Unit-II

Data Link Layer Design Issues

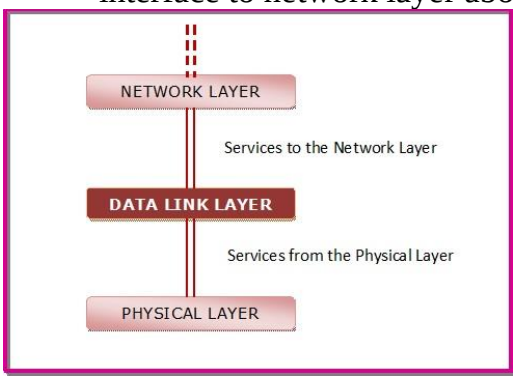
The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

- In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it.
- The data link layer uses the services offered by the physical layer.
- The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

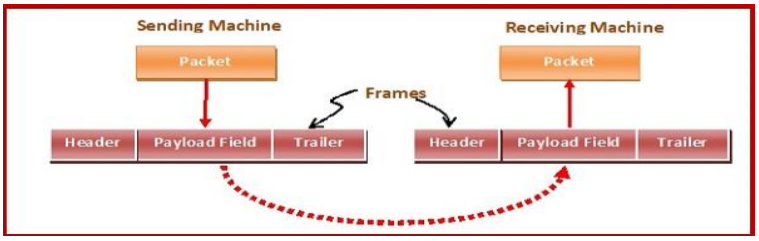
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

- The data link layer regulates flow control so that a fast sender does not drown a slow receiver.
- When the sender sends frames at very high speeds, a slow receiver may not be able to handle it.
- There will be frame losses even if the transmission is error-free.

The two common approaches for flow control are −

- Feedback based flow control
- Rate based flow control

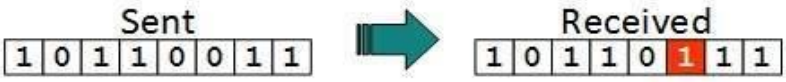
Error Detection and Correction

- There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission.
- The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.
- Hence, the upper layers expect error-free transmission between the systems.
- Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.
- Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

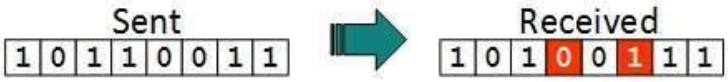
There may be three types of errors:

- **Single bit error**



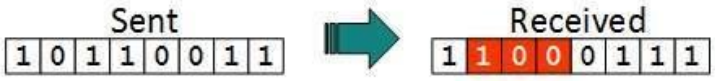
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it.

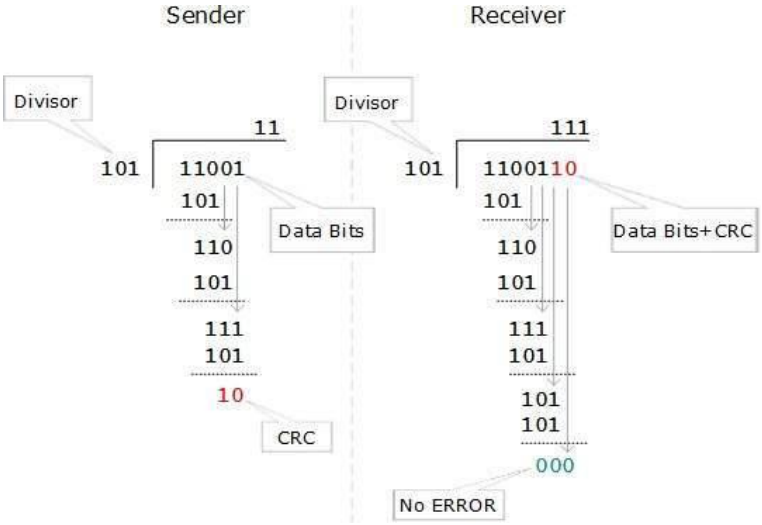
For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erro neous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

- CRC is a different approach to detect if the received frame contains valid data.
- This technique involves binary division of the data bits being sent.
- The divisor is generated using polynomials.
- The sender performs a division operation on the bits being sent and calculates the remainder.
- Before sending the actual bits, the sender adds the remainder at the end of the actual bits.
- Actual data bits plus the remainder is called a codeword.
- The sender transmits data bits as codewords.



- At the other end, the receiver performs division operation on codewords using the same CRC divisor.
- If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

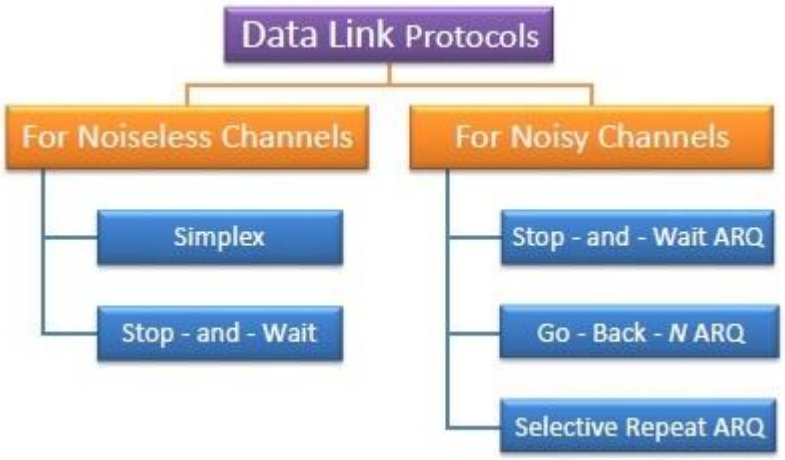
➢ The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive.

➢ For example, fiber optics. But in case of wireless transmission retransmitting may cost too much

➢ In the latter case, Forward Error Correction is used.

- To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection.
- For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.
- For m data bits, r redundant bits are used. r bits can provide 2r combinations of information.
- In m+r bit codeword, there is possibility that the r bits themselves may get corrupted.
- So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.
  - $2^r >= m+r+1$

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Elementary Data Link protocols

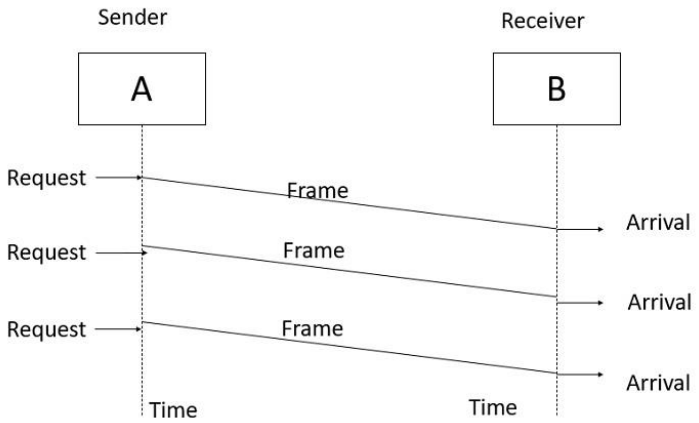
Elementary Data Link protocols are classified into three categories, as given below −

- Protocol 1 − Unrestricted simplex protocol
- Protocol 2 − Simplex stop and wait protocol
- Protocol 3 − Simplex protocol for noisy channels.

Let us discuss each protocol one by one.

Unrestricted Simplex Protocol

- Data transmitting is carried out in one direction only.
- The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored.
- In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.
- The Unrestricted Simplex Protocol is diagrammatically represented as follows −



Simplex Stop and Wait protocol

- In this protocol we assume that data is transmitted in one direction only.
- No error occurs; the receiver can only process the received information at finite rate.
- These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.
- The main problem here is how to prevent the sender from flooding the receiver.
- The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −

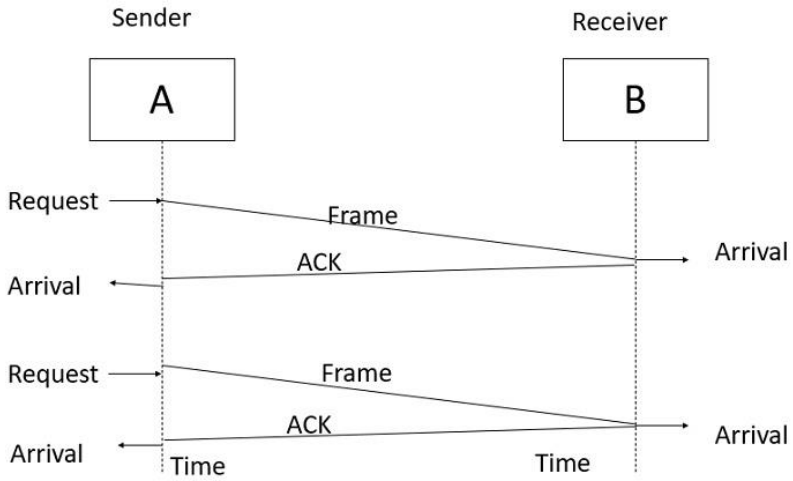
Step1 − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

Step 2 − Permission to send the next frame is granted.

Step 3 − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

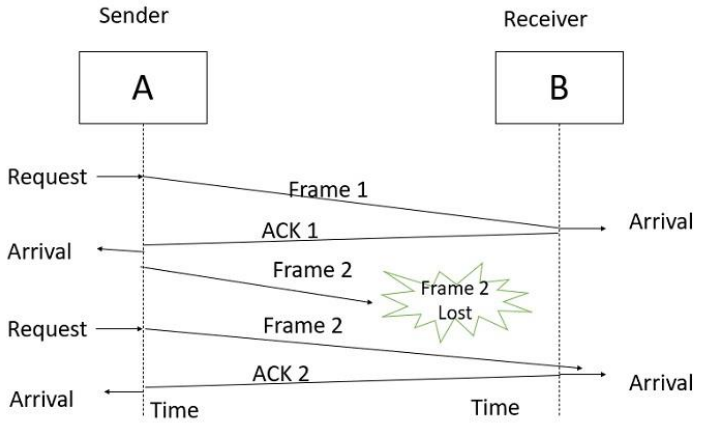
This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

The Simplex Stop and Wait Protocol is diagrammatically represented as follows −



Simplex Protocol for Noisy Channel

- Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver,
- since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.
- After a frame has been transmitted, the timer is started for a finite time.
- Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted,
- when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.
- The Simplex Protocol for Noisy Channel is diagrammatically represented as follows −



Sliding Window Protocol

The sliding window is a technique for sending multiple frames at a time.
It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed.

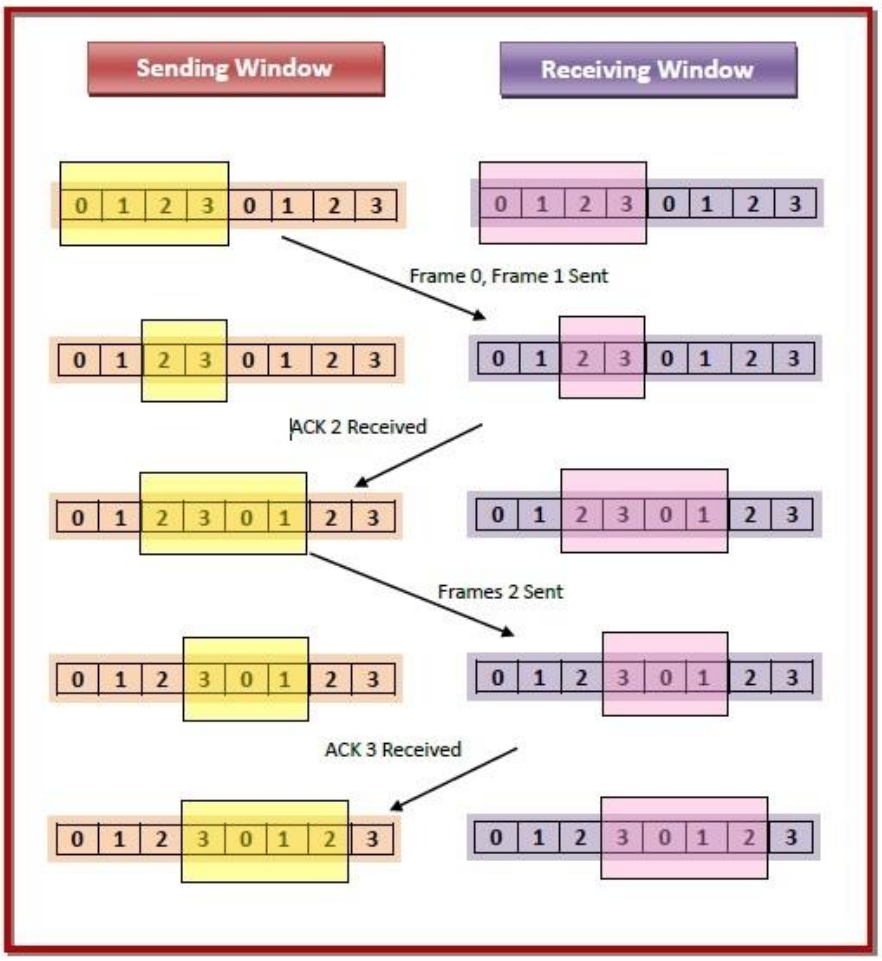
In this technique, each frame has sent from the sequence number.
The sequence numbers are used to find the missing data in the receiver end.
The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.
The size of the sending window determines the sequence number of the outbound frames.
If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1.
Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.
The sequence numbers are numbered as modulo-n.
For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.
The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

Example

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



Types of Sliding Window Protocol

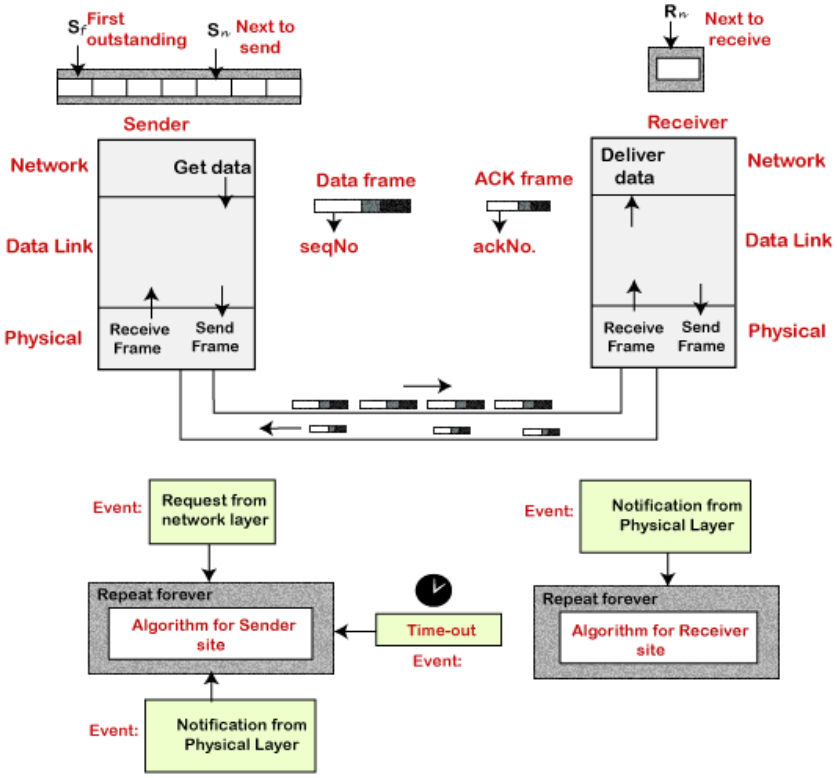
Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

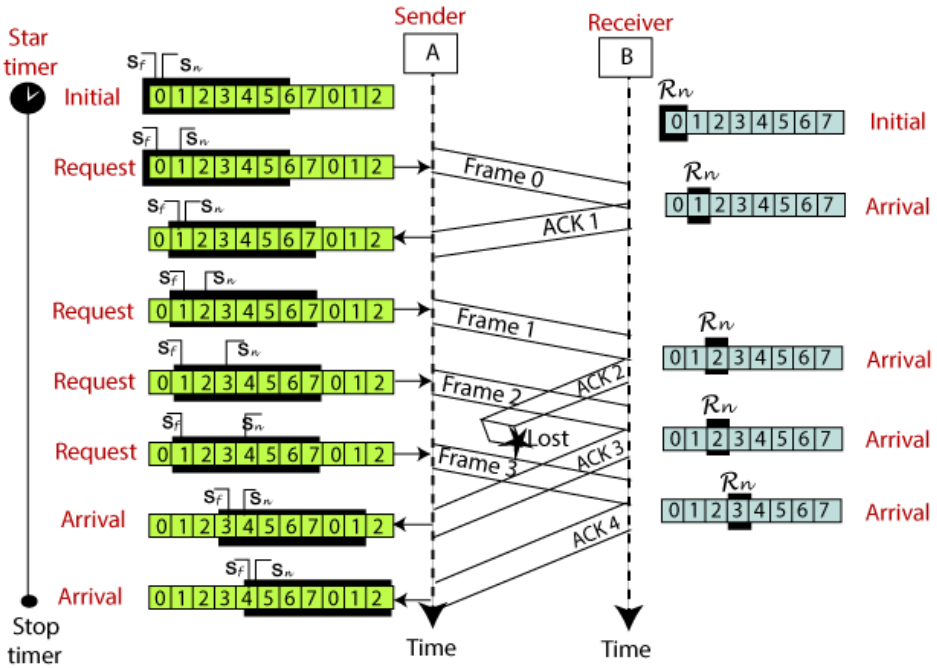
Go-Back-N ARQ

- Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- In this, if any frame is corrupted or lost, all subsequent frames have to be sent again**.**
- The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.
- If the receiver receives a corrupted frame, it cancels it.
- The receiver does not accept a corrupted frame.

- When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.

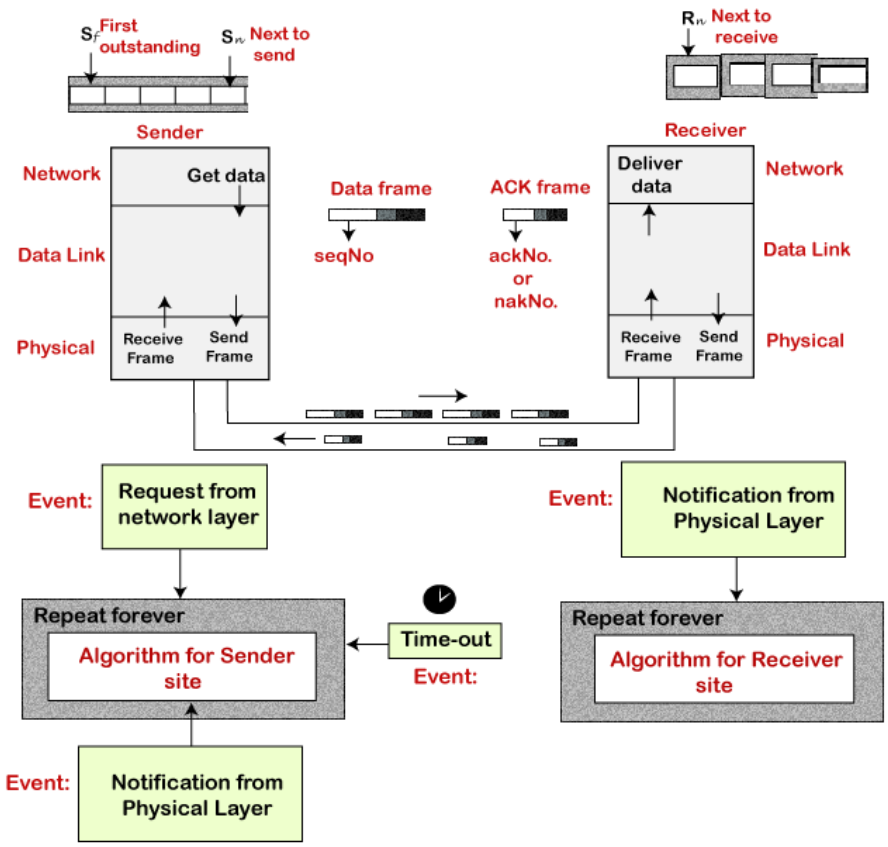


The example of Go-Back-N ARQ is shown below in the figure.

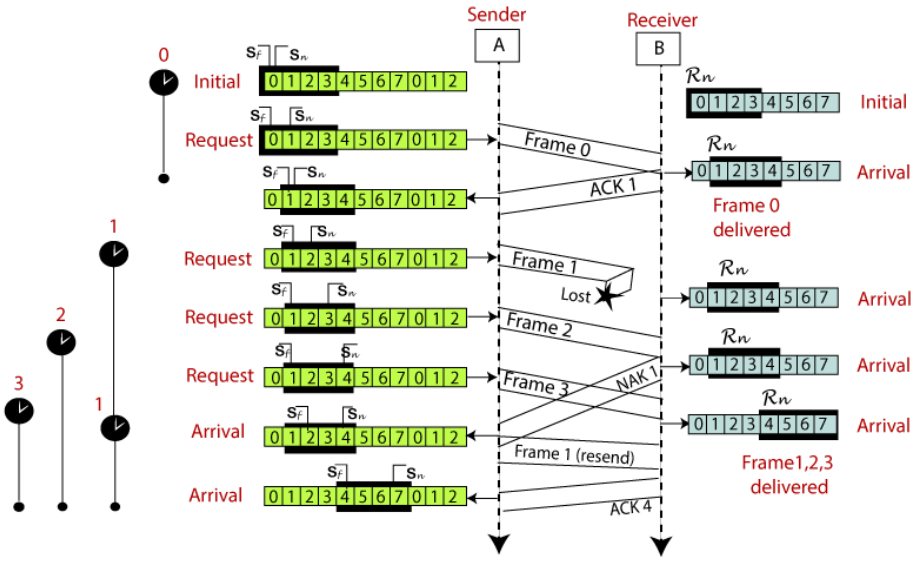


Selective Repeat ARQ

- Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request.
- It is a data link layer protocol that uses a sliding window method.
- The Go-back-N ARQ protocol works well if it has fewer errors.
- But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again.
- So, we use the Selective Repeat ARQ protocol.
- In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.
- If the receiver receives a corrupt frame, it does not directly discard it.
- It sends a negative acknowledgment to the sender.
- The sender sends that frame again as soon as on the receiving negative acknowledgment.
- There is no waiting for any time-out to send that frame.
- The design of the Selective Repeat ARQ protocol is shown below.



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Multiple Access Links and Protocols

There are two types of network links: point-to-point and broadcast links.

- A **point-to-point link** consists of a single sender at one end of the link and a single receiver at the other end of the link.
- A **broadcast link** can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel. The term *broadcast* is used because when any node transmits a frame, the channel broadcasts the frame and each other node receives a copy (ex: ethernet, wireless).

Multiple Access protocols

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.

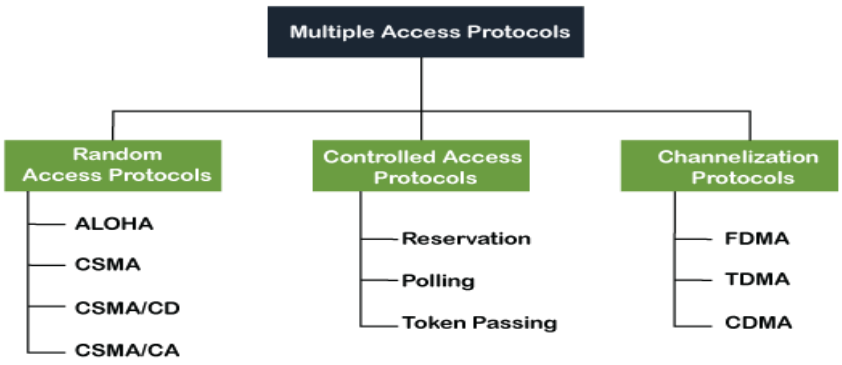
In that case, multiple stations access the channel and simultaneously transmits the data over the channel.

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

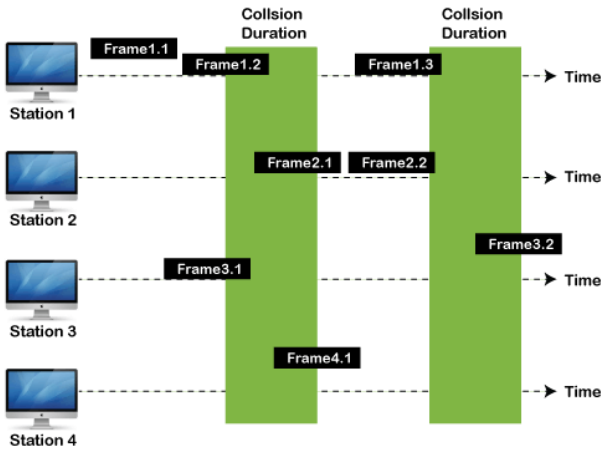
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.

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

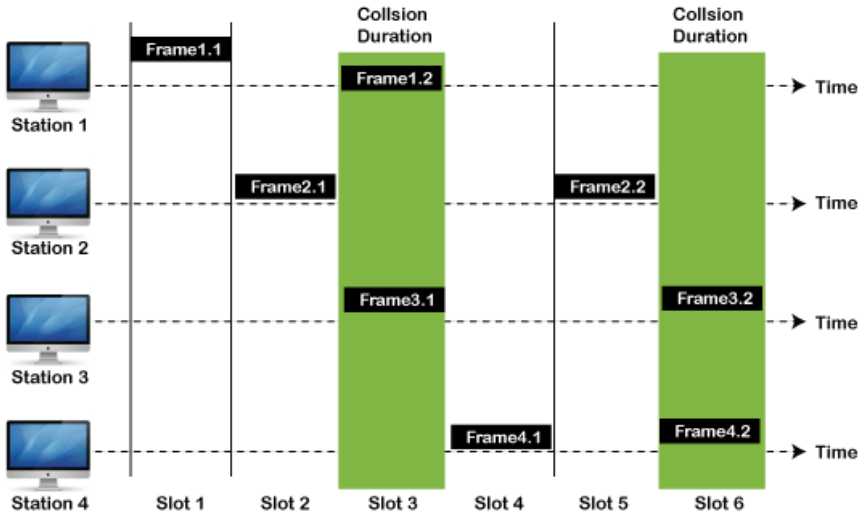
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same 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

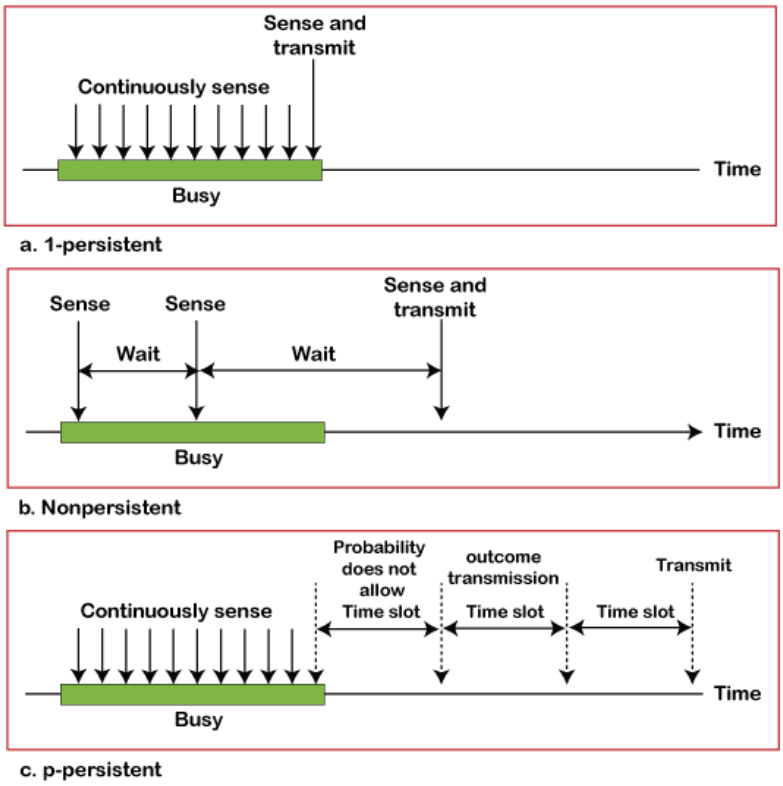
1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data.

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

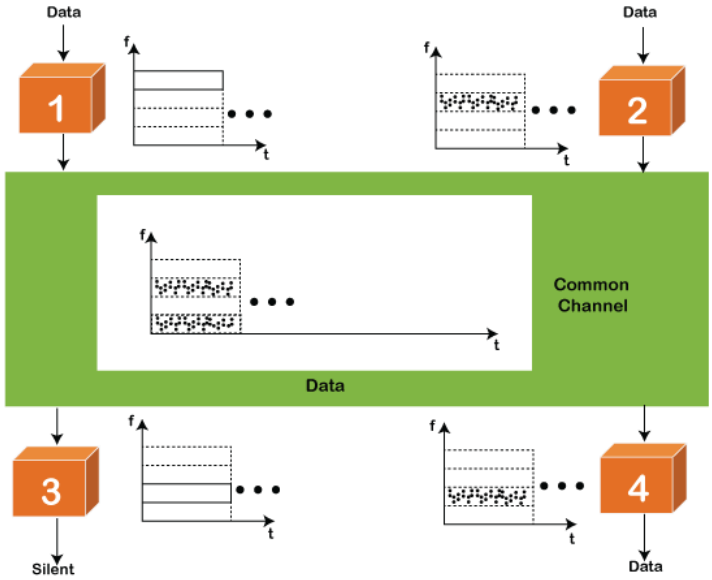
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

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.

Switched Local Area Network

Link Layer Addressing:

- A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
- Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.
- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.
- These two addresses are changed every time the frame moves from one link to another.

Three types of addresses: Some link-layer protocols define three types of addresses:

1. unicast,
2. multicast, and
3. broadcast.

- Unicast Address: Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication.
- Multicast Address: Some link-layer protocols define multicast addresses. Multicasting means one-to-many communication.
- Broadcast Address: Some link-layer protocols define a broadcast address. Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

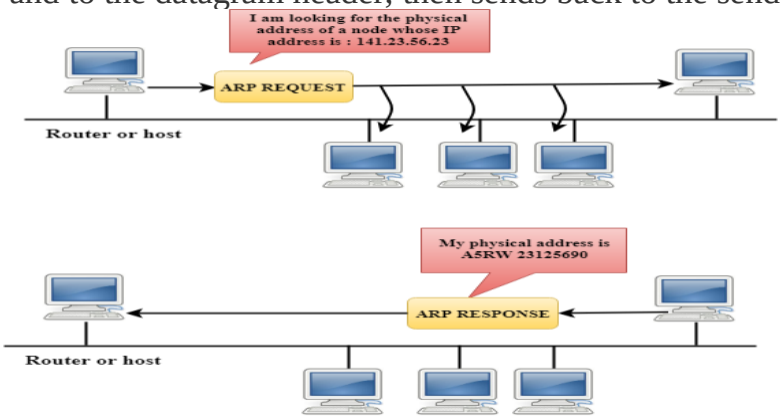
Address Resolution Protocol (ARP):

- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.

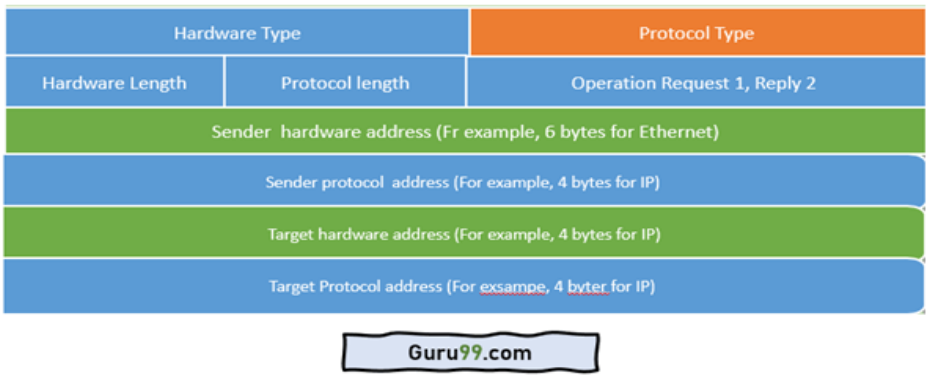
How ARP works

- If the host wants to know the physical address of another host on its network, then it sends an ARP query packet that includes the IP address and broadcast it over the network.

- Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes the IP address and sends back the physical address.
- The host holding the datagram adds the physical address to the cache memory and to the datagram header, then sends back to the sender.



ARP Header:



- **Hardware Type**–It is 1 for Ethernet.
- **Protocol Type**–It is a protocol used in the network layer.
- **Hardware Address Length**–It is the length in bytes so that it would be 6 for Ethernet.
- **Protocol Address Length** – Its value is 4 bytes.
- **Operation Code** indicates that the packet is an ARP Request (1) or an ARP Response (2).
- **Senders Hardware Address** – It is a hardware address of the source node.
- **Senders Protocol Address** -It is a layer 3 address of the source node.
- **Target Hardware Address** – It is used in a RARP request, which response impact both the destination's hardware and layer 3 addresses.
- **Target Protocol Address** – It is used in an ARP request when the response carries both layer 3 addresses and the destination's hardware.

Ethernet:

Ethernet is a LAN architecture or technology developed by XEROX and extended by DEC, IC and Xerox. It is specified by IEEE 802.3, and it defines two categories.

These categories are as follows−

- Baseband
- Broadband

Baseband uses digital signals, while broadband uses analog signals. Baseband is further divided into five standard names as follows −

- 10 Base 5
- 10 Base 2
- 10 Base T
- 1 Base 5
- 100 Base T
  - The first numbers used in all standards, i.e., 10, 1, 100, indicate the data rate in Mbps, while the last numbers 2, 5, and letter T indicate the maximum cable length or type of cable.
  - Only one specification is defined for broadband, and that is 10 Broad 36. 10 Base 5 means a data rate of 10 Mbps and cable length restriction of 500 meters.
  - The network uses Carrier-sense multiple access with collision detection (CSMA/CD) technique.
  - When multiple users access a single line, there is always a chance of overlapping and destroying data called collisions. Thus, if traffic increases on a single line, there are always chances of collision.
  - The carrier senses several access with collision Detection (ICMP/CD) is a technique that can help detect a collision, quits the current transmission and retransmission of data and takes place after waiting for some predetermined time to get the line cleared.

Data Rate

The Ethernet LANs supports a data rate between 1 Mbps to 100 Mbps. Baseband defines 1, 10, and 100 Mbps data rates, while broadband defines a data rate of 10 Mbps.

Frame Format

IEEE 802.3 specifies only one type of frame format that includes seven fields. These fields are as follows−

- **Preamble** − It contains seven bytes (56 bits) and is used for synchronization.
- **Start frame delimiter (SFD)** − It is a one-byte field and is used to signal the frame's beginning.
- Destination Address and Source Address fields are six bytes' fields containing sender and receiver address as declared by the Network Interface Card.
- The next field **length/type** is a two-byte field and indicates the number of PDU bits and its type. It provides a base for other protocols.

- The **PDU** or Data. It can start from the 46th byte and can continue up to the 1500th byte. It is generated by the LLC sublayer depending on the size and type of the PDU, and then it is linked to an 802.3 frame.
- The last field is **CRC**, which contains error detection information.

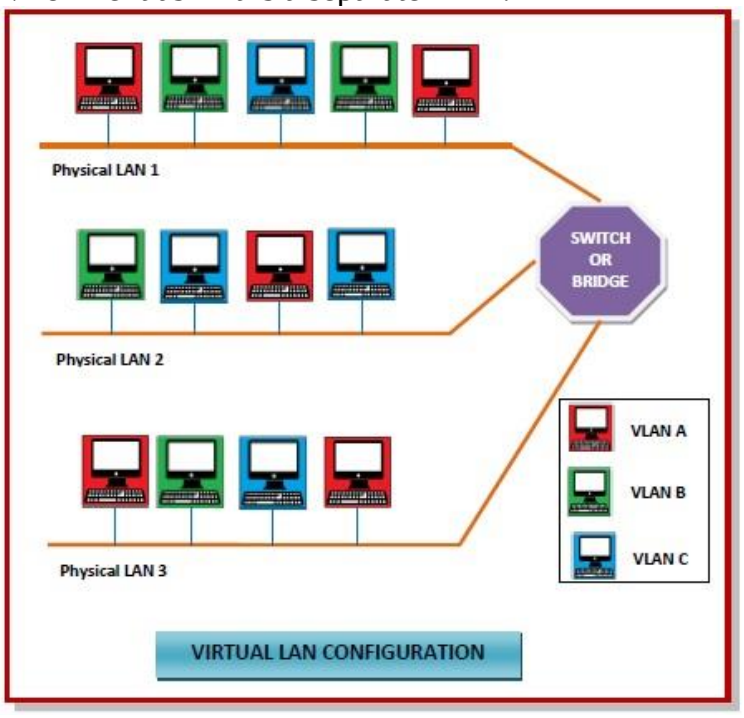
Ethernet (IEEE 802.3) Frame Format –

PREAMBLE	S F D	DESTINATION ADDRESS	SOURCE ADDRESS	LENGTH	DATA	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

IEEE 802.3 ETHERNET Frame Format

Virtual LAN

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

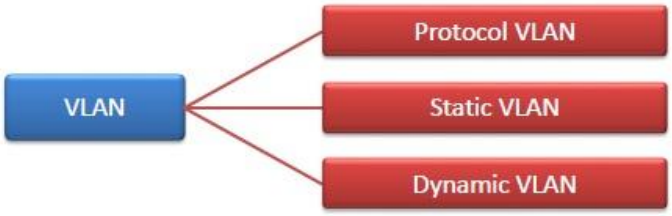


Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.

- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs



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