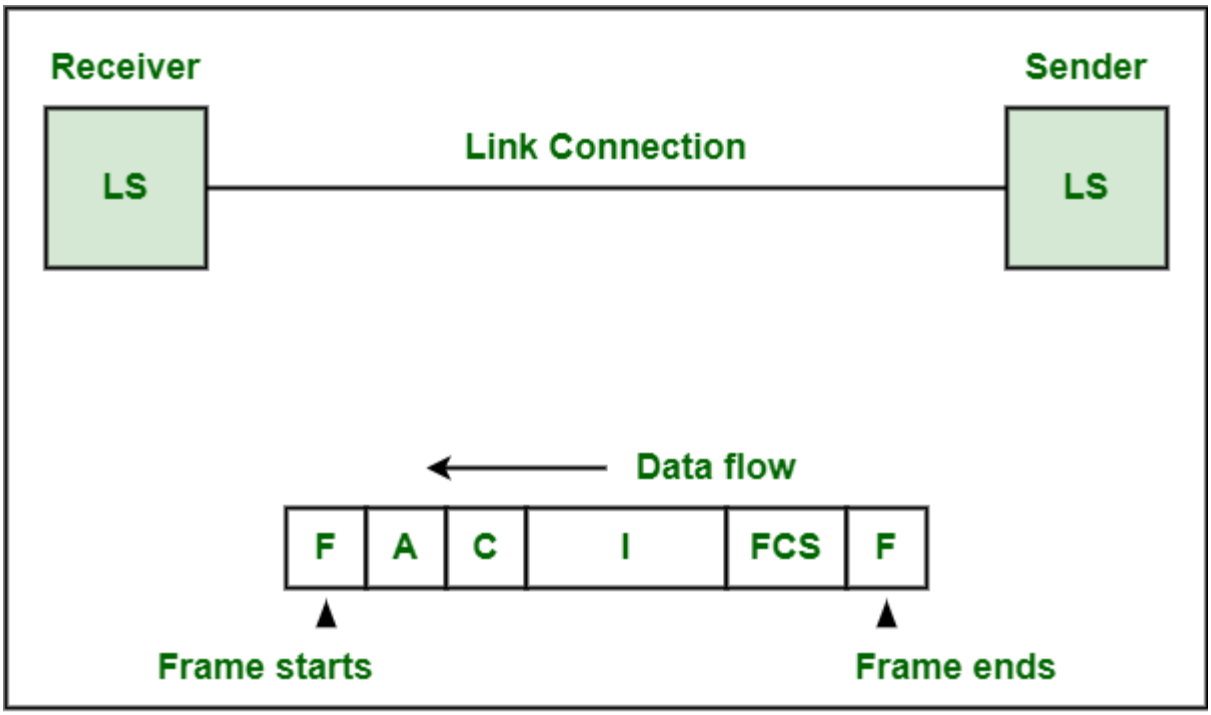
- **I-frame** − I-frames or Information frames carry user data from the network layer. They also include flow and error control information that is piggybacked on user data. The first bit of control field of I-frame is 0.
- **S-frame** − S-frames or Supervisory frames do not contain information field.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



SDLC

Synchronous Data Link Control (SDLC) is generally linked layer protocol that is used with Systems Network Architecture (SNA) environment. SNA is proprietary networking architecture of IBM that is developed in 1974. SDLC also supports huge variety of typologies and different types of data links.

Examples include point-to-point links, multipoint links, switched networks, packet networks, etc. It also uses primary station-secondary station model of data communication. On an SDLC data link, all of data and control transmission are simply organized and managed in specific format that is basically known as transmission frame. Transmission frame is also known as SDLC frame or just a frame.

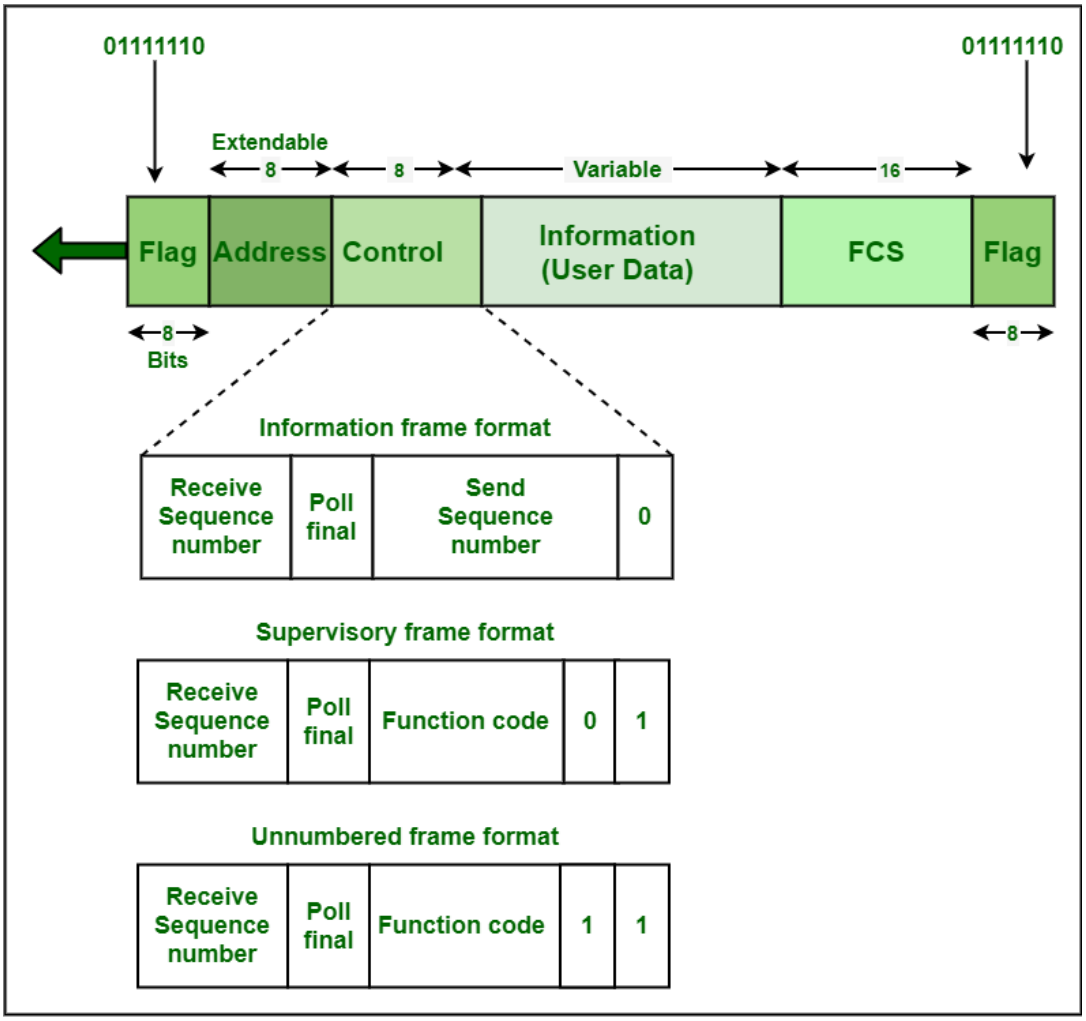


SDLC Transmission Frame

Transmission frame simply carries or transfer control information and data of user among transmitting or sending station and receiving station. It allows and gives permission to receiving station :

- To determine starting and end of frame.
- To identify whether frame is made or intended for that particular station.
- To identify actions that are needed to be performed with received information or data.
- To detect and identify error occurred during transmission in received frames.
- To acknowledge its frames receipt to transmitting station.

Frame Format :
Transmission frame of each of SDLC has specific frame format. Each frame is made up of following fields :



Basic SDLC Frame Structure

1. **Flag Field –**
   Flag (F) is beginning frame that represents beginning of frame. This field is used to initiate and terminate occurrence of error by regular checking.
2. **Address Field –**
   Address (A) filed follows just after beginning flag. It is used to identifies and determines secondary station that is transmitting frame. This is done because frame contains information or data regarding group address, specific address. Broadcast address, etc.
3. **Control Field –**
   Control (C) field follows just after address field. It is used to specify functions of particular frame.
   This field can be present in three types of format as given below :

- **(i). Unnumbered (U) format :**
  It is required to perform various functions such as to establish disconnect link, to report some procedural errors, to transfer or transmit data especially when location or address of data in frame sequence is not needed to be checked.
- **(ii). Supervisory (S) format :**
  It is required to perform various functions such as to acknowledge received frames, to convey ready or busy conditions, report frame numbering errors, etc. This format does not contain any information field.
- **(iii). Information (I) format :**
  It is required to perform various functions such as to transfer data or information, to control sequence in which frames are needed to sent and number of frames.

4. **Information Field –**
   Information (I) field follows just after control field. This field is an optional field that mainly contains information data. The data is needed to be transmitted on data link is present in this field.
5. **FCS Field –**
   Frame Check Sequence (FCS) field follows just after information field. This field especially allows and grants permission to receiving stations to simply ensure and check transmission accuracy of frame. This field simply checks received frame for any kind of error that might have been occurred by link connection.
6. **Ending Flag Field –**
   This field indicates ending of frame.

What is SLIP?

SLIP stands for Serial Line Internet Protocol. SLIP is an Internet protocol that allows users to gain Internet access using a computer modem. Today, SLIP is not used as frequently as its successor, PPP (Point-to-Point Protocol), which provides enhanced error detection and automatic configuration.

SLIP is commonly used on dedicated serial links and sometimes for dialup purposes and is usually used with line speeds between 1200bps and 19.2Kbps. It is useful for allowing mixes of hosts and routers to communicate with one another (host-host, host-router and router- router are all common SLIP network configurations).

SLIP defines a sequence of characters that frame IP packets on a serial line and nothing more. It provides no addressing, packet type identification, error detection/correction or compression mechanisms. Because the protocol does so little, though, it is usually very easy to implement.

Problems of SLIP

The problems associated with SLIP are explained below −

Standardized Datagram Size Specification

SLIP’s maximum datagram size supported is not standardized and depends on the implementation. The usual default is 1006 bytes, which becomes the maximum transmission unit (MTU) for the link. If a different size is used, this must be programmed into the IP layer.

Error Detection/Correction Mechanism

SLIP doesn't provide any way of detecting or correcting errors in transmissions. While such protection is provided at higher layers through IP header checksums and other mechanisms, it is a job “traditionally” also done at layer two.

The reason is that relying on those higher layers means that errors are only detected after an entire datagram has been sent and passed back up the stack at the recipient. Error correction can only come in the form of re-sending any datagrams that were corrupted.

This is inefficient, especially considering that serial links are generally much slower than normal LAN links.

Control Messaging

SLIP provides no way for the two devices to communicate control information between them to manage the link.

Type Identification

Since SLIP includes no headers of its own, it is not possible to identify the protocol it is sending. While developed for IP, you can see that there is no reason another layer three protocols could not be sent using SLIP. However, without type identification, there is no way to mix datagrams from two or more layer three protocols on the same link.

Address Discovery Method

Addressing isn't needed at layer two due to the point-to-point nature of the connection. There are only two devices, so the intended recipient of each message is obvious. However, devices do need some way of learning each other's IP addresses for routing at layer three. SLIP provides no method for this.

Support for Compression

Compression would improve performance over serial lines that are, again, slow compared to other technologies. SLIP provides no compression features. Note that the modems usually do support the compression at layer one for serial connections that use them.

There was also a variant on SLIP called Compressed SLIP or CSLIP that was created in the late 1980s, but it was not as widely deployed as regular SLIP.

Security Features

SLIP provides no methods for authentication of connections or encryption of data, which means even the basics of security are not provided.

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.

Services provided by PPP

- 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.

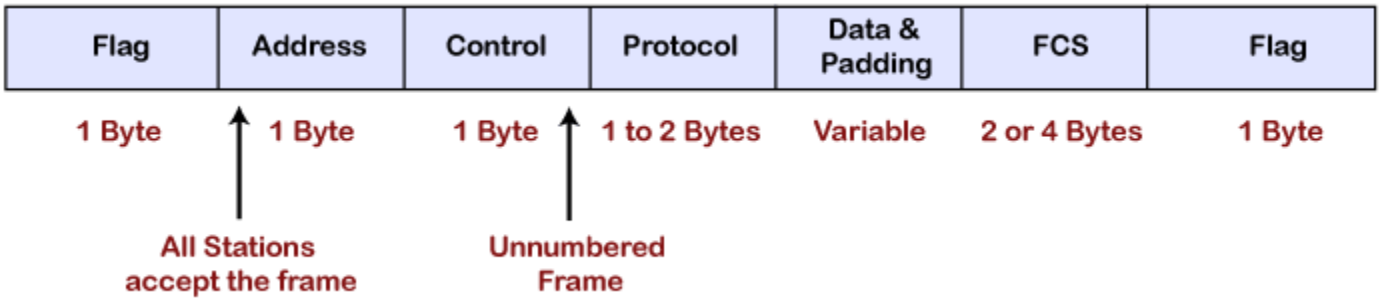
It is a byte-oriented protocol as it provides the frames as a collection of bytes or characters. It is a WAN (Wide Area Network) protocol as it runs over the internet link which means between two routers, internet is widely used.

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:

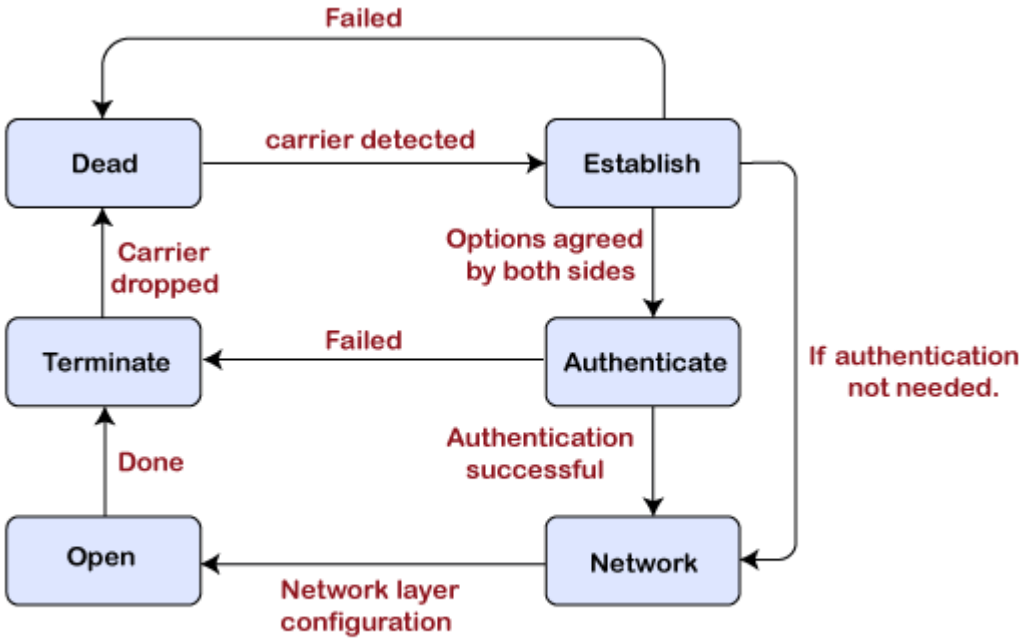


- **Flag:** The flag field is used to indicate the start and end of the frame. The flag field is a 1-byte field that appears at the beginning and the ending of the frame. The pattern of the flag is similar to the bit pattern in HDLC, i.e., 01111110.
- **Address:** It is a 1-byte field that contains the 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.

Transition phases of PPP protocol

The following are the transition phases of a PPP protocol:



Transition phases

- **Dead:** Dead is a transition phase which means that the link is not used or there is no active carrier at the physical layer.
- **Establish:** If one of the nodes starts working then the phase goes to the establish phase. In short, we can say that when the node starts communication or carrier is detected then it moves from the dead to the establish phase.
- **Authenticate:** It is an optional phase which means that the communication can also moves to the authenticate phase. The phase moves from the establish to the authenticate phase only when both the communicating nodes agree to make the communication authenticated.
- **Network:** Once the authentication is successful, the network is established or phase is network. In this phase, the negotiation of network layer protocols take place.

- **Open:** After the establishment of the network phase, it moves to the open phase. Here open phase means that the exchange of data takes place. Or we can say that it reaches to the open phase after the configuration of the network layer.
- **Terminate:** When all the work is done then the connection gets terminated, and it moves to the terminate phase.

On reaching the terminate phase, the link moves to the dead phase which indicates that the carrier is dropped which was earlier created.

There are two more possibilities that can exist in the transition phase:

- The link moves from the authenticate to the terminate phase when the authentication is failed.
- The link can also move from the establish to the dead state when the carrier is failed.

PPP Stack

In PPP stack, there are three set of protocols:

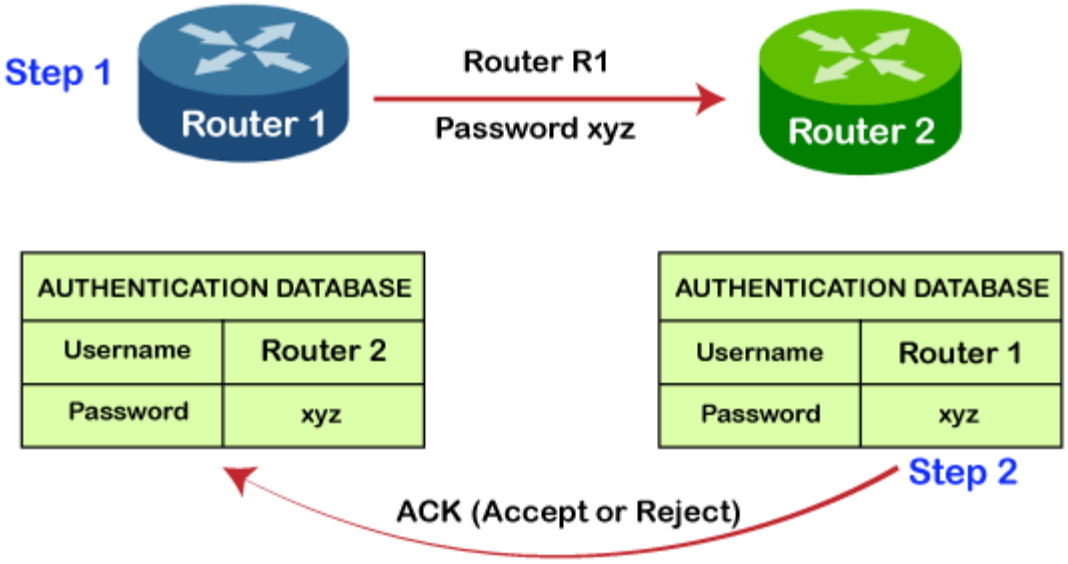
- **Link Control Protocol (LCP)**

The role of LCP is to establish, maintain, configure, and terminate the links. It also provides negotiation mechanism.

- **Authentication protocols**

There are two types of authentication protocols, i.e., PAP (Password Authenticate protocols), and CHAP (Challenged Handshake Authentication Protocols).

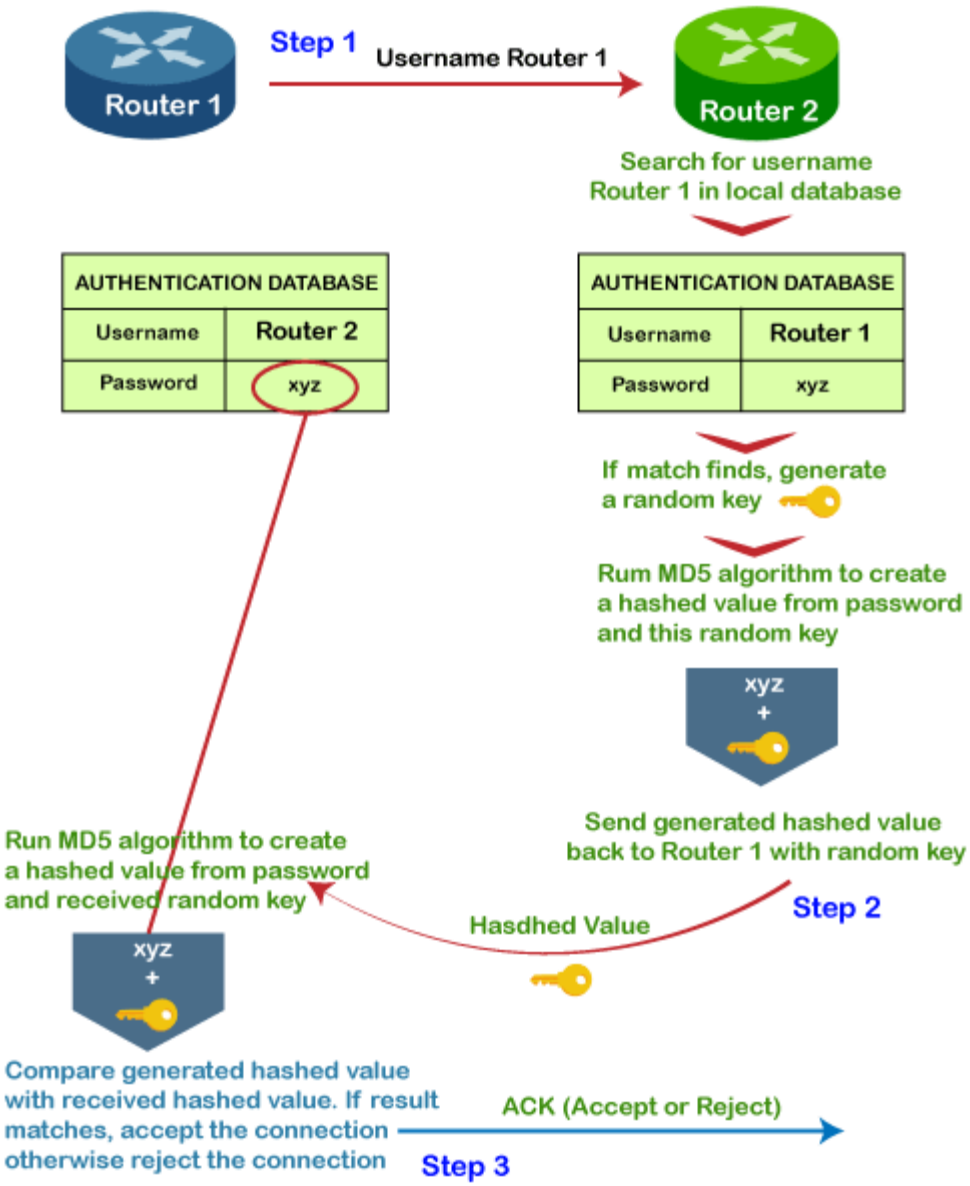
1. PAP (Password Authentication Protocols)



PAP is less secure as compared to CHAP as in case of PAP protocol, password is sent in the form of a clear text. It is a two-step process. Suppose there are two routers, i.e., router 1 and router 2. In the first step, the router 1 wants to authenticate so it sends the username and password for the authentication. In the second step, if the username and password are matched then the router 2 will authenticate the router 1 otherwise the authentication failed.

2. CHAP (Challenged Handshake Authentication Protocol)

CHAP is a three-step process. Let's understand the three steps of CHAP.



Step 1: Suppose there are two routers, i.e., router 1 and router 2. In this step, router 1 sends the username but not the password to the router 2.

Step 2: The router 2 maintains a database that contains a list of allowed hosts with their login credentials. If no data is found which means that the router 1 is not a valid host to connect with it and the connection gets terminated. If the match is found then the random key is passed. This random key along with the password is passed in the MD5 hashing function, and the hashing function generates the hashed value from the password and the random key (password + random key). The hashed value is also known as Challenge. The challenge along with the random key will be sent to the router 1.

Step 3: The router 1 receives the hashed value and a random key from the router 2. Then, the router 1 will pass the random key and locally stored password to the MD5 hashing function. The MD5 hashing function generates the hashed value from the combination of random key and password. If the generated hashed value does not match with the received hashed value then the connection gets terminated. If it is matched, then the connection is granted. Based on the above authentication result, the authentication signal that could be either accepted or rejected is sent to the router 2.

- **Network Control Protocol (NCP)**

After the establishment of the link and authentication, the next step is to connect to the network layer. So, PPP uses another protocol known as network control protocol (NCP). The NCP is a set of protocols that facilitates the encapsulation of data which is coming from the network layer to the PPP frames.

Medium Access Control Sublayer (MAC sublayer)

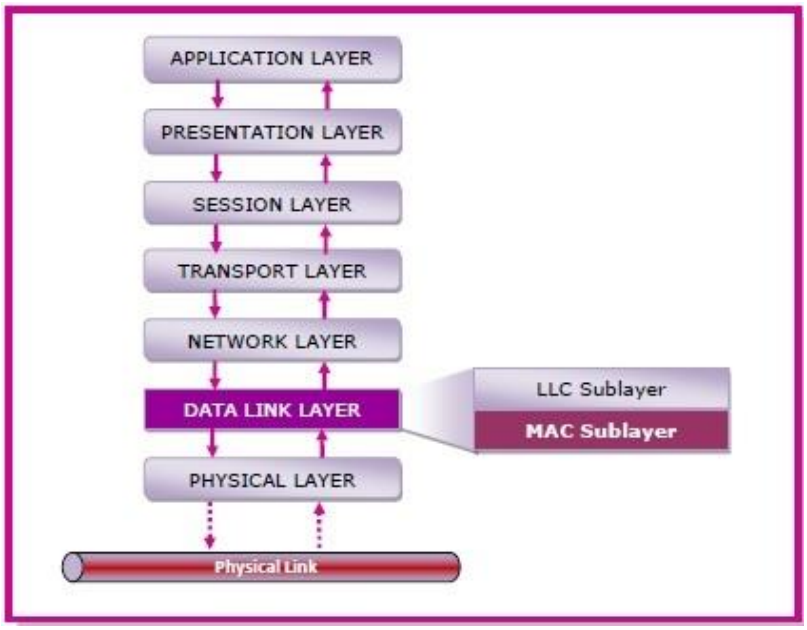
The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

The following diagram depicts the position of the MAC layer −



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 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 initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

Data Link Layer

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.

Data Link Control

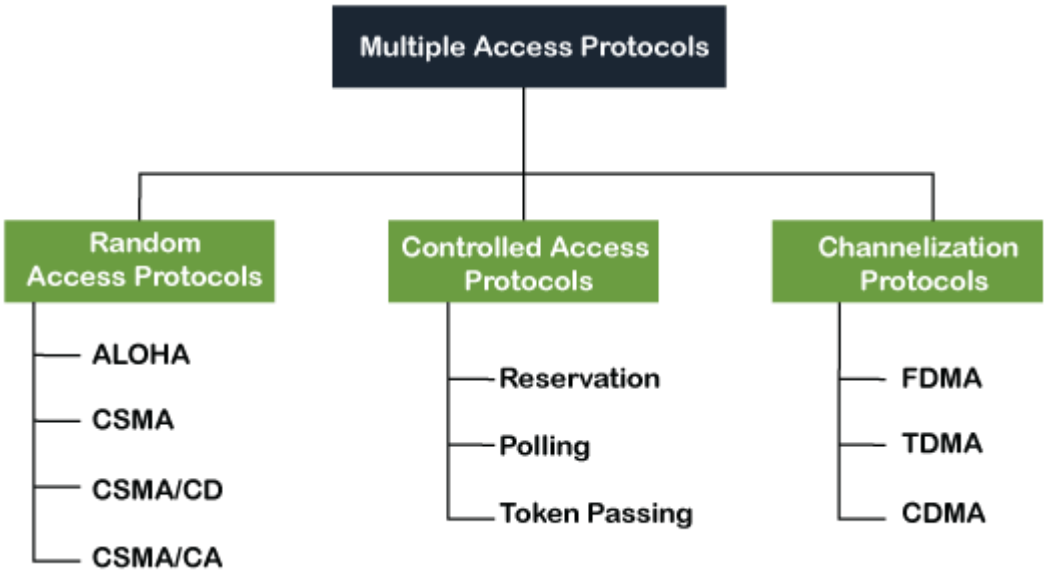
A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

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 transmits 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 nor any station control another station. 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.

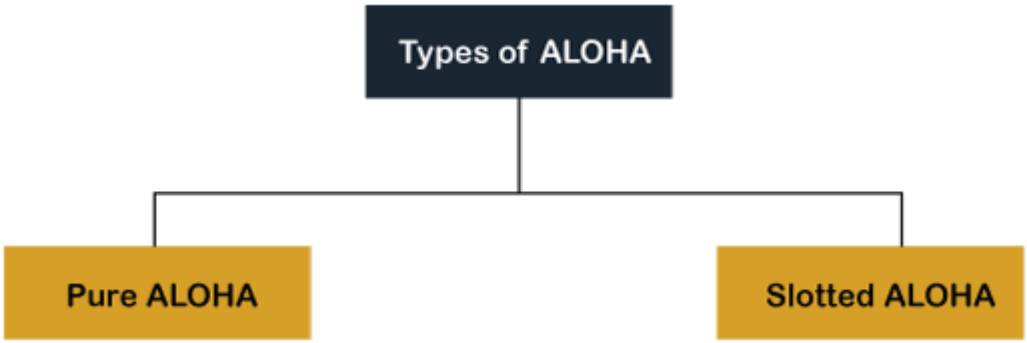
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

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

Aloha Rules

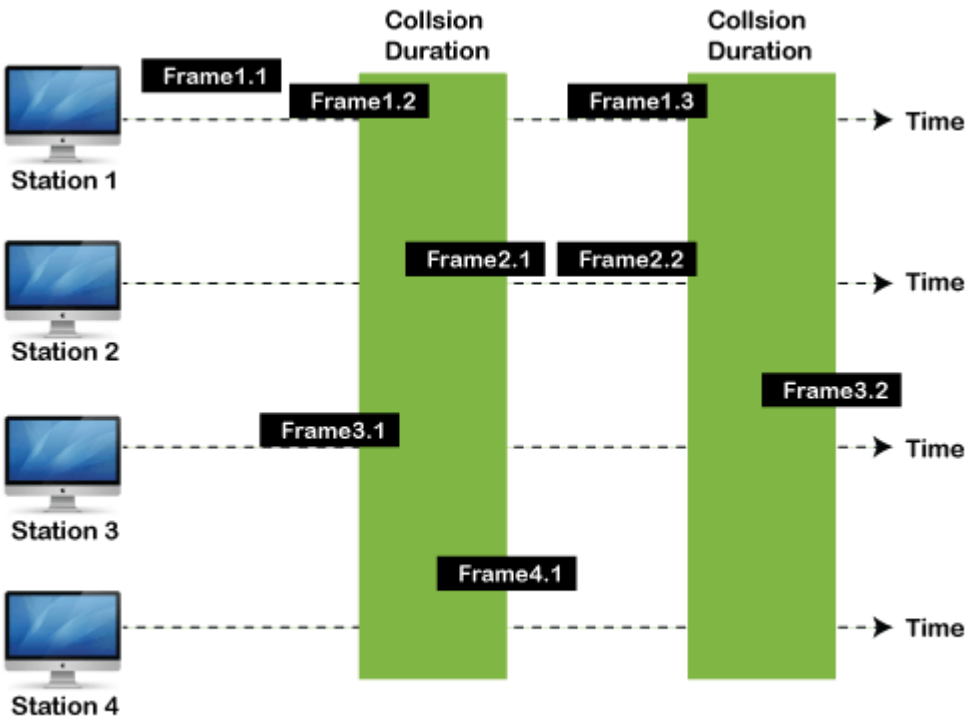
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires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



Pure Aloha

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

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



Frames in Pure ALOHA

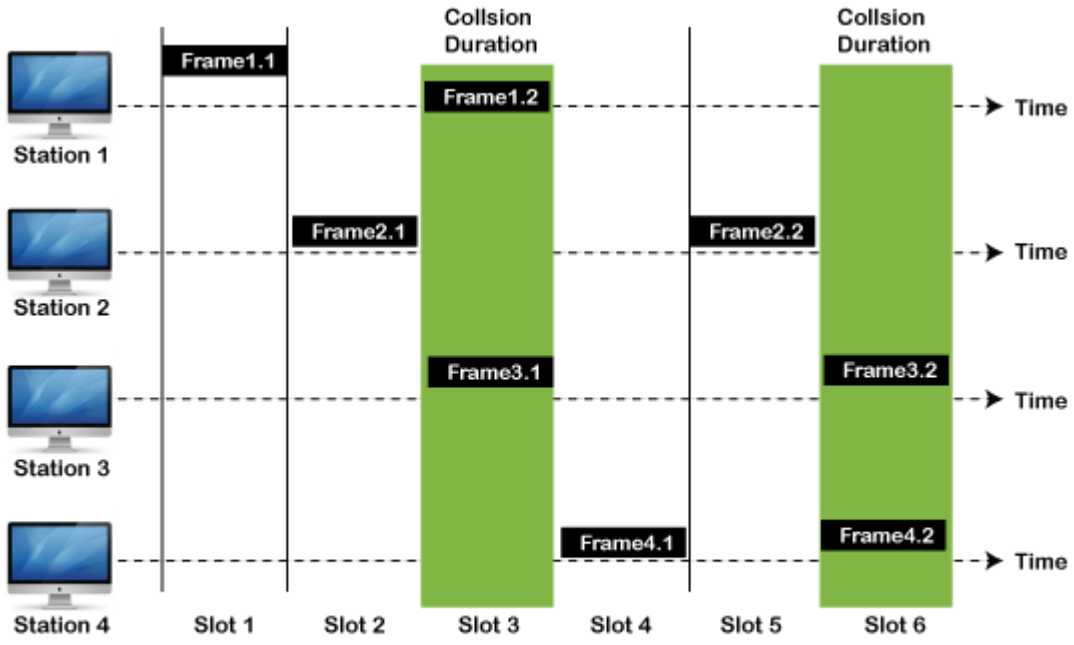
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same 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 ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

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

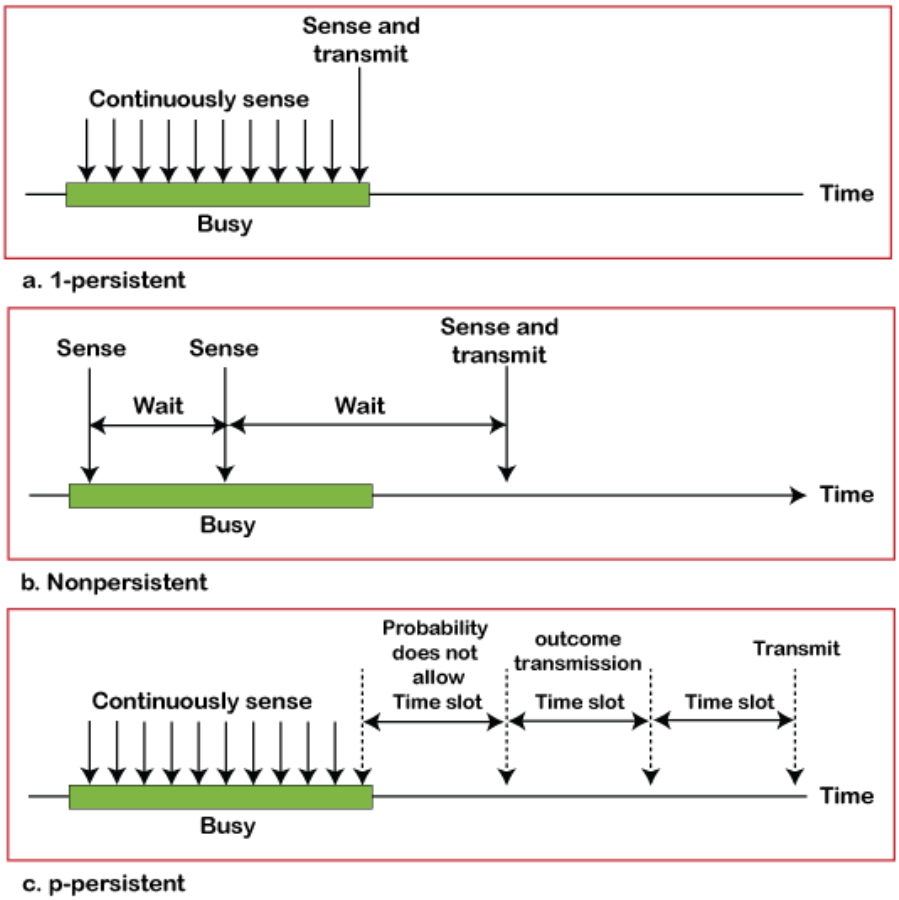
CSMA Access Modes

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

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

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

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols

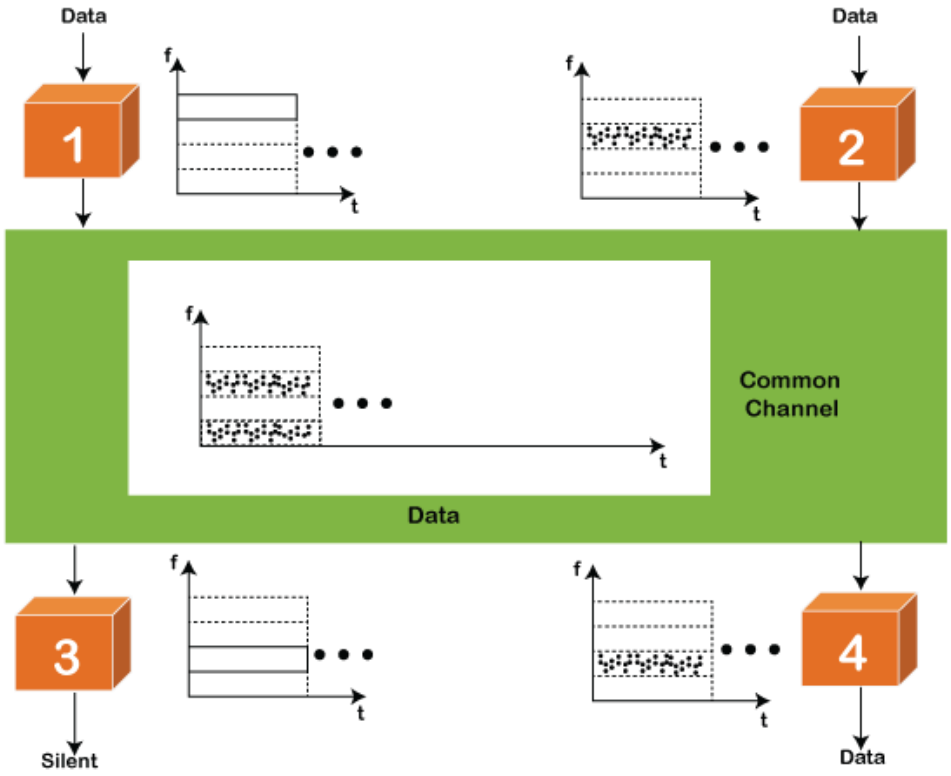
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead

of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.