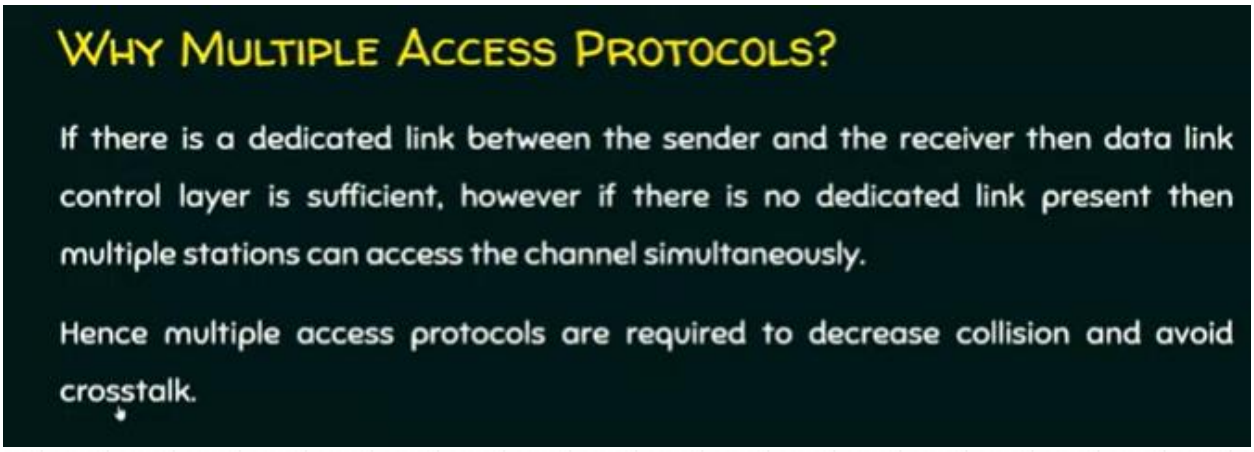
Multiple Access Control

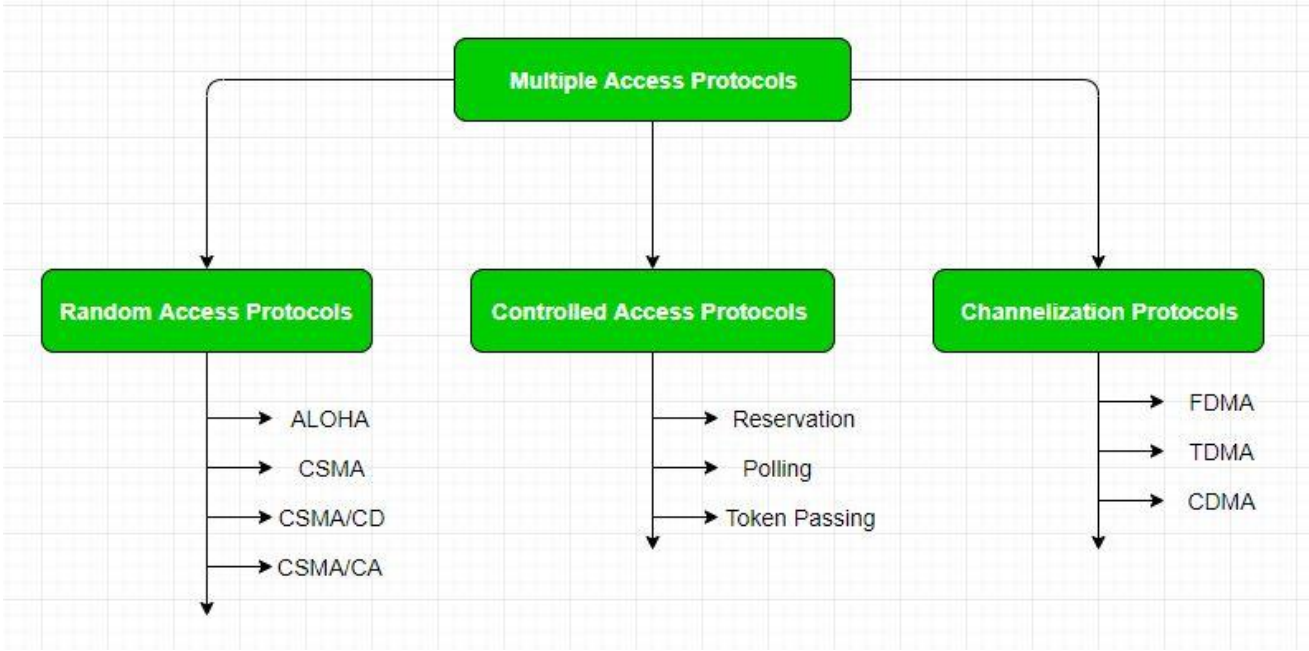
The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

Data Link Control

Multiple Access Control

Data Link control – The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control





Random Access Protocols

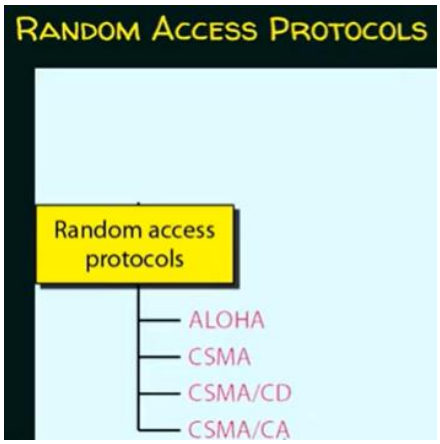
- ★ In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy).
- ★ In a Random access method, each station has the right to the medium without being controlled by any other station.
- ★ If more than one station tries to send, there is an access conflict (COLLISION) and the frames will be either destroyed or modified.

Random Access Protocols

To avoid access conflict, 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 ?

Random Access Protocols

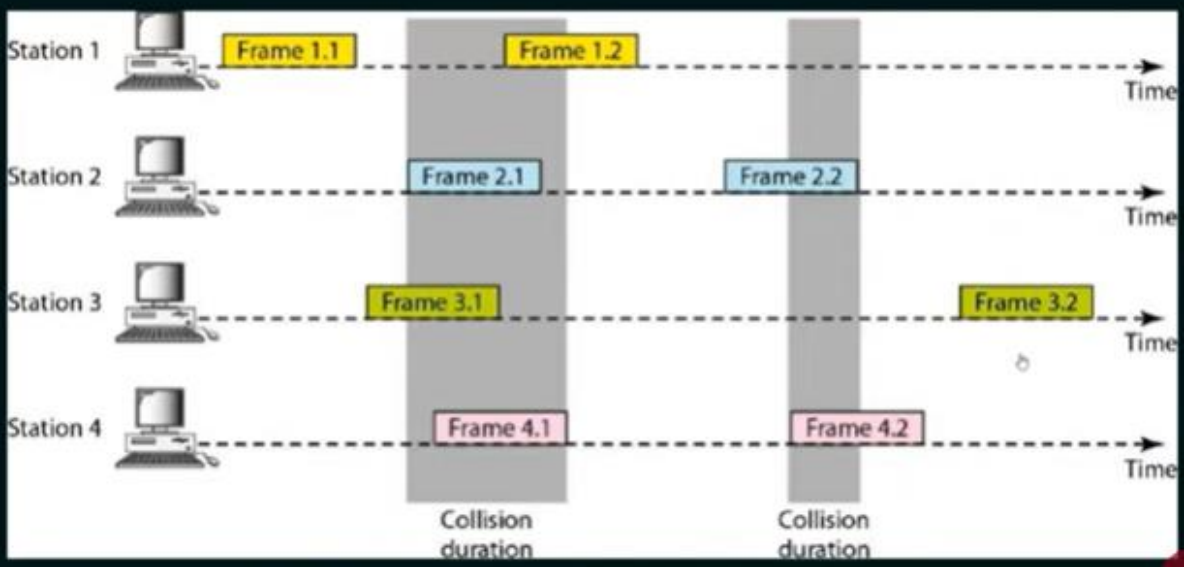


ALOHA

- ★ 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 and can hence lead to collision and data being garbled.

COLLISION

PURE ALOHA



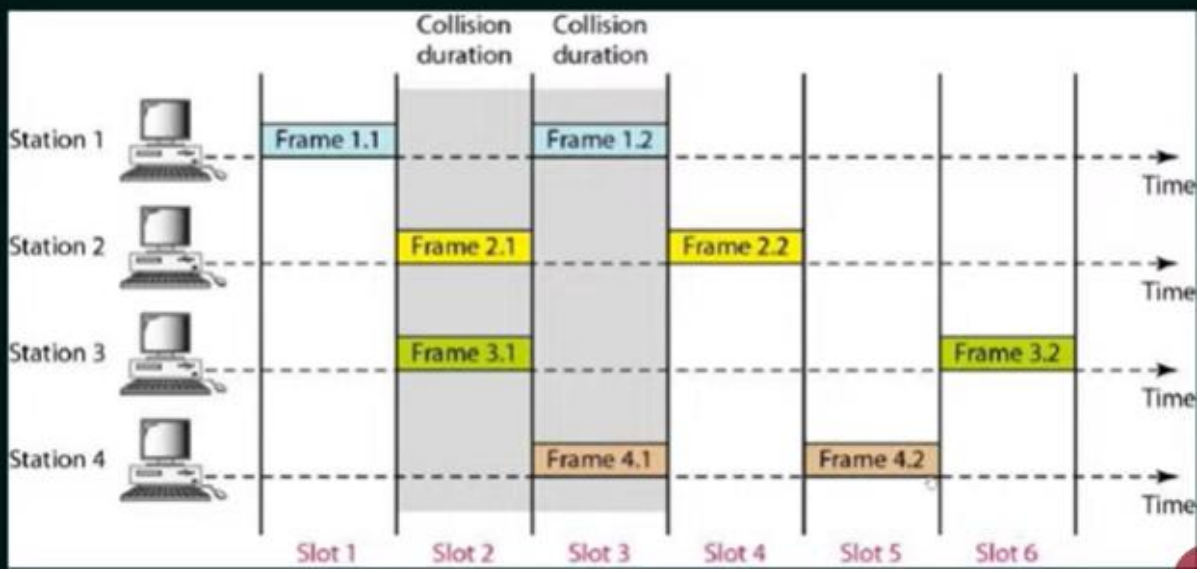
PURE ALOHA

- ★ Pure ALOHA allows stations to transmit whenever they have data to be sent.
- ★ When a station sends data it waits for an acknowledgement.
- ★ If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data.
- ★ Since different stations wait for different amount of time, the probability of further collision decreases.

SLOTTED ALOHA

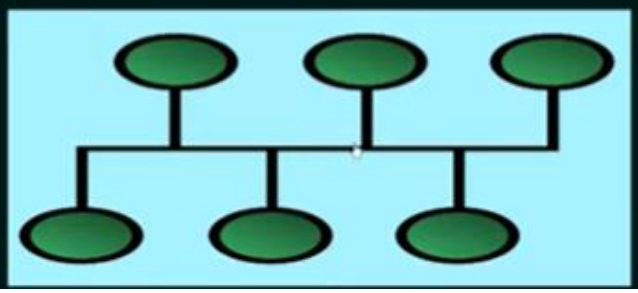
- ★ It was developed just to improve the efficiency of pure aloha as the chances for collision in pure aloha are high.
- ★ The time of the shared channel is divided into discrete time intervals called slots.
- ★ Sending of data is allowed only at the beginning of these slots.

SLOTTED ALOHA



CSMA PROTOCOL

- ★ Carrier Sense Protocol.
- ★ To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- ★ Principle of CSMA: "sense before transmit" or "listen before talk."



- ★ Carrier busy = Transmission is taking place.
- ★ Carrier idle = No transmission currently taking place.
- ★ The possibility of collision still exists because of propagation delay; a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

Types of CSMA

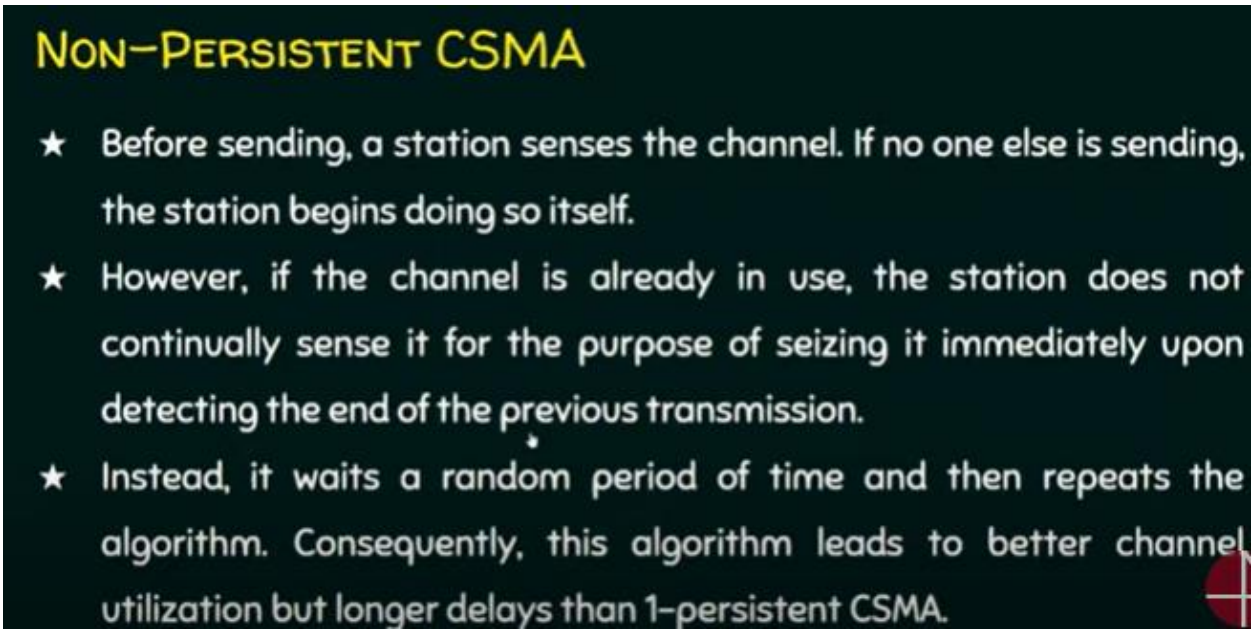
1. 1-Persistent CSMA
2. P-Persistent CSMA
3. Non-Persistent CSMA
4. O-Persistent CSMA

CSMA/CD (CSMA with Collision Detection)

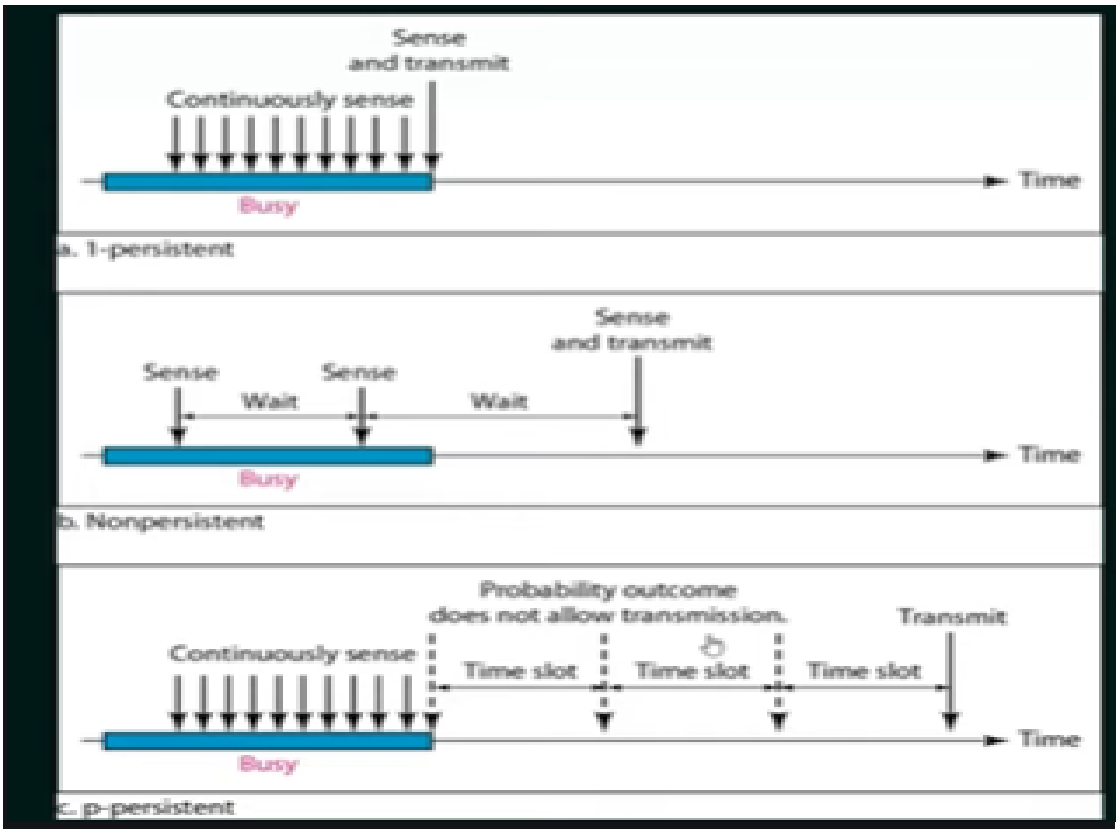
CSMA/CA (CSMA with Collision Avoidance)

1-Persistent CSMA

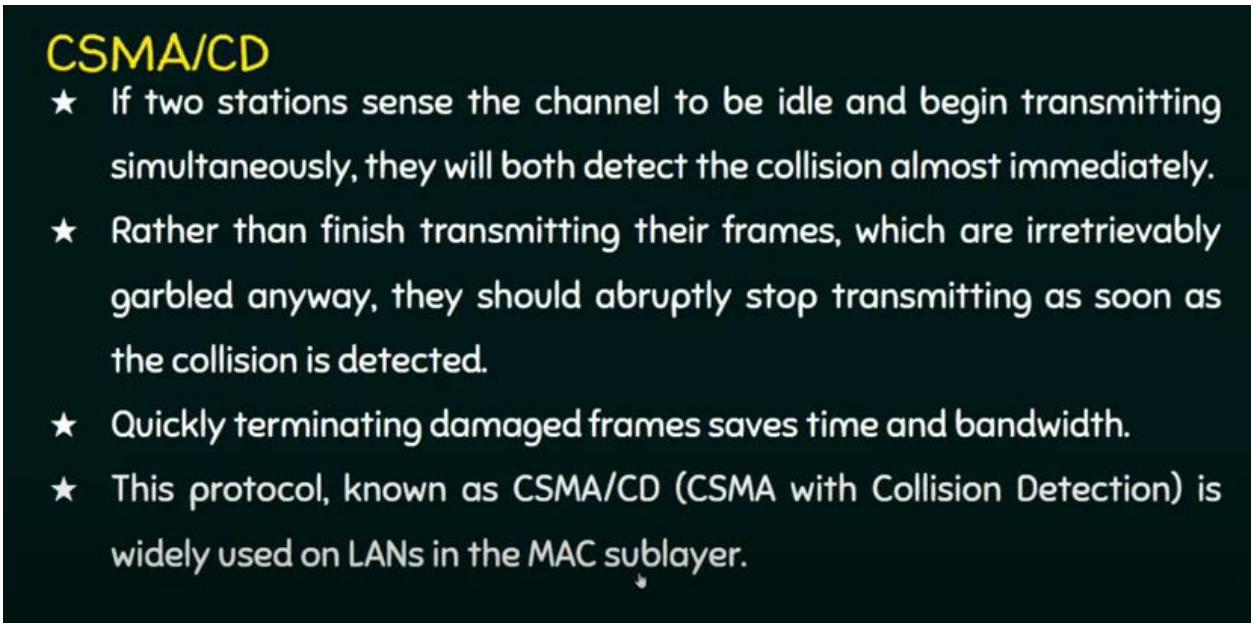
- ★ Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
- ★ If the channel is idle, the station transmits a frame.
- ★ If busy, then it senses the transmission medium continuously until it becomes idle.
- ★ Since the station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



- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.



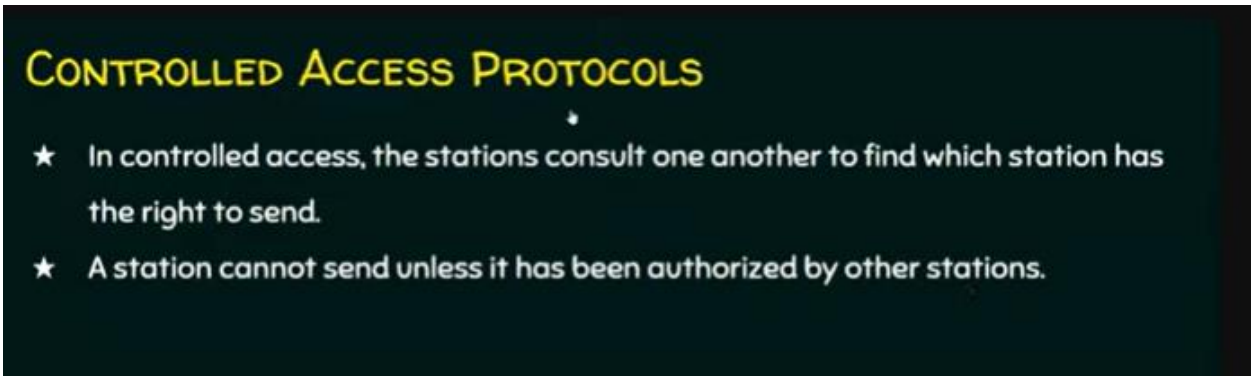
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.



If two or more devices transmit data simultaneously, a collision occurs. When a device detects a collision, it immediately stops transmitting and sends a jam signal to inform all other devices on the network of the collision. The devices then wait for a random time before attempting to transmit again, to reduce the chances of another collision

Carrier sense multiple access with collision avoidance(CSMA/CA)

The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

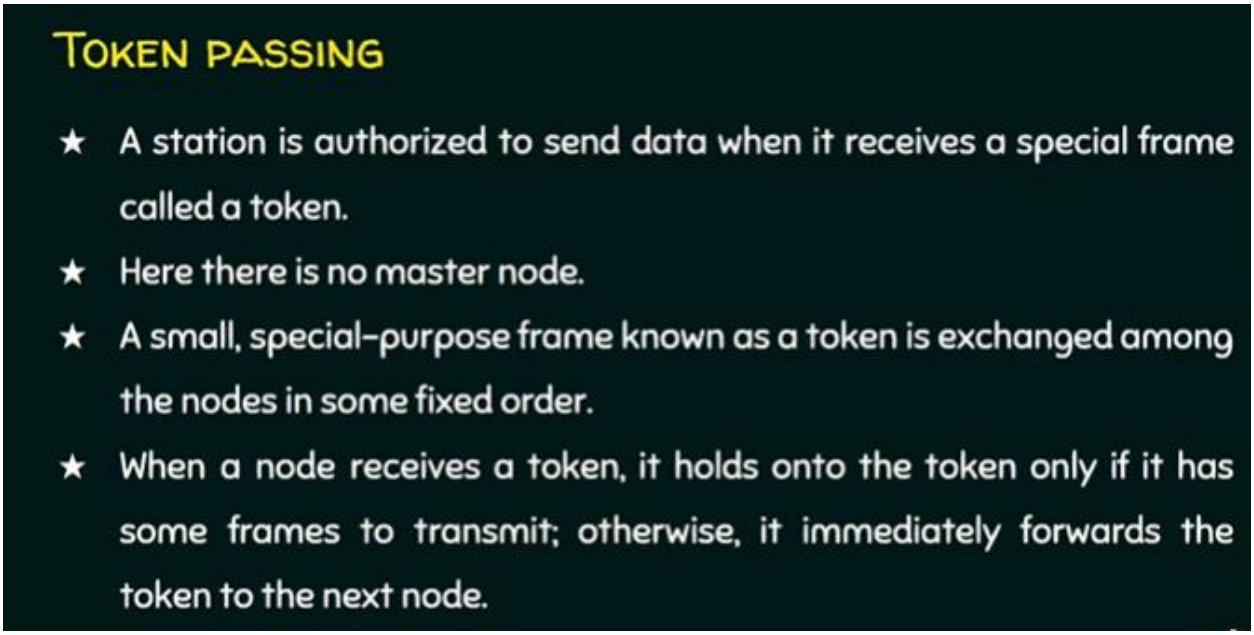


Controlled Access Protocols in Computer Network

In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

- Reservation
- Polling
- Token Passing

Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.



Token passing

- ★ If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node.
- ★ Token passing is decentralized and highly efficient. But it has problems as well.
- ★ For example, the failure of one node can crash the entire channel. Or if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.