3. Data Link Layer

The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN. The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time.

Functions of the data link layer

The data link layer has three main functions:

- It handles problems that occur as a result of bit transmission errors.
- It ensures data flows at a pace that doesn't overwhelm sending and receiving devices.
- It permits the transmission of data to Layer 3, the network layer, where it is addressed and routed.

A) Data Link Layer Design Issues

The data link layer is supported to carry out many specified functions like:

1. Services Provided to the Network Layer :

A well defined serve interface in the network layer. The principle service is transferring data from the network layer on source machine to the network layer on destination machine.

2. Framing

- To provide service to the network layer, the data link layer use the service provided by the physical layer.
- The physical layer accepts raw bit stream and attempt to deliver it the destination. If the channel is noisy, the bit received by data link layer is not guaranteed to be error free. Some bits may have different values and number of bits received may be in correct. It is up to the data link layer to detect and correct the errors.
- The data link layer break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted . When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

3. Error Control

The protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames. If the sender receives a positive acknowledgement about a frame, it knows the frame has arrived safely. On the other hand, a negative acknowledgement means that something has gone wrong and the frame must be transmitted again.

4. Flow Control

The source machine must not be send data frames at a rate faster then the destination machines must be can accepted them. This is an important design issue where the sender is running on a fast powerful computer and receiver is running on slow, low-end machine. The receiver may be unable to handle the frames as fast as they are arrive and will lose some. **Two approaches are commonly used for the above issue:**

a. Feedback-based flow control:

In feedback-based flow control, the receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing. The feedback-based flow control is used in higher layers too.

b. Rate-based flow control.

In rate-based flow control, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

What is LLC Layer (logical link control Layer)?

One of the two sublayers into which the data-link layer of the Open Systems Interconnection (OSI) reference model is subdivided for data-link protocols used on local area networks (LANs). "LLC" sometimes refers to the IEEE 802.2 protocol itself, which is the most common LAN protocol implemented at the LLC layer. The LLC layer serves the purpose of providing end to end flow, error control, and multiplexing different protocols over the Mac layer of the data link layer.

General Information from LLC Protocol

- It is also defined as IEEE 802.2by the Institute of Electrical and Electronics Engineers (IEEE)
- It is in change of the communication between the upper Layers (7-3) with the lower layers (2-1)
- It is the communicator between the software and the hardware. The LLC Sub layer (L2 Sub layer)
- It takes the packets (usually IPV4) and adds the necessary control information for the packet to reach the destination
- It is implemented in software and not in hardware. In a PC, it will be the controller that interacts on the NIC
- In Ethernet, it is in charge of multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving)
- In Flow Control, it is in charge of providing node-to-node flow and error control
- When doing Flow control LLC specifies the order in which the frames are sent

How it works

For LAN data-link protocols such as Ethernet, the data-link layer is divided into an upper layer called the logical link control (LLC) layer and a lower layer called the media access control (MAC) layer. The MAC layer coordinates access to the physical layer according to a media access control method, which for Ethernet is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) scheme. The MAC layer thus provides services to the LLC layer so that protocol data units can be transferred to the medium without any concern about the broadcast, framing, addressing, or error-detection schemes used. The LLC uses the MAC services to provide two types of data-link operations to the network layer above it: LLC1 for connectionless and LLC2 for connection-oriented data-link communication services (known as Type 1 and Type 2, respectively). These LLC services are grouped into two classes:

- **Class 1 services:**

Connectionless services used by applications that do not require error detection or flow control.

- **Class 2 services:**

Either connectionless (Type 1) or balanced-mode connection-oriented (Type 2) data transfer services. The LLC provides the error detection and recovery, flow control, and resequencing services needed for connection-oriented data transfer.

B) Media Access Control, MAC ADDRESS

The MAC sublayer acts as an interface between the logical link control (LLC) Ethernet sublayer and Layer 1 (the physical layer). The MAC sublayer emulates a full-duplex logical communication channel in a multipoint network. This channel may provide unicast, multicast, or broadcast communication service. The MAC sublayer uses MAC protocols to prevent collisions.

In Layer 2, multiple devices on the same physical link can uniquely identify one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

A MAC address is a 12-digit hexadecimal number (48 bits in long). MAC addresses are usually written in one of these formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.
Contrast MAC addressing, which works at Layer 2, with IP addressing, which runs at Layer 3 (networking and routing). One way to remember the difference is that the MAC addresses apply to a physical or virtual node, whereas IP addresses apply to the software implementation of that node. MAC addresses are typically fixed on a per-node basis, whereas IP addresses change when the node moves from one part of the network to another.

MAC Frame Format
Since there are various types of Network Interfaces (Ethernet, Token Ring, FDDI etc.) the MAC frame format differs by protocol according to it's design. However most will have at a minimum the following fields:

MAC CONTROL	DESTINATION MAC ADDRESS	SOURCE MAC ADDRESS	LLC PDU	CRC

i. MAC Control Field
The MAC control field contains all information used for flow control, connection establishment and teardown as well as error control. Not all protocols provide for establishment/teardown, flow control and error recovery. The content of this field is dependent upon the specified standards for that particular data link layer protocol (Ethernet, Token Ring, FDDI etc.)

ii. DESTINATION / SOURCE MAC Fields
The source MAC address field contains the MAC address of the source machine--the transmitting device, and the destination device is the receiver. The destination MAC is closer to the 'front' of the frame for easier scanning, mostly because it is the destination device that is important as that is the device we are trying to reach.

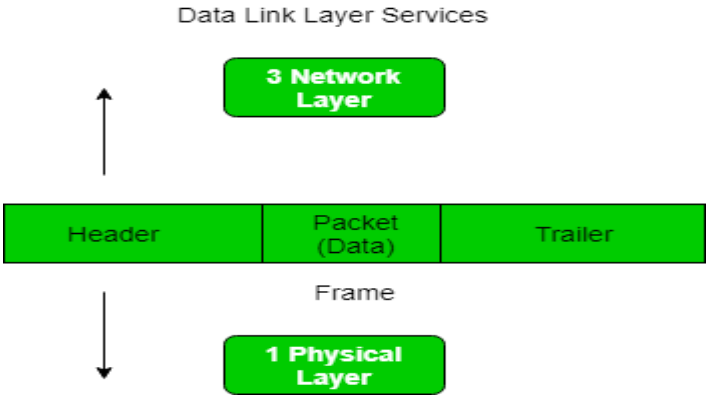
When the receiver responds to the frame, it will use the source address to generate the destination portion of the frame it sends out. In other words, the source MAC in the frame received becomes the destination MAC in the frame transmitted as a response.

iii. LLC PDU Field
The Logical Link Control Packet Data Unit field (LLC PDU) contains data from the from the LLC sub-layer of the data link layer. The LLC information is used to keep track of which piece of data is sent to which IP address and application. For example, the LLC information helps a web browser keep track of which data being received is part of an image in a web page, and which data is the text in the body of the web page itself.

iv. CRC Checksum Field
This field contains what is called a 'checksum' that is the product of a Cyclic Redundancy Check (CRC check). A CRC check is a mathematical formula that uses the data as input and produces a numeric result that is almost as unique as the input data. Using the CRC checksum value it is possible to verify the the integrity of the frame.

C) Farming Methods

Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes. Framing is process of dividing large stream of data into frames.



At data link layer, it extracts message from sender and provide it to receiver by providing sender's and receiver's address. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

Problems in Framing –

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

Types of framing – There are two types of framing:

1. **Fixed size:**
   The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter.
   - **Drawback:** It suffers from internal fragmentation if data size is less than frame size
   - **Solution:** Padding

2. **Variable size:**

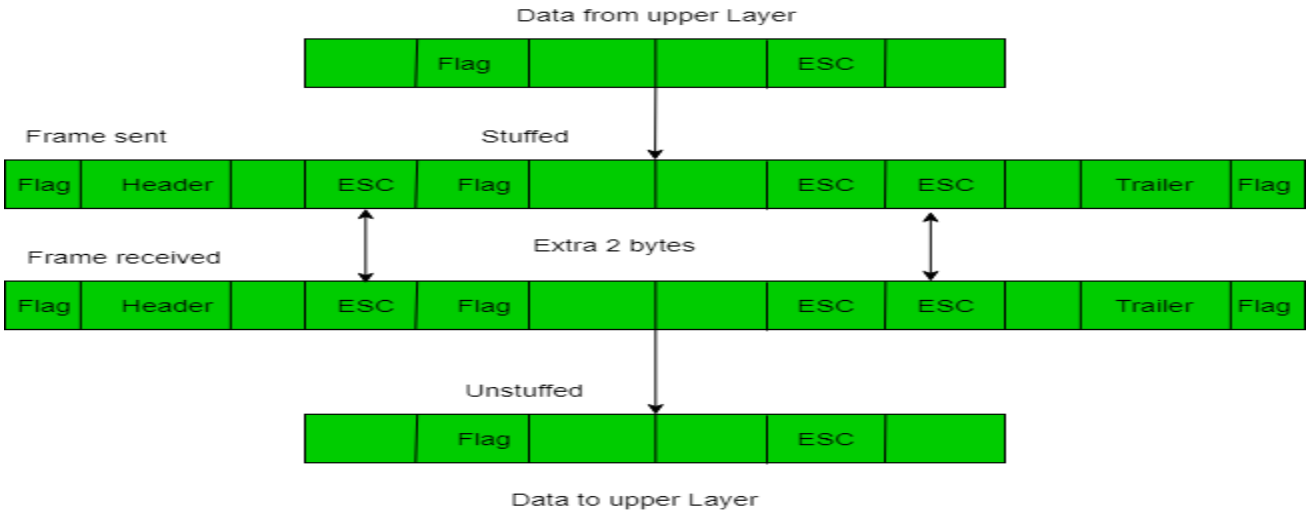
In this there is need to define end of frame as well as beginning of next frame to distinguish.

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

This can be done in two ways:

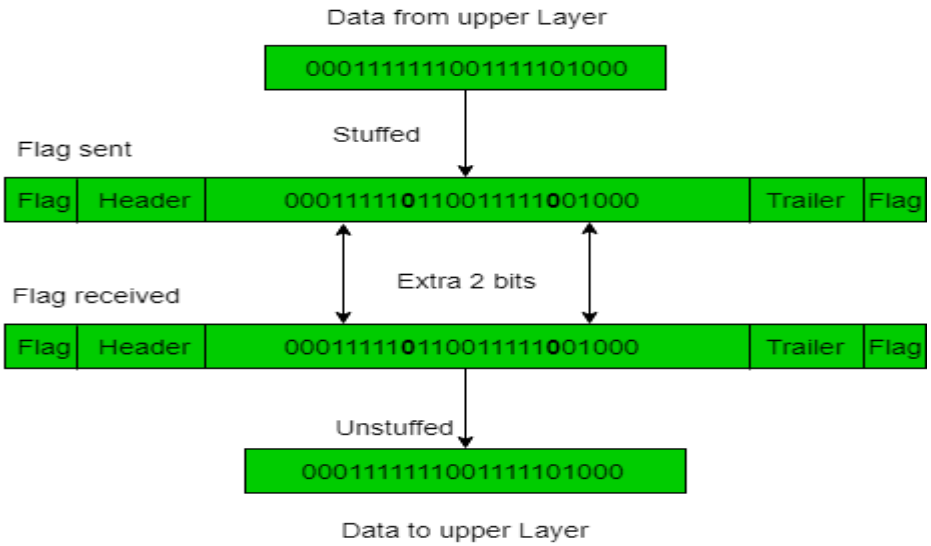
1. **Character count:**
   It is the process of putting frame no in middle of large stream of data to differentiate frames.
   If the frame no is removed(error occurred/noise) then remaining frames will be jumbled up.

2. **Character/Byte Stuffing:**
   Flag are used to represent start and ending of frames. But if flag is a data in frame then it may be misunderstood for frame end. So ESC is used/stuffed to escape and flag. And Esc is also data then another esc can be user before it to make it as data. E.g: ESC ESC.
   Used when frames consist of character. If data contains ED then, byte is stuffed into data to diffentiate it from ED.



   Disadvantage – It is very costly and obsolete method.

3. **Bit Stuffing:**
   Automatically put bit in between frame bits if the data and break pattern(end/start flag) is same.
   Let ED = 01111 and if data = 01111
   –> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data = 0111**0**1.
   –> Receiver receives the frame.
   –> If data contains 01110**1**, receiver removes the 0 and reads the data.



D) Error Control (Detection and Correction)

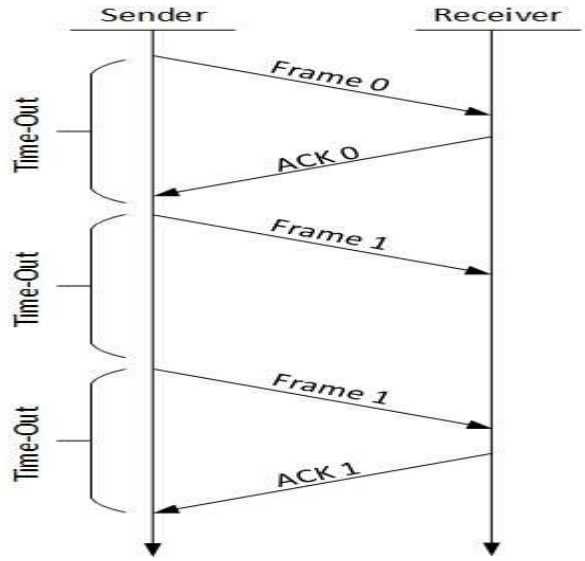
When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

1. Stop-and-wait ARQ

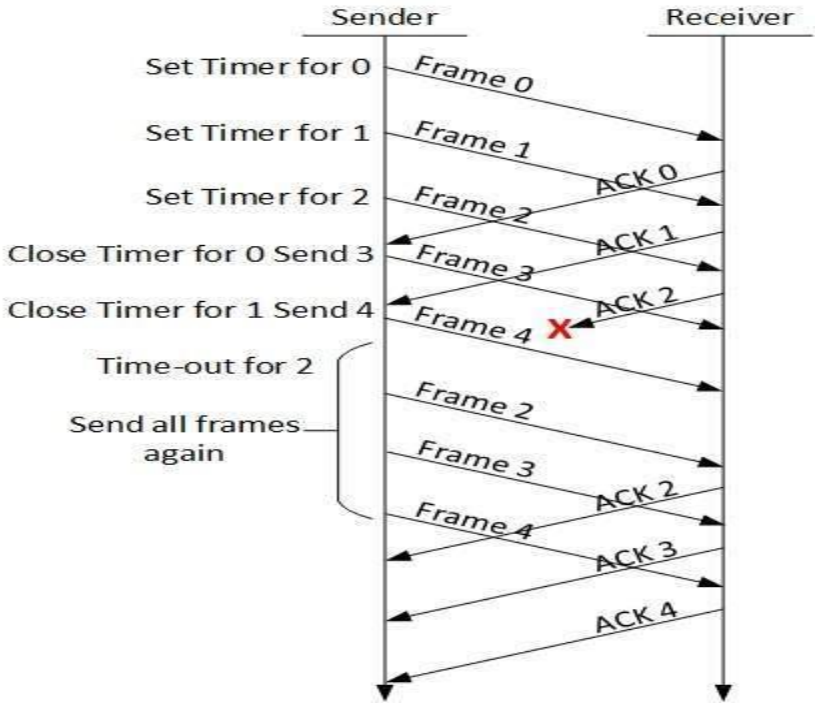


The following transition may occur in Stop-and-Wait ARQ:

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

2. Go-Back-N ARQ

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

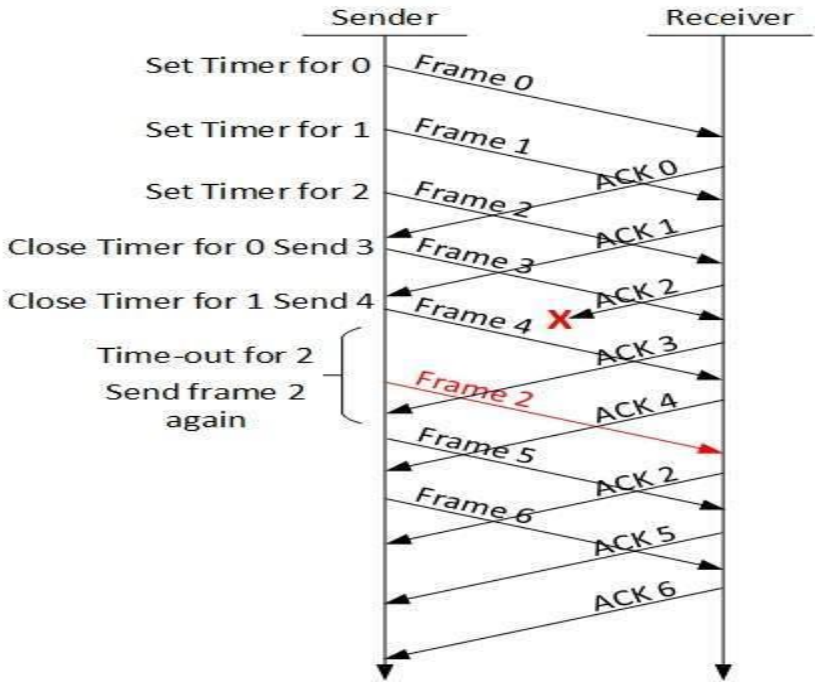


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

3. Selective Repeat ARQ

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



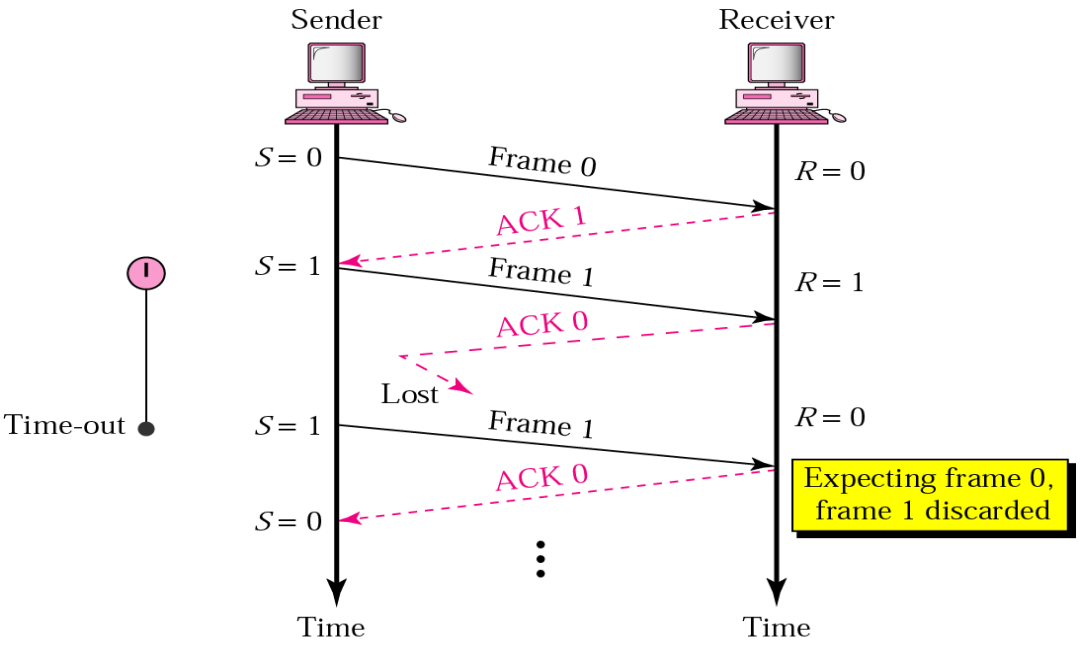
In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.
The sender in this case, sends only packet for which NACK is received.

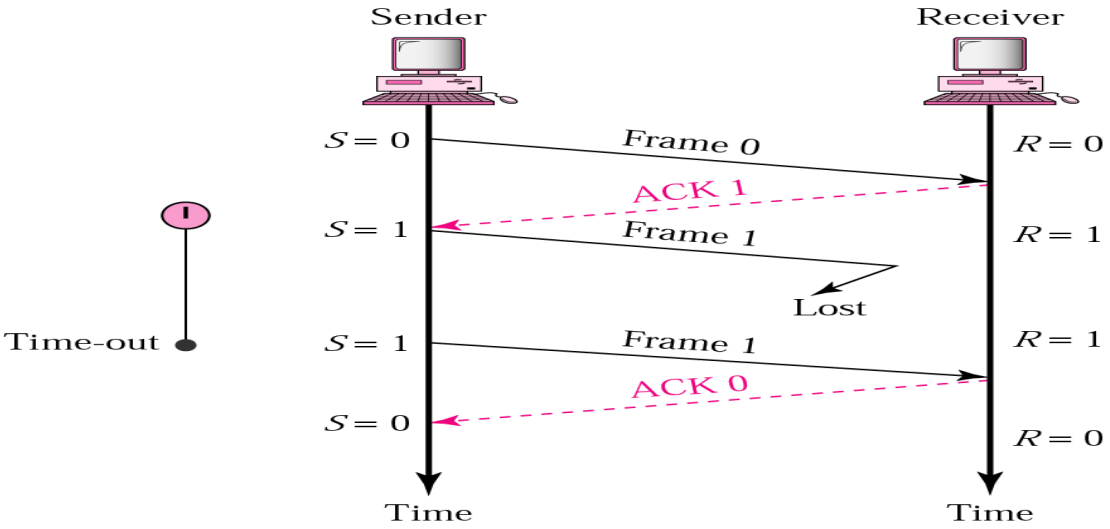
E) FLOW CONTROL

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.
Two types of mechanisms can be deployed to control the flow:

1. Stop and Wait

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



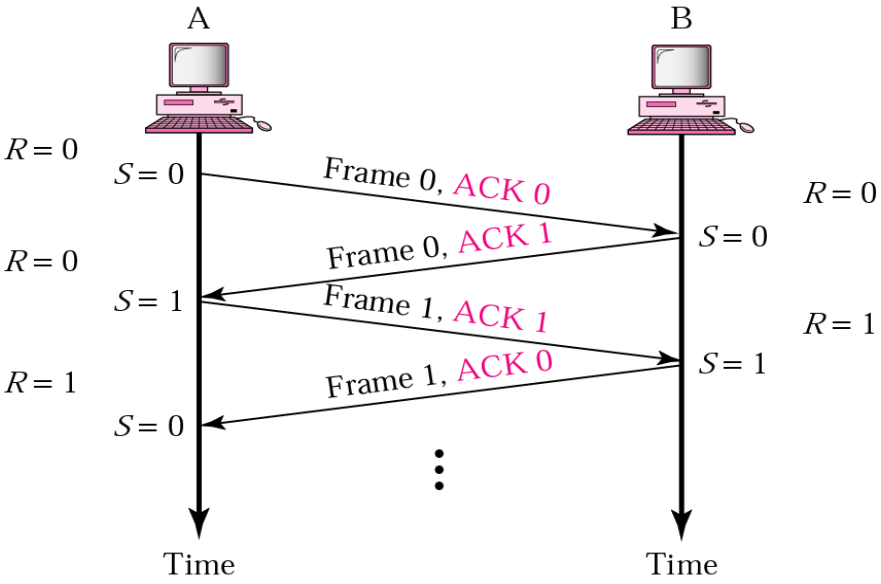


Piggybacking

A method to combine a data frame with ACK.

Station A and B both have data to send.

Instead of sending separately, station A sends a data frame that includes an ACK



Solution for timing complexion

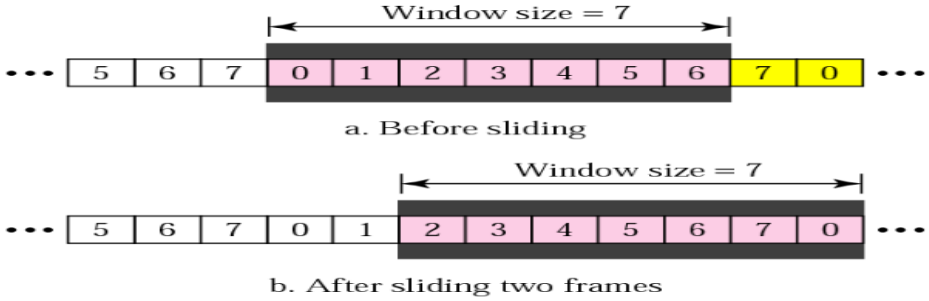
- If a new packet arrives quickly
  - Piggybacking
- If no new packet arrives after a receiver ack timeout
  - Sending a separate acknowledgement frame

2. Sliding Window

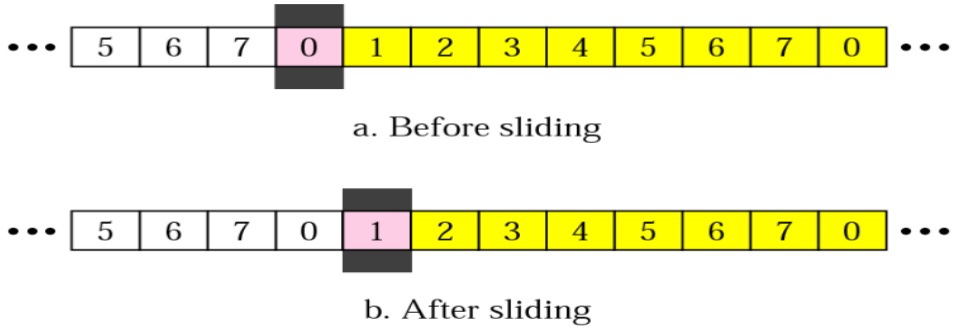
In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

- Both the sender and receiver maintain a finite size buffer to hold outgoing and incoming packets from the other side.
- Every Packet sent by the sender must acknowledged by the receiver. The sender maintains a timer for every packet sent and any packet unacknowledged in certain time is resent.
- Effeciency can also be improved by making use of full-duplex line
- Sender maintains a set of sequence numbers of frames permitted to send
  - These frames fall within sending window
- Receiver maintains a set of sequence numbers of frames permitted to accept
  - These frames fall within receiving window

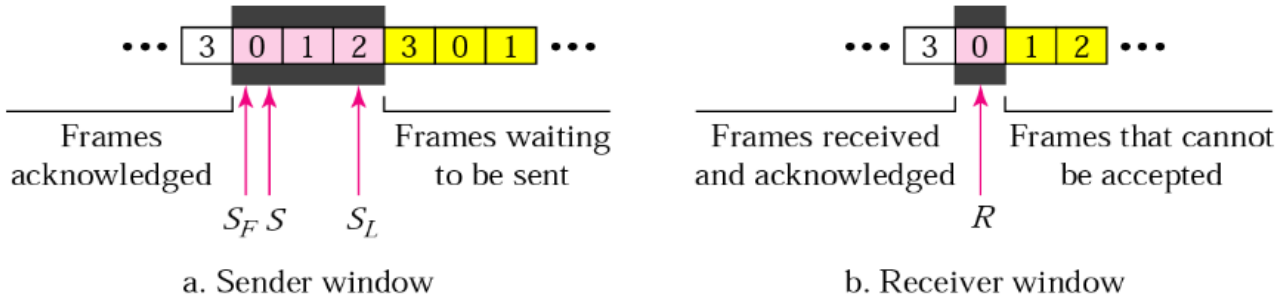
Sender Sliding Window:



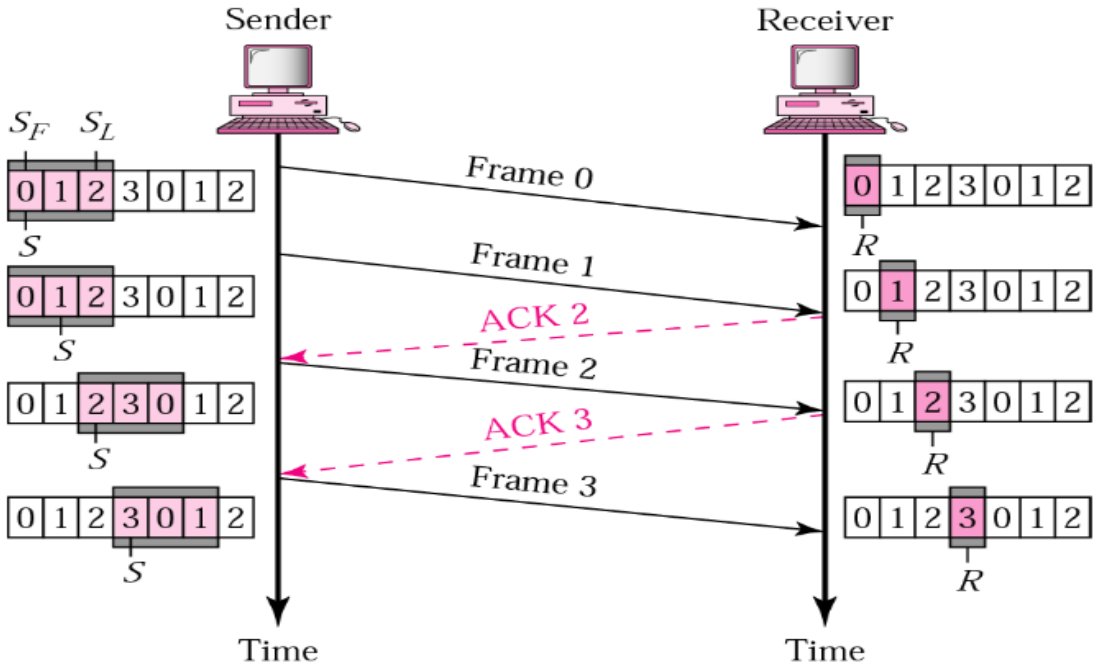
Receiver Sliding Window:



Control Variables:



Normal Operation:



"Go-Back-N Protocol and "Selective Repeat Protocol" are the sliding window protocols. The sliding window protocol is primarily an error control protocol, i.e. it is a method of error detection and error correction. The basic difference between go-back-n protocol and selective repeat protocol is that the "go-back-n protocol" retransmits all the frames that lie after the frame which is damaged or lost. The "selective repeat protocol" retransmits only that frame which is damaged or lost.

BASIS	GO-BACK-N	SELECTIVE REPEAT
Basic	Retransmits all the frames that sent after the frame which suspects to be damaged or lost.	Retransmits only those frames that are suspected to lost or damaged.
Bandwidth Utilization	If error rate is high, it wastes a lot of bandwidth.	Comparatively less bandwidth is wasted in retransmitting.
Complexity	Less complicated.	More complex as it require to apply extra logic and sorting and storage, at sender and receiver.
Window size	N-1	<= (N+1)/2
Sorting	Sorting is neither required at sender side nor at receiver side.	Receiver must be able to sort as it has to maintain the sequence of the frames.
Storing	Receiver do not store the frames received after the damaged frame until the damaged frame is retransmitted.	Receiver stores the frames received after the damaged frame in the buffer until the damaged frame is replaced.
Searching	No searching of frame is required neither on sender side nor on receiver	The sender must be able to search and select only the requested frame.
ACK Numbers	NAK number refer to the next expected frame number.	NAK number refer to the frame lost.
Use	It more often used.	It is less in practice because of its complexity.

a) Go-Back-N

Go-Back-N protocol is a sliding window protocol. It is a mechanism to detect and control the error in datalink layer. During transmission of frames between sender and receiver, if a frame is damaged, lost, or an acknowledgement is lost then the action performed by sender and receiver is explained in the following content.

i. Damaged Frame

If a receiver receives a damaged frame or if an error occurs while receiving a frame then, the receiver sends the NAK (negative acknowledgement) for that frame along with that frame number, that it expects to be retransmitted. After sending NAK, the receiver discards all the frames that it receives, after a damaged frame. The receiver does not send any ACK (acknowledgement) for the discarded frames. After the sender receives the NAK for the damaged frame, it retransmits all the frames onwards the frame number referred by NAK.

ii. Lost frame

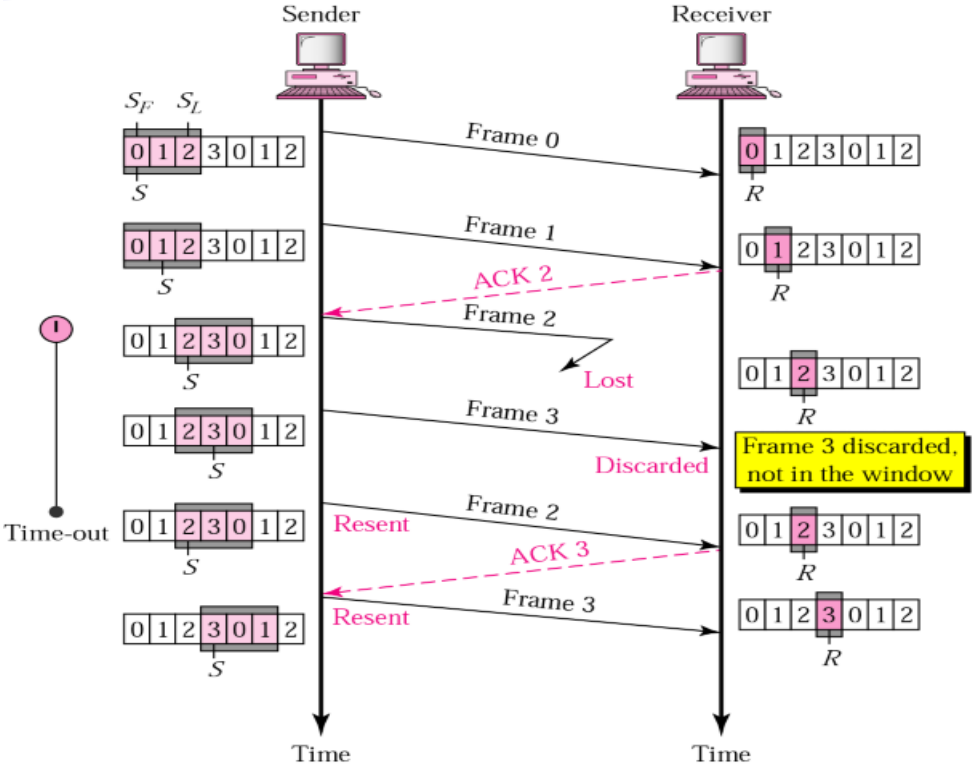
The receiver checks the number on each frame, it receives. If a frame number is skipped in a sequence, then the receiver easily detects the loss of a frame as the newly received frame is received out of sequence. The receiver sends the NAK for the lost frame and then the receiver discards all the frames received after a lost frame. The receiver does not send any ACK (acknowledgement) for that discarded frames. After the sender receives the

NAK for the lost frame, it retransmits the lost frame referred by NAK and also retransmits all the frames which it has sent after the lost frame.

iii. Lost Acknowledgement

If the sender does not receive any ACK or if the ACK is lost or damaged in between the transmission. The sender waits for the time to run out and as the time run outs, the sender retransmits all the frames for which it has not received the ACK. The sender identifies the loss of ACK with the help of a timer.

The ACK number, like NAK (negative acknowledgement) number, shows the number of the frame, that receiver expects to be the next in sequence. The window size of the receiver is 1 as the data link layer only require the frame which it has to send next to the network layer. The sender window size is equal to 'w'. If the error rate is high, a lot of bandwidth is lost wasted.



b) Selective Repeat

Selective repeat is also the sliding window protocol which detects or corrects the error occurred in datalink layer. The selective repeat protocol retransmits only that frame which is damaged or lost. In selective repeat protocol, the retransmitted framed is received out of sequence. The selective repeat protocol can perform following actions

- The receiver is capable of sorting the frame in a proper sequence, as it receives the retransmitted frame whose sequence is out of order of the receiving frame.
- The sender must be capable of searching the frame for which the NAK has been received.
- The receiver must contain the buffer to store all the previously received frame on hold till the retransmitted frame is sorted and placed in a proper sequence.
- The ACK number, like NAK number, refers to the frame which is lost or damaged.
- It requires the less window size as compared to go-back-n protocol.

i. Damaged frames

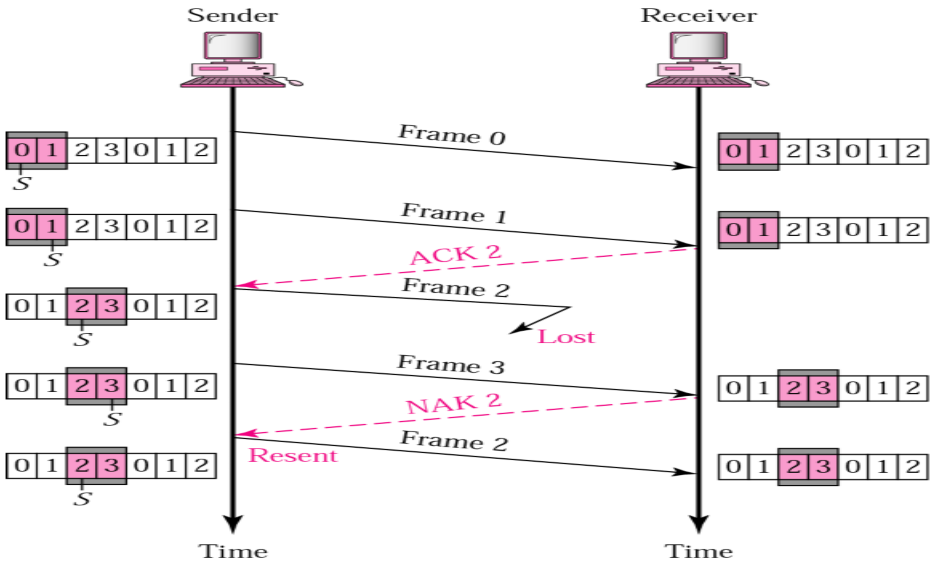
If a receiver receives a damaged frame, it sends the NAK for the frame in which error or damage is detected. The NAK number, like in go-back-n also indicate the acknowledgement of the previously received frames and error in the current frame. The receiver keeps receiving the new frames while waiting for the damaged frame to be replaced. The frames that are received after the damaged frame are not be acknowledged until the damaged frame has been replaced.

ii. Lost Frame

As in a selective repeat protocol, a frame can be received out of order and further they are sorted to maintain a proper sequence of the frames. While sorting, if a frame number is skipped, the receiver recognize that a frame is lost and it sends NAK for that frame to the sender. After receiving NAK for the lost frame the sender searches that frame in its window and retransmits that frame. If the last transmitted frame is lost then receiver does not respond and this silence is a negative acknowledgement for the sender.

iii. Lost Acknowledgement

If the sender does not receive any ACK or the ACK is lost or damaged in between the transmission. The sender waits for the time to run out and as the time run outs, the sender retransmit all the frames for which it has not received the ACK. The sender identifies the loss of ACK with the help of a timer.



F) Data Link Layer Protocols: (HDLC,SLIP,PPP)

1. HDLC:

High-Level Data Control, also known as HDLC, is a bit oriented, switched and non-switched protocol. It is a data link control protocol, and falls within layer 2, the Data Link Layer of the Open Systems Interface (OSI) model. The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct errors.

It has been so widely implemented because it supports both half duplex and full duplex communication lines, point to point(peer to peer) and multi-point networks, and switched or non-switched channels. The procedures outlined in HDLC are designed to permit synchronous, code-transparent data transmission. Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors. It is fast as it has header of one vendor only. Some devices don't work with different vendors. It is point-to-point and proprietary but provides no authentication.

HDLC three station types:

- **Primary Station:** Responsible for controlling the operation of data flow in the link. Frame by this is Command.
- **Secondary Station:** Operates under the control of primary station. Frame issued by a secondary is called response.
- **Combined Station:** Combines the features of primary and secondary.

The Two Link Configuration are:

- **Unbalanced Configuration:** Consists of one primary and one or more secondary stations and supports both full and half duplex transmission.
- **Balanced configuration:** Consists of two combined stations and supports both full and half duplex.

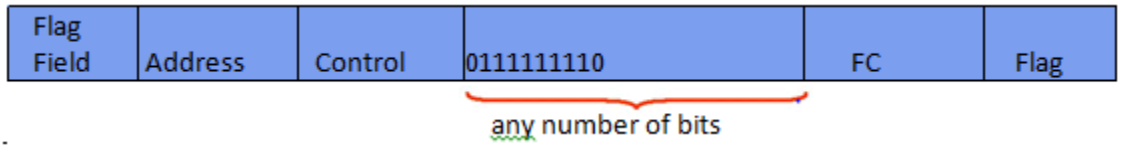
The Three Transfer Modes are:

- **Normal unbalanced/Normal Response Mode(NRM):** The secondary station responds only to the primary station.
- **Asynchronous**: The secondary station can initiate a message.
- **Asynchronous balanced**: Both stations send and receive over its part of a duplex line.

Types of Frames in HDLC

HDLC Frame Structure:

HDLC uses the term "frame" to indicate an entity of data (or a protocol data unit) transmitted from one station to another. Figure below is a graphical representation of a HDLC frame with an information field.



Field Name	Size(in bits)
Flag Field(F)	8 bits
Address Field(A)	8 bits
Control Field(C)	8 or 16 bits
Information Field(I)	Variable; Not used in **Supervisory frame**
Frame Check Sequence(FCS)	16 or 32 bits
Closing Flag Field(F)	8 bits

1. Information frames

Information frames, or I-frames, transport user data from the network layer in the information field. In addition they can also include flow and error control information piggybacked on data.

2. Supervisory frame

Supervisory Frames, or S-frames, are used for flow and error control whenever piggybacking is impossible or inappropriate, such as when a station does not have data to send. S-frames do not have information fields.

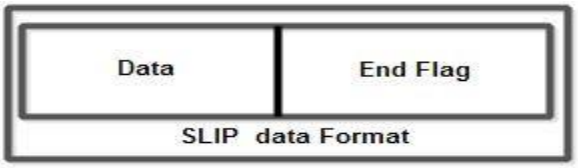
3. Unnumbered frame

- Unnumbered frames, or U-frames, are used for various miscellaneous purposes, including link management. Some U-frames contain an information field, depending on the type.
- U-frames are used to exchange session management and control information between the two connected devices.
- Information field in U-frame does not carry user information rather, it carries system management information.

2. Serial Line Internet Protocol (SLIP)

SLIP is an internet connection protocol that does not execute an error control or an address which makes it obsolete when compared to other protocols. It is the encasing of internet protocols which operate over the modem connections and serial ports. Before it is established, it will require you to set the configuration of an IP address.

The data format of SLIP is shown in fig.



A special END character (equivalent to decimal 192) marks the end of data. If an End character occurs naturally in data, SLIP includes a special ESC character before the END character so that receiving computer does not prematurely stop receiving the packet.

It has a small overhead which makes it suitable for enclosing internet protocol packets. It has existed since the 80s for limited modem communications to 2400 bps. Its primary purpose was to allow easier transmissions across serial lines. It supports asynchronous links and can be effective on RS-232 serial ports.
The dial-up linkage to the server is based upon a slower serial line. It is not associated with the multiplex or parallel lines in which you may need to establish the connection. Workstations are capable of transmitting internet protocol packets over the line at the termination for the purposes of framing. Character staffing is used for solving the problem in situations where the flag byte (OXCO) transpires within the IP packet. In situations where the issue arises, then the two byte sequence is transmitted to provide a replacement. They include OXDB and OXDC.

Although SLIP is the simple protocol but it has some major problems. These are:

- It does not perform any error detection and correction.
- SLIP support only IP (Internet Protocol). So it cannot be used for other networks that do not make use of IP (for *e.g.* Novell LANs).
- It does not Support the allocation of dynamic IP address. Both the communication sites should be assigned a specific IP address before hand and both sites should know each other's address.
- SLIP does not provide any authentication. So both the communicating sites do not know with whom they are communicating.
- SLIP is not an approved Internet standard; so many different and incompatible versions exist that makes networking difficult.

3. Point-to-Point Protocol (PPP)

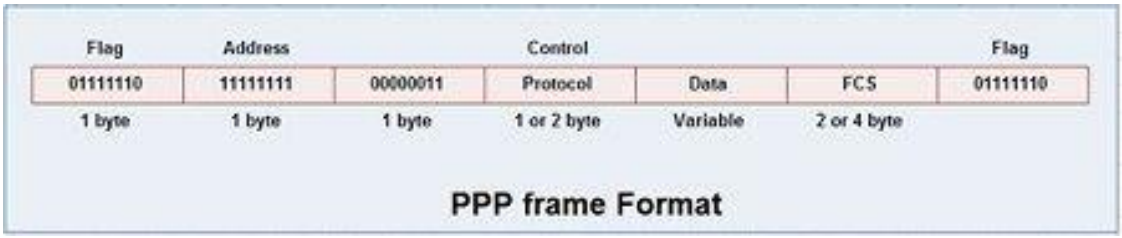
The Point-to-Point Protocol (PPP) is the default RAS protocol in Windows and is a data link-layer protocol used to encapsulate higher network-layer protocols to pass over synchronous and asynchronous communication lines. PPP was originally designed as an encapsulation protocol for transporting multiple network layer traffic over point-to-point links. PPP also established other standards, including asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, session negotiation, and data-compression negotiation. PPP also supports protocols other than TCP/IP, such as IPX/SPX and DECnet. It provides point-to-point authentication, compression and also supports multivendor.

This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

a) PPP defines the format of the frame to be exchanged between the devices.
b) It defines link control protocol (LCP) for:-
   i. Establishing the link between two devices.
   ii. Maintaining this established link.
   iii. Configuring this link.
   iv. Terminating this link after the transfer.
c) It defines how network layer data are encapsulated in data link frame.
d) PPP provides error detection.
e) Unlike SLIP that supports only IP, PPP supports multiple protocols.
f) PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.
g) PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).
h) It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



PPP frame Format

a) **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).
b) **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address i.e. all the stations accept this frame.
c) **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.
d) **Protocol field**: This field specifies the kind of packet in the data field i.e. what is being carried in data field.
e) **Data field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.
f) **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Components of PPP

To make PPP a successful protocol, there are certain essential components which form the basic building blocks of this protocol.

A. Encapsulation in PPP

Point to point protocol encapsulates the network layer packets in its frames. The fact that PPP can encapsulate any network layer packet makes PPP layer three protocol independent and also capable of carrying multiple Layer three packets over a single link.

B. Link Control Protocol

Link Control Protocol is the second component of PPP. The main purpose of LCP is to build and maintain data-link connections. Below are some of the functionalities of this sub-protocol:

i. PPP Authentication

PPP uses its Authentication method to identify the remote device.

ii. Compression

Link Control Protocol (LCP) uses compression to increase overall data transmission speed while saving bandwidth at the same time. LCP compresses data at the sending end and decompresses the same at the receiving end.

iii. Error Detection

LCP utilizes a tool called LQM (Link Quality Monitoring) to monitor different interfaces for their error percentage.

iv. Multilink

LCP can combine two physical links logically in such a way that they seem a single logical connection at layer three, i.e., the network layer. For example, if there are two connections of 128 Kbps then multilink will combine them in such a way that at layer three, they appear as one 256 Kbps connection.

v. Loop Detection

Point to point protocol is also famous for detecting the looped connections. To detect a loop, a node, while sending the PPP LCP messages, might also tag along with a magic number. If the line is looped, the node will get back its sent magic number in return. Otherwise, the node gets the peer's magic number.

C. Network Control Protocol (NCP)

We already know that PPP works in data link layer of the OSI model. The data which comes from the upper layers such as Transport Layer or Network Layer has to be fully compatible with the PPP. For the same purpose, NCP was discovered.

G) ALOHA, CSMA/CD, FDDI, Token Ring, Token Bus and IEEE802.3, 802.4, 802.5

1. ALOHA

ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

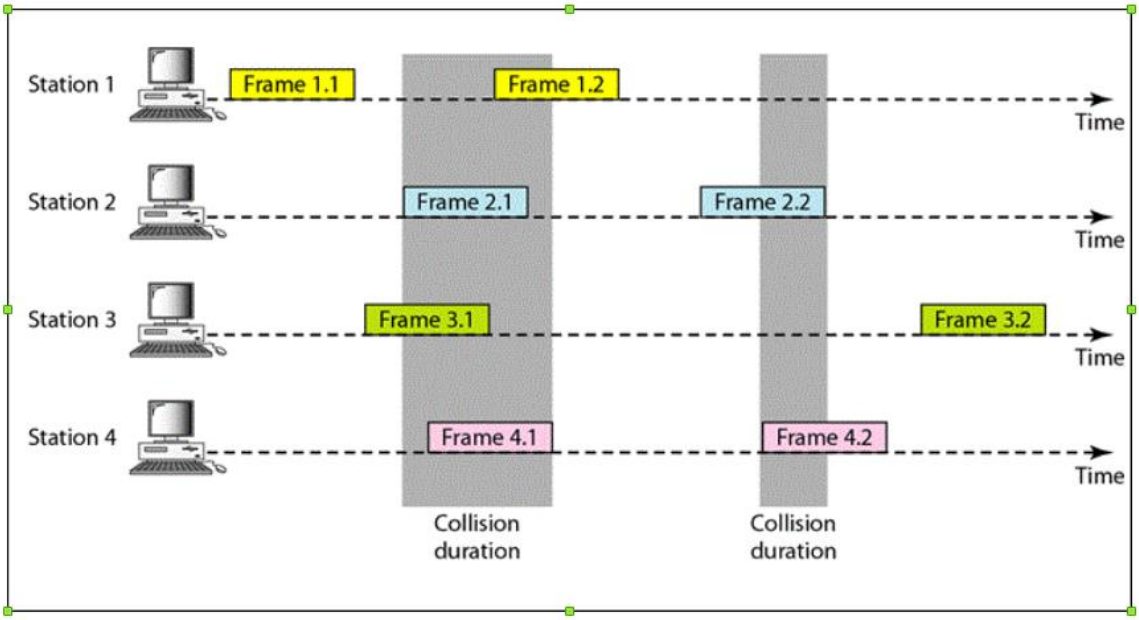
A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA

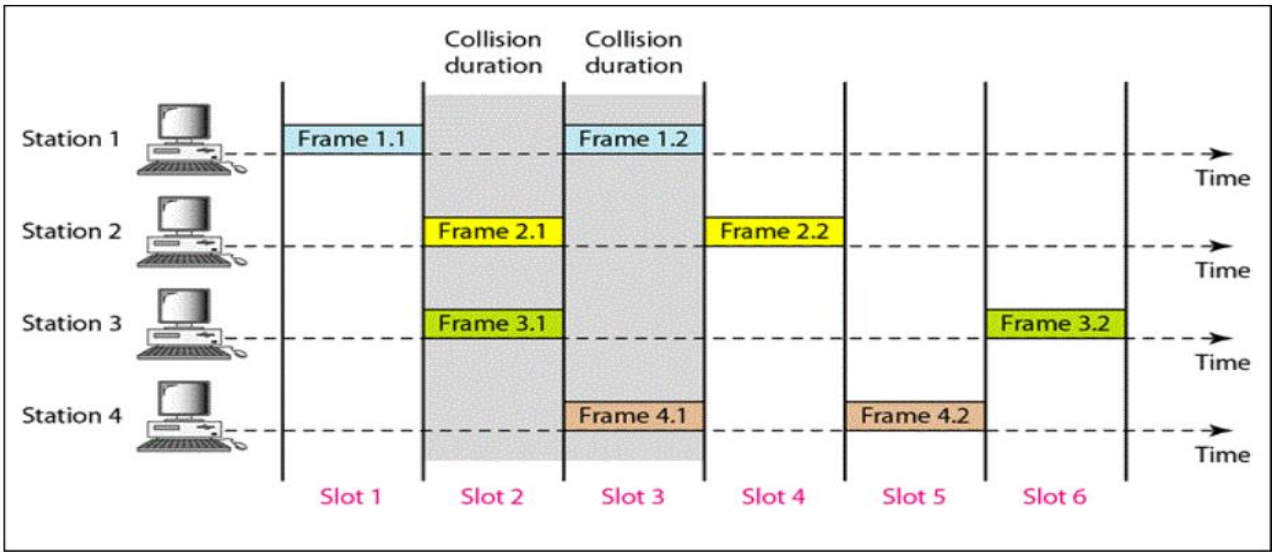
a) Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time. Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax' a station must give up and try later. The efficiency is 18%.



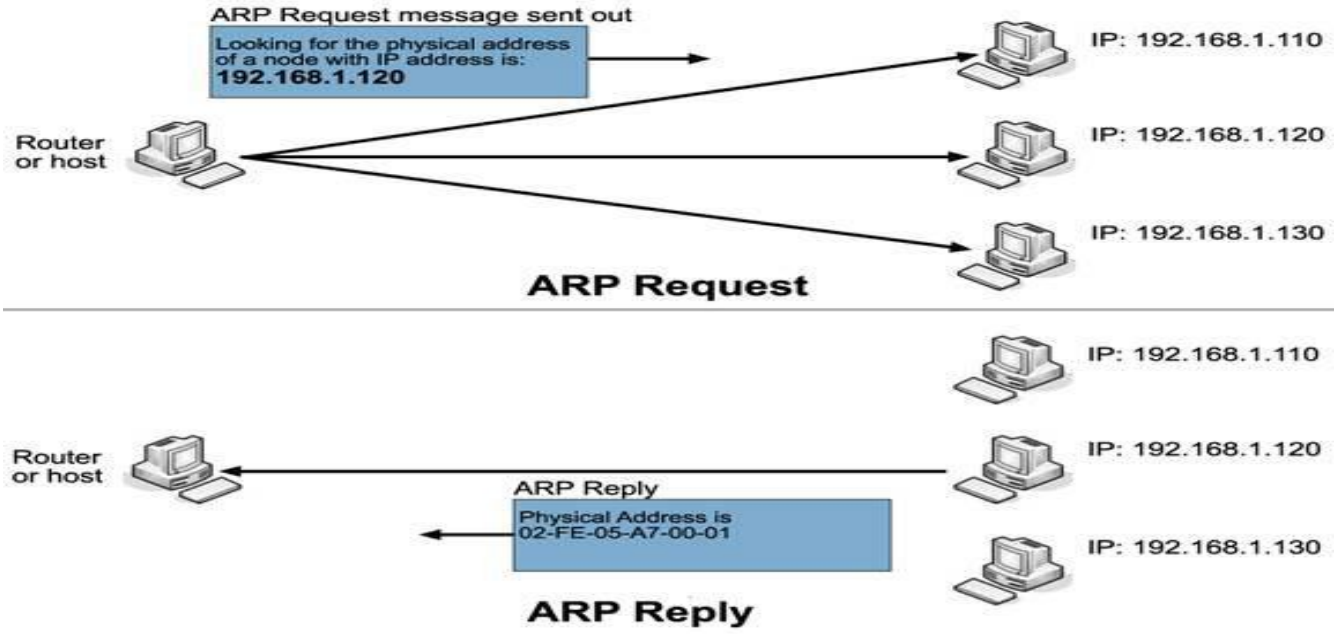
b) Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 x Tfr . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots and force the station to send only at the beginning of the time slot. Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, the efficiency is at 36%.

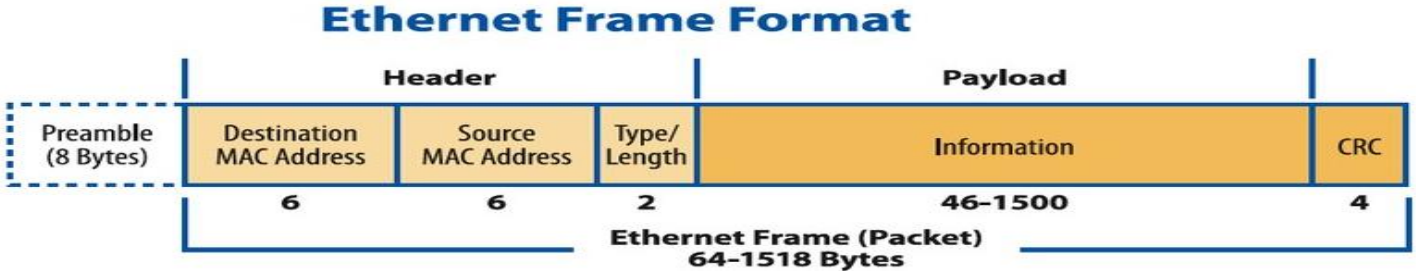


Address Resolution Protocol

The Address Resolution Protocol (ARP) is used to dynamically discover the mapping between a layer 3 (protocol) and a layer 2 (hardware) address. A typical use is the mapping of an IP address (e.g. 192.168.0.10) to the underlying Ethernet address (e.g. 01:02:03:04:05:06). A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address.



2. Ethernet (802.3)



802.3 (Carrier Sense Multiple Access/ Collision Detection)/ Ethernet CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media-access control method widely used in Ethernet technology/LANs.

Consider a scenario where there are 'n' stations on a link and all are waiting to transfer data through that channel. In this case all 'n' stations would want to access the link/channel to transfer their own data. Problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.

CSMA/CD is one such technique where different stations that follow this protocol agree on some terms and collision detection measures for effective transmission. This protocol decides which station will transmit when so that data reaches the destination without corruption.

How CSMA/CD works?

Step 1 **:** Check if the sender is ready for transmitting data packets.

Step 2 **:** Check if the transmission link is idle?

Sender has to keep on checking if the transmission link/medium is idle. For this it continously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise it refrains from sending data. And start random timer before sending data.

Step 3 **:** Transmit the data & check for collisions.

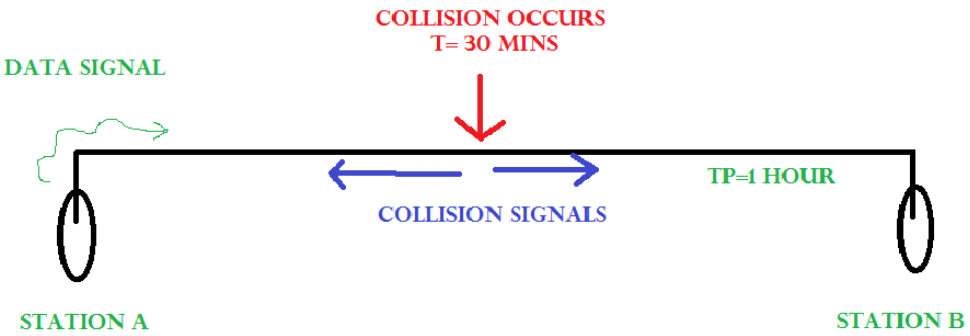
Sender transmits its data on the link. CSMA/CD does not use 'acknowledgement' system. It checks for the successful and unsuccessful transmissions through collision signals. During transmission, if collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time interval before it resends the frame. After some random time, it again attempts to transfer the data and repeats above process.

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

Different protocol standards for different speeds of communication

- 10G bps Ethernet : IEEE 802.3z
- 1G bps Ethernet: IEEE 802.3ab
- 100M bps Ethernet: IEEE 802.3u
- 10M bps Ethernet: IEEE 802.3

How a station knows if its data collides?



Consider the above situation. Two stations, A & B.
Propagation Time: Tp = 1 hr (Signal takes 1 hr to go from A to B)
At time t=0, A transmits its data.
t= 30 mins : Collision occurs.
After collision occurs, a collision signal is generated and sent to both A & B to inform the stations about collision. Since the collision happened midway, the collision signal also takes 30 minutes to reach A & B. This collision signal is received by all the stations on that link.

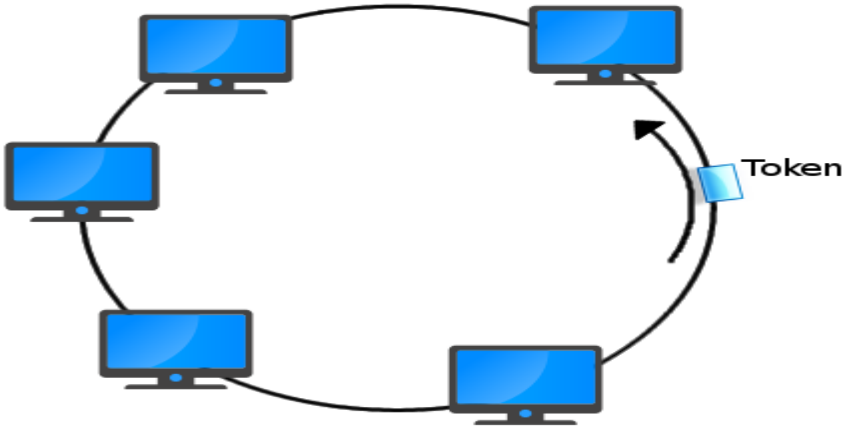
3. 802.5 (Token Ring)

Token Ring protocol is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. The stations are connected to one another in a single ring. It uses a special three-byte frame called a **"token"** that travels around a ring. It makes use of Token Passing controlled access mechanism. Frames are also transmitted in the direction of the token. This way they will circulate around the ring and reach the station which is the destination.

- A number of stations connected by transmission links in a ring topology.
- Information flows in one direction along the ring from source to destination and back to source.
- Medium access control is provided by a small frame, the token, that circulates around the ring when all stations are idle. Only the station possessing the token is allowed to transmit at any given time.
- When a station wishes to transmit, it must wait for token to pass by and seize the token.
  - One approach: change one bit in token which transforms it into a "start-of-frame sequence" and appends frame for transmission.
  - Second approach: station claims token by removing it from the ring.
- Frame circles the ring and is removed by the transmitting station.
- Each station interrogates passing frame, if destined for station, it copies the frame into local buffer. {Normally, there is a one bit delay as the frame passes through a station.}
- Maximum number of stations is 250.
- Waits for last byte of frame to arrive before reinserting token on ring.
- Priority levels provided via two 3-bit fields (priority and reservation) in data and token frames.
- Permits 16-bit and 48-bit addresses (same as 802.3).
- Problems:
  - Loss of token (no token circulating)
  - Duplication of token (forgeries or mistakes)
  - The need to designate one station as the active ring monitor.
  - Persistently circulating frame
  - Deal with active monitor going down.

Prerequisite:-

- **Topology –** Ring topology
- **Transmission –** Unidirectional
- **Encoding –** Differential Manchester encoding
- **Access control –** Token passing
- **Data rates –** 4 Mbps, 16 Mbps



Token Ring Frame format:

Data Frame

SFD	AC	FC	DA	SA	Data	CRC	ED	FS
1	1	1	6	6	>= 0	1	1	1

Token Frame

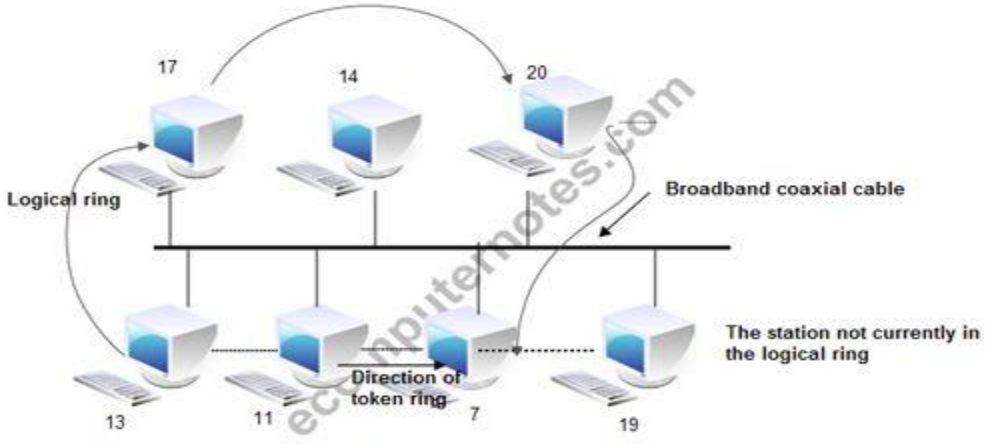
SFD	AC	ED
1	1	1

- **Start frame delimiter (SFD) –** Alerts each station for the arrival of token(or data frame) or start of the frame. It is used to synchronize clocks.
- **Access control (AC)**
- **Frame control (FC) –** First 2 bits indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- **Destination address (DA) and Source address (SA) –** consist of two 6-byte fields which is used to indicate MAC address of source and destination.
- **Data –** Data length can vary from 0 to maximum token holding time (THT) according to token reservation strategy adopted. Token ring imposes no lower bound on size of data i.e. an advantage over Ethernet.
- **Cyclic redundancy check (CRC) –** 32 bit CRC which is used to check for errors in the frame, i.e., whether the frame is corrupted or not. If the frame is corrupted, then its discarded.
- **End delimiter (ED) –** It is used to mark the end of frame. In Ethernet, length field is used for this purpose. It also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence.
- **Frame status (FS) –** It Is a 1-byte field terminating a data frame.

4. IEEE 802.4 Token Bus :

A token bus network is similar to a token ring network in that a station must have possession of a token before it can transmit on the network. However, the topology and token-passing method are different. The IEEE 802.4 Committee has defined token bus standards as broadband networks, as opposed to Ethernet's baseband transmission technique.

The topology of the network can include groups of workstations connected by long trunk cables. These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance. IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology. The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

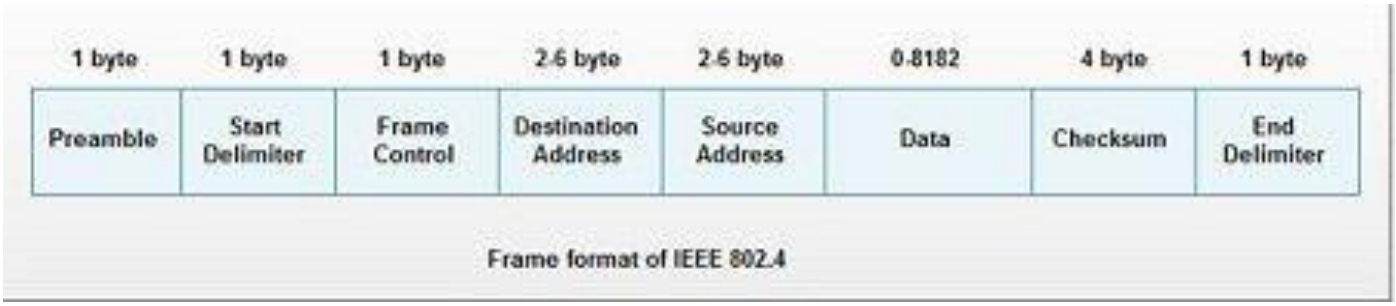


A Token Bus

MAC Sublayer Function

- When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.
- Token passing is done from high to low address.
- Whenever a station acquires the token, it can transmit frames for a specific amount of time.
- If a station has no data, it passes the token immediately upon receiving it.
- The token bus defines four priority classes, 0, 2, 4, and 6 for traffic, with 0 the lowest and 6 the highest.
- Each station is internally divided into four substations, one at each priority level *i.e.* 0,2,4 and 6.
- As input comes in to the MAC sublayer from above, the data are checked for priority and routed to one of the four substations.
- Thus each station maintains its own queue of frames to be transmitted.
- When a token comes into the station over the cable, it is passed internally to the priority 6 substation, which can begin transmitting its frames, if it has any.
- When it is done or when its time expires, the token is passed to the priority 4 substation, which can then transmit frames until its timer expires. After this the token is then passed internally to priority 2 substation.
- This process continues until either the priority 0 substation has sent all its frames or its time expires.
- After this the token is passed to the next station in the ring.

Frame format of Token Bus



Frame format of IEEE 802.4

The various fields present in the frame format are

1. **Preamble**: This. Field is at least 1 byte long. It is used for bit synchronization.
2. **Start Delimiter**: This one byte field marks the beginning of frame.
3. **Frame Control:** This one byte field specifies the type of frame. It distinguishes data frame from control frames. For data frames it carries frame's priority. For control frames, it specifies the frame type. The control frame types include. token passing and various ring maintenance frames, including the mechanism for letting new station enter the ring, the mechanism for allowing stations to leave the ring.
4. **Destination address**: It specifies 2 to 6 bytes destination address.
5. **Source address**: It specifies 2 to 6 bytes source address.
6. **Data**: This field may be upto 8182 bytes long when 2 bytes addresses are used & upto 8174 bytes long when 6 bytes address is used.
7. **Checksum**: This 4 byte field detects transmission errors.
8. **End Delimiter**: This one byte field marks the end of frame.