Data Communication and Computer Networks

UNIT-II

Random Access Protocols

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy).

Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access. Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.

However, 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 access conflict or to resolve it when it happens, each station follows a procedure that answers the following questions:

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 different random access methods are as follows:

ALOHA
CSMA
CSMA/CD
CSMA/CA

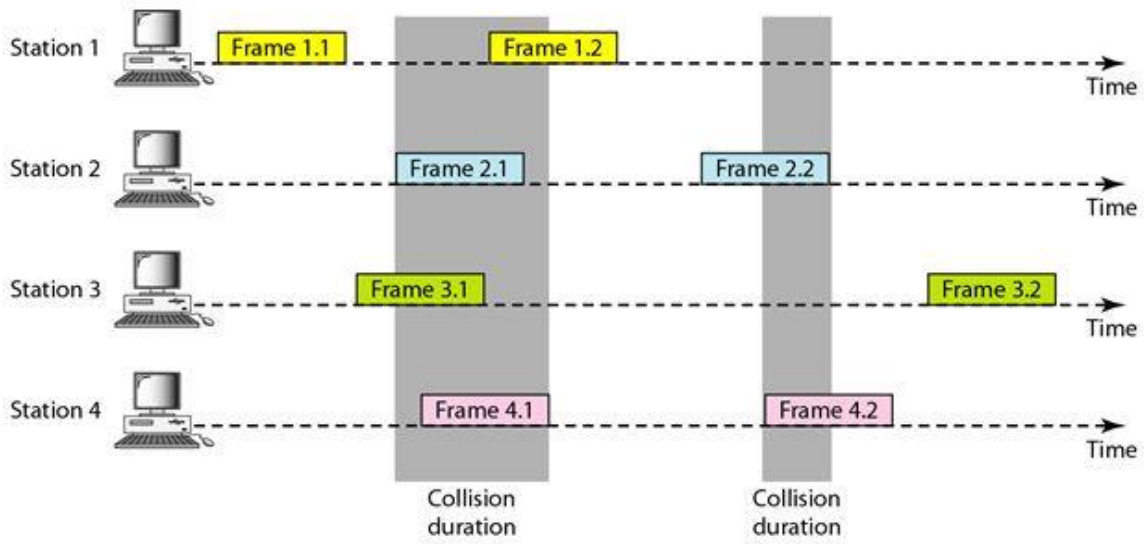
Aloha Protocols

ALOHA, the earliest random access method was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations. The following figure shows an example of frame collisions in pure ALOHA.



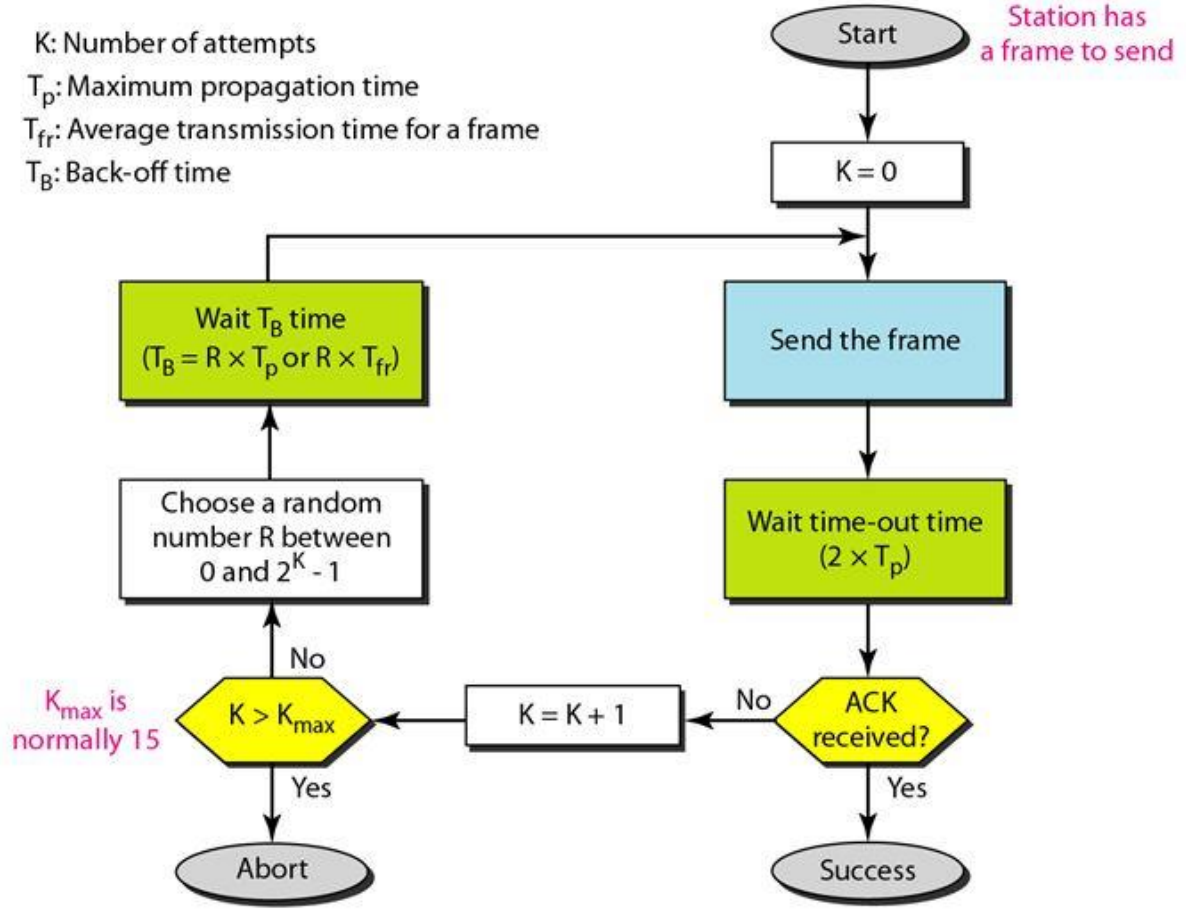
There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel.

The above figure shows that only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed.

It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver. If the acknowledgment does not arrive after a time-out

period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time TB.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax a station must give up and try later. The following figure shows the procedure for pure ALOHA based on the above strategy.

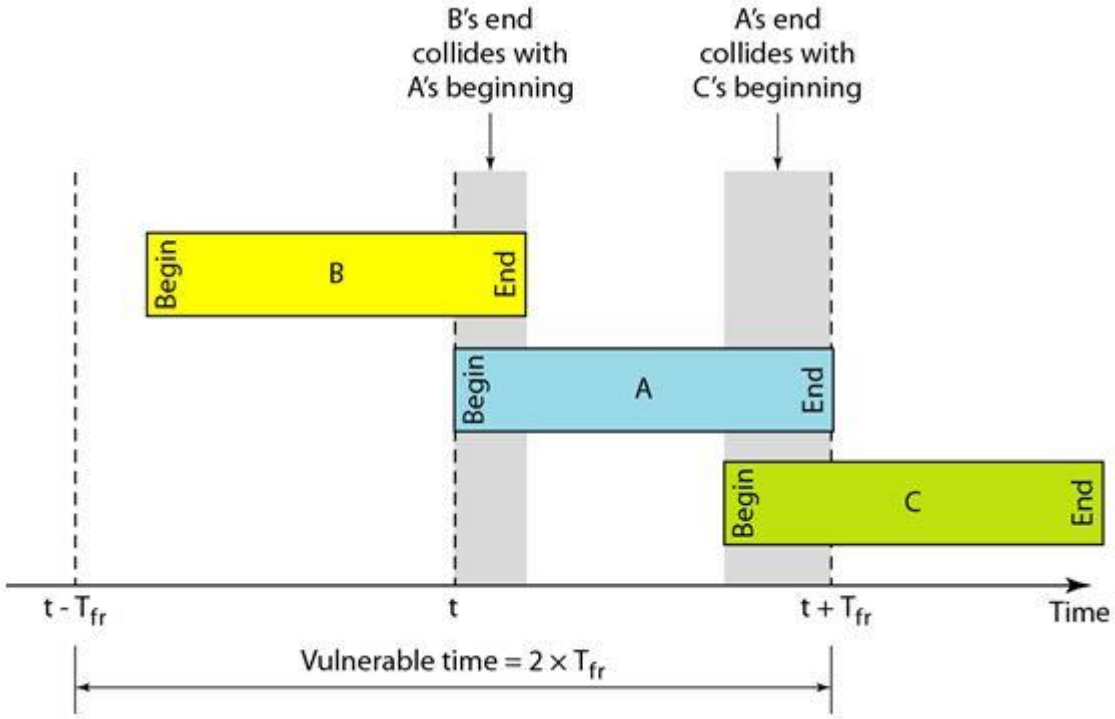


The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations (2 x Tp) The back-off time TB is a random value that normally depends on K (the number of attempted unsuccessful transmissions). The formula for TB depends on the implementation. One common formula is the binary exponential back-off.

In this method, for each retransmission, a multiplier in the range 0 to 2K - 1 is randomly chosen and multiplied by Tp (maximum propagation time) or Tfr (the average time required to send out a frame) to find TB' Note that in this procedure, the range of the random numbers increases after each collision. The value of Kmax is usually chosen as 15.

Vulnerable time:

The vulnerable time is in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking Tfr S to send. The following figure shows the vulnerable time for station A.

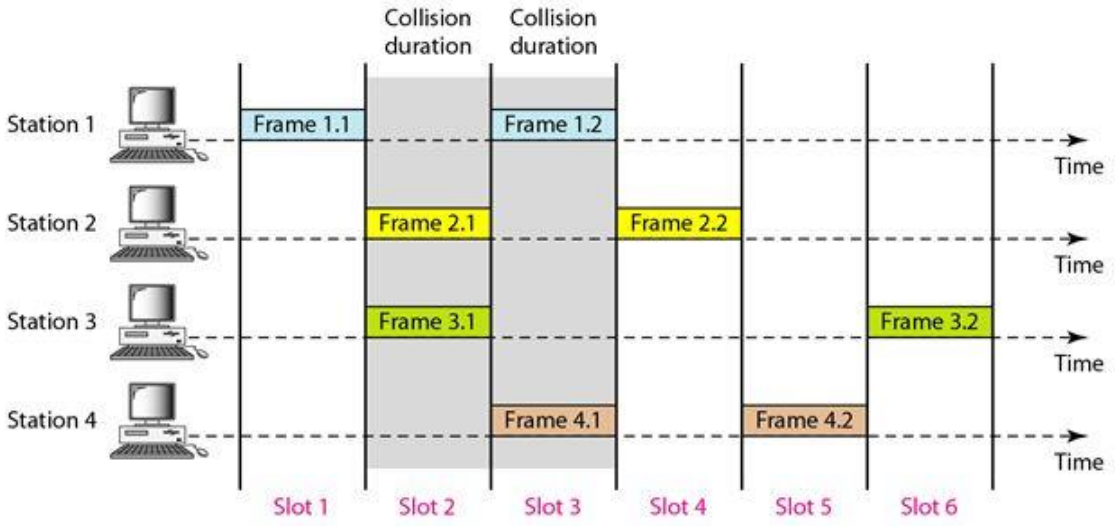


Station A sends a frame at time t. Now imagine station B has already sent a frame between t - Tfr and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame. On the other hand, suppose that station C sends a frame between t and t + Tfr . Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

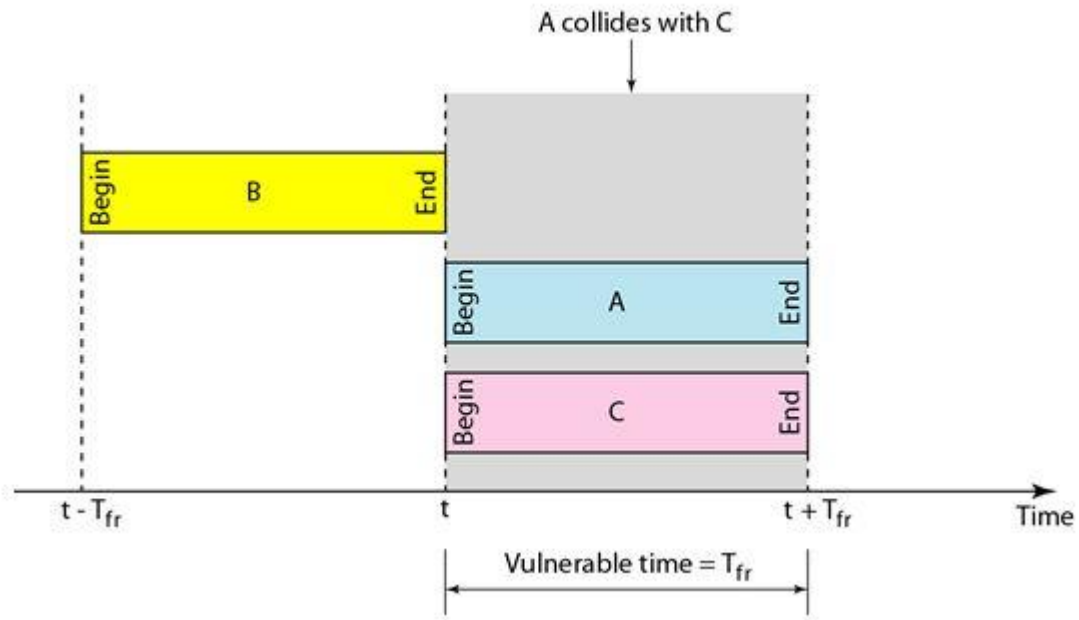
Slotted ALOHA:

Pure ALOHA has a vulnerable time of 2 x Tfr. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.

In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot. The following figure shows an example of frame collisions in slotted ALOHA.

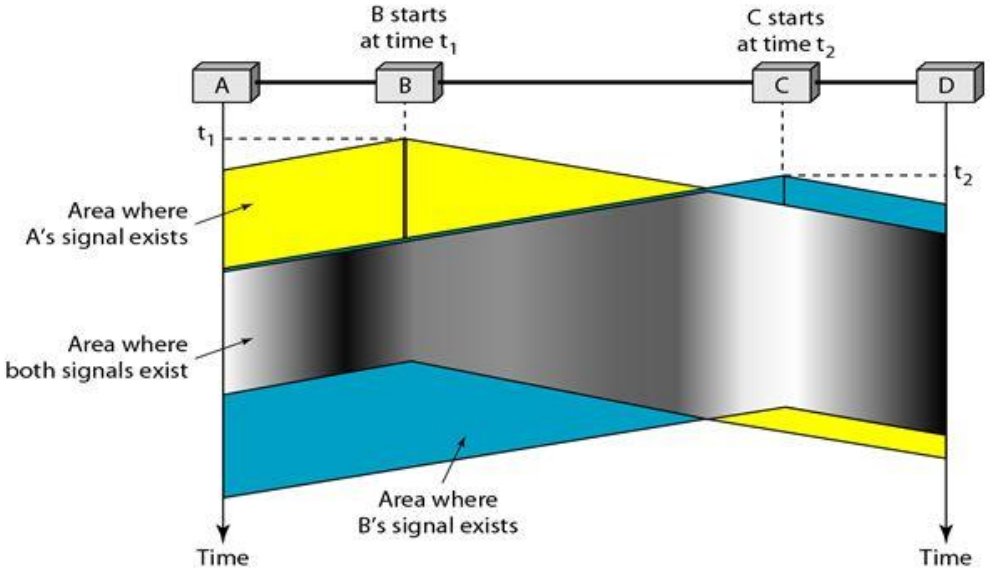


Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. But, still there is the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to Tfr. The following figure shows the situation.



Carrier Sense Multiple Access Protocol

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. CSMA can reduce the possibility of collision, but it cannot eliminate it. The following figure shows a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).

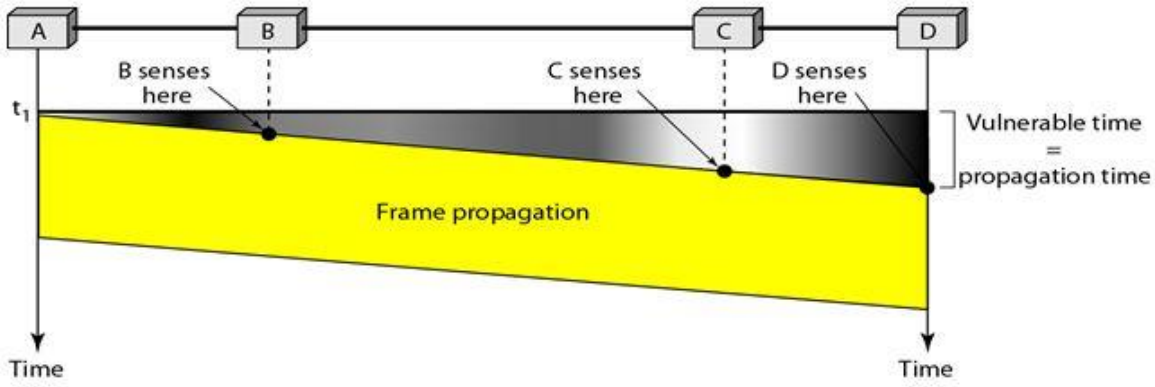


The possibility of collision still exists because of propagation delay, when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

At time t1 station B senses the medium and finds it idle, so it sends a frame. At time t2 (t2> t1) station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.

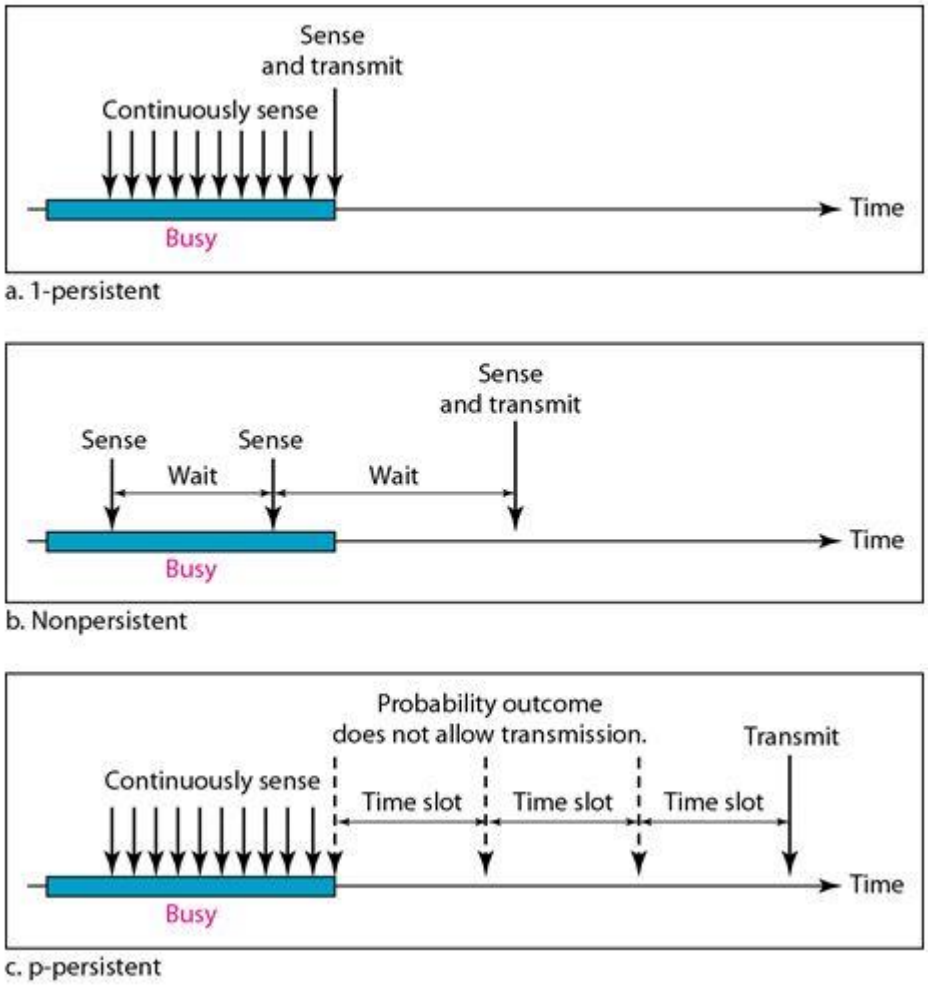
Vulnerable Time:

The vulnerable time for CSMA is the propagation time Tp. This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending. The following figure shows the worst case. The leftmost station A sends a frame at time t1 which reaches the rightmost station D at time t1 + Tp. The gray area shows the vulnerable area in time and space.



Persistence Methods:

What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions: the 1-persistent method, the nonpersistent method, and the p-persistent method. The following figure shows the behavior of three persistence methods when a station finds a channel busy.



• **1-Persistent:** The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

• **Nonpersistent:** In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

• **P-Persistent:** The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves

efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability p, the station sends its frame.

2. With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.

1. If the line is idle, it goes to step 1.

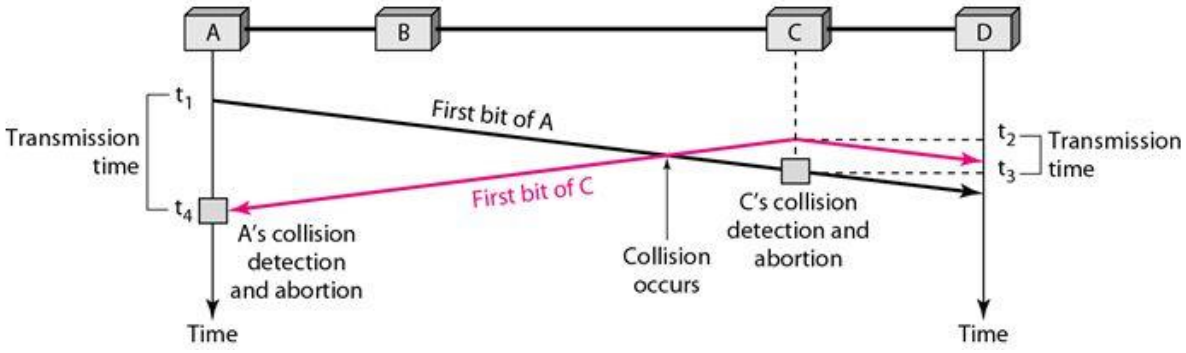
2. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

Carrier Sense Multiple Access with Collision Detection

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In the following Figure stations A and C are involved in the collision.



• At time t 1, station A has executed its persistence procedure and starts sending the bits of its frame.

• At time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.

• The collision occurs sometime after time t2' Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission.

• Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission.

• Looking at the figure, we see that A transmits for the duration t4 – t1. C transmits for the duration t3 - t2. The protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t4, the transmission of A’s frame, though incomplete, is aborted. At time t3, the transmission of C's frame, though incomplete, is aborted.

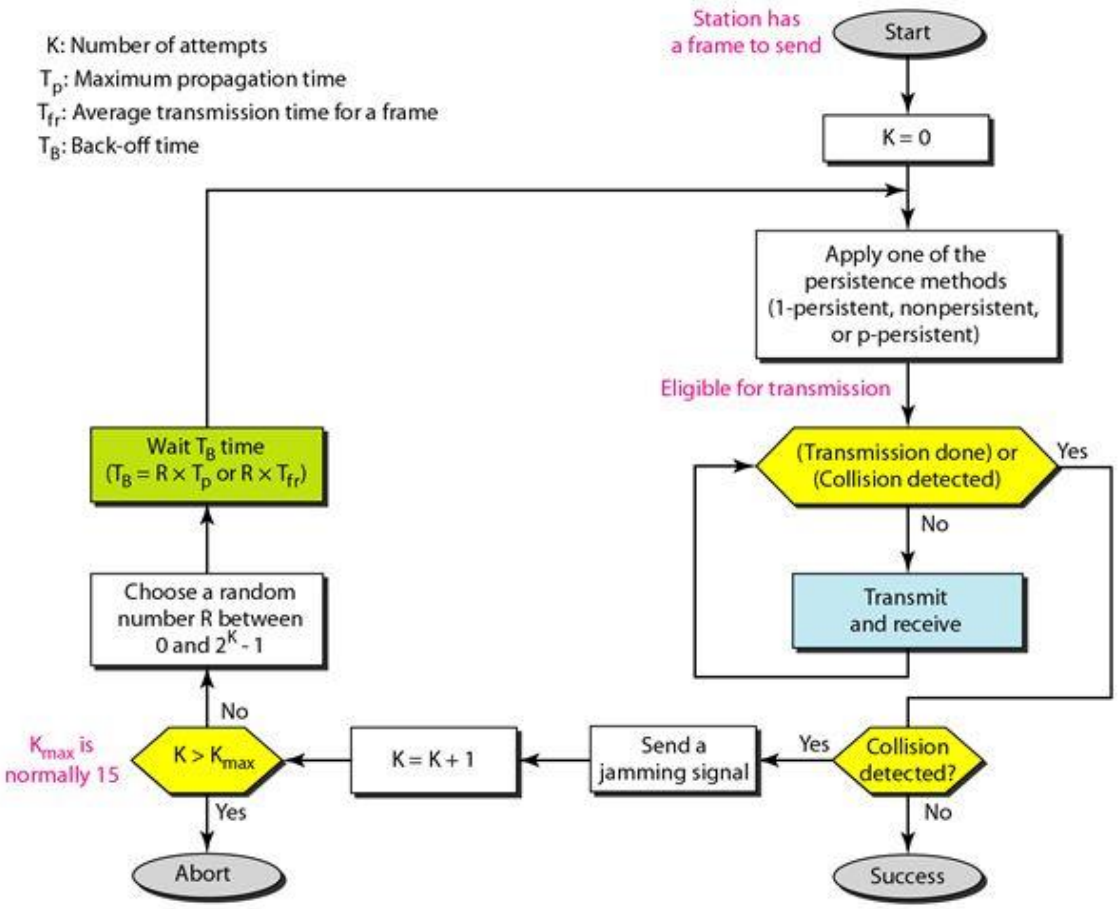
Minimum Frame Size:

For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time Tfr must be at least two times the maximum propagation time Tp.

To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp .

Procedure

Now let us look at the flow diagram for CSMA/CD in the following figure. It is similar to the one for the ALOHA protocol, but there are differences.



• The first difference is the addition of the persistence process. We need to sense the channel before we start sending the frame by using one of the persistence processes we discussed previously (nonpersistent, I-persistent, or p-persistent).

• The second difference is the frame transmission. In ALOHA, we first transmit the entire frame and then wait for an acknowledgment. In CSMA/CD, transmission and collision detection is a continuous process. We constantly monitor in order to detect one of two conditions: either transmission is finished or a collision is detected. Either event stops transmission.

Energy Level:

We can say that the level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level. A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if

the channel is idle, busy, or in collision mode.

Carrier Sense Multiple Access with Collision Avoidance

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles.

However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.

Controlled Access Protocols in Computer Network

Controlled Access Protocols (CAPs) in computer networks control how data packets are sent over a common communication medium. These protocols ensure that data is transmitted efficiently, without collisions, and with little interference from other data transmissions. In this article, we will discuss Controlled Access Protocols.

What is the Controlled Access?

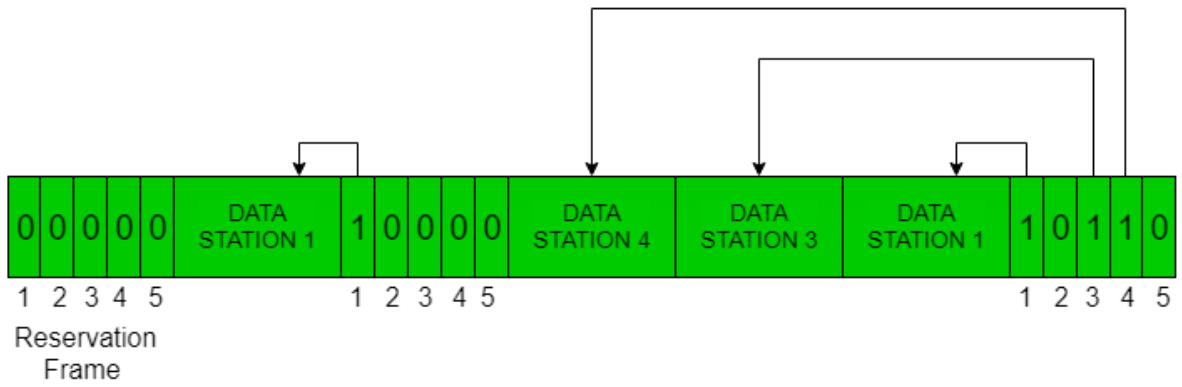
In controlled access, the stations seek data from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:

- Reservation
- Polling
- Token Passing

1. Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
    - Reservation interval of fixed time length
    - Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.
- The stations which have reserved their slots transfer their frames in that order.
- After data transmission period, next reservation interval begins.
- Since everyone agrees on who goes next, there will never be any collisions.

The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



Advantages of Reservation

- The main advantage of reservation is *high rates and low rates of data accessing* time of the respective channel can be predicated easily. Here time and rates are fixed.
- Priorities can be set to provide speedier access from secondary.

- Reservation-based access methods can provide predictable network performance, which is important in applications where latency and jitter must be minimized, such as in real-time video or audio streaming.
- Reservation-based access methods can reduce contention for network resources, as access to the network is pre-allocated based on reservation requests. This can improve network efficiency and reduce packet loss.
- Reservation-based access methods can support QoS requirements, by providing different reservation types for different types of traffic, such as voice, video, or data. This can ensure that high-priority traffic is given preferential treatment over lower-priority traffic.
- Reservation-based access methods can enable more efficient use of available bandwidth, as they allow for time and frequency multiplexing of different reservation requests on the same channel.
- Reservation-based access methods are well-suited to support multimedia applications that require guaranteed network resources, such as bandwidth and latency, to ensure high-quality performance.

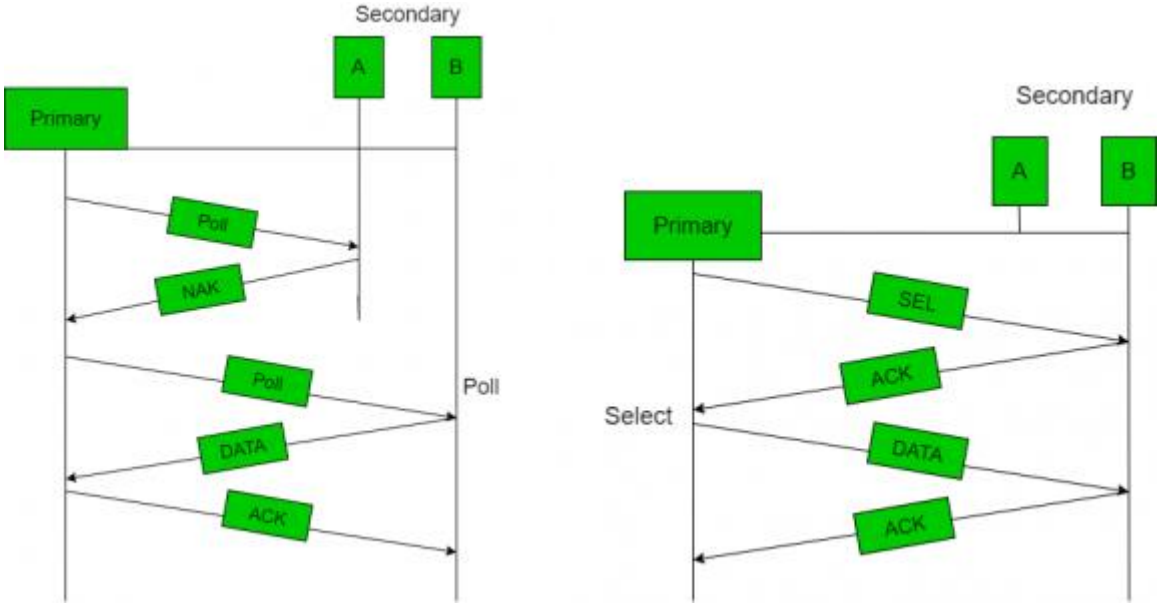
Disadvantages of Reservation

- Highly trust on controlled *dependability*.
- *Decrease in capacity* and channel data rate under light loads; increase in turn-around time.

2. Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.

- Although all nodes receive the message the addressed one responds to it and sends data if any. If there is no data, usually a “poll reject”(NAK) message is sent back.
- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.



Advantages of Polling

- The maximum and minimum access time and data rates on the channel are fixed predictable.
- It has maximum *efficiency*.
- It has maximum *bandwidth*.
- No slot is wasted in polling.
- There is assignment of priority to ensure faster access from some secondary.

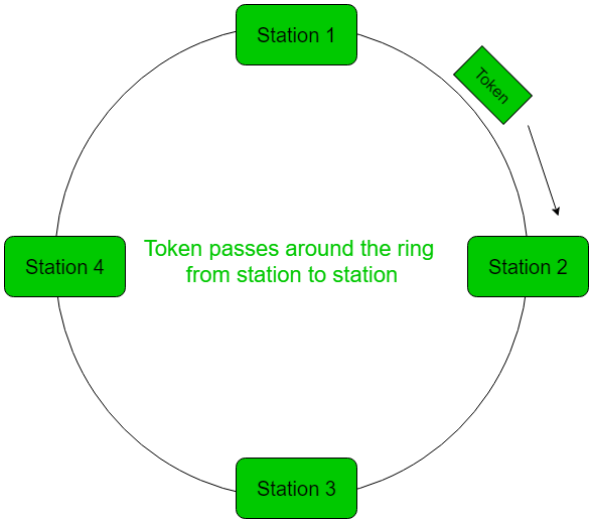
Disadvantages of Polling

- It consume *more time*.
- Since every station has an equal chance of winning in every round, link sharing is *biased*.
- Only some station might run out of data to send.
- An increase in the turnaround time leads to a drop in the data rates of the channel under low loads.

3. Token Passing

- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.

- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas in case of Token bus, each station uses the bus to send the token to the next station in some predefined order.
- In both cases, 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 passes the token simply.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbours and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



Advantages of Token passing

- It may now be applied with routers cabling and includes built-in debugging features like protective relay and auto reconfiguration.
- It provides good throughput when conditions of high load.

Disadvantages of Token passing

- Its cost is expensive.
- Topology components are more expensive than those of other, more widely used standard.

- The hardware element of the token rings are designed to be tricky. This implies that you should choose on manufacture and use them exclusively.