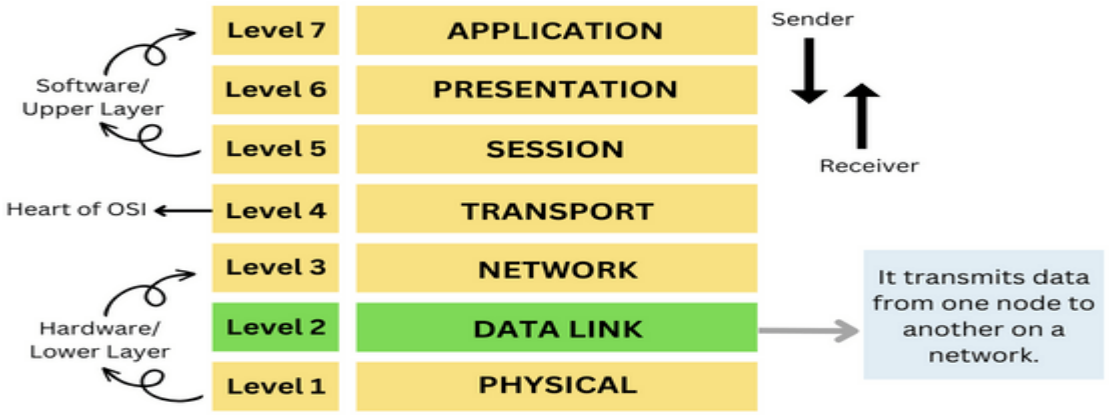
Data-link Layer

The Data Link Layer is the 2nd layer from the bottom to the top of the OSI model. Its job is to provide node-to-node delivery of data. The primary role of the data link layer is to check whether the data transmitted from one point to another node point on the physical layer is error-free or not. If any error occurs during data transmission, the data link layer will discard that data and resend the data. This layer is responsible for reliable and efficient communication between devices.

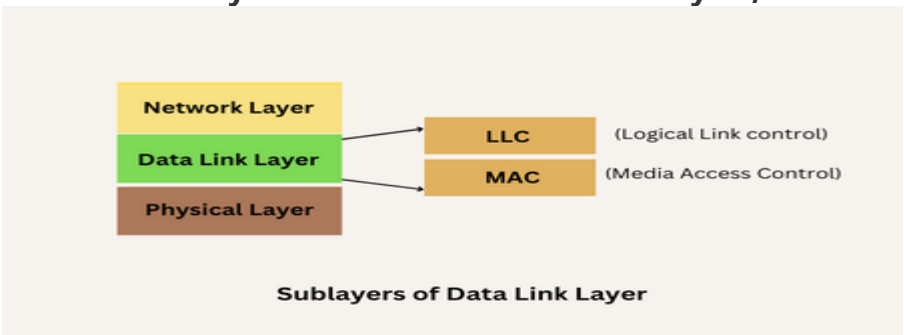


The OSI Model: Data Link Layer

The data packet travels from the network layer to the data link layer. These data packets are further divided into frames, and the frame size is chosen based on the NIC (Network Interface Card) used in the system.

This layer sets a logical layer between two points. It helps to manage the traffic control of frames on the network by stopping the transmitted signal when the frame buffer is full. For the transmission of information, the data link layer uses devices such as switches, bridges, etc.

The data link layer is classified into two sub-layers, which are given below:



Sublayers of Data Link Layer

1. ***Logical Link Control (LLC) or Data Link Control (DLC) Sublayer:*** LLC or DLC is the topmost layer of the data link layer. It deals with the communication between the lower layers and upper layers. This sublayer runs above the data link layer and provides flow control and error information. It is responsible for assigning the frame sequence number. It specifies the mechanism that can be used to address stations on a transmission medium and to control the data exchanged between the sender and the receiver.It deals with protocols, flow-control, and error control
2. ***Media Access Control (MAC) Sublayer:*** The bottom sublayer of the Data Link Layer is the Media Access Control. It is also known as Medium Access Control. It provides multiplexing and flow control for the transmission media. The main responsibility of this sublayer is to encapsulate the frame, check for transmission errors, and then allow the frame to be

forwarded to the upper layer. It determines who is permitted to access the media at any given time.It deals with actual control of media

Functions of Data link layer:

1. ***Hop to Hop or Node to Node delivery of data:*** The responsibility of the Data Link Layer (DLL) is to provide hop-to-hop delivery of data. The data link layer determines the node to which the data should be sent first, then the following node the data should be sent to, and so on, till the information arrives at the destination system.
2. ***Framing:*** It is a process of encapsulating data packets obtained from the network layer into frames for transmission. Each frame consists of a header, a payload field, and a trailer. The header contains the frame start bits, the address of both the source and destination, the type of data, and quality control bits. The payload field contains the data packet. The trailer contains error detection bits, error correction bits, and frame stop bits.
3. ***Physical addressing:*** The Data Link Layer attaches the physical addresses of the receiver and sender to the header of each frame. To send information from source to destination, you must know what we are sending and where we are sending it.
4. ***Error control:*** During transmission, the frame can get corrupted by any cause. The error can be controlled in the data link layer in three phases of error control as follows:
    - ***Error detection:*** The error in the data frame is detected with the help of error detection bits present in the frame trailer.
    - ***Acknowledgment:*** After receiving the data frame, the receiver responds to inform the sender about the successful delivery of the data frame. This acknowledgment can be positive or negative. If the data frame is received successfully, it sends positive feedback to the sender; otherwise, it sends negative feedback to the sender.
    - ***Retransmission:*** If the receiver successfully receives the data frame, the sender sends the next set of data frames, but if the data frame does not reach the receiver successfully, the sender must resend the data frames.
5. ***Flow Control:*** The receiver should be able to receive the data frame at the same speed at which the sender is sending the data frame, i.e., both the sender and the receiver should work at the same speed. If the sender sends frames with high speed and the receiver receives frames with low speed, the sender will be overloaded, resulting in loss of data.

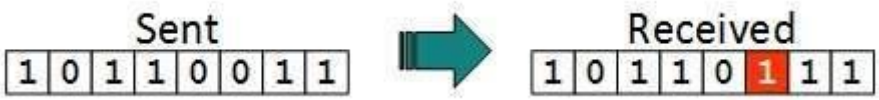
There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing.Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

There may be three types of errors:

- **Single bit error**



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

- **Multiple bits error**

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

- **Burst error**

Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

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

Parity Check

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

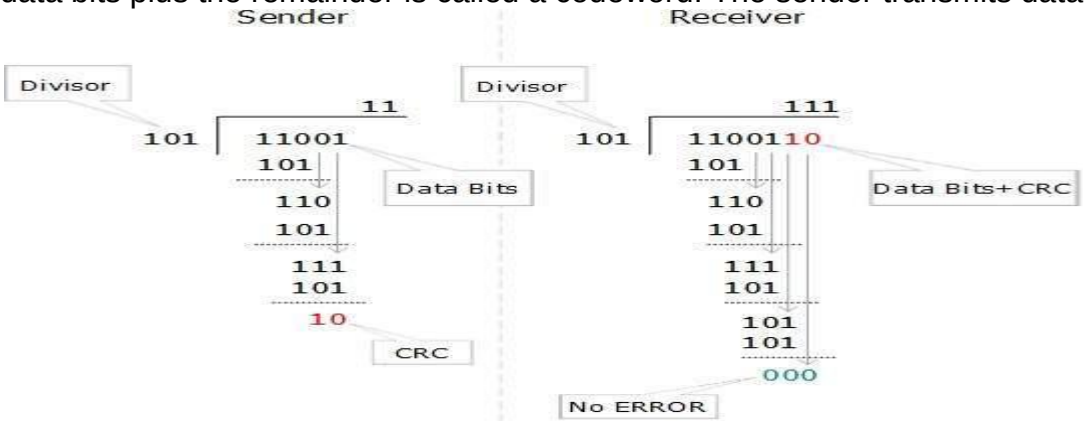
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.If the number of 1s is odd, to make it even a bit with value 1 is added.

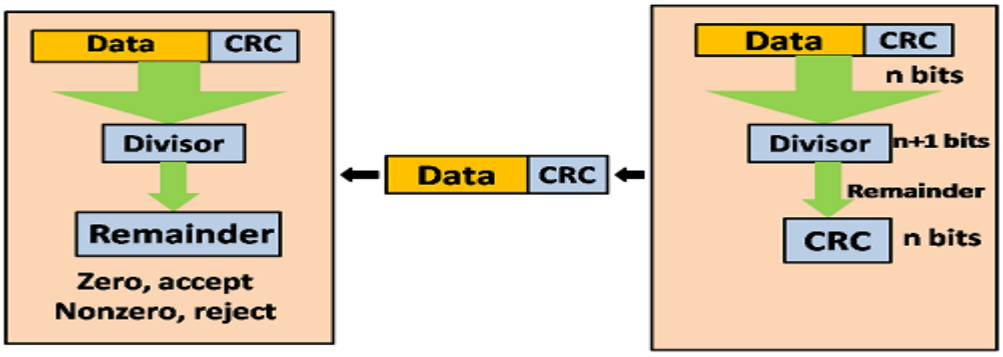
The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

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

Cyclic Redundancy Check (CRC)

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





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

Error Correction

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

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

Data-link Control & Protocols

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

Flow Control

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

- 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 types of mechanisms can be deployed to control the flow:

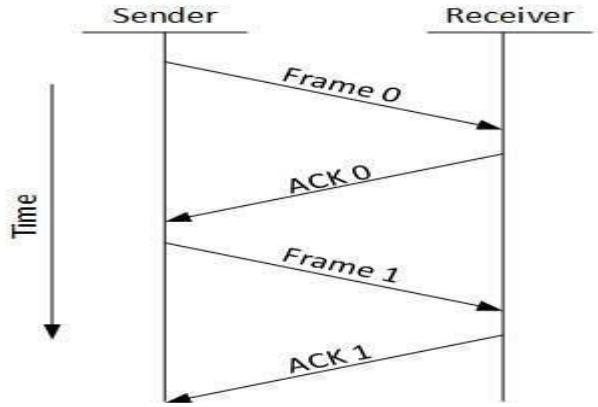
- **Stop and Wait**
  This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.
  - In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends.
  - When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame.

Advantage of Stop-and-wait

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

Disadvantage of Stop-and-wait

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



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

Error Control

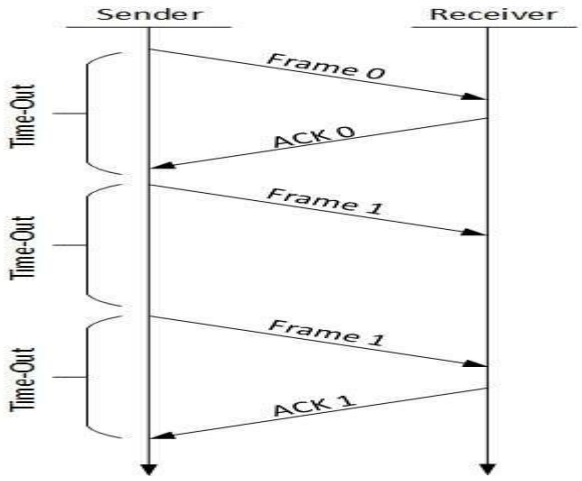
When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss.In such case, both sender and receiver are equipped with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

Requirements for error control mechanism:

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

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

- Stop-and-wait ARQ

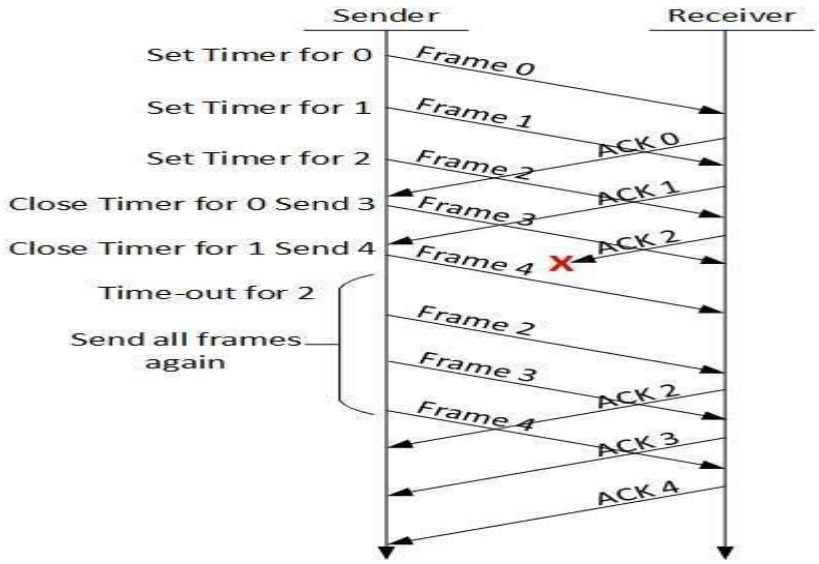


The following transition may occur in Stop-and-Wait ARQ:

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

- Go-Back-N ARQ

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

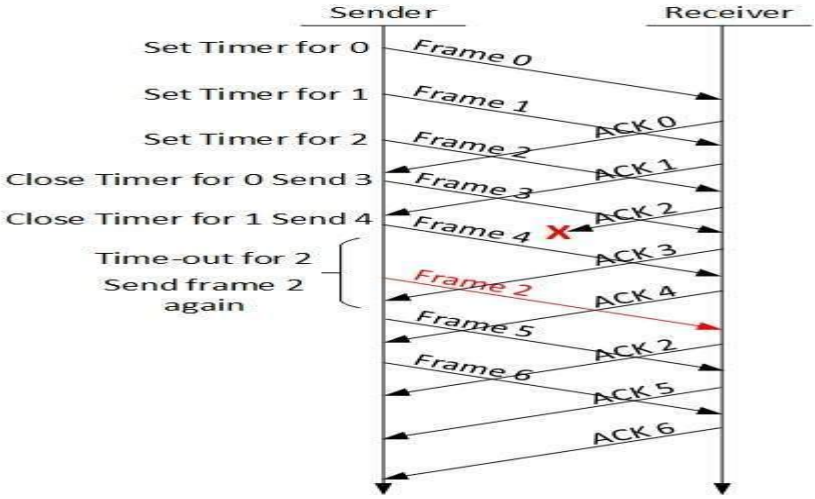


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

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

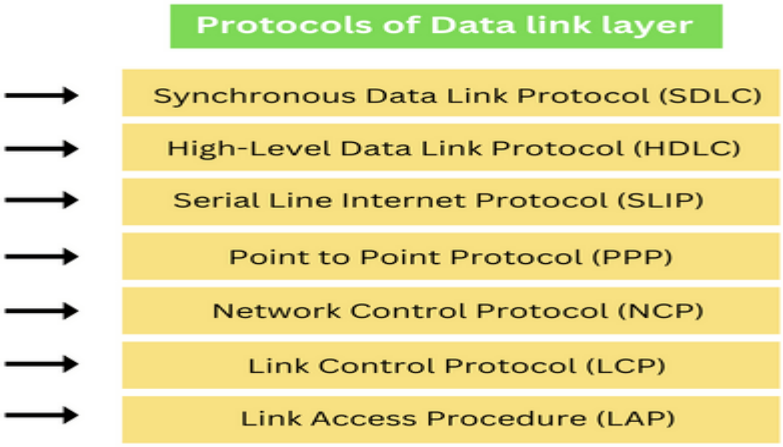
- **Selective Repeat ARQ**

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



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

Protocols of Data link layer:



- ***Synchronous Data Link Protocol (SDLC):*** It is the first bit-oriented protocol and is widely used. It is a subset of the High-Level Data Link Protocol. IBM developed this protocol in 1975. It manages synchronous serially transmitted bits over a data link layer.
- ***High-Level Data Link Protocol (HDLC):*** It is a bit-oriented protocol for conveying data on point-to-multipoint and point-to-point links. The International Organization for Standardization (ISO) developed this protocol in 1979. It is based on Synchronous Data Link Protocol. It provides connectionless and connection-oriented services. It provides two transmission modes: Asynchronous Balanced Mode (ABM) and Normal Feedback Mode (NRM).
- ***Serial Line Internet Protocol (SLIP):*** It is a simple internet protocol through which the user is allowed to access the internet with the help of a computer modem. Rick Adams developed this protocol in 1984. It works with TCP/IP for communication over the router and serial port.
- ***Point to Point Protocol (PPP):*** It is a character-oriented or byte-oriented protocol. PPP is a WAN protocol that runs over an Internet link. It is used in broadband communication. It is used to transmit multiprotocol data between point-to-point devices. It provides transmission encryption, loop connection authentication, and compression of data.

- ***Network Control Protocol (NCP):*** This layer was implemented by ARPANET. It allows transferring data between two devices. It is a part of the point-to-point protocol. This network layer will carry the data packets from the origin to the goal.
- ***Link Control Protocol (LCP):*** This layer is also a component of the point-to-point protocol. It is mainly used for establishing and maintaining the link before sending data.
- ***Link Access Procedure (LAP):*** It is derived from the high-level data link protocol. It is used for framing and data transmission over point-to-point links. It has several Link Access Protocols, such as Multilink Procedure (MLP), Link Access Procedure for Modems (LAPM), Link Access Procedure for Half-Duplex (LAPX), and Link Access Procedure for Frame Relay (LAPF).

Medium access sub layer

Point-to-Point Protocol (PPP)

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

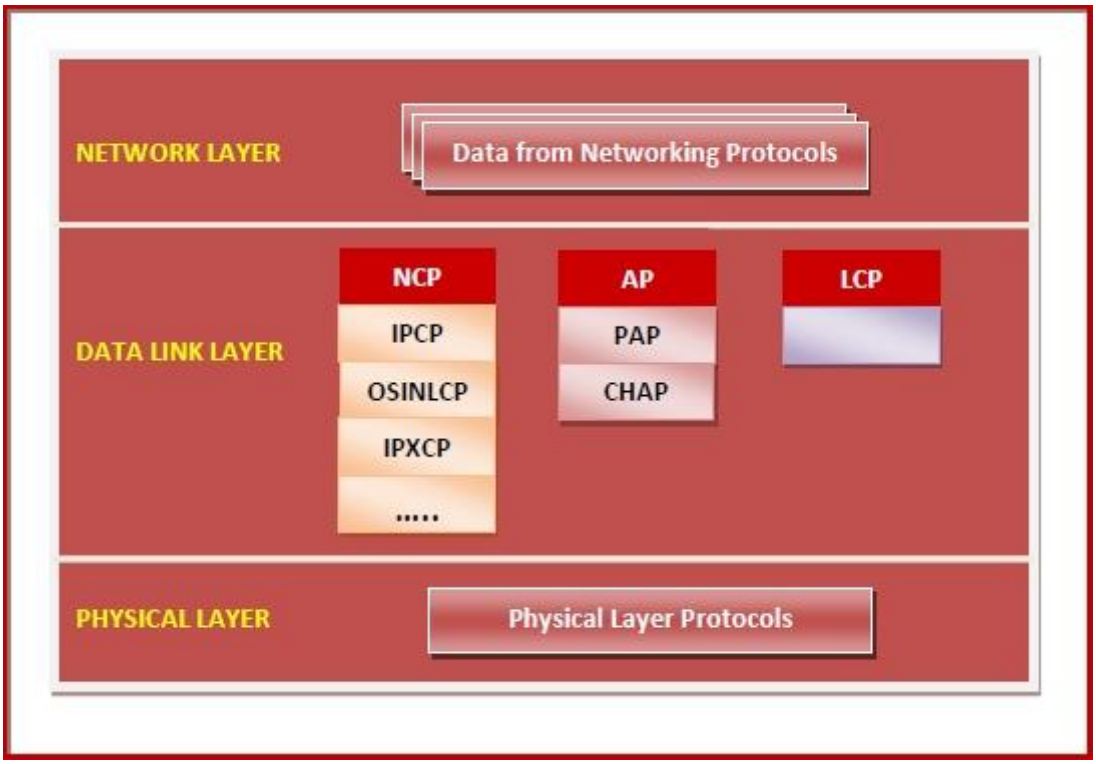
The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)
  - IPv6 Control Protocol (IPV6CP)



FDDI

FDDI stands for **Fiber Distributed Data Interface**. It is a set of ANSI and ISO guidelines for information transmission on fiber-optic lines in Local Area Network (LAN) that can expand in run upto 200 km (124 miles). The FDDI convention is based on the **token ring protocol.**
In expansion to being expansive geographically, an FDDI neighborhood region arranges can support thousands of clients. FDDI is habitually utilized on the spine for a Wide Area Network(WAN).

An FDDI network contains **two token rings,** one for possible backup in case the essential ring falls flat. The primary ring offers up to 100 Mbps capacity. In case the secondary ring isn't required for backup, it can also carry information, amplifying capacity to 200 Mbps. The single ring can amplify the most extreme remove; a double ring can expand 100 km (62 miles).

Characteristics of FDDI

- FDDI gives 100 Mbps of information throughput.
- FDDI incorporates two interfaces.
- It is utilized to associate the equipment to the ring over long distances.
- FDDI could be a LAN with Station Management.
- Allows all stations to have broken even with the sum of time to transmit information.
- FDDI defines two classes of traffic viz. synchronous and asynchronous.

Advantages of FDDI

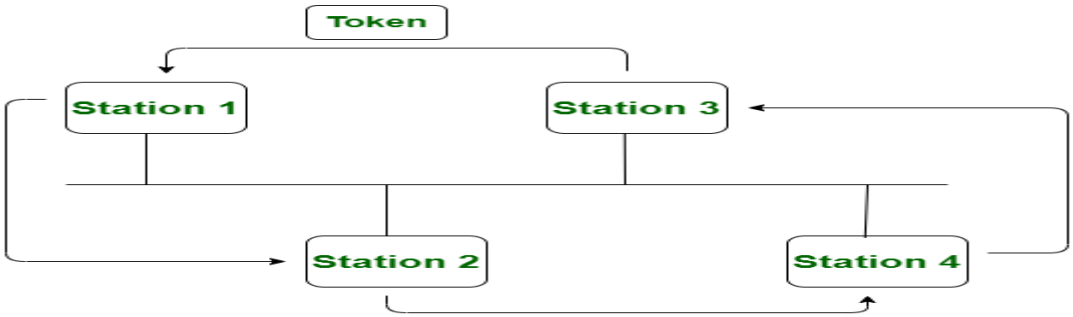
- Fiber optic cables transmit signals over more noteworthy separations of approximately 200 km.
- It is conceivable to supply the need to the work stations associated within the chain. Consequently, based on the prerequisite a few stations are bypassed to supply speedier benefit to the rest.
- FDDI employments different tokens to make strides organize speed.
- It offers a higher transmission capacity (up to 250 Gbps). Thus, it can handle information rates up to 100 Mbps.
- It offers tall security because it is troublesome to spy on the fiber-optic link.
- Fiber optic cable does not break as effectively as other sorts of cables.

Disadvantages of FDDI

- FDDI is complex. Thus establishment and support require an incredible bargain of expertise.
- FDDI is expensive. Typically since fiber optic cable, connectors and concentrators are exceptionally costly.

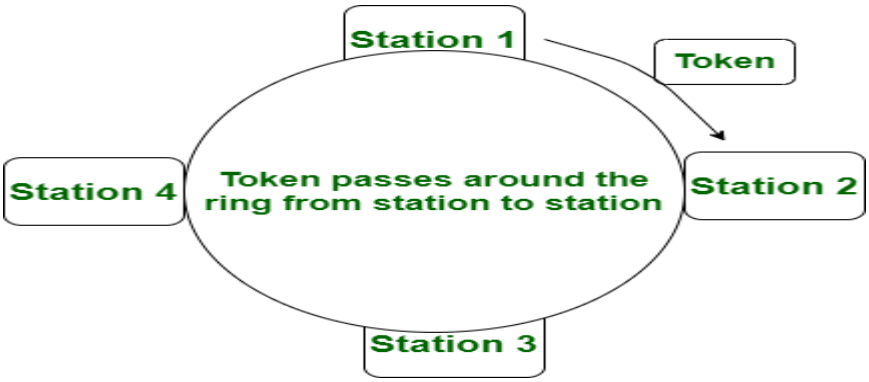
Token Bus and Token Ring Network

Token Bus network is a standard in which tokens are passed along a virtual ring. In the token bus network bus topology is used as physical media.
In this, the virtual ring is created with stations and therefore tokens are subsequently passed from a station during a sequence with this virtual ring. Every station or node in the token bus network knows the address of its predecessor station and its successor station. A node (station) can transmit the data if and only if it has a token. Its working rule is analogous to the token ring network.



Token Bus

Token Ring is defined by the IEEE 802.5 standard. In the token ring network, the token is passed over a physical ring instead of a virtual ring.
In this, a token is a special frame and a station can transmit the data frame if and only if it has a token. And The tokens are issued on successful receipt of the data frame.



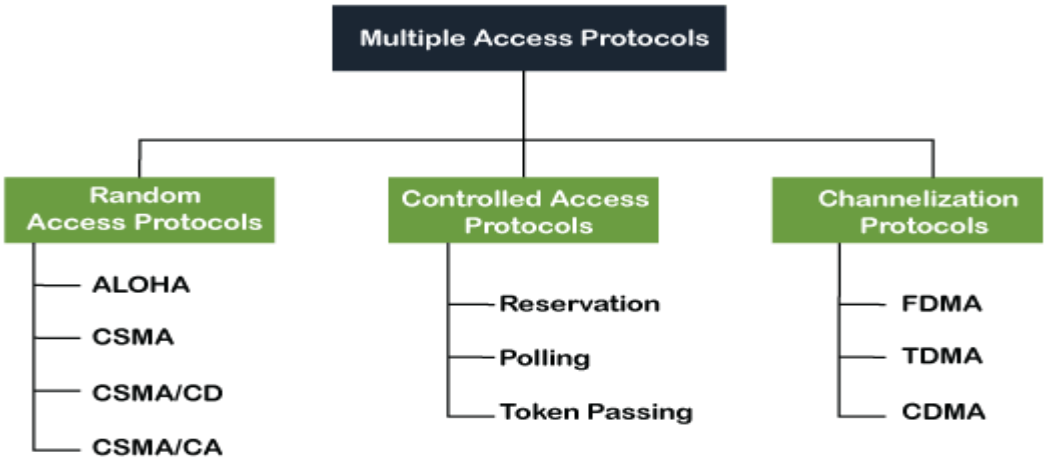
Token Ring

Difference between the Token Bus and the Token Ring:

S. No.	Token Bus Network	Token Ring Network
1.	In the token bus network, the token is passed along a virtual ring.	While in the token ring network the token is passed over a physical ring.
2.	The token bus network is simply designed for large factories.	While the token ring network is designed for the offices.
3.	The token bus network is defined by the IEEE 802.4 standard.	While the token ring network is defined by the IEEE 802.5 standard.
4.	Token bus network provides better bandwidth.	While the token ring network does not provide better bandwidth as compared to the token bus.
5.	In a token bus network, Bus topology is used.	While in token ring network, Star topology is used.
6.	The maximum time it takes to reach the last station in a token bus network cannot be calculated.	While the maximum time to reach the last station in the token ring network can be calculated.
7	In a token bus network, coaxial cable is used	In token ring network, twisted pair and fiber optic is used.

S. No.	Token Bus Network	Token Ring Network
8	In a token bus network, the cable length is 200m to 500m.	In a token ring network, the cable length is 50m to 1000m.
9.	In token bus network, distributed algorithm provide maintenance.	In a token ring network, a designated monitor station performs station maintenance.
10.	The priority handling mechanism is not associated with the transmission of data through workstations with this network.	The priority handling mechanism is associated with the transmission of data through workstations with this network.
11.	These networks are not much reliable.	These networks are reliable.
12.	It does not keep routing details.	It keeps the information of routing.
13.	The network is less expensive compared to the Token Ring network.	It is expensive.

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



Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.
- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the

channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.
CSMA access modes-

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD
(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.
CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

Controlled Access:

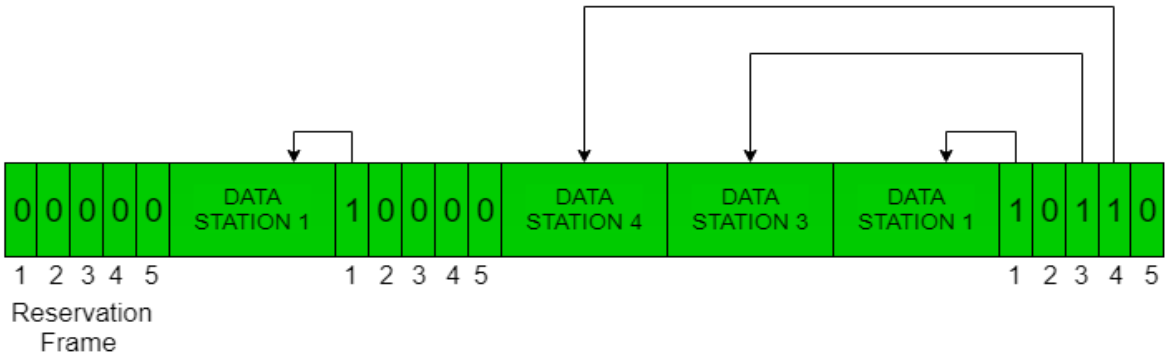
In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
  1. Reservation interval of fixed time length
  2. Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



Advantages of Reservation:

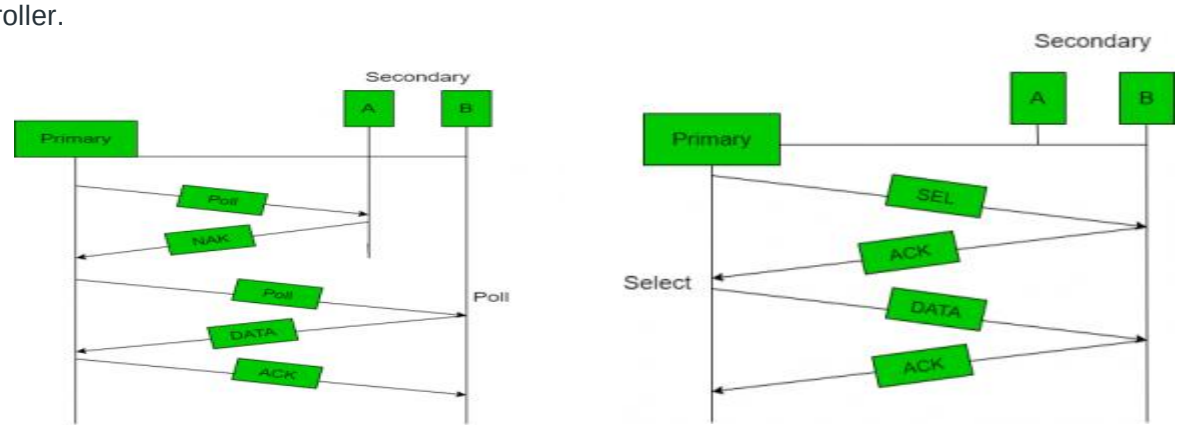
- The main advantage of reservation is *high rates and low rates of data accessing* time of the respective channel can be predicated easily. Here time and rates are fixed.
- Priorities can be set to provide speedier access from secondary.
- Predictable network performance: Reservation-based access methods can provide predictable network performance, which is important in applications where latency and jitter must be minimized, such as in real-time video or audio streaming.
- **Reduced contention:** Reservation-based access methods can reduce contention for network resources, as access to the network is pre-allocated based on reservation requests. This can improve network efficiency and reduce packet loss.
- **Quality of Service (QoS) support**: Reservation-based access methods can support QoS requirements, by providing different reservation types for different types of traffic, such as voice, video, or data. This can ensure that high-priority traffic is given preferential treatment over lower-priority traffic.
- **Efficient use of bandwidth**: Reservation-based access methods can enable more efficient use of available bandwidth, as they allow for time and frequency multiplexing of different reservation requests on the same channel.
- **Support for multimedia applications:** Reservation-based access methods are well-suited to support multimedia applications that require guaranteed network resources, such as bandwidth and latency, to ensure high-quality performance.

Disadvantages of Reservation:

- Highly trust on controlled *dependability.*
- *Decrease in capacity* and channel data rate under light loads; increase in turn-around time.

Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.



Advantages of Polling:

- The maximum and minimum access time and data rates on the channel are fixed predictable.
- It has maximum *efficiency.*
- It has maximum *bandwidth.*
- No slot is wasted in polling.

- There is assignment of priority to ensure faster access from some secondary.

Disadvantages of Polling:

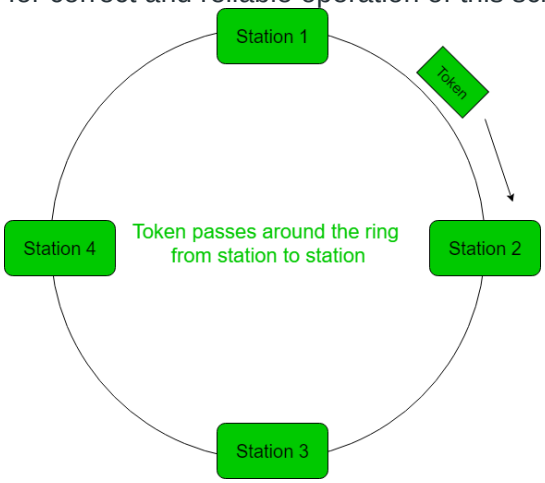
- It consume *more time.*
- Since every station has an equal chance of winning in every round, link sharing is *biased.*
- Only some station might run out of data to send.
- An increase in the turnaround time leads to a drop in the data rates of the channel under low loads.

Efficiency Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

$$Efficiency = T_t/(T_t + T_{poll})$$

Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
2. **Throughput**, which is a measure of successful traffic.

Advantages of Token passing:

- It may now be applied with routers cabling and includes built-in debugging features like *protective relay and auto reconfiguration.*
- It provides *good throughput* when conditions of high load.

Disadvantages of Token passing:

- Its cost is *expensive.*
- Topology components are more expensive than those of other, more widely used standard.
- The hardware element of the token rings are designed to be tricky. This implies that you should choose on manufacture and use them exclusively.

Channelization:

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by

addition of guard bands.

- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages:

- Increase in efficiency
- High data rates
- Good for multimedia traffic

Disadvantages:

- Complex to implement
- High peak to power ratio

- **Spatial Division Multiple Access (SDMA) –** SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages :

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages :

- It is complex to implement
- It require the accurate information about the channel