6.6 Explores the role of Media Access Control (MAC) protocol

Local Area Network (LAN)

Networks with nodes that are in close physical proximity—within the same building, for instance—are called local area networks (LANs).

Typically, LANs span distances less than a mile and are owned and operated by individual organizations.

LANs are widely used by colleges, universities, and other types of organizations to link personal computers and to share printers and other resources.

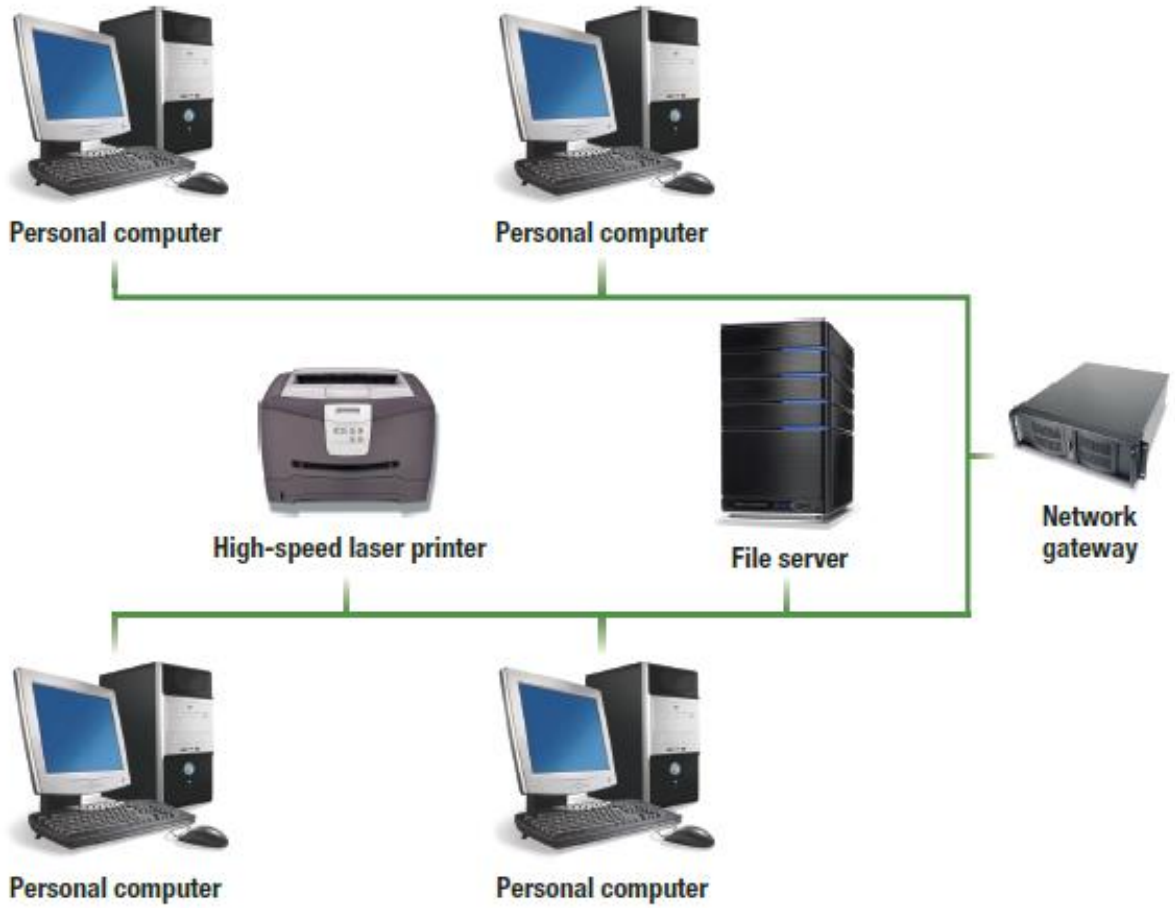
The LAN provides two benefits: economy and flexibility.

People can share costly equipment. For instance, the four personal computers share the high-speed laser printer and the file server, which are expensive pieces of hardware.

Other equipment or nodes also may be added to the LAN—for instance, more personal computers, a mainframe computer, or optical disc storage devices.

Additionally, the network gateway is a device that allows one LAN to be linked to other LANs or to larger networks. For example, the LAN of one office group may be connected to the LAN of another office group.

There are a variety of different standards or ways in which nodes can be connected to one another and ways in which their communications are controlled in a LAN. The most common standard is known as Ethernet. LANs using this standard are sometimes referred to as Ethernet LANs.



Local area network

Identifying devices in the network

In order to communicate or transfer the data from one computer to another computer we need some address. In Computer Network various types of address are introduced; each works at different layer. **Media Access Control Address** is a physical address which works at Data Link Layer.

Protocol

A **PROTOCOL** is nothing but set of defined **rules**, which has to be followed by every connected device across a network to communicate and share information among them.
To facilitates **End to End** communication, a number of protocols worked together to form a **Protocol Suites or Stacks**.

Some basic Protocols are:

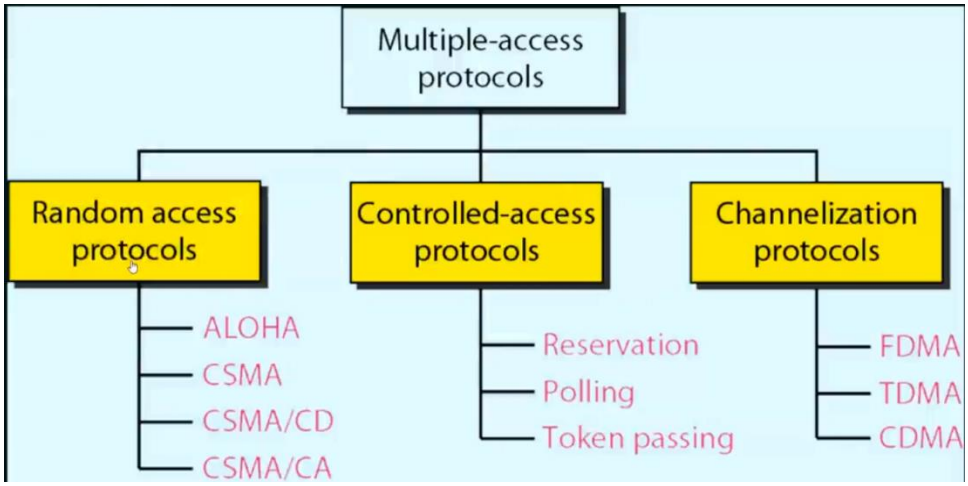
MAC : **Medium Access Control Protocol** – enable the orderly access to a common shared medium of communication. In bus topology, a common medium is shared by many devices and a medium access control protocol can ensure that the medium is accessed in an orderly manner therefore data collisions are avoided.

IP : Internet Protocol
FTP : File Transfer Protocol
SMTP : Simple Mail Transfer Protocol
HTTP : Hyper Text Transfer Protocol

Multiple Access Protocol

Multiple access protocols are a set of protocols operating in the Medium Access Control sublayer (MAC sublayer) of the Open Systems Interconnection (OSI) model. These protocols allow a number of nodes or users to access a shared network channel.

Three types of Multiple Access Protocols



ALOHA, Slotted ALOHA

ALOHA:

Aloha is a random-access protocol, which means any station can send a data any time.

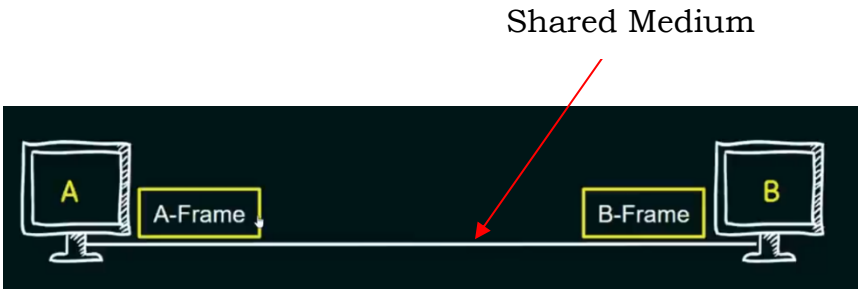
It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii.

It was actually designed for WLAN (Wireless LAN) but it is also applicable for shared medium.

The original system used for ground-based radio broadcasting, but the system has been implemented in satellite communication systems.

Hehe in ALOHA, any station can send a data any time. What if two or more stations transmit data at the same time?
In this, multiple stations can transmit data at the same time and can hence **lead to collision** and **data being garbled**. these data not be useful.it will be either lost or corrupted.

Collision



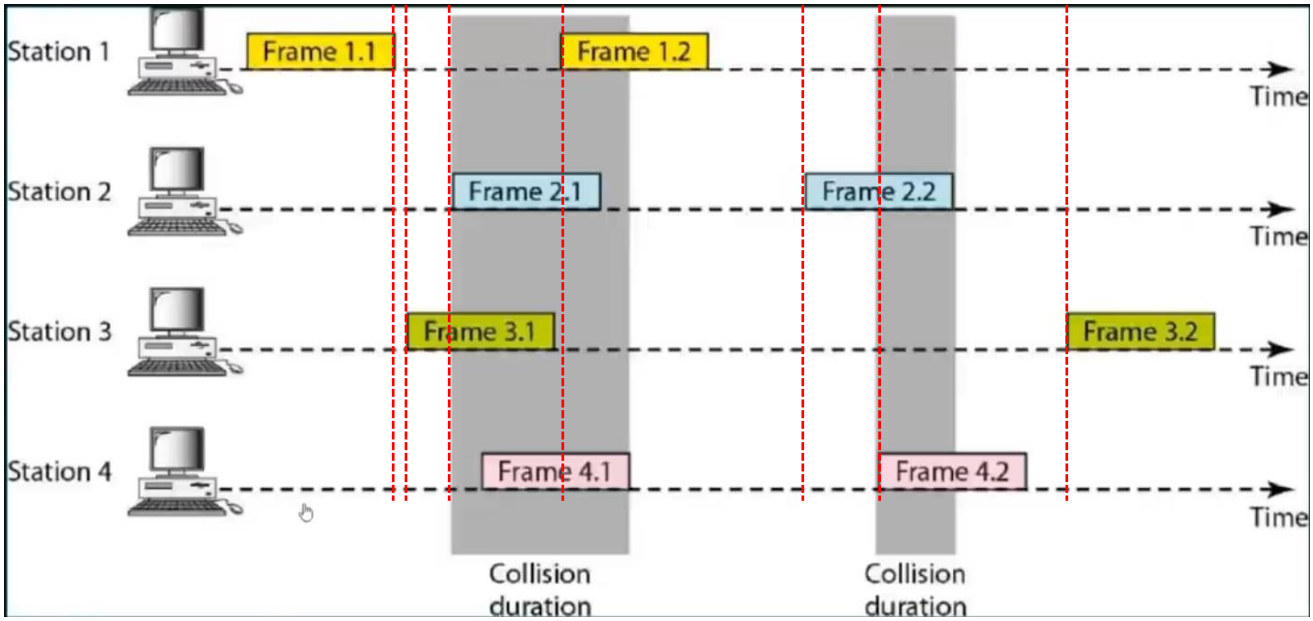
A and B sending data at the same time.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time.

Various types of ALOHA

1. Pure ALOHA
2. Slotted ALOHA

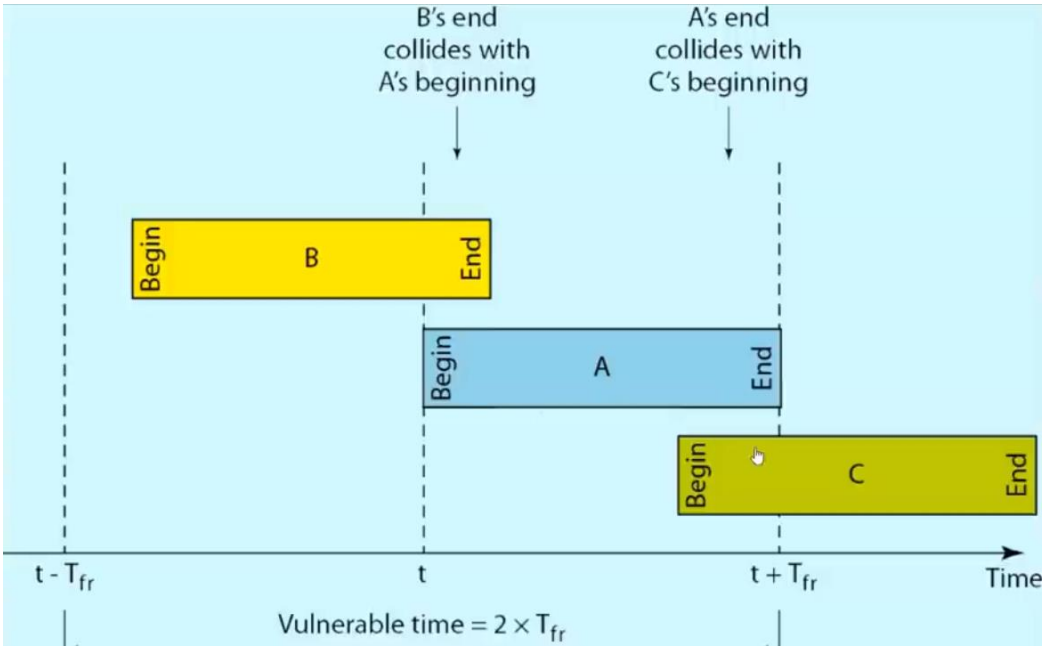
Pure ALOHA



- Here, we have shared medium and 4 stations and time also common for everybody. (**but mention here separately for understandable purpose.**)
- When **Station 1** send data to the common medium, at that time other stations are not sending (transmitting) anything. Therefore Frame 1.1 is survived. Frame 3.2 also survived and other frames are colliding with each other.

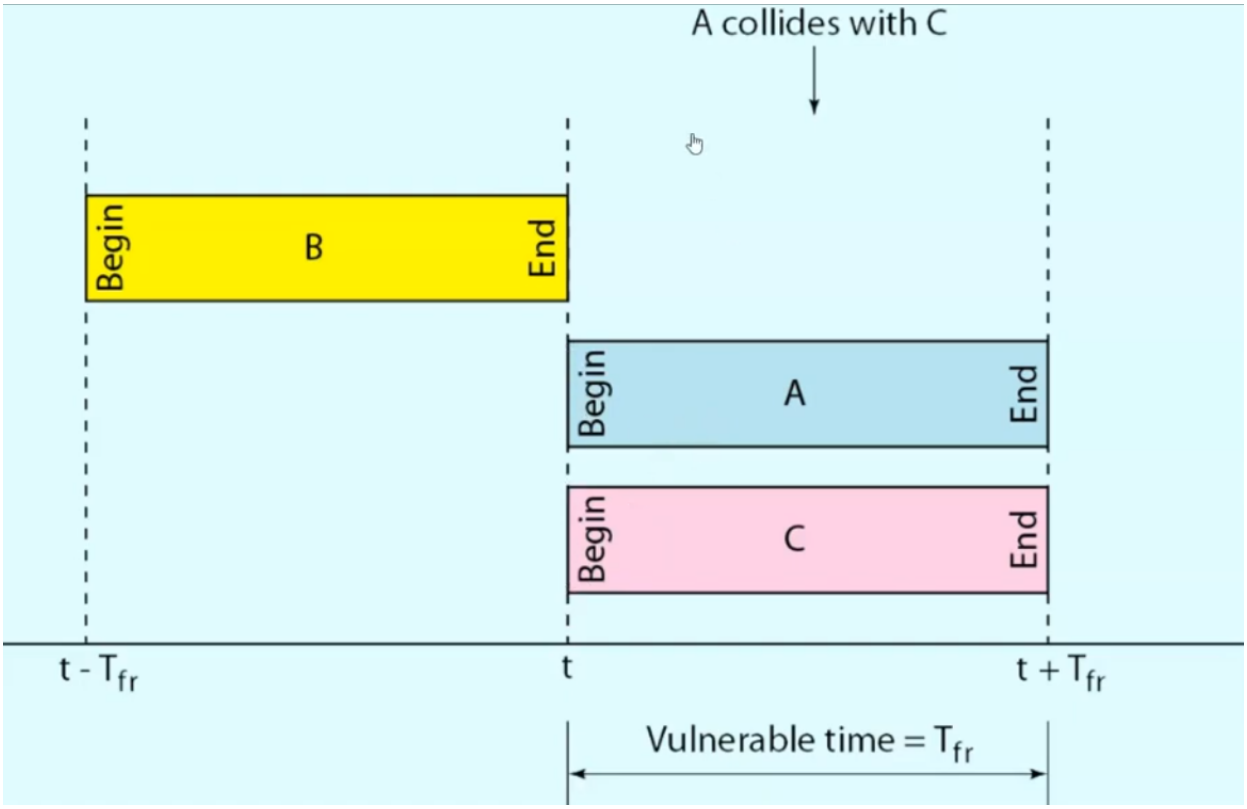
- In pure ALOHA, allows the stations to transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If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

- If the frame is destroyed because of collision the station waits for a random amount of time (back-off time) and re-sends the data. This waiting time must be random otherwise (if it is fixed amount of time) same frames will collide again and again.
- Since different statins wait for different amount of time, the probability of further collision decreases.
- The throughput of pure aloha is maximized when frames are of uniform length.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.



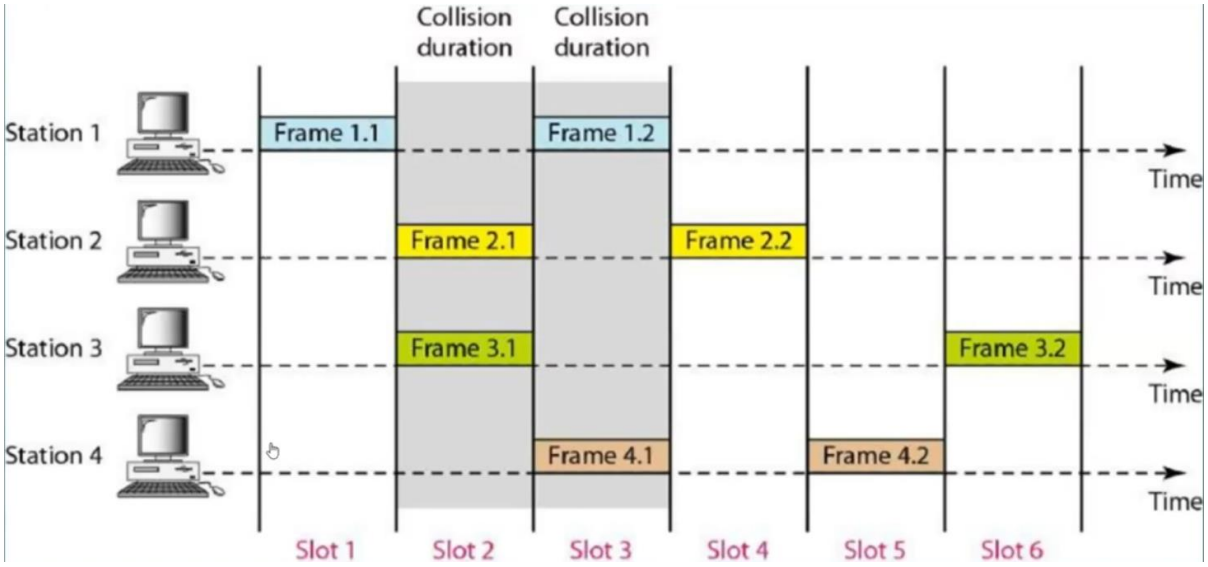
Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots (in pure aloha there is no anything like time slot).
- The stations can send a frame **only at the beginning of the slot** and only one frame is sent in each slot.



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

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



- Here time slot 1, 4,5 and 6 there is no collision occurred.

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

Ethernet:

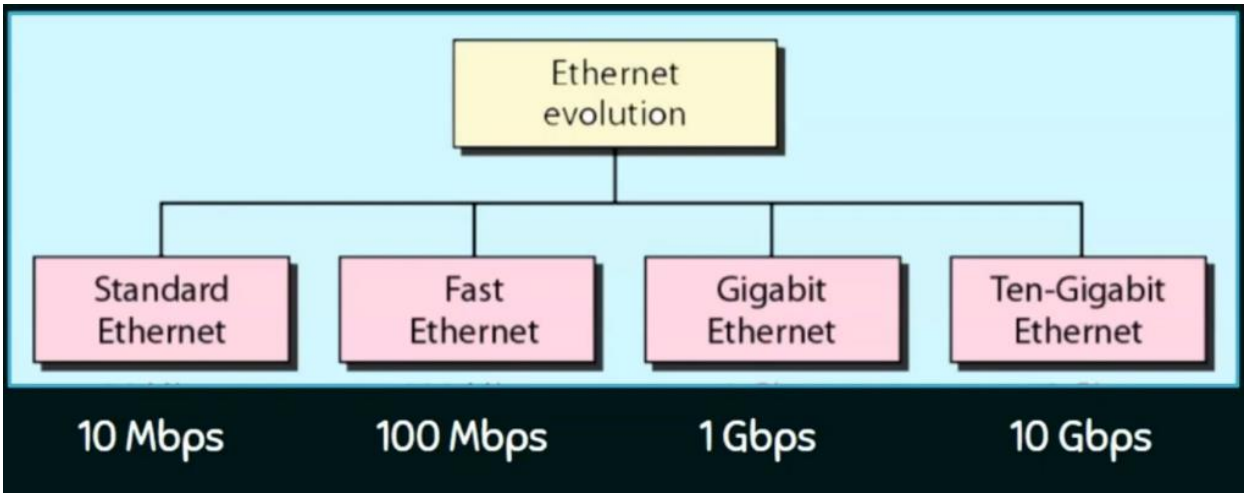
- Ethernet is one of the most widely used Wired LAN Technologies.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet belongs to family of networking technologies that are defined under IEEE 802.2 and 802.3 standards.
- It supports data bandwidth of 10, 100,1000,10000, 40000 and 100000 Mbps (100Gbps) and more.

Ethernet standards

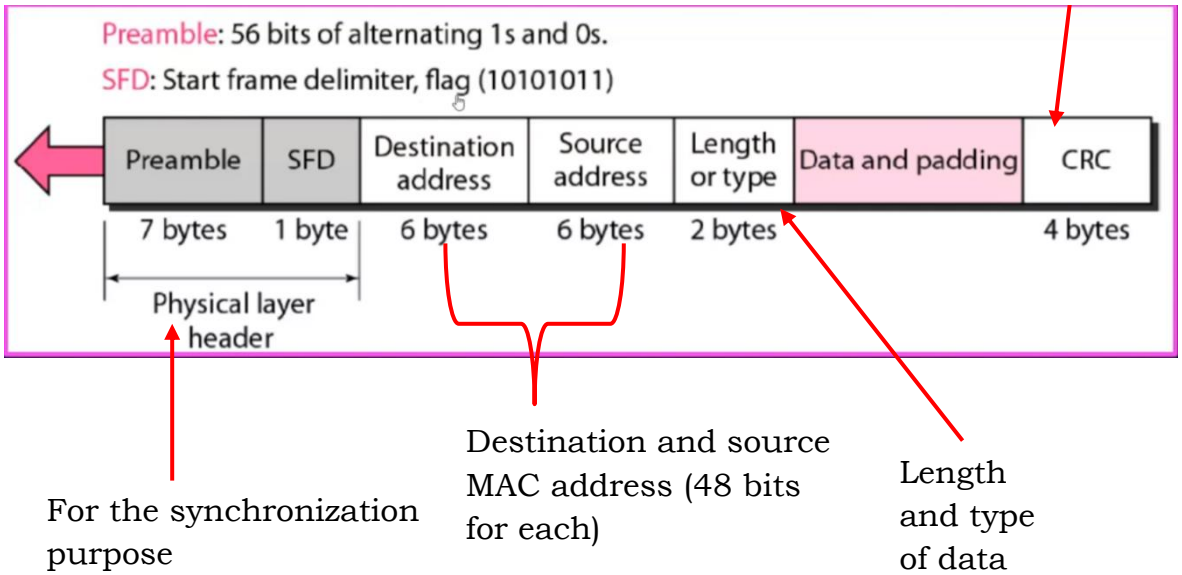
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.

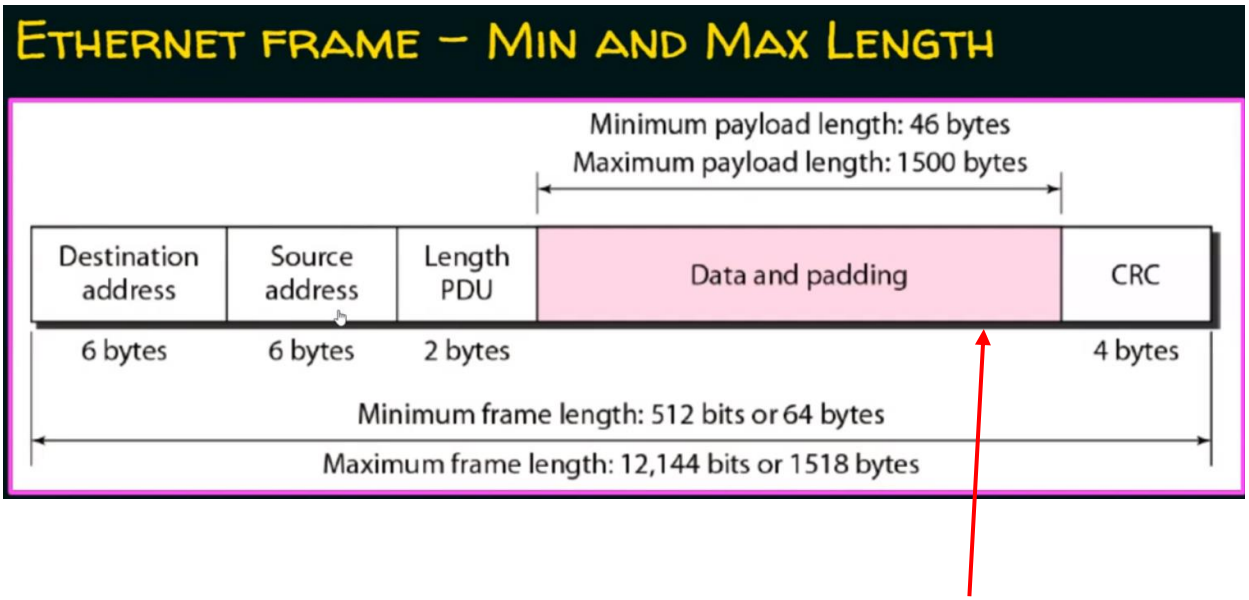
- Ethernet defines **Layer 2 (Data link later) protocols [Ethernet Protocols]** and **Layer 1 (Physical layer) technologies [Ethernet technologies - ethernet cables]**.
- Ethernet has two separate sublayers of data link layer to operate
  - Logical Link Control (LLC) and
  - MAC sublayers.

Ethernet evolution

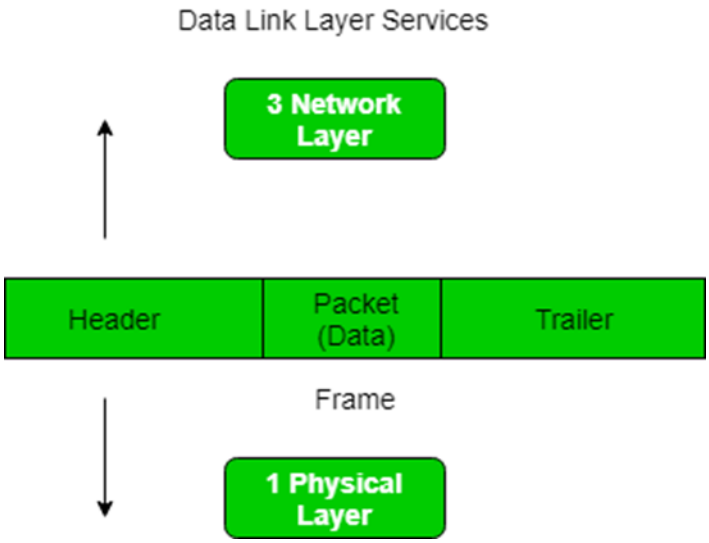


Ethernet Frame Format





Data Packet from Network layer with IP addresses

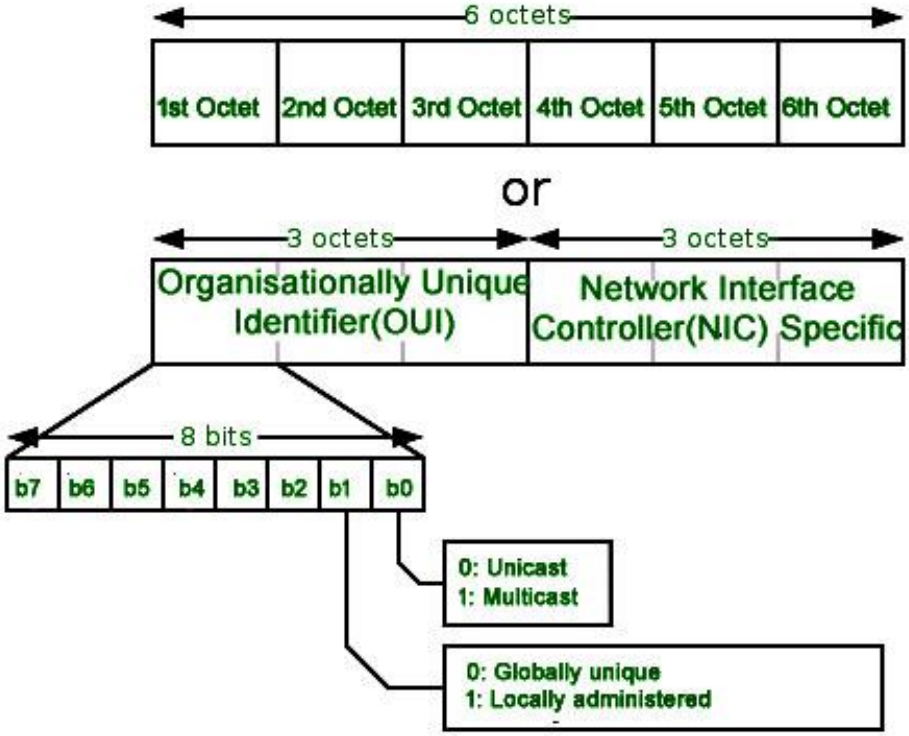


Ethernet Address

- MAC address is also known as Ethernet address. Because in ethernet protocol we are obviously going to use only MAC address.

Media Access Control (MAC) Address

MAC Addresses are unique **48-bits** hardware number of a computer, which is embedded into network card (known as **Network Interface Card**) during the time of manufacturing. MAC Address is also known as **Physical Address** of a network device. MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.



Format of MAC Address –

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

Here are some OUI of well-known manufacturers:

CC: 46:D6 - Cisco

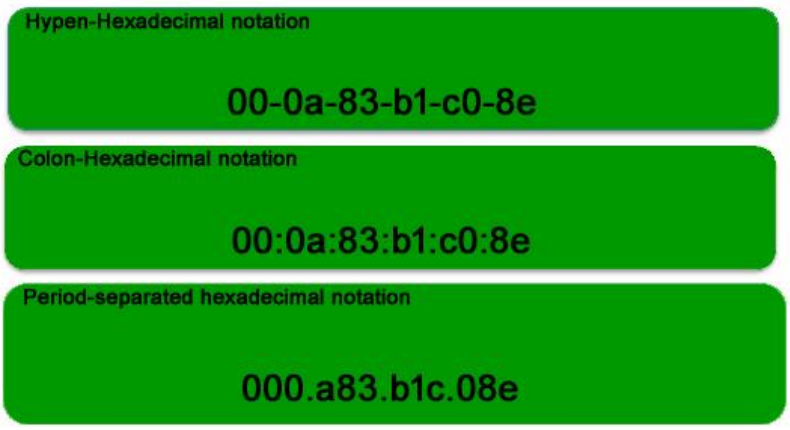
3C:5A:B4 - Google, Inc.

3C:D9:2B - Hewlett Packard

00:9A: CD - HUAWEI TECHNOLOGIES CO., LTD

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

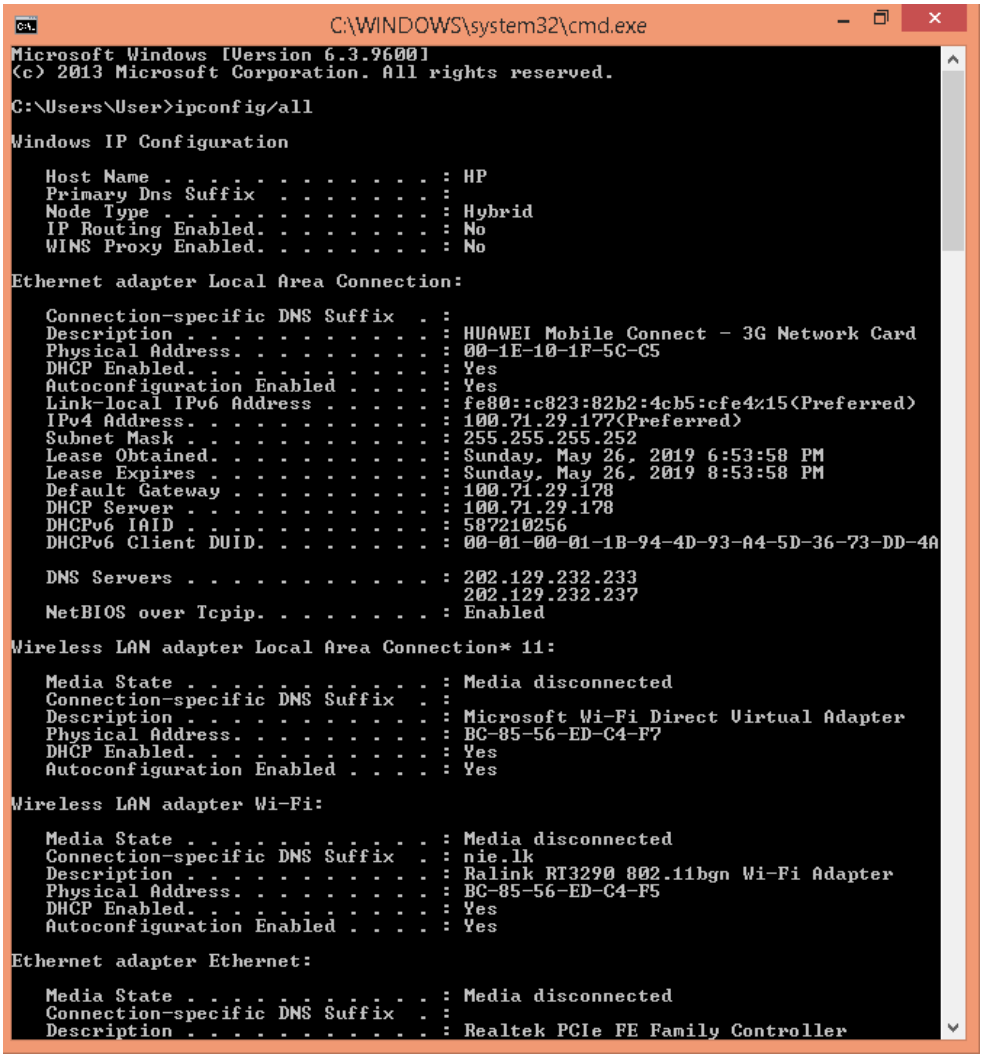
MAC address is represented by Colon-Hexadecimal notation. But this is just a conversion, not mandatory. MAC address can be represented using any of the following formats –



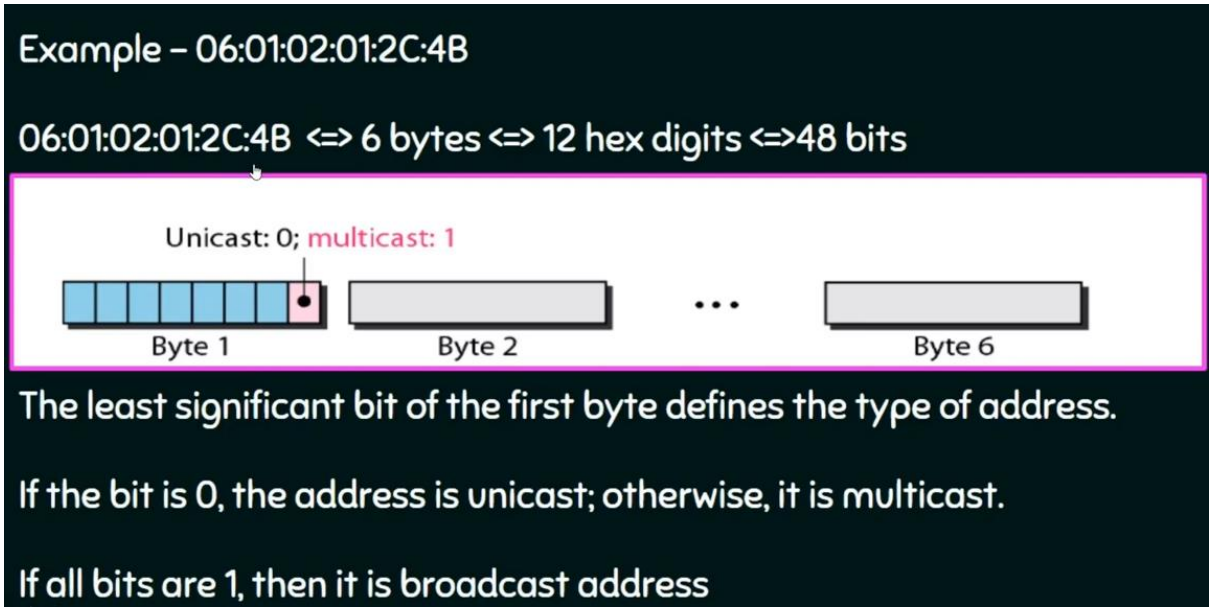
Colon-Hexadecimal notation is used by *Linux OS* and Period-separated Hexadecimal notation is used by *Cisco Systems*.

How to find MAC address –

Command for UNIX/Linux	-	*ifconfig -a*
Command forWindows OS	-	*ipconfig /all*
MacOS	-	*TCP/IP Control Panel*

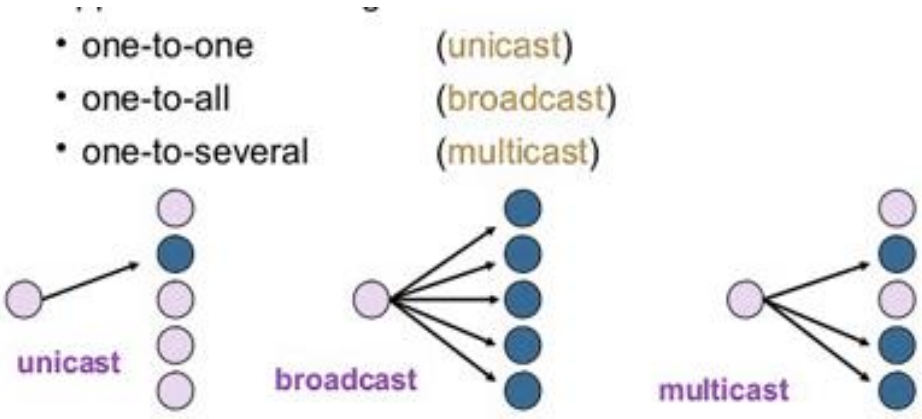


LAN technologies like Token Ring, Ethernet use MAC Address as their Physical address but there are some networks (AppleTalk) which does not use MAC address.



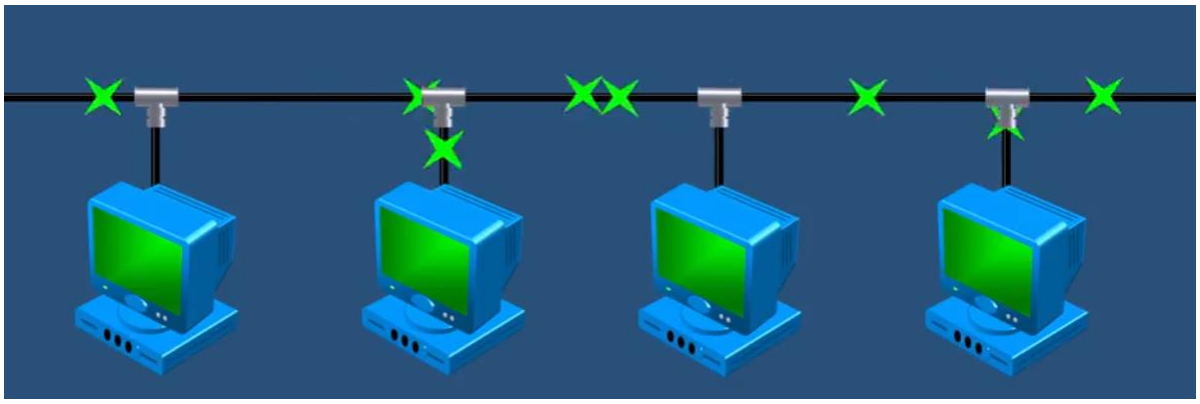
Types of Messages

Three different methods of sending messages over computer networks. Those methods are **unicast**, **multicast** and **broadcast**.

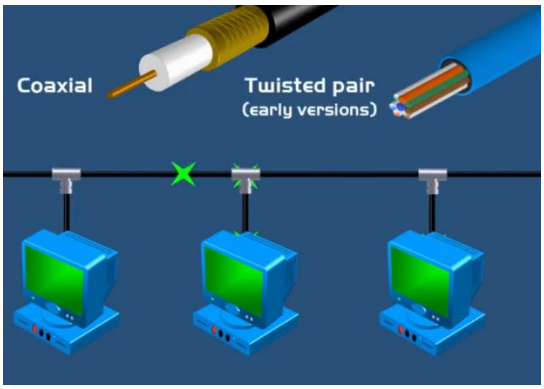


In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

How computers send data without interfering with data from other computers?

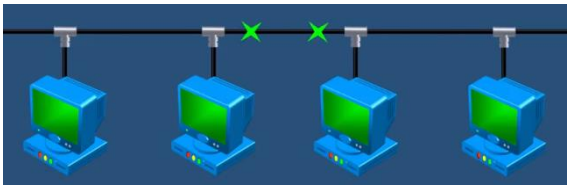


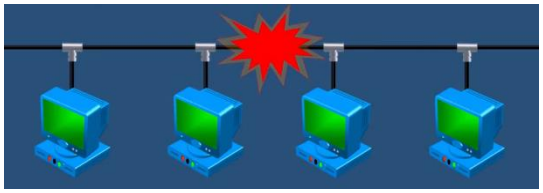
- In older computers, **a technology** was developed not only to help avoid collisions, but also to report correctly if a collision does happen.
- This technology is called **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**.
- CSMA/CD used on early Ethernet networks and utilized coaxial cables and early versions of twisted pair cables.



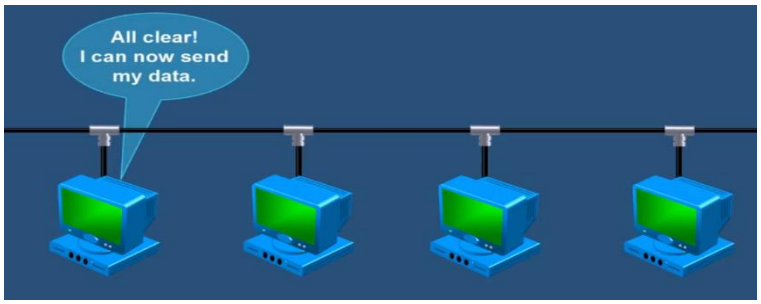
How CSMA/CD works?

- Each computer first senses if the wire is idle. If the wire is idle, it sends its data.
- But if two computers send data at the same time, a collision will happen.

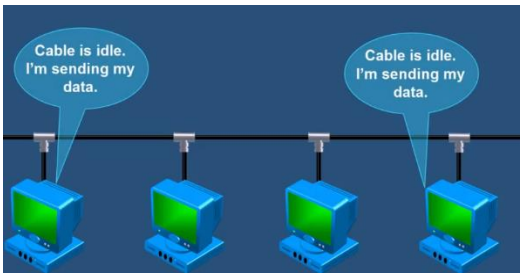


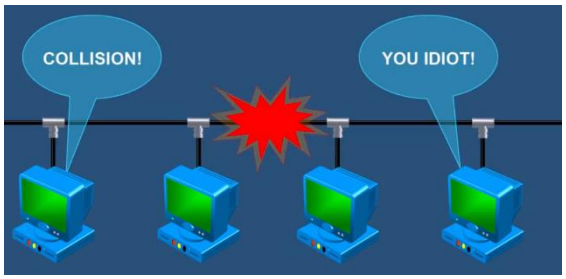


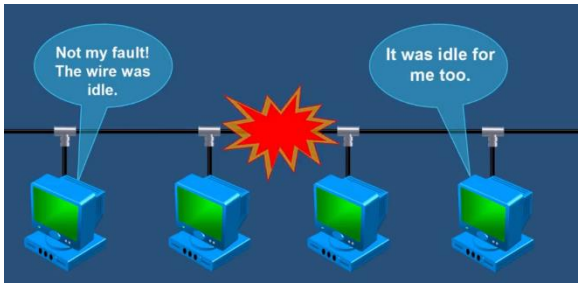
- When collision happens, computers will wait random amount of time and retry to send the data.
- CSMA/CD defines what station can talk at any particular time, and what to do if two or more stations talk at the same time. (**Set of rules**)
- A computer first listens to the network media. If the media is idle, the computer sends its data (**Carrier Sense**).



- Priorities are not assigned to particular stations (**Multiple access**)

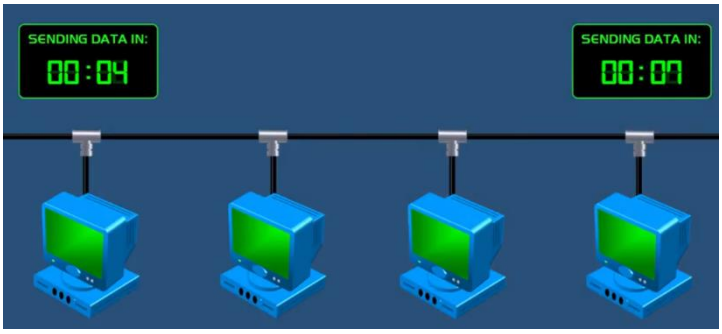


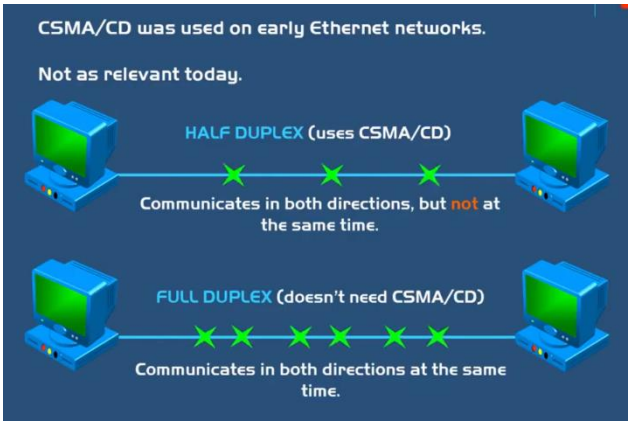




- A collision occurs when two stations listen for network traffic, hear none, and transmit simultaneously (**a collision**).

- In a collision, stations are altered of the collision, and they execute a back off algorithm that randomly schedules retransmission of the frame. (**Collision detection**)





Reference

https://www.geeksforgeeks.org/computer-network-introduction-mac-address/
https://techterms.com/definition/macaddress
https://www.techopedia.com/definition/5301/media-access-control-address-mac-address