VARDHAMAN COLLEGE OF ENGINEERING
(AUTONOMOUS)
Affiliated to **JNTUH**, Approved by **AICTE**, Accredited by **NAAC** with **A++** Grade, **ISO 9001:2015** Certified
Kacharam, Shamshabad, Hyderabad – 501218, Telangana, India.

Department of Artificial Intelligence and Machine Learning

III B.Tech I Sem (R-22)
Course: CN (A8519)

UNIT-II

CHAPTER-II

MEDIUM ACCESS SUBLAYER

CHANNEL ALLOCATION PROBLEM

Introduction to Medium Access Control Sublayer:-

The protocols belong to sublayer of the Data Link Layer called MAC sublayer.

- Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- There are users quantity may vary at every time the process takes place.
- If there are N number of users and channel is divided into N equal sized sub channels, each user is assigned one portion.
- If the numbers of users are small and don't vary at times, then Frequency Division Multiplexing (FDM) can be used as it is a simple and efficient channel bandwidth allocating technique.
- There are two types of channel allocation problems
  (i) Static channel allocation
  (ii) Dynamic channel allocation

1. Static channel allocation:-

- ✓ It is the classical or traditional approach of allocating a single channel among multiple competing users using FDM. Eg: FM radio stations.
- ✓ If there are N users, the frequency channel is divided into N equal sized portions (bandwidth), each user assigned a portion.
- ✓ Since each user has a private frequency band, there is no interference between users.
- ✓ However, it is not suitable in case of large number of users with variable bandwidth requirements.
- ✓ It is not efficient to divide into fixed number of chunks.

2. Dynamic channel allocation:-

- ✓ In this scheme, frequency bands are not permanently assigned to the users. Instead, channels are allotted to users dynamically as needed, from a central pool.
- ✓ The allocation is done considering a number of parameters so that the transmission interference is minimized.
- ✓ This allocation scheme optimizes bandwidth usage and results is faster transmissions.
- ✓ Dynamic channel allocation is further divided into two categories.
  - (i) Centralized allocation
  - (ii) Distributed allocation

Assumptions for Dynamic Channel Allocation:-

1. Independent traffic
2. Single Channel
3. Observable collisions
4. Continuous or slotted time
5. Carrier sense or No carrier sense

1. Independent Traffic:-

- ✓ The model consists of N independent stations (computers, telephones), each with a program or user that generates the frames for transmission.
- ✓ The expected numbers of frames generated in an interval of length Δt is $\lambda\Delta t$, where λ is a constant (the arrival rate of new frames).
- ✓ Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

Note:- Poisson models are used to model independence assumption dur to its tractability.

2. Single Channel:-

- ✓ A single channel is available for all communication.
- ✓ All stations can transmit on it and all can receive from it.
- ✓ The stations are assumed to be equally capable, through protocols may assign them different roles. (priorities)

3. Observable Collisions:-

- ✓ If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is known as a collision.
- ✓ All stations can detect that a collision has occurred. A collided frame must be retransmitted.
- ✓ No errors other than those generated by collision occur.

4. Continuous or Slotted Time:-

- ✓ In continuous time case, frame transmission can begin at any instant.
- ✓ In discrete time case, time is slotted or divided into discrete intervals (called slots).
- ✓ Frame transmissions must begin at the start of a slot.

- ✓ A slot may contain 0,1 or more frames.
- ✓ For 0 - an idle slot, for 1 - a successful transmission, greater than 1 means collision.

5. Carrier Sense or No carrier Sense:-

- ✓ With the carrier sense assumption, stations can tell if the channel is in use before trying to use it.
- ✓ No station will attempt to use the channel while it is sensed as busy.
- ✓ If there is no carrier sense, station can't sense the channel before trying to use it.
- ✓ They will transmit then. Only later they can determine whether the transmission was successful.

MULTIPLE ACCESS PROTOCOLS

- ❖ If there is a dedicated link between the sender and the receiver then data link control layer is sufficient.
- ❖ If there are no dedicated link present then multiple stations can access the channel simultaneously.
- ❖ Hence multiple access protocols are required to decrease collisions.
- ❖ Multiple Access Protocols are broadly categorized into three types.
  (1) Random Access Protocols
  (2) Controlled Access Protocols
  (3) Channelization Protocols

Random Access Protocols:-

- ➢ In this all stations have same priority that is, no station has more priority than other station.
- ➢ Any station can send data depending on medium's state (idle or busy).
- ➢ In this method, each station has the right to the medium without being controlled by any other station.
- ➢ If more than one station tries to send, there is an access conflict (collision) and the frames will be either destroyed or modified.
- ➢ To avoid conflicts, each station follows a procedure.
  - When can the station access the medium?
  - What can the station do if the medium is busy?
  - How can the station determine the success or failure of the transmission?
  - What can the station do if there is an access conflict?
- ➢ The following are some of the random access protocols.
  (1) ALOHA
  (2) CSMA
  (3) CSMA/CA
  (4) CSMA/CD

Controlled Access Protocols:-

- ➢ In this scheme, the stations consult one another to find which station has the right to send.
- ➢ A station can't send unless it has been authorized by other stations.
- ➢ The following are some of controlled access protocols.

(1) Reservation
(2) Polling
(3) Token Passing

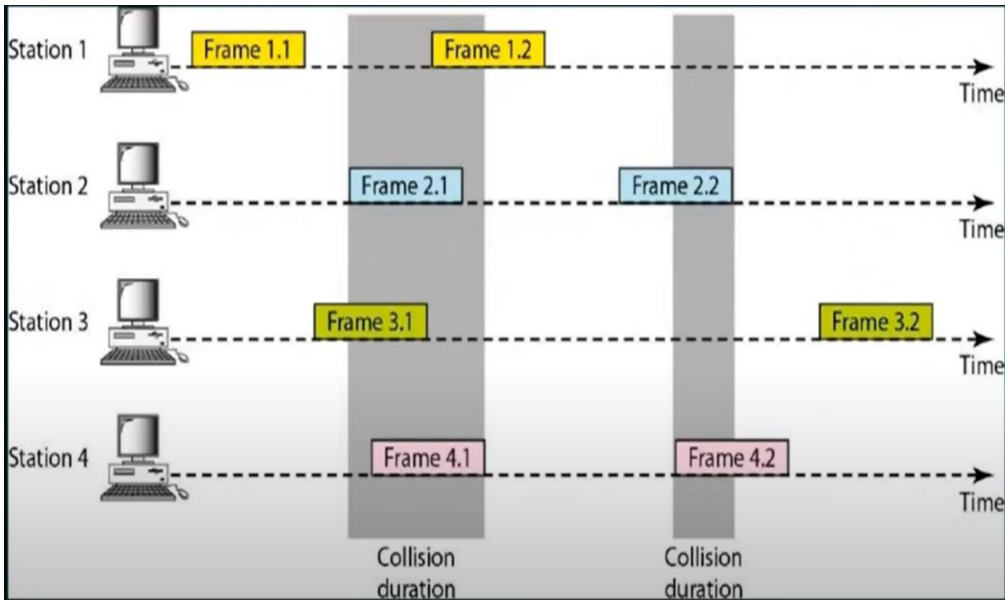
Channelization Protocols:-

- Channelization is a multiple access method in which the available bandwidth of a link is shared time, frequency or through code between different stations.
- The following are some of channelization access protocols.
  (1) FDMA - Frequency Division Multiple Access
  (2) TDMA - Time Division Multiple Access
  (3) CDMA - Code Division Multiple Access

ALOHA

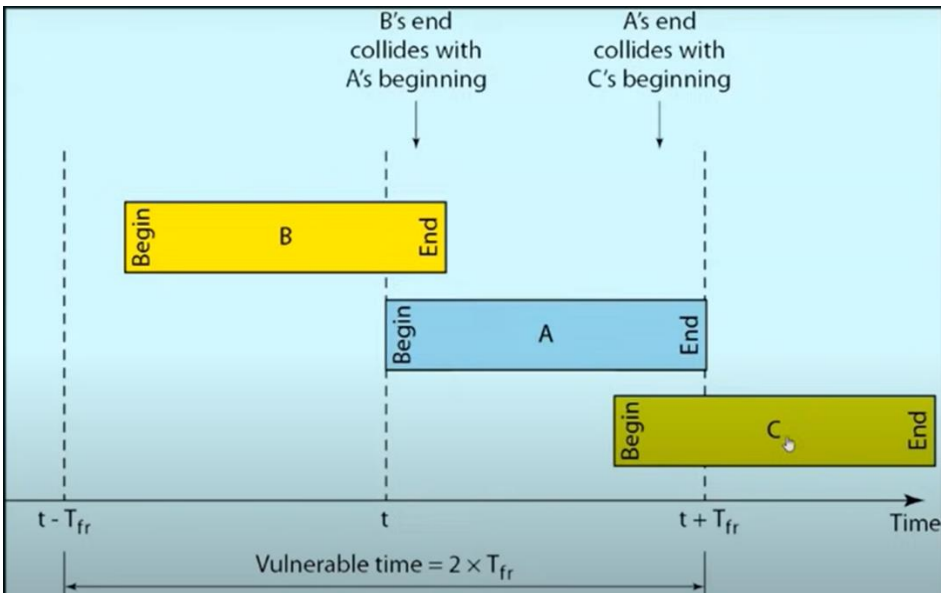
- Aloha is a random access protocol.
- It was actually designed for WLAN but it is also applicable for shared medium.
- In this, multiple stations can transmit data at the same time, hence it lead s to collision and data being lost or corrupted.
- There are two types.
  (1) Pure Aloha
  (2) Slotted Aloha

PURE ALOHA



- Pure ALOHA allows stations to transmit whenever they have data to be sent.
- When a station send data it waits for an acknowledgement.
- If the acknowledgement does not come within the allotted time then the station waits for a random amount of time called **back off time (Tb)** and resends the data.

- Since different stations wait for different amount of time, the probability of further collisions 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 garbled.
- If the 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 later.

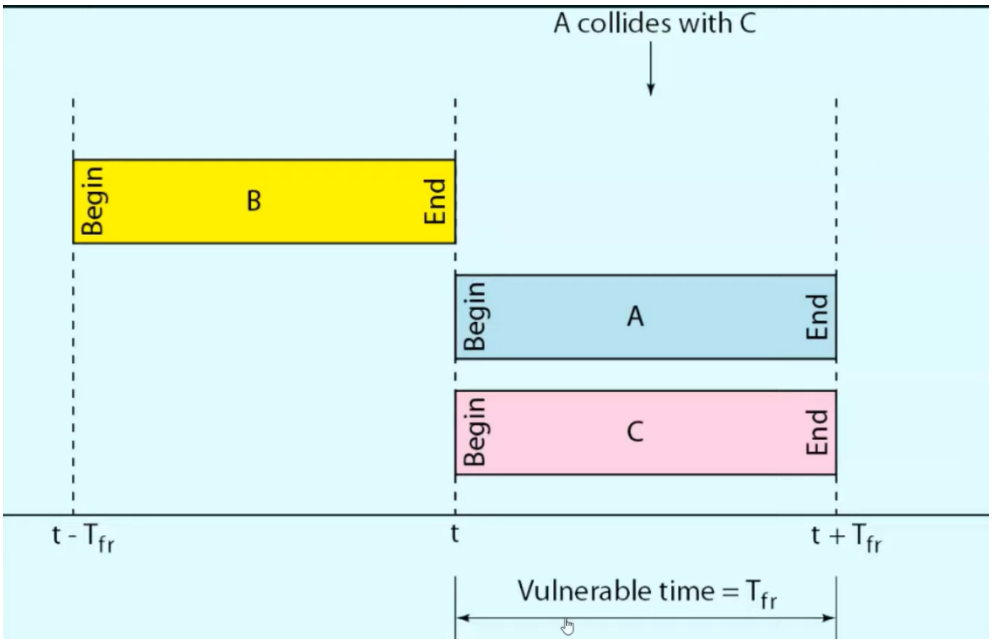


Vulnerable Time = $2*T_{fr}$

Throughput = $G \times e^{-2G}$; Where G is the number of stations wish to transmit in the same time.

SLOTTED ALOHA

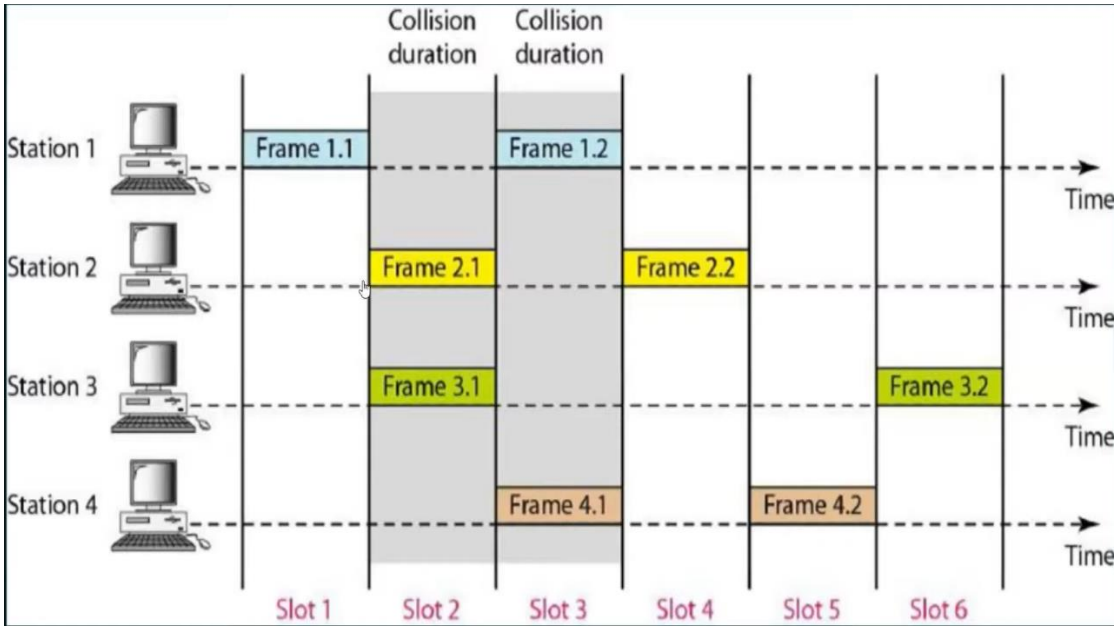
- It was developed just to improve the efficiency of pure ALOHA as the chances for collision in pure ALOHA are high.
- The time of the shared channel is divided into discrete time intervals called slots.
- Sending of data is allowed only at the beginning of these slots.
- If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.



Vulnerable Time = Frame Transmission Time.

Throughput = $G \times e^{-G}$; Where G is the number of stations wish to transmit in the same time.

Maximum throughput = 0.368 for G=1.



PURE ALOHA VS SLOTTED ALOHA	
Pure Aloha	Slotted Aloha
Any station can transmit the data at any time.	Any station can transmit the data at the beginning of any time slot.
The time is continuous and not globally synchronized.	The time is discrete and globally synchronized.
Vulnerable time in which collision may occur $= 2 \times T_{Fr}$	Vulnerable time in which collision may occur $= T_{Fr}$
Probability of successful transmission of data packet= $G \times e^{-2G}$	Probability of successful transmission of data packet= $G \times e^{-G}$
Maximum efficiency = 18.4% (Occurs at G = 1/2)	Maximum efficiency = 36.8% (Occurs at G = 1)
Main advantage: Simplicity in implementation.	Main advantage: It reduces the number of collisions to half and doubles the efficiency of pure aloha.

CSMA PROTOCOL

- Carrier Sense Multiple Access Protocol.
- To minimize the chance of collision and therefore increase the performance, this method was developed.
- The principle of CSMA is **"Sense before transmit".**
- Carrier busy means transmission is taking place.
- Carrier idle means no transmission currently taking place.
- The possibility of collision stills exists because of propagation delay. A station may sense the medium and find it idle, only because the first bit sent by other station has not yet been received.
- There are different types of CSMA.
  1. 1-Persistent CSMA
  2. P- Persistent CSMA
  3. N-Persistent CSMA
  4. O-Persistent CSMA

1. 1-Persistent CSMA

- Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
- If the channel is idle, the station transmits a frame.
- If the channel is busy then it senses the transmission medium continuously until it becomes idle.
- Since the station transmits the frame with the probability of 1 when the carrier or the channel is idle, this scheme of CSMA is called 1-Persistent CSMA.
- The longer the propagation delay, decreases the performance of protocol.

2. N-Persistent CSMA

- Before sending, a station senses the channel. If no one else is sending, the station begins sending.
- If the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting upon the end of previous transmission.
- Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

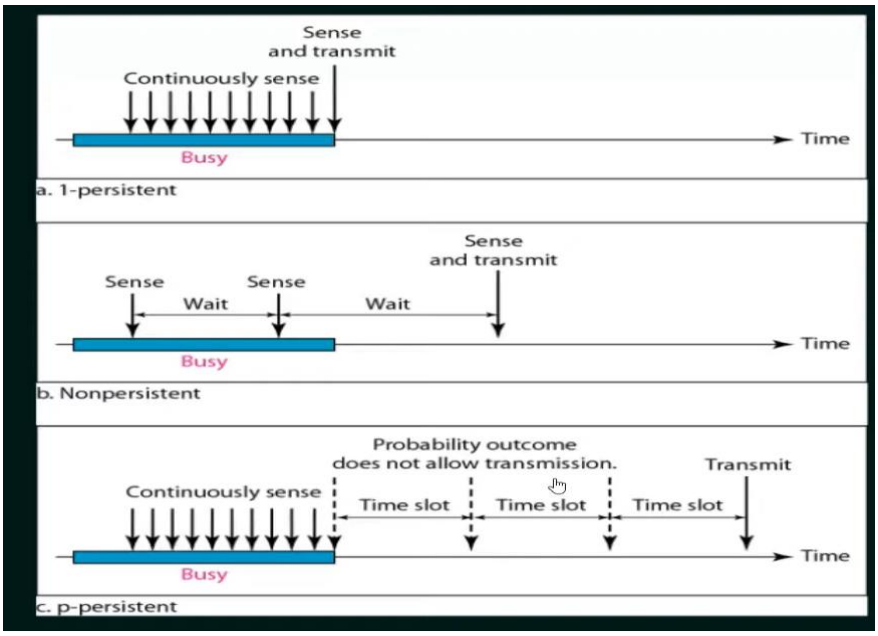
3. P-Persistent CSMA

- It applies to slotted channels.
- When a station becomes ready to send it senses the channel.
- If it is idle, it transmits with a probability P.
- With a probability Q=1-P, it defers until the next slot.
- If that slot is also idle, it either transmits or defers again with probabilities P and Q.
- This process is repeated until either the frame has been transmitted or another station has begun transmitting.
- In the latter case, the unlucky station acts if there had been a collision (i.e., it waits a random time and starts again)
- If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm.

4. O-Persistent CSMA

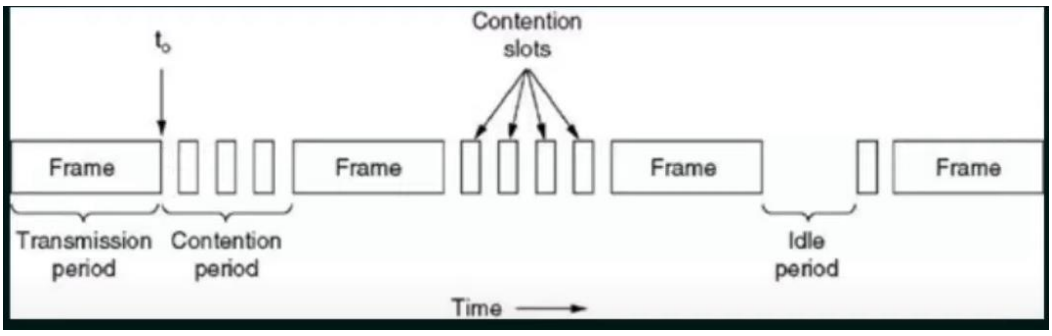
- Each node is assigned a transmission order by a supervisory node.

Comparision of CSMA types:-



CSMA/CD

- If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
- Rather than finish transmitting frames, they should abruptly stop transmitting as soon as the collision is detected.
- Quickly terminating damaged frames saves time and bandwidth.
- This protocol known as, CSMA/CD (Carrier Sense Multiple Access with Collision Detection) which is widely used on LANs in MAC sublayer.
- Access method used by Ethernet: CSMA/CD.



- At the point marked t_0 , a station has finished transmitting its frame.
- Any other station having a frame to send may now attempt to send. If two or more stations decide to transmit simultaneously, there will be a collision.
- Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
- After a station detected a collision, it aborts its transmission, waits a random period of time and then tries again, assuming that no other station has started transmitting in the mean time.
- Therefore, model for CSMA/CD will consists of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.
- If distance increases, the efficiency of CSMA decreases.
- CSMA is not suitable for long distance networks like WAN, but works for LANs.

CSMA/CA

- CSMA with CA is a network multiple access method in which carrier sensing is used, but the nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be **"idle".**
- It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.
- CSMA/CA is unreliable due to the hidden node problem and exposed terminal problem.
- The solution is RTS/ CTS exchange.
- CSMA/CA is a protocol that operates in the DLL(Layer 2) of the OSI model.
- The access method used by IEEE 802.11 Wi-Fi is CSMA/CA.

COLLISION FREE PROTOCOLS

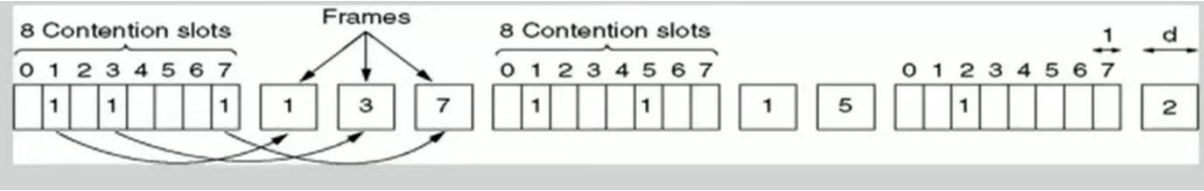
Definition of Collision:-

- In computer networks, when more than one station tries to transmit simultaneously via shared channel, the transmitted data is garbled. This is called **Collision.**
- **Medium Access Control Layer is responsible for handling collisions of frames**.
- The protocols that resolve the contention for the channel without any collisions at all, not even during the contention period. Such protocols are called as **Collision Free Protocols.**
- CSMA/CD, CSMA/CA are used to reduce the collisions. But still collisions occur during contention period if more than one station starts to transmits at the same time.
- In Carrier Sense Multiple Access with Collision Detection (CSMA/CD), a **contention period is a period of time when a station senses the channel and waits to transmit a frame.**
- Here, we assume that there are exactly N stations, each programmed with a unique address from 0 to N-1.
- The following are some of the collision free protocols.
    1. Bitmap protocol.
    2. Token Passing
    3. Binary Countdown.

1. Bit – Map protocol:-

- It resolves the possibility of collisions while multiple stations are contending for acquiring a shared channel for transmission.
- If a station wants to transmit it broadcasts itself before the actual transmission.
- In this protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel.
- If station has a frame to send, it sets the corresponding bit in the slot to 1.
- No other station is allowed to transmit during this slot.

For example, there are 8 stations, so the number of contention slots is 8 (0-7). If the stations 1,3,7 wants to transmit their frames, then they will set the corresponding slots to 1, as shown in below figure.



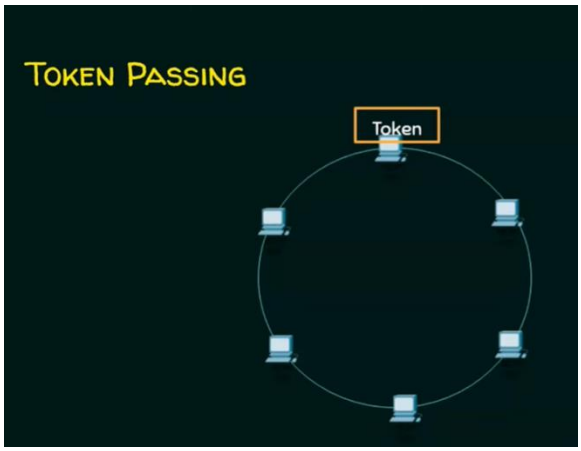
Protocols like this in which the desire to transmit is broadcast before the actual transmission are called **Reservation Protocols.**

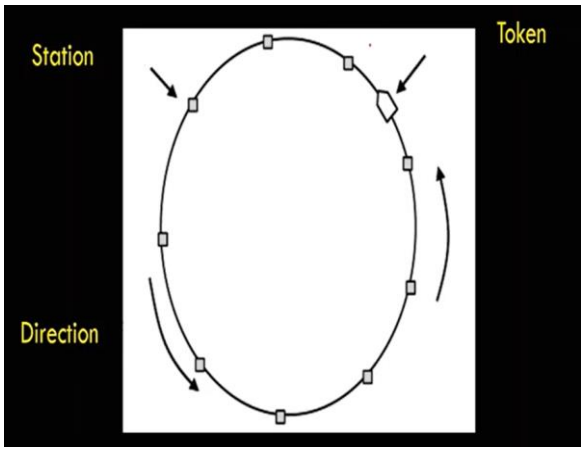
- Generally transmission is done in the order of the slot numbers.

- Each station has complete knowledge whether every other station wants to transmit or not before transmission starts. So all possibilities of collisions are eliminated.

2. Token Passing:-

- A special frame is called **a token** around the ring.
- Token is a empty frame. Only one station will hold the token.
- It prevents the collisions.
- Here also every station should transmit a frame in a predefined order.
- Each station knows its predecessor and successor.
- Pass a small message called a token from one station to the next in the same predefined order.
- The 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 simply passes the token.
- In a token ring protocol, the topology of the network is used to define the order in which stations send.
- The stations are connected one to the next in a single ring.
- Passing the token to the next station consists of receiving the token in from one direction and transmitting it out in the other direction. Frames are also transmitted in the direction of the token.

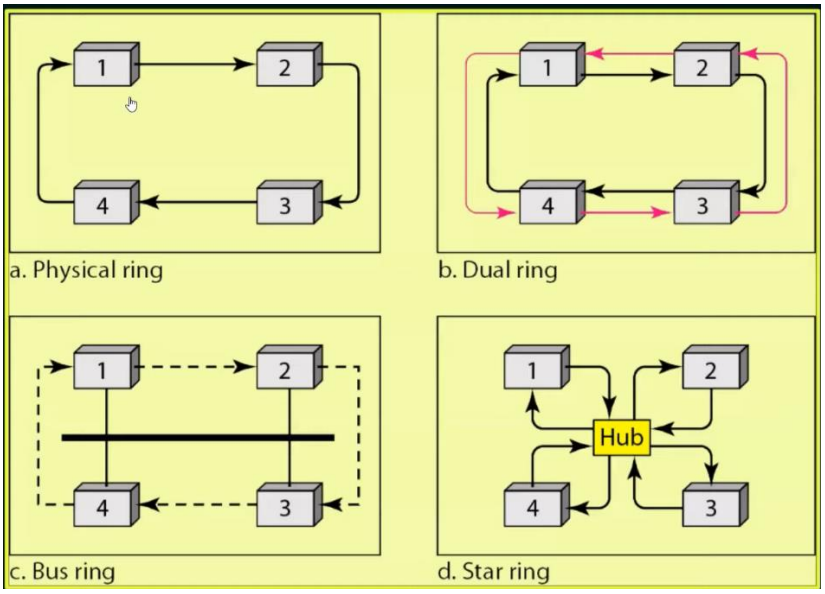




Types of rings:-

1. In **Physical ring**, all stations have been connected physically. It is visible. Here there exists a physical path to transmit the frames through the path by passing token from one station to another in a predefined manner. But if any of the path damaged, there is no chance of sending data in another path. Because the ring is break.
2. In **Dual ring**, there are two rings, named primary ring and secondary ring. Note that only primary ring is used to transmit the frames and pass the token. Secondary ring is used when primary ring fails only until the primary ring recovers.

3. In **Bus ring,** there is no physical ring like structure through which token and frames passes, but through the bus all stations are connected one to another in a ring like fashion to transmit frames and token.
4. In **Star ring,** through the Hub all station are connected to each other. If a station wants to send a frame to another it passes frame and token to next station through the hub. It receives that token and frame and verifies that destination address. If it destination, then it sends acknowledgement along with token. Otherwise it transmits the same frame and token to next station.



3. Binary Countdown:-

- A problem with the basic bit map protocol, token passing is that the overhead is 1 bit per station. This can be resolved by using binary station addresses.
- A station wants to use the channel broadcasts its address as a binary bit string, starting with the high order bit.
- All addresses are assumed to be the same number of bits.
- As soon as a station sees that a higher order bit position that is 0 in its address has been overwritten with 1, it gives up.

For example, five stations are there with the below mentioned addresses

1011, 0010, 0111, 1110 and 1101

1. Step 1: All stations will broadcast its MSB- 1 0 0 1 1
2. Step 2: stations 2, 3 gives up by seeing MSB 1 in 1,4,5.
3. Step 3: Among 1,4,5 stations, next MSB is broadcasted i.e., 0 1 1. By seeing this station 1 give up.
4. Step 4: Now stations 4, 5 will broadcast their next MSB i.e., 1 0. By seeing this station 5 gives up. So station 4 has access to the channel.
5. The same procedure or algorithm is applied until all stations access the medium./channel.

ETHERNET

A local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection between the devices could be wired or wireless. Ethernet, Token rings, and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.

What is Ethernet?

- Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3.
- Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation.
- Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology.
- Ethernet operates in two layers of the OSI model, the physical layer and the data link layer.
- For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.
- Although Ethernet has been largely replaced by wireless networks, wired networking still uses Ethernet more frequently.
- Wi-Fi eliminates the need for cables by enabling users to connect their smartphones or laptops to a network wirelessly.

There are different types of Ethernet networks that are used to connect devices and transfer data.

1. Fast Ethernet

This type of Ethernet network uses cables called twisted pair or CAT5. It can transfer data at a speed of around 100 Mbps (megabits per second). Fast Ethernet uses both fiber optic and twisted pair cables to enable communication. There are three categories of Fast Ethernet: 100BASE-TX, 100BASE-FX, and 100BASE-T4.

2. Gigabit Ethernet

This is an upgrade from Fast Ethernet and is more common nowadays. It can transfer data at a speed of 1000 Mbps or 1 Gbps (gigabit per second). Gigabit Ethernet also uses fiber optic and twisted pair cables for communication. It often uses advanced cables like CAT5e, which can transfer data at a speed of 10 Gbps.

3. 10-Gigabit Ethernet

This is an advanced and high-speed network that can transmit data at a speed of 10 gigabits per second. It uses special cables like CAT6a or CAT7 twisted-pair cables and fiber optic cables. With the help of fiber optic cables, this network can cover longer distances, up to around 10,000 meters.

4. Switch Ethernet

This type of network involves using switches or hubs to improve network performance. Each workstation in this network has its own dedicated connection, which improves the speed and

efficiency of data transfer. Switch Ethernet supports a wide range of speeds, from 10 Mbps to 10 Gbps, depending on the version of Ethernet being used.

In summary, Fast Ethernet is the basic version with a speed of 100 Mbps, Gigabit Ethernet is faster with a speed of 1 Gbps, 10-Gigabit Ethernet is even faster with a speed of 10 Gbps, and Switch Ethernet uses switches or hubs to enhance network performance.