UNIT II

PHYSICAL LAYER AND DATA LINK LAYER

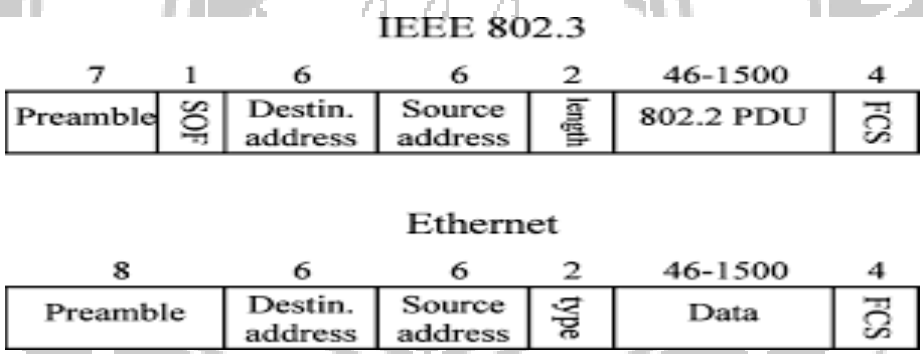
MAC Protocols & Ethernet Standards

MAC protocols and Ethernet standards are related concepts in computer networking where Ethernet standards define the physical and data link layer's architecture, and MAC protocols govern how devices access the shared physical medium to transmit data. Ethernet standards, such as the IEEE 802.3 suite, define speeds like Fast Ethernet (100 Mbps) and Gigabit Ethernet (1 Gbps), while the MAC sublayer within this standard uses protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) to manage data transmission and prevent collisions.

Ethernet Standards (IEEE 802.3)

Ethernet is a family of networking technologies that uses specific standards to define how to send data over a network.

- **Architecture:** The Ethernet protocol is divided into two sublayers: the MAC sublayer, which handles access control and addressing, and the Logical Link Control (LLC) sublayer, which handles error control and communication with upper-layer protocols.



Ethernet and IEEE 802.3 MAC frames

- **IEEE Standards:** The IEEE 802.3 standard is the most common for Ethernet, defining different versions of Ethernet, including:
  - **10BASE-T:** 10 Mbps over twisted pair.
  - **Fast Ethernet (100BASE-T):** 100 Mbps over twisted pair.

- **Gigabit Ethernet (1000BASE-T):** 1 Gbps over twisted pair.
- **10 Gigabit Ethernet:** 10 Gbps over fiber or copper.

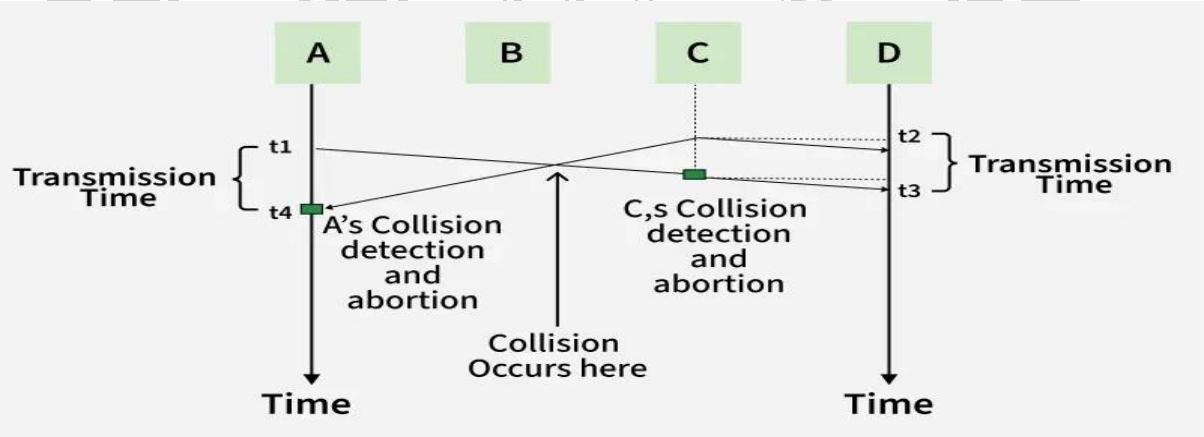
- **Frame Format:** An Ethernet frame includes a preamble, destination and source MAC addresses, a type/length field, the data itself, and a Frame Check Sequence (FCS) for error detection.

MAC Protocols

MAC protocols are the specific rules that devices follow to access a shared network medium without causing data loss.

- **Function:** They specify how to format packets, address devices (using MAC addresses), and regulate the timing of transmissions.
- **CSMA/CD (Carrier Sense Multiple Access with Collision Detection):** The primary MAC protocol for traditional Ethernet, especially in wired networks.

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs, when there used to be shared Bus Topology and each node (Computers) was connected by Coaxial Cables.



Working:

Step 1: Check if the sender is ready to transmit data packets.
Step 2:

- Check if the transmission link is idle.
- The sender has to keep on checking if the transmission link/medium is idle.
- For this, it continuously senses transmissions from other nodes.
- The sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment.

- If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

Step 3:

- Transmit the data & check for collisions.
- The sender transmits its data on the link.
- CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals.
- During transmission, if a collision signal is received by the node, transmission is stopped.
- The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame.
- After some random time, it again attempts to transfer the data and repeats the above process.

Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

- **ALOHA:** A random access protocol where devices send data without listening first, retrying after a random delay if a collision occurs.

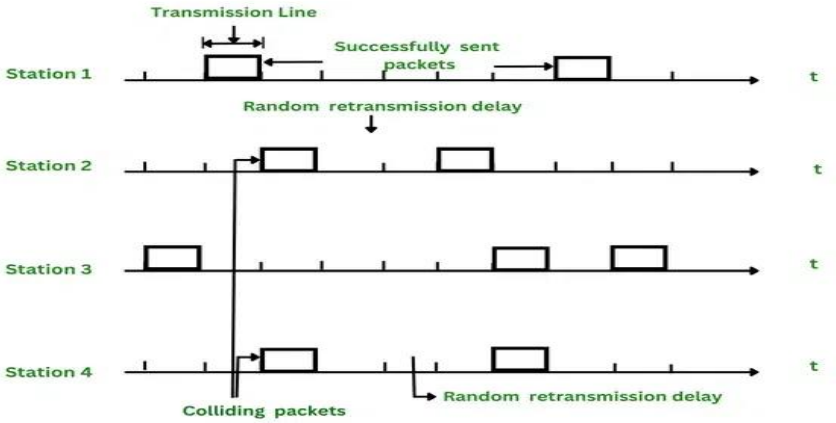
ALOHA is a random access protocol for computer networks that allows multiple devices to transmit data over a shared channel without coordination. Devices transmit whenever they have data, but if two or more devices transmit at the same time, a collision occurs, corrupting the data. To handle this, devices retransmit a corrupted frame after a random delay until it is successfully received.

How ALOHA works

- **Transmission:** A device sends a data frame whenever it has data to transmit, without first checking if the channel is busy.
- **Collision:** If two or more devices transmit at the same time, their frames collide and are corrupted.
- **Acknowledgment (ACK):** The receiver sends an acknowledgment if the frame is received correctly.
- **Retransmission:** If the sender does not receive an ACK within a specific time, it assumes a collision has occurred.
- **Random back-off:** The sender waits for a random amount of time before retransmitting the frame to avoid another immediate collision.

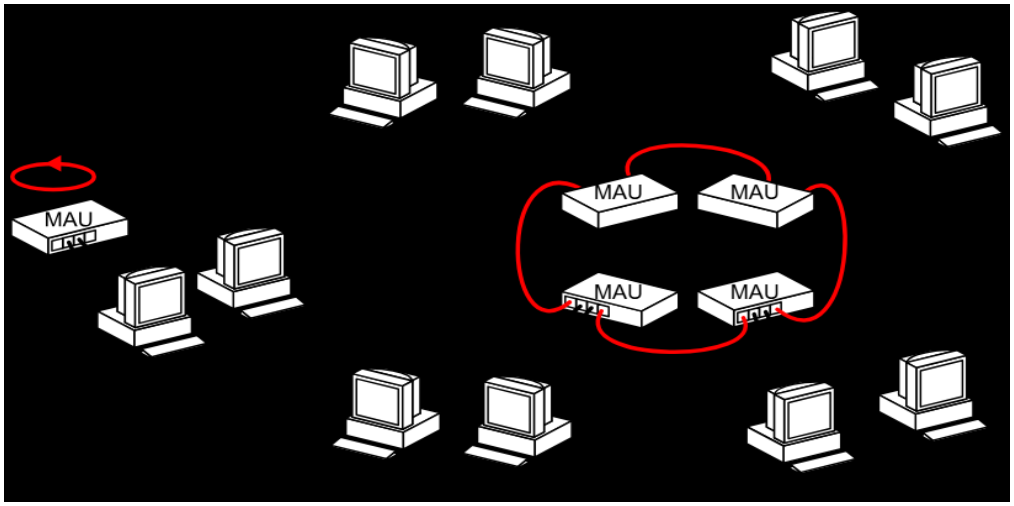
Types of ALOHA

- **Pure ALOHA:** The original version, where frames are transmitted continuously whenever data is available. The main drawback is the high probability of collisions, especially in networks with high traffic.
- **Slotted ALOHA:** A more efficient version that divides time into fixed-size slots. Devices can only transmit at the beginning of a time slot, which significantly reduces the number of collisions.



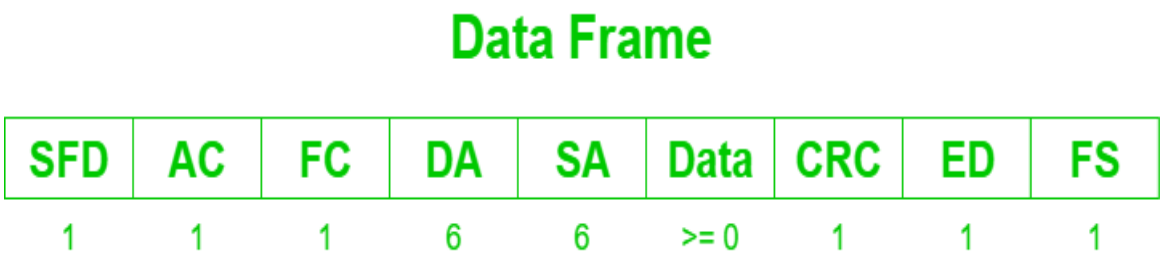
- **Token Ring:** A token-passing protocol where a special "token" circulates, and a device can only transmit data if it holds the token.

In a Token Ring network, frames have a specific format to ensure reliable and orderly communication among nodes. The Token Ring uses a token-passing protocol for access control, and each frame follows a standardized structure as defined in IEEE 802.5.



Structure of a Token Ring Frame

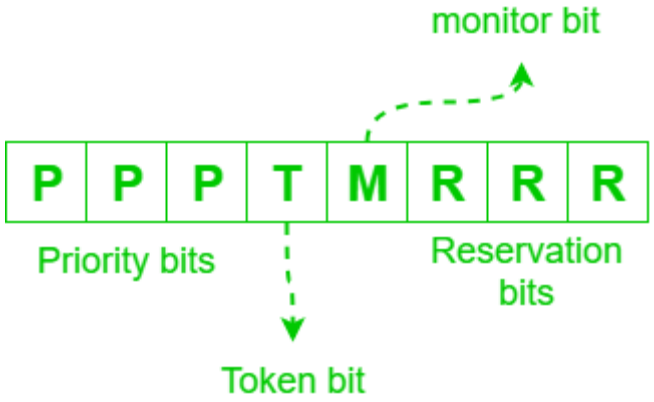
Token Ring is a networking technology where devices are connected in a logical ring. Communication is controlled by a special frame called a token. When a device holds the token, it can transmit data. A Token Ring frame has a specific format to ensure that data is transferred accurately and efficiently.
It consists of the following elements in the structure of the token ring format :



Token Ring Format

Start Delimiter (SD) 1 Byte : Used for the marking the beginning of the frame. This has a unique bit pattern so that the receiving station knows exactly when a new frame starts. It includes symbols to indicate timing and frame synchronization.
Access Control (AC) 1 Byte : Used to manage token passing and transmission control. Fields Include:

- **Priority bits (3 bits):** Used to determine the priority of the frame.
- **Token bit (T):** Indicates whether the frame is a token or data.
- **Monitor bit (M):** Ensures only one token exists in the ring.
- **Reservation bits (3 bits):** Allow a station to reserve the token for higher priority transmissions.



Access Control

Frame Control (FC) 1 Byte : It identifies the type of frame being transmitted. It helps devices interpret the rest of the frame correctly. First 2 bits indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.Types:

- **Data Frame:** Carries user data.
- **MAC Frame:** Used for control purposes such as ring maintenance.

- **CSMA/CA:** Used mainly in wireless networks, where devices listen before sending and use a method to "back off" if they detect a transmission to avoid collisions.

Carrier Sense Multiple Access (CSMA) is a method used in computer networks to help devices share a communication channel without interfering with each other. Before a device sends data, it listens to the channel (or senses the carrier) to check if it's free.

- If the channel is busy, the device waits until it becomes idle.
- This helps prevent data collisions, which can happen when two devices try to send data at the same time.
- CSMA is widely used in networking technologies like Ethernet and Wi-Fi.

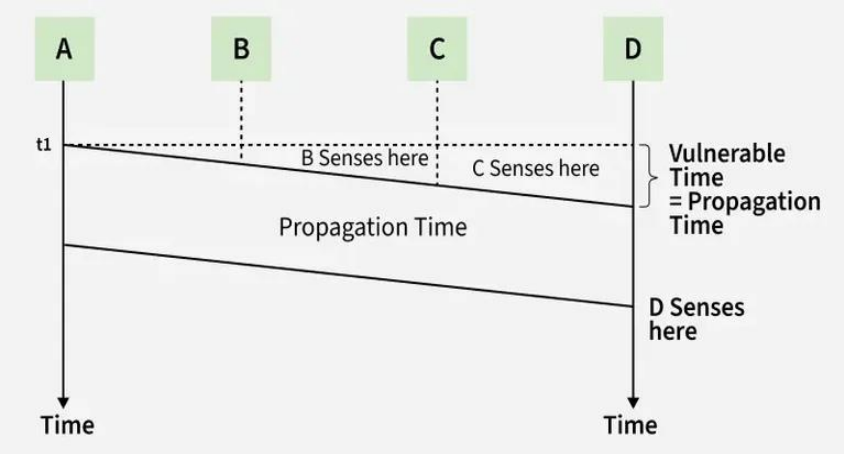
Types of CSMA Protocol

There are two main types of Carrier Sense Multiple Access (CSMA) protocols, each designed to handle how devices manage potential data collisions on a shared communication channel. These types differ based on how they respond to the detection of a busy network:

1. CSMA/CA
2. CSMA/CD

Vulnerable Time in CSMA

Vulnerable time is the short window in which there's a risk of collision between two devices trying to send data on the network at the same time. In CSMA-based networks like Ethernet or Wi-Fi, each device listens to the channel before transmitting.



- If the channel seems free, the device waits a tiny moment and then begins sending.
- However, another device might also sense the channel as free at the same time and they both may start transmitting causing a collision.
- This small time window, where such collisions can still happen even after sensing, is called the vulnerable time.

What is CSMA/CA?

- CSMA/CA is a medium access control (MAC) protocol that prevents data collisions in wireless communication.
- It works by avoiding collisions before they occur.
- This is necessary because, in wireless systems, detecting collisions is difficult due to the high energy required for transmission compared to receiving.
- Thus, CSMA/CA forms the backbone of Wi-Fi (IEEE 802.11) and other wireless technologies.

Why is CSMA/CA Needed?

- In wired networks, devices can detect collisions (CSMA/CD).
- In wireless networks, detecting collisions is nearly impossible because, the transmitting device cannot listen to the channel while sending. Signal interference, noise and hidden terminal problems make detection unreliable.
- Hence, CSMA/CA focuses on collision prevention rather than collision detection.

Working Principle of CSMA/CA

The CSMA/CA protocol ensures that before a device transmits, it checks if the communication channel is free and then uses additional strategies to minimize collision chances.

Process Steps:

1. **Initialize Attempt Counter (K = 0):** Each device keeps track of retransmission attempts.
2. **Sense the Channel:** The device listens to see if the channel is busy, If busy -> Wait until it becomes free.
3. **Interframe Space (IFS):** After the channel is idle, the device waits for a short fixed time.

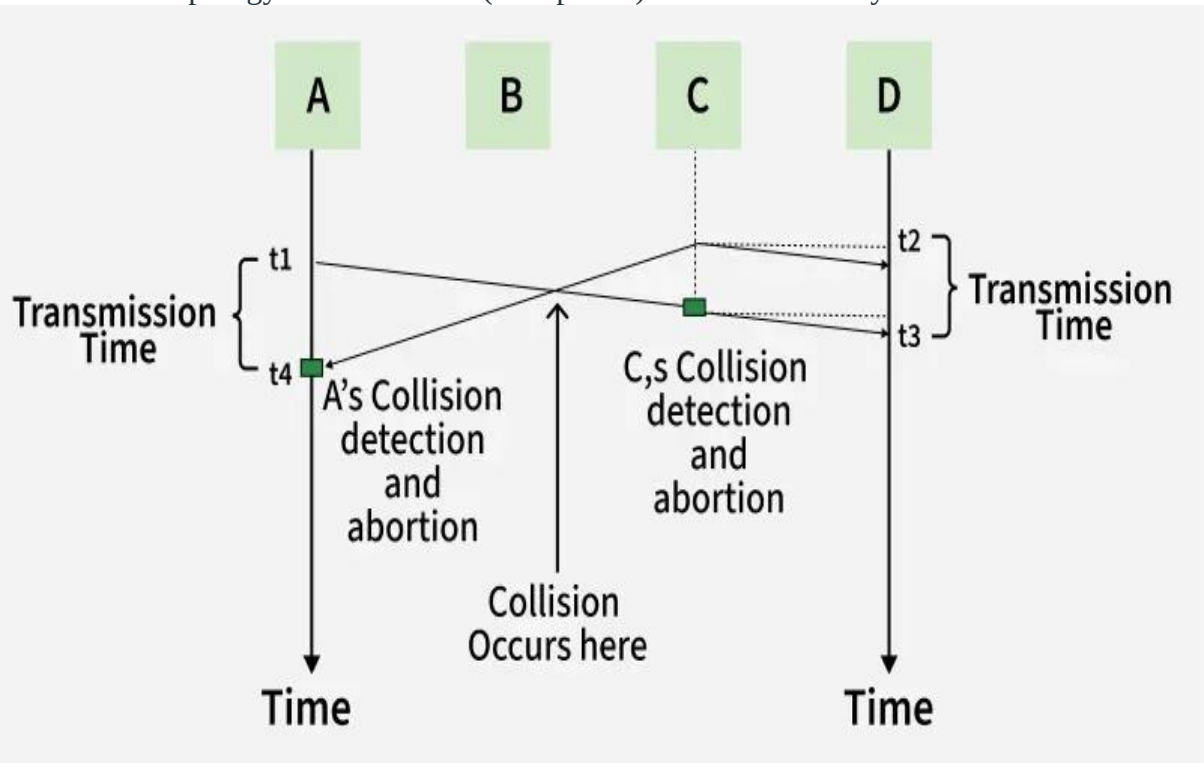
4. **Check Again:** If still idle after IFS, continue; otherwise, repeat sensing.
5. **Random Backoff:** Choose a random number R in a contention window to delay transmission.
6. **Transmit Data Frame.**
7. **Wait for Acknowledgment (ACK):** If ACK received -> Success & If ACK not received -> Assume collision, retry (K=K+1)(*K*=*K*+1).
8. **Retry Limit:** If attempts exceed maximum Kmax*Kmax*, abort transmission.

Strategies Used in CSMA/CA

1. **Interframe Space (IFS):** A short waiting period after the channel becomes idle to avoid immediate collisions. Devices with shorter IFS have higher priority.
2. **Contention Window:** A device waits for a random number of time slots before transmission, reducing the chance of simultaneous access.
3. **Acknowledgments (ACKs):** The receiver sends back an acknowledgment if data is received correctly. If no ACK is received, retransmission occurs.
4. **RTS/CTS Mechanism (Optional):** Request-to-Send (RTS) -> Sender asks for permission. Clear-to-Send (CTS) -> Receiver replies if the channel is clear.

Collision Detection in CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs, when there used to be shared Bus Topology and each node (Computers) was connected by Coaxial Cables.



How Does CSMA/CD Work?

Step 1: Check if the sender is ready to transmit data packets.
Step 2:

- Check if the transmission link is idle.
- The sender has to keep on checking if the transmission link/medium is idle.
- For this, it continuously senses transmissions from other nodes.
- The sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment.
- If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.

Step 3:

- Transmit the data & check for collisions.
- The sender transmits its data on the link.
- CSMA/CD does not use an 'acknowledgment' system. It checks for successful and unsuccessful transmissions through collision signals.
- During transmission, if a collision signal is received by the node, transmission is stopped.
- The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame.
- After some random time, it again attempts to transfer the data and repeats the above process.

Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.