

Module 2

Concept of physical layer

Physical Layer is the bottom-most layer in the Open System Interconnection (OSI) Model which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. Physical Layer sends data bits from one device(s) (like a computer) to another device(s). Physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). Physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

Functions Performed by Physical Layer :

Following are some important and basic functions that are performed by the Physical Layer of the OSI Model –

1. Physical Layer maintains the data rate (how many bits a sender can send per second).
2. It performs Synchronization of bits.
3. It helps in Transmission Medium decision (direction of data transfer).
4. It helps in Physical Topology (Mesh, Star, Bus, Ring) decision (Topology through which we can connect the devices with each other).
5. It helps in providing Physical Medium and Interface decisions.
6. It provides two types of configuration Point to Point configuration and Multi-Point configuration.
7. It provides an interface between devices (like PC's or computers) and transmission medium.
8. It has a protocol data unit in bits.
9. Hubs, Ethernet, etc. device is used in this layer.
10. This layer comes under the category of Hardware Layers (since the hardware layer is responsible for all the physical connection establishment and processing too).
11. It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.
12. It also provides Switching mechanism wherein data packets can be forward from one port (sender port) to the leading destination port.

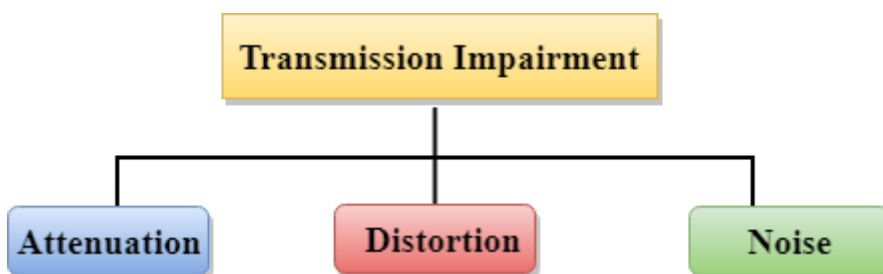
What is Transmission media?

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI**(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

Causes Of Transmission Impairment:

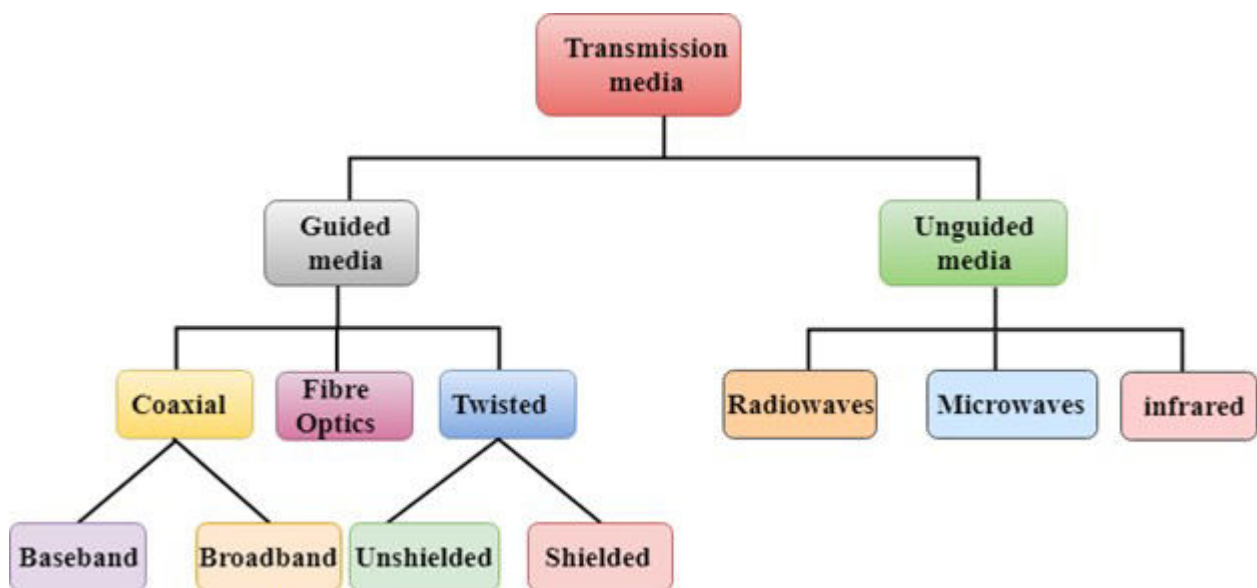


- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Attenuation: Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.

- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Classification Of Transmission Media:



Datalink control and protocol

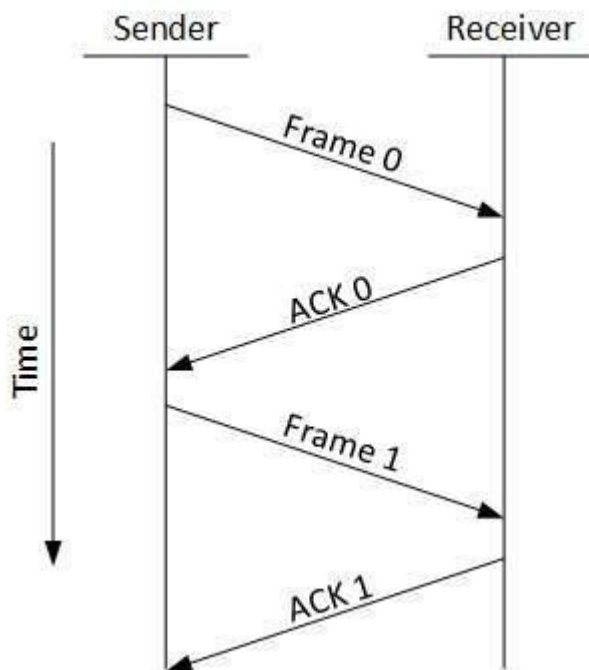
Flow Control

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

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

- **Stop and Wait**

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



- **Sliding Window**

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

Error Control

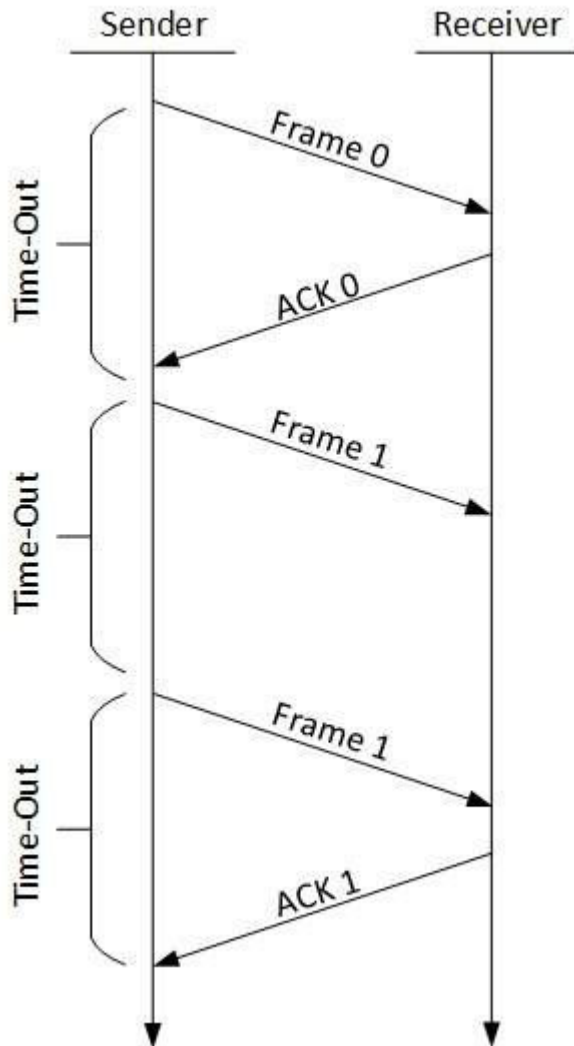
When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with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

Requirements for error control mechanism:

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

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

- **Stop-and-wait ARQ**



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

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

- **Go-Back-N ARQ**

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

MAC(Media Access Control)

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data

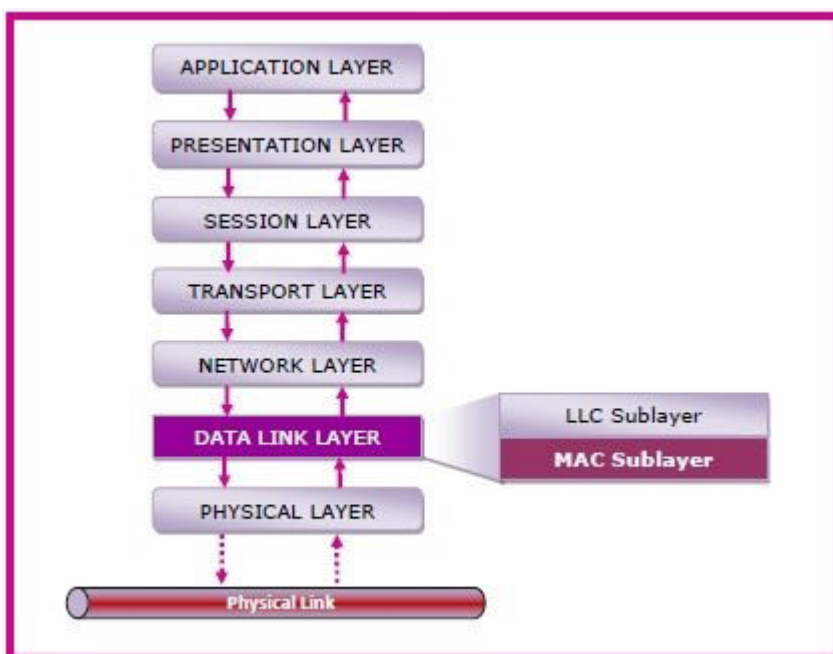
transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

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

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

The following diagram depicts the position of the MAC layer –



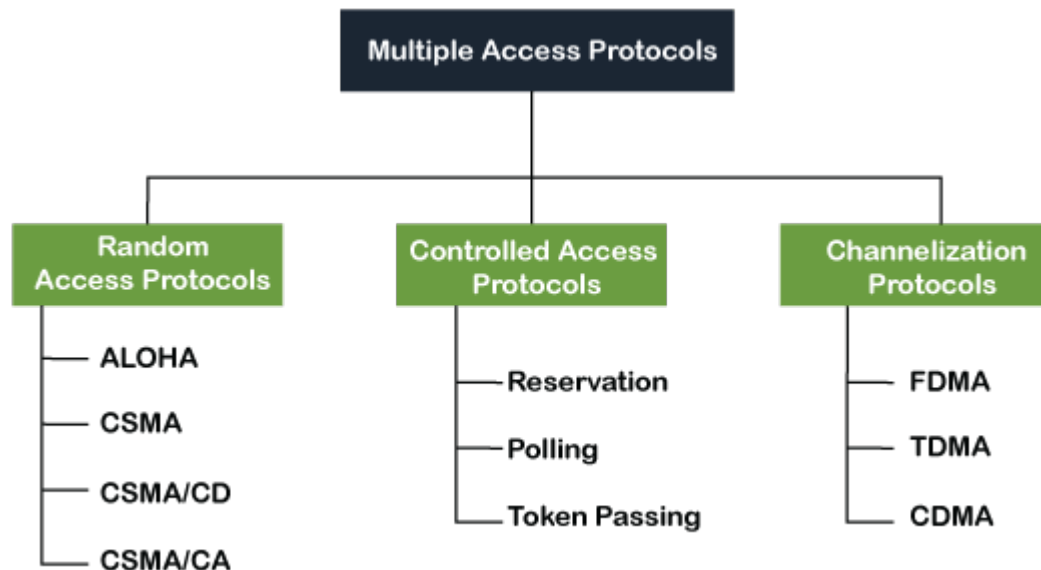
Functions of MAC Layer

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

MAC Addresses

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

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



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

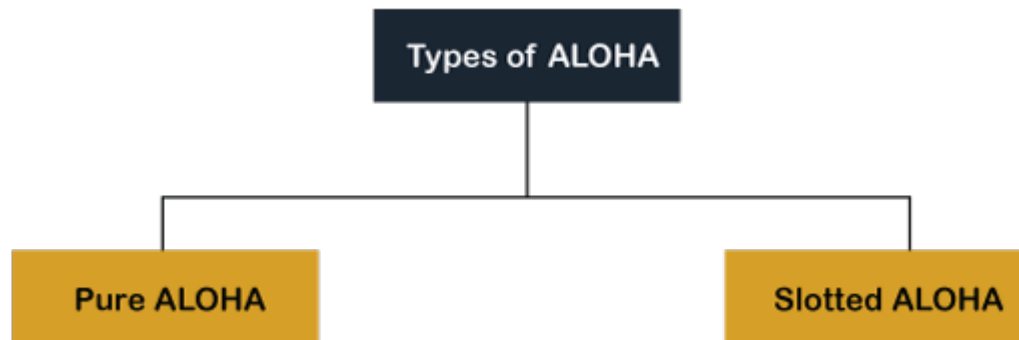
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

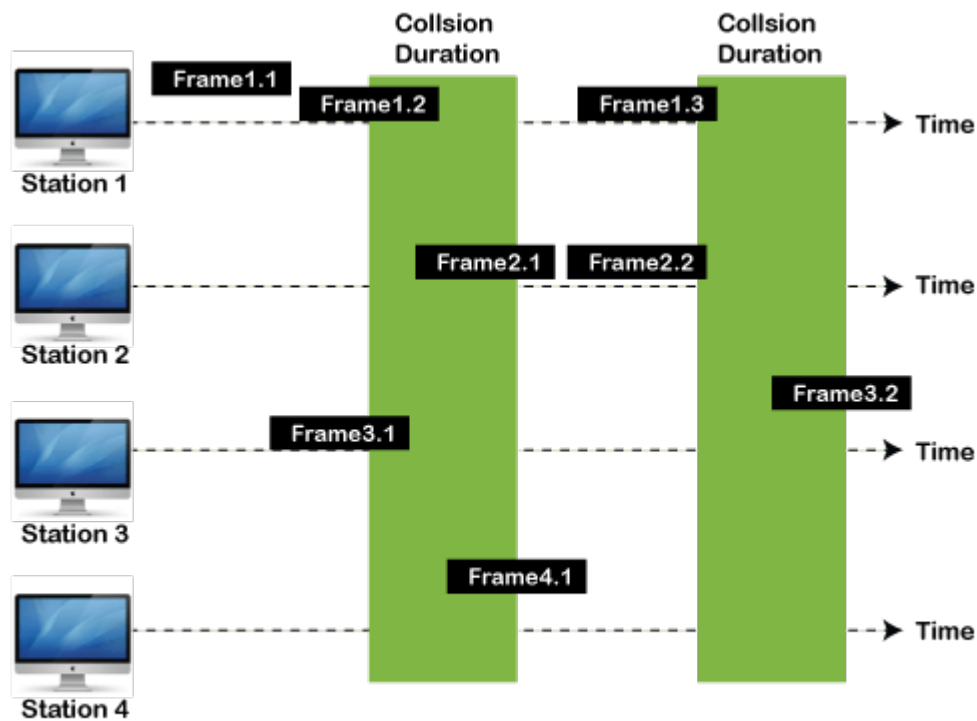
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (T_b). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is $2 * T_{fr}$.
2. Maximum throughput occurs when $G = 1/2$ that is 18.4%.
3. Successful transmission of data frame is $S = G * e^{-2G}$.



Frames in Pure ALOHA

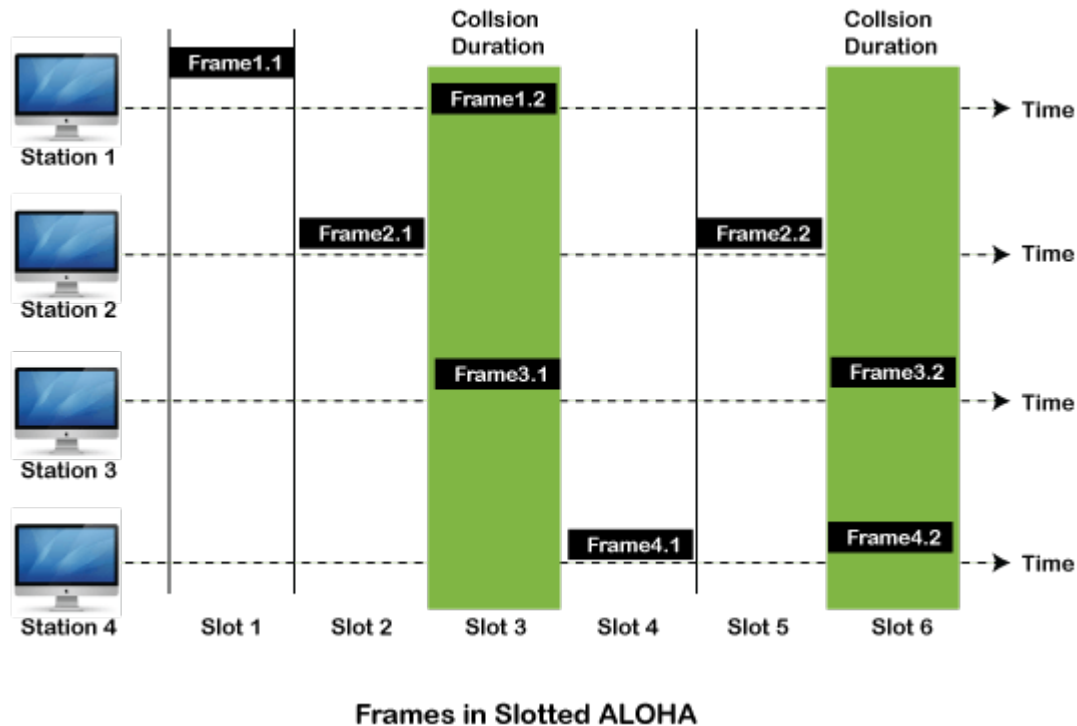
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when $G = 1$ that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is $S = G * e^{-2G}$.

3. The total vulnerable time required in slotted Aloha is T_{fr} .



CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

CSMA Access Modes

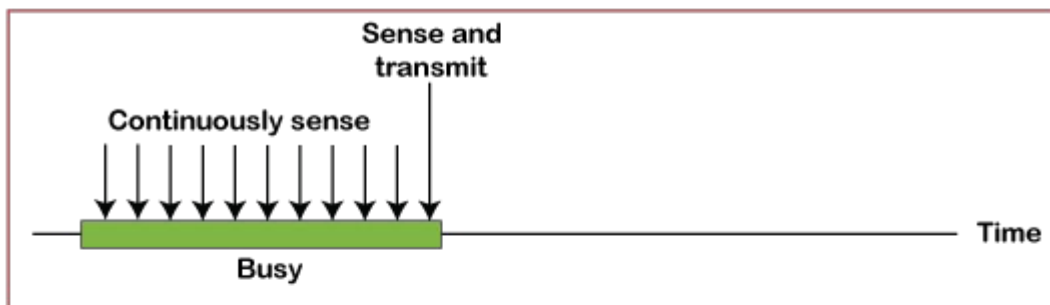
1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the

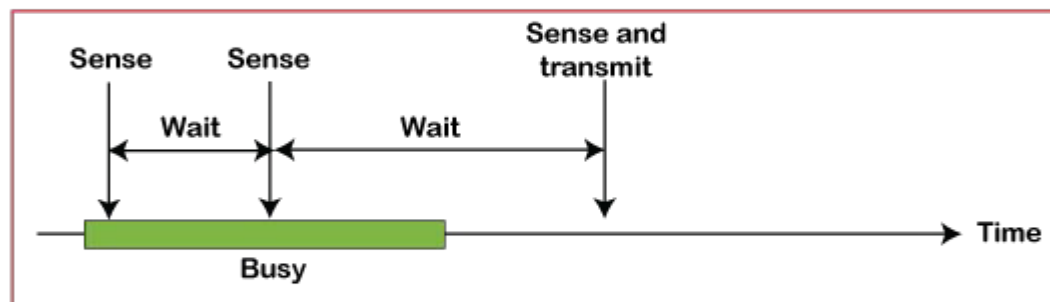
station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**$q = 1-p$ probability**) random time and resumes the frame with the next time slot.

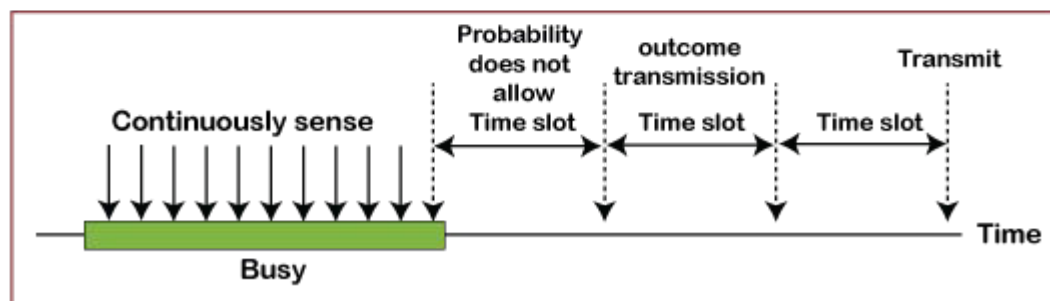
O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the [CSMA/ CA](#) to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

Ethernet

IEEE 802 is a family of [Institute of Electrical and Electronics Engineers](#) (IEEE) standards for [local area networks](#) (LAN), [personal area network](#) (PAN), and [metropolitan area networks](#) (MAN). The IEEE 802 LAN/MAN Standards Committee (LMSC) maintains these standards. The IEEE 802 family of standards has had twenty-four members, numbered 802.1 through 802.24, with a working group of the LMSC devoted to each. However, not all of these working groups are currently active.

The IEEE 802 standards are restricted to [computer networks](#) carrying variable-size packets, unlike [cell relay](#) networks, for example, in which [data](#) is transmitted in short, uniformly sized units called cells. [Isochronous signal](#) networks, in which data is transmitted as a steady stream of [octets](#), or groups of octets, at regular time intervals, are also outside the scope of the IEEE 802 standards.

The number 802 has no significance: it was simply the next number in the sequence that the IEEE used for standards projects.

The services and protocols specified in IEEE 802 map to the lower two layers (data link and physical) of the seven-layer [Open Systems Interconnection \(OSI\)](#) networking reference model. IEEE 802 divides the OSI data link layer into two sub-layers: [logical link control](#) (LLC) and [medium access control](#) (MAC), as follows:

- [Data link layer](#)
 - LLC sublayer
 - MAC sublayer
- [Physical layer](#)

The most widely used standards are for [Ethernet](#), Bridging and Virtual Bridged LANs, [Wireless LAN](#), [Wireless PAN](#), [Wireless MAN](#), [Wireless Coexistence](#), Media Independent Handover Services, and [Wireless RAN](#).

Ethernet Evolution

Name	Description	Status
IEEE 802.1	Higher Layer LAN Protocols Working Group	Active
IEEE 802.2	LLC	Disbanded
IEEE 802.3	Ethernet	Active[3]
IEEE 802.4	Token bus	Disbanded
IEEE 802.5	Token Ring MAC layer	Disbanded
IEEE 802.6	MANs (DQDB)	Disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	Disbanded
IEEE 802.8	Fiber Optic TAG	Disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	Disbanded
IEEE 802.10	Interoperable LAN Security	Disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	Active
IEEE 802.12	100BaseVG	Disbanded
IEEE 802.13	Unused[4]	Reserved for Fast Ethernet development
IEEE 802.14	Cable modems	Disbanded
IEEE 802.15	Wireless PAN	Active
IEEE 802.15.1	Bluetooth certification	Disbanded
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	Hibernating
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB , etc.)	?
IEEE 802.15.4	Low-Rate wireless PAN (e.g., Zigbee , WirelessHART , MiWi , etc.)	Active
IEEE 802.15.5	Mesh networking for WPAN	?

<u>IEEE 802.15.6</u>	<u>Body area network</u>
<u>IEEE 802.15.7</u>	<u>Visible light communications</u>
<u>IEEE 802.16</u>	<u>Broadband Wireless Access (WiMAX certification)</u>
IEEE 802.16.1	<u>Local Multipoint Distribution Service</u>
IEEE 802.16.2	Coexistence wireless access
<u>IEEE 802.17</u>	Resilient packet ring
<u>IEEE 802.18</u>	Radio Regulatory TAG
<u>IEEE 802.19</u>	Wireless Coexistence Working Group
<u>IEEE 802.20</u>	Mobile Broadband Wireless Access
<u>IEEE 802.21</u>	Media Independent Handoff
<u>IEEE 802.22</u>	Wireless Regional Area Network
<u>IEEE 802.23</u>	Emergency Services Working Group
<u>IEEE 802.24</u>	Vertical Applications TAG

Active
?
Hibernating
Hibernating
Hibernating
Disbanded
Active
?
Disbanded
Hibernating
Hibernating
Disbanded
?