Explores the role of Media Access Control (MAC) protocol

6.6 Learning Outcomes:

- Describes the need to uniquely name devices (addresses) so that the sender and the receiver can be identified
- Explains the role of frames as the unit of transmission
- Describes the need of a protocol to ensure orderly access to media with respect to a bus
- Briefly describes the evolution of MAC protocols from ALOHA to Ethernet

Contents:

- Local Area Network (LAN)
- Identifying devices
  - Addresses – MAC addresses
- Frames
  - Orderly access to the media
  - Very simple protocol as an example – ALOHA
- Improvements from ALOHA to Ethernet
- Broadcasting and unicasting messages

Local Area Network (LAN)

- A local area network (LAN) is a collection of devices connected together in one physical location (computers within a limited area), such as a building, office, or home.
- The most common LAN design since the mid-1970s has been the bus-connected Ethernet, originally developed at Xerox PARC
- They are limited to a specific geographical area, usually less than 2 kilometers in diameter.

- In LAN connection we can
  1. Share resources
     Ex- printer, Scanner
  2. Easy to communicate
  3. File sharing ability
  4. Ability to secure files

- Identifying devices
  When transmitting data on a network it is essential to find out what are devices connected to the network
- What are devices sending data and what are devices receive data is essential to know
- To identify devices we can use 2 separate ways
  1. IP address (Logical address)
  2. Physical address (media Access control)

1. **IP address – (user can obtain this address)**
   - it is not a permanent address.it is temporarily
   - if necessary even a permanent address could be obtained

,

2. Physical address (media Access control)

- A MAC address is given to a network adapter when it is manufactured.
- It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it.
- The ARP (Address Resolution Protocol) translates an IP address into a MAC address.
- The ARP is like a passport that takes data from an IP address through an actual piece of computer hardware.
- It is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

- All devices on the same network subnet have different MAC addresses. MAC addresses are very useful in diagnosing network issues

- MAC addresses are useful for network diagnosis because they never change, as opposed to a dynamic IP address, which can change from time to time.

- For a network administrator, that makes a MAC address a more reliable way to identify senders and receivers of data on the network.

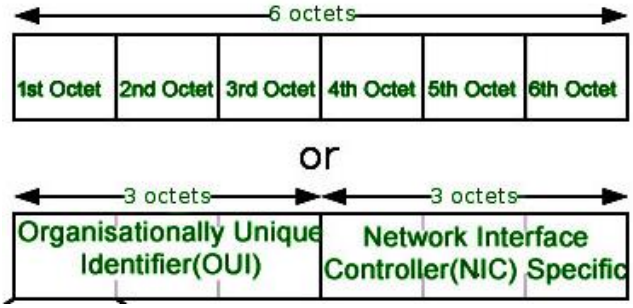
How to find the MAC address

- MAC address is used by Media Access Control (MAC) sub layer of Data-Link Layer.
- MAC Address is word wide unique, since millions of network devices exists and we need to uniquely identify each.
- MAC addresses are made up of six two-digit hexadecimal numbers, separated by colons.
    - example, an Ethernet card may have a MAC address of **00:0d: 83:b1:c0:8F**
- Each two digit divide in to 8bits

Example 83=1000 0011

Mac address is divide in to 2 parts

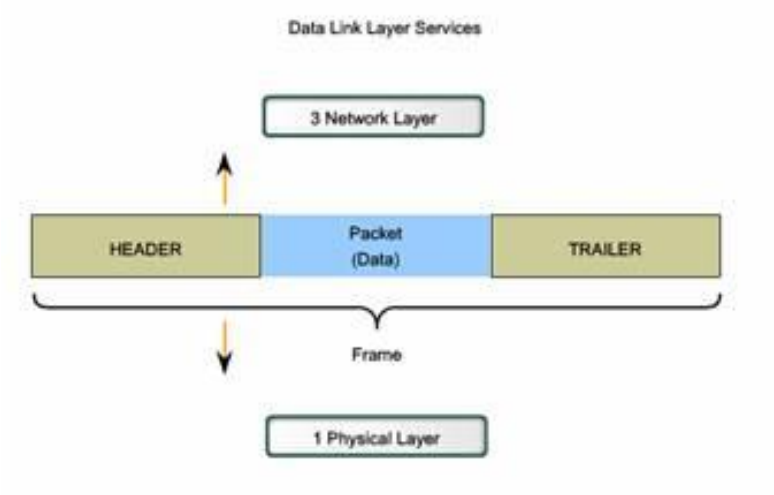
1. First three parts for manufacture
2. Second 3 parts for NIC



- Here are some OUI(**Organizational Unique Identifier**) 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**

Frames

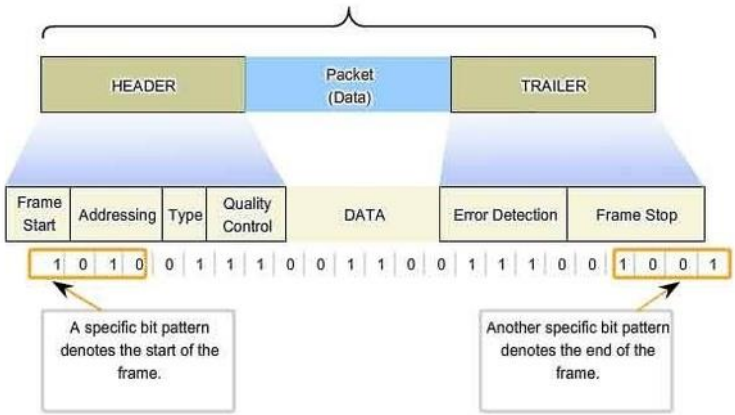
- When data is generated at the source to be sent to the receiver over the communication link, at the Data link layer, data are encapsulated in to the Frame,
- Where the data is inserted in to the frame and the MAC addresses of the sending device and the MAC address of the adjacent node are included in the header of the frame.
- Each frame is made depending on the quality of the link connecting a pair of devices.
- If the frame size becomes too large, then the packet may be divided into small sized frames.
- At receiver' end, data link layer picks up signals from hardware and assembles them into frames.



General Structure of a Frame

- **Frame Header:** It contains the source and the destination addresses of the frame and the control bytes.
- **Addressing** – It is used by the MAC sub layer to identify the source and destination nodes.
- **Type** – It is used by LLC to identify Layer 3 Protocols (mostly IP)
- **Payload field:** It contains the message to be delivered.
- **Trailer:** It contains the error detection and error correction bits. It is also called Frame Check Sequence (FCS).
- **Flag:** Two flag at the two ends mark the beginning and the end of the frame.

Formatting Data for Transmission



Describes the need of a protocol to ensure orderly access to media with respect to a bus

Bus topology

- Bus topology is the cheapest way of connecting computers to form a workgroup or departmental LAN, but it has the disadvantage that a single loose connection or cable break can bring down the entire LAN
- Termination is important issue in bus networks. The electrical signal from a transmitting computer is free to travel the entire length of the cable.
- Without the termination, when the signal reaches the end of the wire, it bounces back and travels back up the wire.
- When a signal echoes back and forth along an unterminated bus. The terminators absorb the electrical energy and stop the reflections.
- When data are transmitted from several devices to the transmission media data should be approached to the transmission media in a manner that they do not collide.

For this purpose **protocol was introduced**

A protocol

- A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.
- a communication network protocol defines the order and the format of data when the data is exchanged between two networking devices.
- Many protocols exist in the networking world and medium access control protocols 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.

MAC protocol

1. Pure ALOHA
2. Slotted ALOHA
3. CSMA/CD
4. CSMA/CA

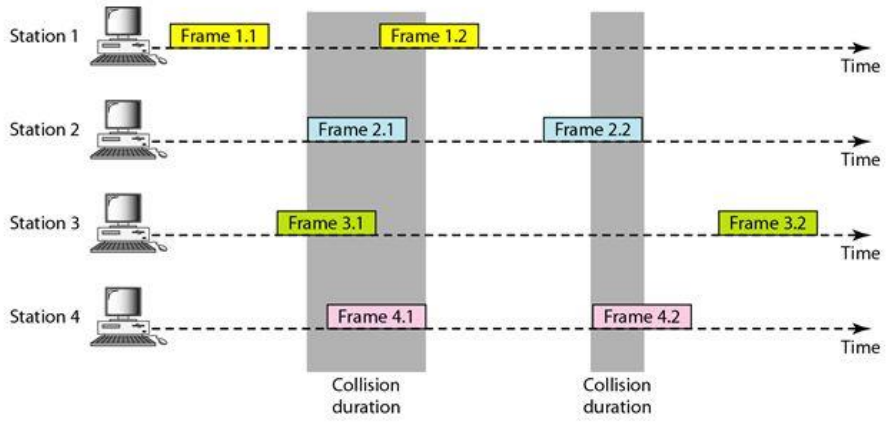
ALOHA

- ALOHA is a medium access control (MAC) protocol for transmission of data via a shared network channel.
- One of the early computer networking designs, development of the ALOHA network was begun in September 1968 at the University of Hawaii under the leadership of **Norman Abramson along with Thomas Gaarder, Franklin Kuo, Shu Lin, Wesley Peterson and Edward ("Ned") Weldon.**
- The goal was to use low-cost commercial radio equipment to connect users on Oahu and the other Hawaiian islands with a central time-sharing computer on the main Oahu campus.
- The first packet broadcasting unit went into operation in June 1971 ALOHA net, also known as the ALOHA System, or simply ALOHA, was a pioneering computer networking system developed at the University of Hawaii.
- ALOHA net became operational in June, 1971, providing the first public demonstration of a wireless packet data network
- Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.
- There are two types of ALOHA protocols – Pure ALOHA

  Slotted ALOHA.

1. Pure ALOHA

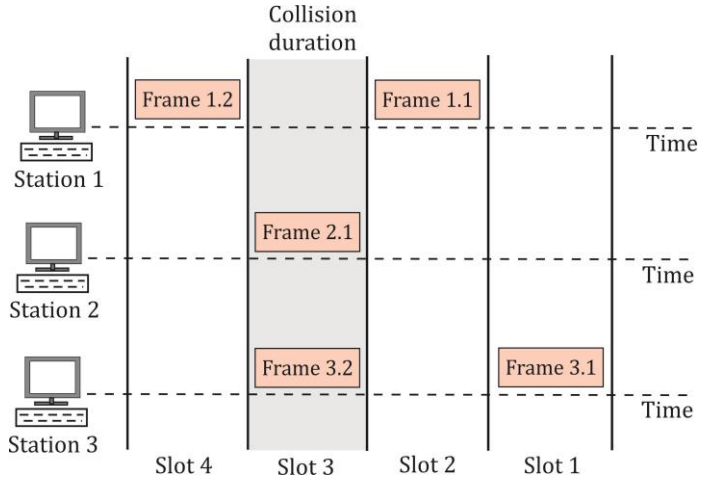
- The original ALOHA protocol is called pure ALOHA.
- When a network station needs to send the frame, it sends immediately and waits for the acknowledgment.
- If the sender receives an acknowledgment, the sender may send the next frame.
- If no acknowledgment sender assumes the frame has been garbled and retransmit the same frame after a random time to avoid collision again



- If a frame is damaged, then the stations wait for a random amount of type and retransmits the frame till it transmits successfully.
- The waiting time of the each station must be random and it must not be same just to avoid the collision of the frames again and again.

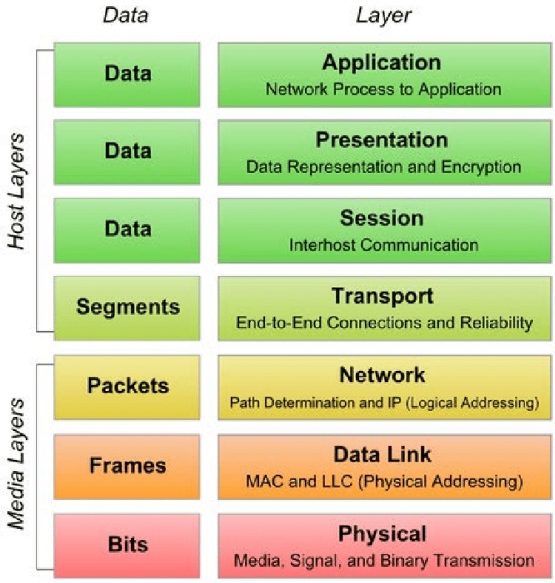
2. Slotted ALOHA

- The Slotted ALOHA requires that time be segmented into slots of a fixed length exactly equal to the packet transmission time.
- Every packet transmitted must fit into one of these slots by beginning and ending in precise synchronization with the slot segments.
- A packet arriving to be transmitted at any given station must be delayed until the beginning of the next slot.
- If more than one station transmit in the same slot, it will lead to collision. Slotted ALOHA reduces this collision in the network system.



Ethernet - logical bus topology

- **Ethernet** is a physical and data link layer technology for local area networks (LANs). **Ethernet was invented by engineer Robert Metcalfe.**
- The protocol introduce to transmit data between two devices of a local area network with a control is called Ethernet. This protocol name IEEE802.3
- Ethernet uses a bus or star topology and supports data transfer rates of 10Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards.
- Ethernet uses a protocol called CSMA/CD, this stands for Carrier Sense, Multiple Access with Collision Detection.



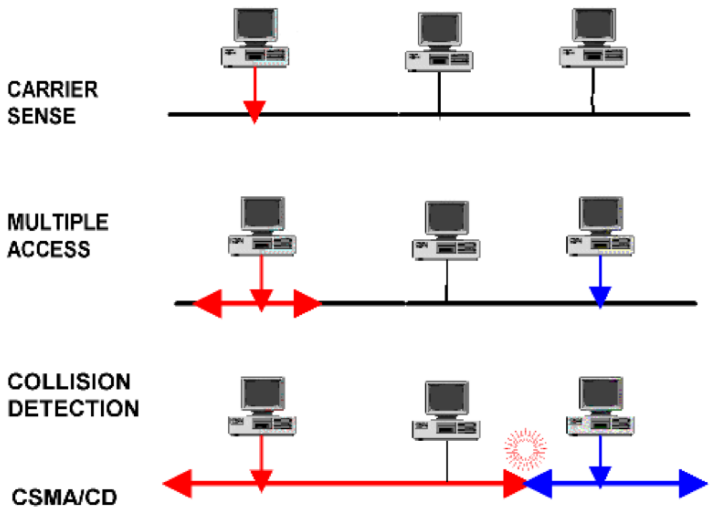
Carrier-sense multiple access with collision detection (CSMA/CD)

- Media access control (MAC) method used most notably in early Ethernet technology for local area networking. It uses carrier-sensing to defer transmissions until no other stations are transmitting.

- **Carrier Sense** - When a device connected to an Ethernet network wants to send data it first checks to make sure it has a carrier on which to send its data (usually a piece of copper cable connected to a hub or another machine).

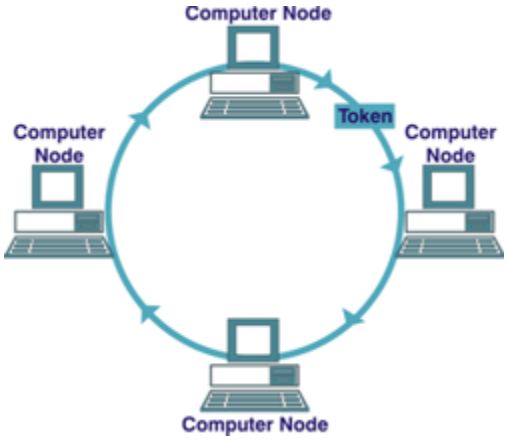
- **Multiple Access** - This means that all machines on the network are free to use the network whenever they like so long as no one else is transmitting.

- **Collision Detection** - A means of ensuring that when two machines start to transmit data simultaneously, that the resultant corrupted data is discarded, and re-transmissions are generated at differing time intervals



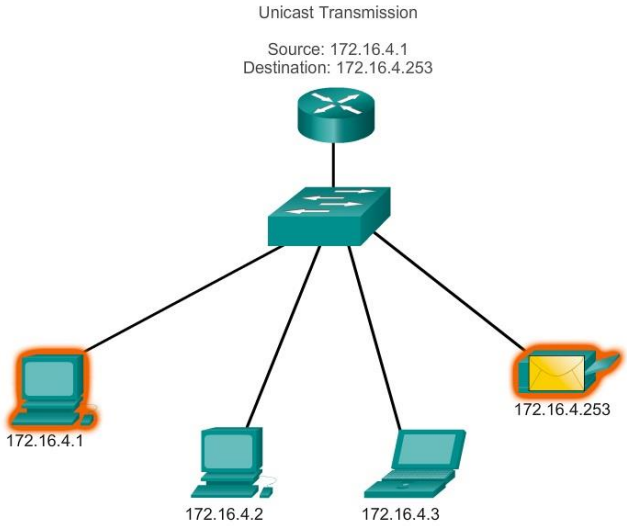
- **Token ring**

Token ring or **IEEE 802.5** is a network where all computers on the network are connected in a circle fashion. The term token is used to describe a segment of information that is sent through that circle; when a computer on the network is able to decode that token, the information is received on that computer. The token ring is used by ARCNET **(Attached Resource Computer NETwork)**, token bus and FDDI **(Fiber Distributed Data Interface).**



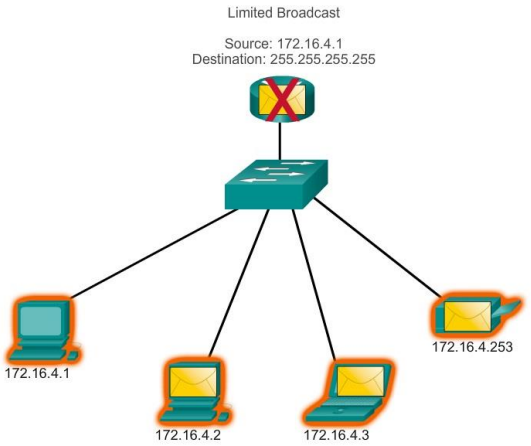
- In the mid-1980s, token ring LAN speeds were standardized between 4 and 16 Mbps.
- The token ring LAN process is delineated by the following sequence of events:
- A token continually circulates inside the token ring LAN
- To transmit a message, a node inserts a message and destination address inside an empty token.
- The token is examined by each successive node.
- The destination node copies the message data and returns the token to the source with the source address and a data receipt message.
- The source receives the returned token, verifies copied and received data and empties the token.
- The empty token now changes to circulation mode, and the process continues.

- There are different modes of transmission at network, and different challenges which need to be met by the source, route, and receiver of each transmission.
- Data is transported over a network by three simple methods
  1. Unicast,
  2. Broadcast
  3. Multicast.



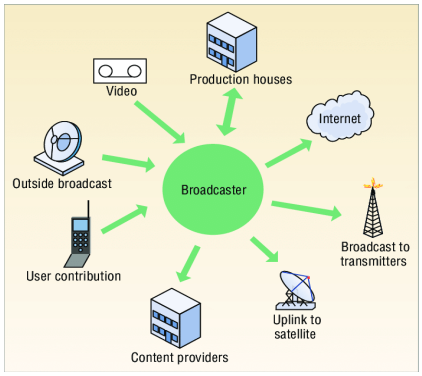
Unicast

- A unicast transmission is a one-to-one communication that passes from a single source to a single receiver or destination. One of the simplest everyday examples of unicast transmission would be a phone call between two people.
- Traffic, many streams of IP packets that move across networks flow from a single point, such as a website server, to a single endpoint such as a client PC. This is the most common form of information transference on networks.



Broadcast:

- Traffic streams from a single point to all possible endpoints within reach on the network, which is generally a LAN. This is the easiest technique to ensure traffic reaches to its destinations.
- This mode is mainly utilized by television networks for video and audio distribution. Even if the television network is a cable television (CATV) system, the source signal reaches to all possible destinations, which is the key reason that some channels' content is scrambled. Broadcasting is not practicable on the public Internet due to the massive amount of unnecessary data that would continually reach at each user's device, the complications and impact of scrambling and related privacy issues.



Multicast

- In this method traffic recline between the boundaries of unicast (one point to one destination) and broadcast (one point to all destinations).
- And multicast is a “one source to many destinations” way of traffic distribution, means that only the destinations that openly point to their requisite to accept the data from a specific source to receive the traffic stream
- Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points
- In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers, or any other number of receivers).
- This poses a major salability issue for applications which required sustained high bandwidth. One way to significantly ease scaling to larger groups of clients is to employ multicast networking.
-