UNIT V DATA LINK AND PHYSICAL LAYERS

Data Link Layer – Framing – Flow control – Error control – Data-Link Layer Protocols – HDLC –PPP - Media Access Control – Ethernet Basics – CSMA/CD – Virtual LAN – Wireless LAN (802.11)- Physical Layer: Data and Signals - Performance – Transmission media- Switching – Circuit

5.1 Data Link Layer

- In the OSI model, the data link layer is a 4th layer from the top and 2nd layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

Following services are provided by the Data Link Layer:

- Framing
- Addressing
- Error Control
- Flow Control

5.2 Framing

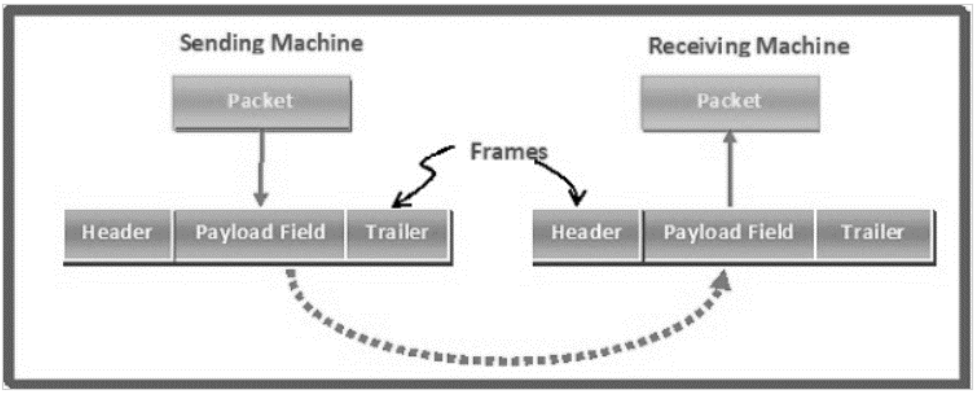
Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information.

Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Frames have headers that contain information such as error-checking codes.

At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender’s and receiver’s addresses.

The process of dividing the data into frames and reassembling it is transparent to the user and is handled by the data link layer.

Framing is an important aspect of data link layer protocol design because it allows the transmission of data to be organized and controlled.

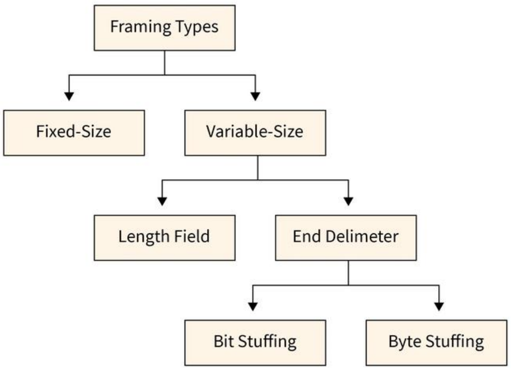


A frame has the following parts −

- Frame Header − It contains the source and the destination addresses of the frame.
- Payload field − It contains the message to be delivered.
- Trailer − It contains the error detection and error correction bits.
- Flag − It marks the beginning and end of the frame.

Types of framing

There are two types of framing:



1. Fixed-size: The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.

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

Solution: Padding

2. Variable size: The size of the frame is variable during this form of framing. In variable-size framing, we are in need of a way to outline the tip of the frame and also the starting of the succeeding frame. This can be utilized in local area networks (LAN).

There are 2 different methods to define the frame boundaries, such as length field and finish decimeters.

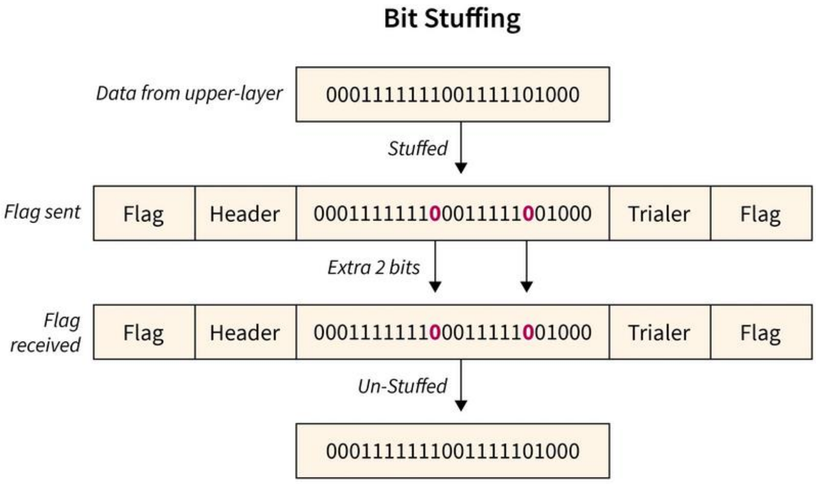
2.1 Length field–To confirm the length of the field, a length field is used. It is utilized in Ethernet (1EEE 802.3).

2.2 End Delimeter–To confirm the size of the frame, a pattern is worn as a delimiter. This methodology is worn in the token ring. In short, it is referred to as ED. Two different methods are used to avoid this condition if the pattern happens within the message.

2.2.1 Bit-Oriented Framing

Most protocols use a special 8-bit pattern flag 01111110 as a result of the delimiter to stipulate the beginning and so the end of the frame. Bit stuffing is completed at the sender end and bit removal at the receiver end.

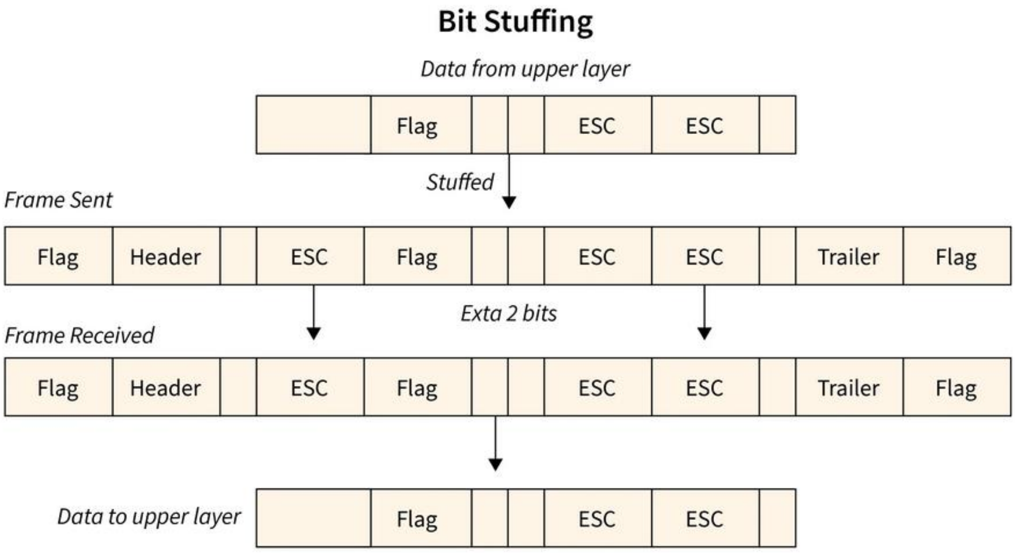
If we have a tendency to get a zero(0) after 5 1s. we have a tendency to tend to still stuff a zero(0). The receiver will remove the zero. Bit stuffing is in addition said as bit stuffing.



2.2.2 Byte-Oriented Framing

Byte stuffing is one of the methods of adding an additional byte once there is a flag or escape character within the text. Take an illustration of byte stuffing as appeared in the given diagram.

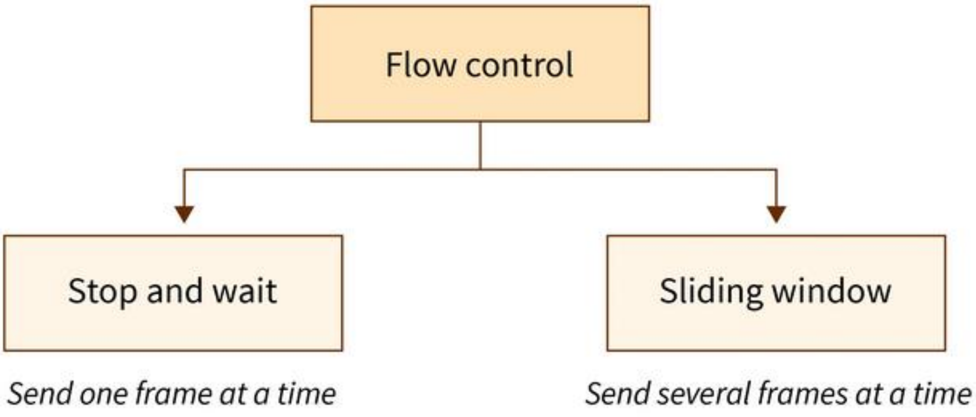
The sender sends the frame by adding three additional ESC bits and therefore the destination machine receives the frame and it removes the extra bits to convert the frame into an identical message.



5.3 Flow Control

Flow control is a set of procedures that restrict the amount of data a sender should send before it waits for some acknowledgment from the receiver.

- Flow Control is an essential function of the data link layer.
- It determines the amount of data that a sender can send.
- It makes the sender wait until an acknowledgment is received from the receiver’s end.
- Methods of Flow Control are **Stop-and-wait**, and **Sliding window**.



Stop-and-wait Protocol

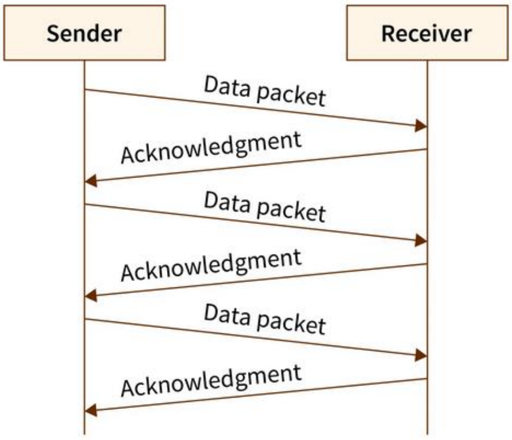
Stop-and-wait protocol works under the assumption that the communication channel is **noiseless** and transmissions are **error-free**.

Working :

- The sender sends data to the receiver.

- The sender stops and waits for the acknowledgment.
- The receiver receives the data and processes it.
- The receiver sends an acknowledgment for the above data to the sender.
- The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
- The process is unidirectional and continues until the sender sends the **End of Transmission (EoT)** frame.

STOPN-AND-WAIT PROTOCOL



Sliding Window Protocol

The **sliding window protocol** is the flow control protocol for noisy channels that allows the sender to send multiple frames even before acknowledgments are received. It is called a **Sliding window** because the sender slides its window upon receiving the acknowledgments for the sent frames.

Working:

- The sender and receiver have a "window" of frames. A window is a space that consists of multiple bytes. The size of the window on the receiver side is always 1.
- Each frame is sequentially numbered from 0 to n - 1, where n is the window size at the sender side.
- The sender sends as many frames as would fit in a window.
- After receiving the desired number of frames, the receiver sends an acknowledgment. The acknowledgment (ACK) includes the number of the next expected frame.

5.4 Error Control

Error control in data link layer is the process of detecting and correcting data frames that have been corrupted or lost during transmission.

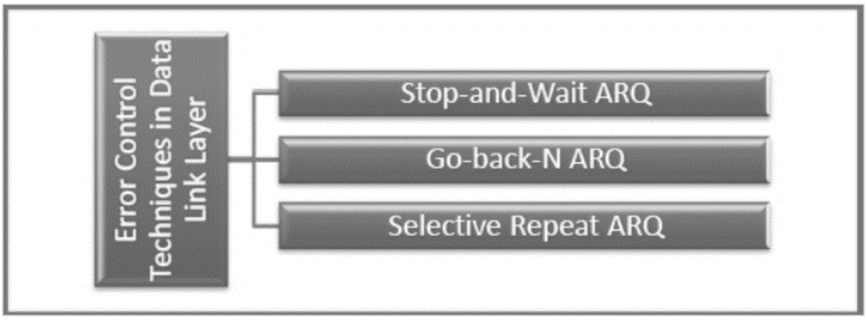
In case of lost or corrupted frames, the receiver does not receive the correct data-frame and sender is ignorant about the loss. Data link layer follows a technique to detect transit errors and take necessary actions, which is retransmission of frames whenever error is detected or frame is lost. The process is called Automatic Repeat Request (ARQ).

The error control mechanism in data link layer involves the following phases −

- **Detection of Error** − Transmission error, if any, is detected by either the sender or the receiver.
- **Acknowledgment** − acknowledgment may be positive or negative.
  - **Positive ACK** − On receiving a correct frame, the receiver sends a positive acknowledge.
  - **Negative ACK** − On receiving a damaged frame or a duplicate frame, the receiver sends a negative acknowledgment back to the sender.
- **Retransmission** − The sender maintains a clock and sets a timeout period. If an acknowledgment of a data-frame previously transmitted does not arrive before the timeout, or a negative acknowledgment is received, the sender retransmits the frame.

Error control technique

There are three main techniques for error control –



Stop and Wait ARQ

This protocol involves the following transitions −

- A timeout counter is maintained by the sender, which is started when a frame is sent.
- If the sender receives acknowledgment of the sent frame within time, the sender is confirmed about successful delivery of the frame. It then transmits the next frame in queue.
- If the sender does not receive the acknowledgment within time, the sender assumes that either the frame or its acknowledgment is lost in transit. It then retransmits the frame.
- If the sender receives a negative acknowledgment, the sender retransmits the frame.

Go-Back-N ARQ

The working principle of this protocol is −

- The sender has buffers called sending window.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.

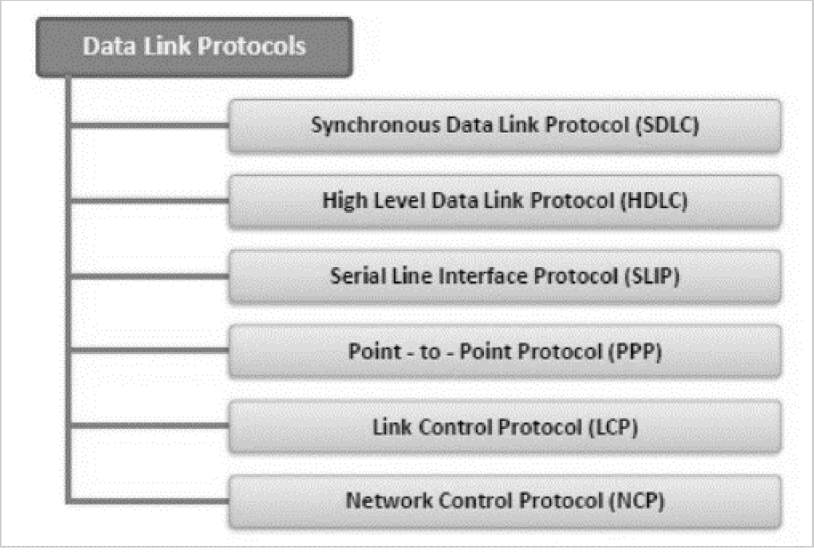
- The receiver receives frames one by one. It keeps track of incoming frame’s sequence number and sends the corresponding acknowledgment frames.
- After the sender has sent all the frames in window, it checks up to what sequence number it has received positive acknowledgment.
- If the sender has received positive acknowledgment for all the frames, it sends next set of frames.
- If sender receives NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK

Selective Repeat ARQ

- Both the sender and the receiver have buffers called sending window and receiving window respectively.
- The sender sends multiple frames based upon the sending-window size, without receiving the acknowledgment of the previous ones.
- The receiver also receives multiple frames within the receiving window size.
- The receiver keeps track of incoming frame’s sequence numbers, buffers the frames in memory.
- It sends ACK for all successfully received frames and sends NACK for only frames which are missing or damaged.
- The sender in this case, sends only packet for which NACK is received.

5.5 Data Link Layer Protocols

Data link layer protocol is generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to bits and bytes being transferred. SDLC, HDLC, SLIP, PPP, LCP, LAP, and NCP are some of the data link layer protocols.


Data Link Protocols
Synchronous Data Link Protocol (SDLC)
High Level Data Link Protocol (HDLC)
Serial Line Interface Protocol (SLIP)
Point - to - Point Protocol (PPP)
Link Control Protocol (LCP)
Network Control Protocol (NCP)

SDLC:

SDLC stands for synchronous data link control protocol, is a communication protocol of a computer.

It is usually used to carry system network architecture traffic. Synchronous data link protocol connects all the remote devices to the mainframe computer at the Central location.

This connection is done in two formats, point to point format i.e. one to one connection, and point to multipoint format, i.e. one to many connections.

SDLC support one to many connections even in case of error detection or error recovery.

SDLC ensures that all the received data units are correct and flow is right from one network point to the next network point.

HDLC:

HDLC stands for High-level data link control protocol, is a bit-orientated code transparent synchronous protocol developed by ISO (International organization for standardization) in1979.

It provides both connection-orientated and connectionless services. HDLC protocol contains various wide-area protocols.

It is based on the SDLC protocol that supports both point-to-point and multipoint communication.

HDLC frames are transferred over synchronous or asynchronous serial communication links. HDLC uses various modes such as normal response mode, asynchronous response mode, asynchronous balanced mode.

Normal response mode is used to share the secondary to primary link without contention. asynchronous response mode is used for full-duplex links. asynchronous balanced mode, support combined terminal which can act as both primary and secondary.

SLIP:

SLIP stands for Serial line interface protocol which is used to add framing byte at the end of the IP Packet. SLIP is a data link layer protocol That transforms the IP packets among ISP (Internet Service Providers) and home user over dial-up links.

SLIP is designed to work with ports and router connections. SLIP does not provide error detection, being reliant on upper-layer protocols for this. Therefore, SLIP on its own is not satisfactory over an error-prone dial-up connection.

PPP:

PPP stands for Point to point protocol. PPP is a data link layer protocol that provides the same services as the Serial line interface protocol.

It is a robust protocol that transfers the other types of pockets also with the IP packets. It provides two protocols LCP and NCP, that we will discuss in the next section. Point to point protocol uses framing methods that describe the frames.

Point to point protocol is also called character orientated protocol which is used to detect errors. PPC provides Connection authentication, data compression, encryption, and transmission. It is used over various networks such as phone lines, cellular telephones, serial cables, trunk lines, ISDNs, Specialized radio links, etc.

LCP:

LCP stands for Link control protocol, is a part of point-to-point control protocol. LCP packets determine the standards of data transmission.

LCP protocol is used to determine the identity of the linked devices, if the device is correct it accepts it otherwise it rejects the device.

It also determines whether the size of the packet is accepted or not. If requirements exceed the parameters, then the link control protocol terminates that link.

LAP:

LAP stands for Link access procedure is a data link layer protocol that is used for framing and transfer the data across point-to-point links.

There are three types of Link access procedure – LAPB (Link Access procedure balanced), LAPF (Link Access Procedure Frame-Mode Bearer Services), and LAPD (Link Access Procedure D-Channel.

LAP was originally derived from HDLC (High-Level Data Link Control), but was later updated and renamed LAPB (LAP Balanced).

NCP:

NCP stands for Network control protocol, is a part of the point-to-point protocol. The network control protocol is used to negotiate the parameter and facilities for the network layer.

For every higher-layer protocol supported by PPP, one NCP is there. IPCP (Internet Protocol control protocol), DNCP (DECnet Phase IV Control Protocol), OSINLCP (OSI Network Layer Control Protocol), IPXCP (Internetwork Packet Exchange Control Protocol), NBFCP (NetBIOS Frames Control Protocol), IPV6CP (IPv6 Control Protocol) are some of the NCPs.

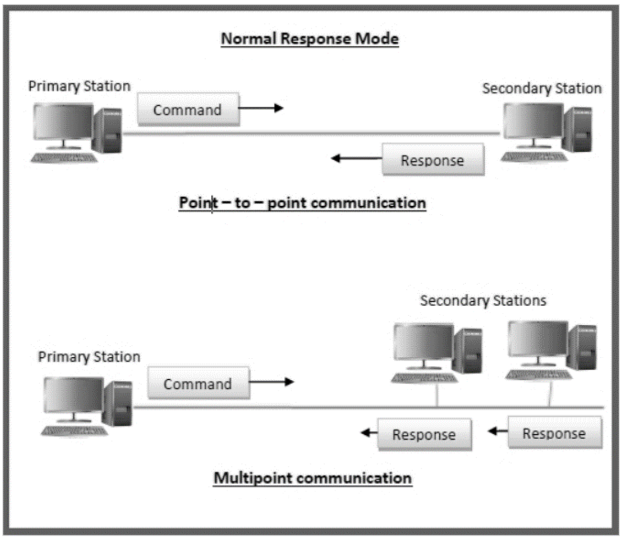
5.6 HDLC

High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

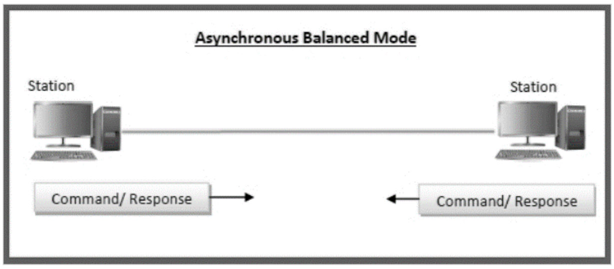
Transfer Modes

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

- **Normal Response Mode (NRM)** − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.



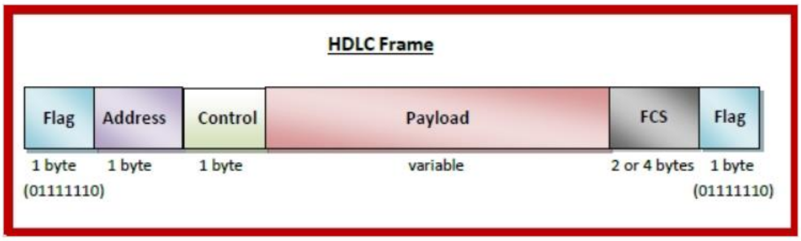
Asynchronous Balanced Mode (ABM) − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



HDLC Frame

HDLC is a bit - oriented protocol where each frame contains up to six fields. The structure varies according to the type of frame. The fields of a HDLC frame are −

- **Flag** − It is an 8-bit sequence that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − It contains the address of the receiver. If the frame is sent by the primary station, it contains the address(es) of the secondary station(s). If it is sent by the secondary station, it contains the address of the primary station. The address field may be from 1 byte to several bytes.
- **Control** − It is 1 or 2 bytes containing flow and error control information.
- **Payload** − This carries the data from the network layer. Its length may vary from one network to another.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



5.7 PPP

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

Components of PPP

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

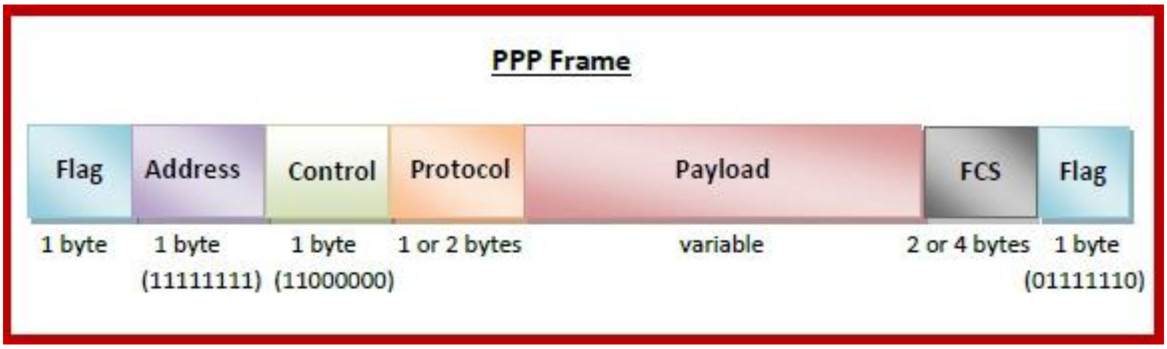
- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for 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)



5.8 Media Access Control

The medium access control (MAC) is a sublayer of the data link layer.

It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

5.8.1 MAC Layer in the OSI Model

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

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

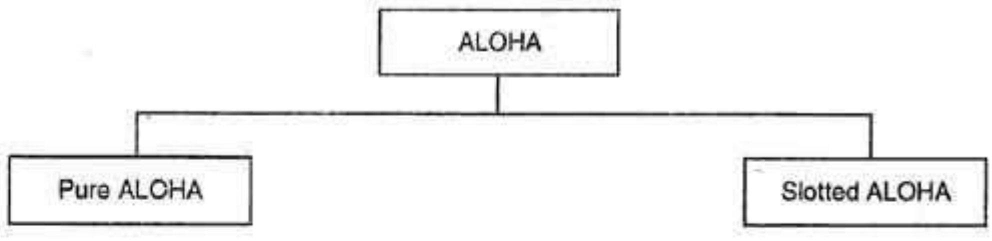
5.8.2 MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth. MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

5.8.3 ALOHA:

ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision.

There are two different versions of ALOHA



Types of ALOHA

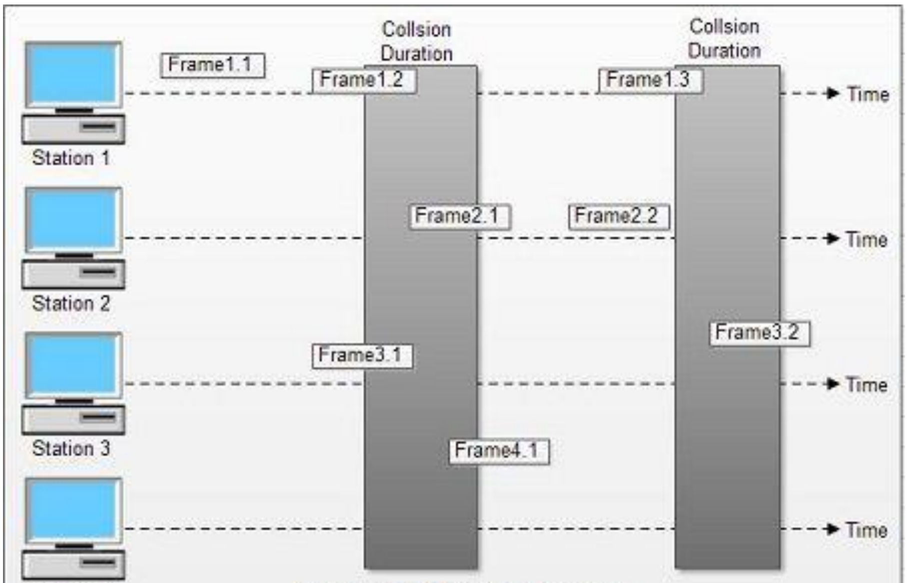
Pure ALOHA

- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

- Figure shows an example of frame collisions in pure ALOHA.



Frames in Pure ALOHA

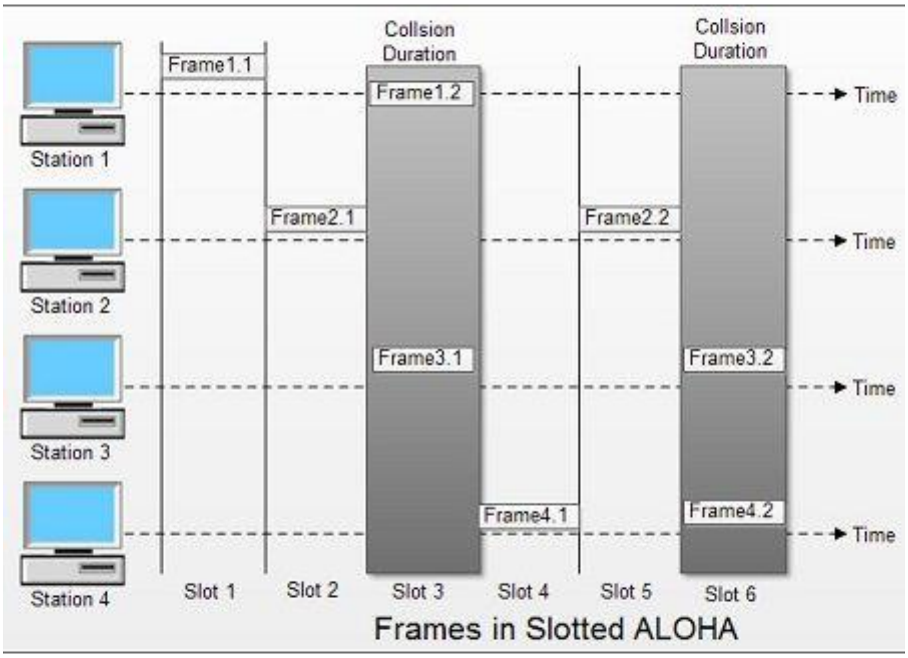
• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



Frames in Slotted ALOHA

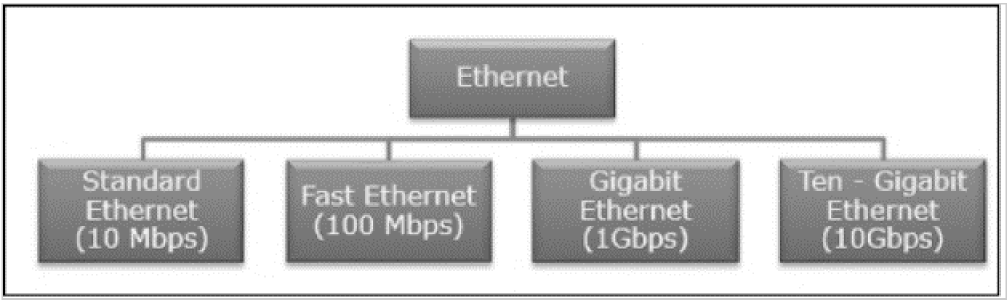
• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot i.e. it misses the time slot then the station has to wait until the beginning of the next time slot.

• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.

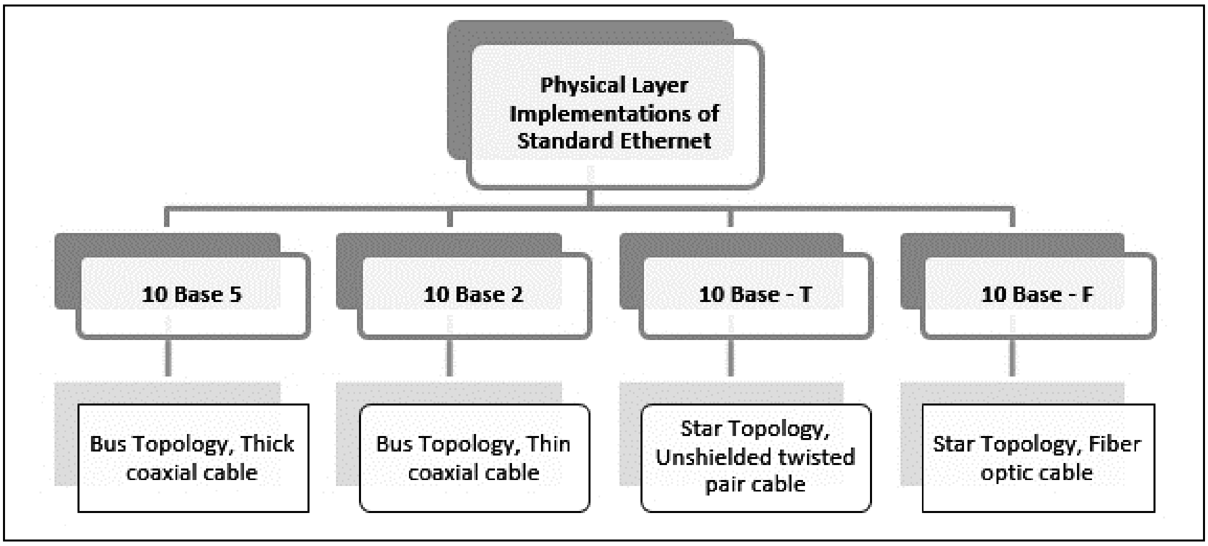
• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

5.9 Ethernet Basics

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


Physical Layer Implementations of Standard Ethernet
10 Base 5
10 Base 2
10 Base - T
10 Base - F
Bus Topology, Thick coaxial cable
Bus Topology, Thin coaxial cable
Star Topology, Unshielded twisted pair cable
Star Topology, Fiber optic cable

10Base5: Thick Ethernet

- The first implementation is called 10Base5, thick Ethernet, or Thicknet.
- 10Base5 was the first Ethernet specification to use a bus topology with an external transceiver(transmitter/receiver) connected via a tap to a thick coaxial cable.

10Base2: Thin Ethernet

- The second implementation is called 10Base2, thin Ethernet, or Cheapernet.

• 10Base2 also uses a bus topology, but the cable is much thinner and more flexible.
• In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station.

10Base-T: Twisted-Pair Ethernet

• The third implementation is called 10Base-T or twisted-pair Ethernet.
• 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable.

10Base-F: Fiber Ethernet

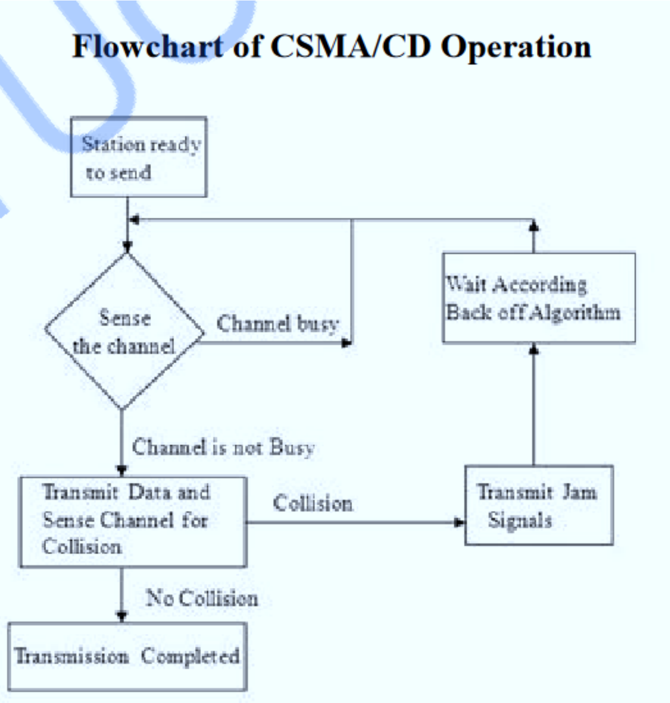
• Although there are several types of optical fiber 10-Mbps Ethernet, the most common is called 10Base-F.
• 10Base-F uses a star topology to connect stations to a hub.
• The stations are connected to the hub using two fiber-optic cables.

Fast Ethernet (100 Mbps)
Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems.
The 100BASE-T standard consists of three different component specifications –
1. 100 BASE-TX
2. 100BASE-T4
3. 100BASE-FX

Gigabit Ethernet (1 Gbps)
• The Gigabit Ethernet upgrades the data rate to 1 Gbps(1000 Mbps).
• Gigabit Ethernet can be categorized as either a two-wire or a four-wire implementation.
• The two-wire implementations use fiber-optic cable (1000Base-SX, short- wave, or 1000Base-LX, long-wave), or STP (1000Base-CX).
• The four-wire version uses category 5 twisted-pair cable (1000Base-T).

5.10 CSMA/CD

¬ Carrier Sense in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.
• If the carrier sensed is idle, then the node transmits the entire frame.
• If the carrier sensed is busy, the transmission is postponed.
¬ Collision Detect means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.



Transmitter Algorithm in CSMA/CD

¬ Transmitter Algorithm defines the procedures for a node that senses a busy medium.

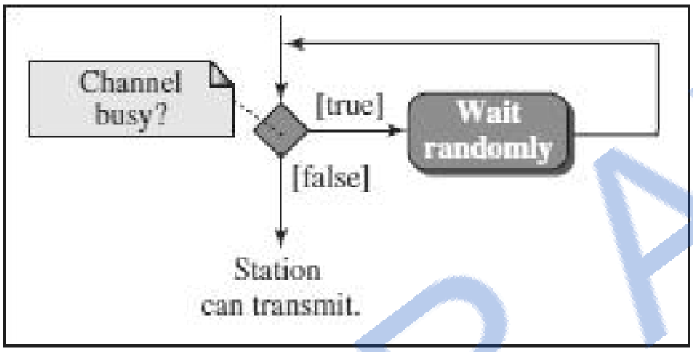
¬ Three types of Transmitter Algorithm exist.

¬ They are

1. Non-Persistent Strategy
2. Persistent Strategy : 1-Persistent & P-Persistent

Non-Persistent Strategy

- In the non-persistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately.
- If the line is not idle, it waits a random amount of time and then senses the line again.

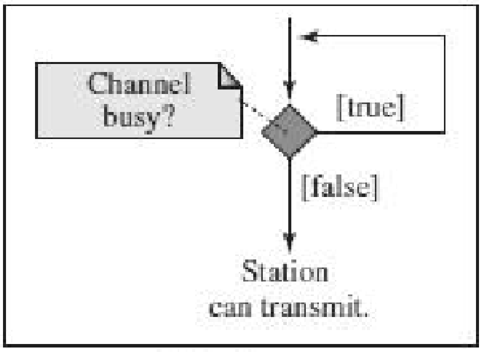


- The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Persistent Strategy

1-Persistent :

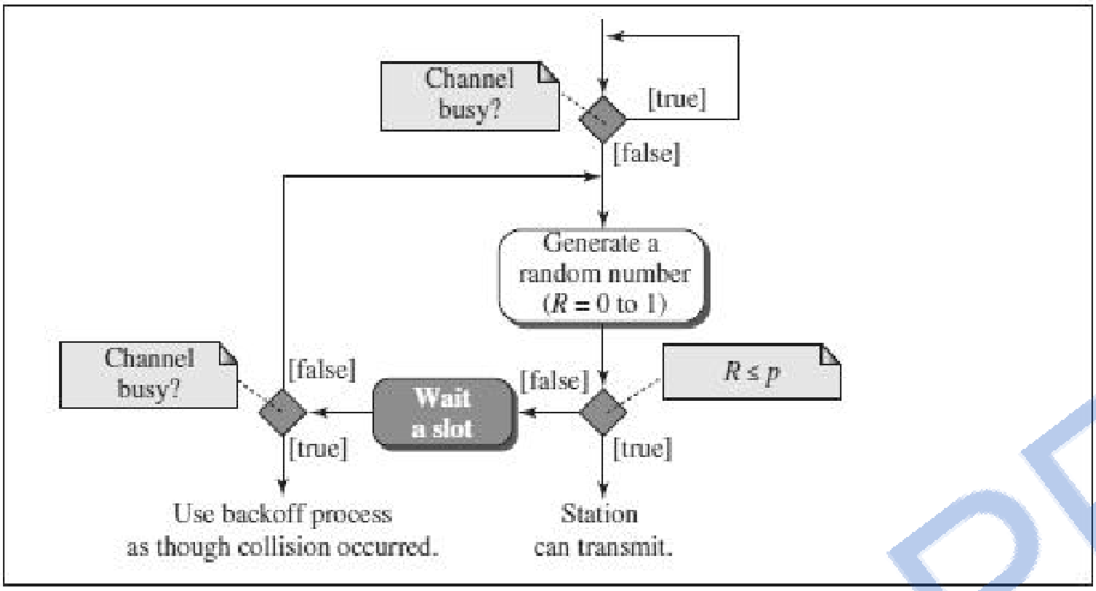
- The 1-persistent method is simple and straightforward.
- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).



- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

P-Persistent :

- In this method, after the station finds the line idle it follows these steps:
- With probability p, the station sends its frame.
- With probability q = 1 − p, the station waits for the beginning of the next time slot and checks the line again.



- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency

EXPONENTIAL BACK-OFF

- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again.
- Each time it tries to transmit but fails, the adaptor doubles the amount of time

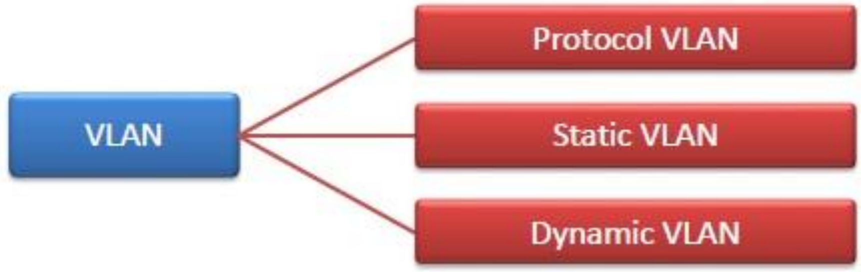
it waits before trying again.

• This strategy of doubling the delay interval between each retransmission attempt is a general technique known as **exponential back-off.**

5.11 Virtual LAN

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

Types of VLANs



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

5.12 Wireless LAN (802.11)

• Wireless communication is one of the fastest-growing technologies.

• The demand for connecting devices without the use of cables is increasing everywhere.

• Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

ADVANTAGES OF WLAN / 802.11

1. Flexibility: Within radio coverage, nodes can access each other as radio waves can penetrate even partition walls.

2. Planning : No prior planning is required for connectivity as long as devices follow standard convention

3. Design : Allows to design and develop mobile devices.

4. Robustness : Wireless network can survive disaster. If the devices survive,communication can still be established.

DISADVANTAGES OF WLAN / 802.11

1. Quality of Service : Low bandwidth (1 – 10 Mbps), higher error rates due to interference, delay due to error correction and detection.
2. Cost : Wireless LAN adapters are costly compared to wired adapters.
3. Proprietary Solution : Due to slow standardization process, many solution are proprietary that limit the homogeneity of operation.
4. Restriction : Individual countries have their own radio spectral policies. This restricts the development of the technology
5. Safety and Security : Wireless Radio waves may interfere with other devices. Eg; In a hospital, radio waves may interfere with high-tech equipment.

TECHNOLOGY USED IN WLAN / 802.11

¬ WLAN's uses Spread Spectrum (SS) technology.

¬ The idea behind Spread spectrum technique is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.

¬ There are two types of Spread Spectrum:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

¬ Frequency hopping is a spread spectrum technique that involves transmitting the signal over a random sequence of frequencies.

¬ That is, first transmitting at one frequency, then a second, then a third, and so on.

¬ The random sequence of frequencies is computed by a pseudorandom number generator.

¬ The receiver uses the same algorithm as the sender and initializes it with the same seed and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.

Direct Sequence Spread Spectrum (DSSS)

¬ Each bit of data is represented by multiple bits in the transmitted signal.

¬ DSSS takes a user data stream and performs an XOR operation with a pseudo –random number.

¬ This pseudo random number is called as chipping sequence.

TOPOLOGY IN WLAN / 802.11

WLANs can be built with either of the following two topologies /architecture:

- Infra-Structure Network Topology
- Ad Hoc Network Topology

Infra-Structure Topology (AP based Topology)

- An infrastructure network is the network architecture for providing communication between wireless clients and wired network resources.
- The transition of data from the wireless to wired medium occurs via a Base Station called AP(Access Point).
- An AP and its associated wireless clients define the coverage area.

Ad-Hoc Topology (Peer-to-Peer Topology)

- An adhoc network is the architecture that is used to support mutual communication between wireless clients.

- Typically, an ad- hoc network is created spontaneously and does not support access to wired networks.
- An adhoc network does not require an AP.

5.13 Physical Layer

Physical layer in the OSI model plays the role of interacting with actual hardware and signaling mechanism. Physical layer is the only layer of OSI network model which actually deals with the physical connectivity of two different stations.

Physical layer provides its services to Data-link layer. Data-link layer hands over frames to physical layer. Physical layer converts them to electrical pulses, which represent binary data.The binary data is then sent over the wired or wireless media.

5.13.1 Data and signals

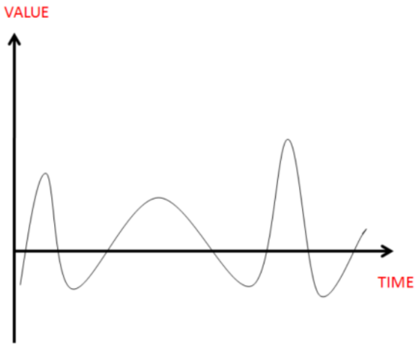
Data or the signal whichever is used in a network, it can be either digital or analog.

Analog and Digital Data

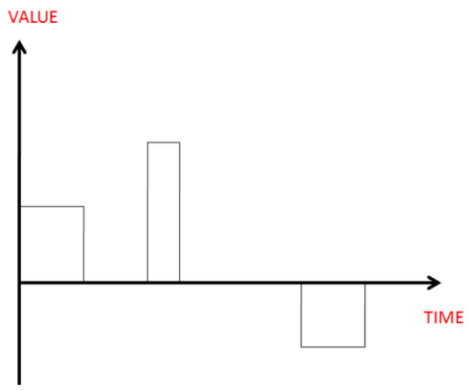
Analog data refers to data that is of continuous format whereas digital data is one which has discrete states. So the analog data takes continuous values and digital data takes discrete values. Analog data can be directly converted into an analog signal or sampled and converted to digital signal. In quite a similar fashion digital data can also be converted to digital signal or into analog signal after modulation. These are converted so that efficient transmission can take place.

Analog and Digital Signal

Similar to data, the signals which represent these can also be digital or analog. Analog signals are known to have many levels of intensity over a given period of time. As the wave moves from one value to another, along the path it traverses via infinite number of values. Digital signals rather have only definite set of values. These are represented using a pair of perpendicular axes. The vertical axis represents the strength of the signal and the horizontal axis gives the time period.



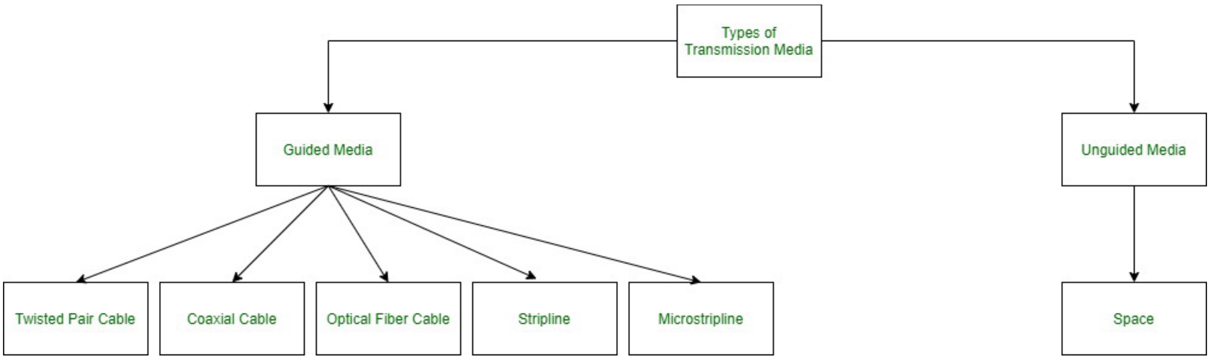
ANALOG SIGNAL



DIGITAL SIGNAL

5.13.2 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.

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.

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

(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.

Advantages:

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

Disadvantages:

- Single cable failure can disrupt the entire network

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.

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

(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.

(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.

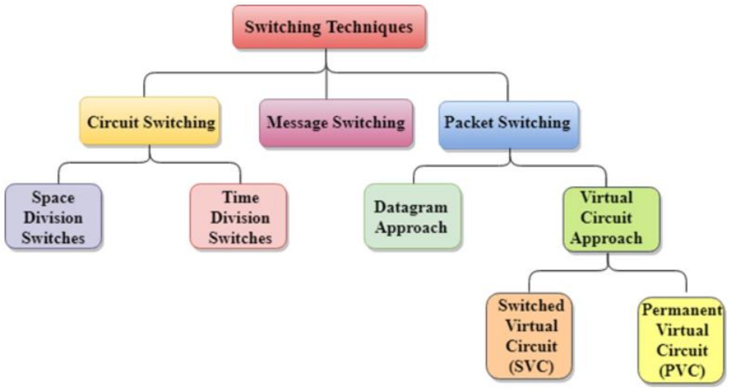
(iii) Infrared –
Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

5.13.3 Switching

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.

- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.

Time Division Switching

The incoming and outgoing signals when received and re-transmitted in a different time slot, is called **Time Division Switching.**

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.

- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

Approaches Of Packet Switching:

There are two approaches to Packet Switching:

Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.