Hi, my name is Nor Arni Zuraimi

The objective of this ……. is understand medium access control (MAC).

Let's us begin by watching this short video…..

This is the scenario in a classroom while waiting for the arrival of the next lecturer. The class is so noisy, everybody seem talking to each other without someone lead the class. The situation continue until the next lecturer came for the session.

Well, did you gain something from the previous video? Hopefully you can relate with what we are going to do next.

At the end of this learning session, you must be able to identify the importance of MAC. You must also be able to explain types of MAC particularly Carrier Sense Multiple Access/Collision Detection (CSMA/CD), Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) and Token Passing.

Hope you will enjoy watching this ……

Have you ever heard of Medium Access Control or MAC.

Medium Access Control or MAC is refers to technology or technique that controls access to media or channel.

It is a sublayer of the data link layer (DLL) in the seven-layer Open System Interconnection or OSI network reference model. What is OSI?.

OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network.

In general, MAC is responsible for the transmission of data packets.

Now let's take a look at OSI Reference Model.

OSI layers contain seven layers which are :

- **Layer 1: Physical Layer**
- **Layer 2: Data link Layer**
- **Layer 3: Network Layer**
- **Layer 4: Transport Layer**
- **Layer 5: Session Layer**
- **Layer 6: Presentation Layer**
- **Layer 7: Application Layer**

Data Link Layer is divided into two sublayers:

a. **Logical Link Control (LLC)**

b. **Medium Access Control (MAC)**

LLC sublayer is responsible for error and flow control.

While MAC sublayer is responsible for framing, addressing mechanism and channel access so that each node available on a network can communicate with other nodes available on the same or other networks.

Why MAC is so important in a network?

Here we can identify the Importance of Media Access Control (MAC) :

1. **MAC is a protocol or a set of rules, used to access the media in a shared network in order to avoid or detect a collision.**
2. **MAC is a set of rules that determines when a station can use the medium, what a station should do when the medium is busy and what the station should do when it is involved in collision.**
3. **MAC is necessary to ensure that systems on the network can communicate with each other and to ensure that everyone gets an opportunity to use the network.**

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer.

Here, we are going to discover three types of media access control. The three types are:

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**
- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**
- **Token passing**

Before we go on, let's take a look at Carrier Sense Multiple Access – CSMA

Carrier sense (CS) means the device or the station that would be communicating on the network is listening to the channel to determine if someone else is transmitting. And if there is someone else transmitting, then that device is not going to transmit at that time. If the channel is free or no station is transmitting any data, then the station may proceed to transmit the data.

Multiple access (MA) means that multiple stations or devices send and receive on the medium and are connected in the network. Transmissions by one node are generally received by all other stations connected to the medium. They are going to try to communicate together and they are going to use CSMA to be able to do that.

Do you have a clear understanding of CSMA?

Alright then, let's move on further to Carrier Sense Multiple Access/Collision Detection

Carrier sense multiple access/collision detection (CSMA /CD) is one of the most popular access methods in use today.

Ethernet uses CSMA/CD to manage media access, as defined in the IEEE 802.3 specification. CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

How does the station detect the collision? As you know, the station will always monitor the media while transmitting. If the observed power is more than the transmitted power of its own signal, it means collision occurred.

In CSMA/CD access method, every station has equal access to the channel or media and can place the data on the media or can send the data when the media is free from traffic.

When a station has data to send, it will first 'listens' or 'senses' the media/channel to determine if there is a signal or traffic already on the channel. If there is traffic already on the channel, the station will wait until it become idle before transmitting the data and if there is no traffic, the station will transmit the data.

If there are two stations on the channel that "sense" the channel at the same time, they will both send data out at the same time if the medium is free. When the two station transmit at the same time, they will collide with one another, and the data will be destroyed. When this occurs a collision will take place, and then a jamming signal is sent throughout the network in order to notify all stations of the collision.

What is a jam signal? A jam signal is a signal that carries a 32-bit or 48-bit binary pattern sent by a transmitting station to inform the other stations that they must not transmit.

If the data is destroyed during transmission, the data will need to be retransmitted.

After collision, each station will wait for a small interval of time referred to as the 'back-off'and again the data will be retransmitted at the different time, to avoid collision again. So now one station begin to transmit, the other station can now hear it since it has carrier sense and it will only transmit when the other has done.

Let's have a look at this animation.

In this illustration, we have a four computer on a CSMA/CD bus network. Computer A wants to send a packet to Computer D.

Station A will first listen or sense the media/channel to see if any other station transmitting. If no other station is transmitting, A sends the frame out of the network. When A send the packet, all of the station can see the transmission. Station A will now listens to its own transmission to see if it returned exactly the way it was sent out.. If A detects no collision, everything is assumed to be successful and D receives the packet. Then the transmission process completed.

Now look at this scenarios. And again we have a four Computer on a CSMA/CD bus network. Computer A wants to send a packet to workstation D at the same time that D want to transmit to Computer C.

Both of the station listen at the time to see anyone else is transmitting. Here, both A and D sense that the communication channel is free. After being confirm that the channel is free, both A and D send their packets out on the network at the same time.

Now, all the data in both frame is now destroyed. Both A and D listen to their own transmission to see if they returned exactly the way it was sent out.

Now A and D detect a collision. Both must now try again after waiting a random period of time. When A's random time is up and it must check again to see the channel is clear.

Every station 'sees' the transmission and D still waiting to transmit the data. D's random wait is over now. D now will listen to see if the channel is clear. If no one else is transmitting, then D sends the packet on the network.

Every station see the transmission and D checks for collision. If no collision detected, the transmission proses ends.

You may also visualize CSMA/CD in a flowchart form.

Let's take a look at this illustration of CSMA/CD

At the beginning, both station will first 'listens' or 'senses' to determine if there is a traffic on the channel/medium.

If the channel is free from traffic, at time t=0, a frame is sent on the idle medium by station A.

A short time later, station B also transmits. (In this case, the medium, as observed by station B happens to be idle too, in which A and B sense the medium at the same instant).

After a period, equal to the propagation delay of the network, the station B detects the other transmission from A, and is aware of a collision, but station A has not yet observed that station B was also transmitting. B continues to transmit, sending the Jam signal (32 bits or 48 bits).

After one complete round trip propagation time (twice the one way propagation delay), both station are aware of the collision. B will shortly cease transmission of the Jam signal, however A will continue to transmit a complete Jam signal. Finally the medium becomes idle.

So, how does it going so far?

Next, let us move on to the second type of CSMA which is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CD)

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) is an access method uses signal avoidance rather than detection. CSMA/CA acts to prevent collisions before they happen. This access method is used in Wireless LAN (WLAN), particularly the 802.11 wireless standards.

The CSMA/CA access method uses a "listen before talking" strategy. Any system wanting to transmit data must first verify that the channel is clear before transmitting, thereby avoiding potential collisions.

In CSMA/CA, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called interframe space or IFS.

Now let's have a look at the algorithm of CSMA/CA

Before a station sending a frame, it first sense the medium to determine if another station is transmitting. If the medium is free or idle, the station waits for a periode of time called the distributed interframe space (DIFS), then the station sends a control frame called the request to send (RTS). After receiving the RTS and waiting a periode of time called the short interframe space (SIFS), the destination station sends a control frame , called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.

The source station sends data after waiting an amount of time equal to SIFS. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been arrived.

Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination.

Now , you also can visualize CSMA/CD in a flowchart form.

Now, we come to the third type of MAC ,Token Passing

In a token-passing method, the station in a network are organized in a logical ring.

Token is a special control frame on token ring networks that determines which stations can transmit data on a shared network. The node that has the token can transmit the data.

A station wishing to transmit must wait until it detects a token passing by. It then seizes the token by changing one bit in the token, which transforms it from a token to a start-of-frame sequence for a data frame. The station then appends and transmits the remainder of the fields needed to construct a data frame.

When a station seizes a token and begins to transmit a data frame, there is no token on the ring, so other stations wishing to transmit must wait. The frame on the ring will make a round trip until and be absorbed by the transmitting station.

Then the transmitting station will insert a new token on the ring when the station has completed transmission of its frame. Once the new token has been inserted on the ring, the next station wishing to transmit the data will be able seize the token and transmit the data.

Now let's observed this animation.

As we have noticed earlier, token is passed around the network. Only the computer that hold the token can transmit data. As soon as the computer on the token ring network goes online, the network generate the token.

This token is passed around the every computer on the ring until one of the computer takes control of it. As soon as the computer has captured or seized the token, it sends out the data frame to the network. This frame is passed around the ring until it reach to the computer whose address matched the destination of the frame.

This frame is then copied by the destination computer and marked to indicate the data has reached its destination.

Then the frame is passed around the ring again until it get back to the same computer or the sender. When the transmission is confirm successful then the frame is deleted. After that, the same computer or the previous sender send out a new token to the ring, so that the other computer can transmit their data as well.

Now, let's look at this simplified algorithm.

Any device that wanted to transmit data had to wait until it received the token.

When the token has reached the station, the station can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.

The station can now transmit data. Data is transmitted in frames, and additional information, such as address, is attached to the frame in the form of headers and trailers.

While the token is in use by this station, other station cannot transmit the data. Because only one station at a time can use the token, no contention and no collision take place.