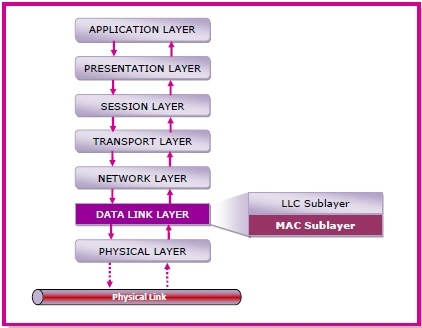
**Topic: MAC SUBLAYER**

The [medium access control](https://www.tutorialspoint.com/multiple-access-protocols-in-computer-networks) (MAC) is a sublayer of the [data link layer](https://www.tutorialspoint.com/data_communication_computer_network/data_link_layer_introduction.htm) of the [open system interconnections (OSI) reference model](https://www.tutorialspoint.com/The-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.



**TOPIC: Channel Allocation: Static, Dynamic**

When there are more than one user who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users. The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.

**Channel Allocation Schemes**

Channel Allocation may be done using two schemes −

* Static Channel Allocation
* Dynamic Channel Allocation

## Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.

This scheme is also referred as fixed channel allocation or fixed channel assignment.

In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

## Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

This allocation scheme optimises bandwidth usage and results is faster transmissions.

**TOPIC: MAC PROTOCOLS – ALOHA, CSMA, Collision-Free Protocols, Limited-Contention Protocols**

* The [data link layer](https://www.javatpoint.com/data-link-layer) is used in a computer network to transmit the data between two devices or nodes.
* It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**.
* The upper layer has the responsibility to **flow control and the error control** in the data link layer, and hence it is termed as **logical of data link control**.
* Whereas the lower sub-layer **is used to handle and reduce the collision or multiple access** on a channel. Hence it is termed as [**media access control**](https://www.javatpoint.com/mac-full-form) or the multiple access resolutions.

## Data Link Control

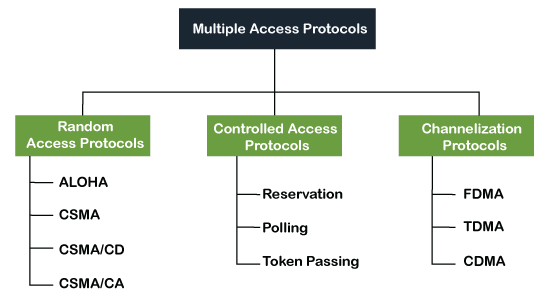
A [data link control](https://www.javatpoint.com/data-link-controls) is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

## What is a multiple access protocol?

* When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel.
* Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

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



### **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.

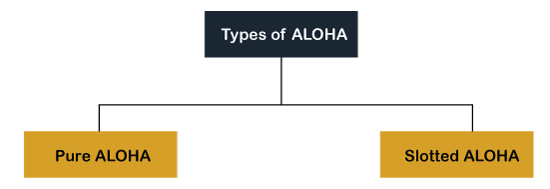
* Aloha
* CSMA
* CSMA/CD
* CSMA/CA

### 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.

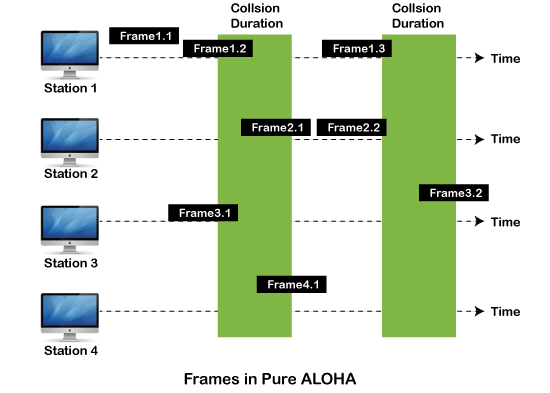


**Pure Aloha**

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 (Tb)**. 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.

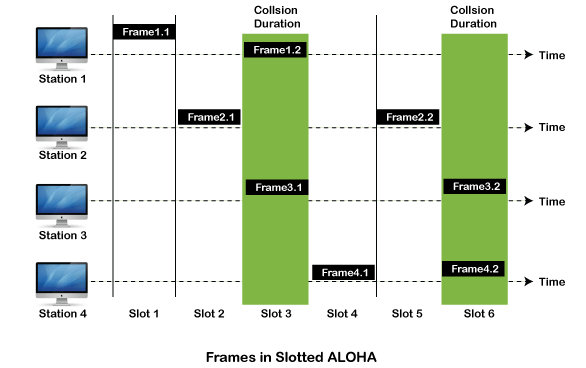


As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same 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.



### **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.

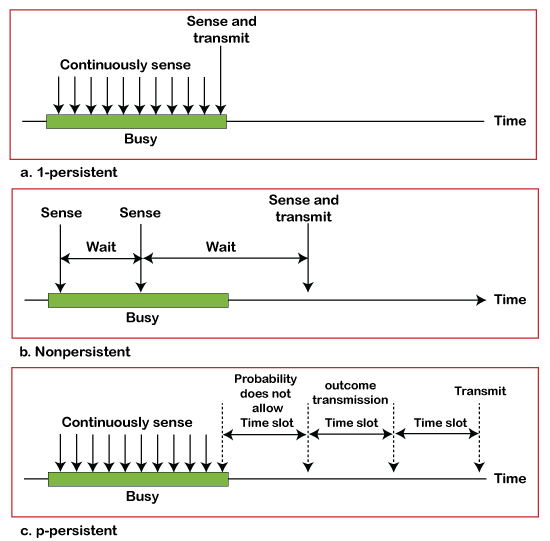
**CSMA Access Modes**

**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.



**TOPIC: COLLISSION FREE PROTOCOLS**

In computer networks, when more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled. This event is called collision.

The Medium Access Control (MAC) layer of the OSI model is responsible for handling collision of frames.

Collision – free protocols are devised so that collisions do not occur. Protocols like CSMA/CD and CSMA/CA nullifies the possibility of collisions once the transmission channel is acquired by any station. However, collision can still occur during the contention period if more than one stations starts to transmit at the same time.

Collision – free protocols resolves collision in the contention period and so the possibilities of collisions are eliminated.

## Types of Collision – free Protocols

## https://www.tutorialspoint.com/assets/questions/media/22915/types_of_collisions.jpg

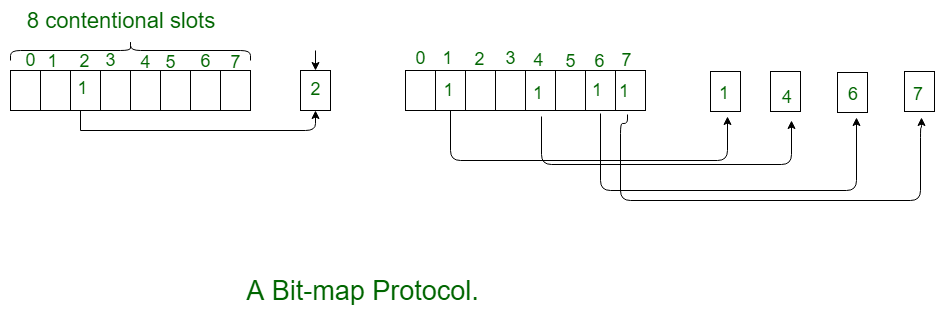
## Bit – map Protocol

In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot. So, before transmission, each station knows whether the other stations want to transmit. Collisions are avoided by mutual agreement among the contending stations on who gets the channel.

In this protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot.

Suppose that there are 10 stations. So the number of contention slots will be 10. If the stations 2, 3, 8 and 9 wish to transmit, they will set the corresponding slots to 1 as shown in the following diagram:

Once each station announces itself, one of them gets the channel based upon any agreed criteria. Generally, transmission is done in the order of the slot numbers. Each station has complete knowledge whether every other station wants to transmit or not, before transmission starts. So, all possibilities of collisions are eliminated.



## Binary Countdown

This protocol overcomes the overhead of 1 bit per station of the bit – map protocol. Here, binary addresses of equal lengths are assigned to each station. For example, if there are 6 stations, they may be assigned the binary addresses 001, 010, 011, 100, 101 and 110. All stations wanting to communicate broadcast their addresses. The station with higher address gets the higher priority for transmitting.

In a binary countdown protocol, each station is assigned a binary address. The binary addresses are bit strings of equal lengths. When a station wants to transmit, it broadcasts its address to all the stations in the channel, one bit at a time starting with the highest order bit.

In order to decide which station gets the channel access, the addresses of the stations which are broadcasted are ORed. The higher numbered station gets the channel access.

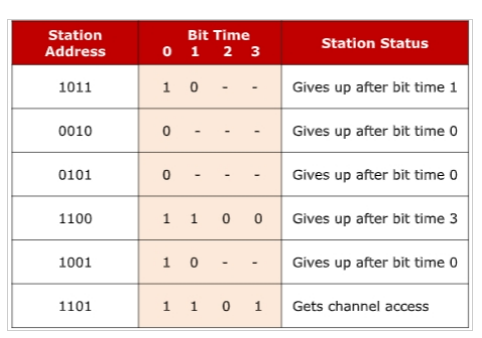
## Example

Suppose that six stations contend for channel access which have the addresses: 1011, 0010, 0101, 1100, 1001 and 1101.

The iterative steps are −

* All stations broadcast their most significant bit, i.e. 1, 0, 0, 1, 1, 1. Stations 0010 and 0101 sees 1 bit in other stations, and so they give up competing for the channel.
* The stations 1011, 1100, 1001 and 1101 continue. They broadcast their next bit, i.e. 0, 1, 0, 1. Stations 1011 and 1001 sees 1 bit in other stations, and so they give up competing for the channel.
* The stations 1100 and 1101 continue. They broadcast their next bit, i.e. 0, 0. Since both of them have same bit value, both of them broadcast their next bit.
* The stations 1100 and 1101 broadcast their least significant bit, i.e. 0 and 1. Since station 1101 has 1 while the other 0, station 1101 gets the access to the channel.
* After station 1101 has completed frame transmission, or there is a time-out, the next contention cycle starts.

The procedure is illustrated as follows −



## Limited Contention Protocols

These protocols combines the advantages of collision based protocols and collision free protocols. Under light load, they behave like ALOHA scheme. Under heavy load, they behave like bitmap protocols.

## Adaptive Tree Walk Protocol

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows -

## https://www.tutorialspoint.com/assets/questions/media/22915/adaptive_tree_walk_protocol.jpg

Initially all nodes (A, B ……. G, H) are permitted to compete for the channel. If a node is successful in acquiring the channel, it transmits its frame. In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). Nodes belonging to only one of them is permitted for competing. This process continues until successful transmission occurs.

**TOPIC: LIMITED CONTENTION PROTOCOL**

Limited Contention Protocols are the media access control (MAC) protocols that combines the advantages of collision based protocols and collision free protocols. They behave like slotted ALOHA under light loads and bitmap protocols under heavy loads.

**Concept**

In computer networks, when more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled, an event called collision.

In collision based protocols like ALOHA, all stations are permitted to transmit a frame without trying to detect whether the transmission channel is idle or busy.

In slotted ALOHA, the shared channel is divided into a number of discrete time intervals called slots. Any station having a frame can start transmitting at the beginning of a slot. Since, this works very good under light loads, limited contention protocols behave like slotted ALOHA under low loads.

However, with the increase in loads, there occurs exponential growth in number of collisions and so the performance of slotted ALOHA degrades rapidly. So, under high loads, collision free protocols like bitmap protocols work best.

In collision free protocols, channel access is resolved in the contention period and so the possibilities of collisions are eliminated. In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel. If a station has a frame to send, it sets the corresponding bit in the slot. So, before transmission, each station knows whether the other stations want to transmit. Collisions are avoided by mutual agreement among the contending stations on who gets the channel. Limited contention protocols behave like slotted ALOHA under low loads.

**Working Principle**

Limited contention protocols divide the contending stations into groups, which may or not be disjoint.

At slot 0, only stations in group 0 can compete for channel access. At slot 1, only stations in group 1 can compete for channel access and so on.

In this process, if a station successfully acquires the channel, then it transmits its data frame. If there is a collision or there are no stations competing for a given slot in a group, the stations of the next group can compete for the slot.

By dynamically changing the number of groups and the number of stations allotted in a group according to the network load, the protocol changes from slotted ALOHA under low loads to bit map protocol under high loads.

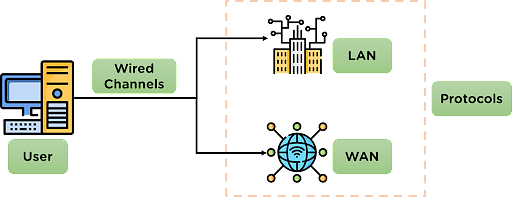
Under low loads, only one group is there containing all stations, which is the case of slotted ALOHA. As the load increases, more groups are added and the size of each group is reduced. When the load is very high, each group has just one station, i.e. only one station can compete at a slot, which is the case of bit map protocol.

The performance of limited contention protocol is highly dependent upon the algorithm to dynamically adjust the group configurations to the changes in network environment.

**Example** − An example of limited contention protocol is Adaptive Tree Walk Protocol

**TOPIC: ETHERNET**

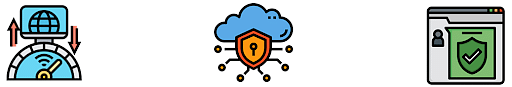
## What Is Ethernet?



Ethernet is designed for the [transmission of data](https://www.simplilearn.com/understanding-data-security-rar30-article) over the channel using wired technology and is used for high-speed data transmission. It is also responsible for applying some protocols for smooth and efficient data transmission over the network.

Ethernet uses cables to transmit data in a network model, such as LAN and, in some cases, WAN. It is more reliable and secure, providing better network connectivity.

## Why Use Ethernet?



Ethernet technology is used for establishing connections and is preferred for network channels. It is used in industry networks, college campuses, and medical institutions because it provides services to the data being transmitted.

* Ethernet provides high-speed data transmission in the network.
* It establishes a secure connection for transferring data in the network.
* Ethernet is reliable, as the possibility of outside interference is very low as cable data is difficult to hack into.

## Types of Ethernet

Depending on the network requirements, the type of ethernet networks applied in the communication also varies. The different types of ethernet connections are mentioned below:

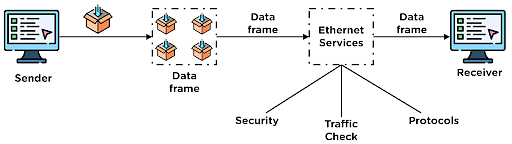
* Fast Ethernet: This Ethernet type is used for transferring data around the network at a speed of 100 Mbps through twisted-pair cables or optical cables. This type of data transmitted can be done without applying protocols.
* Gigabit Ethernet: This type of Ethernet also uses optical and twisted pair cables for data transmission at 1000 Mbps. This is also one of the most preferred Ethernet networks.
* Switched Ethernet: This Ethernet type installs network devices such as switches or hubs to improve the network transmission. The transmission range for this type ranges from 1000Mbps to 10Gbps.

## Working of Ethernet Network

The Ethernet network is designed to work in the 1st layer (physical layer) and 2nd layer (Data Link Layer) of the OSI model.

Ethernet divides the transmission of data into two parts: packets and frames.

* Packet–Refers to a unit of data in the network.
* Frame–Refers to the collection of data packets being transmitted.



The data to be transmitted is converted into data packets in the network and then transferred to the channel. At a point, multiple data packets are collected to form a data frame, which is then transmitted further in the network channel.

During data transmission, Ethernet applies various services over the data being transmitted, such as security checks, traffic control services & other protocols.

## Advantages and Disadvantages of Ethernet

|  |  |
| --- | --- |
| Advantages | Disadvantages |
| 1. The cost of installing an Ethernet connection is affordable. | Ethernet networks are more suited for short-distance connections. |
| 2. Provides high-speed data transmission for data in the network. | Troubleshooting faults in the ethernet connection is difficult. |
| 3. It maintains data quality and also provides a secure channel for data transmission. | Increased cases of network traffic in the network channel. |

## Ethernet vs Internet

### Network Model

|  |  |
| --- | --- |
| Ethernet | Internet |
| Ethernet is preferred for small distance network connections, such as schools, hospitals, etc. | Internet connections are available for all distance network channels. |

### Network Security and Reliability

|  |  |
| --- | --- |
| Ethernet | Internet |
| Ethernet connections are secure and are less prone to external interference and provide data security. | The Internet is an open format network connection, so it is affected more because of external interference. |

### Network Control

|  |  |
| --- | --- |
| Ethernet | Internet |
| Ethernet is less complex due to being wired in connection and provides much better transmission of data. | The Internet is a connection of multiple networks, so it requires a regular inspection from [network administrators](https://www.simplilearn.com/boost-networking-career-with-cisco-credentials-article). |

# IEEE 802.11 Architecture

The IEEE 802.11 standard, commonly known as Wi-Fi, outlines the architecture and defines the MAC and physical layer specifications for wireless LANs (WLANs). Wi-Fi uses high-frequency radio waves instead of cables for connecting the devices in LAN. Given the mobility of WLAN nodes, they can move unrestricted within the network coverage zone. The 802.11 structure is designed to accommodate mobile stations that participate actively in network decisions. Furthermore, it can seamlessly integrate with 2G, 3G, and 4G networks.

The Wi-Fi standard represents a set of wireless LAN standards developed by the Working Group of IEEE LAN/MAN standards committee (IEEE 802). The term 802.11x is also used to denote the set of standards. Various specifications and amendments include 802.11a, 802.11b, 802.11e, 802.11g, 802.11n etc.