

**Q1. What are the design issue in Data link Layer?**

Ans. The design issues in the Data Link Layer include the following:

1. **Framing:** Determining how to break the data stream into manageable units or frames, including defining frame boundaries.
2. **Error Detection and Correction:** Implementing mechanisms to detect and correct errors that may occur during data transmission. This includes techniques like checksums, CRC, and Hamming codes.
3. **Flow Control:** Managing the rate of data transmission between sender and receiver to prevent the sender from overwhelming the receiver. Common methods include stop-and-wait and sliding window protocols.
4. **Access Control:** Regulating how multiple devices access the shared medium, especially in networks with multiple nodes. Protocols like CSMA/CD and token ring help manage this.
5. **Link Layer Protocols:** Defining the specific protocols used for communication at the Data Link Layer, such as Ethernet, PPP (Point-to-Point Protocol), and HDLC (High-Level Data Link Control).
6. **Physical Addressing:** Including the use of MAC addresses to identify devices on the network for proper data delivery.
7. **Link Management:** Establishing, maintaining, and terminating connections between devices, ensuring reliable communication.

**Q2. What are Data Link Control and Protocols? Explain in detail.**

Ans. Data Link Control refers to the protocols and mechanisms used in the Data Link Layer of the OSI model to manage data transmission between directly connected network nodes. It ensures that data frames are transmitted reliably and efficiently over the physical medium. The primary functions of Data Link Control include framing, addressing, error detection and correction, flow control, and medium access control. Here's a detailed overview:

1. **Framing:** This process involves encapsulating network layer packets into frames with defined headers and trailers. The header typically includes source and destination MAC addresses, while the trailer may include error-checking information. Various methods can be used for framing, including byte stuffing, bit stuffing, and fixed-size frames.
2. **Addressing:** Data Link Layer protocols use physical addressing to identify devices on a local network. Each network interface card (NIC) has a unique MAC address, which is used to ensure that frames reach the correct destination.
3. **Error Detection and Correction:** Protocols implement mechanisms to identify and correct errors that occur during data transmission. Common techniques include:
  - **Checksums:** A simple method that sums the data in a frame and appends the result.

- **Cyclic Redundancy Check (CRC):** A more robust method that treats data as polynomials and checks for errors using polynomial division.
  - **Hamming Code:** An error-correcting code that allows for the detection and correction of single-bit errors.
4. **Flow Control:** This ensures that a sender does not overwhelm a receiver by sending data too quickly. Common flow control methods include:
- **Stop-and-Wait ARQ:** The sender transmits one frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
  - **Sliding Window Protocol:** This allows multiple frames to be in transit before requiring an ACK, increasing efficiency and throughput.
5. **Medium Access Control (MAC):** In networks where multiple devices share the same communication medium, MAC protocols manage how devices gain access to the medium. Various methods include:
- **Carrier Sense Multiple Access (CSMA):** Devices listen to the medium before transmitting.
  - **Token Ring:** A token circulates around the network, and only the device holding the token can transmit.
  - **Time Division Multiple Access (TDMA):** Time slots are assigned to devices for transmission.
6. **Link Layer Protocols:** Several specific protocols operate at the Data Link Layer, including:
- **Ethernet:** The most widely used LAN technology, utilizing CSMA/CD for collision detection.
  - **PPP (Point-to-Point Protocol):** Commonly used for direct connections between two nodes, providing authentication and compression.
  - **HDLCL (High-Level Data Link Control):** A bit-oriented protocol used for point-to-point and multipoint connections, providing framing, error control, and flow control.

In summary, Data Link Control and its associated protocols play a crucial role in ensuring that data is transmitted reliably, efficiently, and securely across the physical network. They manage the complexities of data communication, allowing higher layers of the OSI model to focus on processing and interpreting the data rather than the details of transmission.

### Q3. What is Flow and Error Control, Stop-and-wait ARQ? Explain in detail.

Ans. Flow and error control are essential functions of the Data Link Layer, ensuring reliable communication between devices in a network. Here's a detailed explanation:

#### Flow Control

Flow control is a technique used to manage the pace at which data is sent from a sender to a receiver, ensuring that the receiver is not overwhelmed by too much data at once. It helps prevent buffer overflow at the receiver, which can lead to data loss. The main methods of flow control include:

##### 1. Stop-and-Wait Protocol:

- In this protocol, the sender transmits a single frame and waits for an acknowledgment (ACK) from the receiver before sending the next frame.
- This method is simple and easy to implement, but it can be inefficient, especially in high-latency networks, as the sender remains idle while waiting for the ACK.

## 2. Sliding Window Protocol:

- This method allows multiple frames to be sent before requiring an ACK for the first frame.
- The sender maintains a "window" of frames that can be sent without waiting for acknowledgment, increasing the throughput and efficiency of the communication.
- The size of the window can be adjusted based on network conditions, allowing for more flexibility.

## Error Control

Error control involves techniques used to detect and correct errors that may occur during data transmission. The primary methods for error control include:

### 1. Error Detection:

- Mechanisms that identify errors in transmitted frames. Common techniques include:
  - **Checksums:** A simple error detection method where a checksum value is calculated from the data and sent along with the frame. The receiver calculates the checksum again to check for discrepancies.
  - **Cyclic Redundancy Check (CRC):** A more robust method that treats data as polynomials and checks for errors using polynomial division. It provides better error detection capabilities than checksums.

### 2. Error Correction:

- Mechanisms that not only detect errors but also correct them. Common techniques include:
  - **Hamming Code:** A method that adds redundant bits to the data, allowing the detection and correction of single-bit errors.
  - **Reed-Solomon Code:** A more advanced error-correcting code that can correct multiple errors, widely used in data storage and transmission.

## Stop-and-Wait ARQ

Stop-and-Wait Automatic Repeat reQuest (ARQ) is a specific protocol used in flow and error control. It combines the concepts of flow control with error detection and correction. Here's how it works:

### 1. Transmission Process:

- The sender transmits a data frame to the receiver.
- After sending the frame, the sender waits for an acknowledgment (ACK) from the receiver before sending the next frame.

### 2. Acknowledgment:

- The receiver checks the received frame for errors using a detection method (e.g., CRC).

- If the frame is received correctly, the receiver sends an ACK back to the sender.
- If an error is detected, the receiver sends a negative acknowledgment (NACK) or does not respond, prompting the sender to retransmit the same frame.

### 3. Efficiency:

- While the Stop-and-Wait ARQ is simple and easy to implement, it can be inefficient in high-latency environments due to the idle time spent waiting for ACKs.
- The protocol is best suited for low-speed networks or situations where reliability is crucial.

In summary, flow and error control are critical for ensuring reliable communication in data networks. The Stop-and-Wait ARQ method effectively manages data transmission by combining flow control with error detection and correction, although it may not be the most efficient approach in high-latency environments.

### Q4. Explain Sliding Window Protocol in detail?

Ans. The Sliding Window Protocol is an efficient flow control method used in the Data Link Layer of network communication. It allows for the transmission of multiple frames before requiring an acknowledgment (ACK) for the first frame, optimizing the use of available bandwidth and reducing idle time. Here's a detailed explanation of how the Sliding Window Protocol works:

#### Key Concepts

##### 1. Window Size:

- The window size determines how many frames can be sent before receiving an acknowledgment. This size can be fixed or variable, depending on the implementation.
- A sender can transmit a specified number of frames (the window size) without needing to wait for an acknowledgment for the first transmitted frame.

##### 2. Frames and Sequence Numbers:

- Each frame is assigned a unique sequence number to keep track of the order in which frames are sent and received.
- The sequence numbers help manage retransmissions in case of errors.

##### 3. Sender and Receiver Windows:

- **Sender Window:** Represents the range of sequence numbers that the sender is allowed to transmit without waiting for an acknowledgment. The sender can send frames within this window.
- **Receiver Window:** Indicates the range of sequence numbers that the receiver is expecting to receive in order. This helps the receiver identify out-of-order frames.

#### Working Mechanism

##### 1. Initialization:

- The sender initializes the window with a specified size (N), allowing N frames to be sent before requiring an acknowledgment.
- The sender keeps track of the sequence numbers of the frames being sent and the next expected ACK.

## 2. Frame Transmission:

- The sender can transmit all frames within the current window. Once the sender transmits a frame, it slides the window forward by one frame as it receives ACKs.
- The sender maintains a buffer of frames that have been sent but not yet acknowledged.

## 3. Acknowledgment:

- The receiver sends an ACK for the highest-sequence-numbered frame received in order. If all frames up to a certain number have been received, the receiver sends an ACK for that number.
- If the receiver detects an error in a frame, it may send a negative acknowledgment (NACK) for that specific frame, prompting the sender to retransmit it.

## 4. Sliding the Window:

- When the sender receives an ACK, it slides the window forward to allow the transmission of new frames. For example, if the sender's window size is 4 and it has transmitted frames 0, 1, 2, and 3, once it receives an ACK for frame 0, it can slide the window to transmit frame 4.
- If the receiver sends a NACK or does not send an ACK for an expected frame, the sender does not slide the window and retransmits the missing frame.

## Advantages

- **Increased Throughput:** By allowing multiple frames to be sent before requiring an acknowledgment, the Sliding Window Protocol effectively utilizes the available bandwidth and reduces idle time.
- **Flow Control:** The protocol manages the flow of frames based on the receiver's capacity, preventing buffer overflow.
- **Error Handling:** The use of sequence numbers and acknowledgments allows for effective error detection and retransmission.

## Types of Sliding Window Protocols

### 1. Go-Back-N ARQ:

- The sender can send multiple frames (up to the window size), but if an error occurs, all subsequent frames must be retransmitted, even if they were received correctly.

### 2. Selective Repeat ARQ:

- Similar to Go-Back-N, but the sender only retransmits the specific frames that were detected as erroneous, allowing for more efficient use of bandwidth.

## Summary

The Sliding Window Protocol is a robust and efficient method for managing data transmission in computer networks. By allowing multiple frames to be in transit at once and utilizing sequence numbers for error detection and acknowledgment, it enhances the reliability and efficiency of communication between devices. The protocol is widely used in various networking technologies, including TCP/IP, ensuring smooth data flow in both wired and wireless networks.

### Q5. What is Go-Back-N ARQ?

Ans. Go-Back-N ARQ (Automatic Repeat reQuest) is an error control protocol used in data communication for reliable transmission. It is a type of sliding window protocol that allows a sender to send multiple frames before needing an acknowledgment for the first frame sent. Here's a concise explanation of its key features and functioning:

#### Key Features

##### 1. Window Size (N):

- The sender can send up to N frames before waiting for an acknowledgment. The receiver can only receive frames in order.

##### 2. Sequence Numbers:

- Each frame is assigned a unique sequence number. The sequence numbers help in tracking the order of frames and managing retransmissions.

##### 3. Acknowledgment:

- The receiver sends an acknowledgment (ACK) for the highest-numbered frame that it has received in order. If a frame is missing or erroneous, the receiver does not acknowledge frames that follow the erroneous one.

#### Working Mechanism

##### 1. Frame Transmission:

- The sender transmits frames sequentially up to the window size. For example, if the window size is 4, frames 0, 1, 2, and 3 can be sent before requiring an ACK.

##### 2. Receiving ACK:

- When the receiver gets a frame correctly, it sends an ACK for the highest correctly received frame. For instance, if frames 0, 1, and 2 are received correctly, the receiver will send an ACK for frame 2.

##### 3. Handling Errors:

- If the receiver detects an error in a frame (e.g., frame 3 is lost or corrupted), it will not acknowledge frame 3 or any subsequent frames. Instead, the sender must go back and retransmit frame 3 and all subsequent frames (frames 4 and onwards) even if they were received correctly.

##### 4. Sliding the Window:

- Upon receiving an ACK, the sender slides the window forward, allowing it to send new frames. For example, if the sender receives an ACK for frame 2, it can send frame 4 next, keeping the window size intact.

#### Advantages

- **Simplicity:** Go-Back-N is straightforward to implement and understand.
- **Error Recovery:** It efficiently manages errors by allowing for quick retransmissions of lost frames.

## Disadvantages

- **Inefficiency with High Loss Rates:** If the error rate is high, a large number of frames may need to be retransmitted, which can lead to inefficiency.
- **Increased Latency:** Retransmitting all frames after an error can introduce delays, particularly in high-latency networks.

## Summary

Go-Back-N ARQ is a reliable data transmission protocol that balances the need for speed and reliability. It is commonly used in various networking applications where maintaining the order and integrity of transmitted data is crucial, such as in TCP/IP networks.

## Q6. Explain Selective Repeat ARQ?

Ans. Selective Repeat ARQ (Automatic Repeat reQuest) is an error control protocol used in data communication that allows a sender to retransmit only the frames that were lost or corrupted, rather than all frames following an error. This protocol enhances efficiency and reduces unnecessary retransmissions compared to the Go-Back-N ARQ protocol. Here's a detailed overview:

### Key Features

#### 1. Window Size (N):

- Like Go-Back-N, Selective Repeat uses a sliding window mechanism where the sender can send multiple frames before requiring an acknowledgment. The window size is defined by N, determining how many frames can be in transit without acknowledgment.

#### 2. Sequence Numbers:

- Each frame is assigned a unique sequence number. This allows both the sender and receiver to keep track of which frames have been transmitted and acknowledged.

#### 3. Acknowledgment:

- The receiver sends individual acknowledgments (ACKs) for each correctly received frame. If a frame is received with errors or is missing, the receiver will send a negative acknowledgment (NAK) for that specific frame.

### Working Mechanism

#### 1. Frame Transmission:

- The sender transmits frames up to the window size. For instance, if the window size is 4, the sender can send frames 0, 1, 2, and 3.

#### 2. Receiving ACKs:

- The receiver acknowledges each correctly received frame. For example, if frames 0 and 1 are received correctly, the receiver sends ACKs for both frames.

#### 3. Handling Errors:

- If a frame is lost or corrupted (e.g., frame 2), the receiver sends a NAK for that specific frame. The sender only retransmits frame 2 instead of all subsequent frames.

#### 4. Sliding the Window:

- Upon receiving ACKs, the sender can slide the window forward to send new frames. If frame 2 is retransmitted and received correctly, the sender can then proceed to send frames 4 and onwards.

### Advantages

- **Efficiency:** Selective Repeat is more efficient than Go-Back-N because it reduces the number of retransmissions by only resending erroneous or lost frames.
- **Reduced Latency:** By avoiding unnecessary retransmissions, Selective Repeat can achieve lower latency, especially in networks with higher error rates.

### Disadvantages

- **Complexity:** Selective Repeat is more complex to implement than Go-Back-N due to the need for maintaining multiple buffers for received frames and the management of individual ACKs and NAKs.
- **Buffering Requirements:** The receiver needs to have sufficient buffering to hold out-of-order frames until the missing frames are received.

### Summary

Selective Repeat ARQ is a reliable data transmission protocol that optimizes the error recovery process by only retransmitting the affected frames, making it suitable for high-speed networks where minimizing delays and maximizing efficiency are essential. It is widely used in various communication systems, including wireless and data link layer protocols.

### Q7. What is HDLC?

Ans. HDLC (High-Level Data Link Control) is a bit-oriented synchronous data link layer protocol used for transmitting data over point-to-point and multipoint links. It was developed by the International Organization for Standardization (ISO) and is widely used in various communication systems. Here's an overview of HDLC:

#### Key Features

##### 1. Framing:

- HDLC uses a specific frame structure to encapsulate data. Each frame begins and ends with a unique flag sequence (01111110), which allows the receiver to identify the start and end of the frame.

##### 2. Frame Types:

- HDLC defines three types of frames:
  - **Information Frame (I-frame):** Carries user data and control information. It is used for the transfer of data between devices.
  - **Supervisory Frame (S-frame):** Provides control information to manage the flow of data (e.g., acknowledgments, requests for retransmission).
  - **Unnumbered Frame (U-frame):** Used for various control functions such as connection establishment and termination.

##### 3. Addressing:



- Each HDLC frame can include an address field to identify the sender and receiver, allowing communication between multiple devices on the same link.

#### 4. Error Control:

- HDLC employs mechanisms for error detection using a Frame Check Sequence (FCS), typically based on a cyclic redundancy check (CRC). If an error is detected, the receiver can request retransmission of the affected frame.

#### 5. Flow Control:

- HDLC supports flow control to manage data transmission rates between sender and receiver, ensuring that the sender does not overwhelm the receiver with too much data.

### Operation

- **Synchronous Transmission:** HDLC operates synchronously, meaning both the sender and receiver are synchronized to a common clock.
- **Bit-Oriented:** It is a bit-oriented protocol, meaning it processes data as a stream of bits rather than bytes, allowing it to manage various data sizes efficiently.

### Applications

- HDLC is commonly used in telecommunications, including point-to-point links, leased lines, and satellite communication. It serves as a foundation for several higher-level protocols, such as Frame Relay and X.25.

### Summary

HDLC is a robust and versatile data link layer protocol designed for reliable communication over various network types. Its features, including framing, error control, and flow control, make it suitable for both point-to-point and multipoint configurations in diverse communication environments.

### Q8. Elaborate Point-to-Point Access: PPP Point-to-Point Protocol, PPP Stack.

Ans. Point-to-Point Protocol (PPP) is a widely used data link layer protocol that facilitates direct communication between two network nodes, typically over serial links. It is commonly used for establishing internet connections via dial-up modems, DSL, and other types of point-to-point communications. Here's an elaboration on PPP and its stack:

#### Key Features of PPP

##### 1. Encapsulation:

- PPP encapsulates network layer packets (such as IP packets) within its frames, allowing different types of protocols to be transmitted over the same physical link.

##### 2. Link Quality Monitoring:

- PPP includes mechanisms for monitoring the quality of the link, allowing it to detect issues like link failures and initiate recovery processes.

##### 3. Authentication:

- PPP supports multiple authentication methods, including Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP), to verify the identity of the connecting device.

#### 4. Multilink Support:

- PPP can aggregate multiple physical connections into a single logical connection using Multilink PPP (MLPPP), enhancing bandwidth and redundancy.

#### 5. Network Layer Protocol Support:

- PPP can carry multiple network layer protocols by using a Protocol field in its frame header, allowing interoperability with various networking technologies.

### PPP Frame Structure

A typical PPP frame consists of the following fields:

- **Flag:** A single byte marking the start and end of the frame (0x7E).
- **Address:** Usually set to a broadcast address (0xFF) in point-to-point links.
- **Control:** Generally set to 0x03, indicating unnumbered information frames.
- **Protocol:** Specifies the encapsulated protocol (e.g., 0x0021 for IP).
- **Information:** Contains the encapsulated data payload.
- **FCS (Frame Check Sequence):** A sequence used for error detection, typically a CRC.

### PPP Stack

PPP operates on a layered architecture, allowing it to interact with various network protocols. The key components of the PPP stack include:

#### 1. Physical Layer:

- The physical medium over which the PPP frames are transmitted (e.g., serial links, ISDN, etc.).

#### 2. Data Link Layer (PPP):

- Implements the PPP protocol itself, handling framing, error detection, link quality monitoring, and authentication.

#### 3. Network Layer:

- Carries the actual network layer protocols, such as IP, IPv6, IPX, and AppleTalk, encapsulated within PPP frames. PPP provides a flexible mechanism to support various protocols without changing its core functionality.

#### 4. Control Protocols:

- PPP uses several control protocols to negotiate the link parameters and establish the connection:
  - **LCP (Link Control Protocol):** Used for establishing, configuring, and testing the data link connection.
  - **NCP (Network Control Protocol):** Used for establishing and configuring the network layer protocols. Different NCPs exist for different protocols, such as IPCP (Internet Protocol Control Protocol) for IP.

## Conclusion

PPP is a versatile and robust protocol for point-to-point communications, offering encapsulation, authentication, and link quality monitoring. Its layered architecture and support for multiple network layer protocols make it suitable for various networking applications, providing reliable connections for both dial-up and dedicated links.

### Q9. Explain the function and requirements of DLL protocols.

Ans. **Explain the function and requirements of DLL protocols.**

Ans. Data Link Layer (DLL) protocols ensure reliable and error-free communication between two directly connected nodes in a network. Their main functions include:

1. **Framing:** Dividing data into manageable frames for transmission.
2. **Error Control:** Detecting and correcting errors in the frames.
3. **Flow Control:** Ensuring the sender doesn't overwhelm the receiver with too much data.
4. **Addressing:** Identifying source and destination MAC addresses.
5. **Synchronization:** Ensuring both devices are ready for data transmission.

Requirements include reliable error detection, acknowledgment mechanisms, and efficient data transmission without loss or duplication.\

### Q10. In sliding window protocol, can the sender receive an ACK for a packet that falls outside its current window? If yes, specify the scenario under which this occurs as well.

Yes, in the sliding window protocol, the sender can receive an ACK for a packet that falls outside its current window. This happens when the receiver sends a cumulative acknowledgment, acknowledging all packets up to a certain point. If the sender has moved its window forward after receiving earlier ACKs, it may receive an ACK for a packet that is no longer in its current window. The scenario occurs when the window slides, and the ACK refers to a previously transmitted packet that was within the window before it shifted.

---

### Q11. In stop and wait ARQ, what happens if a negative acknowledgement is lost in transit?

In stop-and-wait ARQ, if a negative acknowledgment (NAK) is lost, the sender will not receive it and will continue waiting for an acknowledgment. The sender has a timeout mechanism that triggers retransmission if no ACK or NAK is received within a certain time frame. If the NAK is lost, the sender will eventually time out and resend the packet, ensuring reliable data transmission even if the negative acknowledgment fails to reach the sender.

---

### Q12. What is CSMA? How is p-persistent CSMA different from non-persistent?

**CSMA (Carrier Sense Multiple Access)** is a network protocol where a device checks the network to determine whether the communication channel is clear before attempting to transmit data. CSMA helps reduce collisions by ensuring that devices only transmit when the channel is idle.

- **p-persistent CSMA:** In this method, when a device senses that the channel is idle, it transmits with a probability  $p$ . If it does not transmit, it waits for the next time slot and tries again with the same probability. This approach allows for better control of collision probability.

- **Non-persistent CSMA:** In non-persistent CSMA, when a device finds the channel busy, it waits for a random amount of time before checking the channel again. If the channel is free, it transmits immediately. This reduces collisions, but can lead to longer delays compared to p-persistent CSMA.
- 

#### Q13. How is selective repeat better than Go-Back-N?

Selective Repeat is better than Go-Back-N in several ways, particularly in terms of efficiency. In Go-Back-N, if an error occurs in one frame, the sender must retransmit all frames starting from the erroneous frame, even if subsequent frames were received correctly. This can lead to a lot of unnecessary retransmissions.

In contrast, **Selective Repeat** only retransmits the specific frames that were lost or erroneous. The receiver keeps track of each frame individually and can acknowledge non-erroneous frames even if they arrive out of order. This reduces the number of retransmissions, improving bandwidth utilization and overall throughput. However, Selective Repeat requires more buffer space and more complex logic compared to Go-Back-N.

---

#### Q14. Compare the throughput of a pure ALOHA network with a slotted ALOHA network.

- **Pure ALOHA:** In pure ALOHA, stations can transmit data whenever they have data to send, without waiting for a specific time slot. However, if two stations transmit at the same time, their packets collide, leading to a loss of both packets. The maximum throughput of pure ALOHA is **18.4%** of the total available bandwidth. This low efficiency is due to the high likelihood of collisions, as packets can be sent at any time.
- **Slotted ALOHA:** In slotted ALOHA, time is divided into discrete slots, and stations are only allowed to send data at the beginning of these time slots. This reduces the chances of collisions since stations are synchronized to transmit at specific intervals. The maximum throughput of slotted ALOHA is **36.8%**, which is significantly better than pure ALOHA due to the reduction in collision probability.

The higher efficiency of slotted ALOHA comes from the fact that it organizes transmissions into slots, minimizing the chances that two stations will collide by starting transmission simultaneously.

# Medium Access Control Sublayer (MAC sublayer)

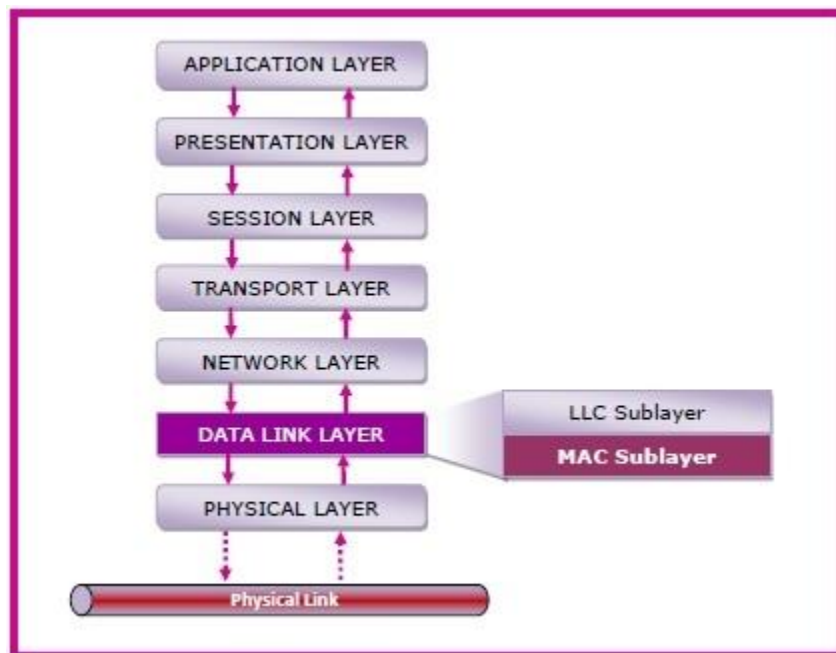
The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. 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.

## What is MAC Address?

- MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address**. It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.
- It stands for **Media Access Control**, and also known as **Physical address, hardware address, or BIA (Burned In Address)**.
- It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as **00:0a:95:9d:67:16**.

- It is 12-digit, and 48 bits long, out of which the first 24 *bits are used for **OUI**(Organization Unique Identifier)*, and 24 *bits are for NIC/vendor-specific*.
- It works on the data link layer of the OSI model.
- It is provided by the device's vendor at the time of manufacturing and embedded in its NIC, which is ideally cannot be changed.
- The **ARP protocol** is used to associate a logical address with a physical or MAC address.

## Reason to have both IP and MAC addresses.

As we already had the **IP** address to communicate a computer to the internet, why we need the **MAC** address. The answer to this question is that every mac address is assigned to the **NIC** of a hardware device that helps to identify a device over a network.

When we request a page to load on the internet, the request is responded and sent to our **IP** address.

Both MAC and IP addresses are operated on different layers of the internet protocol suite. The MAC address works on layer 2 and helps identify the devices within the same broadcast network (such as the router). On the other hand, the IP addresses are used on layer 3 and help identify the devices on different networks.

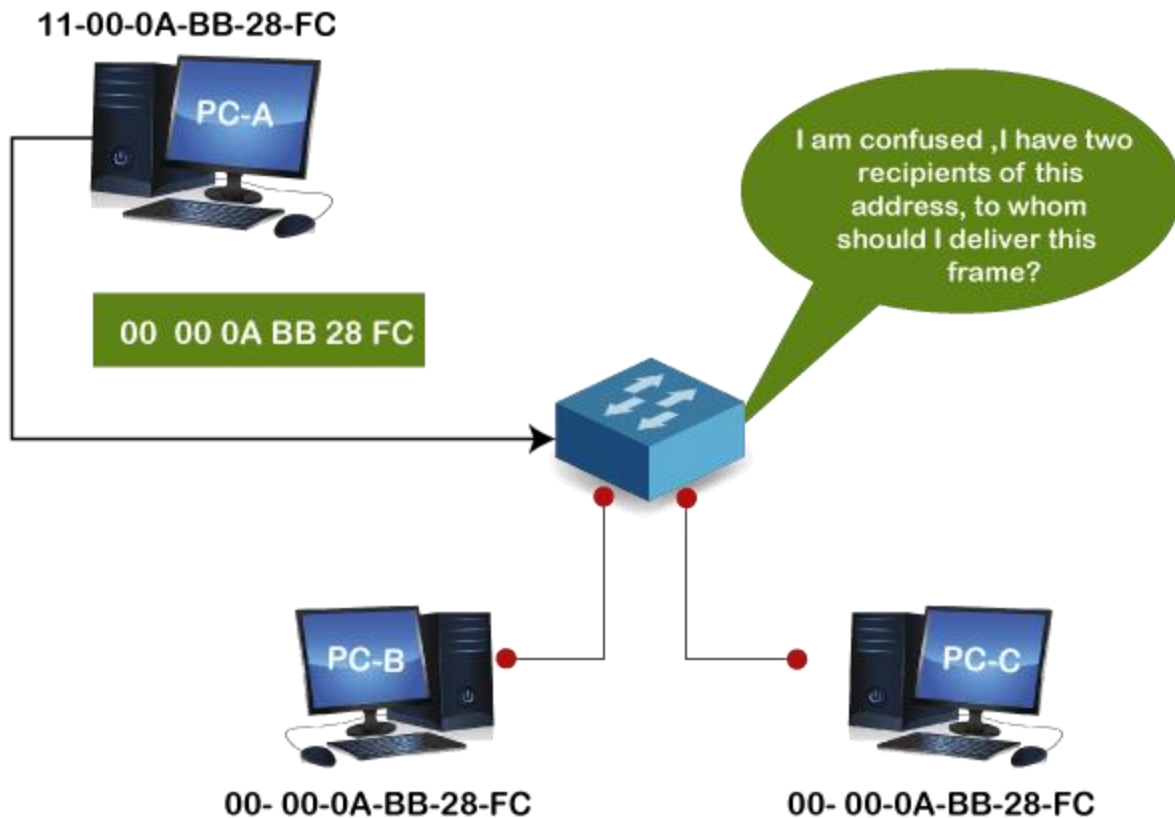
We have the IP address to identify the device through different networks, we still need a MAC address to find the devices on the same network.

## Why should the MAC address be unique in the LAN network?

If a **LAN** network has two or more devices with the same MAC address, that network will not work.

Suppose three devices A, B, and C are connected to a network through a switch. The MAC addresses of these devices are 11000ABB28FC, 00000ABB28FC, and 00000ABB28FC, respectively. The **NIC** of devices B and C have the same MAC address. If device A sends a data frame to the address 00000ABB28FC, the switch will fail to deliver this frame to the destination, as it has two recipients of this data frame.

We can understand this example with the below image:

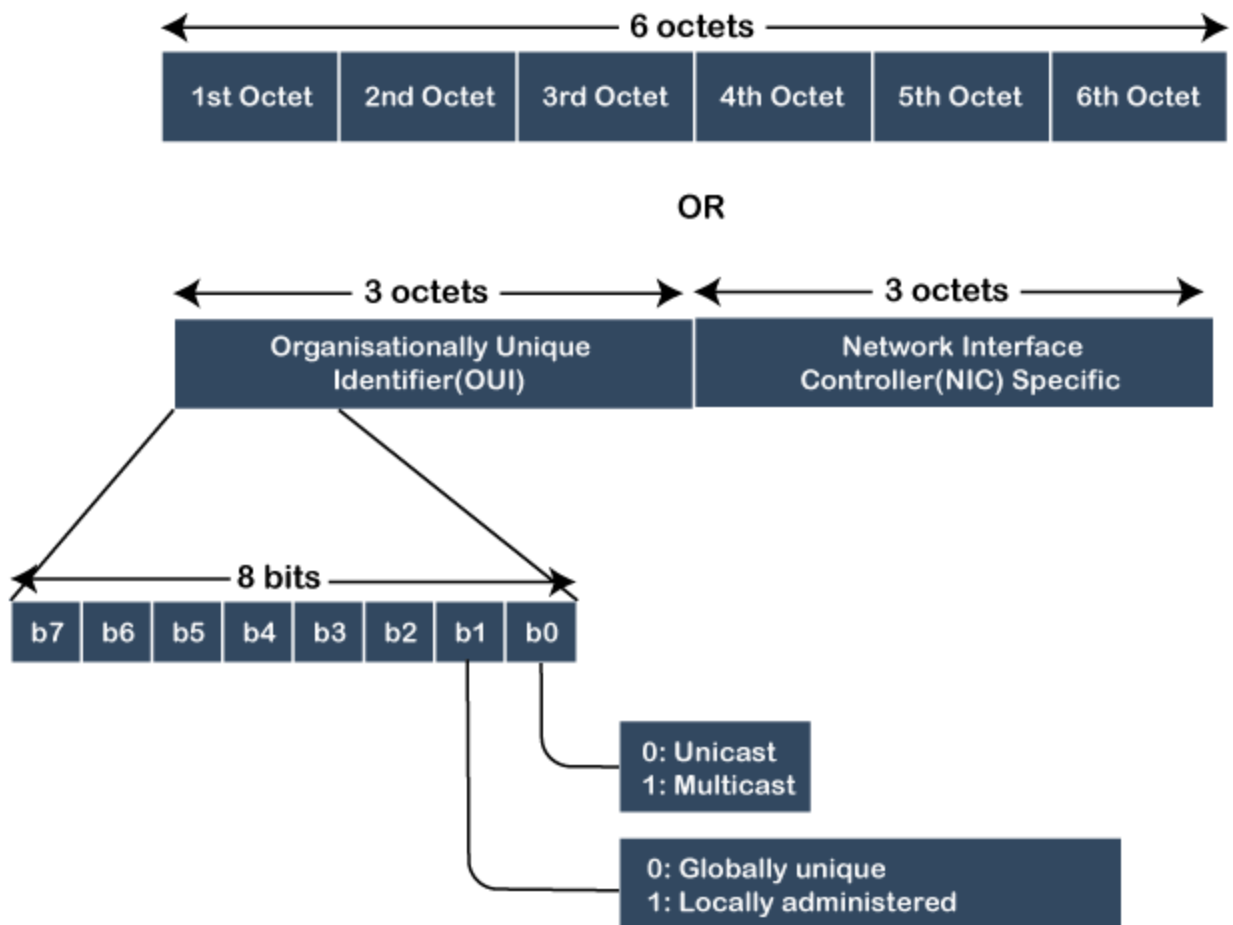


## Format of MAC address

As we have already discussed in the above section, we cannot assign the MAC address to the device's NIC; it is preconfigured by the manufacturers. So, let's understand how it is configured and what format is selected.

- It is 12 digits or 6-byte hexadecimal number, which is represented in colon-hexadecimal notation format. It is divided into six octets, and each octet contains 8 bits.
- The first three octets are used as the **OUI or Organisationally Unique Identifier**. These MAC prefixes are assigned to each organization or vendor by the IEEE Registration Authority Committee.
- Some example of OUI of known vendors are:
  - CC:46:D6 - Cisco**
  - 3C:5A:B4 - Google, Inc.**
  - 3C:D9:2B - Hewlett Packard**
  - 00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD**





- The last three octets are NIC specific and used by the manufacturer to each NIC card. Vendors or manufacturers can use any sequence of digits to the NIC specific digits, but the prefix should be the same as provided by the IEEE.

- The MAC address can be represented in below three formats:

Hyphen-Hexadecimal notation

00-0b-56-b1-c0-6e

Colon-Hexadecimal notation

00:0b:56:b1:c0:6e

Period-separated hexadecimal notation

000.b56.b1c.06e

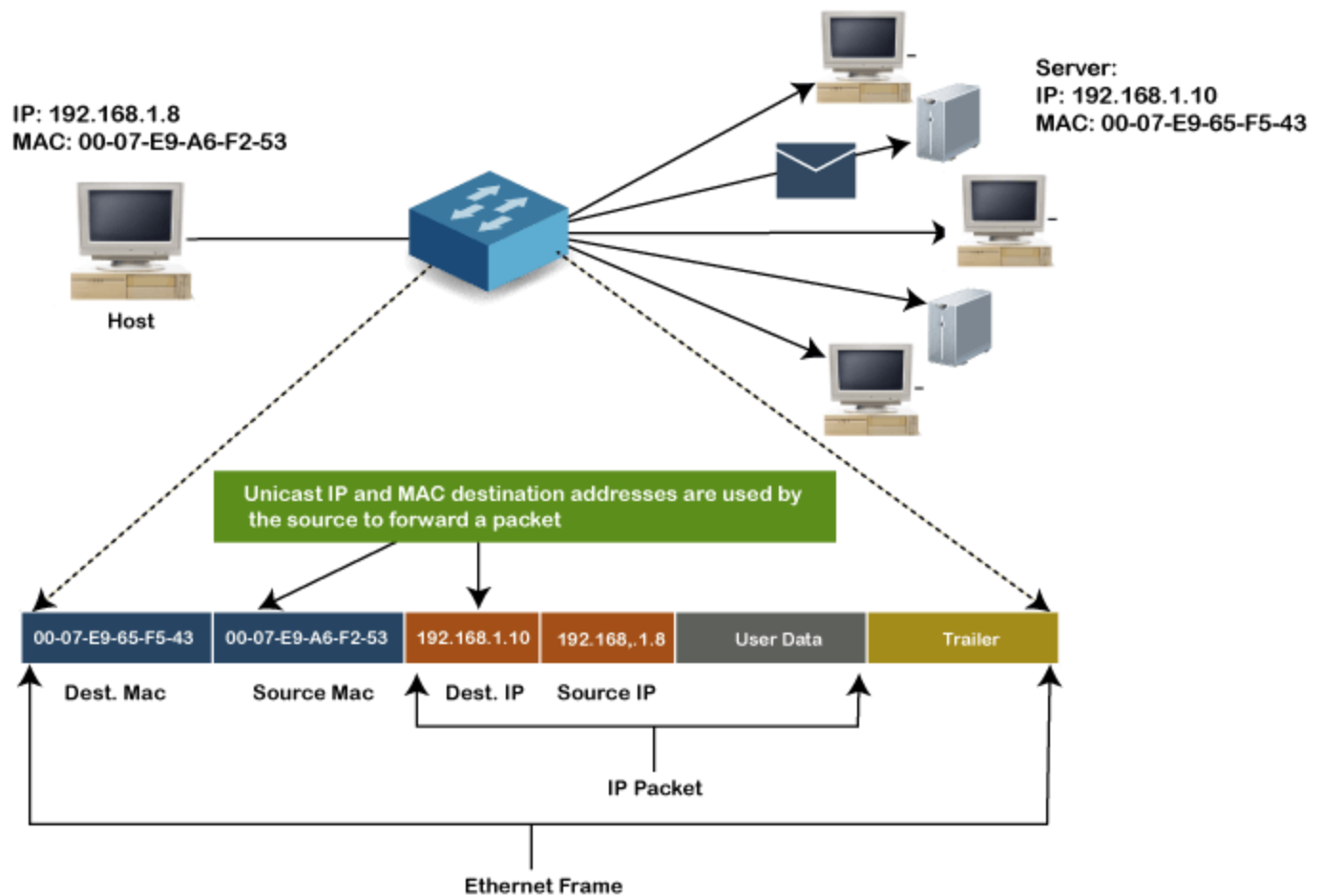
## Types of MAC address

There are three types of MAC addresses, which are:

1. **Unicast MAC Address**
2. **Multicast MAC address**
3. **Broadcast MAC address**

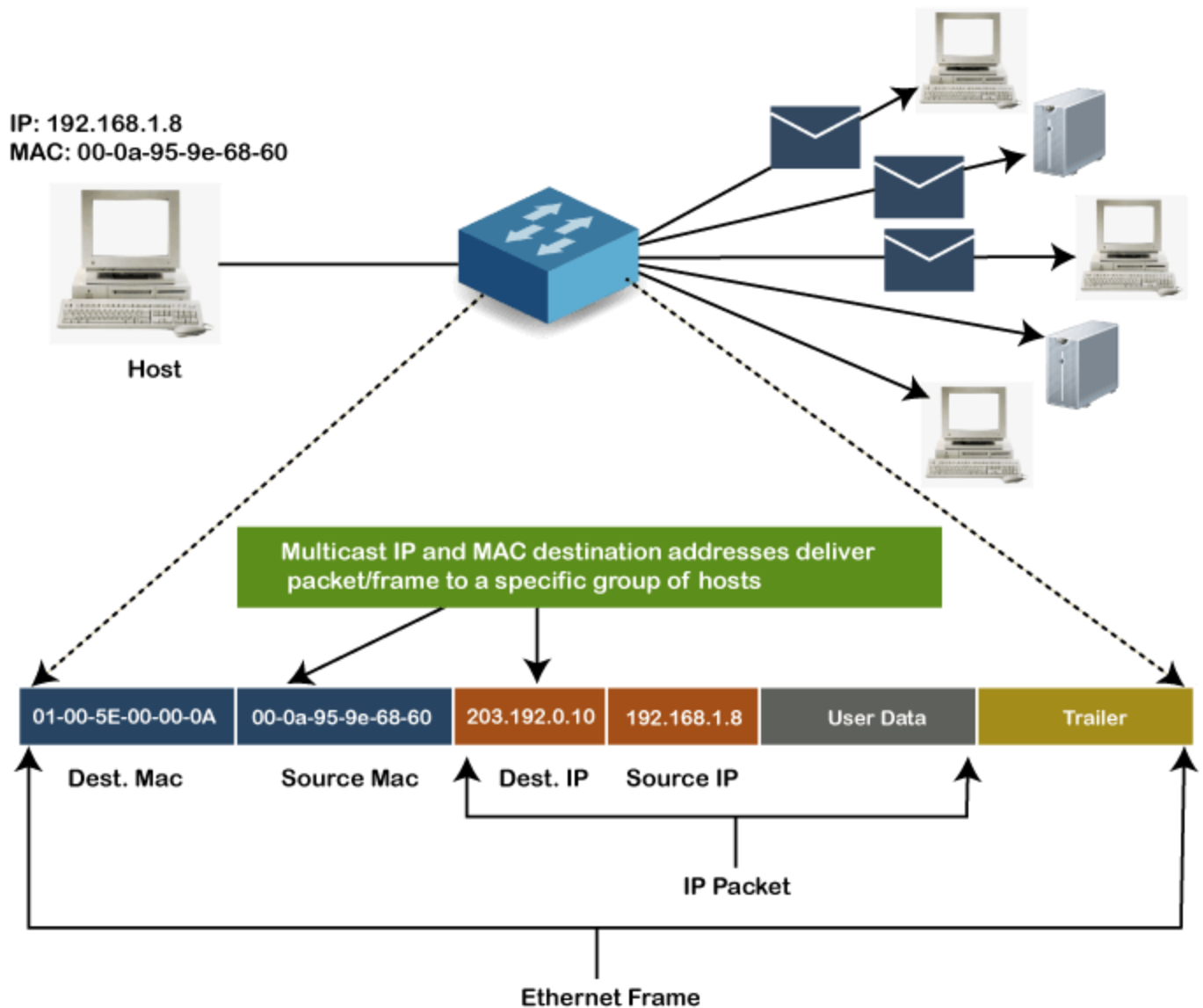
### Unicast MAC address:

The Unicast MAC address represents the specific NIC on the network. A Unicast MAC address frame is only sent out to the interface which is assigned to a specific NIC and hence transmitted to the single destination device. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one destination NIC.



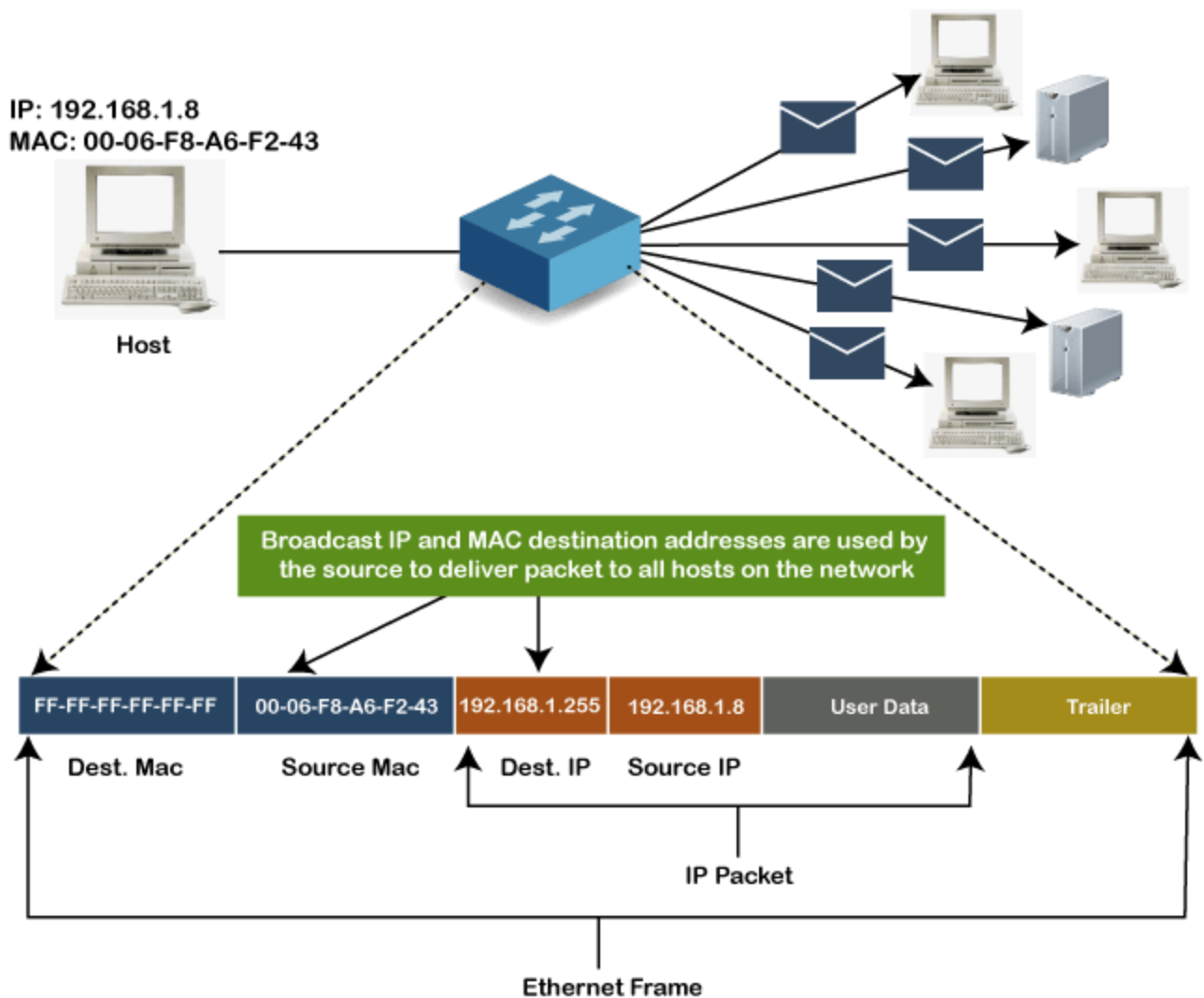
## Multicast MAC Address:

Multicast addresses enable the source device to transmit a data frame to multiple devices or NICs. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) or first 3 bytes of the first octet of an address is set to one and reserved for the multicast addresses. The rest 24 bits are used by the device that wants to send the data in a group. The multicast address always starts with the prefix 01-00-5E.



## Broadcast MAC address

It represents all devices within a Network. In broadcast MAC address, Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are known as a **broadcast address**. All these bits are the reserved addresses for the broadcast. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belong to that LAN segment. Hence if a source device wants to send the data to all the devices within a network, that can use the broadcast address as the destination MAC address.



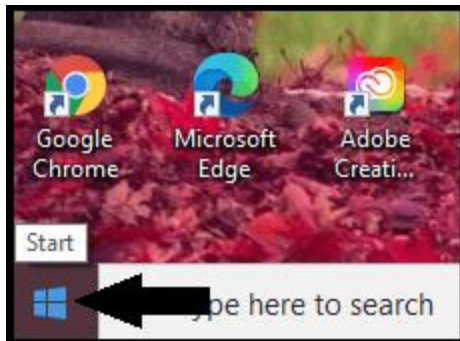
## How to find the MAC address of a device

We can easily find or check the address of our computer device with any operating device. Every device connected to the home network contains a unique MAC address, but if your system has multiple network adapters, such as an Ethernet adapter or wireless adapter, each adapter or NIC has its own MAC address or physical address.

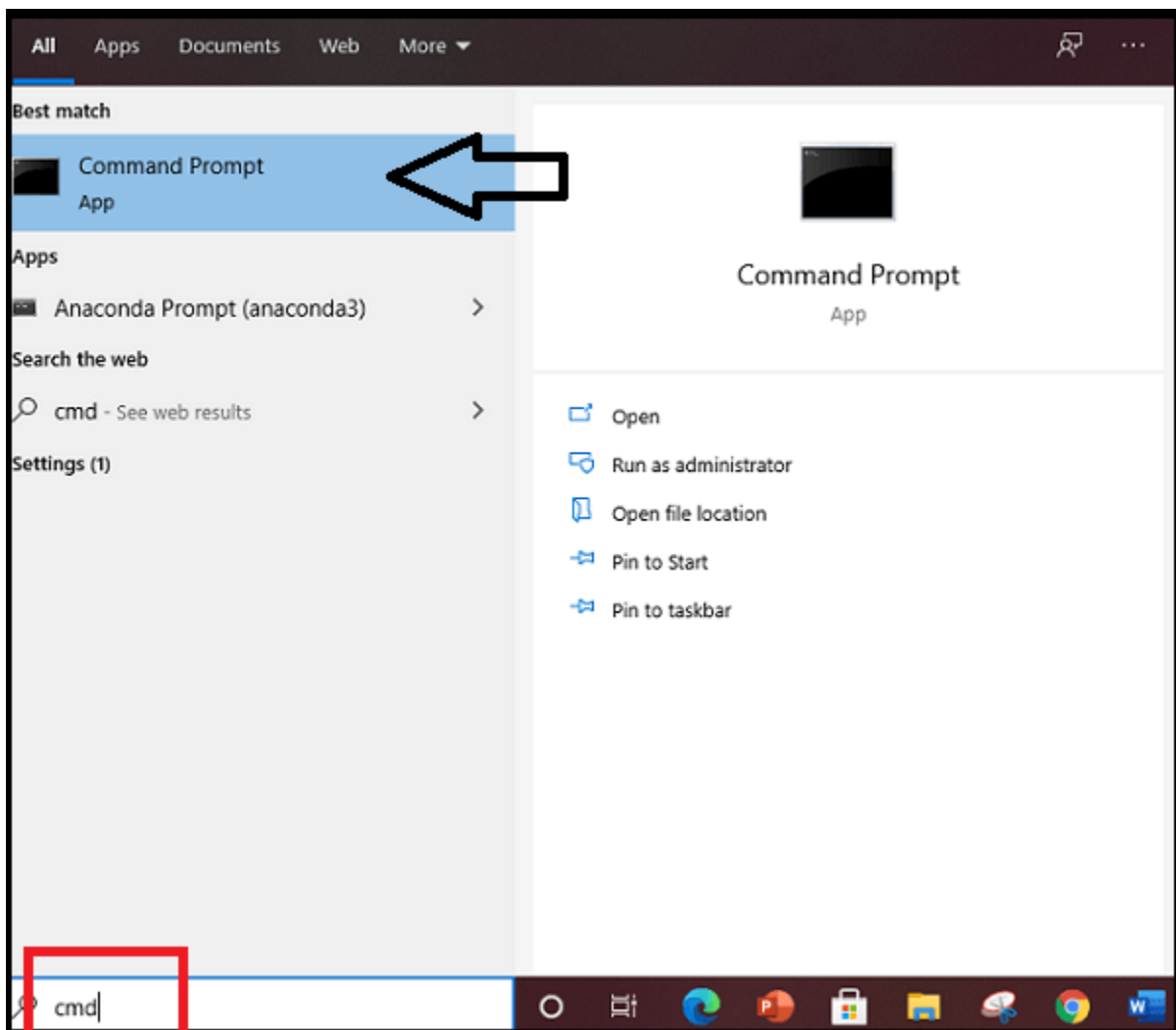
Follow the below steps to [find the MAC addresses](#) of a device on a different OS.

### MAC address on Windows:

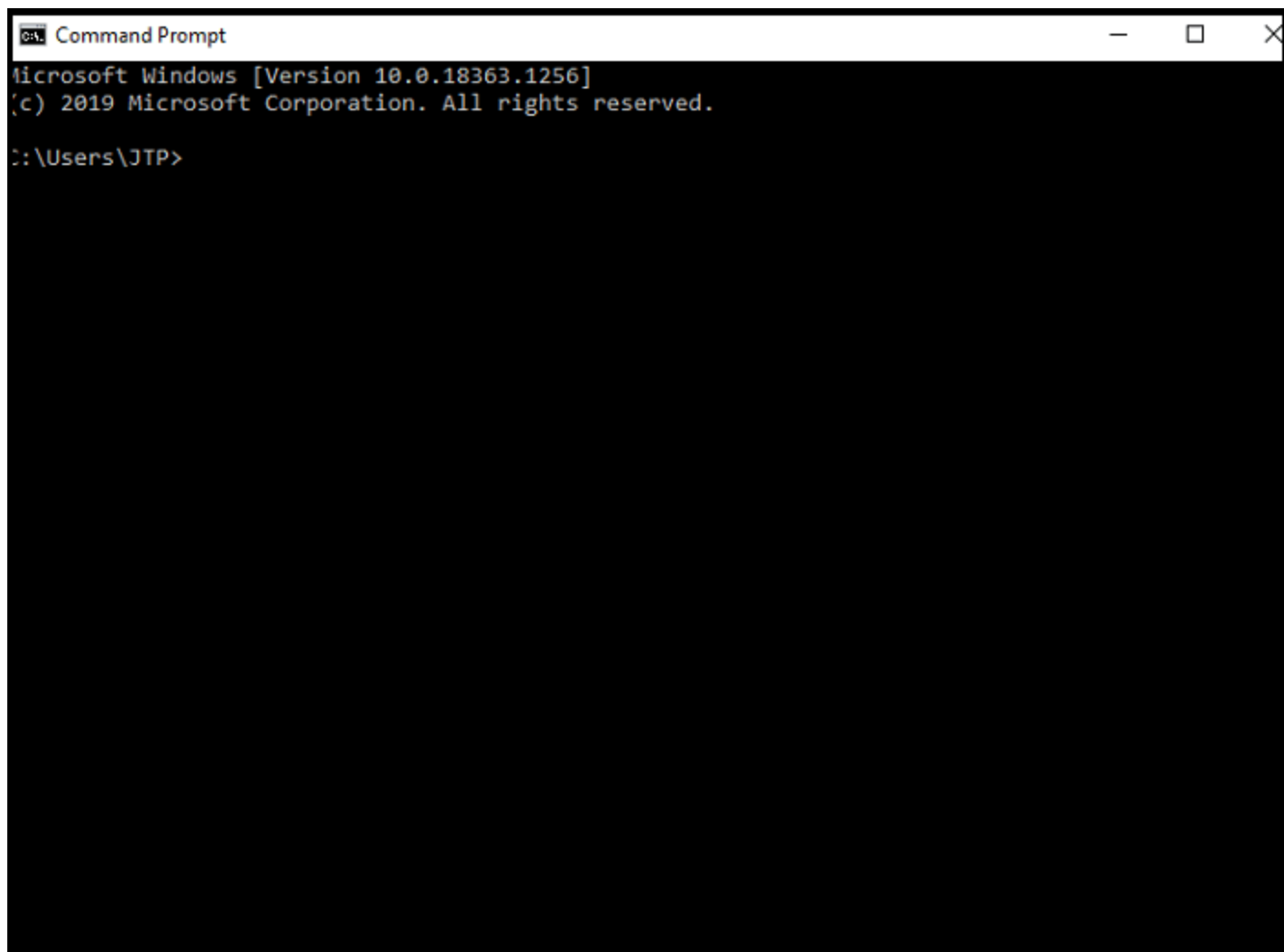
1. Click **Window Start** or Press the Windows Key.



2. In the given search box, type **cmd** to open the command prompt.



3. Press the Enter key, and the command prompt window will display, as shown below image:



```
Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\JTP>
```

4. Type ipconfig/all command and press enter.
5. It will show different information, scroll down and look for the physical address. Each physical address is the MAC address of your device.

```
Select Command Prompt
Microsoft Windows [Version 10.0.18363.1256]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\JTP>ipconfig/all

Windows IP Configuration

Host Name . . . . . : DESKTOP-KQ3AJLF
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : C4-65-16-E8-E5-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4c03:d594:5ea3:56d5%20(Preferred)
IPv4 Address. . . . . : 192.168.13.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

As we can see in the above image, there are two physical addresses shown with different values, one is for the Ethernet adapter, and the other one is for the VMware network adapter.

## MAC address on Macintosh OS:

Follow the below steps to find the MAC address on the Macintosh OS:

1. Select the Apple icon or open the Apple Menu, and click on System Preferences.
2. Under system preferences → Select Network →
3. The above path will open a network box.
4. Select the Wi-Fi option from here. It will show the Wi-Fi address or Airport Address displays; it is the MAC address of your device.



## Cloning of MAC address

MAC cloning is a way to fix the connectivity issues of the device with ISP. In this method, we need to set the MAC address of a device WAN port to be the similar MAC address of your PC or another device.

The connectivity issue arises mainly when we add new MAC address to a network, and this issue can be fixed with the help of MAC cloning.

For example, Some ISPs use the MAC address of your device when the service is installed. Now, if we place a router behind the cable modem or DSL modem, the ISP will not recognize the MAC address from the device's WAN port. For such a case, either you can call to ISP provider to register the MAC of your device, or you can clone the MAC address of the WAN port to the same as the computer MAC address.

## Difference between MAC address and IP address

Both the MAC address and IP address are the way to identify the device on the network. Following are some important differences between both:

MAC address	IP address
It stands for Media Access Control.	It stands for Internet Protocol.
It is the unique address provided by the manufacturer.	It is the logical address provided by the ISP or Internet Service Provider.
It is the physical address of the device's NIC that is used to identify a device within a network.	It is the logical address that identifies a network or device on the internet.
It operates on the data link layer.	It operates on a network Layer.
It is the 6 -bytes hexadecimal address.	It is of 4 bytes for IPv4 and 8 bytes for IPv6 addresses.

# Controlled Access Protocols

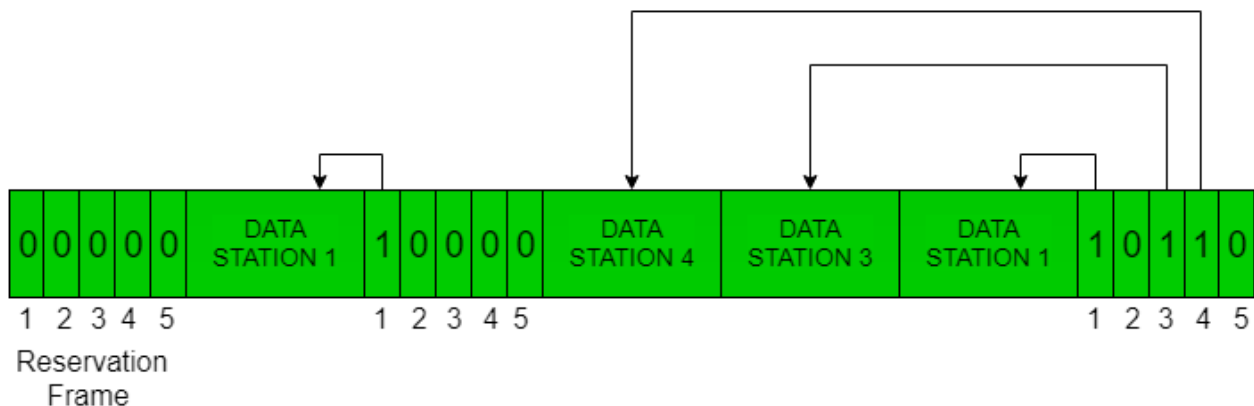
In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

1. Reservation
2. Polling
3. Token Passing

## Reservation

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

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



### Advantages of Reservation:

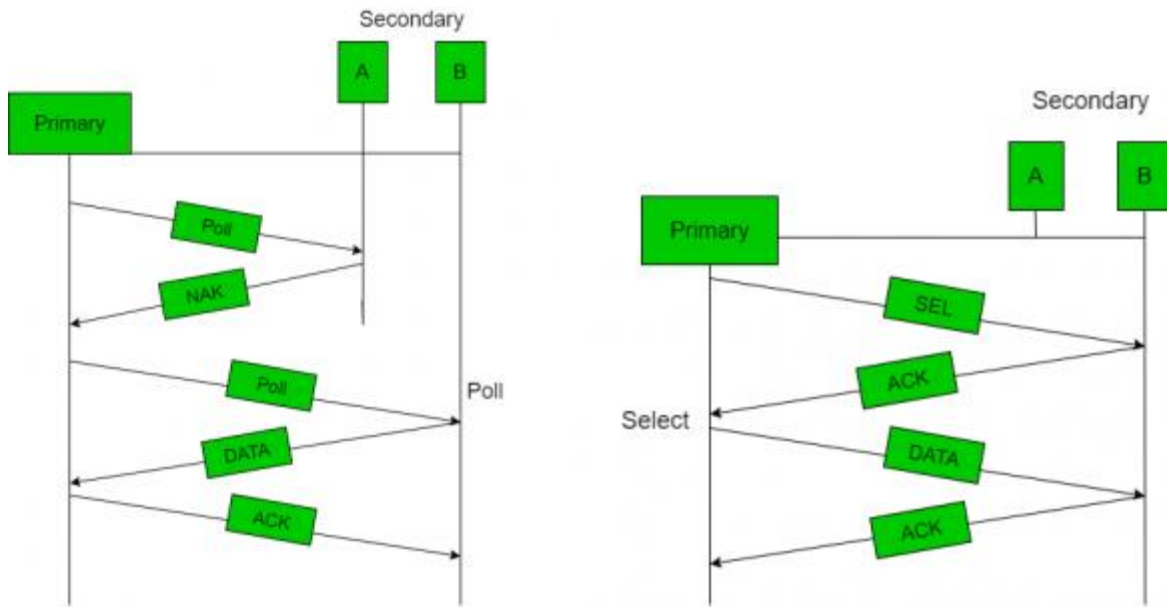
- The main advantage of reservation is *high rates and low rates of data accessing* time of the respective channel can be predicated easily. Here time and rates are fixed.
- Priorities can be set to provide speedier access from secondary.
- Predictable network performance: Reservation-based access methods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

### Disadvantages of Reservation:

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

## Polling

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



### Advantages of Polling:

- The maximum and minimum access time and data rates on the channel are fixed predictable.
- It has maximum *efficiency*.
- It has maximum *bandwidth*.
- No slot is wasted in polling.
- There is assignment of priority to ensure faster access from some secondary.

### Disadvantages of Polling:

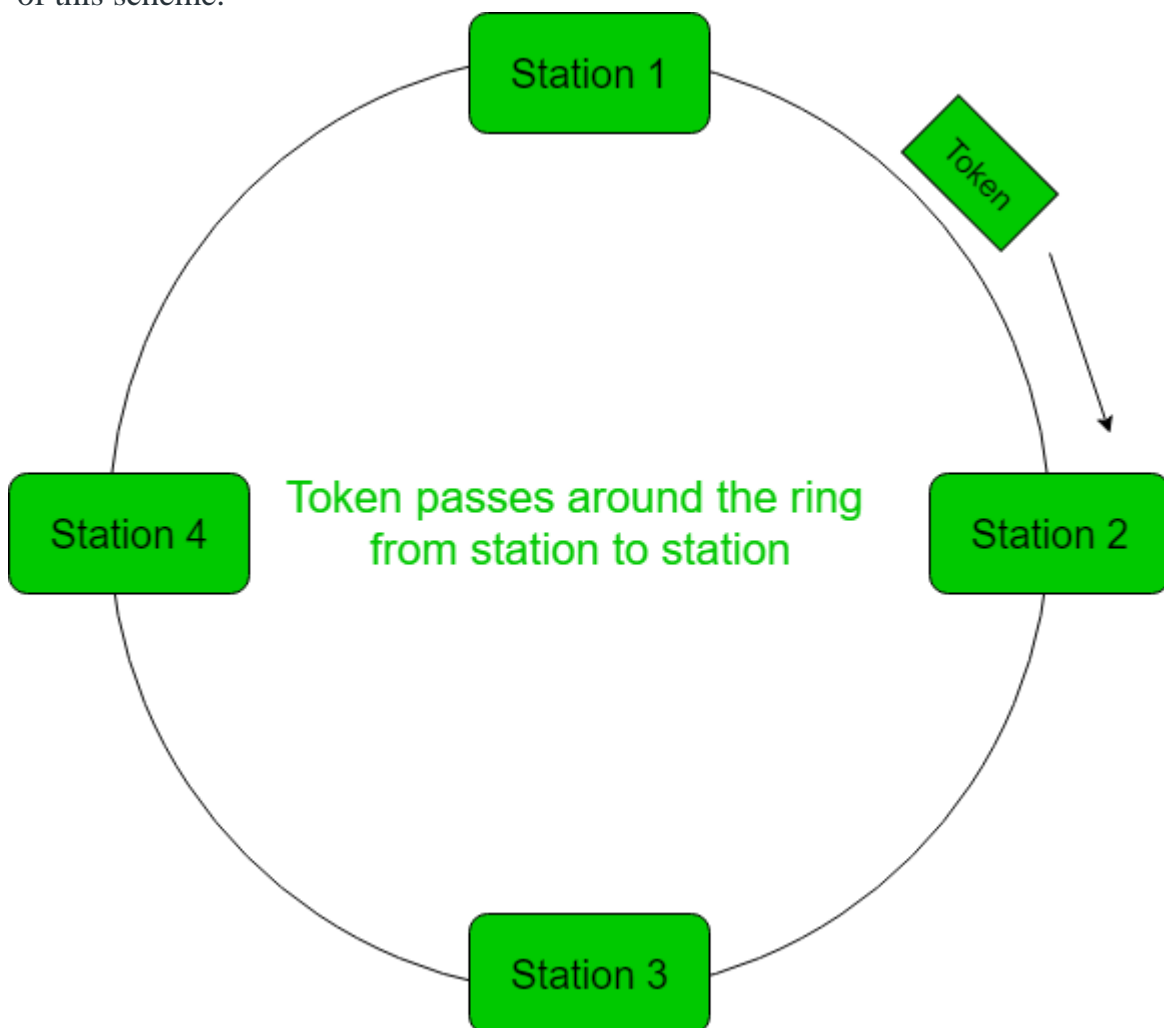
- It consume *more time*.
- Since every station has an equal chance of winning in every round, link sharing is *biased*.
- Only some station might run out of data to send.
- An increase in the turnaround time leads to a drop in the data rates of the channel under low loads.

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

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

## Token Passing

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



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

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

2. **Throughput**, which is a measure of successful traffic.

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

and

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

where  $N$  = number of stations

$a = T_p/T_t$

( $T_p$  = propagation delay and  $T_t$  = transmission delay)

### **Advantages of Token passing:**

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

### **Disadvantages of Token passing:**

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

# Multiple access protocol- ALOHA, CSMA, CSMA/CA and CSMA/CD

## Data Link Layer

The [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](#) or the multiple access resolutions.

## Data Link Control

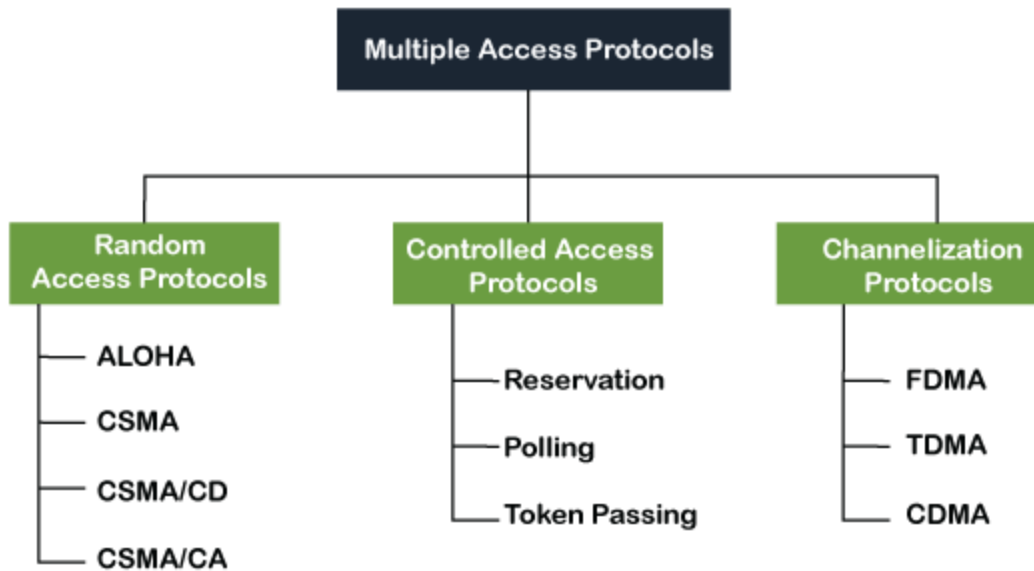
A [data link control](#) is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

## 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:



## 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

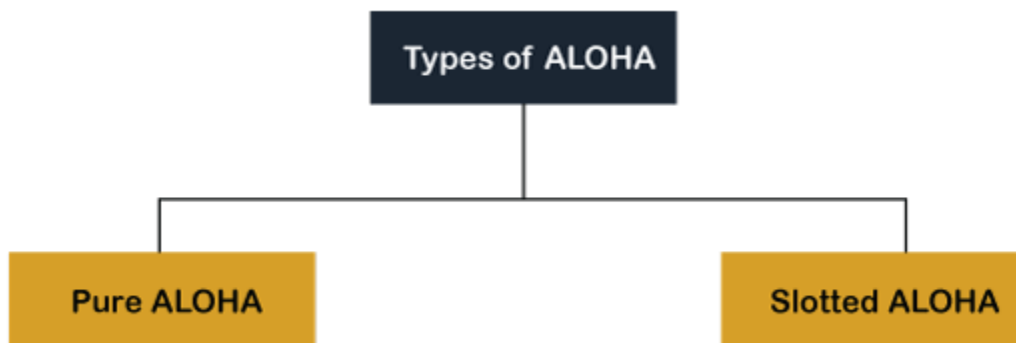
### ALOHA Random Access Protocol

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



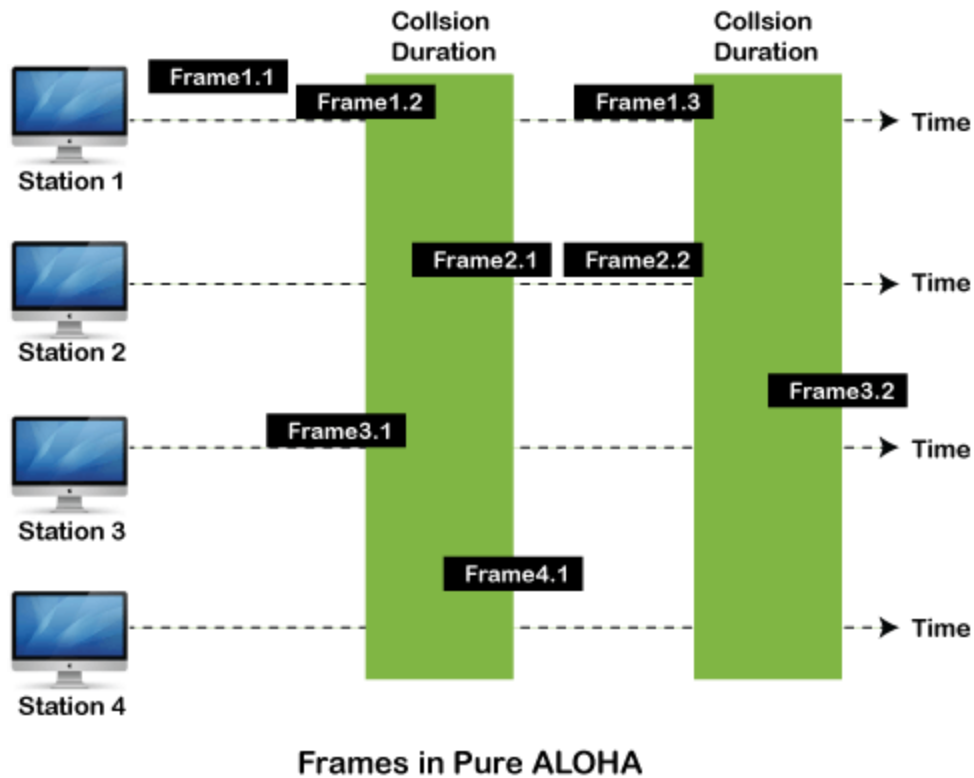
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires 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  $S = G * e^{-2G}$ .



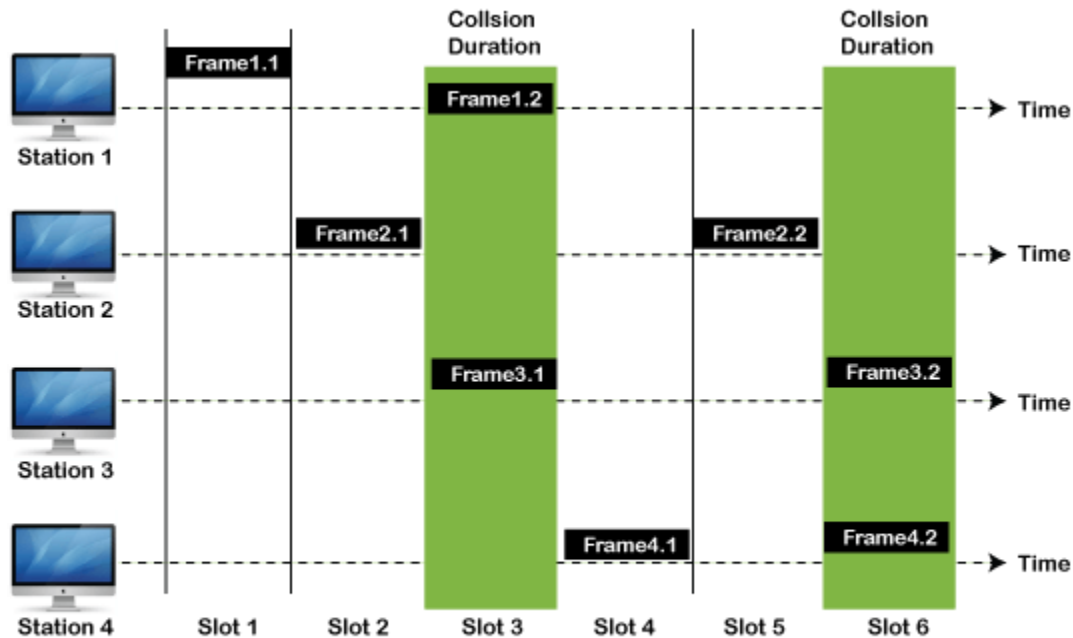
As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same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



Frames in Slotted ALOHA

## 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.

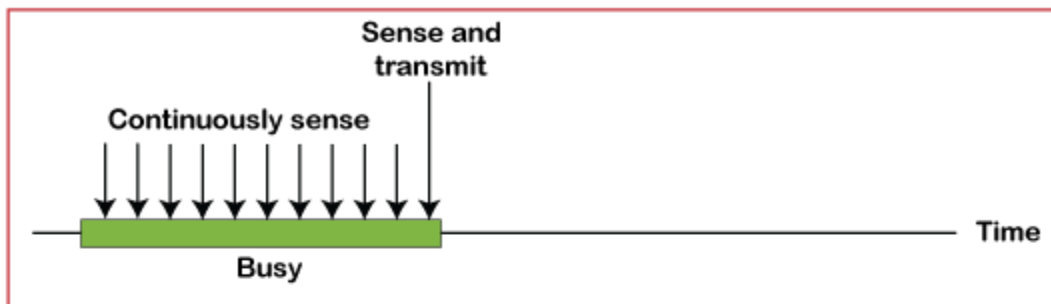
### CSMA Access Modes

**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.

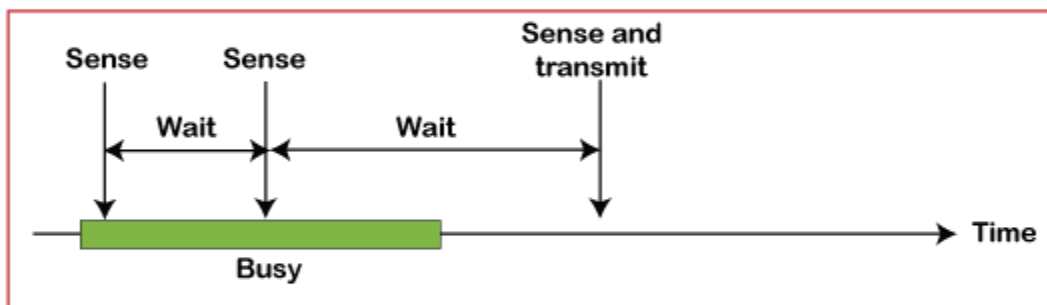
**Non-Persistent:** It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, 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.

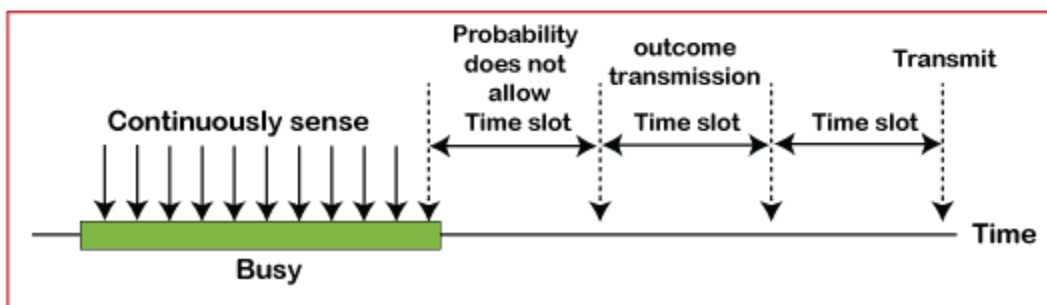
**O- Persistent:** It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



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.

## B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation**, **Polling**, and **Token Passing**.

## C. Channelization Protocols

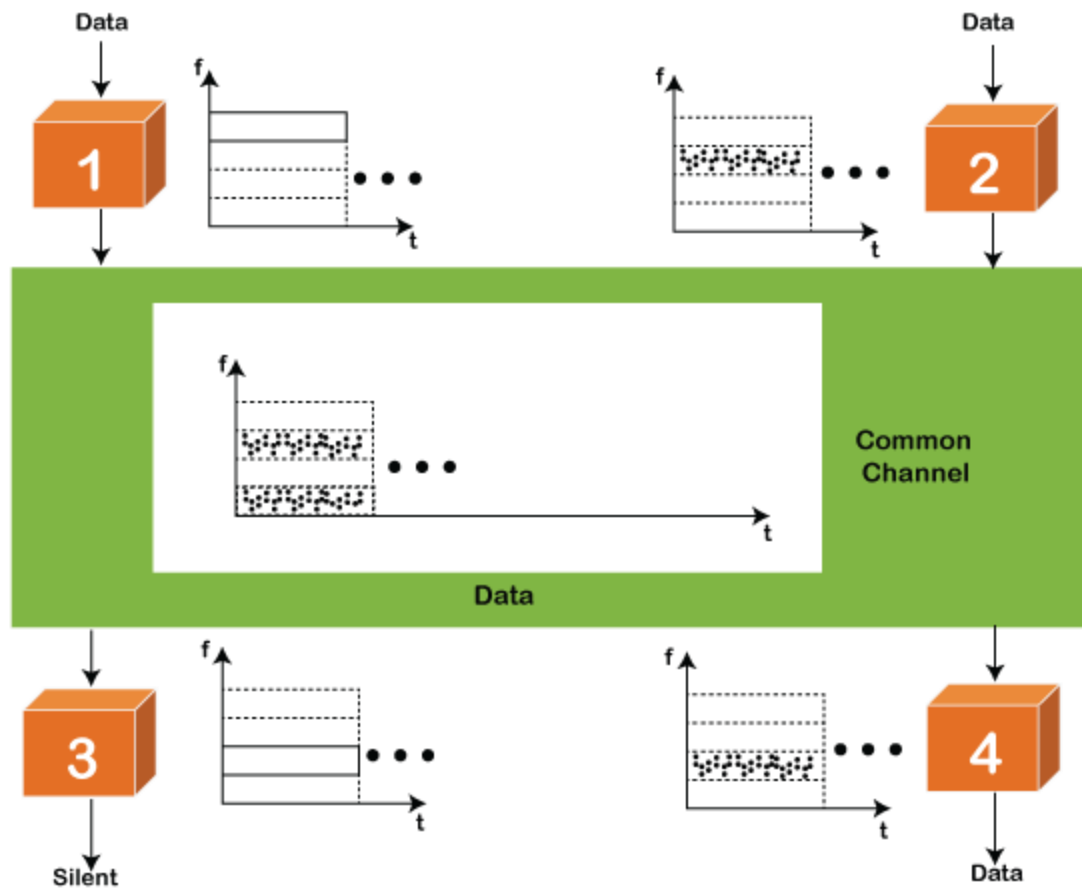
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

### **FDMA**

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



## TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

## CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a

room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.