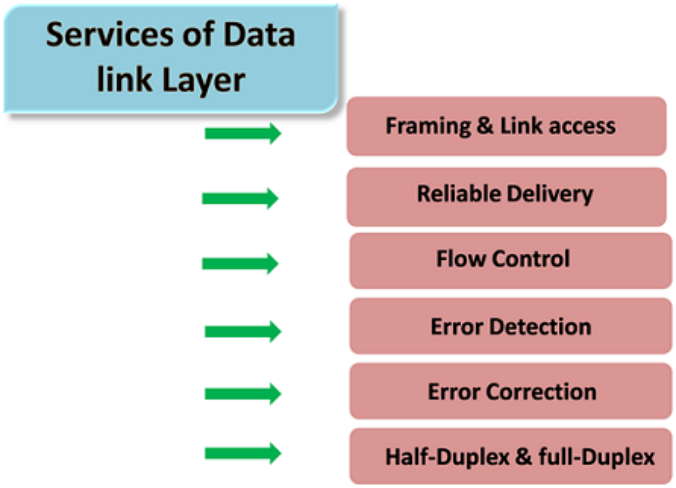
UNIT-II

Data Link Layer

Introduction

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.
- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

Services are provided by the Data Link Layer:



- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the

sending node on one side of the link from overwhelming the receiving node on another side of the link.

- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Data Link Layer Design Issues

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

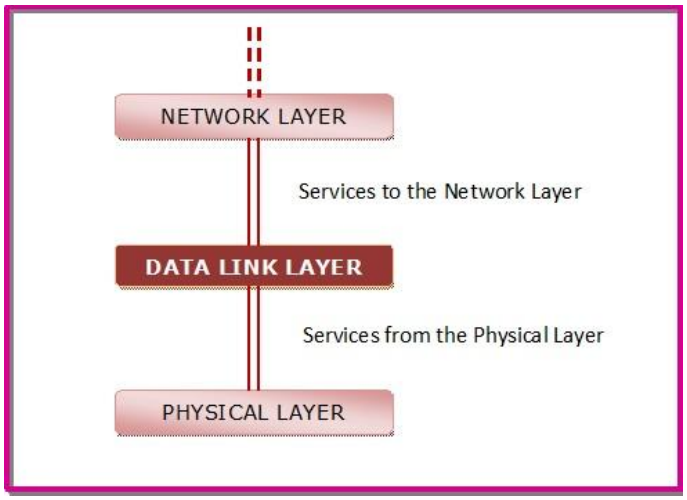
The data link layer is divided into two sub-layers:

- **Logical Link Control Sub-layer (LLC) –** Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –
  (i) Error Recovery.
  (ii) It performs the flow control operations.
  (iii) User addressing.
- **Media Access Control Sub-layer (MAC) –** It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card. Functions are –
  (i) To perform the control of access to media.
  (ii) It performs the unique addressing to stations directly connected to LAN.
  (iii) Detection of errors.

Design issues with data link layer are:

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

   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 –

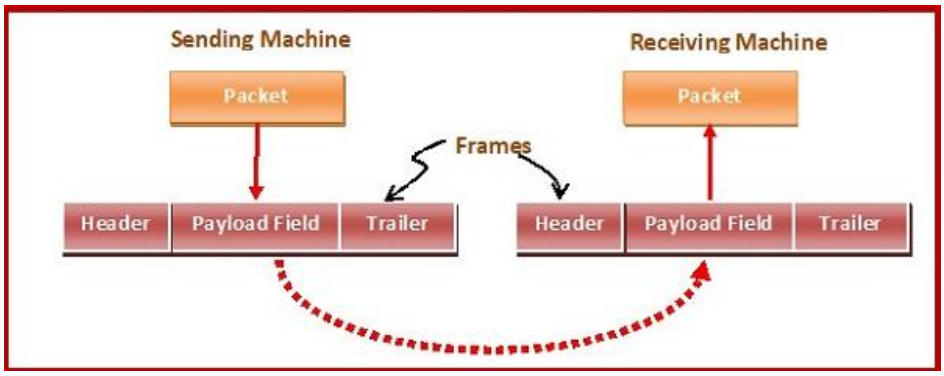
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

2) **Frame synchronization –** The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine.

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



3) **Flow control –** Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

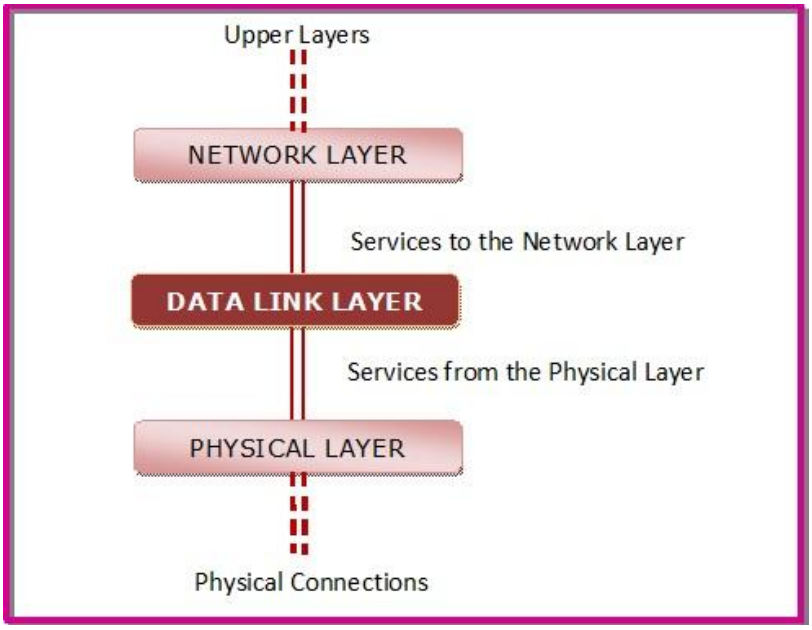
The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control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

- Feedback based flow control
- Rate based flow control

4) **Error control** – Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.
   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

Services Provided to the Network Layer

In the OSI (Open System Interconnections) Model, each layer uses the services of the layer below it and provides services to the layer above it. The primary function of the data link layer is to provide a well-defined service interface to the network layer above it.

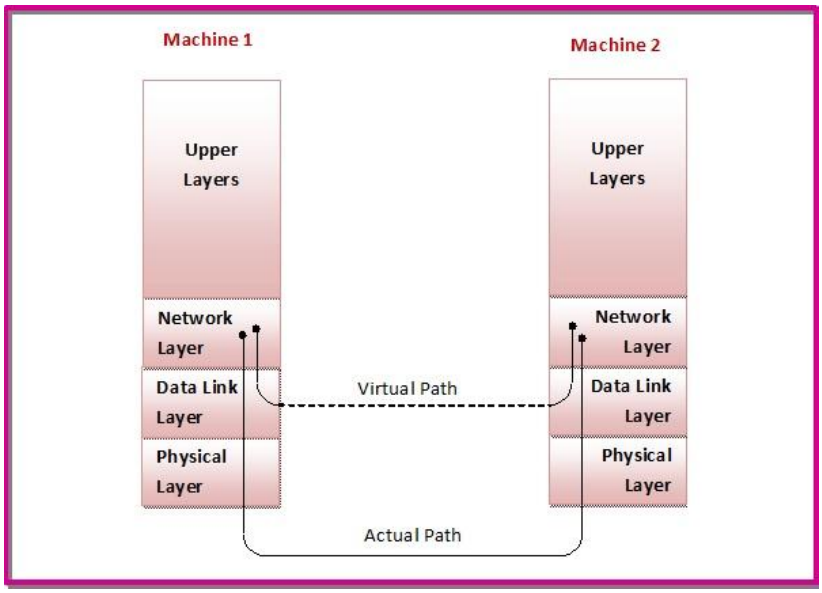


Virtual Communication versus Actual Communication

The main service provided is to transfer data packets from the network layer on the sending machine to the network layer on the receiving machine. Data link layer of the sending machine transmits accepts data from the network layer and sends them to the data link layer of the destination machine which hands them to the network layer there.

In actual communication, the data link layer transmits bits via the physical layers and physical medium. However virtually, this can be visualized as the two data link layers communicating with each other using a data link protocol.

The processes are depicted in the following diagram –



Types of Services

The data link layer offers three types of services.

a) **Unacknowledged connectionless service** – Here, the data link layer of the sending machine sends independent frames to the data link layer of the receiving machine. The receiving machine does not acknowledge receiving the frame. No logical connection is set up between the host machines. Error and data loss is not handled in this service. This is applicable in Ethernet services and voice communications.

b) **Acknowledged connectionless service** – Here, no logical connection is set up between the host machines, but each frame sent by the source machine is acknowledged by the destination machine on receiving. If the source does not receive the acknowledgment within a stipulated time, then it resends the frame. This is used in Wifi (IEEE 802.11) services.

c) **Acknowledged connection-oriented service** – This is the best service that the data link layer can offer to the network layer. A logical connection is set up between the two machines and the data is transmitted along this logical path. The frames are numbered, that keeps track of loss of frames and also ensures that frames are received in correct order. The service has three distinct phases –
   - Set up of connection – A logical path is set up between the source and the destination machines. Buffers and counters are initialised to keep track of frames.
   - Sending frames – The frames are transmitted.
   - Release connection – The connection is released, buffers and other resources are released.

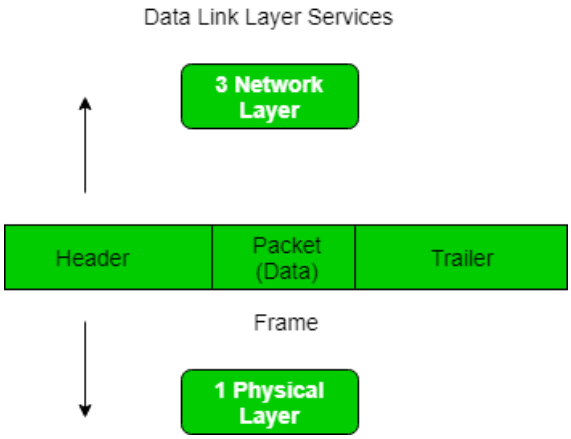
   It is appropriate for satellite communications and long-distance telephone circuits.

Framing in Data Link Layer

Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy. Frame is continuously used in Time Division Multiplexing process.

Framing is a point-to-point connection between two computers or devices consisting 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.



At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.
The process of dividing the data into frames and reassembling it is transparent to the user and is handled by the data link layer.

Framing is an important aspect of data link layer protocol design because it allows the transmission of data to be organized and controlled, ensuring that the data is delivered accurately and efficiently.

Problems in Framing

a) **Detecting start of the frame:** When a frame is transmitted, every station must be able to detect it. Station detects frames by looking out for a special sequence of bits that marks the beginning of the frame i.e. SFD (Starting Frame Delimiter).
b) **How does the station detect a frame:** Every station listens 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.
c) **Detecting end of frame:** When to stop reading the frame.
d) **Handling errors:** Framing errors may occur due to noise or other transmission errors, which can cause a station to misinterpret the frame. Therefore, error detection and correction mechanisms, such as cyclic redundancy check (CRC), are used to ensure the integrity of the frame.
e) **Framing overhead:** Every frame has a header and a trailer that contains control information such as source and destination address, error detection code, and other protocol-related information. This overhead reduces the available bandwidth for data transmission, especially for small-sized frames.
f) **Framing incompatibility:** Different networking devices and protocols may use different framing methods, which can lead to framing incompatibility issues. For example, if a device using one framing method sends data to a device using a different framing method, the receiving device may not be able to correctly interpret the frame.

g) **Framing synchronization:** Stations must be synchronized with each other to avoid collisions and ensure reliable communication. Synchronization requires that all stations agree on the frame boundaries and timing, which can be challenging in complex networks with many devices and varying traffic loads.

h) **Framing efficiency:** Framing should be designed to minimize the amount of data overhead while maximizing the available bandwidth for data transmission. Inefficient framing methods can lead to lower network performance and higher latency.

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, the length of the frame itself acts as a delimiter.

Drawback: It suffers from internal fragmentation if the data size is less than the frame size

Solution: Padding

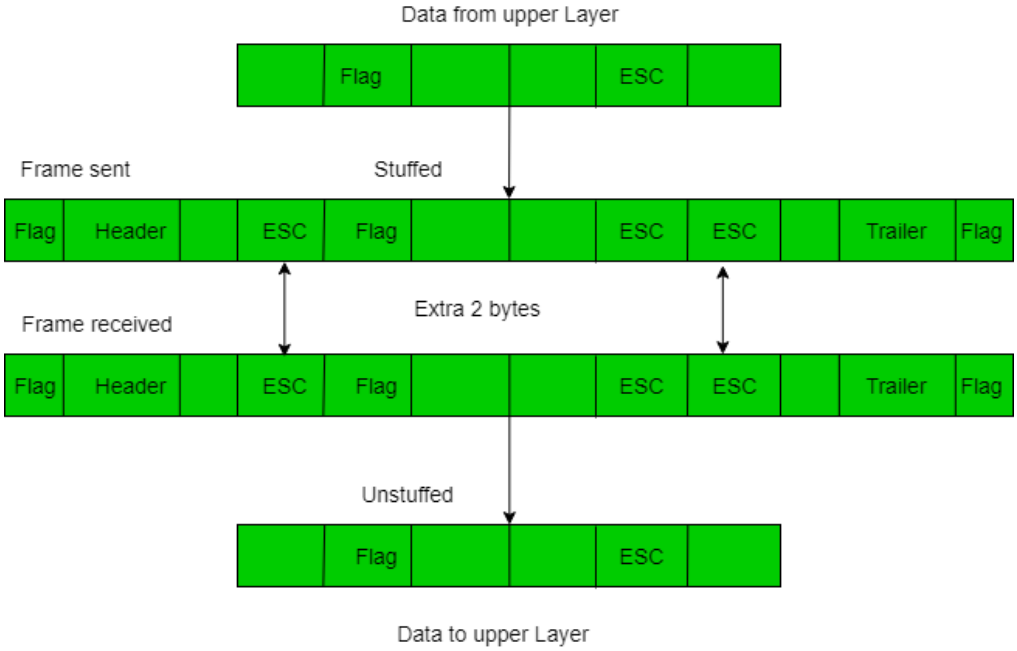
2) Variable size: In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish. This can be done in two ways:

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 Delimiter (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:

a) Character/Byte Stuffing: Used when frames consist of characters. If data contains ED then, a byte is stuffed into data to differentiate it from ED.

Let ED = "$" –> if data contains '$' anywhere, it can be escaped using '\O' character.
–> if data contains '\O$' then, use '\O\O\O$'($ is escaped using \O and \O is escaped using \O).



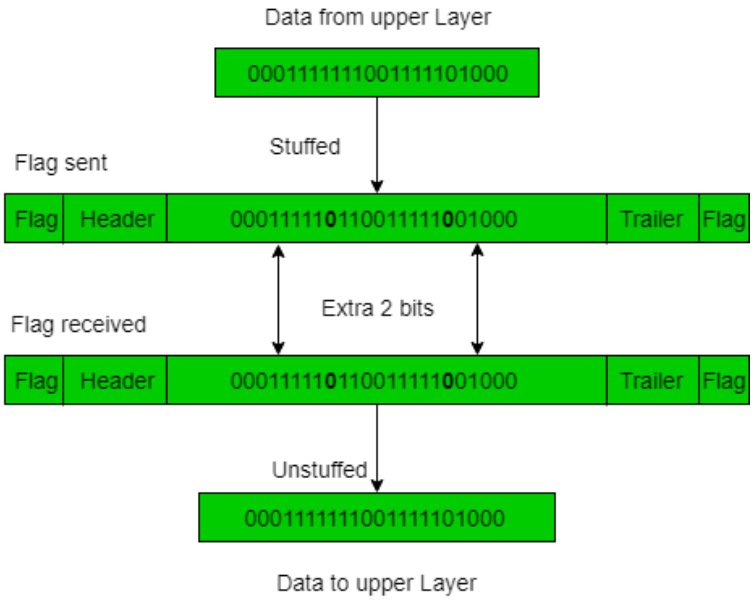
Disadvantage – It is very costly and obsolete method.

b) Bit Stuffing: Let ED = 01111 and if data = 01111

–> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data = 01110**1**.

–> Receiver receives the frame.

–> If data contains 01110**1**, receiver removes the 0 and reads the data.



Examples:

- If Data –> 011100011110 and ED –> 0111 then, find data after bit stuffing.
  --> 011**0**10001**1**0**1**1**0**0
- If Data –> 110001001 and ED –> 1000 then, find data after bit stuffing?
  --> 1100**1**0100**1**1

framing in the Data Link Layer also presents some challenges, which include:

- **Variable frame length:** The length of frames can vary depending on the data being transmitted, which can lead to inefficiencies in transmission. To address this issue, protocols such as HDLC and PPP use a flag sequence to mark the start and end of each frame.
- **Bit stuffing:** Bit stuffing is a technique used to prevent data from being interpreted as control characters by inserting extra bits into the data stream. However, bit stuffing can lead to issues with synchronization and increase the overhead of the transmission.
- **Synchronization:** Synchronization is critical for ensuring that data frames are transmitted and received correctly. However, synchronization can be challenging, particularly in high-speed networks where frames are transmitted rapidly.
- **Error detection:** Data Link Layer protocols use various techniques to detect errors in the transmitted data, such as checksums and CRCs. However, these techniques are not foolproof and can miss some types of errors.
- **Efficiency:** Efficient use of available bandwidth is critical for ensuring that data is transmitted quickly and reliably. However, the overhead associated with framing and error detection can reduce the overall efficiency of the transmission.

Various kind of Framing in Data link layer (Methods of Framing)

Framing is function of Data Link Layer that is used to separate message from source or sender to destination or receiver or simply from all other messages to all other destinations just by adding sender address and destination address. The destination or receiver address is simply used to represent where message or packet is to go and sender or source address is simply used to help recipient to acknowledge receipt.

Frames are generally data unit of data link layer that is transmitted or transferred among various network points. It includes complete and full addressing, protocols that are essential, and information under control. Physical layers only just accept and transfer stream of bits without any regard to meaning or structure. Therefore it is up to data link layer to simply develop and recognize frame boundaries.

This can be achieved by attaching special types of bit patterns to start and end of the frame. If all of these bit patterns might accidentally occur in data, special care is needed to be taken to simply make sure that these bit patterns are not interpreted incorrectly or wrong as frame delimiters.

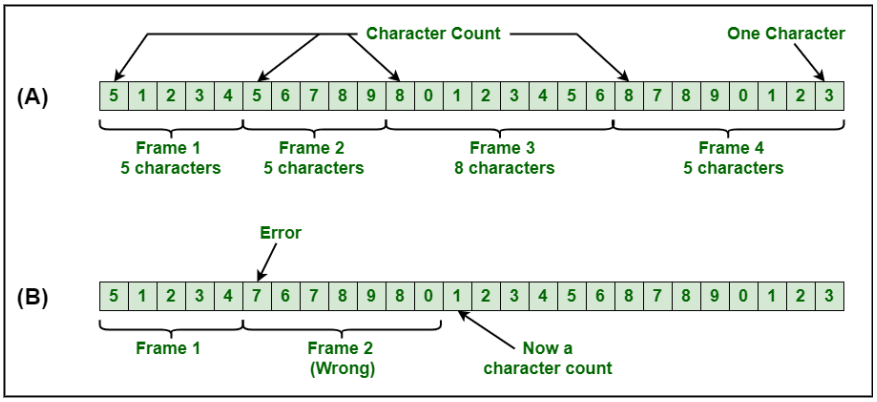
Framing is simply point-to-point connection among two computers or devices that consists or includes wire in which data is transferred as stream of bits. However, all of these bits should be framed into discernible blocks of information.

Methods of Framing:

There are basically four methods of framing as given below –

a) Character Count
b) Flag Byte with Character Stuffing
c) Starting and Ending Flags, with Bit Stuffing
d) Encoding Violations

a) Character Count: This method is rarely used and is generally required to count total number of characters that are present in frame. This is be done by using field in header. Character count method ensures data link layer at the receiver or destination about total number of characters that follow, and about where the frame ends.



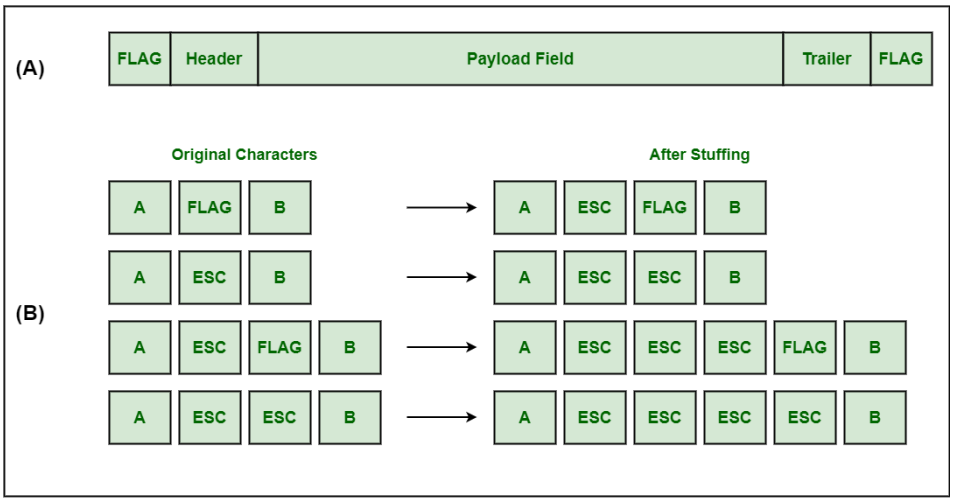
A Character Stream

(A) Without Errors
(B) With one Error

There is disadvantage also of using this method i.e., if anyhow character count is disturbed or distorted by an error occurring during transmission, then destination or receiver might lose synchronization. The destination or receiver might also be not able to locate or identify beginning of next frame.

b) Character Stuffing: Character stuffing is also known as byte stuffing or character-oriented framing and is same as that of bit stuffing but byte stuffing actually operates on bytes whereas bit stuffing operates on bits. In byte stuffing, special byte that is basically known as ESC (Escape Character) that has predefined pattern is generally added to data section of the data stream or frame when there is message or character that has same pattern as that of flag byte.

But receiver removes this ESC and keeps data part that causes some problems or issues. In simple words, we can say that character stuffing is addition of 1 additional byte if there is presence of ESC or flag in text.



A Character Stuffing
(A) A frame delimited by flag bytes
(B) Four examples of byte sequences before and after byte stuffing

c) Bit Stuffing: Bit stuffing is also known as bit-oriented framing or bit-oriented approach. In bit stuffing, extra bits are being added by network protocol designers to data streams. It is generally insertion or addition of extra bits into transmission unit or message to be transmitted as simple way to provide and give signaling information and data to receiver and to avoid or ignore appearance of unintended or unnecessary control sequences.

It is type of protocol management simply performed to break up bit pattern that results in transmission to go out of synchronization. Bit stuffing is very essential part of transmission process in network and communication protocol. It is also required in USB.

d) Physical Layer Coding Violations: Encoding violation is method that is used only for network in which encoding on physical medium includes some sort of redundancy i.e., use of more than one graphical or visual structure to simply encode or represent one variable of data.

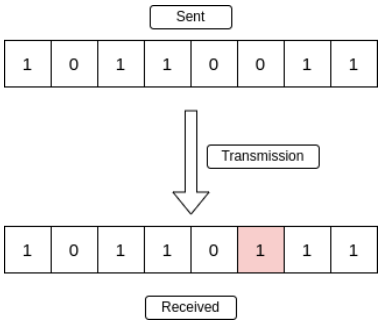
Error Detection in Computer Networks

Error is a condition when the receiver's information does not match the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

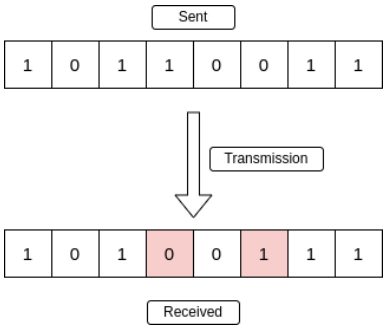
Types of Errors

Single-Bit Error - A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.

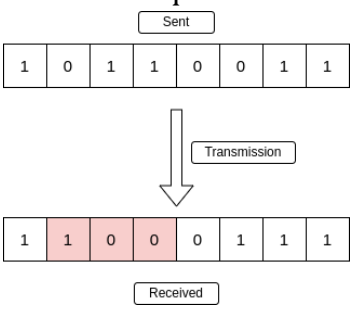


Single-Bit Error

Multiple-Bit Error - A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected. Although multiple-bit errors are relatively rare when compared to single-bit errors, they can still occur, particularly in high-noise or high-interference digital environments.



Burst Error - When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.



Burst Error

To detect errors, a common technique is to introduce redundancy bits that provide additional information. Various techniques for error detection include:

a) Simple Parity Check
b) Two-dimensional Parity Check
c) Checksum
d) Cyclic Redundancy Check (CRC)

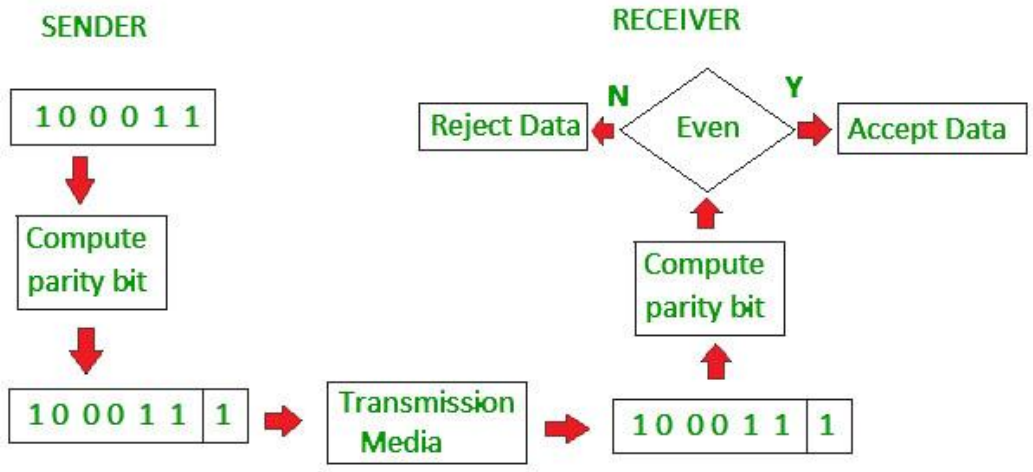
Error Detection Methods

Simple Parity Check

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

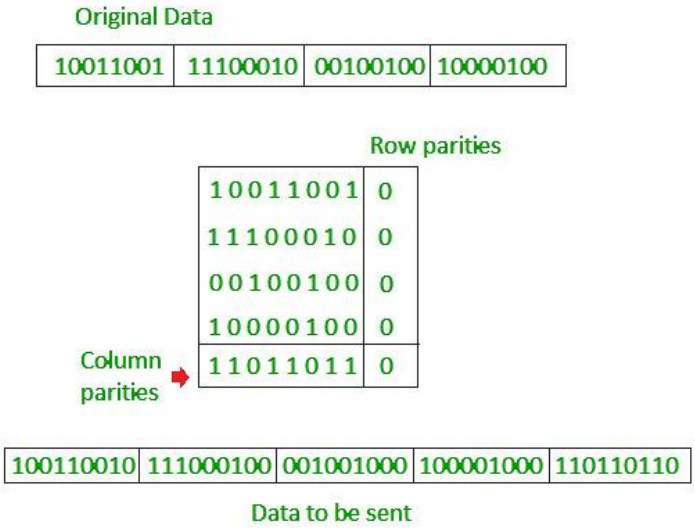


Disadvantages

- Single Parity check is not able to detect even no. of bit error.
- **For example,** the Data to be transmitted is **101010**. Codeword transmitted to the receiver is 1010101 (we have used even parity).
  Let's assume that during transmission, two of the bits of code word flipped to 1111101. On receiving the code word, the receiver finds the no. of ones to be even and hence **no error,** *which is a wrong assumption.*

Two-dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



Checksum

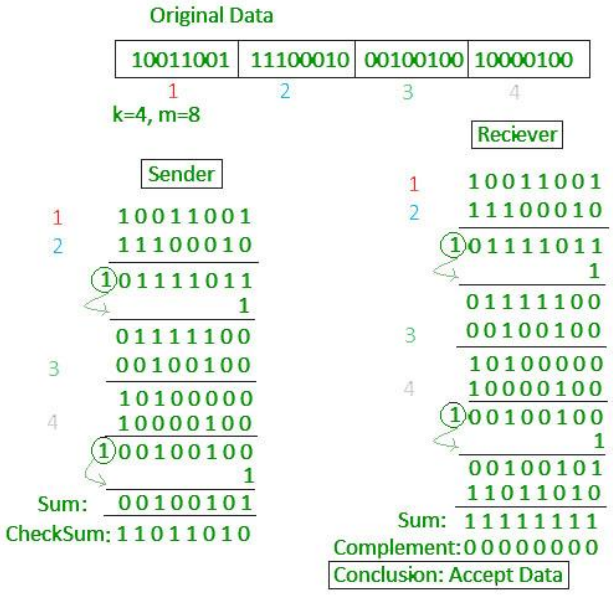
Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum – Operation at Sender's Side

- Firstly, the data is divided into k segments each of m bits.
- On the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

Checksum – Operation at Receiver's Side

- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.

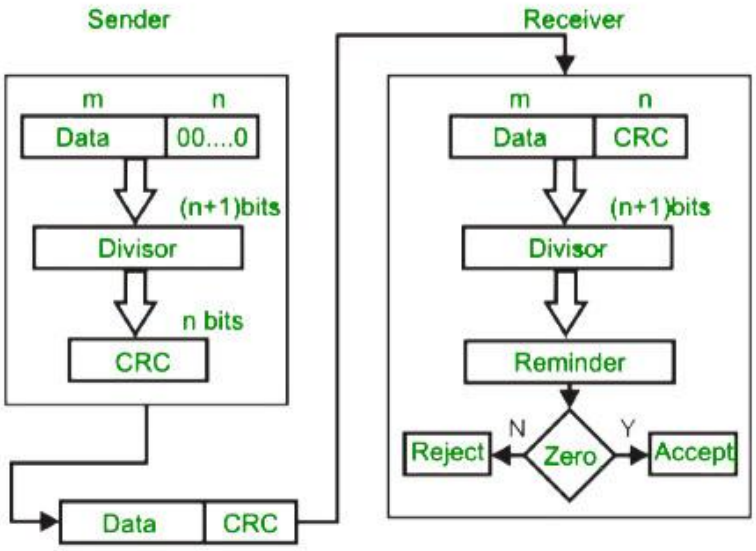


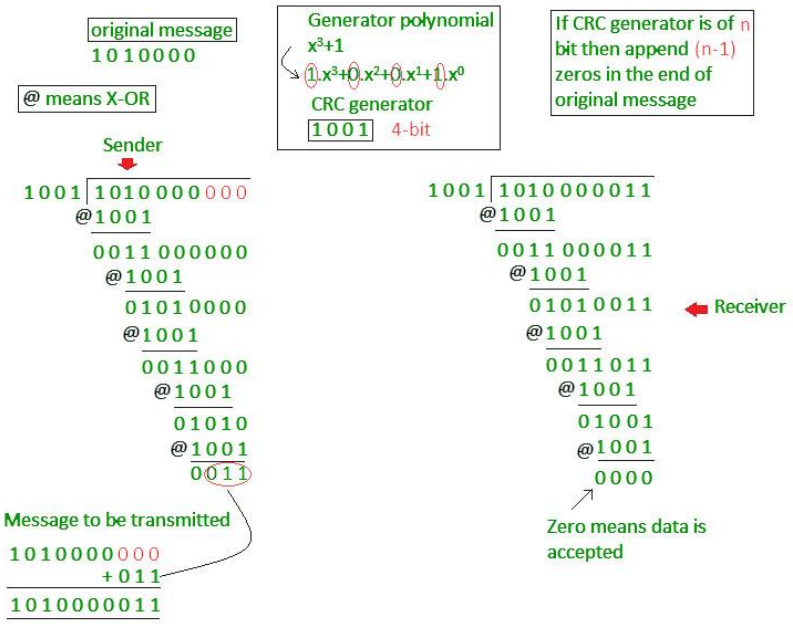
Disadvantages

- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged.

Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.





Advantages:

- **Increased Data Reliability:** Error detection ensures that the data transmitted over the network is reliable, accurate, and free from errors. This ensures that the recipient receives the same data that was transmitted by the sender.
- **Improved Network Performance:** Error detection mechanisms can help to identify and isolate network issues that are causing errors. This can help to improve the overall performance of the network and reduce downtime.
- **Enhanced Data Security:** Error detection can also help to ensure that the data transmitted over the network is secure and has not been tampered with.

Disadvantages:

- **Overhead**: Error detection requires additional resources and processing power, which can lead to increased overhead on the network. This can result in slower network performance and increased latency.
- **False Positives**: Error detection mechanisms can sometimes generate false positives, which can result in unnecessary retransmission of data. This can further increase the overhead on the network.
- **Limited Error Correction**: Error detection can only identify errors but cannot correct them. This means that the recipient must rely on the sender to retransmit the data, which can lead to further delays and increased network overhead.

Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

a) **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
b) **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

For correcting the errors, one has to know the exact position of the error. For example, If we want to calculate a single-bit error, the error correction code will determine which one of seven bits is in error. To achieve this, we have to add some additional redundant bits.

Suppose **r** is the number of redundant bits and d is the total number of the data bits. The number of redundant bits r can be calculated by using the formula:

$$2^r >= d+r+1$$

The value of r is calculated by using the above formula. For example, if the value of d is 4, then the possible smallest value that satisfies the above relation would be 3.

To determine the position of the bit which is in error, a technique developed by R.W Hamming is Hamming code which can be applied to any length of the data unit and uses the relationship between data units and redundant units.

Hamming Code

Parity bits: The bit which is appended to the original data of binary bits so that the total number of 1s is even or odd.

Even parity: To check for even parity, if the total number of 1s is even, then the value of the parity bit is 0. If the total number of 1s occurrences is odd, then the value of the parity bit is 1.

Odd Parity: To check for odd parity, if the total number of 1s is even, then the value of parity bit is 1. If the total number of 1s is odd, then the value of parity bit is 0.

Algorithm of Hamming code:

- An information of 'd' bits are added to the redundant bits 'r' to form d+r.
- The location of each of the (d+r) digits is assigned a decimal value.
- The 'r' bits are placed in the positions 1,2,.....2^{k-1}.
- At the receiving end, the parity bits are recalculated. The decimal value of the parity bits determines the position of an error.

Relationship b/w Error position & binary number

Error Position	Binary Number
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Let's understand the concept of Hamming code through an example:

Suppose the original data is 1010 which is to be sent.

Total number of data bits 'd' = 4

Number of redundant bits r : $2^r >= d+r+1$

$2^r >= 4+r+1$

Therefore, the value of r is 3 that satisfies the above relation.

Total number of bits = d+r = 4+3 = 7;

Determining the position of the redundant bits

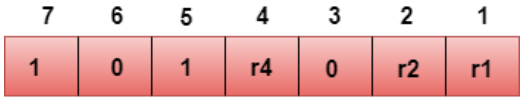
The number of redundant bits is 3. The three bits are represented by r1, r2, r4. The position of the redundant bits is calculated with corresponds to the raised power of 2. Therefore, their corresponding positions are **1, 2^1, 2^2**.

The position of r1 = 1

The position of r2 = 2

The position of r4 = 4

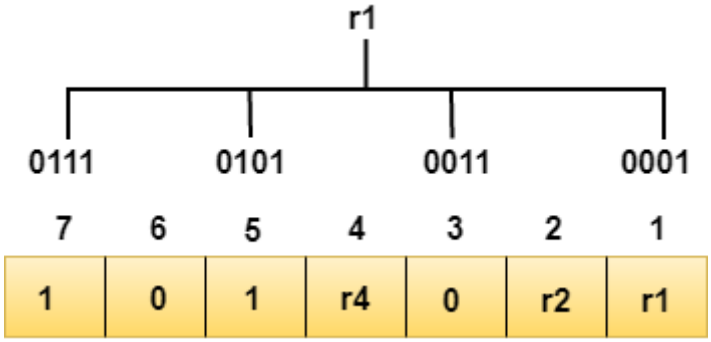
Representation of Data on the addition of parity bits:



Determining the Parity bits

Determining the r1 bit

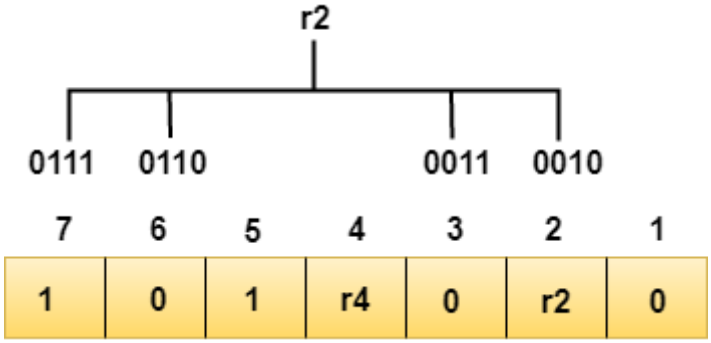
The r1 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the first position.



We observe from the above figure that the bit positions that includes 1 in the first position are 1, 3, 5, 7. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r1 is **even, therefore, the value of the r1 bit is 0**.

Determining r2 bit

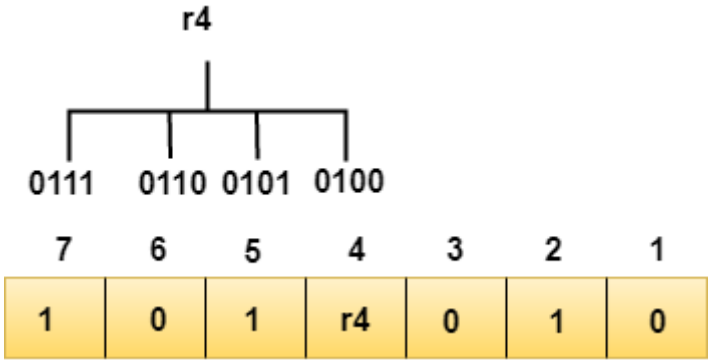
The r2 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the second position.



We observe from the above figure that the bit positions that includes 1 in the second position are **2, 3, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r2 is **odd, therefore, the value of the r2 bit is 1**.

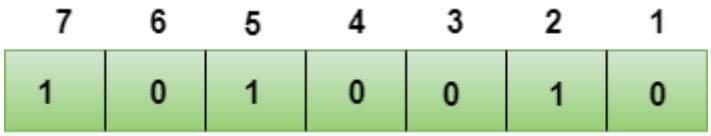
Determining r4 bit

The r4 bit is calculated by performing a parity check on the bit positions whose binary representation includes 1 in the third position.



We observe from the above figure that the bit positions that includes 1 in the third position are **4, 5, 6, 7**. Now, we perform the even-parity check at these bit positions. The total number of 1 at these bit positions corresponding to r4 is **even, therefore, the value of the r4 bit is 0**.

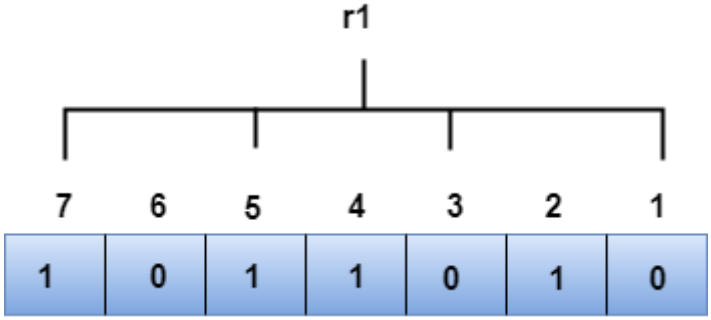
Data transferred is given below:



Suppose the 4th bit is changed from 0 to 1 at the receiving end, then parity bits are recalculated.

R1 bit

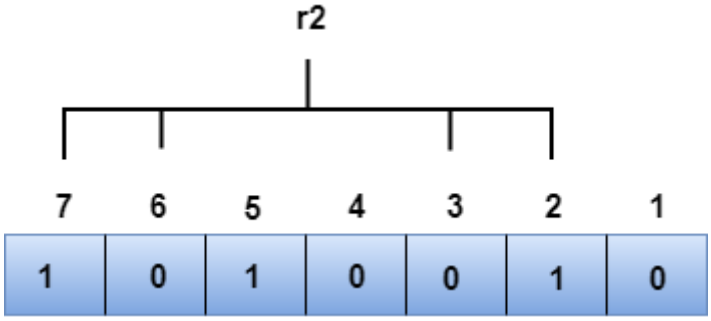
The bit positions of the r1 bit are 1,3,5,7



We observe from the above figure that the binary representation of r1 is 1100. Now, we perform the even-parity check, the total number of 1s appearing in the r1 bit is an even number. Therefore, the value of r1 is 0.

R2 bit

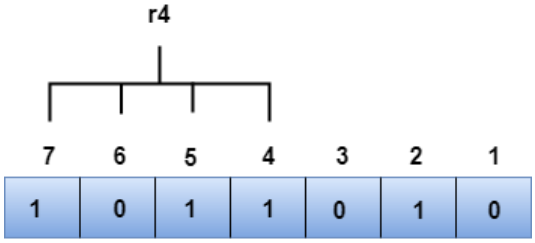
The bit positions of r2 bit are 2,3,6,7.



We observe from the above figure that the binary representation of r2 is 1001. Now, we perform the even-parity check, the total number of 1s appearing in the r2 bit is an even number. Therefore, the value of r2 is 0.

R4 bit

The bit positions of r4 bit are 4,5,6,7.



We observe from the above figure that the binary representation of r4 is 1011. Now, we perform the even-parity check, the total number of 1s appearing in the r4 bit is an odd number. Therefore, the value of r4 is 1.

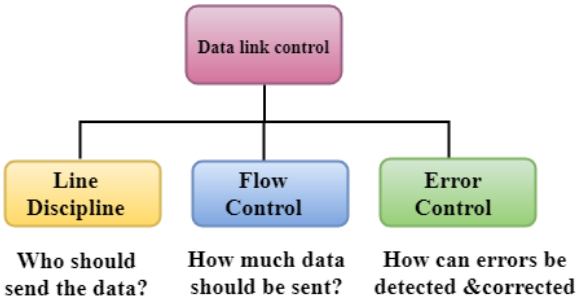
The binary representation of redundant bits, i.e., r4r2r1 is 100, and its corresponding decimal value is 4. Therefore, the error occurs in a 4th bit position. The bit value must be changed from 1 to 0 to correct the error.

Data Link Controls

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

The Data link layer provides three functions:

1) Line Discipline
2) Flow Control
3) Error Control



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

   Line Discipline can be achieved in two ways:

   a) ENQ/ACK
   b) Poll/select

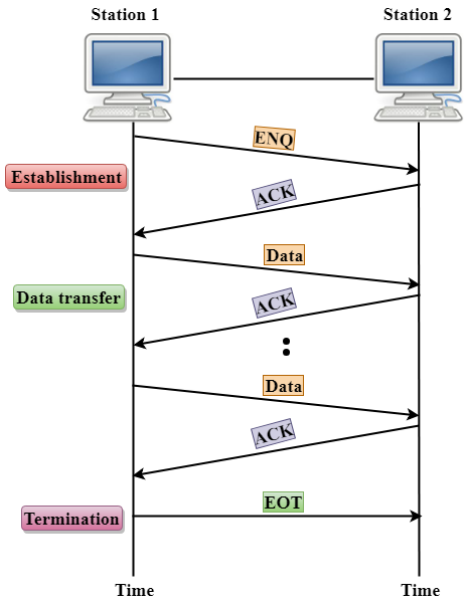
a) END/ACK - END/ACK stands for Enquiry/Acknowledgement is used when there is no wrong receiver available on the link and having a dedicated path between the two devices so that the device capable of receiving the transmission is the intended one.
END/ACK coordinates which device will start the transmission and whether the recipient is ready or not.

Working of END/ACK

The transmitter transmits the frame called an Enquiry (ENQ) asking whether the receiver is available to receive the data or not.
The receiver responses either with the positive acknowledgement(ACK) or with the negative acknowledgement(NACK) where positive acknowledgement means that the receiver is ready to receive the transmission and negative acknowledgement means that the receiver is unable to accept the transmission.

Following are the responses of the receiver:

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



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

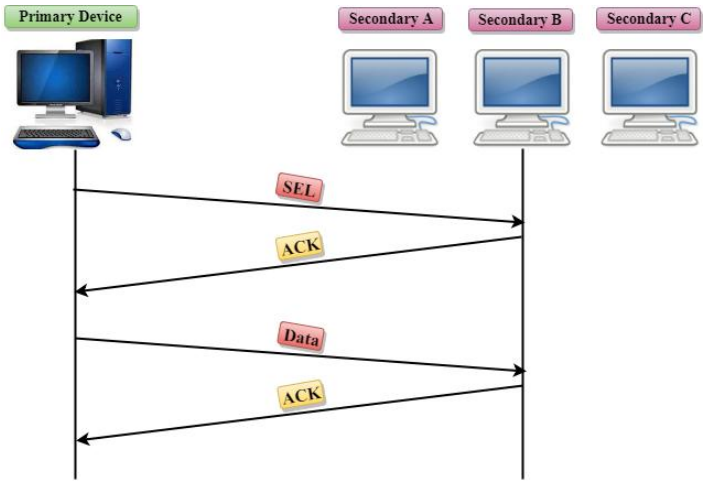
Working of Poll/Select

- In this, the primary device and multiple secondary devices consist of a single transmission line, and all the exchanges are made through the primary device even though the destination is a secondary device.
- The primary device has control over the communication link, and the secondary device follows the instructions of the primary device.

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

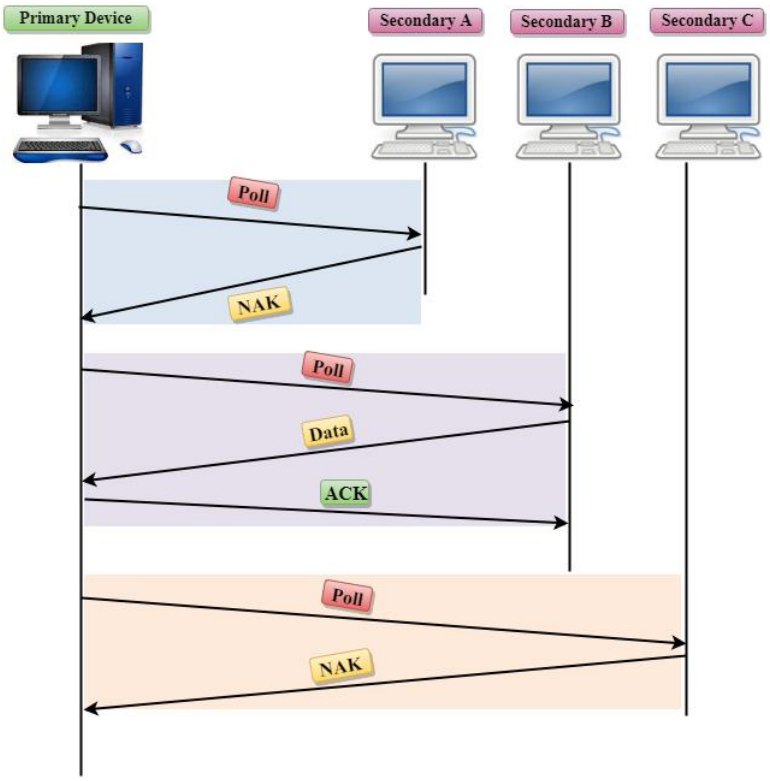
Select

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



Poll

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



2) **Flow Control**

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

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

a) Stop-and-wait
b) Sliding window

a) Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

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

Disadvantage of Stop-and-wait

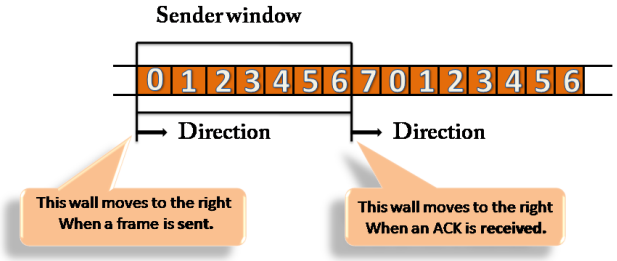
Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link.

b) Sliding Window

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

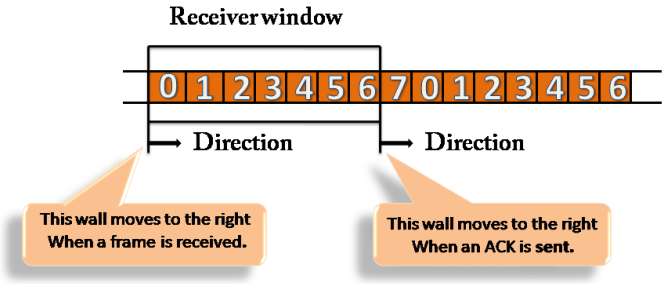
Sender Window

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



Receiver Window

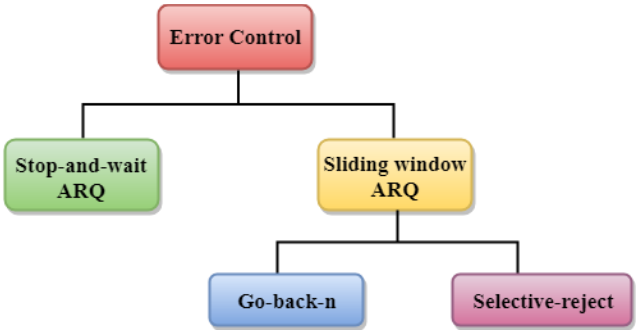
- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- The receiver window does not represent the number of frames received, but it represents the number of frames that can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



3) **Error Control**

Error Control is a technique of error detection and retransmission.

Categories of Error Control:



Stop-and-wait ARQ

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

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

Four features are required for the retransmission:

a) The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly.

b) Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0

frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame.

c) If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data.
d) It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame.

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame.
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame.

Sliding Window ARQ

SlidingWindow ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

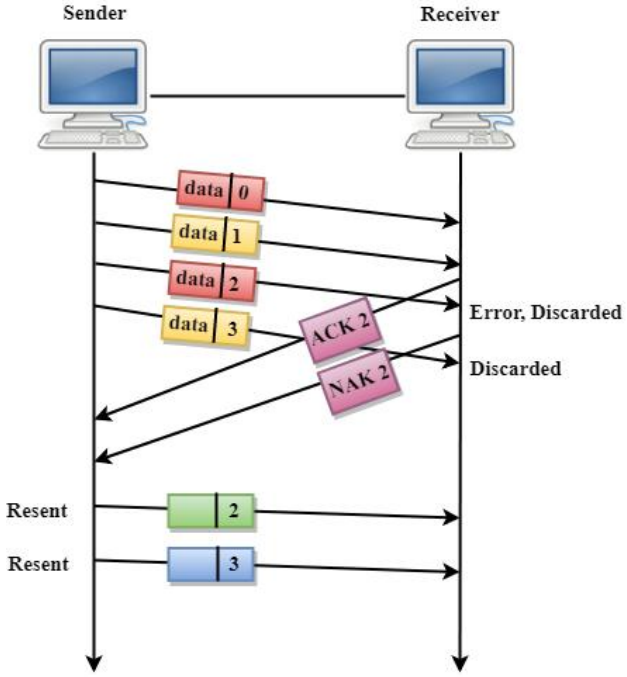
a) In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly.
b) The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

Two protocols used in sliding window ARQ:

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

Three possibilities can occur for retransmission:

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

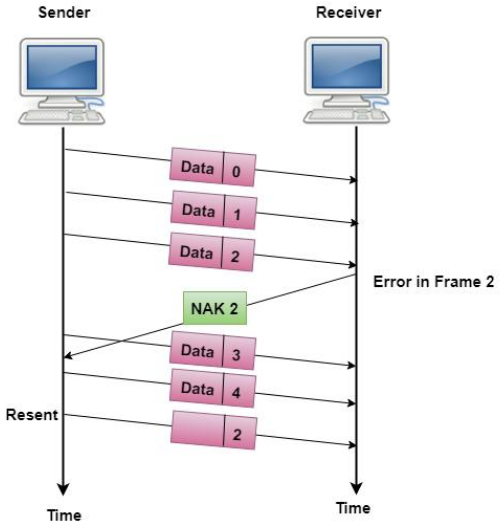


In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame.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

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame.
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK.

Selective-Reject ARQ

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



Flow Control and Error Control

Flow Control

It is an important function of the Data Link Layer. It refers to a set of procedures that tells the sender how much data it can transmit before waiting for acknowledgment from the receiver.

Purpose of Flow Control:

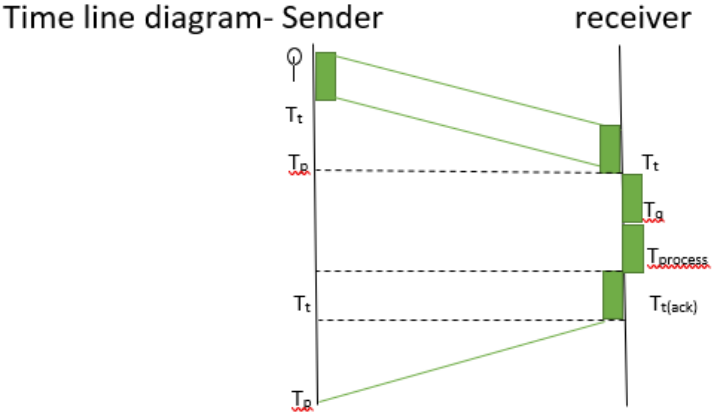
Any receiving device has a limited speed at which it can process incoming data and also a limited amount of memory to store incoming data. If the source is sending the data at a faster rate than the capacity of the receiver, there is a possibility of the receiver being swamped. The receiver will keep losing some of the frames simply because they are arriving too quickly and the buffer is also getting filled up.

This will generate waste frames on the network. Therefore, the receiving device must have some mechanism to inform the sender to send fewer frames or stop transmission temporarily. In this way, flow control will control the rate of frame transmission to a value that can be handled by the receiver.

Example – Stop & Wait Protocol

It is the simplest flow control method in which the sender will send the packet and then wait for the acknowledgement by the receiver that it has received the packet then it will send the next packet.

Stop and wait protocol is very easy to implement.



Total time taken to send is,

Ttotal = Tt(data) + Tp + Tq + Tprocess + Tt(ack) + Tp

(since, Tq and Tprocess = 0)

Ttotal = Tt(data) + 2Tp + Tt(ack)

Ttotal = Tt(data) + 2Tp

(when Tt(ack) is negligible)

Efficiency

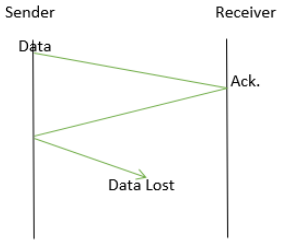
= useful time / total cycle time

= Tt / (Tt+2Tp)

= 1 / (1+2a) [a = Tp/Tt]

Note: Stop and wait is better for less distance. Hence it is a good protocol for LAN. Stop and wait is favorable for bigger packets.

What if the data packet is lost in between?



- According to sender, receiver is busy but actually data is lost.
- Receiver will assume, no packet has been sent by sender.
- Both will be waiting for each other and there will be a deadlock.

Need for timeout timer:

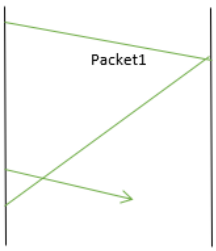
A timer is applied and the receiver will wait till the timeout timer for the data after that it will confirm that the data has been lost.

What if the data packet has been lost?

After timeout timer expires, sender will assume that the data is lost but actually the acknowledgement is lost. By assuming this it will send the data packet again but according to receiver it is a new data packet, hence it will give rise to duplicate packet problem.

To eliminate duplicate packet problem sequence number is added to the data packet. So using packet numbers it can easily determine the duplicate packets.

What if there is a delay in receiving acknowledgement?



According to sender, the acknowledgement of packet 1 is delayed and packet 2 has been lost. But the receiver assumes that the acknowledgement that has been received was of packet 2. This problem is called missing packet problem.
Missing packet problem can be solved if acknowledgements also have numbers.

Error Control

The error control function of the data link layer detects the errors in transmitted frames and re-transmits all the erroneous frames.

Purpose of Error Control:
The function of error control function of the data link layer helps in dealing with data frames that are damaged in transit, data frames lost in transit and acknowledged frames that are lost in transmission. The method used for error control is called Automatic Repeat Request (ARQ) which is used for the noisy channel.

Example – Stop & Wait ARQ and Sliding Window ARQ

- Used in Connection-oriented communication.
- It offers error and flows control
- It is used in Data Link and Transport Layers
- Stop and Wait for ARQ mainly implements the Sliding Window Protocol concept with Window Size 1

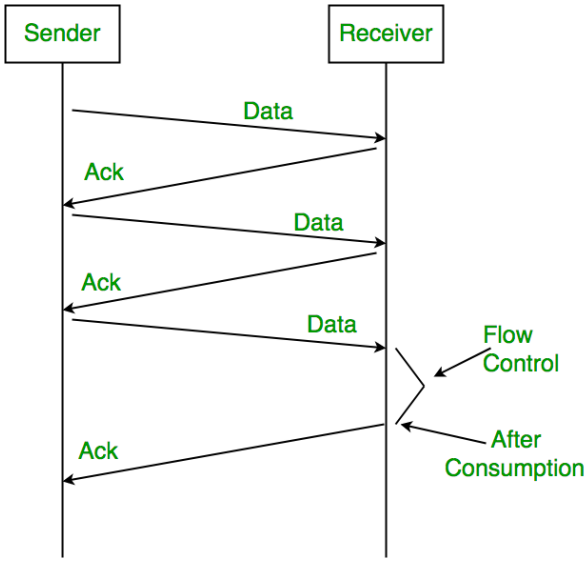
Useful Terms:

- **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.
- Propagation Delay = (Distance between routers) / (Velocity of propagation)
- RoundTripTime (**RTT**) = Amount of time taken by a packet to reach the receiver + Time taken by the Acknowledgement to reach the sender
- TimeOut (**TO**) = 2* RTT
- Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 255 seconds)

Simple Stop and Wait

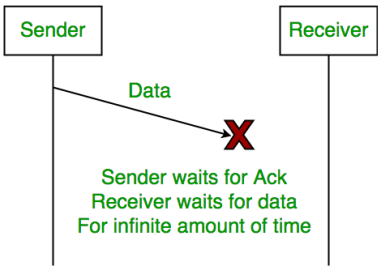
Sender:
Rule 1) Send one data packet at a time.
Rule 2) Send the next packet only after receiving acknowledgement for the previous.

Receiver:
Rule 1) Send acknowledgement after receiving and consuming a data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)

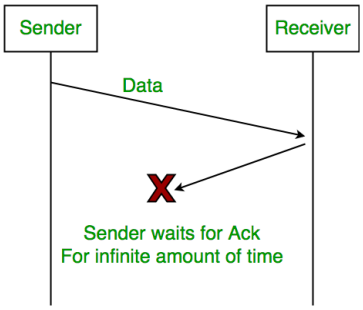


Problems:

1. **Lost Data**



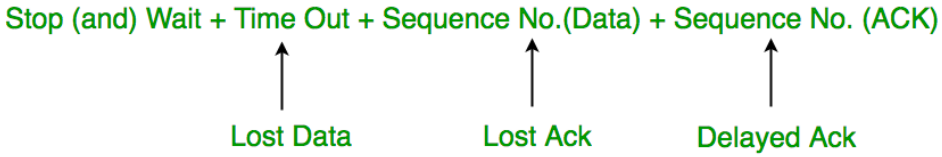
2. **Lost Acknowledgement:**



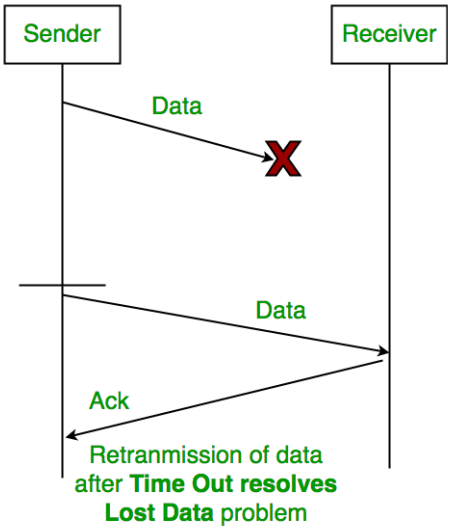
3. **Delayed Acknowledgement/Data:** After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait for ARQ (Automatic Repeat Request)

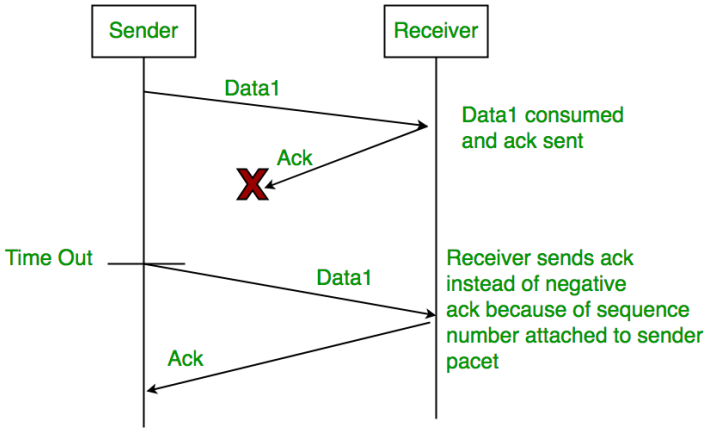
The above 3 problems are resolved by Stop and Wait for ARQ (Automatic Repeat Request) that does both error control and flow control.



1. **Time Out:**



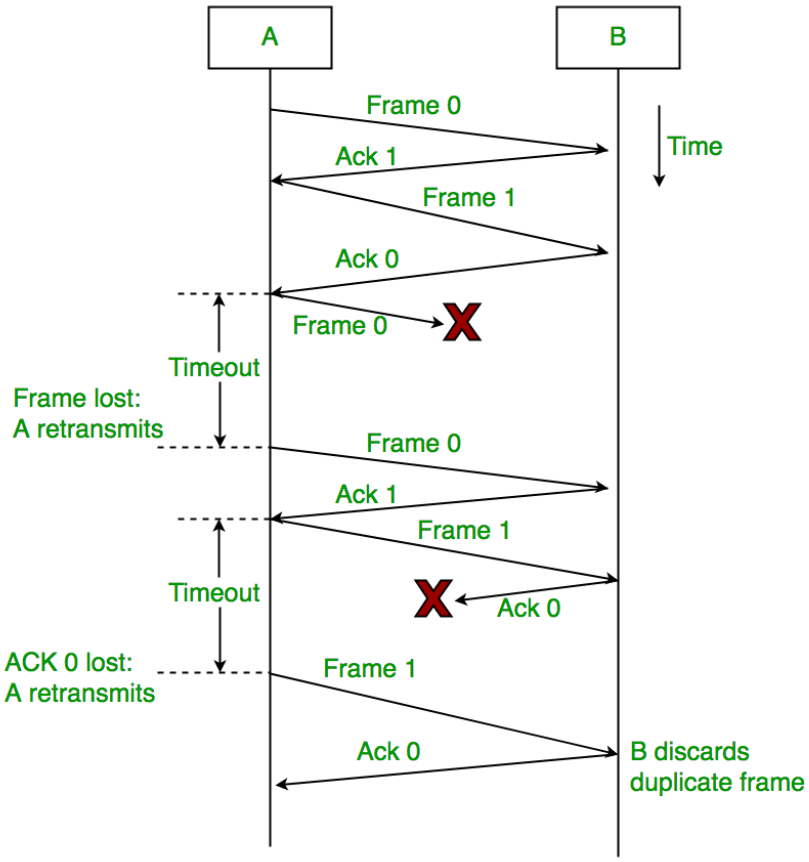
2. **Sequence Number (Data)**



3. **Delayed Acknowledgement:**
   This is resolved by introducing sequence numbers for acknowledgement also.

Working of Stop and Wait for ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving the data frame, sends an acknowledgement with sequence number 1 (the sequence number of the next expected data frame or packet)
   There is only a one-bit sequence number that implies that both sender and receiver have a buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ:

- It uses a link between sender and receiver as a half-duplex link
- Throughput = 1 Data packet/frame per RTT
- If the Bandwidth*Delay product is very high, then they stop and wait for protocol if it is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example of "**Closed Loop OR connection-oriented** " protocols
- It is a special category of SWP where its window size is 1
- Irrespective of the number of packets sender is having stop and wait for protocol requires only 2 sequence numbers 0 and 1

Constraints:

Stop and Wait ARQ has very less efficiency, it can be improved by increasing the window size. Also, for better efficiency, Go back N and Selective Repeat Protocols are used.

The Stop and Wait ARQ solves the main three problems but may cause big performance issues as the sender always waits for acknowledgement even if it has the next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country through a high-speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence number. We will be discussing these protocols in the next articles.

So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections but performs badly for distant connections like satellite connections.

Advantages of Stop and Wait ARQ :

- **Simple Implementation:** Stop and Wait ARQ is a simple protocol that is easy to implement in both hardware and software. It does not require complex algorithms or hardware components, making it an inexpensive and efficient option.
- **Error Detection:** Stop and Wait ARQ detects errors in the transmitted data by using checksums or cyclic redundancy checks (CRC). If an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, indicating that the data needs to be retransmitted.
- **Reliable:** Stop and Wait ARQ ensures that the data is transmitted reliably and in order. The receiver cannot move on to the next data packet until it receives the current one. This ensures that the data is received in the correct order and eliminates the possibility of data corruption.
- **Flow Control:** Stop and Wait ARQ can be used for flow control, where the receiver can control the rate at which the sender transmits data. This is useful in situations where the receiver has limited buffer space or processing power.
- **Backward Compatibility:** Stop and Wait ARQ is compatible with many existing systems and protocols, making it a popular choice for communication over unreliable channels.

Disadvantages of Stop and Wait ARQ:

- **Low Efficiency:** Stop and Wait ARQ has low efficiency as it requires the sender to wait for an acknowledgment from the receiver before sending the next data packet. This results in a low data transmission rate, especially for large data sets.
- **High Latency:** Stop and Wait ARQ introduces additional latency in the transmission of data, as the sender must wait for an acknowledgment before sending the next packet. This can be a problem for real-time applications such as video streaming or online gaming.
- **Limited Bandwidth Utilization:** Stop and Wait ARQ does not utilize the available bandwidth efficiently, as the sender can transmit only one data packet at a time. This results in underutilization of the channel, which can be a problem in situations where the available bandwidth is limited.
- **Limited Error Recovery:** Stop and Wait ARQ has limited error recovery capabilities. If a data packet is lost or corrupted, the sender must retransmit the entire packet, which can be time-consuming and can result in further delays.
- **Vulnerable to Channel Noise:** Stop and Wait ARQ is vulnerable to channel noise, which can cause errors in the transmitted data. This can result in frequent retransmissions and can impact the overall efficiency of the protocol.

Difference between Flow Control and Error Control

S.No.	Flow control	Error control
1.	Flow control is meant only for the transmission of data from sender to receiver.	Error control is meant for the transmission of error free data from sender to receiver.
2.	For Flow control there are two approaches: Feedback-based Flow Control and Rate-based Flow Control.	To detect error in data, the approaches are: Checksum, Cyclic Redundancy Check and Parity Checking. To correct error in data, the approaches are: Hamming code, Binary Convolution codes, Reed-Solomon code, Low-Density Parity Check codes.
3.	It prevents the loss of data and avoid over running of receive buffers.	It is used to detect and correct the error occurred in the code.
4.	Example of Flow Control techniques are: Stop & Wait Protocol and Sliding Window Protocol.	Example of Error Control techniques are: Stop & Wait ARQ and Sliding Window ARQ (Go-back-N ARQ, Selected Repeat ARQ).

Elementary Data Link Layer Protocols

When the data link layer receives a packet, it is encapsulated in a frame, including a data link header and trailer. A frame is made up of an embedded packet that carries control information as well as a checksum. The hardware computes the checksum when a frame arrives at the receiver. If an error is discovered, it is reported to the data link layer. If no errors are detected, it simply checks the control data in the header and sends the packet to the network's layer.

Primary data link layer protocol Classification

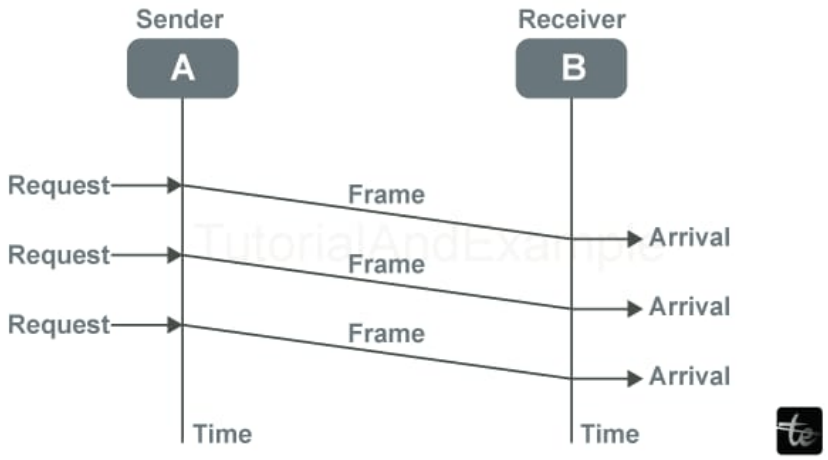
Elementary Data Link protocols are divided into three types, as shown below-

a) Protocol 1 – Unrestricted simplex protocol
b) Protocol 2 – Simplex stop-and-wait protocol
c) Protocol 3 – Simplex protocol for noisy channels.

a) Unrestricted simplex protocol:

Data transmission is only done in one direction. Transmission (Tx) and reception (Rx) are always available; processing time is irrelevant. This protocol has an infinite buffer space and no faults, meaning no damaged or lost frames.

The graphic below depicts the Unrestricted Simplex Protocol-



b) Simplex stop-and-wait protocol:

This protocol assumes that data is only transferred in one way. There is no inaccuracy; the receiver can only process data constantly. These assumptions imply that the transmitter cannot send frames faster than the receiver can process them. The critical issue here is preventing the transmitter from flooding the receiver. The typical solution for this problem is for the receiver to provide feedback to the sender; the approach is as follows:

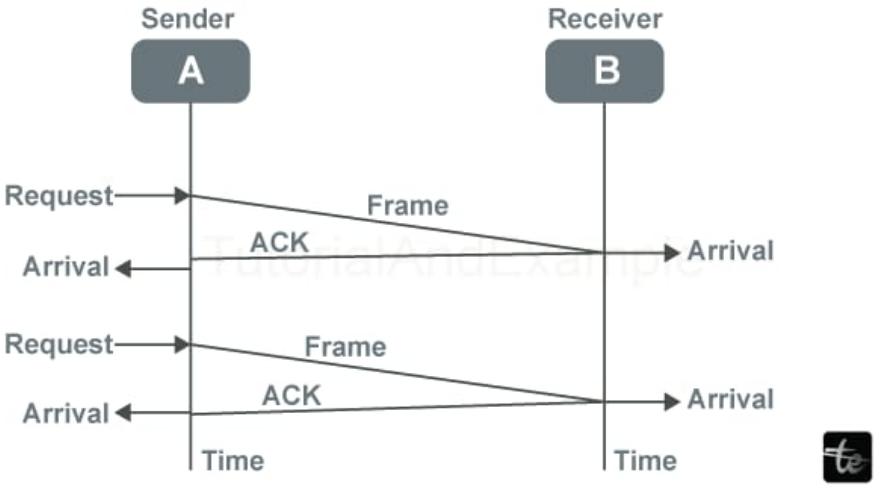
Step 1: The acknowledgement frame is returned to the sender, informing it that the most recently received frame has been processed and transmitted to the host.

Step 2: Permission is granted to send the following frame.

Step 3: The sender must wait for an acknowledgement frame from the receiver after transmitting the sent frame preceding sending another frame.

The Simplex stop-and-wait protocol is utilized when the sender sends one frame and waits for the recipient's response. When an acknowledgement is received, the sender sends the frame as below.

The Simplex Stop & Wait Protocol is depicted diagrammatically as follows-



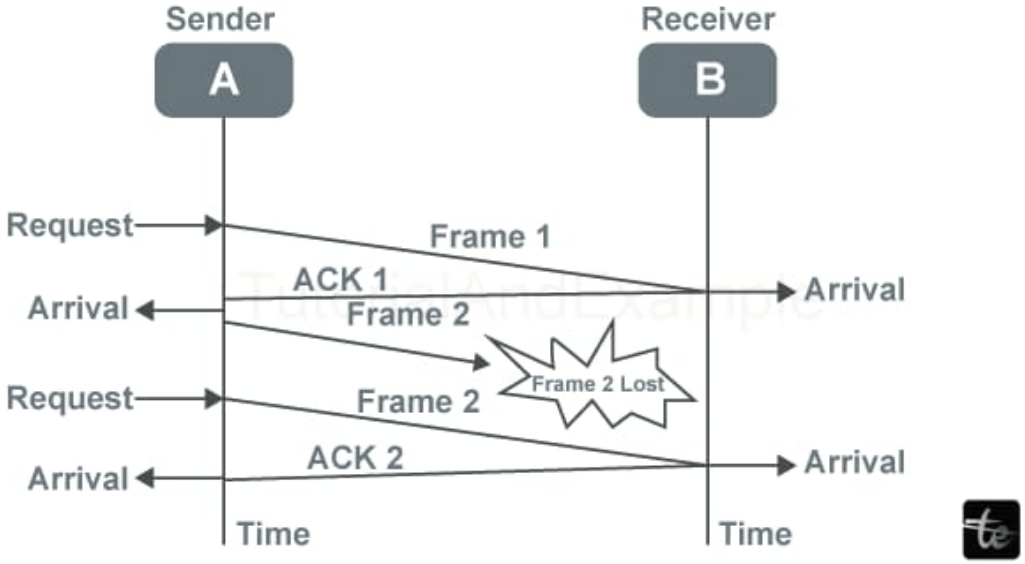
c) Simplex protocol for noisy channels:

Data transfer is one-way, with a separate recipient and sender, restricted processing capacity & speed at the receiver, and errors in data frames & acknowledgement frames to be expected due to the noisy channel. Each frame has its sequence number.

The timer is initiated for a limited time after a frame is transferred. If the acknowledgement isn't received before the timer ends, the frame is retransmitted; if the

acknowledgement is malformed or the transferred data frames are damaged, the sender must wait indefinitely before transmitting the next frame.

The Simplex Protocols for Noisy Channels are depicted diagrammatically as follows-



Data Link Layer Devices

The Data Link Layer employs several devices, which are described below.

- **Bridge:** A bridge is an electrical device used in computer networking that aids in establishing connections with another bridge using a comparable protocol.
- **Switches:** A switch is a hardware device that connects numerous devices via a network at the data link layer of the OSI model. It employs multiple packet-switching techniques to receive and send data packets across the network.
- **Modem:** A modem is a "Modulator - De-modulator" and transfers information via telephone lines from one computer network to another.
  The modulator converts all data from digital to analogue over the transmitting point and the opposite end. De-Modulators can transform analogue signals to digital signals when in reception mode.
- **Network Interface Card:** Also referred to as a "Network Interface Controller", "Network Adapter"/"LAN Adapter". A network interface card, or a NIC, is a circuit board used in computer systems to offer a dedicated network connection.

Data Link Layer Protocol Examples:

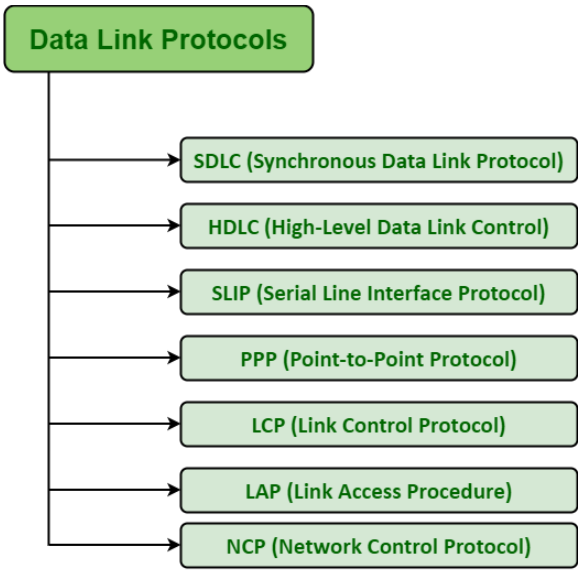
Some Examples of Major Data Link Protocols: Wide Area Networks (WAN) and modem connections require multiple data link protocols. Logical communication Control (LLC) is a data communication protocol commonly used in LANs. Some instances of data link protocols are as follows:

List of Data Link Layer Protocols

a) Synchronous Data Link Protocol (SDLC)
b) High-Level Data Link Protocol (HDLC)
c) Serial Line Interface Protocol (SLIP)
d) Point to Point Protocol (PPP)
e) Link Control Protocol (LCP)

f) Link Access Procedure (LAP)

g) Network Control Protocol (NCP)



a) Synchronous Data Link Protocol (SDLC)

SDLC protocol was developed by International Business Machine (IBM) in mid-1970s for its use in environments of Systems Network Architecture (SNA). SDLC is first link-layer protocol that is based in synchronous, bit-oriented operation.

Data Link Layer generally provides error-free transmission of data among Network Addressable Units (NAUs) within given network of communication via this SDLC protocol.

There are generally two types of links:

- **I/O Channel Communication link –**These links are basically hard-wired among all co-located nodes. They also usually operate at almost high rate of data and generally error-free.
- **Non-I/O Channel Communication Link –**These links generally use some form of data communications equipment to transmit data among several nodes. SDLC protocol is basically required to ensure error-free performance over all these links.

SDLC was initially used in Wide Area Network (WANs) that basically use leased line simply to connect mainframe SNA hosts and remote terminals. SDLC is also equivalent to layer 2 of Open System Interconnection (OSI) model of network communication. It is primary protocol that is very essential in entire layering and data transfer process.

SDLC also supports various types of architectures as given below:

- Normal Disconnected Mode (NDM) and Normal Response Mode (NRM)
- Two-way alternate (half-duplex) data flow
- Secondary station point-to-point, multipoint, and multi-multipoint configurations
- Primary station point-to-point and multipoint configurations
- Modulo 8 transmit-and-receive sequence counts
- Nonextended (single-byte) station address

Types of network nodes in SDLC:

SDLC generally identifies and describes two types of Network nodes as given below :

1) **Primary Node –**The primary node is generally responsible for handling all secondary nodes and also responsible for controlling all operations and links. Data is processed only through this node. This node polls secondaries in predetermined order and then secondaries can then send if they have any data to be sent. This node also sets up and tears down links and manages link while it is operational.
2) **Secondary Node –**A secondary node is generally responsible for sending all of data that is being received to primary node. This node is controlled by primary node i.e., secondaries will only transmit data to primary only if primary allows and grants permission to do so.

Basic Configurations followed by SDLC nodes:

SDLC primary and secondary node generally gets connected in four different basic configurations as given below:

- **Point-to-Point -** As the name suggests, in Point-to-Point configuration, there are only two nodes. One node is primary and other one is secondary node.
- **Multipoint –**As the name suggests, in Multipoint configuration, there are multiple nodes. One node is primary and all of other are secondary nodes. It is also known as multidrop configuration. In this, secondaries are polled separately in predefined sequence.
- **Loop –**As the name suggests, in Loop configuration, primary node is connected to first secondary node and last secondary node in loop. In simple words, primary node is connected to secondary nodes and has two nodes on either side. In this, intermediate secondary nodes transmit data through one another as they give responses to primary requests.
- **Hub go-ahead –** This configuration generally involves inbound and outbound channels. The primary node simply requires outbound channel to transmit data with secondary node whereas secondary node simply requires inbound channel to transmit data with primary node.

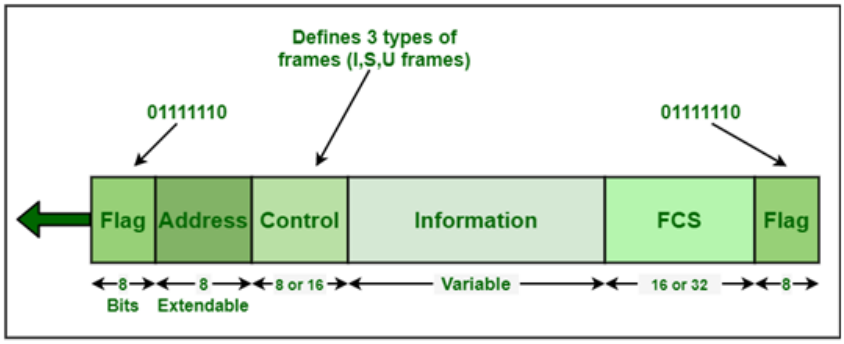
b) High-Level Data Link Protocol (HDLC)

HDLC is a protocol that has become a catch-all for several Wide Area protocols. It is also a component of the X.25 network. ISO conceived and developed it in 1979. In general, this protocol is built on SDLC. It also provides both unreliable best-effort service as well as accurate service. HDLC is a bit-oriented protocol that can communicate in point-to-point and multipoint modes.

Basic Frame Structure of HDLC

High-Level Data Link Control (HDLC) generally uses term “frame” to indicate and represent an entity of data or a protocol of data unit often transmitted or transferred from one station to another station. Each and every frame on link should begin and end with Flag Sequence Field (F). Each of frames in HDLC includes mainly six fields. It begins with a flag field, an address field, a control field, an information field, an frame check sequence (FCS) field, and an ending flag field. The ending flag field of one frame can serve as beginning flag field of the next frame in multiple-frame transmissions.

The basic frame structure of HDLC protocol is shown below:



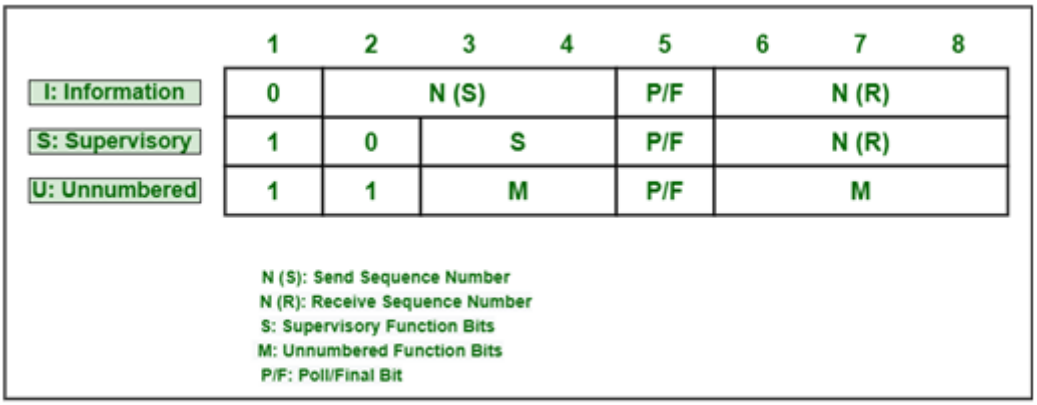
Basic Frame Structure

Size of Different Fields:

Field Name	Size (bits)
Flag Field	8 bits
Address Field	8 bits
Control Field	8 or 16 bits
Information Field	Variable (not used in some type of HDLC frames)
FCS (Frame Check Sequence) Field	16 or 32 bits
Closing Flag Field	8 bits

Let us understand these fields in details:

- **Flag Field –**The flag field is generally responsible for initiation and termination of error checking. In HDLC protocol, there is no start and stop bits. So, the flag field is basically using delimiter 0x7e to simply indicate beginning and end of frame.
  It is an 8-bit sequence with a bit pattern 01111110 that basically helps in identifying both starting and end of a frame. This bit pattern also serves as a synchronization pattern for receiver. This bit pattern is also not allowed to occur anywhere else inside a complete frame.
- **Address Field –**The address field generally includes HDLC address of secondary station. It helps to identify secondary station will sent or receive data frame. This field also generally consists of 8 bits therefore it is capable of addressing 256 addresses. This field can be of 1 byte or several bytes long, it depends upon requirements of network. Each byte can identify up to 128 stations.
  This address might include a particular address, a group address, or a broadcast address. A primary address can either be a source of communication or a destination that eliminates requirement of including address of primary.
- **Control Field –**HDLC generally uses this field to determine how to control process of communication. The control field is different for different types of frames in HDLC protocol. The types of frames can be Information frame (I-frame), Supervisory frame (S-frame), and Unnumbered frame (U-frame).



Control Field Format

This field is a 1-2-byte segment of frame generally requires for flow and error control. This field basically consists of 8 bits but it can be extended to 16 bits. In this field, interpretation of bits usually depends upon the type of frame.

- **Information Field –**This field usually contains data or information of users sender is transmitting to receiver in an I-frame and network layer or management information in U-frame. It also consists of user's data and is fully transparent. The length of this field might vary from one network to another network. Information field is not always present in an HDLC frame.
- **Frame Check Sequence (FCS) –**FCS is generally used for identification of errors i.e., HDLC error detection. In FCS, CRC16 (16-bit Cyclic Redundancy Check) or CRC32 (32-bit Cyclic Redundancy Check) code is basically used for error detection. CRC calculation is done again in receiver. If somehow result differs even slightly from value in original frame, an error is assumed.
  This field can either contain 2 byte or 4 bytes. This field is a total 16 bit that is required for error detection in address field, control field, and information field. FCS is basically calculated by sender and receiver both of a data frame. FCS is used to confirm and ensure that data frame was not corrupted by medium that is used to transfer frame from sender to receiver.

c) SLIP (Serial Line Interface Protocol)

SLIP is an outdated protocol that adds a framing byte to the end of an IP packet. A data link control capability is required for sending IP packets over a dial-up link between Internet Service Providers (ISPs) and residential users. It is a TCP/IP encapsulation created for communication through serial ports and multiple router connections. It has shortcomings, such as the need for error correction or detection tools.

SLIP stands for **Serial Line Internet Protocol**. It is a TCP/IP implementation which was described under **RFC 1055 (Request for Comments)**. SLIP establishes point to point serial connections which can be used in dial-up connections, serial ports and routers. It frames the encapsulated IP packets across a serial line for establishing connection while using line speed between 12000 bps and 19.2 Kbps.

SLIP was introduced in 1984 when Rick Adams used it to connect 4.2 Berkeley Unix and Sun Microsystems workstations. It soon caught up with the rest of the world as a credible TCP/IP implementation. It has now become obsolete after being replaced by PPP (Point to Point Protocol) which solves many deficiencies present in it.

Characteristics

1) It introduces two special characters END(decimal 192) and ESC(decimal 129). Depending, on whether data byte code represents END or ESC character, the two byte sequence of ESC and octal 334 or ESC and octal 335 respectively is sent in data packet.
2) There is no maximum packet size in SLIP since it has no standard specification. However, the widely accepted value is 1006 bytes of datagram for both sending and receiving.
3) The sender and receiver should be aware of IP address for both ends while using SLIP.
4) It only supports static assignment during IP addressing.
5) It transfers data in synchronous form.
6) A SLIP frame consists of a payload (data) and a flag to act as a end delimiter.

Advantages

1) It can allow different combinations of network configurations such as host-host, host-router, router-router etc.
2) It can be easily used in microcontrollers because of small overhead.
3) It is easy to implement being a basic packet protocol and due to wide application of TCP/IP.

Disadvantages

1) It does not perform any authentication of data and IP addresses cannot be dynamically assigned while using SLIP.
2) SLIP provides no type identification method. The type of protocol sent cannot be detected. Hence, only one protocol can run over a SLIP connection.
3) It has no error detection or correction mechanism in data transmission.
4) A SLIP connection provides no mechanism for hosts to communicate addressing information.
5) SLIP provides no compression features to improve packet throughput. CSLIP was a variant used for same purpose but it could not achieve wide application.

d) PPP (Point-to-Point Protocol)

PPP is Windows' default Remote Access Service (RAS) protocol and is Data Link Layer (DLL) protocol used to encapsulate higher network layer protocols to pass through synchronous and asynchronous lines of communication. Initially created as an encapsulation protocol to carry numerous layer of network traffic over point-to – point connections. In addition, PPP settled various measures including asynchronous and bit-oriented synchronous encapsulation, multiplexing of network protocols, negotiation of sessions, and negotiation of data-compression. PPP also bolsters non-TCP / IP protocols, such as IPX / SPX and DECnet. A prior standard known as Serial Link Internet Protocol (SLIP) has been largely supplanted by it. PPP provides wide variety of configurable options to make it robust option to exemplify data over leased lines. Above all, PPP underpins verification, which can be used at either end of point-to-point association to confirm identity of equipment or clients. Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) can both be used on Cisco router for validation.

History of PPP : PPP returns to late 1980s, when true standard for sequential IP executions was SLIP. RFC 1134, distributed in 1989, was principal formal IETF report identified with PPP. This RFC isn't just standard yet proposal for what could be characterized as primary PPP standard, RFC 1171, in 1990. This early report has been re-examined numerous times and included few different records characterizing different protocols that contain entire PPP suite. Instead of trying to create PPP from scratch, IETF built PPP on basis of ISO High-Level Data Link Control (HDLC) protocol, which was initially developed by IBM. Developers of PPP adopted its framing mechanism from HDLC protocol and component of its general operation.

Features of PPP:

a) **Packet Framing –** Network layer data packet formulation within data link block.
b) **Multi-Protocol –** Yield information from any NCP network layer upwards at same time as demultiplex.
c) **Bit Transparency –** Should carry certain bit pattern in field of data.
d) **Error Detection –** No modification.

Components of PP

It uses three components to allow PPP to transmit data over serial point-to – point link. Each part has its own autonomous role and entails use of other two unabridged its tasks. These three components are :

a) **High-Level Data-Link Control (HDLC) protocol –** HDLC is method used to frame data over PPP links. On account of PPP, the standard version of OSI is used instead of proprietary version of Cisco. This standardization assists in ensuring that different vendors can properly communicate PPP executions.
b) **Link Control Protocol (LCP) –** It is liable for formulating, configuring, testing, sustaining and terminating transmission links. Additionally, two endpoints of connections impart negotiation for setting up of alternatives and use of features.
c) **Network Control Protocols (NCPs) –** NCP frames are used to communicate and customize protocols on Network layer that can be used over PPP session. There is one NCP for every higher-layer protocol that is upheld by PPP. NCPs enable PPP to work over analogous connection in consonance with many Network layer protocols.

Working of PPP

PPP jointly uses these three components to enable communication. There are four main steps to establish, maintain and terminate PPP session:

- **Step-1:** Initial step of setting up PPP session between devices includes both sending LCP link-establishment frame for configuration and testing purposes. Such frames also characterize which alternatives, for instance compression, authentication, and multilink, given PPP host chooses. If authentication is established and needed it will take place during this step.
- **Step-2:** It uses LCP frames to test link 's nature. Assembled data can be used to evaluate if links is appropriate for dealing different protocols on upper layer.
- **Step-3:** NCP frames are sent over link to determine which network layer protocols need configuration. For instance, connection to use IP, IPX, AppleTalk and so on can need to be optimized.

- **Step-4:** In this step, when ending PPP session, LCP link-termination frames are used to cut connection. Third category of LCP frame (Link-Maintenance) is often used for leveraging and troubleshooting PPP links.

Advantages of PPP:

- A key benefit of PPP is that it's an extensible suite of protocols.
- It bolsters authentication by PAP and CHAP.
- Quality management feature of links evaluates quality of links. PPP takes down link in case of too many errors.
- A mechanism of gradual framing, compared with single END character in SLIP.
- A sturdy process for negotiating link variables, including maximum possible frame size.

e) LCP (Link Control Protocol) - IEEE 802.2 was the first to develop and create it. It also provides HDLC-style services on local area networks (LANs). LCP is a PPP protocol for establishing, setting, testing, maintaining, and finishing/terminating links for data frame transmission.

f) Link Access Protocol (LAP) - LAP protocols are data link layer protocols used for data framing and transmission over point-to-point connections. It also includes details about service dependability. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services) are the three versions of LAP. It is derived via IBM SDLC, which IBM has submitted to the ISP for standardization.

g) Network Control Protocol (NCP) - NCP was another older protocol used by ARPANET. It allows users to use computers & various gadgets from remote locations and transmit files between two or more machines. PPP is often defined as a collection of protocols. Every higher-layer protocol supported by PPP has constant access to NCP. TCP/IP supplanted NCP in the 1980s.

Data Link Layer Functions

- **Linking and Framing:**The data link layer receives each packet from the network layer, bundles it into frames, and then moves every frame bit by bit using network hardware devices. The data link layer receives every signal from hardware devices & collects them into Frame form on the receiver side.
- **Addressing:**The data link layer generates the complete layer 2 addressing mechanism system, and then entire hardware addresses are identified as unique at the connection. It enables them to encode into hardware at the time of production.
- **Synchronization:**After sending all frames over the link, both machines should be synchronized to communicate.
- **Controlling Errors:**Some signals are having transition issues, and bits are being flipped due to a few issues. To discover those errors & precede them to recover to obtain the original data bits, it then forwards the error reporting system to the sender end.
- **Flow control:**Suppose numerous stations with varying speeds or capacities are offered on the same link. With flow control, the data link layer enables both machines to interchange data at comparable speeds.

- **Multi-Access:**If the host attempts to transport data over a shared link, the probability of collision increases. The data connection layer provides a CSMA/CD technique to allow various systems to access shared media.

Sliding Window Protocol

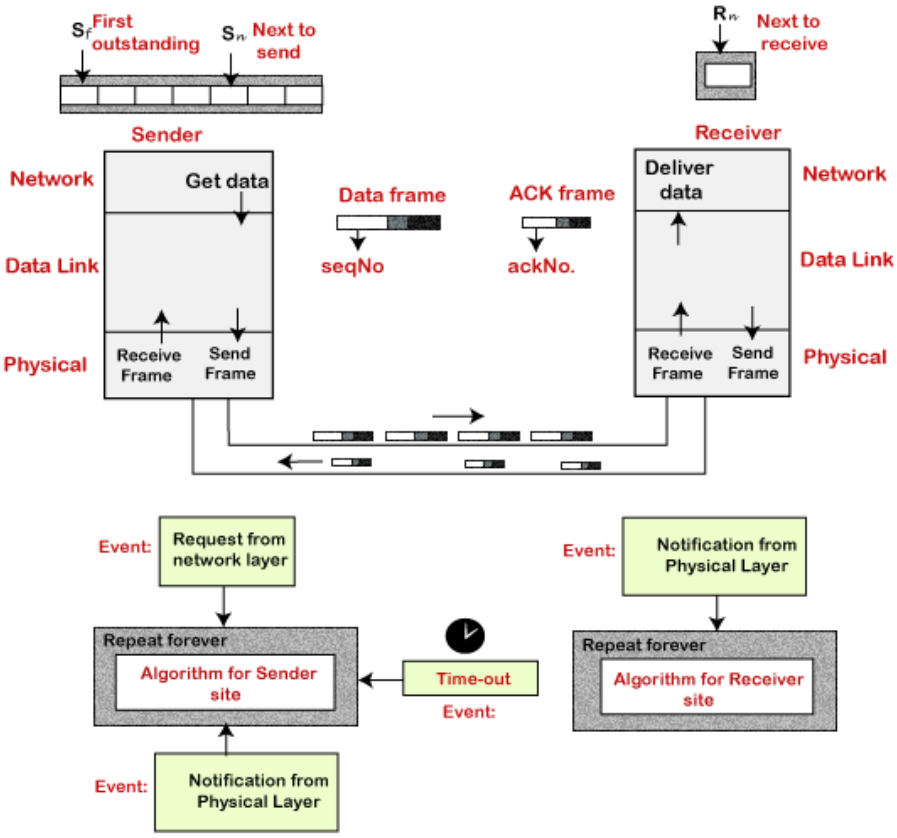
The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

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.

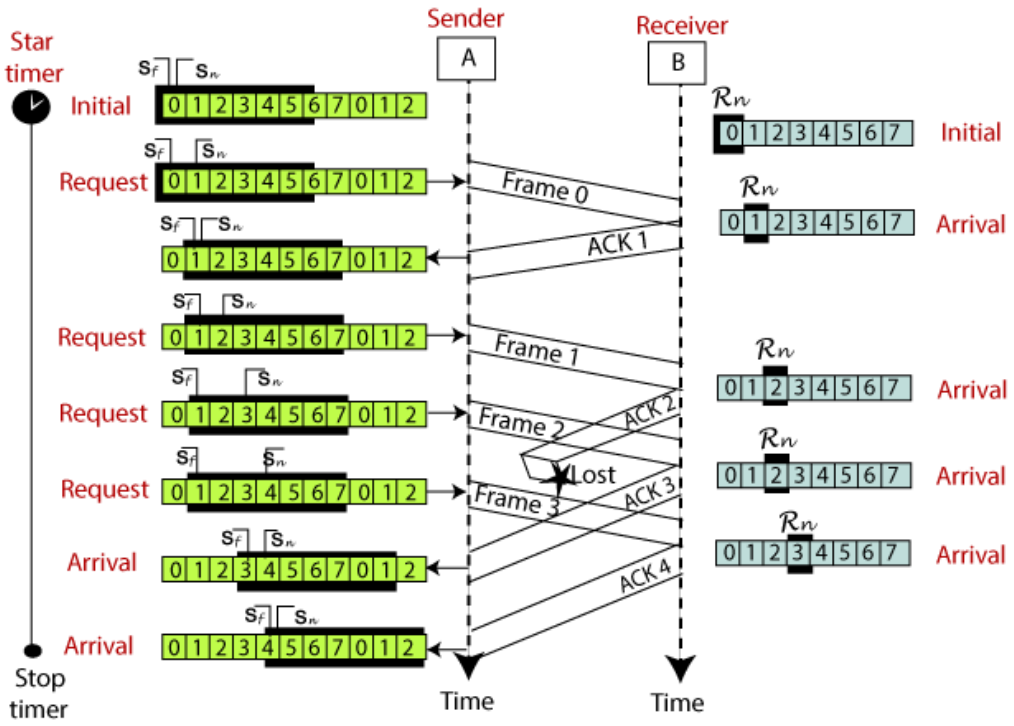
Types of Sliding Window Protocol
Sliding window protocol has two types:

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

1) **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.

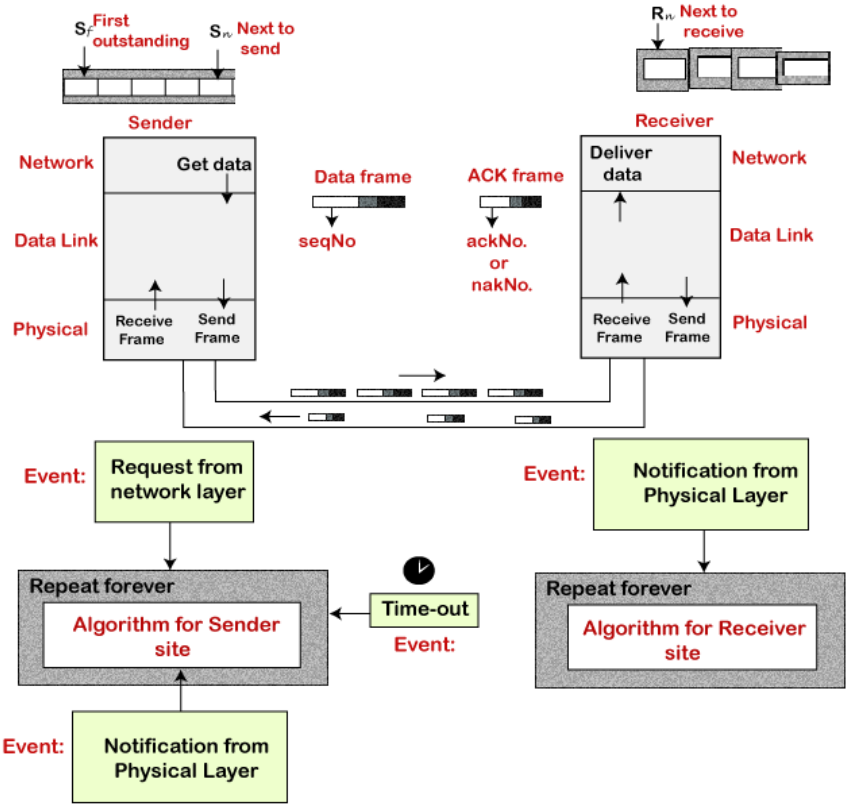


The example of Go-Back-N ARQ is shown below in the figure.

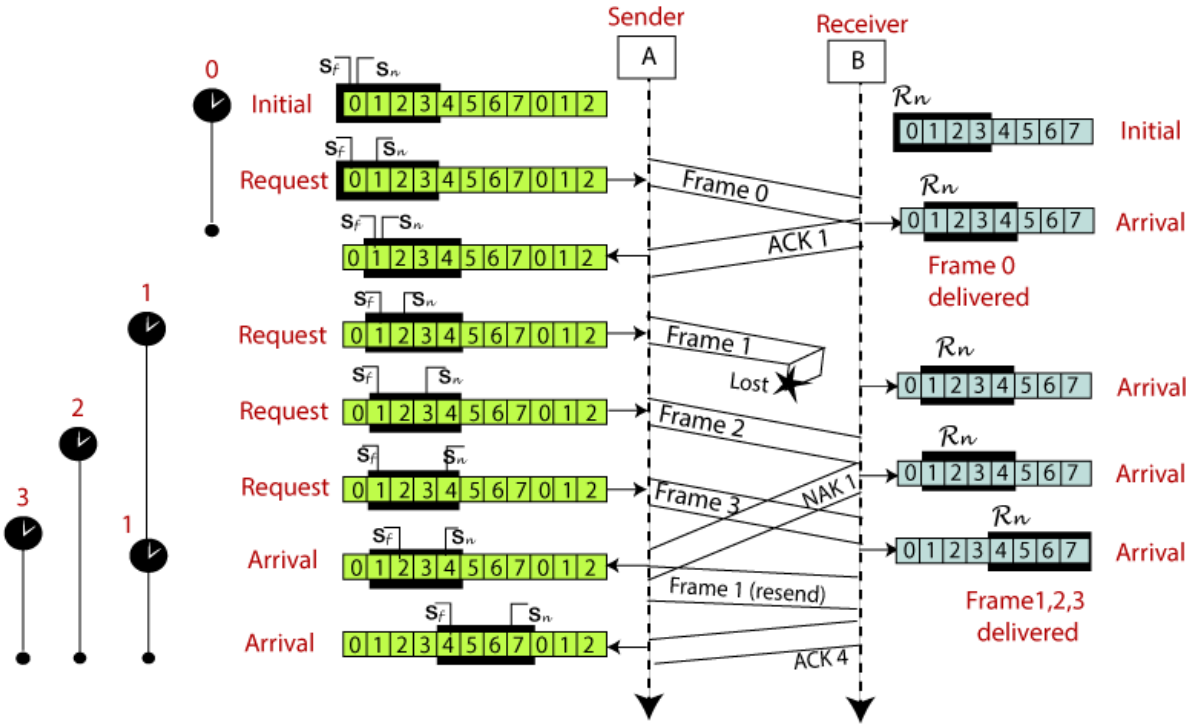


2) Selective Repeat ARQ

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.



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



Difference between the Go-Back-N ARQ and Selective Repeat ARQ

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

Medium Access Control

Introduction

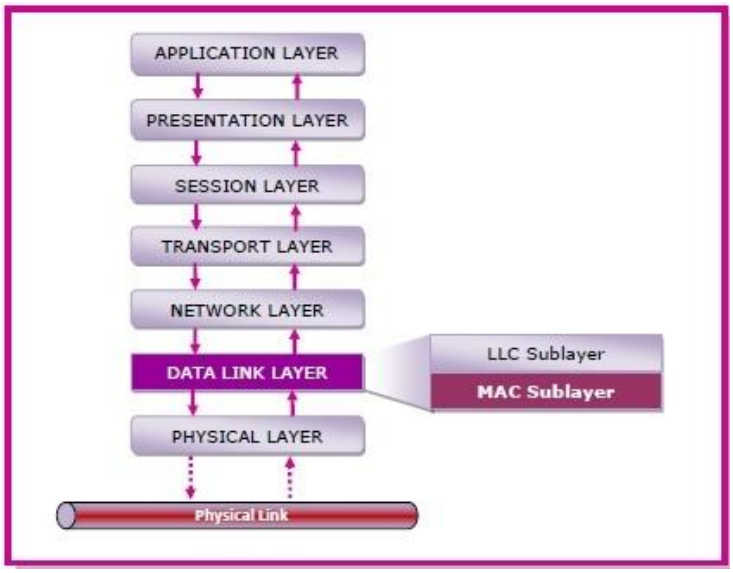
The Medium Access Control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels.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

MAC Layer in the OSI Model

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

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

The following diagram depicts the position of the MAC layer –



Functions of MAC Layer

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

MAC Addresses

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

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

Channel Allocation Problem

In a broadcast network, the single broadcast channel is to be allocated to one transmitting user at a time. When multiple users use a shared network and want to access the same network. Then channel allocation problem in computer networks occurs.

So, to allocate the same channel between multiple users, techniques are used, which are called channel allocation techniques in computer networks.

Channel Allocation Techniques

For the efficient use of frequencies, time-slots and bandwidth channel allocation techniques are used. There are three types of channel allocation techniques that you can use to resolve channel allocation problem in computer networks as follows:

a) Static channel allocation
b) Dynamic channel allocation
c) Hybrid channel allocation.

a) Static Channel Allocation

The traditional way of allocating a single channel between multiple users is called static channel allocation. Static channel allocation is also called fixed channel allocation. Such as a telephone channel among many users is a real-life example of static channel allocation.

The frequency division multiplexing (FDM) and time-division multiplexing (TDM) are two examples of static channel allocation. In these methods, either a fixed frequency or fixed time slot is allotted to each user.

b) Dynamic Channel Allocation

The technique in which channels are not permanently allocated to the users is called dynamic channel allocation. In this technique, no fixed frequency or fixed time slot is allotted to the user.

The allocation depends upon the traffic. If the traffic increases, more channels are allocated, otherwise fewer channels are allocated to the users.

This technique optimizes bandwidth usage and provides fast data transmission. Dynamic channel allocation is further categorized into two parts as follows:

Centralized dynamic channel allocation

Distributed dynamic channel allocation

The following are the assumptions in dynamic channel allocation:

- **Station Model:** Comprises N independent stations with a program for transmission.
- **Single Channel:** A single channel is available for all communication.
- **Collision:** If frames are transmitted at the same time by two or more stations, then the collision occurs.
- **Continuous or slotted time:** There is no master clock that divides time into discrete time intervals.

- **Carrier or no carrier sense:** Stations sense the channel before transmission.

c) Hybrid Channel Allocation

The mixture of fixed channel allocation and dynamic channel allocation is called hybrid channel allocation. The total channels are divided into two sets, fixed and dynamic sets. First, a fixed set of channels is used when the user makes a call. If all fixed sets are busy, then dynamic sets are used. When there is heavy traffic in a network, then hybrid channel allocation is used.

Difference between Static and Dynamic Channel Allocation

There are some differences between static and dynamic channel allocation. The following table shows the comparison of fixed channel allocation and dynamic channel allocation.

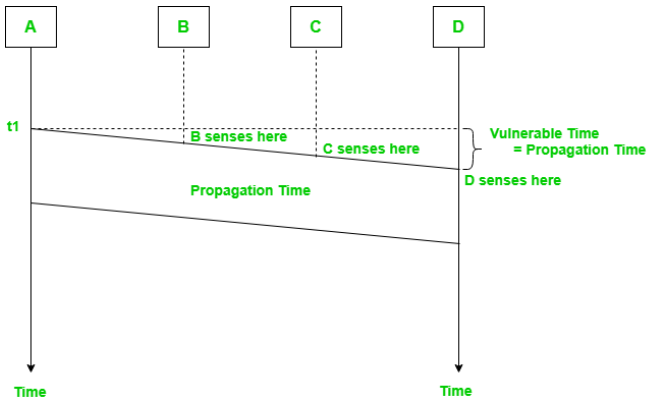
Fixed Channel allocation	Dynamic Channel allocation
In this technique, a fixed number of channels are allocated to the cells.	In this technique, channels are not permanently allocated to the cells.
Mobile station centre has fewer responsibilities.	The mobile station centre has more responsibilities.
The allocation is not dependent on traffic.	The allocation depends on the traffic.
Fixed channel allocation is cheaper than dynamic channel allocation.	Dynamic channel allocation is costly as compared to fixed channel allocation.
In this no need of complex algorithms.	Complex algorithms are used in this.

Carrier Sense Multiple Access (CSMA)

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

Vulnerable Time:

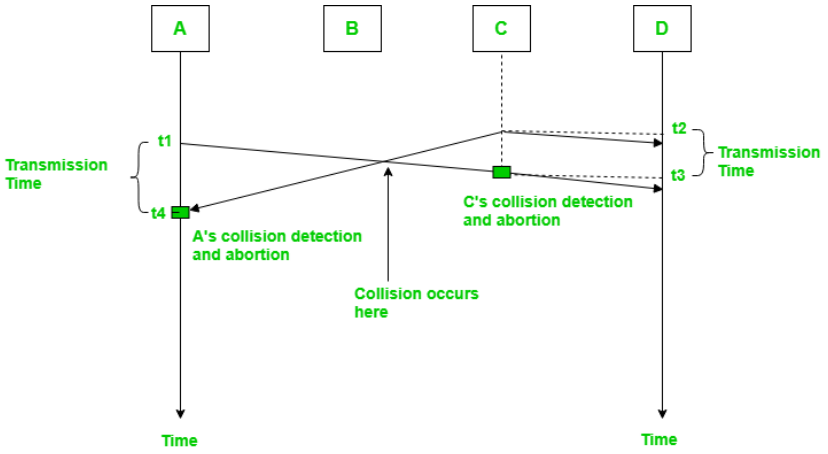
Vulnerable time = Propagation time (Tp)



The persistence methods can be applied to help the station take action when the channel is busy/idle.

1) Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

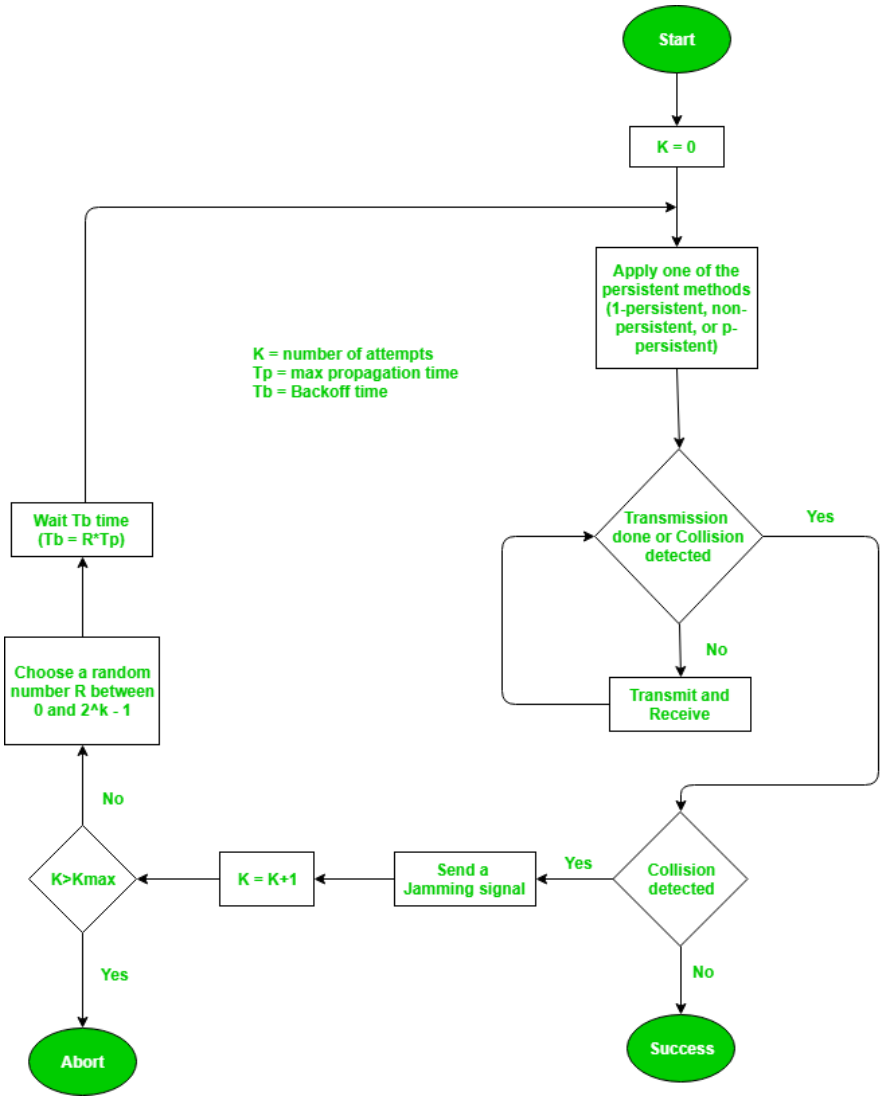
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.



In the diagram, *starts* sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.

Process: The entire process of collision detection can be explained as follows:



Throughput and Efficiency: The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For the 1-persistent method, throughput is 50% when G=1.
- For the non-persistent method, throughput can go up to 90%.

2) Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

a) **InterFrame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
b) **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.
c) **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

Characteristics of CSMA/CA :

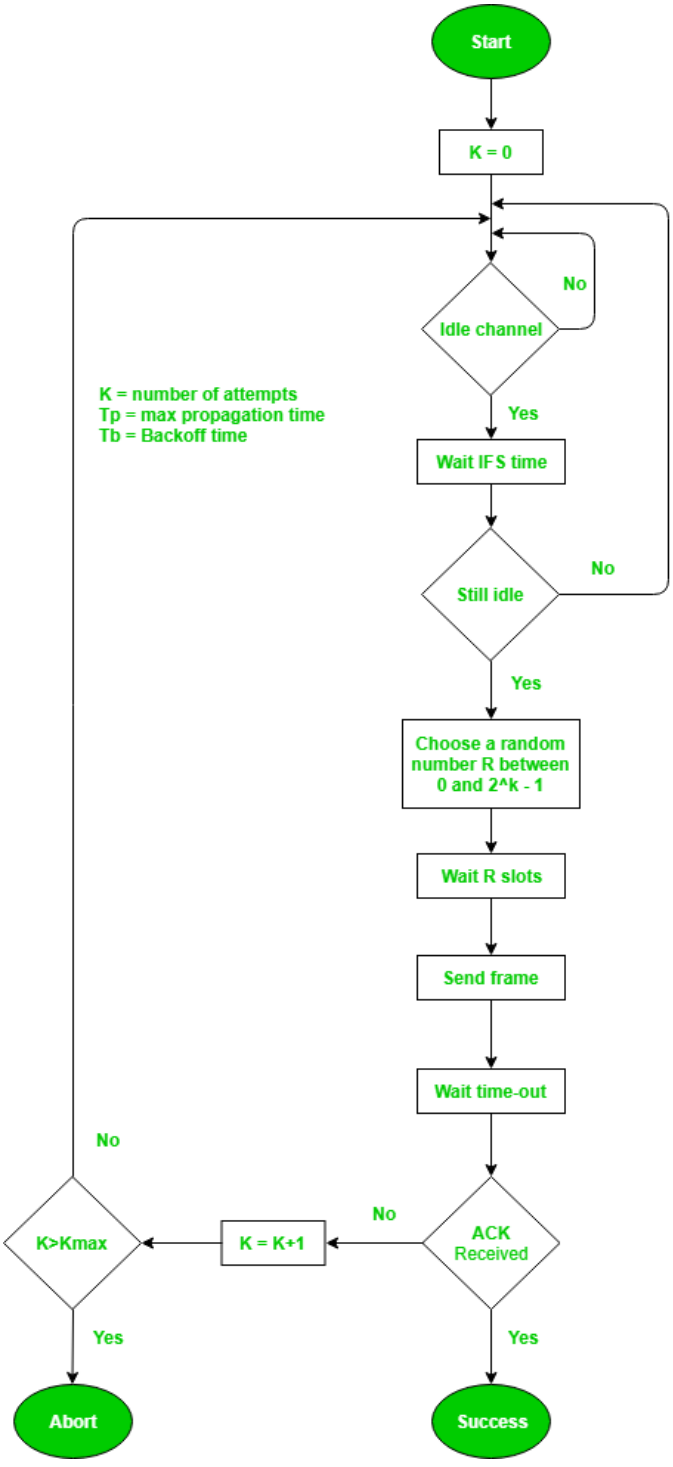
a) **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.
b) **Multiple Accesses**: Multiple devices share the same channel and can transmit simultaneously.
c) **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random back off time intervals to avoid collisions.
d) **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
e) **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
f) **Binary Exponential Back off**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.
g) **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
h) **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.

i) **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.

j) **Adaptive Behavior**: CSMA/CA can dynamically adjust its behavior in response to changes in network conditions, ensuring the efficient use of the channel and avoiding congestion.

Overall, CSMA/CA balances the need for efficient use of the shared channel with the need to avoid collisions, leading to reliable and fair communication in a wireless network.

Process: The entire process of collision avoidance can be explained as follows:



Types of CSMA Access Modes:

There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decide the time to start sending data across shared media.

a) **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and ***continuously*** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.

b) **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (***not continuously***), and when it discovers the channel is empty, it sends the frames.

c) **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the 1Persistent mode, and if the channel is idle, it sends a frame with a P probability. If the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.

d) **O-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

- **Advantages of CSMA:**
  - **Increased efficiency:** CSMA ensures that only one device communicates on the network at a time, reducing collisions and improving network efficiency.
  - **Simplicity:** CSMA is a simple protocol that is easy to implement and does not require complex hardware or software.
  - **Flexibility:** CSMA is a flexible protocol that can be used in a wide range of network environments, including wired and wireless networks.
  - **Low cost:** CSMA does not require expensive hardware or software, making it a cost-effective solution for network communication.
- **Disadvantages of CSMA:**
  - **Limited scalability:** CSMA is not a scalable protocol and can become inefficient as the number of devices on the network increases.
  - **Delay:** In busy networks, the requirement to sense the medium and wait for an available channel can result in delays and increased latency.
  - **Limited reliability:** CSMA can be affected by interference, noise, and other factors, resulting in unreliable communication.
  - **Vulnerability to attacks:** CSMA can be vulnerable to certain types of attacks, such as jamming and denial-of-service attacks, which can disrupt network communication.

Comparison of various protocols:

Protocol	Transmission behavior	Collision detection method	Efficiency	Use cases
Pure ALOHA	Sends frames immediately	No collision detection	Low	Low-traffic networks
Slotted ALOHA	Sends frames at specific time slots	No collision detection	Better than pure ALOHA	Low-traffic networks
CSMA/CD	Monitors medium after sending a frame, retransmits if necessary	Collision detection by monitoring transmissions	High	Wired networks with moderate to high traffic
CSMA/CA	Monitors medium while transmitting, adjusts behavior to avoid collisions	Collision avoidance through random backoff time intervals	High	Wireless networks with moderate to high traffic and high error rates

Difference between CSMA/CA and CSMA/CD

CSMA/CD stands for **Carrier Sense Multiple Access / Collision Detection** is a network protocol for carrier transmission. It is operated in the medium access control layer. It senses of the shared channel is busy for broadcasting and interrupts the broadcast until the channel is free. In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped, and a jam signal is sent by the stations and then the station waits for a random time context before retransmission.

CSMA/CA stands for **Carrier Sense Multiple Access / Collision Avoidance** is a network protocol for carrier transmission. Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD(that is effective after a collision) CSMA / CA is effective before a collision.

S. No.	CSMA/CD	CSMA/CA
1	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2	CSMA / CD are used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4	CSMA / CD resend the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11

		standard.
6	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).
7	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
8	It is work in MAC layer.	It is also work in MAC layer.

Collision Free Protocol

Almost all collisions can be avoided in **CSMA/CD** but they can still occur during the contention period. The collision during the contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network came into use. Here we shall discuss some protocols that resolve the collision during the contention period.

- Bit-map Protocol
- Binary Countdown
- Limited Contention Protocols
- The Adaptive Tree Walk Protocol

Pure and slotted Aloha, CSMA and CSMA/CD are **Contention based Protocols:**

- Try-if collide-Retry
- No guarantee of performance
- What happen if the network load is high?

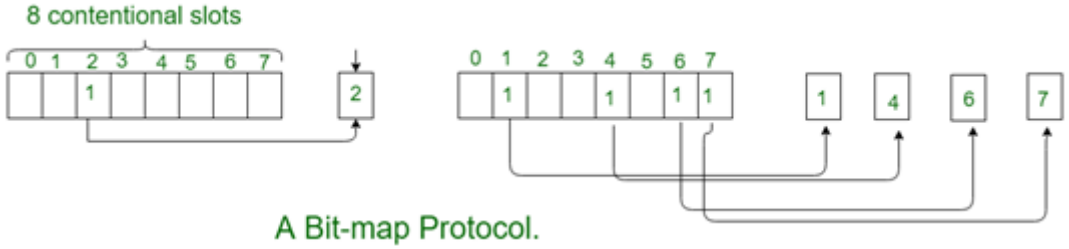
Collision Free Protocols:

- Pay constant overhead to achieve performance guarantee
- Good when network load is high

1) Bit-map Protocol:

Bit map protocol is collision free Protocol. In bitmap protocol method, each contention period consists of exactly N slots. If any station has to send frame, then it transmits a 1 bit in the corresponding slot. For example, if station 2 has a frame to send, it transmits a 1 bit to the 2nd slot.

In general, Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.



Bit Map Protocol fig (1.1)

For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of d time units. Under low load

conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

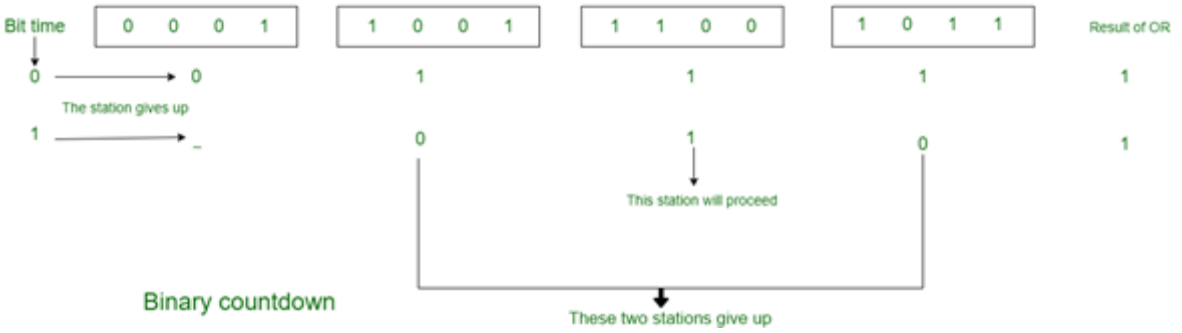
Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

2) **Binary Countdown:**

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are read together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are read together. Station 0001 see the 1 MSB in another station address and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next station at which next bit is 1 is at station 1100, so station 1011 and 1001 give up because there 2nd bit is 0. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.



Binary Countdown fig (1.2)

3) **Limited Contention Protocols:**

Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.

Collision free protocols (bitmap, binary Countdown) are good when load is high.

How about combining their advantages :

Behave like the ALOHA scheme under light load

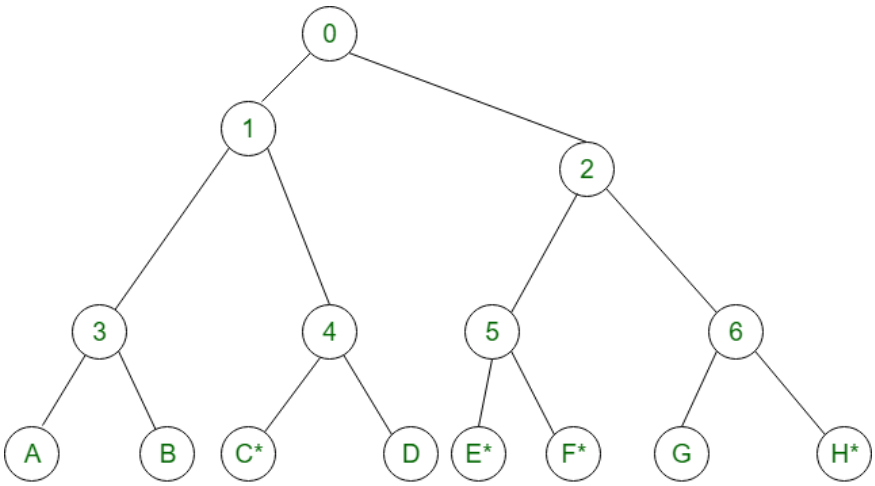
Behave like the bitmap scheme under heavy load.

4) **Adaptive Tree Walk Protocol:**

- Partition the group of station and limit the contention for each slot.
- Under light load, everyone can try for each slot like aloha
- Under heavy load, only a group can try for each slot
- How do we do it :

a) treat every stations as the leaf of a binary tree

b) first slot (after successful transmission), all stations can try to get the slot(under the root node).
c) If no conflict, fine.
d) Else, in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



Adaptive Tree Walk Protocol fig (1.3)

Slot-0 : C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
Slot-1 : C* (all nodes under node 1 can try}, C sends
Slot-2 : E*, F*, H*(all nodes under node 2 can try}, conflict
Slot-3 : E*, F* (all nodes under node 5 can try to send), conflict
Slot-4 : E* (all nodes under E can try), E sends
Slot-5 : F* (all nodes under F can try), F sends
Slot-6 : H* (all nodes under node 6 can try to send), H sends.

Collision Free Protocols

Almost all collisions can be avoided in **CSMA/CD** but they can still occur during the contention period. The collision during the contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network came into use. Here we shall discuss some protocols that resolve the collision during the contention period.

a) Bit-map Protocol
b) Binary Countdown
c) Limited Contention Protocols
d) The Adaptive Tree Walk Protocol

Pure and slotted Aloha, CSMA and CSMA/CD are **Contention based Protocols:**

- Try-if collide-Retry
- No guarantee of performance
- What happen if the network load is high?

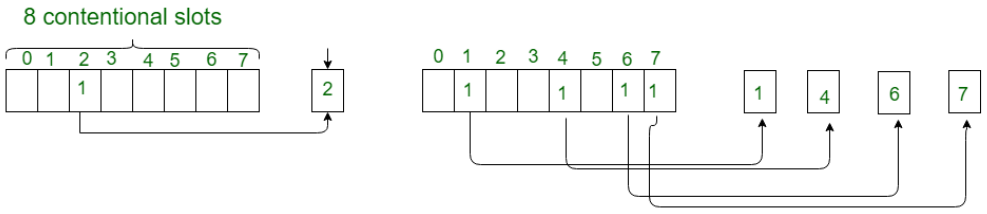
Collision Free Protocols:

- Pay constant overhead to achieve performance guarantee
- Good when network load is high

a) Bit-map Protocol

Bit map protocol is collision free Protocol. In bitmap protocol method, each contention period consists of exactly N slots. If any station has to send frame, then it transmits a 1 bit in the corresponding slot. For example, if station 2 has a frame to send, it transmits a 1 bit to the 2nd slot.

In general, Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called Reservation Protocols.



A Bit-map Protocol.

For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of d time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

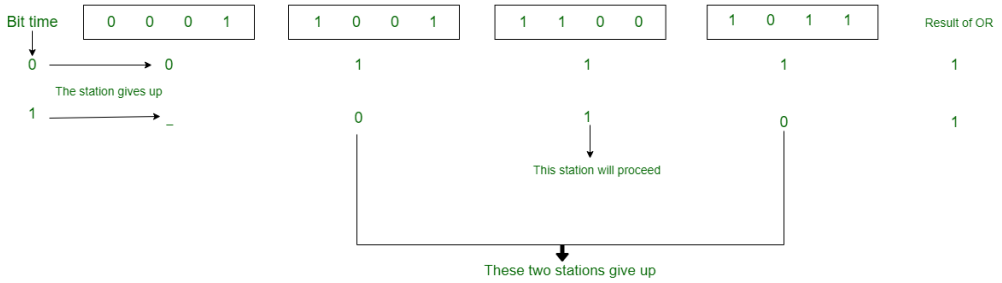
Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

b) Binary Countdown:

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are read together who decide the priority of transmitting. If these stations 0001, 1001, 1100, 1011 all are trying to seize the channel for transmission. All the station at first broadcast their most significant address bit that is 0, 1, 1, 1 respectively. The most significant bits are read together. Station 0001 see the 1 MSB in another station address and knows that a higher numbered station is competing for the channel, so it gives up for the current round.

Other three stations 1001, 1100, 1011 continue. The next station at which next bit is 1 is at station 1100, so station 1011 and 1001 give up because there 2nd bit is 0. Then station 1100 starts transmitting a frame, after which another bidding cycle starts.



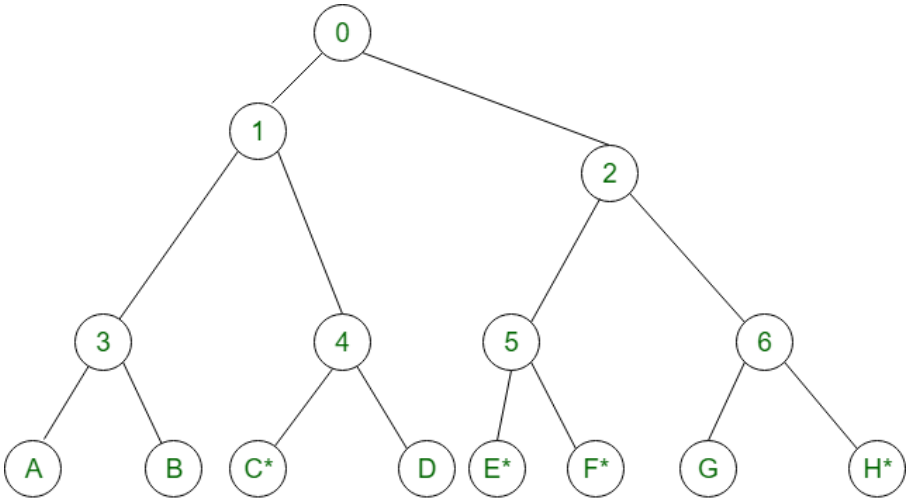
Binary countdown

c) Limited Contention Protocols:

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.
- How about combining their advantages :
  - i. Behave like the ALOHA scheme under light load
  - ii. Behave like the bitmap scheme under heavy load.

d) Adaptive Tree Walk Protocol:

i. Partition the group of station and limit the contention for each slot.
ii. Under light load, everyone can try for each slot like aloha
iii. Under heavy load, only a group can try for each slot
iv. How do we do it :
- treat every stations as the leaf of a binary tree
- First slot (after successful transmission), all stations can try to get the slot(under the root node).
- If no conflict, fine.
- Else, in case of conflict, only nodes under a subtree get to try for the next one. (depth first search)



Slot-0 : C*, E*, F*, H* (all nodes under node 0 can try which are going to send), conflict
Slot-1 : C* (all nodes under node 1 can try}, C sends
Slot-2 : E*, F*, H*(all nodes under node 2 can try}, conflict
Slot-3 : E*, F* (all nodes under node 5 can try to send), conflict
Slot-4 : E* (all nodes under E can try), E sends

Slot-5 : F* (all nodes under F can try), F sends
Slot-6 : H* (all nodes under node 6 can try to send), H sends.

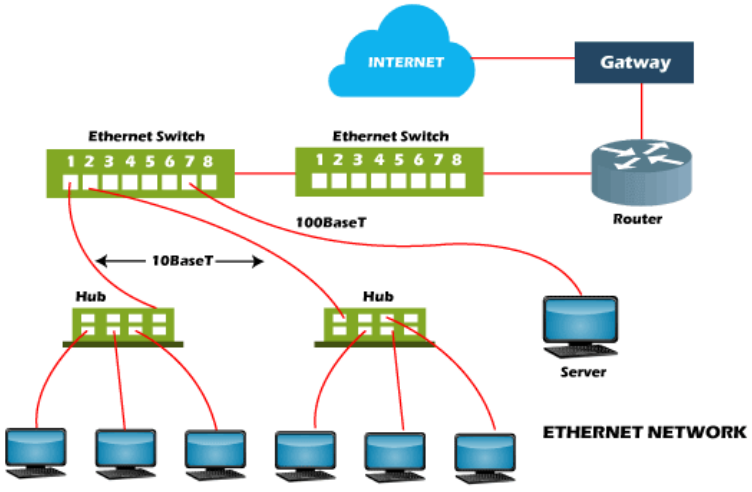
Ethernet

Ethernet is a type of communication protocol that is created at Xerox PARC in 1973 by Robert Metcalfe and others, which connects computers on a network over a wired connection. It is a widely used LAN protocol, which is also known as Alto Aloha Network. It connects computers within the local area network and wide area network. Numerous devices like printers and laptops can be connected by LAN and WAN within buildings, homes, and even small neighborhoods.

It offers a simple user interface that helps to connect various devices easily, such as switches, routers, and computers. A local area network (LAN) can be created with the help of a single router and a few Ethernet cables, which enable communication between all linked devices. This is because an Ethernet port is included in your laptop in which one end of a cable is plugged in and connect the other to a router. Ethernet ports are slightly wider, and they look similar to telephone jacks.

With lower-speed Ethernet cables and devices, most of the Ethernet devices are backward compatible. However, the speed of the connection will be as fast as the lowest common denominator. For instance, the computer will only have the potential to forward and receive data at 10 Mbps if you attach a computer with a 10BASE-T NIC to a 100BASE-T network. Also, the maximum data transfer rate will be 100 Mbps if you have a Gigabit Ethernet router and use it to connect the device.

The wireless networks replaced Ethernet in many areas; however, Ethernet is still more common for wired networking. Wi-Fi reduces the need for cabling as it allows the users to connect smartphones or laptops to a network without the required cable. While comparing with Gigabit Ethernet, the faster maximum data transfer rates are provided by the 802.11ac Wi-Fi standard. Still, as compared to a wireless network, wired connections are more secure and are less prone to interference. This is the main reason to still use Ethernet by many businesses and organizations.



Different Types of Ethernet Networks

An Ethernet device with CAT5/CAT6 copper cables is connected to a fiber optic cable through fiber optic media converters. The distance covered by the network is significantly increased by this extension for fiber optic cable. There are some kinds of Ethernet networks, which are discussed below:

a) **Fast Ethernet:** This type of Ethernet is usually supported by a twisted pair or CAT5 cable, which has the potential to transfer or receive data at around100 Mbps. They function at 100Base and 10/100Base Ethernet on the fiber side of the link if any device such as a camera, laptop, or other is connected to a network. The fiber optic cable and twisted pair cable are used by fast Ethernet to create communication. The 100BASE-TX, 100BASE-FX, and 100BASE-T4 are the three categories of Fast Ethernet.

b) **Gigabit Ethernet:** This type of Ethernet network is an upgrade from Fast Ethernet, which uses fiber optic cable and twisted pair cable to create communication. It can transfer data at a rate of 1000 Mbps or 1Gbps. In modern times, gigabit Ethernet is more common. This network type also uses CAT5e or other advanced cables, which can transfer data at a rate of 10 Gbps.

   The primary intention of developing the gigabit Ethernet was to full fill the user's requirements, such as faster transfer of data, faster communication network, and more.

c) **10-Gigabit Ethernet:** This type of network can transmit data at a rate of 10 Gigabit/second, considered a more advanced and high-speed network. It makes use of CAT6a or CAT7 twisted-pair cables and fiber optic cables as well. This network can be expended up to nearly 10,000 meters with the help of using a fiber optic cable.

d) **Switch Ethernet**: This type of network involves adding switches or hubs, which helps to improve network throughput as each workstation in this network can have its own dedicated 10 Mbps connection instead of sharing the medium. Instead of using a crossover cable, a regular network cable is used when a switch is used in a network. For the latest Ethernet, it supports 1000Mbps to 10 Gbps and 10Mbps to 100Mbps for fast Ethernet.

Advantages of Ethernet

- It is not much costly to form an Ethernet network. As compared to other systems of connecting computers, it is relatively inexpensive.
- Ethernet network provides high security for data as it uses firewalls in terms of data security.
- Also, the Gigabit network allows the users to transmit data at a speed of 1-100Gbps.
- In this network, the quality of the data transfer does maintain.
- In this network, administration and maintenance are easier.
- The latest version of gigabit ethernet and wireless ethernet have the potential to transmit data at the speed of 1-100Gbps.

Disadvantages of Ethernet

- It needs deterministic service; therefore, it is not considered the best for real-time applications.
- The wired Ethernet network restricts you in terms of distances, and it is best for using in short distances.

- If you create a wired ethernet network that needs cables, hubs, switches, routers, they increase the cost of installation.
- Data needs quick transfer in an interactive application, as well as data is very small.
- In ethernet network, any acknowledge is not sent by receiver after accepting a packet.
- If you are planning to set up a wireless Ethernet network, it can be difficult if you have no experience in the network field.
- Comparing with the wired Ethernet network, wireless network is not more secure.
- The full-duplex data communication mode is not supported by the 100Base-T4 version.
- Additionally, finding a problem is very difficult in an Ethernet network (if has), as it is not easy to determine which node or cable is causing the problem.

History of Ethernet

At the beginning of the 1970s, Ethernet was developed over several years from ALOHAnet from the University of Hawaii. Then, a test was performed, which was peaked with a scientific paper in 1976, and published by Metcalfe together with David Boggs. Late in 1977, a patent on this technology was filed by Xerox Corporation.

The Ethernet as a standard was established by companies Xerox, Intel, and Digital Equipment Corporation (DEC); first, these companies were combined to improve Ethernet in 1979, then published the first standard in 1980. Other technologies, including CSMA/CD protocol, were also developed with the help of this process, which later became known as IEEE 802.3. This process also led to creating a token bus (802.4) and token ring (802.5).

In 1983, the IEEE technology became standard, and before 802.11, 802.3 was born. Many modern PCs started to include Ethernet cards on the motherboard, as due to the invention of single-chip Ethernet controllers, the Ethernet card became very inexpensive. Consequently, the use of Ethernet networks in the workplace began by some small companies but still used with the help of telephone-based four-wire lines.

Until the early 1990s, creating the Ethernet connection through twisted pair and fiberoptic cables was not established. That led to the development of the 100 MB/s standard in 1995.

Ethernet standards

There are different standards of Ethernet, which are discussed below with additional information about each of them.

Ethernet II / DIX / 802.3

A studied edition of Ethernet, Ethernet II, also called as DIX. The DIX stands for Digital, Intel, and Xerox. And, 802.3, which is rewritten by Digital Equipment Corp, Xerox, and Intel.

Fast Ethernet / 100BASE-T / 802.3u

Fast Ethernet (100BASE-T or 802.3u) is a communications protocol, which is usually supported by a twisted pair or CAT5 cable.

The 100BASE-T standards have two types. The 100BASE-T is the first standard that makes use of CSMA/CD.

Three different kinds of cable technologies are available with 100BASE-T.

- 100BASE-T4: It is utilized for a network that requires a low-quality twisted-pair on a 100-Mbps Ethernet.
- 100BASE-TX: It makes use of two-wire data grade twisted-pair wire, developed by ANSI 100BASE-TX, which is also called 100BASE-TX and 100BASE-X.
- 100BASE-FX: It uses 2 stands of fiber cable and developed by ANSI.

Gigabit Ethernet / 1000BASE-T / 802.3z / 802.ab

Gigabit Ethernet has the potential to transmit data up to 1 Gbps, which makes use of all four copper wires in category 5, which is also called 1000BASE-T or 802.3z / 802.3ab.

10 Gigabit Ethernet / 802.3ae

10 Gigabit Ethernet (10GE or 10 GbE or 10 GigE) is a new standard that defines only full-duplex point-to-point links. It supports up to 10 Gb/s transmissions that were published in 2002, which is also known as 802.3ae. The hubs, CSMA/CD, and half-duplex operation do not exist in 10 GbE.

How to connect or plug in an Ethernet cable

The process will be the same, whether you are connecting an Ethernet cable to your computer or setting up a home network. As the below image is representing that it appears to be a large telephone cord jack. Once you have located it, then, until you hear a click, you have to push the cable connector into the port. You will see a green light that indicates a signal is found if the connection is properly established on the other end.

Why is Ethernet used?

Ethernet is still a common form of network connection, which is used for its high speed, security, and reliability. It is used to connect devices in a network that is used by specific organizations for local networks, organizations such as school campuses and hospitals, company offices, etc.

As compared to technology such as IBM's Token Ring, due to Ethernet's low price, it initially grew popular. As gradually network technology advanced, Ethernet ensured its sustained popularity as it has the potential to develop and deliver higher levels of performance with maintaining backward compatibility. In the mid-1990s, the original ten megabits per second of Ethernet increased to 100 Mbps. Furthermore, up to 400 gigabits per second can be supported by current versions of Ethernet.

How Ethernet Works

The Ethernet, in the OSI model, facilitates the operation of physical and data link layers and resides in the lower layers of the Open Systems Interconnection. There are seven layers available in the OSI model, which are as follow:

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

The application layer is the topmost layer that makes capable of users to download and access data from a mail client or a web browser. Users enter their queries with the help of the application; then, it is sent to the next layer, where the request is known as a "packet." The information about the sender and the destination web address is contained by the packet. Until the packet is reached the bottom layer, called the Ethernet frame, the packet is transmitted from the application layer. The layer closest to your device is the first or bottom layer.

Wireless LANS

WLAN stands for **Wireless Local Area Network.** WLAN is a local area network that uses radio communication to provide mobility to the network users while maintaining the connectivity to the wired network. A WLAN basically, extends a wired local area network. WLAN's are built by attaching a device called the access point(AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter which is similar in function to an ethernet adapter. It is also called a LAWN is a Local area wireless network.

The performance of WLAN is high compared to other wireless networks. The coverage of WLAN is within a campus or building or that tech park. It is used in the mobile propagation of wired networks. The standards of WLAN are HiperLAN, Wi-Fi, and IEEE 802.11. It offers service to the desktop laptop, mobile application, and all the devices that work on the Internet. WLAN is an affordable method and can be set up in 24 hours. WLAN gives users the mobility to move around within a local coverage area and still be connected to the network. Most latest brands are based on IEE 802.11 standards, which are the WI-FI brand name.

History

A professor at the University of Hawaii who's name was Norman Abramson, developed the world's first wireless computer communication network. In 1979, Gfeller and u. Bapst published a paper in the IEE proceedings reporting an experimental wireless local area network using diffused infrared communications. The first of the IEEE workshops on Wireless LAN was held in 1991.

WLAN Architecture

Components in Wireless LAN architecture as per IEEE standards are as follows:

a) **Stations:** Stations consist of all the equipment that is used to connect all wireless LANs. Each station has a wireless network controller.

b) **Base Service Set(BSS):** It is a group of stations communicating at the physical layer.
c) **Extended Service Set(ESS):** It is a group of connected Base Service Set(BSS).
d) **Distribution Service (DS):** It connects all Extended Service Set(ESS).

Types of WLANs

As per IEEE standard WLAN is categorized into two basic modes, which are as follows:

a) **Infrastructure:** In Infrastructure mode, all the endpoints are connected to a base station and communicate through that; and this can also enable internet access. A WLAN infrastructure can be set up with: a wireless router (base station) and an endpoint (computer, mobile phone, etc). An office or home WiFi connection is an example of Infrastructure mode.
b) **Ad Hoc:** In Ad Hoc mode WLAN connects devices without a base station, like a computer workstation. An Ad Hoc WLAN is easy to set up it provides peer-to-peer communication. It requires two or more endpoints with built-in radio transmission.

Working of WLAN

WLAN transmits data over radio signals and the data is sent in the form of a packet. Each packet consists of layers, labels, and instructions with unique MAC addresses assigned to endpoints. This enables routing data packets to correct locations.

Characteristics of WLAN

a) Seamless operation.
b) Low power for battery use.
c) Simple management, easy to use for everyone.
d) Protection of investment in wired networks.
e) Robust transmission technology.

Advantages of WLAN

a) Installation speed and simplicity.
b) Installation flexibility.
c) Reduced cost of ownership.
d) Reliability.
e) Mobility.
f) Robustness.

Disadvantages of WLAN

a) Slower bandwidth.
b) Security for wireless LANs is the prime concern.
c) Less capacity.
d) Wireless networks cost four times more than wired network cards.
e) Wireless devices emit low levels of RF which can be harmful to our health.

IEEE 802.11 WirelessLAN

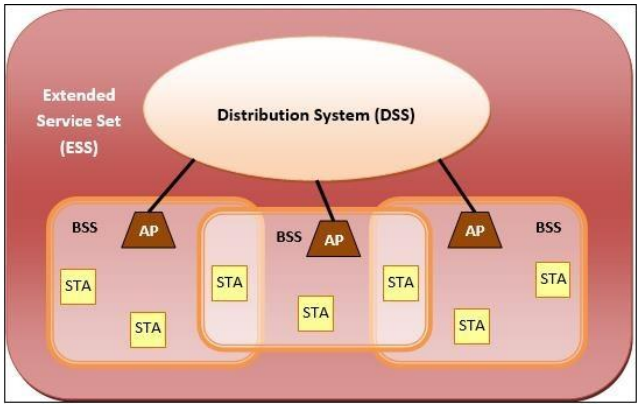
Wireless LANs are those Local Area Networks that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows

1) **Stations (STA) –** Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:
   a. **Wireless Access Pointz (WAP) –** WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
   b. **Client. –** Clients are workstations, computers, laptops, printers, smartphones, etc.

   Each station has a wireless network interface controller.
2) **Basic Service Set (BSS) –**A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:
   a. **Infrastructure BSS –** Here, the devices communicate with other devices through access points.
   b. **Independent BSS –** Here, the devices communicate in peer-to-peer basis in an ad hoc manner.
3) **Extended Service Set (ESS) –** It is a set of all connected BSS.
4) **Distribution System (DS) –** It connects access points in ESS.



- **Advantages of WLANs**
  - They provide clutter free homes, offices and other networked places.
  - The LANs are scalable in nature, i.e. devices may be added or removed from the network at a greater ease than wired LANs.
  - The system is portable within the network coverage and access to the network is not bounded by the length of the cables.
  - Installation and setup is much easier than wired counterparts.
  - The equipment and setup costs are reduced.
- **Disadvantages of WLANs**
  - Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
  - Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
  - WLANs are slower than wired LANs.

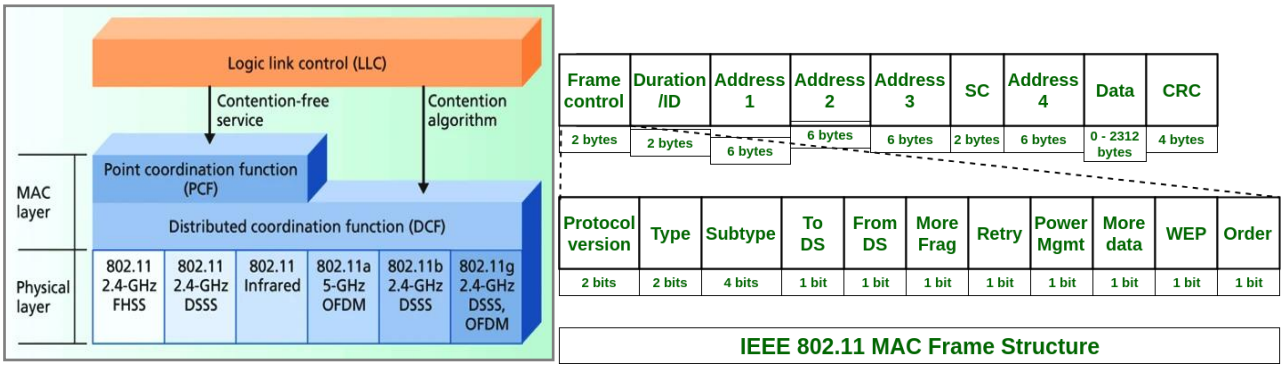
IEEE 802.11 Mac Frame

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and optional time-bounded service. IEEE 802.11 defines two MAC sub-layers:-

a) **Distributed Coordination Function (DCF) –** DCF uses CSMA/CA as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.

b) **Point Coordination Function (PCF)** – PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

MAC Frame: The MAC layer frame consists of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



- **Frame Control (FC)** – It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
  - **a) Version:** It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
  - **b) Type**: It is a 2 bit long field which determines the function of frame i.emanagement(00), control(01) or data(10). The value 11 is reserved.
  - **c) Subtype:** It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
  - **d) To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
  - **e) From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
  - **f) More frag (More fragments):** It is 1 bit long field which when set to 1 means frame is followed by other fragments.
  - **g) Retry:** It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
  - **h) Power Mgmt (Power management):** It is 1-bit long field that indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
  - **i) More data:** It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be

used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

j) **WEP**: It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

k) **Order**: It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- **Duration/ID** – It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).
- **Address 1 to 4** – These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.
- **SC (Sequence control)** – It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
- **Data –** It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
- **CRC (Cyclic redundancy check)** – It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

Features of the IEEE 802.11 MAC frame:

- **Frame Control Field**: The frame control field contains information about the type of frame, the data rate, and the power management status.
- **Duration Field**: The duration field specifies the length of time that the channel will be occupied by the transmission.
- **Address Fields:** The address fields specify the source and destination MAC addresses of the Wi-Fi devices involved in the communication.
- **Sequence Control Field:** The sequence control field is used to identify and manage the transmission sequence of the frames.
- **Frame Body:** The frame body contains the actual data being transmitted between Wi-Fi devices, such as IP packets, TCP segments, or UDP datagrams.
- **Frame Check Sequence:** The frame check sequence (FCS) is used to check the integrity of the data transmitted in the frame and to detect any transmission errors.
- **Management, Control, and Data Frames:** The IEEE 802.11 MAC frame defines three types of frames: management frames, control frames, and data frames. Management frames are used for network management, control frames are used for coordination between Wi-Fi devices, and data frames are used for the transmission of actual data.
- **Fragmentation: T**he IEEE 802.11 MAC frame supports fragmentation, which allows large data packets to be divided into smaller fragments for transmission.
- **Acknowledgments:** The IEEE 802.11 MAC frame uses acknowledgments to confirm the successful transmission of frames and to request the retransmission of any frames that were not successfully received.

Bluetooth

Bluetooth is universal for short-range wireless voice and data communication. It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific, and medical (ISM) band from 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges up to 10 meters. It provides data rates up to 1 Mbps or 3 Mbps depending upon the version. The spreading technique that it uses is FHSS (Frequency-hopping spread spectrum). A Bluetooth network is called a **piconet** and a collection of interconnected piconets is called **scatternet**.

What is Bluetooth?

Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

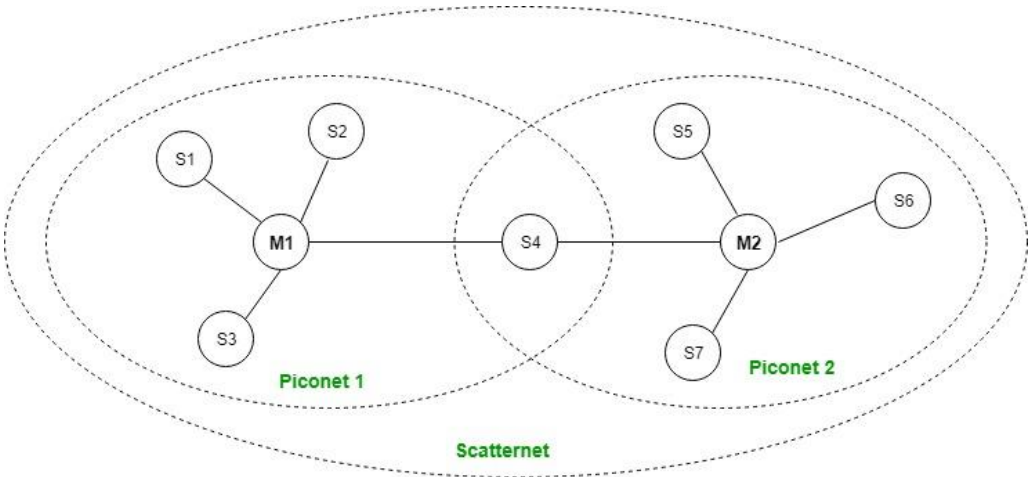
Points to remember for Bluetooth:

- Bluetooth Transmission capacity 720 kbps.
- Bluetooth is Wireless.
- Bluetooth is a Low-cost short-distance radio communications standard.
- Bluetooth is robust and flexible.
- Bluetooth is cable replacement technology that can be used to connect almost any device to any other device.
- The basic architecture unit of Bluetooth is a piconet.

Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1) Piconet
2) Scatternet

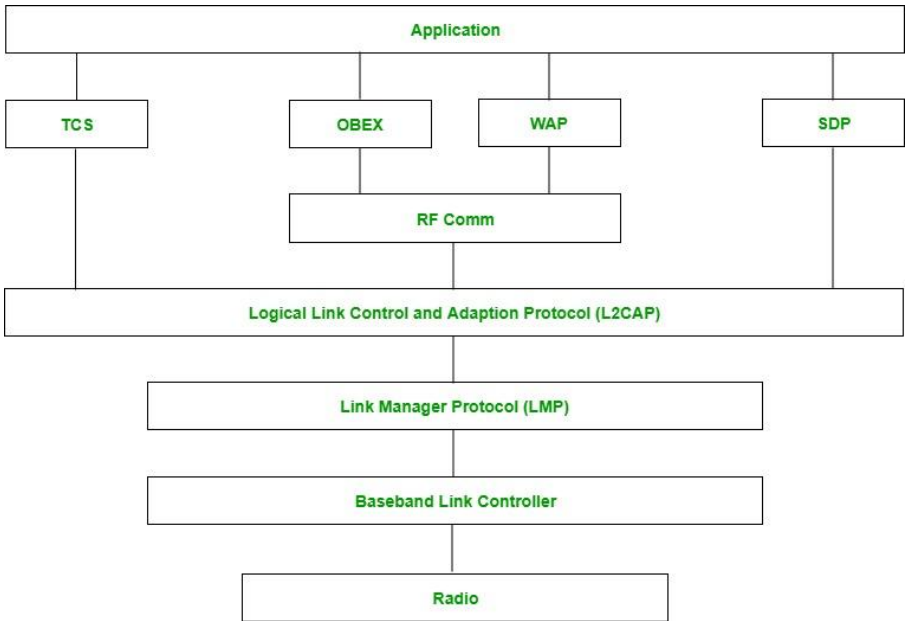


1) **Piconet:** Piconet is a type of Bluetooth network that contains **one primary node** called the master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has **255 parked nodes**, these are secondary nodes

and cannot take participation in communication unless it gets converted to the active state.

2) **Scatternet:**It is formed by using **various piconets**. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

Bluetooth protocol stack:



1) **Radio (RF) layer:** It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.
2) **Baseband Link layer:** The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sub layer in LANs. It performs the connection establishment within a piconet, addressing, packet format, timing and power control.
3) **Link Manager Protocol Layer:** It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.
4) **Logical Link Control and Adaption (L2CAP) Protocol layer:** It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.
5) **Service Discovery Protocol (SDP) layer:** It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.
6) **RF Comm Layer:** It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.

7) **OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.
8) **WAP:** It is short for Wireless Access Protocol. It is used for internet access.
9) **TCS:** It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.
10) **Application layer:** It enables the user to interact with the application.

Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

a) In-Car Headset: One can make calls from the car speaker system without the use of mobile phones.
b) Stereo Headset: To listen to music in car or in music players at home.
c) Webcam: One can link the camera with the help of Bluetooth with their laptop or phone.
d) Bluetooth-equipped Printer: The printer can be used when connected via Bluetooth with mobile phone or laptop.
e) Bluetooth Global Positioning System (GPS): To use GPS in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Advantage:

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

a) It can be used in laptops, and in wireless PCs, printers.
b) It can be used in wireless headsets, wireless PANs, and LANs.
c) It can connect a digital camera wirelessly to a mobile phone.
d) It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
e) It is used in the sectors of Medical health care, sports and fitness, Military.