# Data Link Layer

# LAN Technologies | ETHERNET

Ethernet

- uses **Bus Topology**
- Operates on **Physical Layer** and **Data Link Layer**
- the protocol data unit is **Frame**
- to handle collision, the **Access control mechanism** used in Ethernet is **CSMA/CD**
- **Manchester Encoding** Technique is used in Ethernet.

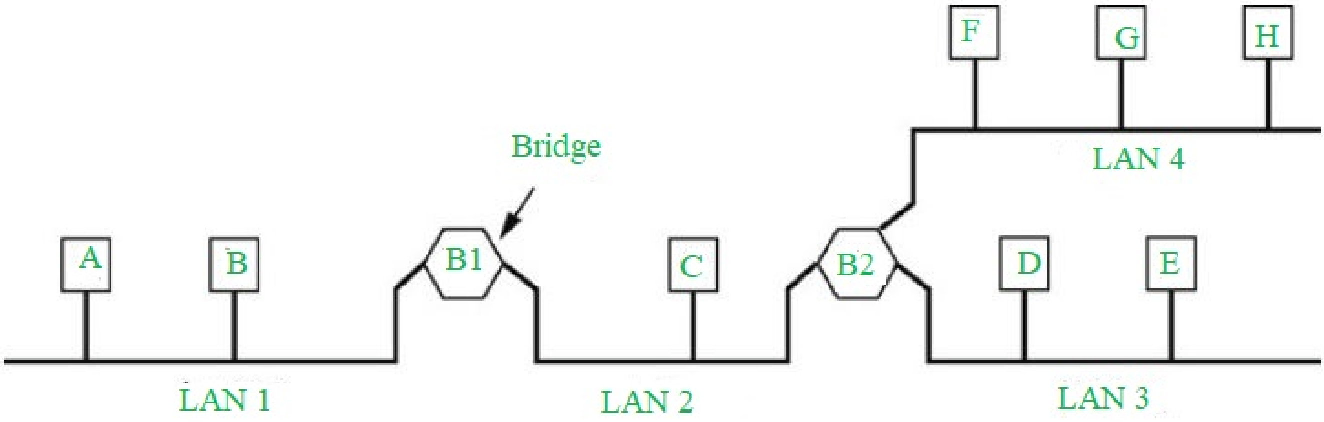
`Advantages :`

- Ethernet provides significantly more speed. Because Ethernet is a one-to-one connection, this is the case. As a result, speeds of up to **10 Gigabits per second (Gbps) or even 100 Gigabits per second (Gbps)** are possible.
- consumes less electricity, even less than a wifi connection
- Because it is resistant to noise, the information transferred is of high quality.

```
Baud rate = 2* Bit rate
```

# Bridges

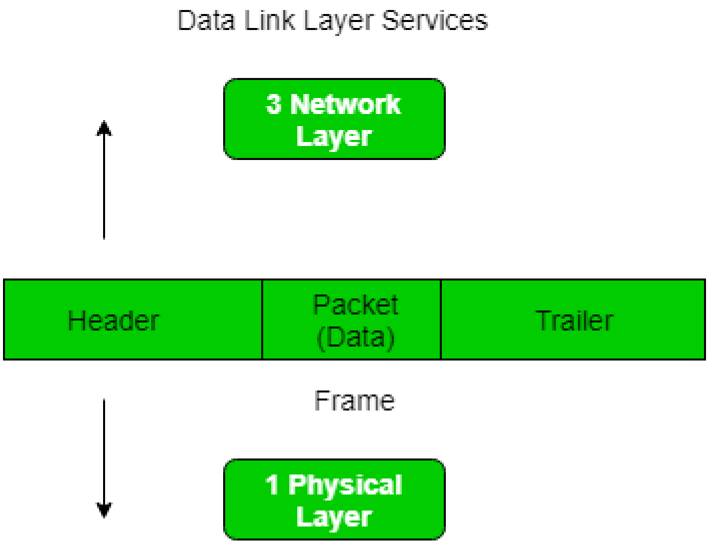
Bridges are a data link layer device and can connect to different networks as well as connect different networks of different types. Bridge follows a protocol in IEEE format execute 802.1 which is a spanning tree of bridges.



It **stores and forwards** Ethernet frames, i.e., it has to do with the **MAC** address rather than the IP address, they handle the hardware addresses. I also examine the frame header and selectively forward frames based on MAC destination address, such as in the given figure if Bridge 2 receives a packet then it will selectively decide whether to send it to LAN 3 or LAN 4. When a frame is to be forwarded in a segment it uses **CSMA/CD** to access the segment. These are transparent, i.e., hosts are unaware of the presence of bridges, it appears to them as a single whole network. Bridges need not be configured they are plug-and-play and self-learning devices, i.e. a bridge has a learning table, they learn which hosts can be reached through which interfaces. At the physical level, the bridge boosts the signal strength like a repeater or completely regenerates the signal.

# Framing in Data Link Layer

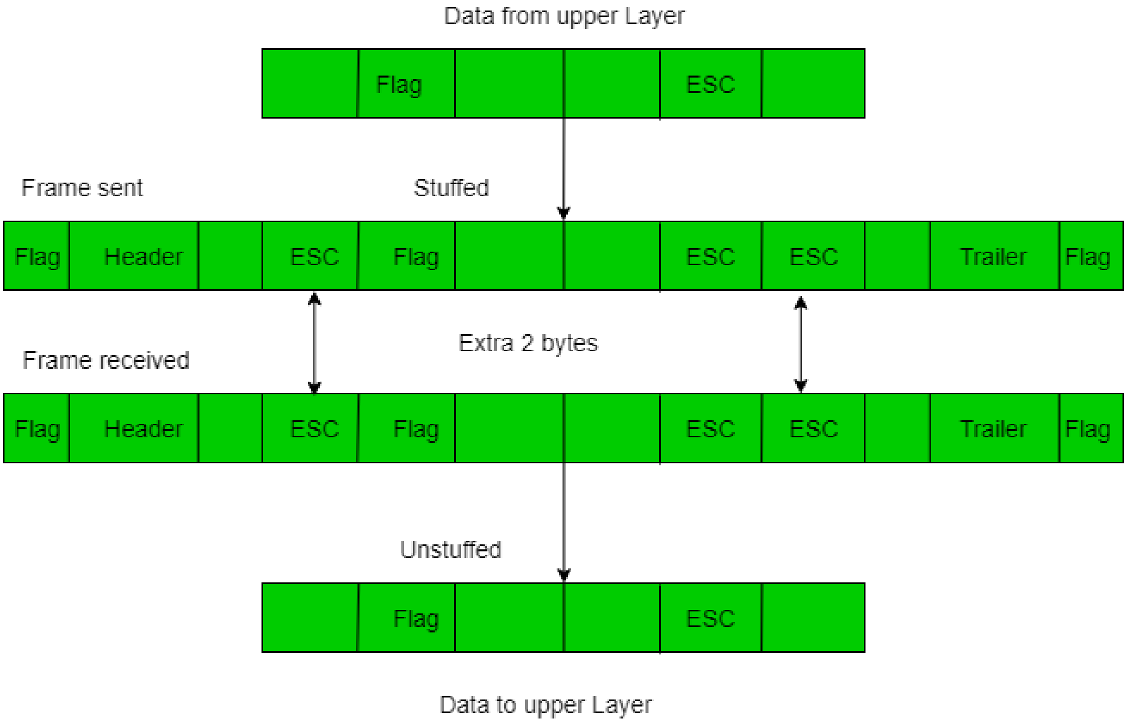
Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy.



At the data link layer, it extracts the message from the sender and provides it to the receiver by providing the sender's and receiver's addresses. The advantage of using frames is that data is broken up into recoverable chunks that can easily be checked for corruption.

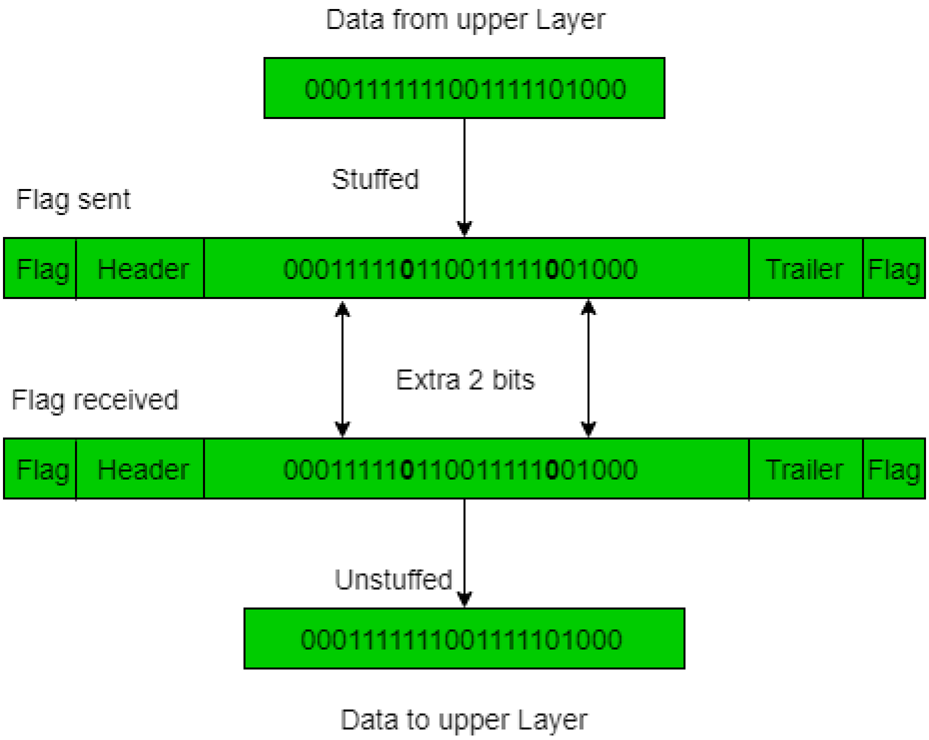
Types of framing:

- `Fixed size:` The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.
- `Variable Size:` In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish. This can be done in two ways:
  - `Length field` – We can introduce a length field in the frame to indicate the length of the frame. The problem with this is that sometimes the length field might get corrupted.
  - `End Delimiter (ED)` – We can introduce an ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with this is that ED can occur in the data. This can be solved by:
    - `Character/Byte Stuffing:` Used when frames consist of characters. If data contains ED then, a byte is stuffed into data to differentiate it from ED.



**Disadvantage** – It is very costly.

- `Bit Stuffing:`



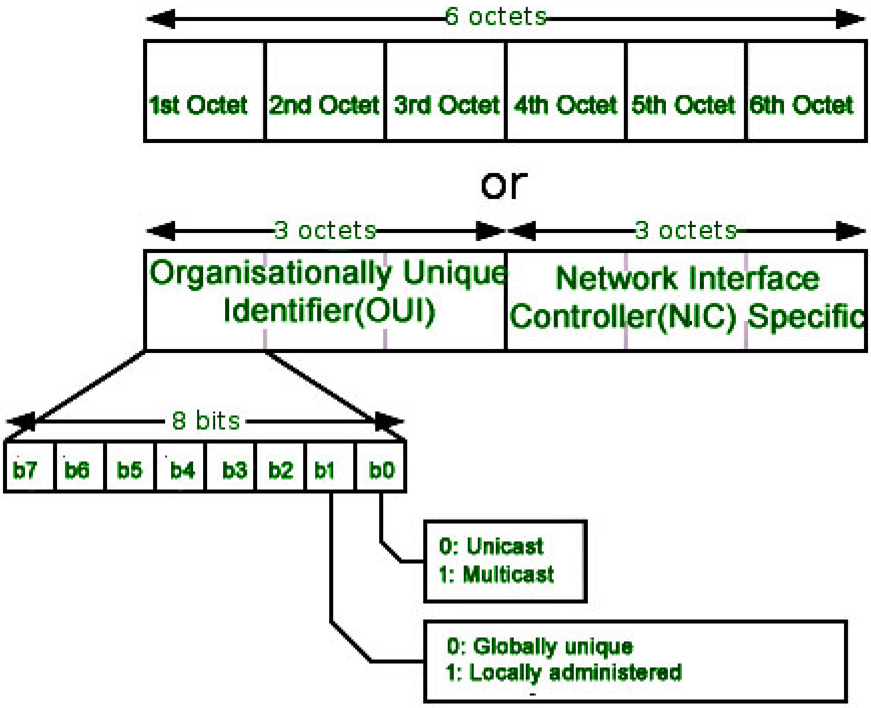
# Introduction of MAC Address

### Media Access Control (MAC) Address –

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into a network card (known as a **Network Interface Card**) during the time of manufacturing. MAC Address is also known as the **Physical Address** of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers

- Logical Link Control(LLC) Sublayer

- Media Access Control(MAC) Sublayer

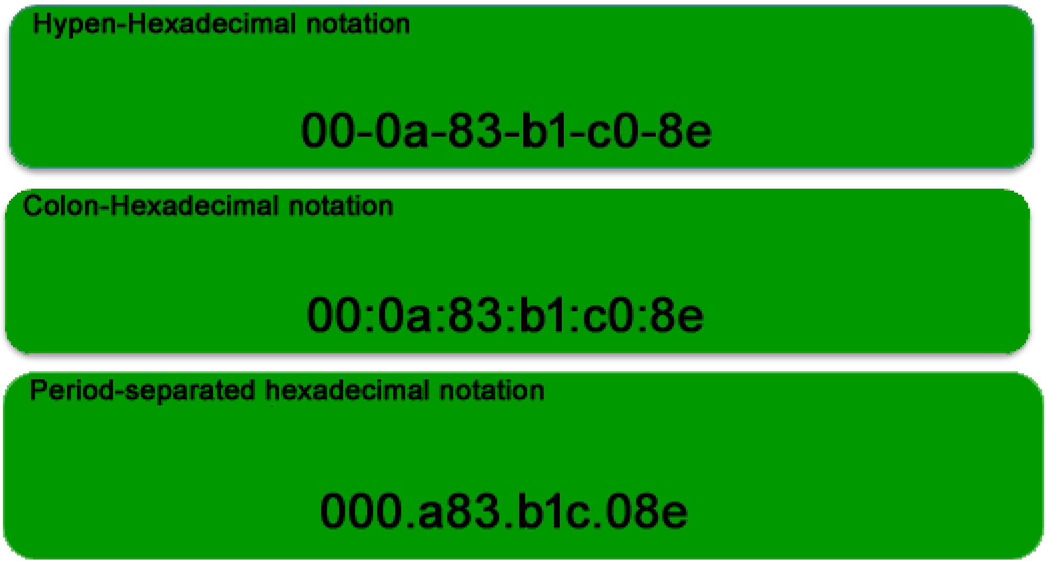


Format of MAC Address –

MAC Address is a **12-digit hexadecimal number (6-Byte binary number)**, which is mostly represented by **Colon-Hexadecimal notation.** The First 6-digits (say 00:40:96) of MAC Address identifies the **manufacturer, called OUI (Organizational Unique Identifier)**. **IEEE Registration Authority Committee** assigns these MAC prefixes to its registered vendors. Here are some OUI of well-known manufacturers :

```
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc.
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD
```

The rightmost six digits represent **Network Interface Controller**, which is assigned by the manufacturer.

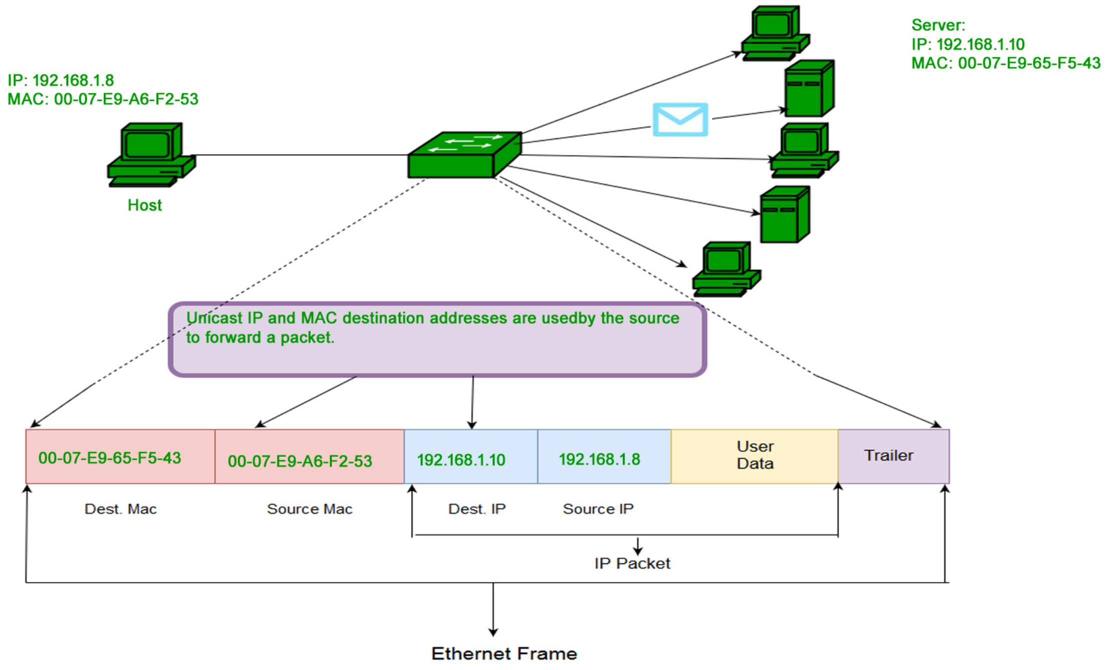

Hypen-Hexadecimal notation
00-0a-83-b1-c0-8e
Colon-Hexadecimal notation
00:0a:83:b1:c0:8e
Period-separated hexadecimal notation
000.a83.b1c.08e

How to find MAC address –

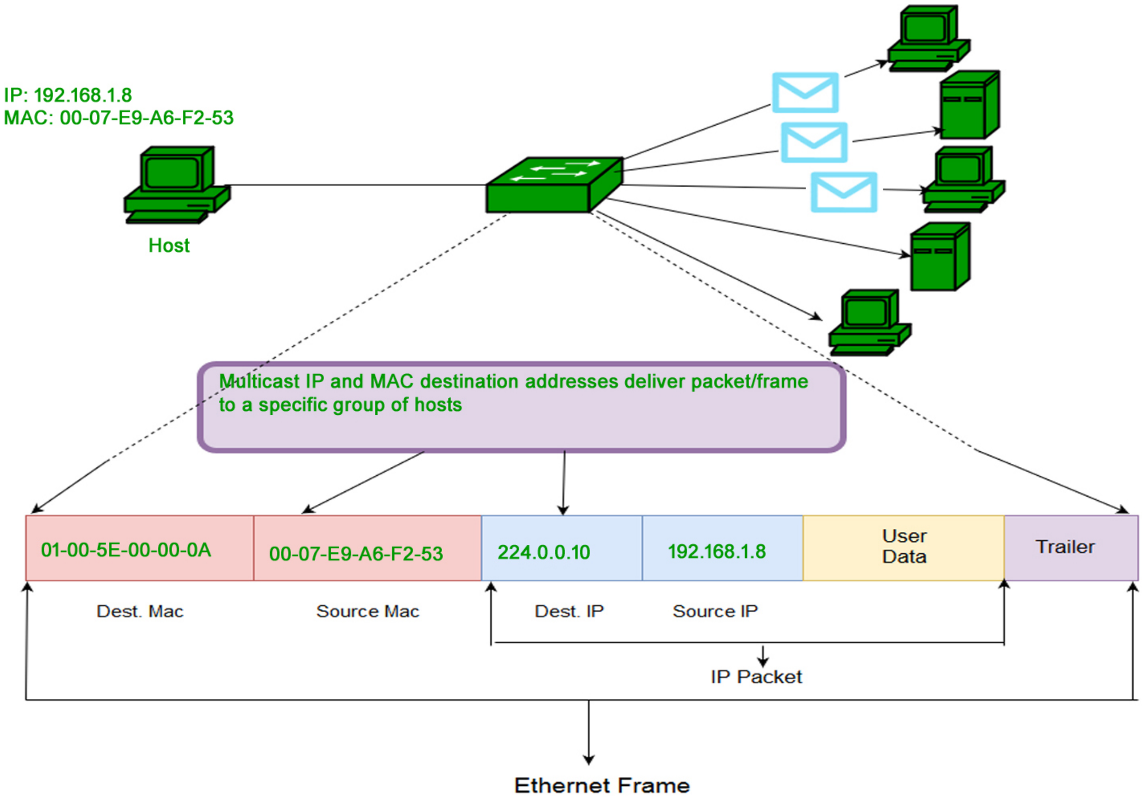
```
Command for UNIX/Linux -  ifconfig -a
                          ip link list
                          ip address show

Command forWindows OS -   ipconfig /all

MacOS -                   TCP/IP Control Panel
```

Types of MAC Address:

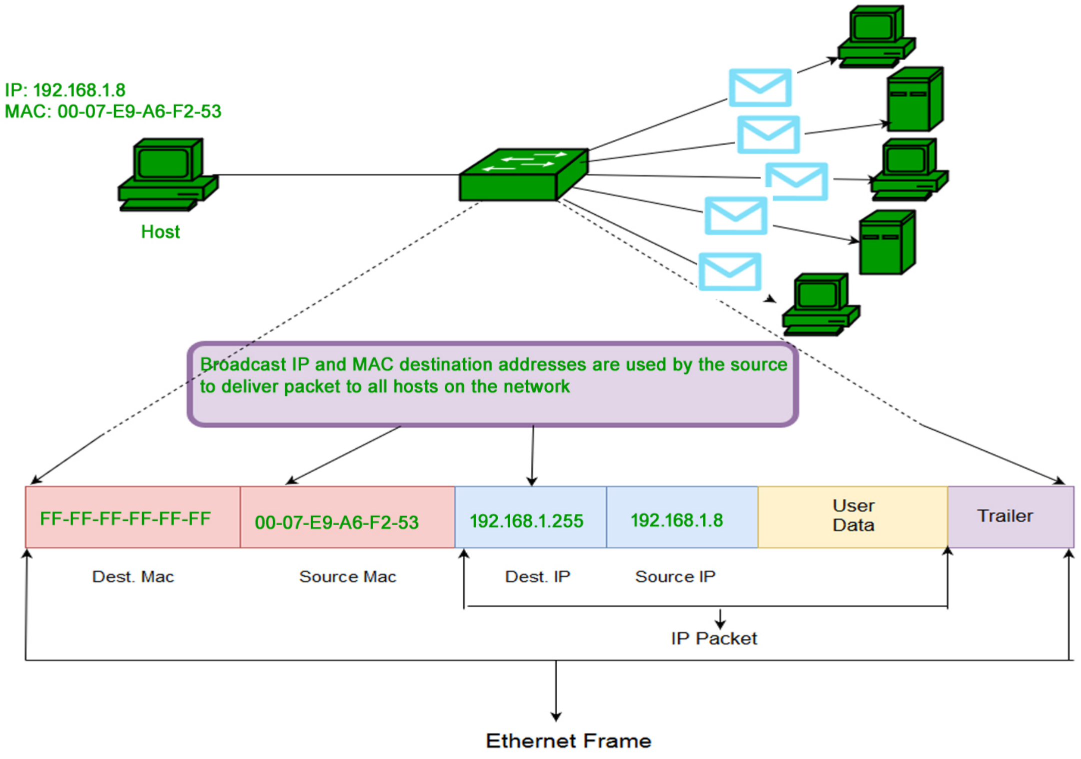
- `Unicast:` A Unicast addressed frame is only sent out to the interface leading to a specific NIC. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC Address of source machine is always Unicast.



- `Multicast:` The multicast address allows the source to send a frame to a group of devices. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) of the first octet of an address is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx (01-80-C2-00-00-00 to 01-80-C2-FF-FF-FF) for group addresses for use by standard protocols.



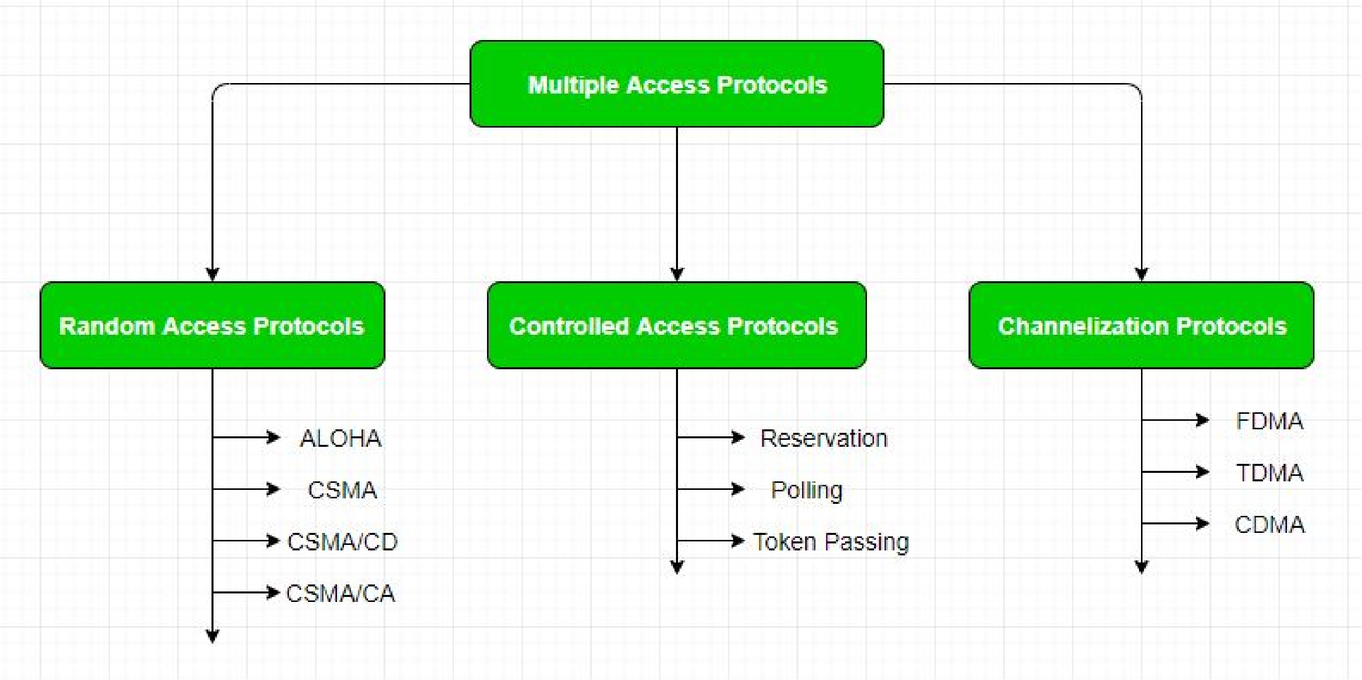
- `Broadcast:` Similar to Network Layer, Broadcast is also possible on the underlying layer( Data Link Layer). **Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are referred to as the broadcast addresses.** Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belonging to that LAN segment



# Multiple Access Protocols

## Multiple Access Control –

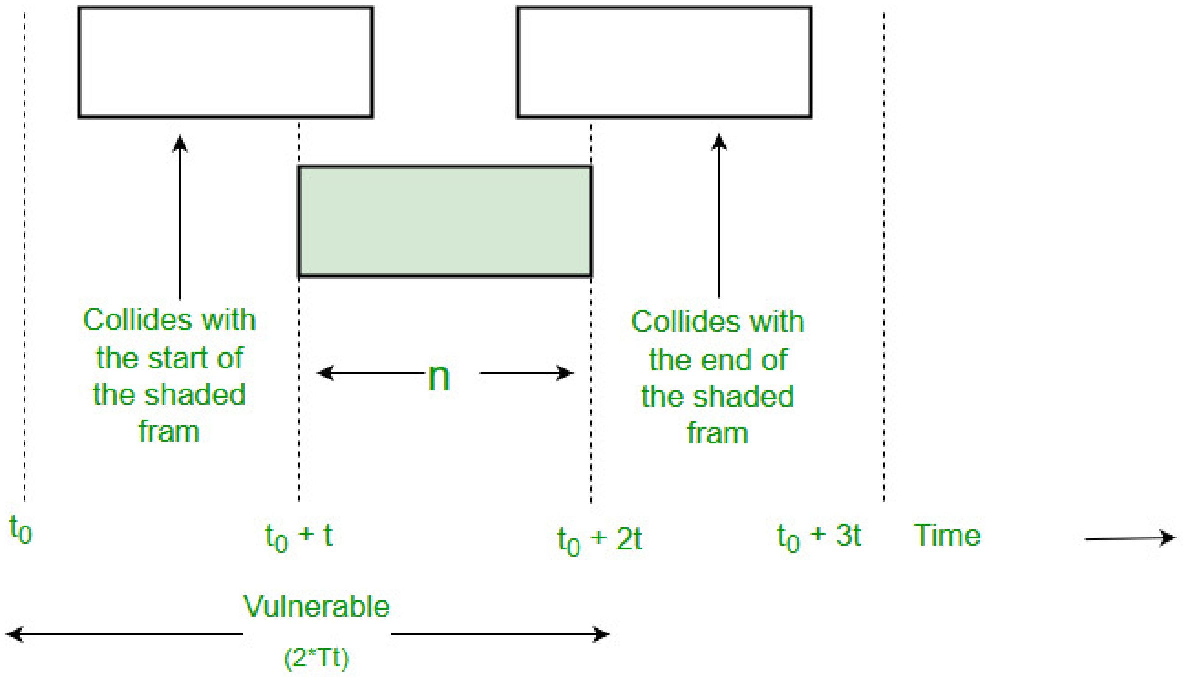
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.



## Random Access Protocol:

In this, all stations have same superiority that is no station has more priority than another station.

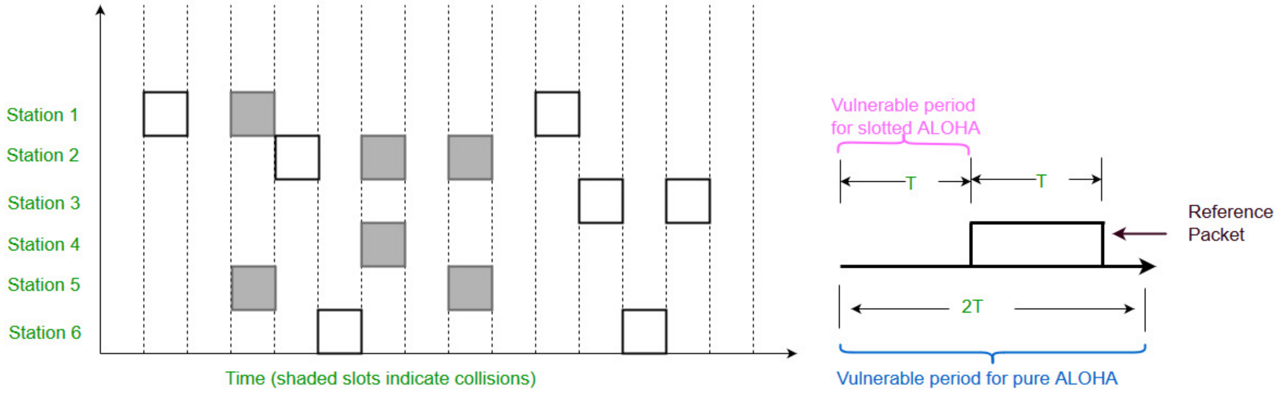
- `Aloha:` Aloha is a multiple access protocol at the data link layer and proposes how multiple terminals access the medium without interference or collision.
  There are two different versions of ALOHA:
  - `Pure Aloha:` Pure Aloha is an un-slotted, decentralized, and simple to implement the protocol. In pure ALOHA, the stations simply transmit frames whenever they want data to send. It does not check whether the channel is busy or not before transmitting. In case, two or more stations transmit simultaneously, the collision occurs and frames are destroyed. Whenever any station transmits a frame, it expects acknowledgement from the receiver. If it is not received within a specified time, the station assumes that the frame or acknowledgement has been destroyed. Then, the station waits for a random amount of time and sends the frame again. This randomness helps in avoiding more collisions. This scheme works well in small networks where the load is not much. But in largely loaded networks, this scheme fails poorly. This led to the development of Slotted Aloha.



Collides with the start of the shaded fram
n
Collides with the end of the shaded fram
$t_0$
$t_0 + t$
$t_0 + 2t$
$t_0 + 3t$
Time
Vulnerable
(2*Tt)

```
Vulnerable Time = 2 * Tt
Spure= G * e^-2G
where G is number of stations wants to transmit in Tt slot.

Maximum Efficiency:
Maximum Efficiency will be obtained when G=1/2

(Spure)max = 1/2 * e^-1
        = 0.184

Which means, in Pure ALOHA, only about 18.4% of the time is used for
successful transmissions.
```

  - `Slotted Aloha:` This is quite similar to Pure Aloha, differing only in the way transmissions take place. Instead of transmitting right at demand time, the sender waits for some time. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called Slots. The stations are eligible to send a frame only at the beginning of the slot and only one frame per slot is sent. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the beginning of the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot. But still, the number of collisions that can possibly take place is reduced by a large margin and the performance becomes much well compared to Pure Aloha.


Station 1
Station 2
Station 3
Station 4
Station 5
Station 6
Time (shaded slots indicate collisions)
Vulnerable period for slotted ALOHA
T
T
Reference Packet
2T
Vulnerable period for pure ALOHA

```
Vulnerable Time = Tt
Sslotted = G * e^-G

Maximum Efficiency:
(Sslotted)max = 1 * e^-1
              = 1/e = 0.368
Maximum Efficiency, in Slotted ALOHA, is 36.8%.
```

- `CSMA –` **Carrier Sense Multiple Access** ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.
  CSMA access modes-
  - `1-persistent:` The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
  - `Non-Persistent:` The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
  - `P-persistent:` The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
  - `O-persistent:` Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

- `CSMA/CD` – **Carrier sense multiple access with collision detection.** Stations can terminate transmission of data if collision is detected.

- `CSMA/CA` – **Carrier sense multiple access with collision avoidance**. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. CSMA/CA avoids collision by:

  - `Interframe space` – Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
  - `Contention Window` – It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
  - `Acknowledgement` – The sender re-transmits the data if acknowledgement is not received before time-out.

### 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 collision of messages on shared medium.

- Reservation
- Polling
- Token Passing

#### Reservation

- In the reservation method, a station needs to make a reservation before sending data.

- The time line has two kinds of periods:

  - Reservation interval of fixed time length
  - Data transmission period of variable frames.

- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.

- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.

- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.

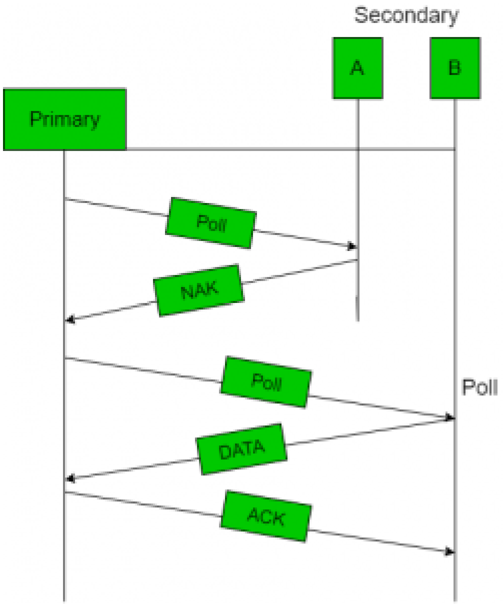
- The stations which have reserved their slots transfer their frames in that order.

- After data transmission period, next reservation interval begins.

- Since everyone agrees on who goes next, there will never be any collisions.

**Polling**

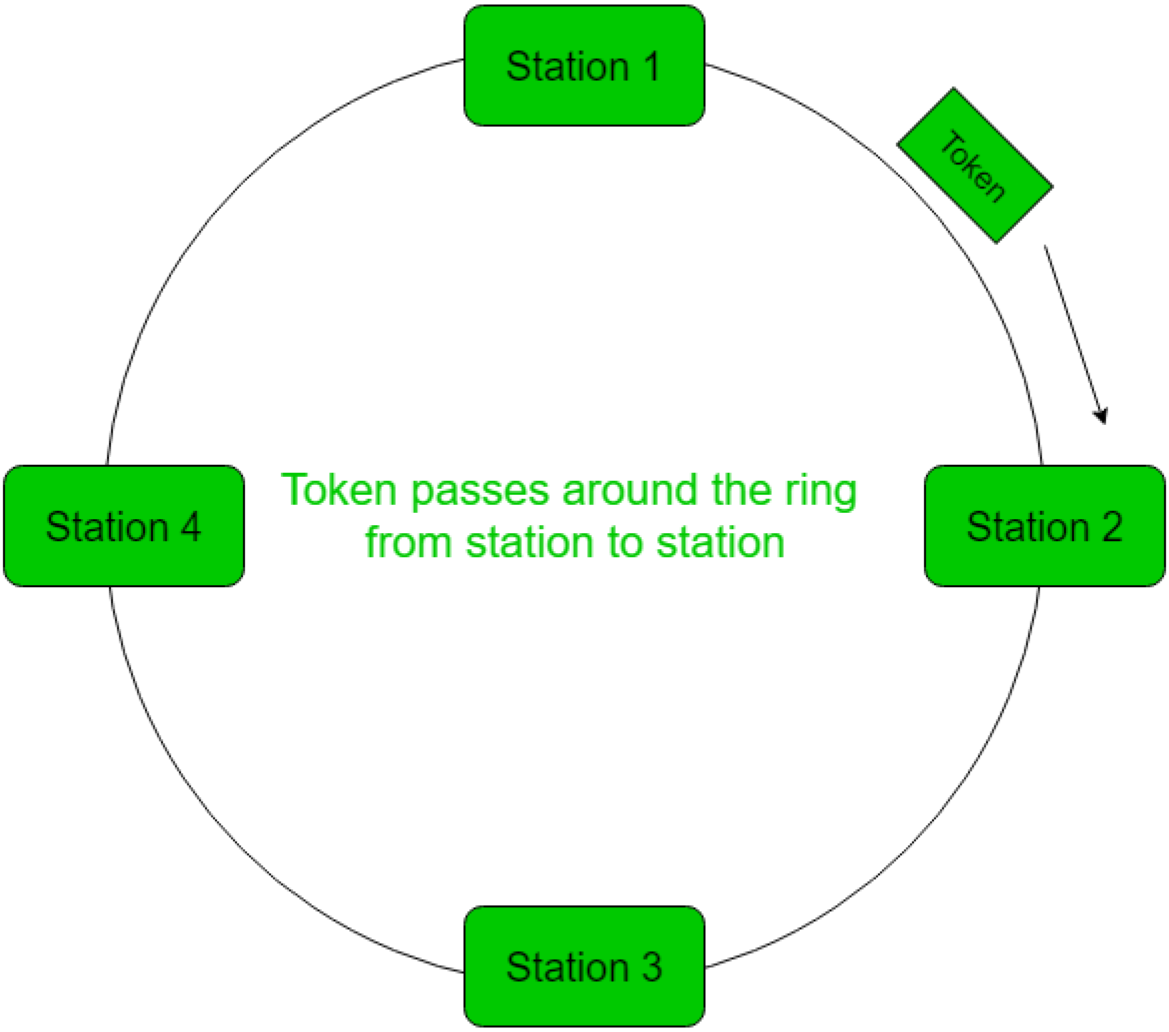
- Polling process is similar to the roll-call performed in class.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.
- Although all nodes receive the message but 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.



```
Tpoll = time for polling
Tt = time required for transmission of data

Efficiency = Tt/(Tt + Tpoll)
```

**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.



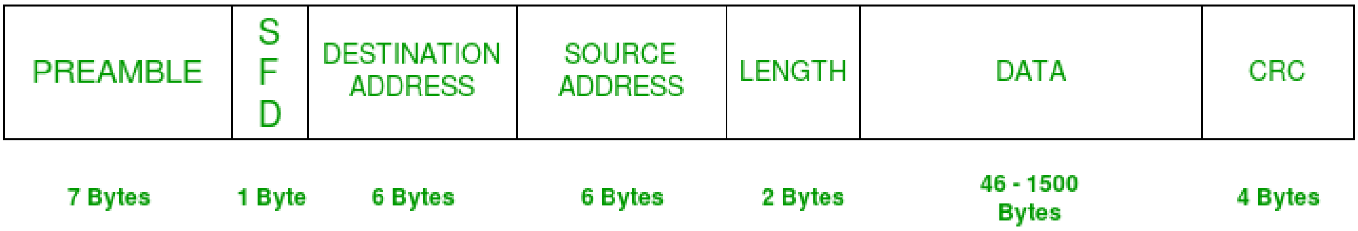
```
Throughput, S = 1/(1 + a/N) for a<1
 S = 1/{a(1 + 1/N)} for a>1.
       where N = number of stations
             a = Tp/Tt
(Tp = propagation delay and Tt = transmission delay)
```

## Channelization

- `Frequency Division Multiple Access (FDMA)` – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- `Time Division Multiple Access (TDMA)` – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands. For more details refer – Circuit Switching
- `Code Division Multiple Access (CDMA)` – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.

# Ethernet Frame Format

Ethernet frame starts with Preamble and SFD, both works at the physical layer. Ethernet header contains both Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error.



| PREAMBLE | SFD | DESTINATION ADDRESS | SOURCE ADDRESS | LENGTH | DATA | CRC |
|---|---|---|---|---|---|---|
| 7 Bytes | 1 Byte | 6 Bytes | 6 Bytes | 2 Bytes | 46 - 1500 Bytes | 4 Bytes |

IEEE 802.3 ETHERNET Frame Format

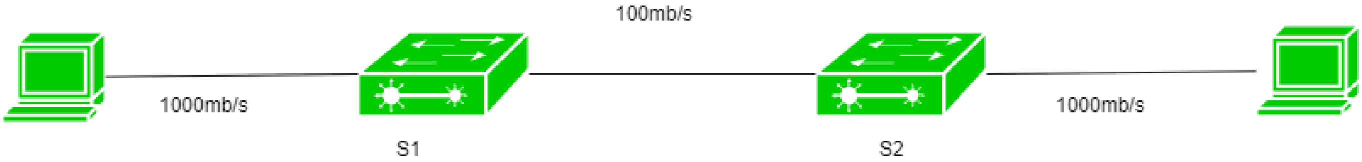
- `PREAMBLE –`
  - It is 7-BYtes Long.
  - It is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization.
  - Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays.
- `Start of frame delimiter (SFD) –`
  - It is a 1 Byte field which is always set to **10101011**.
  - SFD indicates that upcoming bits are starting of the frame, which is the destination address.
  - Sometimes, SFD also considered as a part of Preamble.
- `Destination Address –` This is 6-Byte field which contains the MAC address of machine for which data is destined.
- `Source Address –`
  - This is a 6-Byte field which contains the MAC address of source machine.
  - As Source Address is always an individual address (Unicast), the least significant bit of first byte is always 0.
- `Length –` Length is a 2-Byte field, which indicates the length of entire Ethernet frame. This 16-bit field can hold the length value between **0 to 65534**, but length cannot be larger than **1500** because of some own limitations of Ethernet.
- `Data -`
  - Place where actual data is inserted, also known as **Payload**
  - The maximum data present may be as long as **1500 Bytes**.
  - In case data length is less than minimum length i.e. **46 bytes**, then padding 0's is added to meet the minimum possible length.
- `Cyclic Redundancy Check (CRC) –` CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

**Note – Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).**

# EtherChannel in Computer Network

EtherChannel is a port link aggregation technology in which multiple physical port links are grouped into one logical link. It is used to provide high-speed links and redundancy. A **maximum of 8 links** can be aggregated to form a single logical link.

### Need of EtherChannel -



Now, suppose if you want to send traffic of more than 100mb/s then we have congestion as the link between the switches is of 100mb/s only and packets will start dropping. Now, to solve this problem, we should have a high-speed link between the switches. To achieve this, We can simply replace the current link with a high-speed link or we can bundle up more than one link of the same speed of 100mb/s. By forming an EtherChannel, you can bundle up more than one link into a single logical link.

`Criteria –` To form an EtherChannel, all ports should have:

- Same duplex
- Same speed
- Same VLAN configuration (i.e., native VLAN and allowed VLAN should be same)
- Switch port modes should be the same (access or trunk mode

# Circuit Switching

In circuit switching network resources (bandwidth) are divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established. **Telephone system network** is one of the example of Circuit switching.

- `Frequency Division Multiplexing :` Divides into multiple bands FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands,where each sub-band carry different signal. Practical use in **radio spectrum & optical fibre** to share multiple independent signals.
- `Time Division Multiplexing :` Divides into frames TDM is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user. TDM is also known as a **digital circuit switched.**

`Advantages of Circuit Switching:`

- A dedicated transmission channel is established between the computers which give a guaranteed data rate.
- In-circuit switching, there is no delay in data flow because of the dedicated transmission path.

`Disadvantages of Circuit Switching:`

- It takes a long time to establish a connection.
- More bandwidth is required in setting up dedicated channels.
- It cannot be used to transmit any other data even if the channel is free as the connection is dedicated to circuit switching.

```
Transmission rate = Link Rate or Bit rate /
                    no. of slots = R/h bps
Transmission time = size of file /
                    transmission rate
                 = x / (R/h) = (x*h)/R second
Total time to send packet to destination =
               Transmission time + circuit setup time
```

# Packet Switching

Packet switching is a method of transferring the data to a network in form of packets. In order to transfer the file fast and efficiently manner over the network and minimize the transmission latency, the data is broken into small pieces of variable length, called Packet. At the destination, all these small parts (packets) have to be reassembled, belonging to the same file. A packet composes of payload and various control information. No pre-setup or reservation of resources is needed.
Packet Switching uses **Store and Forward** technique while switching the packets; while forwarding the packet each hop first stores that packet then forward. This technique is very beneficial because packets may get discarded at any hop due to some reason. More than one path is possible between a pair of sources and destinations. Each packet contains Source and destination address using which they independently travel through the network. In other words, packets belonging to the same file may or may not travel through the same path. If there is congestion at some path, packets are allowed to choose different paths possible over an existing network.

`Advantage of Packet Switching over Circuit Switching :`

- More efficient in terms of bandwidth, since the concept of reserving circuit is not there.
- Minimal transmission latency.
- More reliable as a destination can detect the missing packet.
- More fault tolerant because packets may follow a different path in case any link is down, Unlike Circuit Switching.
- Cost-effective and comparatively cheaper to implement.

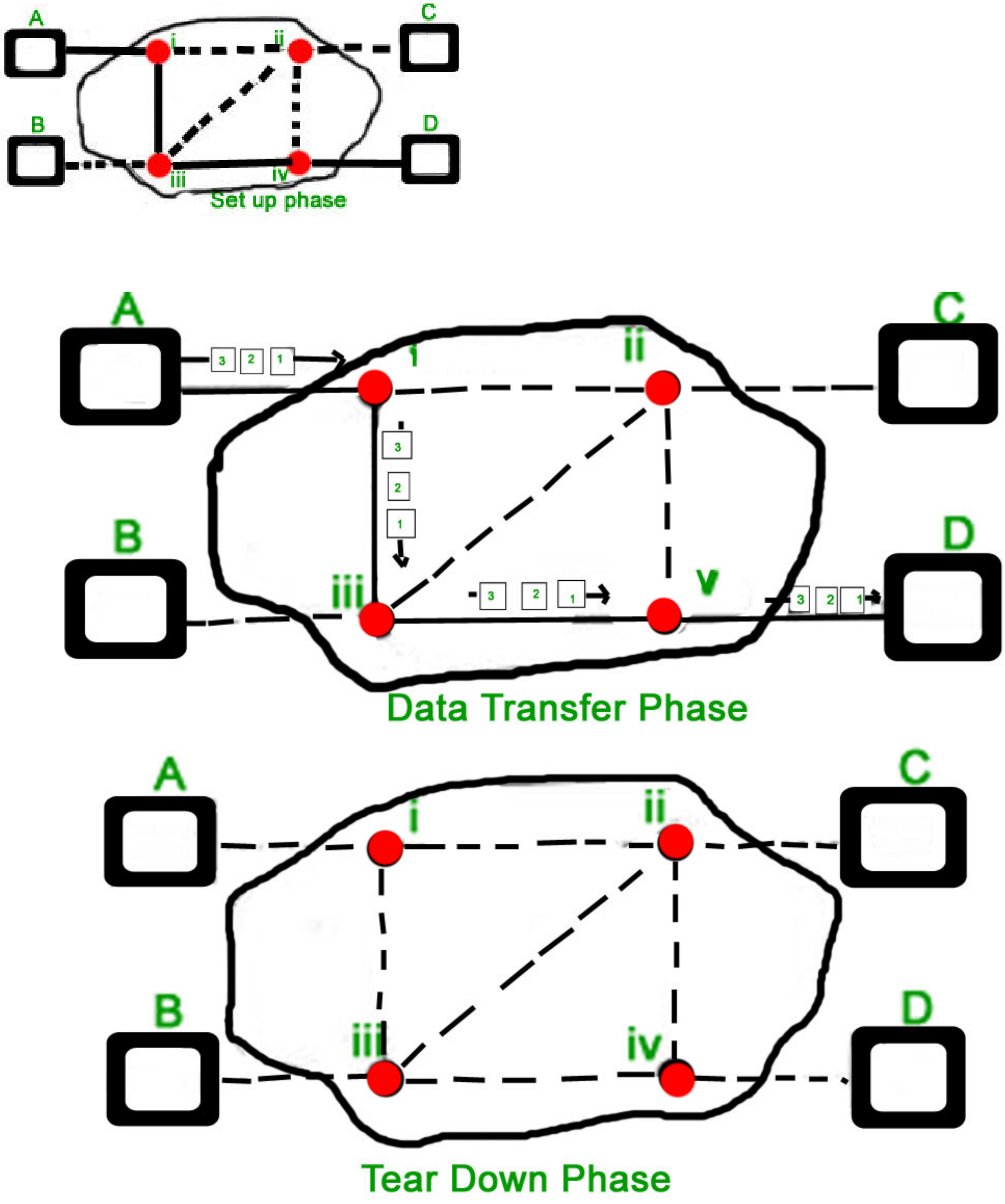
`The disadvantage of Packet Switching over Circuit Switching :`

- Packets are unordered
- Since the packets are unordered, we need to provide sequence numbers for each packet.
- Complexity is more at each node because of the facility to follow multiple paths.
- Transmission delay is more because of rerouting.
- **Packet Switching is beneficial only for small messages, but for bursty data (large messages) Circuit Switching is better.**

# Modes of Packet Switching :

1. Connection-oriented Packet Switching (Virtual Circuit) :

Before starting the transmission, it establishes a logical path or virtual connection using signaling protocol, between sender and receiver and all packets belongs to this flow will follow this predefined route. Virtual Circuit ID is provided by switches/routers to uniquely identify this virtual connection. Data is divided into small units and all these small units are appended with help of sequence numbers. Overall, three phases take place here- The setup, data transfer and tear down phase.



Set up phase

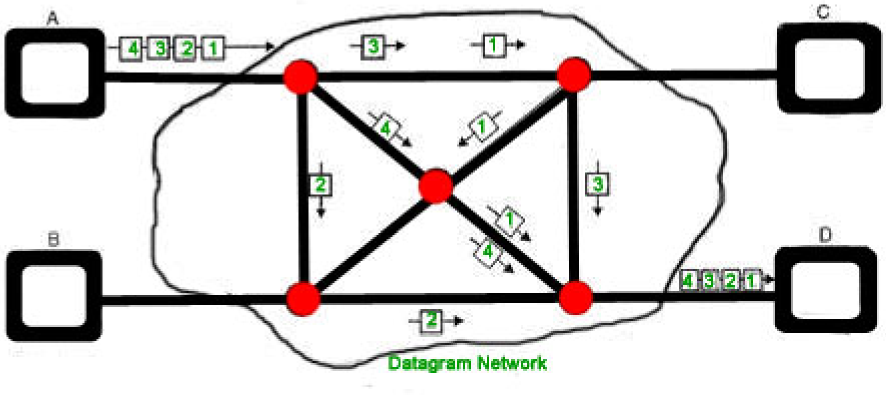
Data Transfer Phase

Tear Down Phase

Phases in virtual circuit packet switching

2. Connectionless Packet Switching (Datagram) :

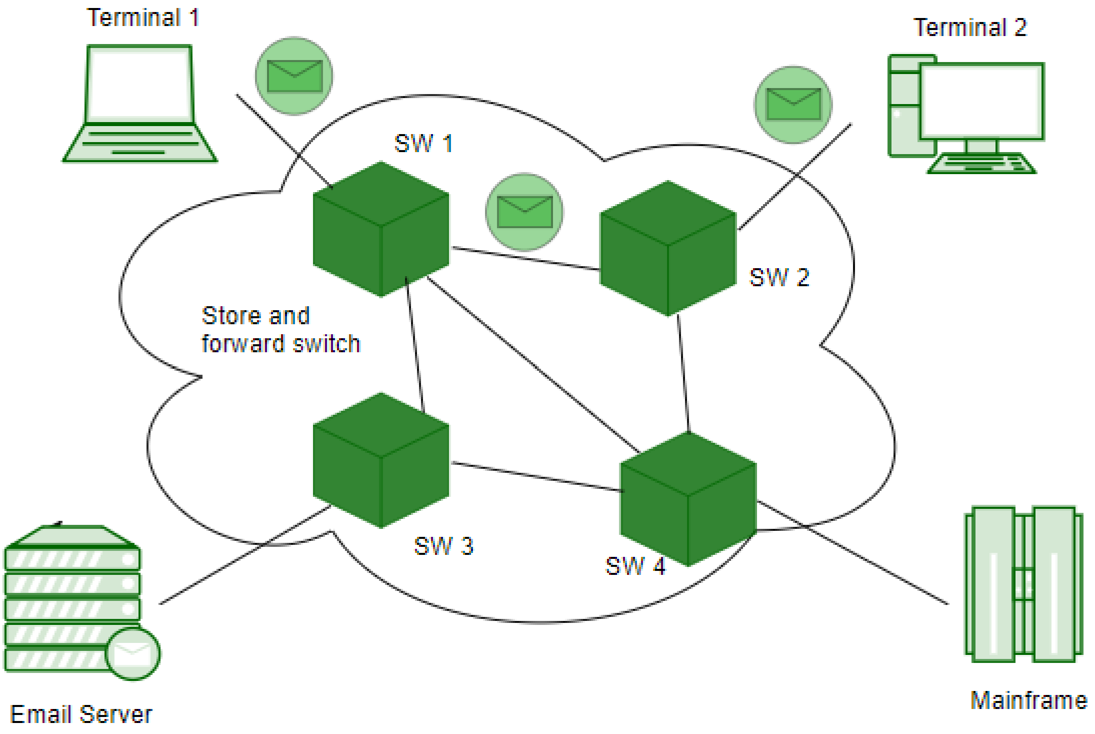
Unlike Connection-oriented packet switching, In Connectionless Packet Switching each packet contains all necessary addressing information such as source address, destination address and port numbers, etc. In Datagram Packet Switching, each packet is treated independently. Packets belonging to one flow may take different routes because routing decisions are made dynamically, so the packets arrived at the destination might be out of order. It has no connection setup and teardown phase, like Virtual Circuits.



Datagram Packet Switching

## Message Switching –

Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced. In message switching, end-users communicate by sending and receiving messages that included the entire data to be shared. Messages are the smallest individual unit. Also, the sender and receiver are not directly connected. There are a number of intermediate nodes that transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems. It uses **store and forward** technique.
`Message delivery` – This implies wrapping the entire information in a single message and transferring it from the source to the destination node. Each message must have a header that contains the message routing information, including the source and destination.


Terminal 1
Terminal 2
SW 1
SW 2
Store and forward switch
SW 3
SW 4
Email Server
Mainframe