UNIT 5
DATA LINK AND PHYSICAL LAYERS
1. DATA LINK LAYER

The Data-link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible to encode, decode and organize the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

Sub-layers of Data Link Layer:

The data link layer is further divided into two sub-layers, which are as follows:

Logical Link Control (LLC):

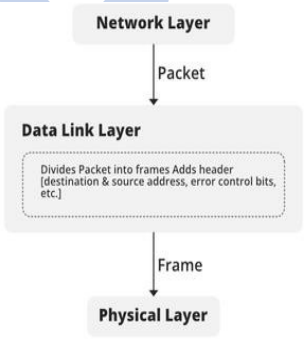
This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC):

MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access.

The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Functions of the Data-link Layer:



1. Framing: The packet received from the Network layer is known as a frame in the Data link layer. At the sender's side, DLL receives packets from the Network layer and divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end, DLL takes bits from the Physical layer organizes them into the frame, and sends them to the Network layer.

2. Addressing: The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to

ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.

3. Error Control: Data can get corrupted due to various reasons like noise, attenuation, etc. So, it is the responsibility of the data link layer, to detect the error in the transmitted data and correct it using error detection and correction techniques respectively. DLL adds error detection bits into the frame's header, so that receiver can check received data is correct ornot.

4. Flow Control: If the receiver's receiving speed is lower than the sender's sending speed, then this can lead to an overflow in the receiver's buffer and some frames may get lost. So, it's the responsibility of DLL to synchronize the sender's and receiver's speeds and establish flow control between them.

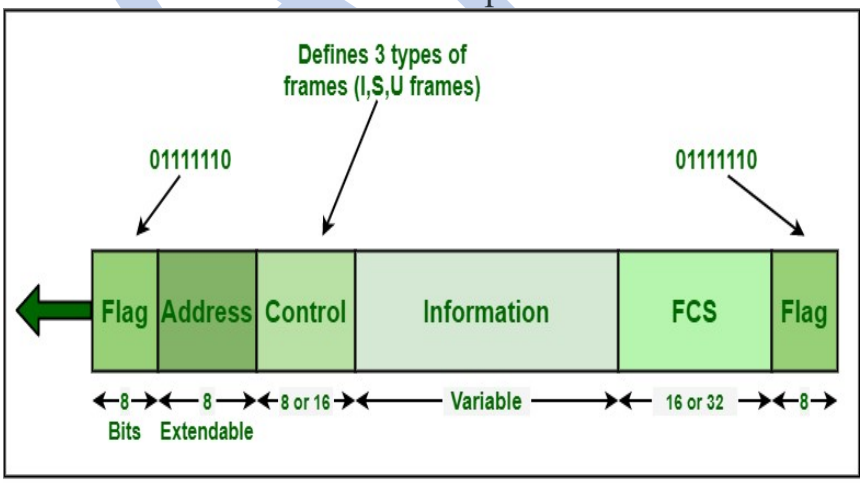
5. Access Control: When multiple devices share the same communication channel there is a high probability of collision, so it's the responsibility of DLL to check which device has control over the channel and CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.

2. DATALINK LAYER PROTOCOLS-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, and 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 :

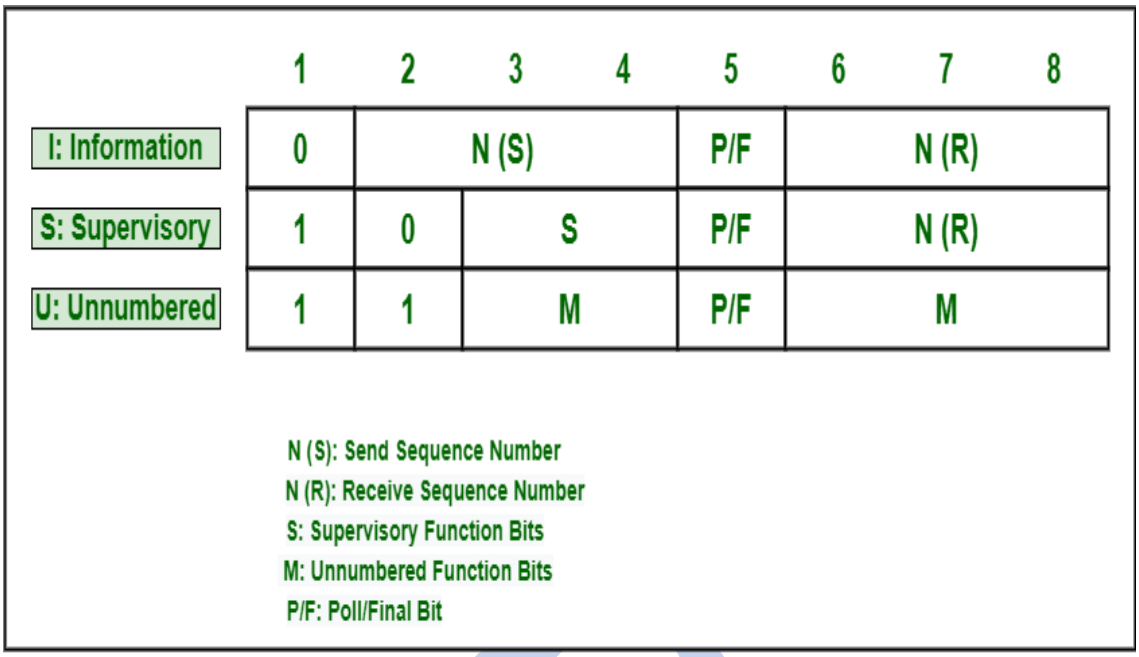
Field Name	Size (bits)
Flag Field	8 bits
Address Field	8 bits
Control Field	8 or 16 bits
Information Field	Variable (not used in some type of HDLC frames)
FCS (Frame Check Sequence) Field	16 or 32 bits
Closing Flag Field	8 bits

Let us understand these fields in details:

1. **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.

2. **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 byteslong, it depends upon requirements of network. Each byte can identify upto 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.

3. **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).

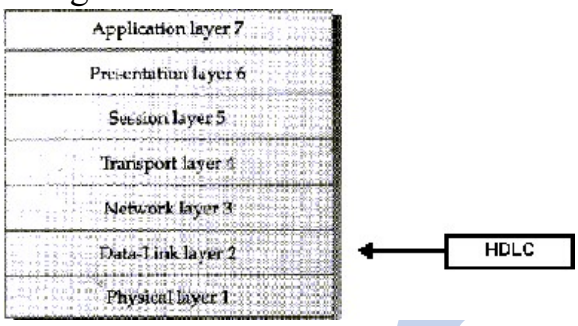


Control Field Format

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.

4. **Information Field** –This field usually contains data or information of user's 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.
5. **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.

High-Level Data Link Control, also know as HDLC, is a bit oriented, switched and non-switched protocol. It is a data link control protocol, and falls within layer 2, the Data Link Layer, of the Open Systems Interface(OSI) model as shown in figure 1.



HDLC is a protocol developed by the International Organization for Standardization(ISO). It falls under the ISO standards ISO 3309 and ISO 4335. It has found itself being used throughout the world. It has been so widely implemented because it supports both half duplex and full duplex communication lines, point to point(peer to peer) and multi-point networks, and switched or non-switched channels. The procedures outlined in HDLC are designed to permit synchronous, code-transparent data transmission. Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors. It has also led to many subsets. Two subsets widely in use are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B). This technical overview will be concerned with the following aspects of HDLC:

- Stations and Configurations
- Operational Modes
- Non-Operational Modes
- Frame Structure
- Commands and Responses
- HDLC Subsets(SDLC and LAPB)

HDLC STATIONS AND CONFIGURATIONS

HDLC specifies the following three types of stations for data link control:

- Primary Station
- Secondary Station
- Combined Station

PRIMARY STATION

Within a network using HDLC as its data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the responsibility of controlling all other stations on the link (usually secondary stations). Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the

link. It also takes care of error recovery at the data link level (layer 2 of the OSI model).

SECONDARY STATION

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station.

COMBINED STATION

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station.

HDLC also defines three types of configurations for the three types of stations:

- Unbalanced Configuration
- Balanced Configuration
- Symmetrical Configuration

UNBALANCED CONFIGURATION

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced occurs because one stations controls the other stations. In a unbalanced configurations, any of the following can be used:

- Full - Duplex or Half - Duplex operation
- Point to Point or Multi-point networks

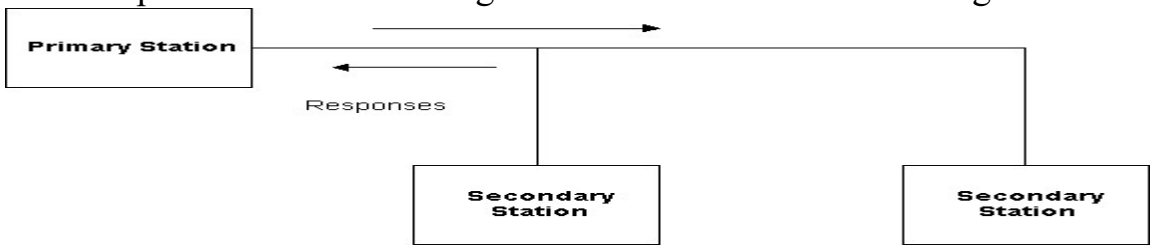
An example of an unbalanced configuration can be found below in figure 2.a

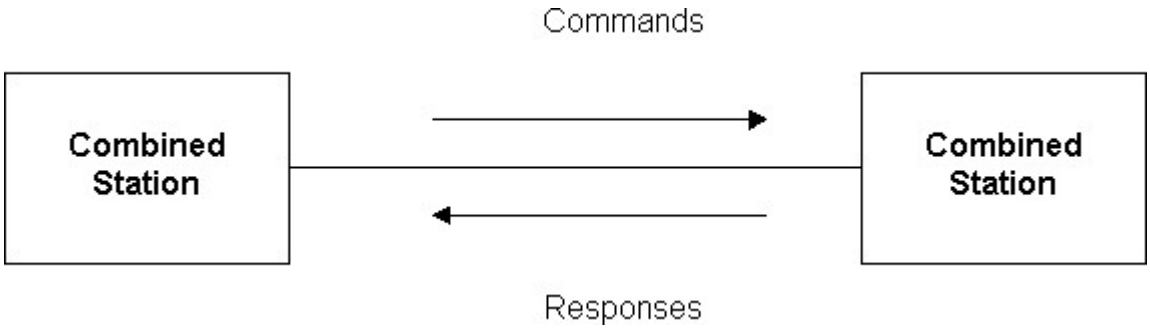
BALANCED CONFIGURATION

The balanced configuration in an HDLC link consists of two or more combined stations. Each of the stations have equal and complimentary responsibility compared to each other. Balanced configurations can used only the following:

- Full - Duplex or Half - Duplex operation
- Point to Point networks

An example of a balanced configuration can be found below in figure 2.b





SYMMETRICAL CONFIGURATION

This third type of configuration is not widely in use today. It consists of two independent point to point, unbalanced station configurations. In this configurations, each station has a primary and secondary status. Each station is logically considered as two stations.

HDLC Operational Modes

HDLC offers three different modes of operation. These three modes of operations are:

- Normal Response Mode(NRM)
- Asynchronous Response Mode(ARM)
- Asynchronous Balanced Mode(ABM)

Normal Response Mode

This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. In other words, the secondary station must receive explicit permission from the primary station to transfer a response. After receiving permission from the primary station, the secondary station initiates it's transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. It may in fact be more than one information frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.

Asynchronous Response Mode

In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However some limitations do exist. Due to the fact that this mode is Asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames. This is when the ARM link is operating at half-duplex. If the ARM link is operating

at full-duplex, the secondary station can transmit at any time. In this mode, the primary station still retains responsibility for error recovery, link setup, and link disconnection.

Asynchronous Balanced Mode

This mode uses combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.

Normal Response Mode is used most frequently in multi-point lines, where the primary station controls the link. Asynchronous Response Mode is better for point to point links, as it reduces overhead. Asynchronous Balanced Mode is not used widely today.

The "asynchronous" in both ARM and ABM does not refer to the format of the data on the link. It refers to the fact that any given station can transfer frames without explicit permission or instruction from any other station.

HDLC Non-Operational Modes

HDLC also defines three non-operational modes. These three non-operational modes are:

- Normal Disconnected Mode(NDM)
- Asynchronous Disconnected Mode(ADM)
- Initialization Mode(IM)

The two disconnected modes(NDM and ADM) differ from the operational modes in that the secondary station is logically disconnected from the link(note the secondary station is not physically disconnected from the link). The IM mode is different from the operations modes in that the secondary station's data link control program is in need of regeneration or it is in need of an exchange of parameters to be used in an operational mode.

HDLC Frame Structure

HDLC uses the term "frame" to indicate an entity of data(or a protocol dataunit) transmitted from one station to another. Figure 3 below is a graphical representation of a HDLC frame with an information field.

Figure 3 An HDLC frame with an information field.



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

THE FLAG FIELD

Every frame on the link must begin and end with a flag sequence field(F). Stations attached to the data link must continually listen for a flag sequence. The flag sequence is an octet looking like 01111110. Flags are continuously transmitted on the link between frames to keep the link active. Two other bit sequences are used in HDLC as signals for the stations on the link. These two bit sequences are:

- Seven 1's, but less than 15 signals an abort signal. The stations on the link know there is a problem on the link.
- 15 or more 1's indicate that the channel is in an idle state.

The time between the transmissions of actual frames is called the inter frame time fill. The inter frame time fill is accomplished by transmitting continuous flags between frames. The flags may be in 8 bit multiples.

HDLC is a code-transparent protocol. It does not rely on a specific code for interpretation of line control. This means that if a bit at position N in an octet has a specific meaning, regardless of the other bits in the same octet. If an octet has a bit sequence of 01111110, but is not a flag field, HLDC uses a technique called bit-stuffing to differentiate this bit sequence from a flag field. Once the transmitter detects that it is sending 5 consecutive 1's, in inserts a 0 bit to prevent a "phony" flag.

At the receiving end, the receiving station inspects the incoming frame. If it detects 5 consecutive 1's it looks at the next bit. If it is a 0, it pulls it out. If it is a 1, it looks at the 8^{th} bit. If the 8^{th} bit is a 0, it know an abort or idle signal has been sent. It then proceeds to inspect the following bits to determine appropriate action. This is the manner in which HDLC achieves code-transparency. HDLC is not concerned with any specific bit code inside the data stream. It is only concerned with keeping flags unique.

THE ADDRESS FIELD

The address field (A) identifies the primary or secondary stations involvement in the frame transmission or reception. Each station on the link has a unique address. In an unbalanced configuration, the A field in both commands and responses refers to the secondary station. In a balanced configuration, the command frame contains the destination station address and the response frame has the sending station's address.

THE CONTROL FIELD

HDLC uses the control field(C) to determine how to control the communications process. This field contains the commands, responses and sequences numbers used to maintain the data flow accountability of the link, defines the functions of the frame and initiates the logic to control the movement of traffic between sending and receiving stations. There three control field formats:

- **Information Transfer Format**

The frame is used to transmit end-user data between two devices.

- **Supervisory Format**

The control field performs control functions such as acknowledgment of frames, requests for re-transmission, and requests for temporary suspension of frames being transmitted. Its use depends on the operational mode being used.

- **Unnumbered Format**

This control field format is also used for control purposes. It is used to perform link initialization, link disconnection and other link control functions.

THE POLL/FINAL BIT (P/F)

The 5th bit position in the control field is called the poll/final bit, or p/f bit. It can only be recognized when it is set to 1. If it is set to 0, it is ignored. The poll/final bit is used to provide dialogue between the primary station and secondary station. The primary station uses P=1 to acquire a status response from the secondary station. The P bit signifies a poll. The secondary station responds to the P bit by transmitting a data or status frame to the primary station with the P/F bit set to F=1. The F bit can also be used to signal the end of a transmission from the secondary station under Normal Response Mode.

THE INFORMATION FIELD

This field is not always in a HDLC frame. It is only present when the Information Transfer Format is being used in the control field. The information field contains the actually data the sender is transmitting to the receiver.

THE FRAME CHECK SEQUENCE FIELD

This field contains a 16 bit, or 32 bit cyclic redundancy check. It is used for error detection.

3. POINT TO POINT PROTOCOL

PPP is a protocol that is generally used to provide similar functionality as SLIP. It is the best robust protocol that can transfer different types of packets also along with IP Packets. It can also be needed for dial-up and hired router-router lines. It generally supports the framing techniques to represent frames.

It can transfer diagrams across a serial connection to transfer IP traffic over the point-to-point connection as an encapsulation protocol.

It can provide the responsibility and executive of IP addresses, asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, etc. It can support an extensible Link Control Protocol(LCP) along with Network Control Protocols (NCP).

PPP Components

The point-to-point protocol includes the following components for sending diagrams over serial point-to-point connections −

Encapsulating Diagrams

PPP operates the High-Level Data Link Control (HDLC) protocol to encapsulate diagrams over the point-to-point connection. The HDLC protocol represents the boundaries around the single PPP frames and supports a 16-bit checksum.

A PPP frame inserts a protocol field to the primary HDLC frame to recognize the type of packet transported by the frame to manage packets from protocols other than IP, including Novell's IPX or Appletalk.

Implementing LCP

An extensible link control LCP can start, construct and check the data-link connections. It is executed on top of HDLC to arrange preferences about the data link.

Implementing NCP

Classification of network control protocols (NCPs) can start and construct multiple network-layer protocols such as IP and Appletalk, routed across the data link. They are set up powerfully using an equivalent NCP.

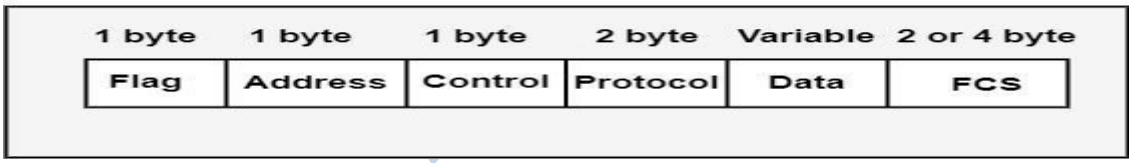
Before transmitting IP diagrams across the link, both the host running PPP must negotiate the IP address used by each of them. The control protocols used for such negotiations is called Internet Protocol Control Protocol (IPCP).

PPP Frame

The PPP frame format is shown in the figure below and includes the following –

- Flag: It includes a single byte that denotes the starting or end of a frame.
- Address: Address includes a single byte that contains the binary sequence. PPP does not allow single station addresses.
- Control: It creates an individual byte that includes the binary sequence, which calls for user information communication. It is a connectionless link function equivalent to that of Logical Link Control (LLC).
- Protocol: It includes two bytes that recognize the protocol encapsulated in the frame's information field.
- Data: Data can range from zero or more bytes, including the datagram for the protocol defined in the protocol field. The default highest duration of the information field is 1,500 bytes.
- Frame Check Sequence (FCS): It accepts 2 bytes. In this term, it can also use 4-byte FCS for upgraded error detection but with previous agreement.

PPP Frame



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 −

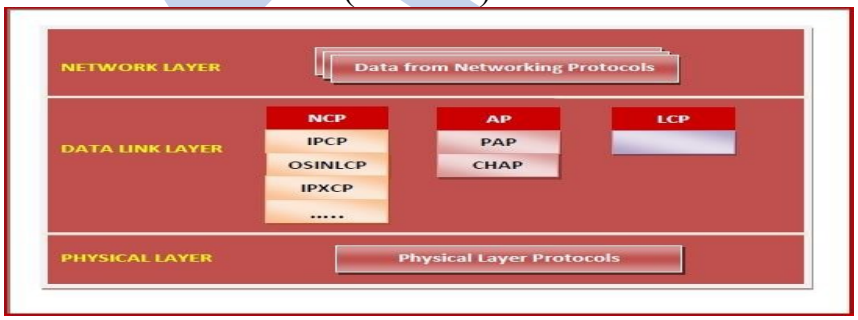
- Defining the frame format of the data to be transmitted.

- 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)

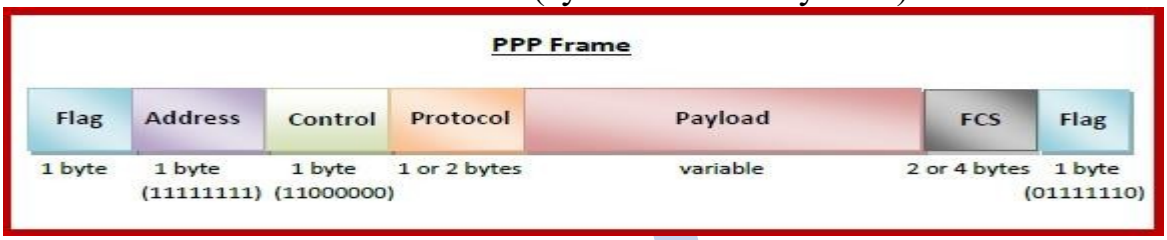


PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

- Flag − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- Address − 1 byte which is set to 11111111 in case of broadcast.

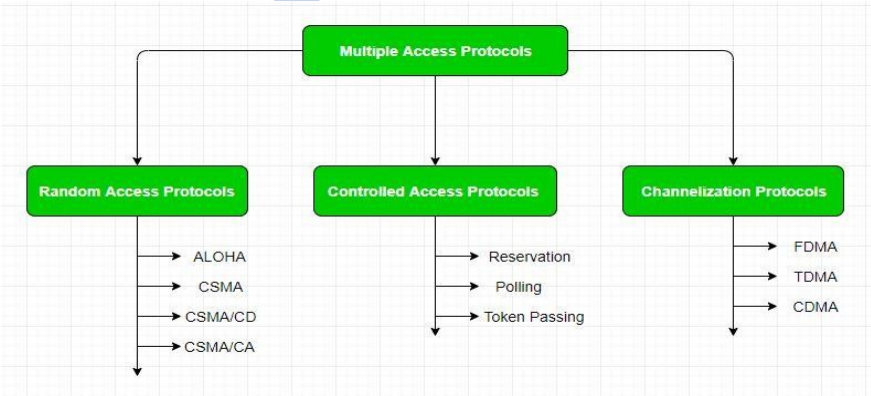
- Control − 1 byte set to a constant value of 11000000.
- Protocol − 1 or 2 bytes that define the type of data contained in the payload field.
- Payload − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- FCS − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Byte Stuffing in PPP Frame − Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

4. *MEDIA ACCESS CONTROL*

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time. Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as –



5. *RANDOM ACCESS*

whenever you call someone, a connection between you and the desired person is established, also anyone can call anyone. So here we have all the users (stations) at an equal priority, where any station can send data depending on the medium's state whether it is idle or busy, meaning that if your friend is talking to someone else through the mobile phone, then its status is busy and you cannot establish a connection and since all the users are assigned equal priority you can not disconnect your friend's ongoing call and connect yours.

The random access protocols consist of the following characteristics:

1. There is **no time restriction for sending the data** (you can talk to your friend without a time restriction).
2. There is a **fixed sequence of stations** that are transmitting the data.

As in the above diagram you might have observed that the random-access protocol is further divided into four categories, which are:

1. ALOHA
2. CSMA
3. CSMA/CD
4. CSMA/CA

Let's cover each one of them, one by one.

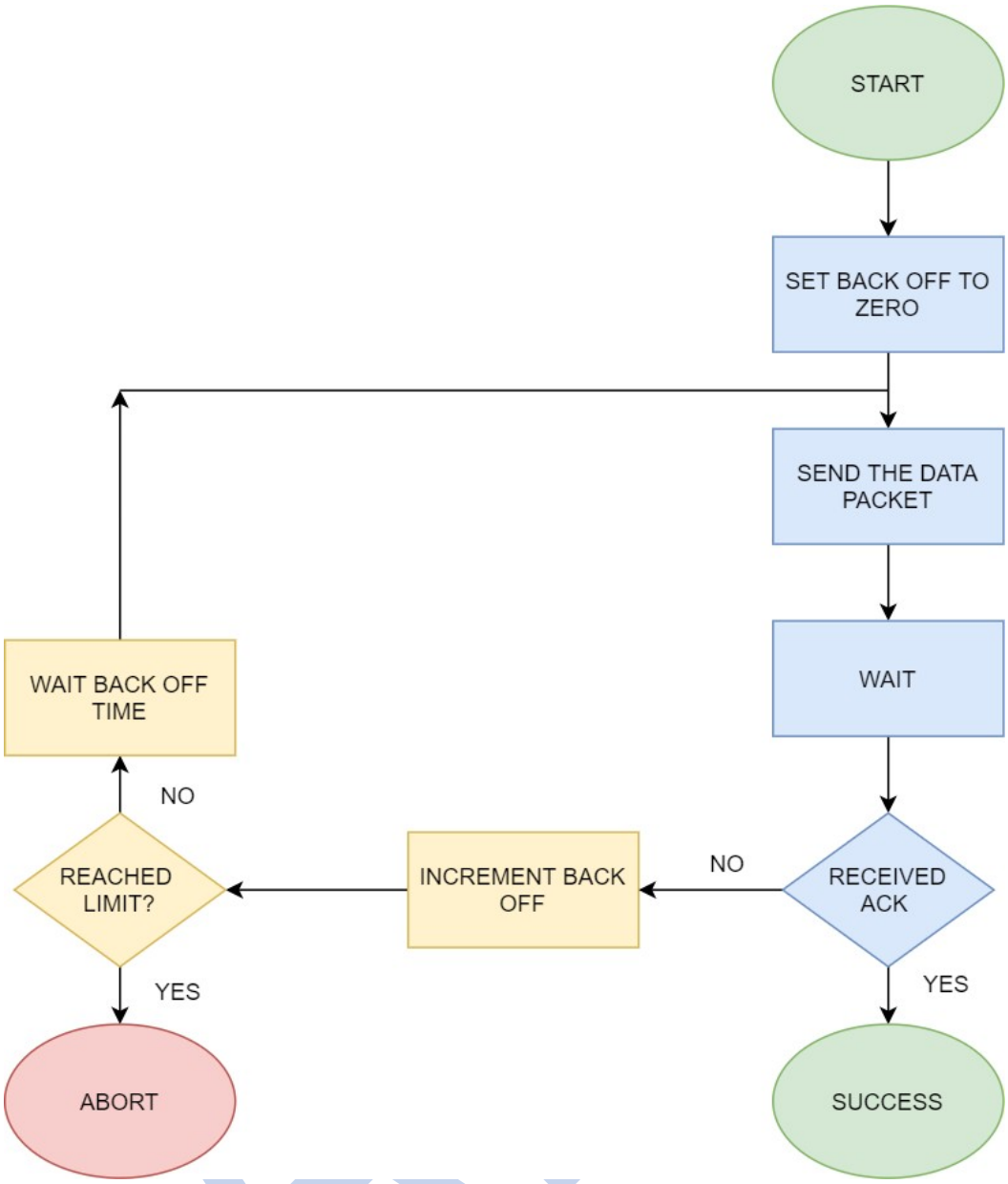
ALOHA Random Access Protocol

The ALOHA protocol or also known as the **ALOHA method** is a random access protocol in which every transmitting station or source in a network will send the data whenever a frame is available for transmission. If we succeed and the frame reaches its destination, the next frame is lined-up for transmission. But remember, if the data frame is not received by the receiver (maybe due to collision) then the frame is sent again until it successfully reaches the receiver's end.

Whenever we talk about a wireless broadcast system or a half-duplex two-way link, the ALOHA method works efficiently. But as the network becomes more and more complex e.g. the ethernet. Now here in the ethernet, the system involves multiple sources and destinations which share a common data path or channel, then the conflict occurs because data-frames collide, and the information is lost. Following is the flow chart of **Pure ALOHA**.

So, to minimize these collisions and to optimize network efficiency as well as to increase the number of subscribers that can use a given network, the **slotted ALOHA** was developed. This system consists of signals termed beacons which are sent at precise time intervals and inform each source when the channel is clear to send the frame.

Now, as we came to know about ALOHA's 2 types i.e. Pure & Slotted ALOHA, the following is the difference between these protocols.



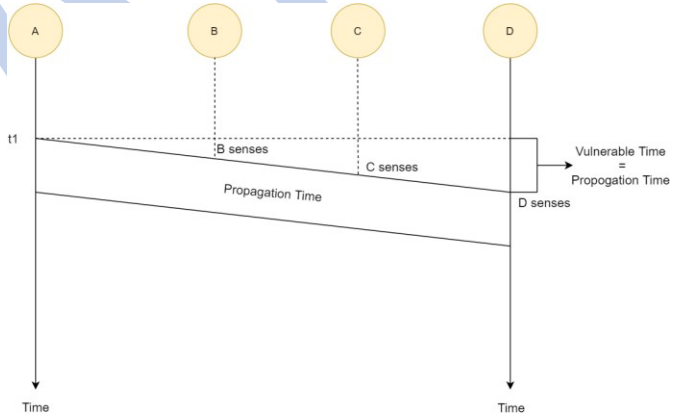
	PURE ALOHA	**SLOTTED ALOHA**
Data transmission	Stations can transmit the data randomly i.e. any number of stations can transmit data at any time.	here, any random station can transmit the data at the beginning of any random time slot
Time status	Here, the time is continuous and is not globally synchronized with any other station.	Here, the time is discrete unlike pure ALOHA, and is also globally synchronized

	PURE ALOHA	SLOTTED ALOHA
Vulnerable time	2*Frame transmission time	Frame transmission time
Probability of successful transmission of a data packet	G*e-2G where, G = no. of stations willing to transmit data	G*e-G
Maximum efficiency	18.4%	36.8%
Collision status	It does not reduce the total number of collisions to half	Here, it reduces the total number of collisions to half and doubles the efficiency of pure ALOHA

CSMA Random Access Protocol

CSMA stands for **Carrier Sense Multiple Access**. Till now we have understood that when 2 or more stations start sending data, then a collision occurs, so this CSMA method was developed to decrease the chances of collisions when 2 or more stations start sending their signals over the data link layer. But how do they do it? The CSMA makes each station to first check the medium (whether it is busy or not) before sending any data packet.

Here, **Vulnerable time = Propagation Time**



But, what to do if the channels are busy? Now, here the persistence methods can be applied to help the station act when the channel is busy or idle.

The CSMA has 4 access modes:

- **1-persistent mode**: In this, first the node checks the channel, if the channel is idle then the node or station transmits data, otherwise it keeps on waiting and whenever the channel is idle, the stations transmit the data frame.

- **Non-persistent mode**: In this, the station checks the channel similarly as the 1-persistent mode, but the only difference is that when the channel is busy it checks it again after a random amount of time, unlike the 1-persistent where the stations keep on checking continuously.
- **P-persistent mode**: In this, the station checks the channel and if found idle then it transmits the data frame with the probability of P and if the data is not transmitted (1-P) then the station waits for a random amount of time and again transmits the data with the probability P and this cycle goes on continuously until the data-frame is successfully sent.
- **O-persistent:** In this, the transmission occurs based on the superiority of stations which is decided beforehand and transmission occurs in that order. If the channel is idle, then the station waits for its turn to send the data frame.

Throughput & Efficiency of CSMA:

It is comparatively much greater than the throughput of pure and slotted ALOHA. Here, for the 1-persistent mode, the throughput is 50% when G=1; for the Non-persistent mode, the throughput can reach 90%.

CSMA/CD Random Access Protocol

CSMA/CD means **CSMA with Collision Detection**.

In this, whenever the station transmits data-frame it then monitors the channel or the medium to acknowledge the state of the transmission i.e. successfully transmitted or failed. If the transmission succeeds, then it prepares for the next frame otherwise it resends the previously failed data frame. The point to remember here is, that the frame transmission time should be at least twice the maximum propagation time, which can be deduced when the distance between the two stations involved in a collision is maximum.

CSMA/CA Random Access Protocol

CSMA/CA means **CSMA with collision avoidance**.

To detect the possible collisions, the sender receives the acknowledgment and if there is only one acknowledgment present (its own) then this means that the data frame has been sent successfully. But, if there are 2 or more acknowledgment signals then this indicates that the collision has occurred.

This method avoids collisions by:

- **Interframe space:** in this case, assume that your station waits for the channel to become idle and found that the channel is idle, then it will not send the data frame immediately (in order to avoid collision due to propagation delay) it rather waits for some time called interframe space or IFS, and after this time the station again checks the medium for being idle. But it should be kept in mind that the IFS duration depends on the priority of the station.
- **Contention Window:** here, the time is divided into slots. Say, if the sender is ready for transmission of the data, it then chooses a random number of slots as waiting time which doubles every time whenever the

channel is busy. But, if the channel is not idle at that moment, then it does not restart the entire process but restarts the timer when the channel is found idle again.

- **Acknowledgment:** as we discussed above that the sender station will re-transmit the data if acknowledgment is not received before the timer expires.

6.CONTROLLED ACCESS

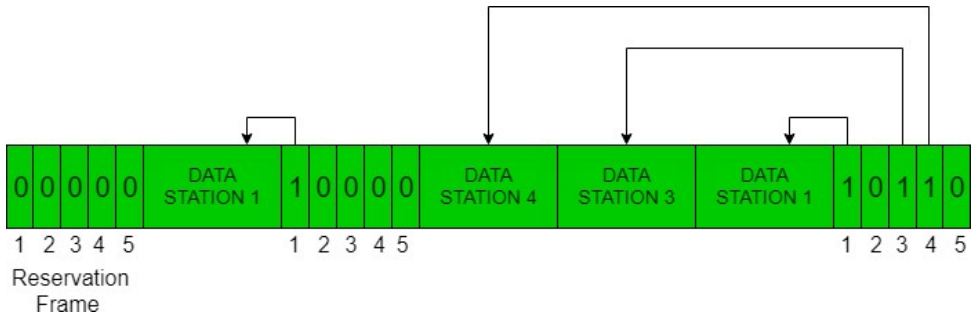
In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

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:

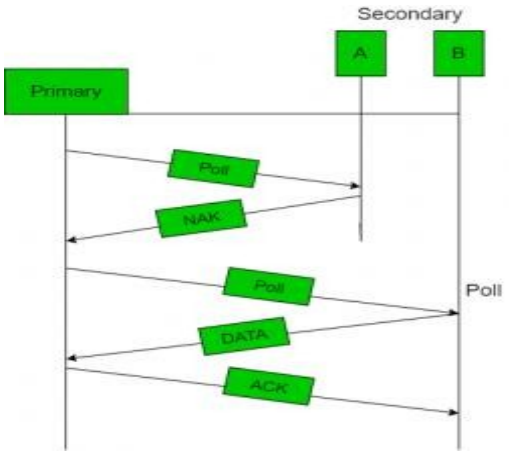
- The main advantage of reservation is *high rates and low rates of data accessing* time of the respective channel can be predicated easily. Here time and rates are fixed.
- Priorities can be set to provide speedier access from secondary.
- Predictable network performance: Reservation-based access methods 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.

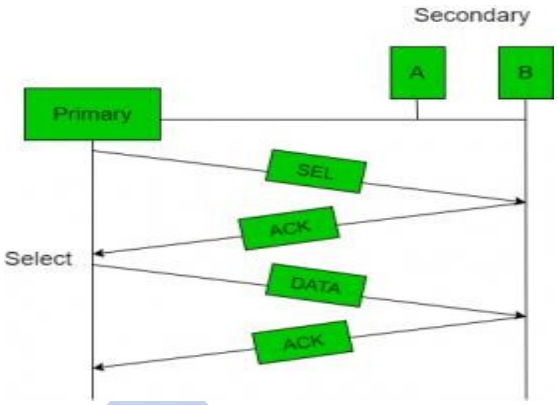
Disadvantages of Reservation:

- 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.

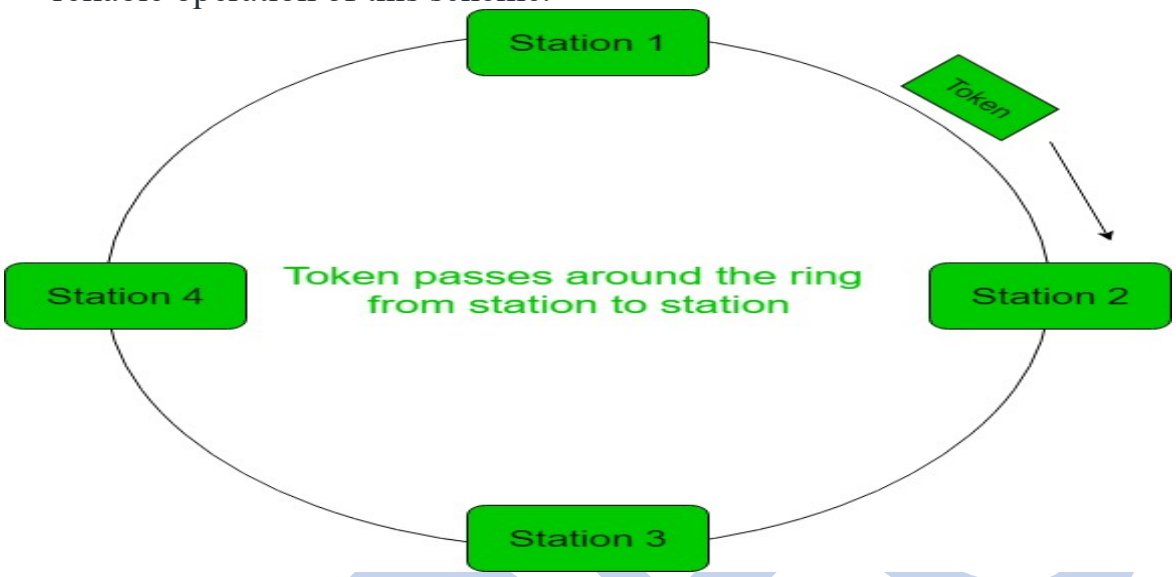
Efficiency Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

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.

Throughput, $S = 1/(1 + a/N)$ for $a<1$

and

$$S = 1/\{a(1 + 1/N)\} \text{ for } a>1.$$

where N = number of stations

$a = T_p/T_t$

(T_p = propagation delay and T_t = transmission delay)

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.

6.ETHERNET BASICS-CSMA/CD

Ethernet is a packet-switched LAN technology introduced by Xerox PARC in the early 1970s. Ethernet was designed to be a shared bus technology where multiple hosts are connected to a shared communication medium. All hosts connected to an Ethernet receive every transmission, making it possible to broadcast a packet to all hosts at the same time.

Ethernet uses a distributed access control scheme called Carrier Sense Multiple Access with Collision Detect (CSMA/CD). Multiple machines can access an Ethernet at the same time. Each machine senses whether a carrier wave is present to determine whether the network is idle before it sends a packet. Only when the network is not busy sending another message can transmission start.

In the early days of LAN technology, an Ethernet speed of 10 million bits per second (10 Mbps) (10Base-T) was quite sufficient. However, with the dramatic increase in CPU speed and advances in network technology, a 10 Mbps Ethernet became an obvious bottleneck.

Fast Ethernet uses twisted-pair wiring, was later introduced with the speed of 100 Mbps (100Base-T). Dual-speed Ethernet (10/100 Ethernet) was also introduced to accommodate both 10 and 100 Mbps connections.

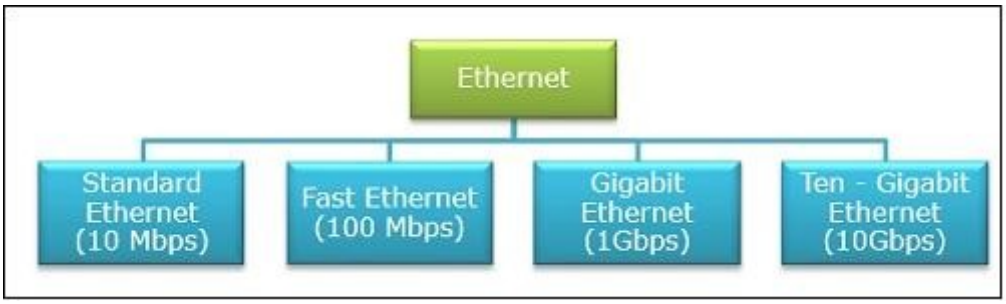
By late 1990, demand has increased for even higher speed Ethernet. Therefore Gigabit Ethernet was introduced. Gigabit Ethernet (1000Base-T) extended the Ethernet technology to a bit rate of 1 gigabit per second (1 Gbps).

Each computer connected to an Ethernet network is assigned a unique 48-bit address known as its Ethernet address. Ethernet manufacturers assign unique Ethernet addresses as they produce hardware interfaces. The Ethernet address, which is also called a media access (MAC) address, is fixed in a machine-readable form on the host interface hardware.

The address can specify the physical address of one network interface, the network broadcast address, or a multicast. In addition to its MAC address, an interface must recognize a broadcast address (all 1s) and the group addresses in the case of multicast. The Ethernet interface hardware is usually given the set of addresses to recognize by the operating system during boot time.

The host interface hardware, which receives a copy of every packet that passes by, will use the destination address to determine the packets that should be passed to the host. Other packets addressed to other hosts will be ignored.

Ethernet is a set of technologies and protocols that are used primarily in LANs. However, Ethernet can also be used in MANs and even WANs. It was first standardized in the 1980s as IEEE 802.3 standard. Since then, it has gone through four generations, as shown in the following chart

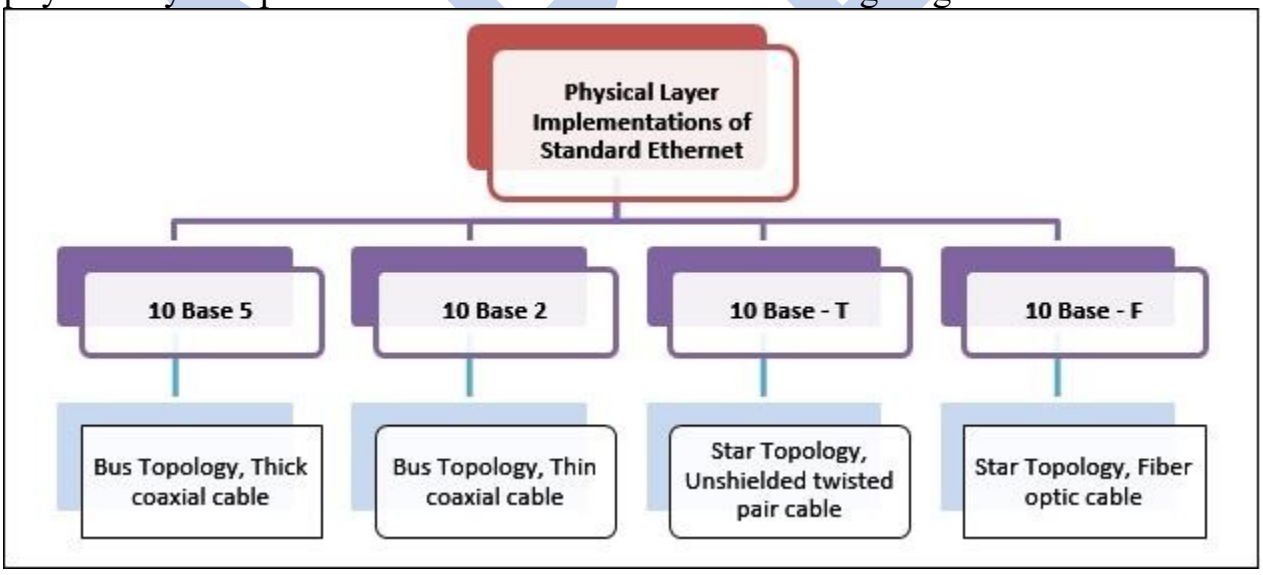


Standard Ethernet is also referred to as Basic Ethernet. It uses 10Base5 coaxial cables for communications. Ethernet provides service up to the data link layer. At the data link layer, Ethernet divides the data stream received from the upper layers and encapsulates it into frames, before passing them on to the physical layer.

The main parts of an Ethernet frame are

- **Preamble** − It is the starting field that provides alert and timing pulse for transmission.
- **Destination Address** − It is a 6-byte field containing the physical address of destination stations.
- **Source Address** − It is a 6-byte field containing the physical address of the sending station.
- **Length** − It stores the number of bytes in the data field.
- **Data and Padding** − This carries the data from the upper layers.
- **CRC** − It contains error detection information.

Standard Ethernet has many physical layer implementations. The four main physical layer implementations are shown in the following diagram



Ethernet is a set of technologies and protocols that are used primarily in LANs. The performance of Ethernet is analysed by computing the efficiency of the channel under different load conditions.

Let us assume an Ethernet network has k stations and each station transmits with a probability p during a contention slot. Let A be the probability that some station acquires the channel. A is calculated as −

$$A = kp\,(1-p)^{kp}$$

The value of A is maximized at p = 1/k. If there can be innumerable stations connected to the Ethernet network, i.e. k → ∞, the maximum value of A will be 1/e.

Let Q be the probability that the contention period has exactly j slots. Q is calculated as −

$$Q = A\,(1-A)^{j-1}$$

Let M be the mean number of slots per contention. So, the value of M will be −

$$M = \sum_{j=0}^{\infty} jA\,(1-A)^{j-1} = \frac{1}{A}$$

Given that τ is the propagation time, each slot has duration 2τ. Hence the mean contention interval, *w* will be 2τ/A.

Let P be the time is seconds for a frame to propagate.

The channel efficiency, when a number of stations want to send frame, can be calculated as −

$$Channel\ Efficiency = \frac{P}{P + 2\tau/A}$$

Let F be the length of frame, B be the cable length, L be the cable length, c be the speed of signal propagation and e be the contention slots per frame. The channel efficiency in terms of these parameters is −

$$Channel\ Efficiency = \frac{1}{1 + 2BLe/cF}$$

8.VIRTUAL LAN

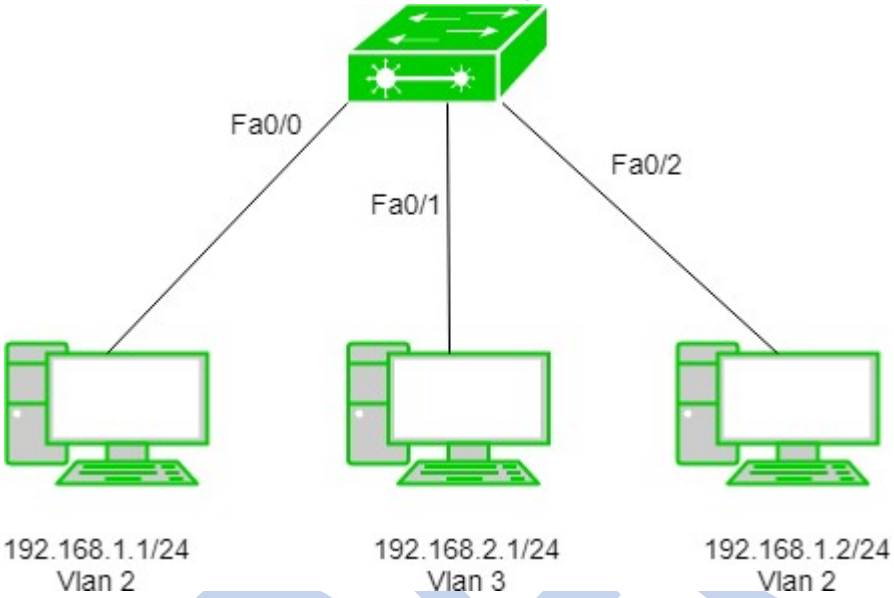
Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN.

A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter Vlan routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

VLAN ranges:

- **VLAN 0, 4095:** These are reserved VLAN which cannot be seen or used.
- **VLAN 1:** It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can't be deleted or edit but can be used.

- **VLAN 2-1001:** This is a normal VLAN range. We can create, edit and delete these VLAN.
- **VLAN 1002-1005:** These are CISCO defaults for fddi and token rings. These VLAN can't be deleted.
- **Vlan 1006-4094:** This is the extended range of Vlan.



VLANs offer several features and benefits, including:

- **Improved network security:** VLANs can be used to separate network traffic and limit access to specific network resources. This improves security by preventing unauthorized access to sensitive data and network resources.
- **Better network performance:** By segregating network traffic into smaller logical networks, VLANs can reduce the amount of broadcast traffic and improve network performance.
- **Simplified network management:** VLANs allow network administrators to group devices together logically, rather than physically, which can simplify network management tasks such as configuration, troubleshooting, and maintenance.
- **Flexibility:** VLANs can be configured dynamically, allowing network administrators to quickly and easily adjust network configurations as needed.
- **Cost savings:** VLANs can help reduce hardware costs by allowing multiple virtual networks to share a single physical network infrastructure.
- **Scalability:** VLANs can be used to segment a network into smaller, more manageable groups as the network grows in size and complexity.

Some of the key features of VLANs include:

- **VLAN tagging:** VLAN tagging is a way to identify and distinguish VLAN traffic from other network traffic. This is typically done by adding a VLAN tag to the Ethernet frame header.

- **VLAN membership:** VLAN membership determines which devices are assigned to which VLANs. Devices can be assigned to VLANs based on port, MAC address, or other criteria.
- **VLAN trunking:** VLAN trunking allows multiple VLANs to be carried over a single physical link. This is typically done using a protocol such as IEEE 802.1Q.
- **VLAN management:** VLAN management involves configuring and managing VLANs, including assigning devices to VLANs, configuring VLAN tags, and configuring VLAN trunking.

Types of connections in VLAN –

There are three ways to connect devices on a VLAN, the type of connections are based on the connected devices i.e. whether they are VLAN-aware(A device that understands VLAN formats and VLAN membership) or VLAN-unaware(A device that doesn't understand VLAN format and VLAN membership).

1. **Trunk Link –**
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access link –**
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames on the access link must be untagged.
3. **Hybrid link –**
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

Advantages –

- **Performance** –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.
- **Formation of virtual groups –** As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
- **Security –** In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
- **Flexibility –** VLAN provide flexibility to add, remove the number of host we want.

- **Cost reduction –** VLANs can be used to create broadcast domains which eliminate the need for expensive routers. By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

Disadvantages of VLAN

1. **Complexity:** VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.
2. **Limited scalability:** VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.
3. **Limited security**: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.
4. **Limited interoperability**: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.
5. **Limited mobility**: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.
6. **Cost:** Implementing and maintaining VLANs can be costly, especially if specialized hardware or software is required.
7. **Limited visibility:** VLANs can make it more difficult to monitor and troubleshoot network issues, as traffic is isolated in different segments.

Real-Time Applications of VLAN

Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:

1. **Voice over IP (VoIP)** : VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.
2. **Video Conferencing** : VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.
3. **Remote Access** : VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users from the rest of the network.
4. **Cloud Backup and Recovery** : VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.
5. **Gaming** : VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.

6. **IoT** : VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion.

9. WIRELESS LAN

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:

- **Wireless Access Pointz (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client.** − Clients are workstations, computers, laptops, printers, smartphones, etc.

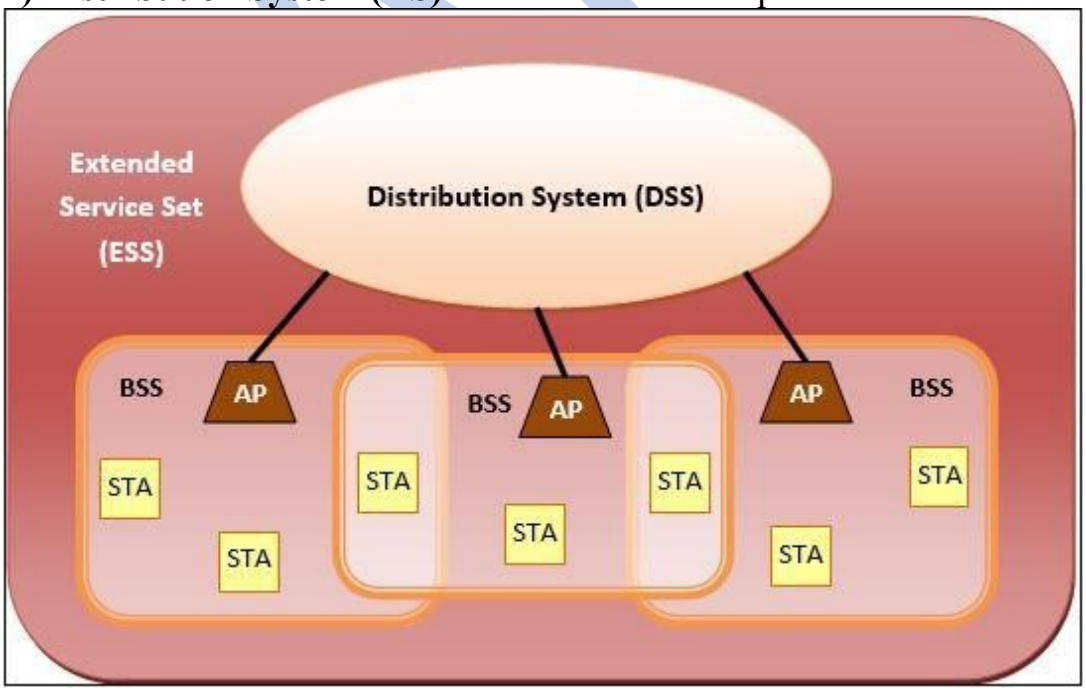
Each station has a wireless network interface controller.

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:

- **Infrastructure BSS** − Here, the devices communicate with other devices through access points.
- **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

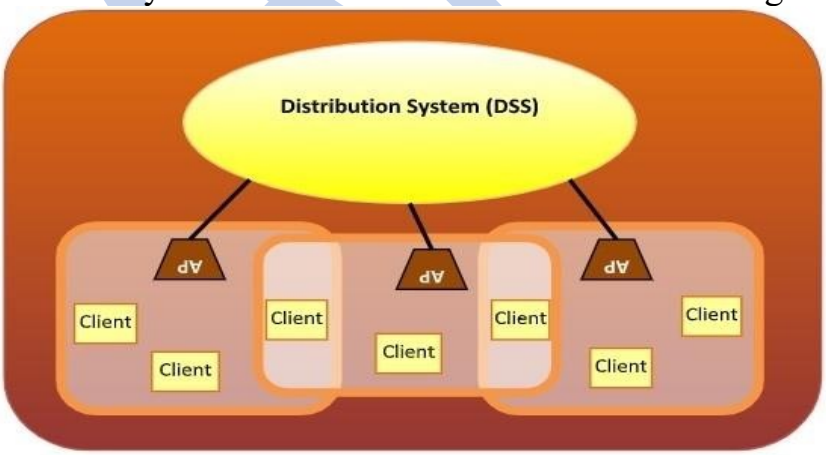
- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.
- WLANs are slower than wired LANs.

LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. 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.

Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of metres within the range of an AP.



Types of WLAN Protocols

IEEE 802.11 or Wi-Fi has a number of variations, the main among which are −

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals

have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).

- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.
- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

10. DATA AND SIGNALS

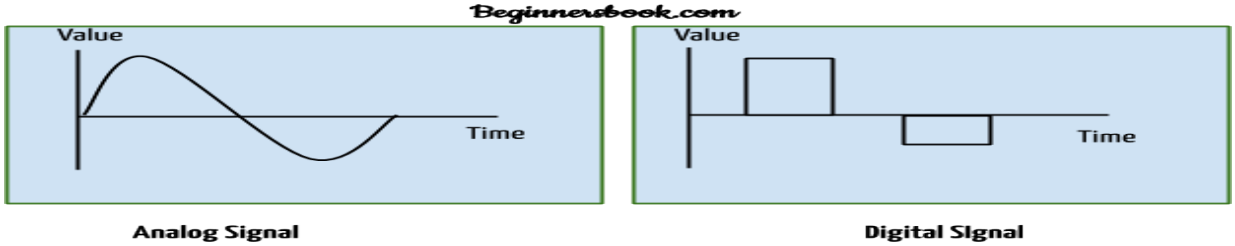
One of the major role of **Physical layer** is to transfer the **data in form of signals** through a transmission medium. It doesn't matter what data you are sending, it can be text, audio, image, video etc. everything is transferred in form of signals. This happens because a data cannot be send as it is over a transmission medium, it must be converted to a form that is acceptable by the transmission media, signals are what a transmission medium carry.

Analog and Digital

Both the data and the signal can be represented in form of Analog and digital.

Analog and Digital Data: Analog data is continuous data that keeps changing over time, for example in an analog watch, the hour, minute and second hands keep moving so you infer the time by looking at it, it keeps changing. On the other hand digital watch shows you discrete data such as 12:20 AM, 5:30 PM etc. at a particular moment of time.

Analog and Digital Signals: Similar to data, a signal can be analog or digital. An analog signal can have infinite number of values in a given range, on the other hand a digital signal has limited number of values in a given range. The following diagram shows analog and digital signals.



Analog Signal Digital Signal

1. Analog Signals

An analog signal can be be categorized as **simple** or **composite**.

Simple Analog signal

A simple analog signal can be represented in form of sine wave. A sine wave is shown in the above diagram.

A simple analog signal is smooth, consistent and continuous. As you can see in the diagram above that a arc above the time axis is followed by the similar arc below the time axis and so on. Parameters of simple Analog signal – Sine wave

There are three parameters that defines a sine wave – peak amplitude, frequency and phase.

Peak amplitude: Absolute value of highest intensity of sine wave.

Frequency and Period: Period is the amount of time a signal takes to complete one cycle, it is denoted by T. Frequency refers to the number of cycles in 1 second, it is denoted by f. They are inversely proportional to each other which means f = 1/T.

Phase: Phase refers to the position of sine wave relative to the time 0. For example if the sine wave is at its highest intensity at the time zero then the phase value for this sine wave is 90 degrees. Phase is measured in degrees or radians.

Composite Analog signal

Unlike sine wave which is smooth and consistent, composite analog signals or waves are not smooth and consistent, which means an arc above the time axis doesn't necessarily followed by arc below the time axis. You can imagine them as a group of sine waves with different frequency, amplitude and period.

Bandwidth: The range of frequencies in a composite signal is calledbandwidth. For example if a composite signal contains waves with the frequencies ranging from 2000 to 4000 then you can say that the bandwidth of this composite signal is 4000-2000 = 2000Hz. Bandwidth is measured in Hz.

2. Digital Signals

Similar to analog signals, data can be transmitted in form of digital signals. For example a data that is converted it into a machine language (combination of 0s and 1s) such as 1001 can be represented in form digital signals. 1 represents high voltage and 0 represents low voltage. **Bit Rate:** A bit rate is measured as bits per second, it represents the number of 1s send in 1 second.

Bit Length: A bit length is the distance a bit occupies on the transmission medium.

11. PERFORMANCE

The performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. Finding the performance of a network depends on both quality of the network and the quantity of the network.

Parameters for Measuring Network Performance

- Bandwidth
- Latency (Delay)
- Bandwidth – Delay Product
- Throughput
- Jitter

BANDWIDTH

One of the most essential conditions of a website's performance is the amount of bandwidth allocated to the network. Bandwidth determines how rapidly the webserver is able to upload the requested information. While there are different factors to consider with respect to a site's performance, bandwidth is every now and again the restricting element. Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices, the bandwidth is measured in bits per second(bps) or bytes per second. In the case of analog devices, the bandwidth is measured in cycles per second, or Hertz (Hz). Bandwidth is only one component of what an individual sees as the speed of a network. True internet speed is actually the amount of data you receive every second and that has a lot to do with latency too. "Bandwidth" means "Capacity" and "Speed" means "Transfer rate".

LATENCY

In a network, during the process of data communication, latency(also known as delay) is defined as the total time taken for a complete message to arrive at the destination, starting with the time when the first bit of the message is sent out from the source and ending with the time when the last bit of the message is delivered at the destination. The network connections where small delays occur are called "Low-Latency-Networks" and the network connections which suffer from long delays are known as "High-Latency-Networks".

High latency leads to the creation of bottlenecks in any network communication. It stops the data from taking full advantage of the network pipe and conclusively decreases the bandwidth of the communicating network. The effect of the latency on a network's bandwidth can be temporary or never-ending depending on the source of the delays. Latency is also known as a ping rate and is measured in milliseconds(ms).

- In simpler terms latency may be defined as the time required to successfully send a packet across a network.
- It is measured in many ways like a round trip, one-way, etc.
- It might be affected by any component in the chain utilized to vehiculate data, like workstations, WAN links, routers, LAN, and servers, and eventually may be limited for large networks, by the speed of light.

Latency = Propagation Time + Transmission Time + Queuing Time + Processing Delay

Propagation Time

It is the time required for a bit to travel from the source to the destination. Propagation time can be calculated as the ratio between the link length (distance) and the propagation speed over the communicating medium. For example, for an electric signal, propagation time is the time taken for the signal to travel through a wire.

Propagation time = Distance / Propagation speed

Example:

Input: What will be the propagation time when the distance between two points is 12, 000 km?

Assuming the propagation speed to be 2.4 * 10^8 m/s in cable.

Output: We can calculate the propagation time as-

Propagation time = (12000 * 10000) / (2.4 * 10^8) = 50 ms

Transmission Time

Transmission Time is a time based on how long it takes to send the signal down the transmission line. It consists of time costs for an EM signal to propagate from one side to the other, or costs like the training signals that are usually put on the front of a packet by the sender, which helps the receiver synchronize clocks. The transmission time of a message relies upon the size of the message and the bandwidth of the channel.

Transmission time = Message size / Bandwidth

Example:

Input: What will be the propagation time and the transmission time for a 2.5-kbyte

message when the bandwidth of the network is 1 Gbps? Assuming the distance between

sender and receiver is 12, 000 km and speed of light is 2.4 * 10^8 m/s.

Output: We can calculate the propagation and transmission time as-

Propagation time = (12000 * 10000) / (2.4 * 10^8) = 50 ms

Transmission time = (2560 * 8) / 10^9 = 0.020 ms

Queuing Time

Queuing time is a time based on how long the packet has to sit around in the router. Quite frequently the wire is busy, so we are not able to transmit a packet immediately. The queuing time is usually not a fixed factor, hence it changes with the load thrust in the network. In cases like these, the packet sits waiting, ready to go, in a queue. These delays are predominantly characterized by the measure of traffic on the system. The more the traffic, the more likely a packet is stuck in the queue, just sitting in the memory, waiting.

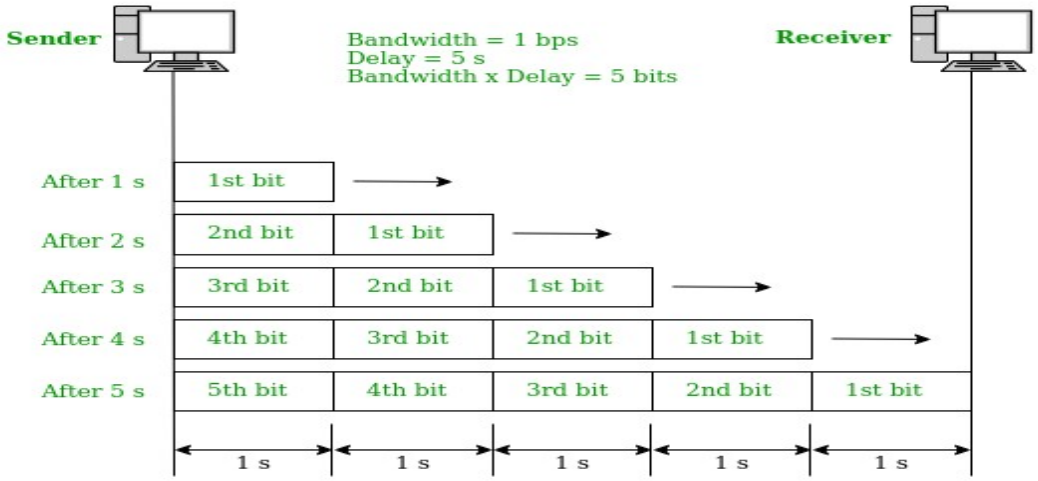
Processing Delay

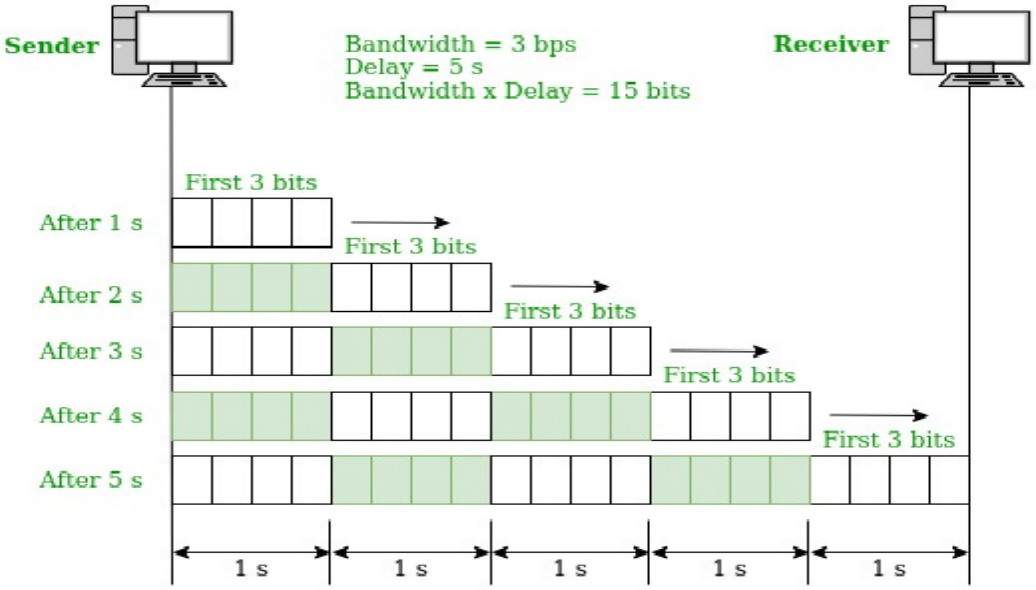
Processing delay is the delay based on how long it takes the router to figure out where to send the packet. As soon as the router finds it out, it will queue the packet for transmission. These costs are predominantly based on the

complexity of the protocol. The router must decipher enough of the packet to make sense of which queue to put the packet in. Typically the lower-level layers of the stack have simpler protocols. If a router does not know which physical port to send the packet to, it will send it to all the ports, queuing the packet in many queues immediately. Differently, at a higher level, like in IP protocols, the processing may include making an ARP request to find out the physical address of the destination before queuing the packet for transmission. This situation may also be considered as a processing delay.

BANDWIDTH – DELAY PRODUCT

Bandwidth and Delay are two performance measurements of a link. However, what is significant in data communications is the product of the two, the bandwidth-delay product. Let us take two hypothetical cases as examples.





For both examples, the product of bandwidth and delay is the number of bits that can fill the link. This estimation is significant in the event that we have to send data in bursts and wait for the acknowledgment of each burst before sending the following one. To utilize the maximum ability of the link, we have to make the size of our burst twice the product of bandwidth and delay. Also, we need to fill up the full-duplex channel. The sender ought to send a burst of data of (2*bandwidth*delay) bits. The sender at that point waits for the receiver's acknowledgement for part of the burst before sending another burst. The amount: 2*bandwidth*delay is the number of bits that can be in transition at any time.

THROUGHPUT

Throughput is the number of messages successfully transmitted per unit time. It is controlled by available bandwidth, the available signal-to-noise ratio, and hardware limitations. The maximum throughput of a network may be consequently higher than the actual throughput achieved in everyday consumption. The terms 'throughput' and 'bandwidth' are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.

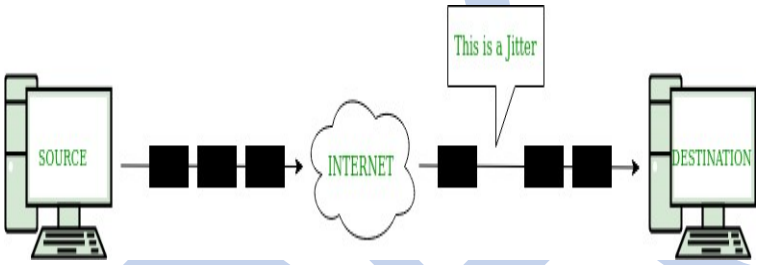
Throughput is measured by tabulating the amount of data transferred between multiple locations during a specific period of time, usually resulting in the unit of bits per second(bps), which has evolved to bytes per second(Bps), kilobytes per second(KBps), megabytes per second(MBps) and gigabytes per second(Gbps). Throughput may be affected by numerous factors, such as the hindrance of the underlying analog physical medium, the available processing power of the system components, and end-user behaviour. When numerous protocol expenses are taken into account, the use rate of the transferred data can be significantly lower than the maximum achievable throughput.

JITTER

Jitter is another performance issue related to the delay. In technical terms, jitter is a "packet delay variance". It can simply mean that jitter is considered a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds(ms). It is defined as an interference in the normal order of sending data packets. Simply, a jitter is any deviation in or displacement of, the signal pulses in a high-frequency digital signal. The deviation can be in connection with the amplitude, the width of the signal pulse, or the phase timing. The major causes of jitter are electromagnetic interference(EMI) and crosstalk between signals. Jitter can lead to the flickering of a display screen, affects the capability of a processor in a desktop or server to proceed as expected, introduce clicks or other undesired impacts in audio signals, and loss of transmitted data between network devices.

Jitter is harmful and causes network congestion and packet loss.

- Congestion is like a traffic jam on the highway. Cars cannot move forward at a reasonable speed in a traffic jam. Like a traffic jam, in congestion, all the packets come to a junction at the same time. Nothing can get loaded.
- The second negative effect is packet loss. When packets arrive at unexpected intervals, the receiving system is not able to process the information, which leads to missing information also called "packet loss". This has negative effects on video viewing. If a video becomes pixelated and is skipping, the network is experiencing a jitter. The result of the jitter is packet loss. When you are playing a game online, the effect of packet loss can be that a player begins moving around on the screen randomly. Even worse, the game goes from one scene to the next, skipping over part of the gameplay.



Factors Affecting Network Performance

Below mentioned are the factors that affect the network performance.

- Network Infrastrucutre
- Applications used in the Network
- Network Issues
- Network Security

Network Infrastructure

Network Infrastructure is one of the factors that affect network performance. Network Infrastructure consists of routers, switches services of a network like IP Addressing, wireless protocols, etc., and these factors directly affect the performance of the network.

Applications Used in the Network

Applications that are used in the Network can also have an impact on the performance of the network as some applications that have poor performance can take large bandwidth, for more complicated applications, its maintenance is also important and therefore it impacts the performance of the network.

Network Issues

Network Issue is a factor in Network Performance as the flaws or loopholes in these issues can lead to many systemic issues. Hardware issues can also impact the performance of the network.

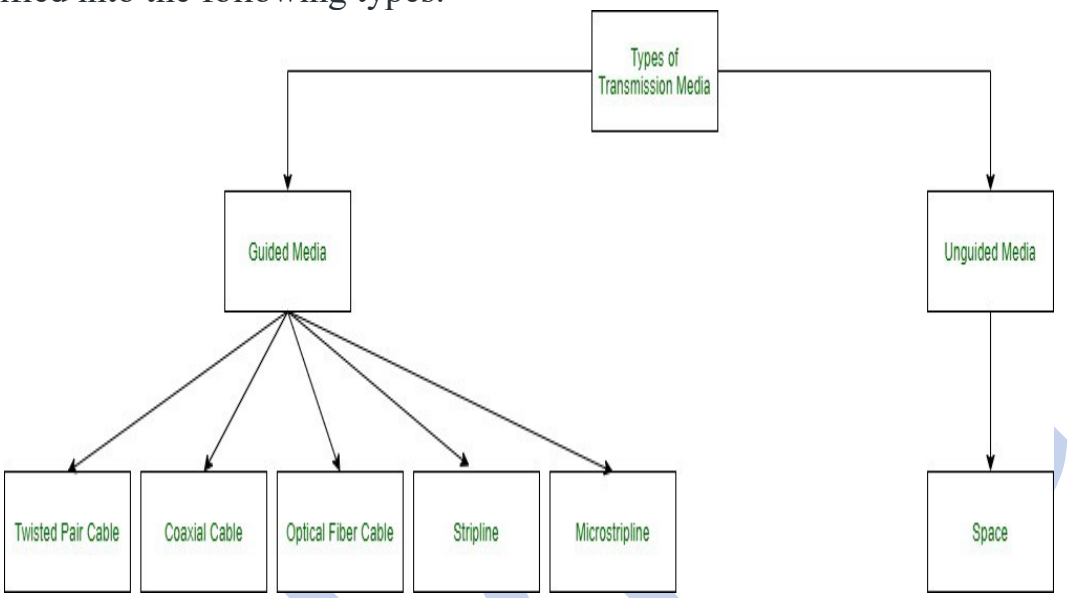
Network Security

Network Security provides privacy, data integrity, etc. Performance can be influenced by taking network bandwidth which has the work of managing the

scanning of devices, encryption of data, etc. But these cases negatively influence the network.

12. TRANSMISSION MEDIA

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. **Guided Media:** It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

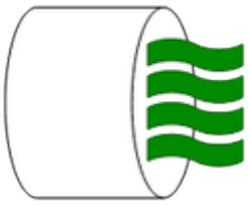
Features:

- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

(i) Twisted Pair Cable – It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):** UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

Advantages:

⇢ Least expensive
⇢ Easy to install
⇢ High-speed capacity

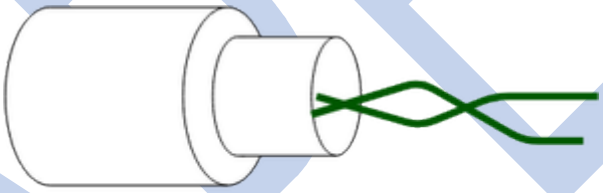
Disadvantages:

⇢ Susceptible to external interference
⇢ Lower capacity and performance in comparison to STP
⇢ Short distance transmission due to attenuation

Applications:

Used in telephone connections and LAN networks

- **Shielded Twisted Pair (STP):** This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

Advantages:

⇢ Better performance at a higher data rate in comparison to UTP
⇢ Eliminates crosstalk
⇢ Comparatively faster

Disadvantages:

⇢ Comparatively difficult to install and manufacture
⇢ more expensive
⇢ Bulky

Applications:

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

(ii) Coaxial Cable –It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband

mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

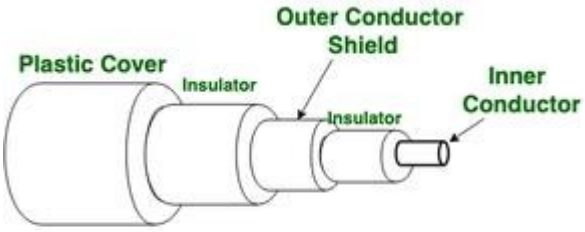


Figure of Coaxial Cable

Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Applications:

Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

(iii) Optical Fiber Cable – It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

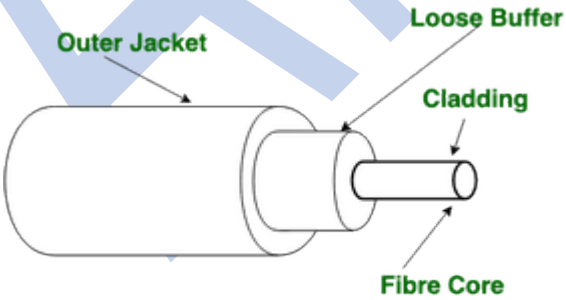


Figure of Optical Fibre Cable

Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference

- Resistance to corrosive materials

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Applications:

- Medical Purpose: Used in several types of medical instruments.
- Defence Purpose: Used in transmission of data in aerospace.
- For Communication: This is largely used in formation of internet cables.
- Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

(iv) Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline

In this, the conducting material is separated from the ground plane by a layer of dielectric.

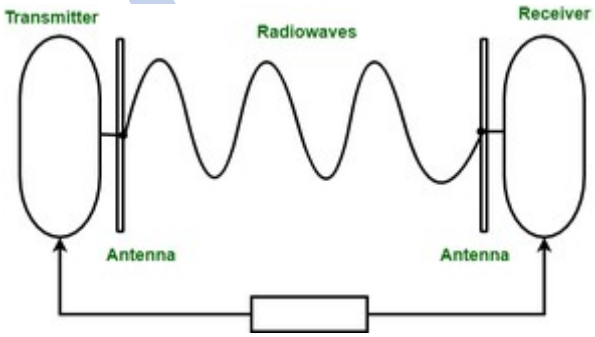
2. **Unguided Media:** It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

Features:

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) Microwaves – It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

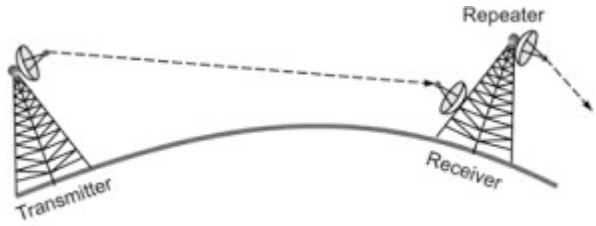


Fig: Microwave Transmission

(iii) Infrared – Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

13. GUIDED MEDIA

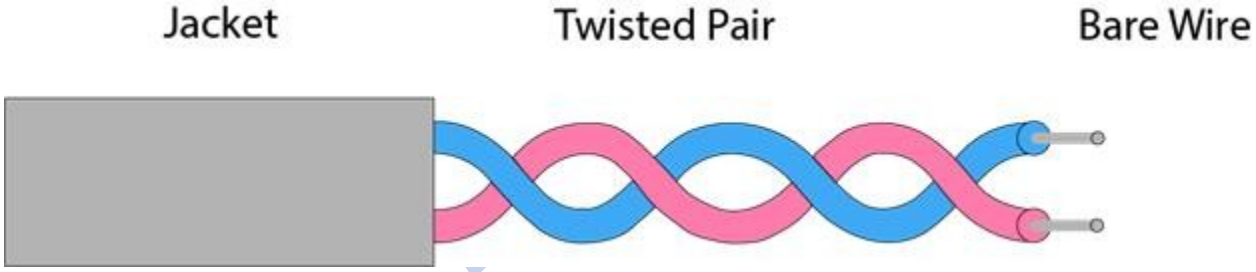
It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

Types Of Guided media:

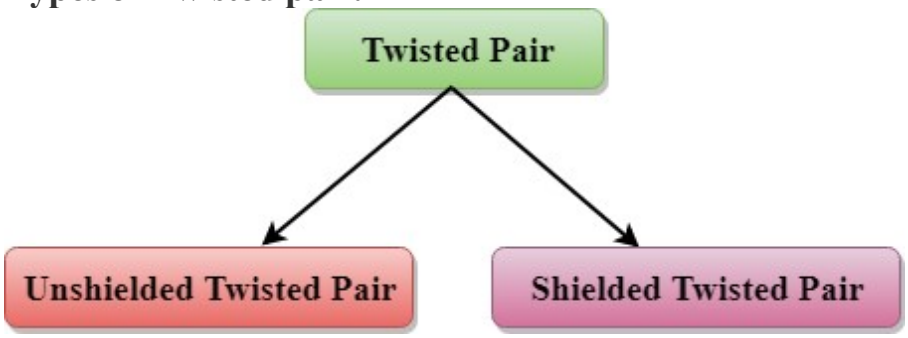
Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.



Types of Twisted pair:



Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

- **Category 1:** Category 1 is used for telephone lines that have low-speed data.
- **Category 2:** It can support upto 4Mbps.
- **Category 3:** It can support upto 16Mbps.
- **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
- **Category 5:** It can support upto 200Mbps.

Advantages Of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantage:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

Characteristics Of Shielded Twisted Pair:

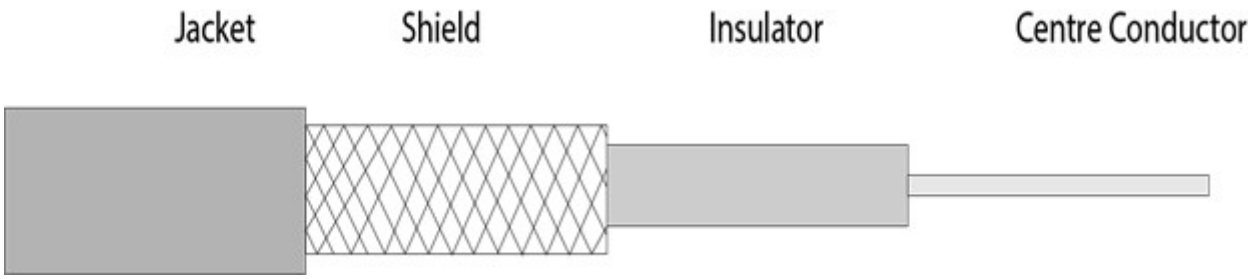
- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate.

Coaxial Cable

- Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
- The name of the cable is coaxial as it contains two conductors parallel to each other.
- It has a higher frequency as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.
- It provides higher bandwidth.

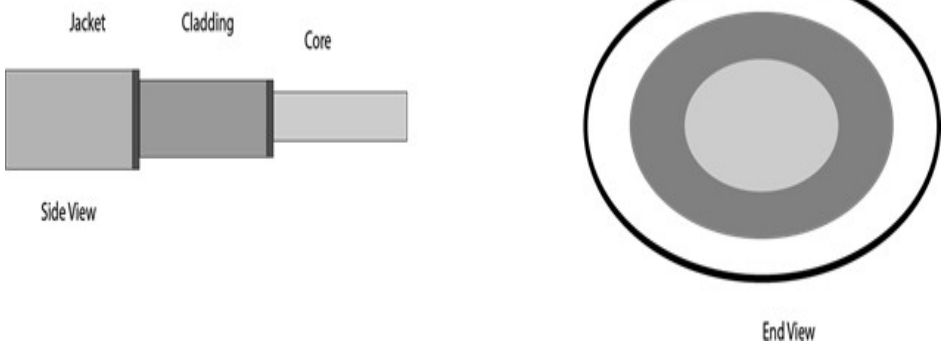
Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fibre Optic

- Fibre optic cable is a cable that uses electrical signals for communication.
- Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
- Fibre optics provide faster data transmission than copper wires.

Diagrammatic representation of fibre optic cable:



Basic elements of Fibre optic cable:

- **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
- **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the

core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.

- **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

Following are the advantages of fibre optic cable over copper:

- **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
- **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
- **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
- **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
- **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

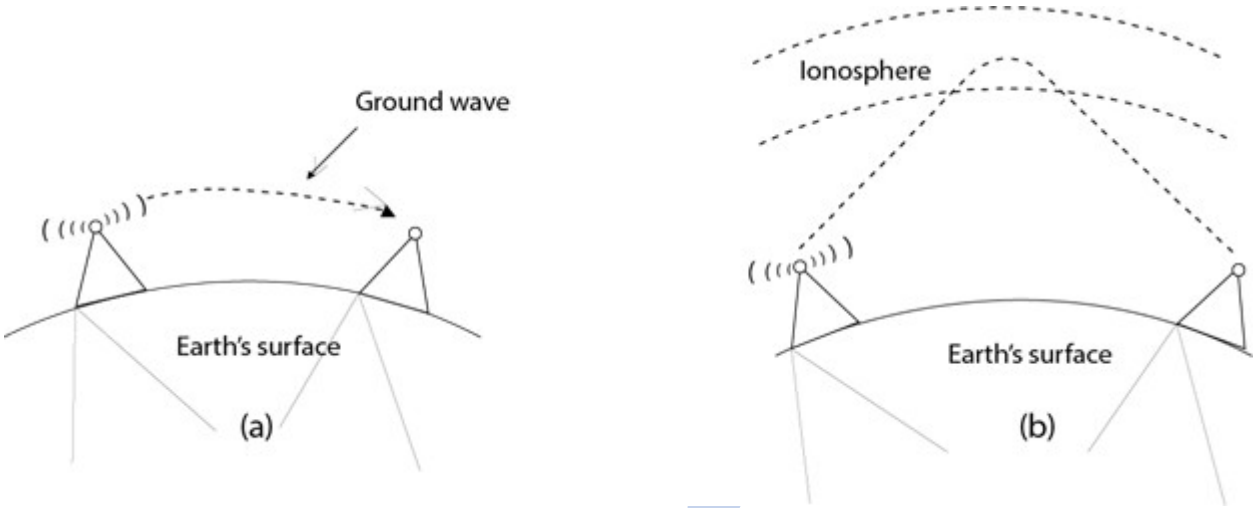
14. UNGUIDED MEDIA

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 khz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of the radio wave is **FM radio**.



Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a large area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves

Microwaves are of two types:

- Terrestrial microwave
- Satellite microwave communication.

Terrestrial Microwave Transmission

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are the electromagnetic waves having the frequency in the range from 1GHz to 1000 GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line of sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Characteristics of Microwave:

- **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.

- **Short distance:** It is inexpensive for short distance.
- **Long distance:** It is expensive as it requires a higher tower for a longer distance.
- **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.

Advantages Of Microwave:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- Microwave transmission provides an easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages of Microwave transmission:

- **Eavesdropping:** An eavesdropping creates insecure communication. Any malicious user can catch the signal in the air by using its own antenna.
- **Out of phase signal:** A signal can be moved out of phase by using microwave transmission.
- **Susceptible to weather condition:** A microwave transmission is susceptible to weather condition. This means that any environmental change such as rain, wind can distort the signal.
- **Bandwidth limited:** Allocation of bandwidth is limited in the case of microwave transmission.

Satellite Microwave Communication

- A satellite is a physical object that revolves around the earth at a known height.
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fibre optic systems.
- We can communicate with any point on the globe by using satellite communication.

Infrared

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.

- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

15. SWITCHING

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

APEC