1.Explain ALOHA and types of ALOHA in detail.

Aloha is a type of Random access protocol it was developed at the University of Hawaii in early 1970, it is a LAN-based protocol this type there are more chances of occurrence of collisions during the transmission of data from any source to the destination, Aloha has two types one Pure Aloha and another Slotted Aloha.

Pure Aloha

Pure Aloha can be termed as the main Aloha or the original Aloha. Whenever any frame is available, each station sends it, and due to the presence of only one channel for communication, it can lead to the chance of collision.

In the case of the pure aloha, the user transmits the frame and waits till the receiver acknowledges it, if the receiver does not send the acknowledgment, the sender will assume that it has not been received and sender resends the acknowledgment.

Pure Aloha

For more, refer to Pure Aloha.

Slotted Aloha

Slotted Aloha is simply an advanced version of pure Aloha that helps in improving the communication network. A station is required to wait for the beginning of the next slot to transmit. The vulnerable period is halved as opposed to Pure Aloha.

Slotted Aloha helps in reducing the number of collisions by properly utilizing the channel and this basically results in the somehow delay of the users. In Slotted Aloha, the channel time is separated into particular time slots.

Slotted Aloha

For more, refer to Slotted Aloha.

Differences Between Pure Aloha and Slotted Aloha

Pure Aloha	**Slotted Aloha**
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 x Tt	Vulnerable time for Slotted Aloha = Tt

Pure Aloha	**Slotted Aloha**
In Pure Aloha, the Probability of successful transmission of the data packet $= G \text{ x } e^{-2G}$	In Slotted Aloha, the Probability of successful transmission of the data packet $= G \text{ x } e^{-G}$
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduce the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

1. What is the advantage of Pure Aloha over Slotted Aloha?

Answer:
The advantage of pure aloha over slotted aloha is that there is no fixed size, and it has the ability to start transmission at any particular time and no need for synchronization.

2. What is the formula for Pure Aloha and Slotted Aloha?

Answer:
Pure Aloha: $S = G \text{ x } e^{-2G}$
Slotted Aloha: $S = G \text{ x } e^{-G}$

4. A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces 1000 frames per second?
a) 150 frames
b) 80 frames
c) 135 frames
d) 96 frames Answer: c
Explanation: Frame transmission time
Tfr= 200/200 kbps or 1 ms.
If the system creates 1000 frames per second, or 1 frame
per millisecond, then G = 1
S = G × e−2G = 0.135 (13.5 percent)
This means that,
Throughput =1000 × 0.135 = 135 frames.

5. Write and explain about various multiple access protocols.

Data Link Layer

The data link layer is used in a computer network to transmit the data between two devices or nodes. It divides the layer into parts such as **data link control** and the **multiple access resolution/protocol**. The upper layer has the responsibility to flow control and the error control in the data link layer, and hence it is termed as **logical of data link control**. Whereas the lower sub-layer is used to handle and reduce the collision or multiple access on a channel. Hence it is termed as **media access control** or the multiple access resolutions.

Data Link Control

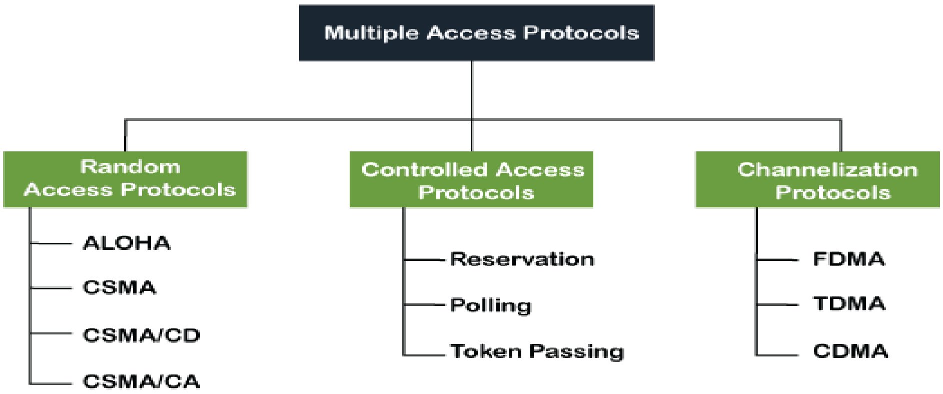
A data link control is a reliable channel for transmitting data over a dedicated link using various techniques such as framing, error control and flow control of data packets in the computer network.

What is a multiple access protocol?

When a sender and receiver have a dedicated link to transmit data packets, the data link control is enough to handle the channel. Suppose there is no dedicated path to communicate or transfer the data between two devices. In that case, multiple stations access the channel and simultaneously transmits the data over the channel. It may create collision and cross talk. Hence, the multiple access protocol is required to reduce the collision and avoid crosstalk between the channels.

For example, suppose that there is a classroom full of students. When a teacher asks a question, all the students (small channels) in the class start answering the question at the same time (transferring the data simultaneously). All the students respond at the same time due to which data is overlap or data lost. Therefore it is the responsibility of a teacher (multiple access protocol) to manage the students and make them one answer.

Following are the types of multiple access protocol that is subdivided into the different process as:



A. Random Access Protocol

In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station. Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict. Due to the collision, the data frame packets may be lost or changed. And hence, it does not receive by the receiver end.

Following are the different methods of random-access protocols for broadcasting frames on the channel.

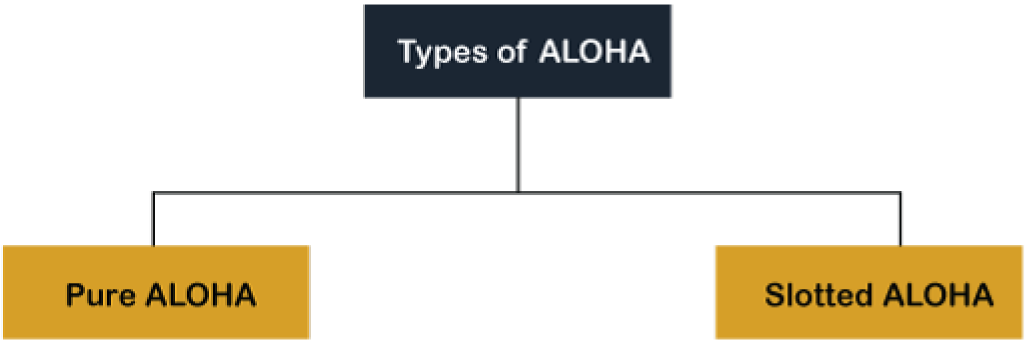
- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

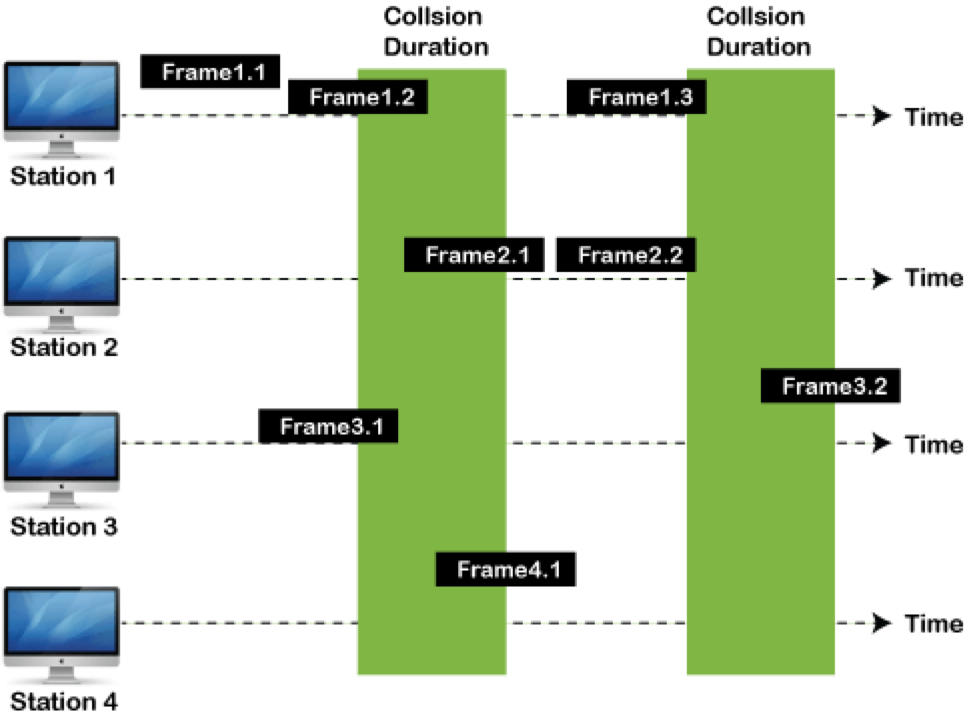
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.



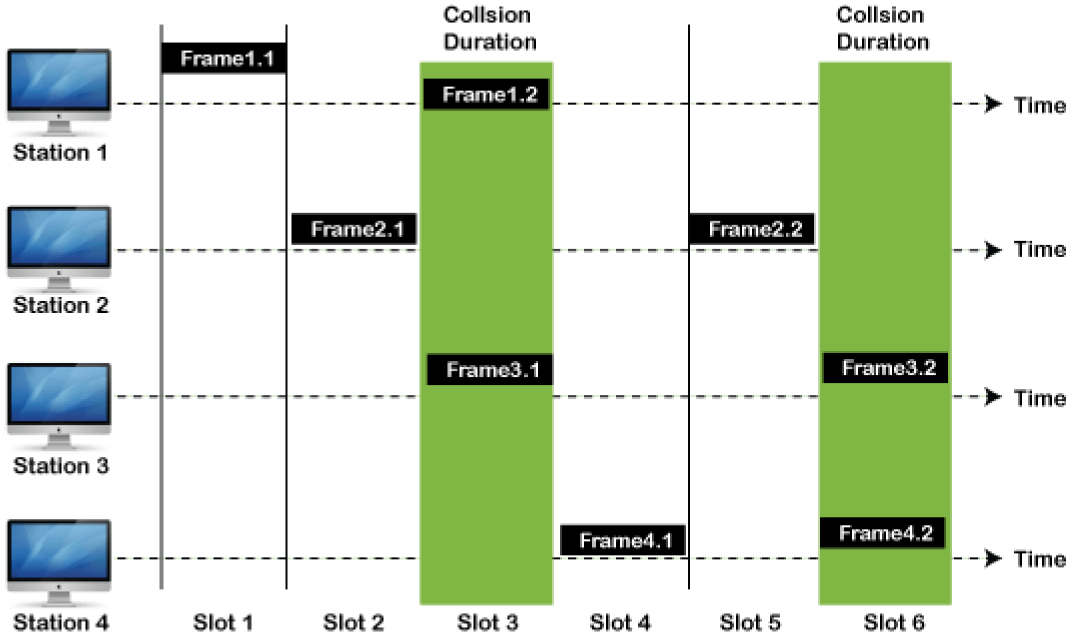
Frames in Pure ALOHA

As we can see in the figure above, there are four stations for accessing a shared channel and transmitting data frames. Some frames collide because most stations send their frames at the same time. Only two frames, frame 1.1 and frame 2.2, are successfully transmitted to the receiver end. At the same time, other frames are lost or destroyed. Whenever two frames fall on a shared channel simultaneously, collisions can occur, and both will suffer damage. If the new frame's first bit enters the channel before finishing the last bit of the second frame. Both frames are completely finished, and both stations must retransmit the data frame.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.



Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

It is a **carrier sense multiple access** based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

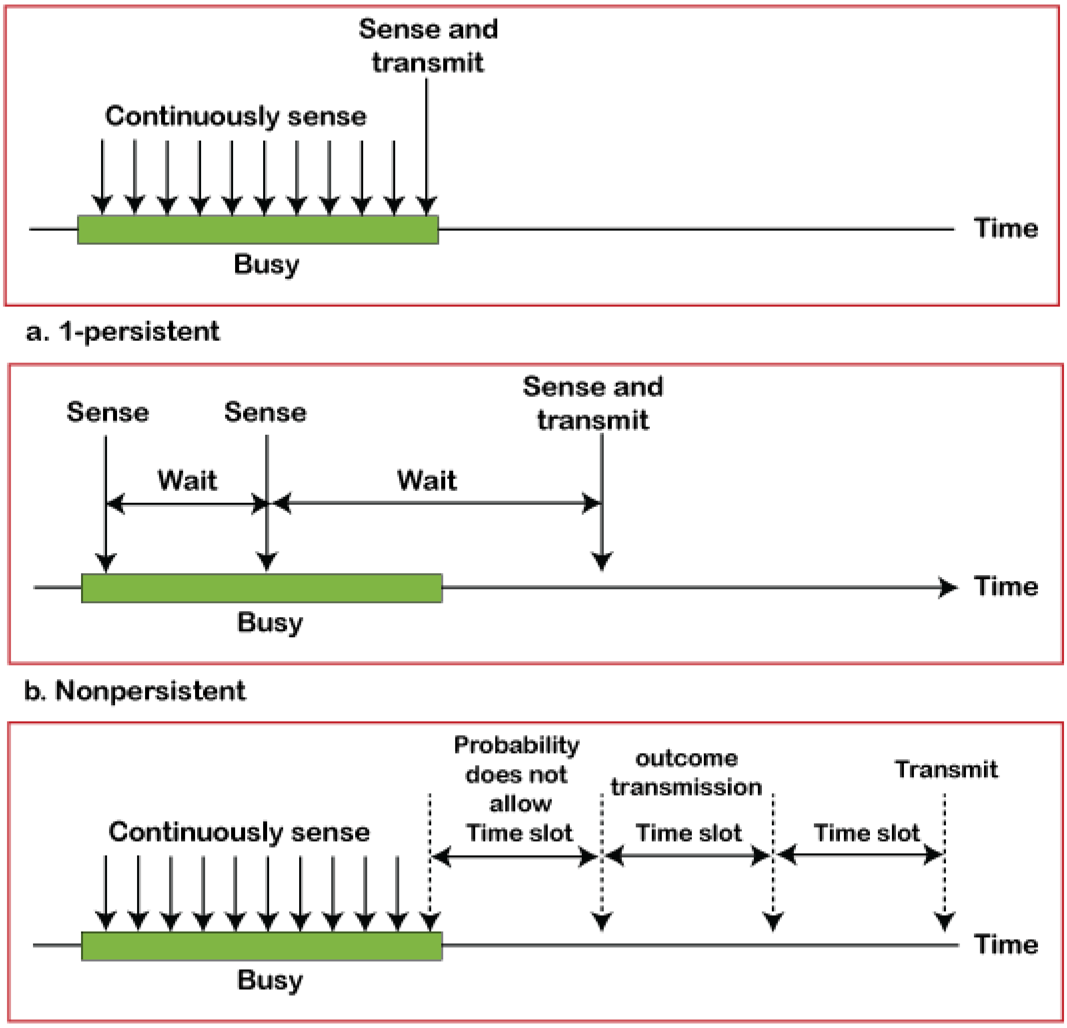
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.

Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

P-Persistent: It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.

O- Persistent: It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.



a. 1-persistent

b. Nonpersistent

c. p-persistent

CSMA/ CD

It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer. Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful. If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer. When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver. But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:

Interframe space: In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Interframe** space or IFS. However, the IFS time is often used to define the priority of the station.

Contention window: In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.

Acknowledgment: In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

B. Controlled Access Protocol

It is a method of reducing data frame collision on a shared channel. In the controlled access method, each station interacts and decides to send a data frame by a particular station approved by all other stations. It means that a single station cannot send the data frames unless all other stations are not approved. It has three types of controlled access: **Reservation, Polling**, and **Token Passing**.

C. Channelization Protocols

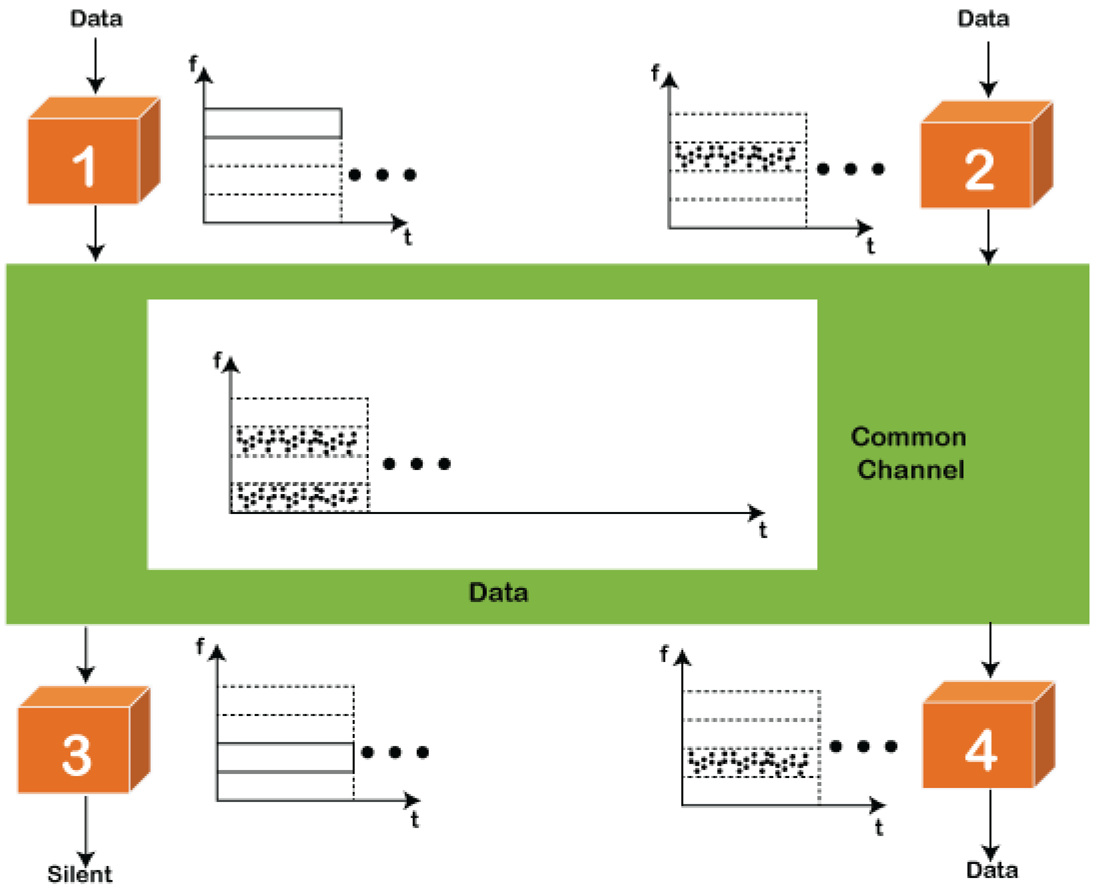
It is a channelization protocol that allows the total usable bandwidth in a shared channel to be shared across multiple stations based on their time, distance and codes. It can access all the stations at the same time to send the data frames to the channel.

Following are the various methods to access the channel based on their time, distance and codes:

1. FDMA (Frequency Division Multiple Access)
2. TDMA (Time Division Multiple Access)
3. CDMA (Code Division Multiple Access)

FDMA

It is a frequency division multiple access (**FDMA**) method used to divide the available bandwidth into equal bands so that multiple users can send data through a different frequency to the subchannel. Each station is reserved with a particular band to prevent the crosstalk between the channels and interferences of stations.



TDMA

Time Division Multiple Access (**TDMA**) is a channel access method. It allows the same frequency bandwidth to be shared across multiple stations. And to avoid collisions in the shared channel, it divides the channel into different frequency slots that allocate stations to transmit the data frames. The same **frequency** bandwidth into the shared channel by dividing the signal into various time slots to transmit it. However, TDMA has an overhead of synchronization that specifies each station's time slot by adding synchronization bits to each slot.

CDMA

The code division multiple access (CDMA) is a channel access method. In CDMA, all stations can simultaneously send the data over the same channel. It means that it allows each station to transmit the data frames with full frequency on the shared channel at all times. It does not require the division of bandwidth on a shared channel based on time slots. If multiple stations send data to a channel simultaneously, their data frames are separated by a unique code sequence. Each station has a different unique code for transmitting the data over a shared channel. For example, there are multiple users in a room that are continuously speaking. Data is received by the users if only two-person interact with each other using the same language. Similarly, in the network, if different stations communicate with each other simultaneously with different code language.

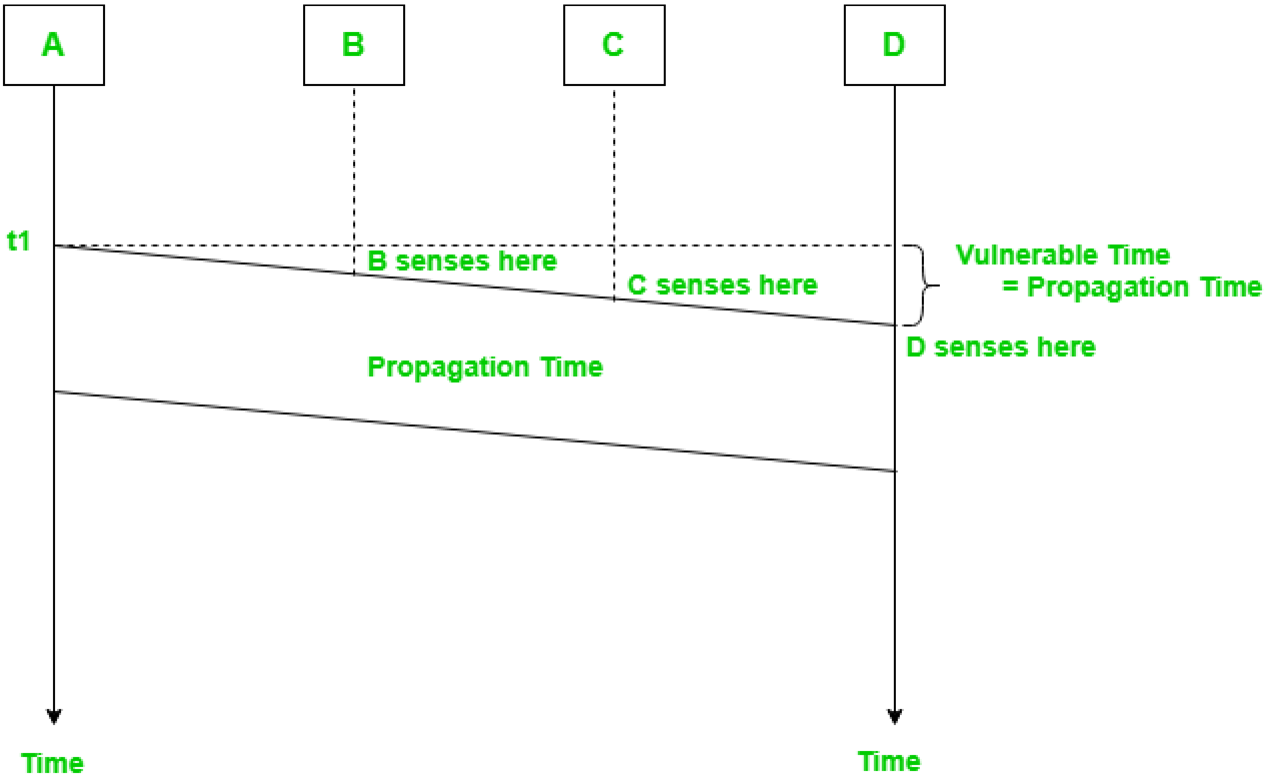
6. Briefly explain the concept of Carrier Sense Multiple Access protocol in detail.

This method was developed to decrease the chances of collisions when two or more stations start sending their signals over the data link layer. Carrier Sense multiple access requires that each station **first check the state of the medium** before sending.

Prerequisite - Multiple Access Protocols

Vulnerable Time:

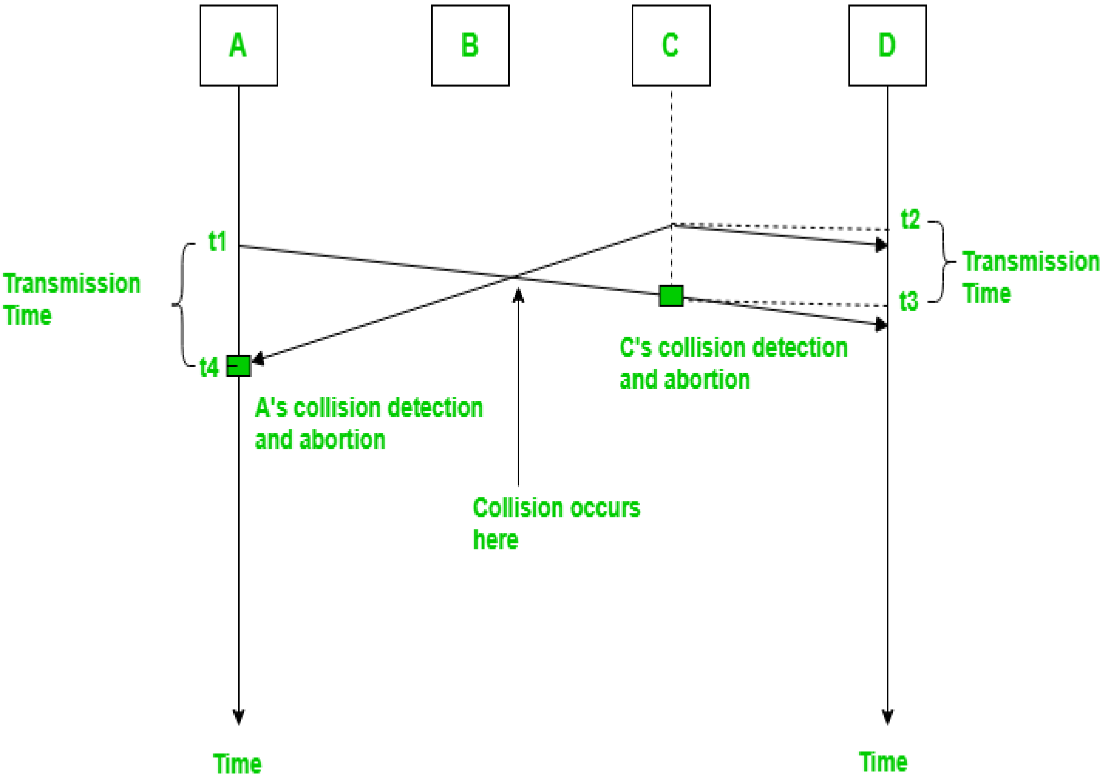
Vulnerable time = Propagation time (Tp)



The persistence methods can be applied to help the station take action when the channel is busy/idle.

1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

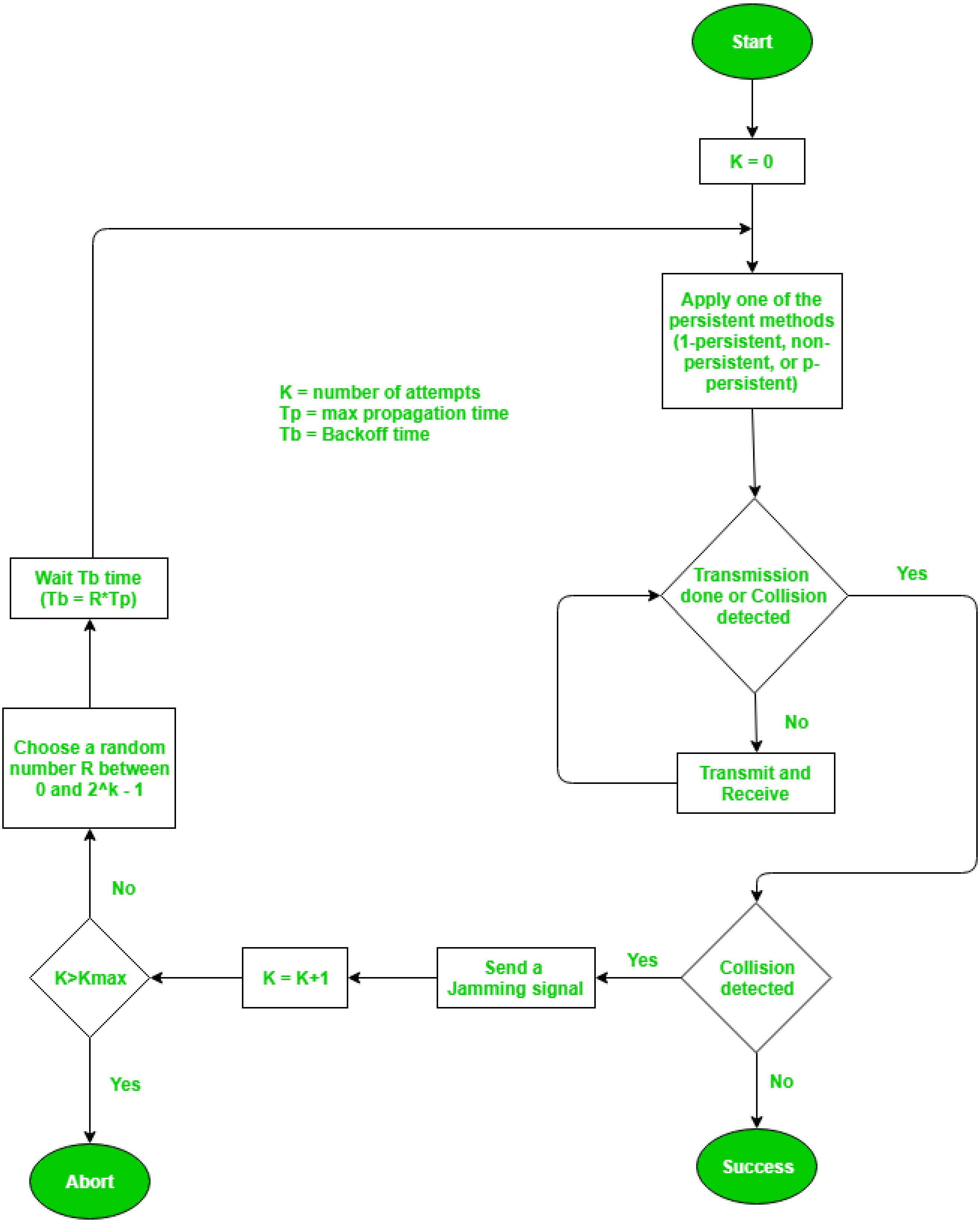
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.



In the diagram, starts sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1

So, the **frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp)**. This can be deduced when the two stations involved in a collision are a maximum distance apart.

Process: The entire process of collision detection can be explained as follows:


Start
K = 0
Apply one of the persistent methods (1-persistent, non-persistent, or p-persistent)
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Transmission done or Collision detected
Yes
No
Transmit and Receive
Wait Tb time (Tb = R*Tp)
Choose a random number R between 0 and 2^k - 1
No
K>Kmax
K = K+1
Send a Jamming signal
Yes
Collision detected
Yes
No
Abort
Success

Throughput and Efficiency: The throughput of CSMA/CD is much greater than pure or slotted ALOHA.

- For the 1-persistent method, throughput is 50% when G=1.
- For the non-persistent method, throughput can go up to 90%.

2. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) –

The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations. In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can't be used by the station to sense collision. Therefore **CSMA/CA has been specially designed for wireless networks**.

These are three types of strategies:

1. **InterFrame Space (IFS):** When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called **IFS time**. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
2. **Contention Window:** It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as **wait time**.
3. **Acknowledgments:** The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

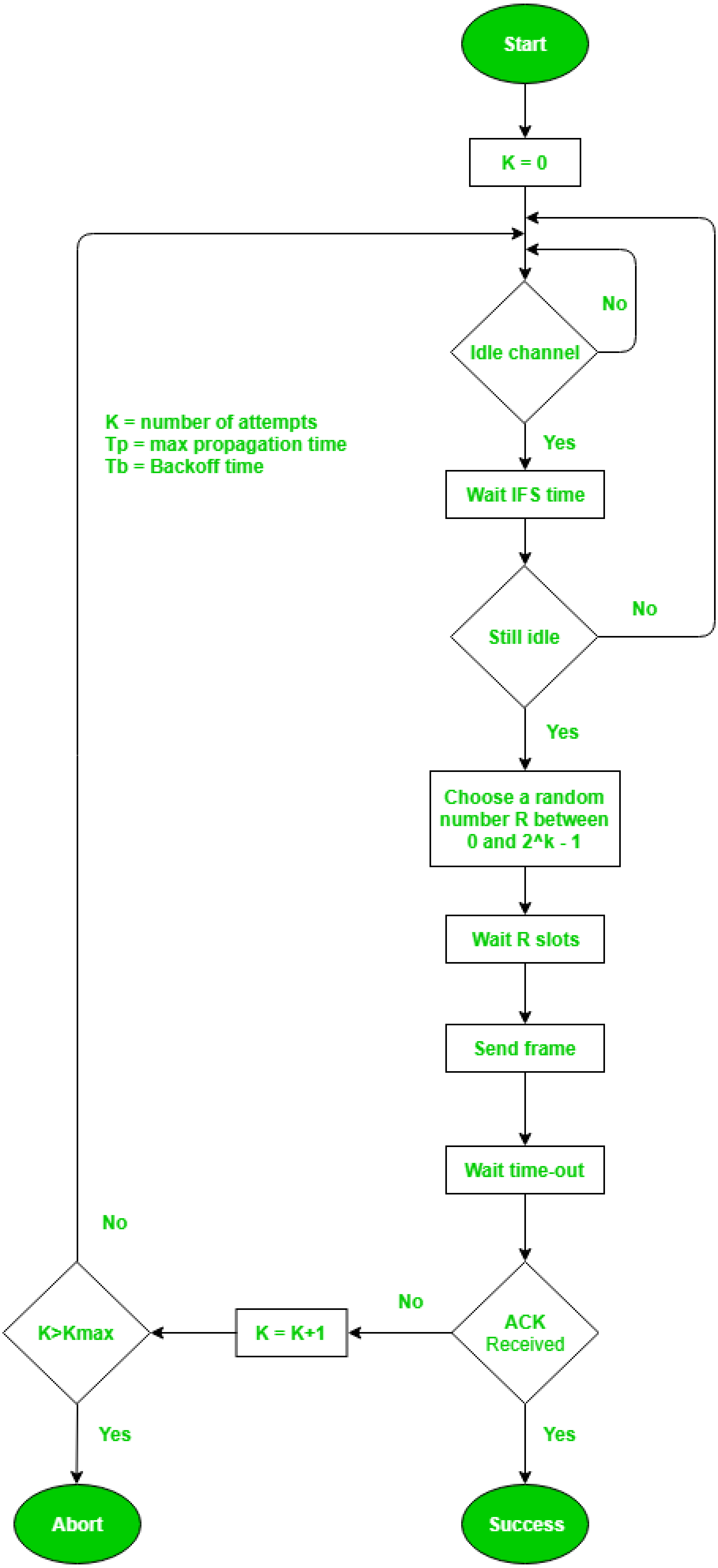
Characteristics of CSMA/CA :

1. **Carrier Sense**: The device listens to the channel before transmitting, to ensure that it is not currently in use by another device.
2. **Multiple Access**: Multiple devices share the same channel and can transmit simultaneously.
3. **Collision Avoidance**: If two or more devices attempt to transmit at the same time, a collision occurs. CSMA/CA uses random backoff time intervals to avoid collisions.
4. **Acknowledgment (ACK)**: After successful transmission, the receiving device sends an ACK to confirm receipt.
5. **Fairness**: The protocol ensures that all devices have equal access to the channel and no single device monopolizes it.
6. **Binary Exponential Backoff**: If a collision occurs, the device waits for a random period of time before attempting to retransmit. The backoff time increases exponentially with each retransmission attempt.
7. **Interframe Spacing**: The protocol requires a minimum amount of time between transmissions to allow the channel to be clear and reduce the likelihood of collisions.
8. **RTS/CTS Handshake**: In some implementations, a Request-To-Send (RTS) and Clear-To-Send (CTS) handshake is used to reserve the channel before transmission. This reduces the chance of collisions and increases efficiency.
9. **Wireless Network Quality**: The performance of CSMA/CA is greatly influenced by the quality of the wireless network, such as the strength of the signal, interference, and network congestion.

10. **Adaptive Behavior**: CSMA/CA can dynamically adjust its behavior in response to changes in network conditions, ensuring the efficient use of the channel and avoiding congestion.

Overall, CSMA/CA balances the need for efficient use of the shared channel with the need to avoid collisions, leading to reliable and fair communication in a wireless network.

Process: The entire process of collision avoidance can be explained as follows:


Start
K = 0
Idle channel
No
Yes
K = number of attempts
Tp = max propagation time
Tb = Backoff time
Wait IFS time
Still idle
No
Yes
Choose a random number R between 0 and 2^k - 1
Wait R slots
Send frame
Wait time-out
No
K>Kmax
K = K+1
No
ACK Received
Yes
Yes
Abort
Success

Types of CSMA Access Modes:
There are 4 types of access modes available in CSMA. It is also referred as 4 different types of CSMA protocols which decide the time to start sending data across shared media.

1. **1-Persistent:** It senses the shared channel first and delivers the data right away if the channel is idle. If not, it must wait and **continuously** track for the channel to become idle and then broadcast the frame without condition as soon as it does. It is an aggressive transmission algorithm.
2. **Non-Persistent:** It first assesses the channel before transmitting data; if the channel is idle, the node transmits data right away. If not, the station must wait for an arbitrary amount of time (**not continuously**), and when it discovers the channel is empty, it sends the frames.
3. **P-Persistent:** It consists of the 1-Persistent and Non-Persistent modes combined. Each node observes the channel in the 1Persistent mode, and if the channel is idle, it sends a frame with a P probability. If the data is not transferred, the frame restarts with the following time slot after waiting for a (q = 1-p probability) random period.
4. **O-Persistent:** A supervisory node gives each node a transmission order. Nodes wait for their time slot according to their allocated transmission sequence when the transmission medium is idle.

Advantages of CSMA:

1. **Increased efficiency:** CSMA ensures that only one device communicates on the network at a time, reducing collisions and improving network efficiency.
2. **Simplicity:** CSMA is a simple protocol that is easy to implement and does not require complex hardware or software.
3. **Flexibility:** CSMA is a flexible protocol that can be used in a wide range of network environments, including wired and wireless networks.
4. **Low cost:** CSMA does not require expensive hardware or software, making it a cost-effective solution for network communication.

Disadvantages of CSMA:

1. **Limited scalability:** CSMA is not a scalable protocol and can become inefficient as the number of devices on the network increases.
2. **Delay:** In busy networks, the requirement to sense the medium and wait for an available channel can result in delays and increased latency.
3. **Limited reliability:** CSMA can be affected by interference, noise, and other factors, resulting in unreliable communication.
4. **Vulnerability to attacks:** CSMA can be vulnerable to certain types of attacks, such as jamming and denial-of-service attacks, which can disrupt network communication.

Comparison of various protocols:

Protocol	**Transmission behavior**	**Collision detection method**	**Efficiency**	**Use cases**
Pure ALOHA	Sends frames immediately	No collision detection	Low	Low-traffic networks
Slotted ALOHA	Sends frames at specific time slots	No collision detection	Better than pure ALOHA	Low-traffic networks
CSMA/CD	Monitors medium after sending a frame, retransmits if necessary	Collision detection by monitoring transmissions	High	Wired networks with moderate to high traffic
CSMA/CA	Monitors medium while transmitting, adjusts behavior to avoid collisions	Collision avoidance through random backoff time intervals	High	Wireless networks with moderate to high traffic and high error rates

12,13,14 Controlled Access Protocols
Reservation, Polling & Token Passing
Can two people speak at the same time and still understand each other's statements? Well, not. The same goes for data frames **in a computer network**. If we transmit two frames at a time, they'll collide with each other, and data will get lost.

Before discussing Controlled access protocols, please refer to Random access protocols.

So **how are controlled access protocols different from random access protocols?**

The difference is, only that station can transmit the data which is approved by all other stations in that network. And we saw that in random access protocols, the transmission is based on the availability of the transmission channel.

So, here in controlled access protocols, only one station can transmit the data frames at a time, which leads us to a collision-free transmission through the communication channel.

Let us now discuss the types of controlled access protocols. There are three types of Controlled access protocols:

1. **Reservation**
2. **Polling**
3. **Token Passing**

Let's learn about them one by one.

Controlled Access Protocols

1) Reservation in Computer Network

Whenever we travel on a train or an airplane, the first thing we do is to reserve our seats, similarly, here a station must make a reservation first before transmitting any data frames.

This reservation in the Computer Network timeline consists of two kinds of periods:

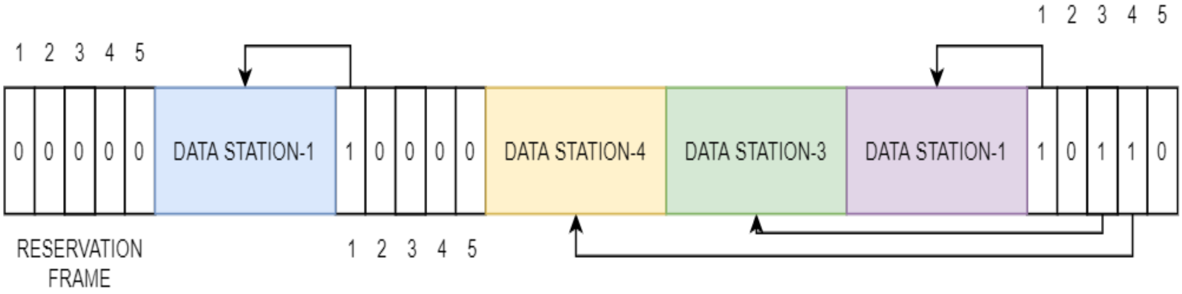
1. Reservation interval of a fixed time duration
2. Data transmission period of variable frames

Consider there are 4 stations then the reservation intervals are divided into 4 slots so that each station has a slot. This means if n number of stations are there then n slot will be allotted.

Now let us assume that these 4 stations are 4 friends, now if friend-1 speaks in his slot-1 then no other friend can speak at this time. Similarly, if station-1 transmits a 1-bit data frame in slot-1 then at that time no other station can transmit its data frames and they must wait for their time slot. After all the slots have been transmitted and checked then each station knows which station now wishes for transmission.

The biggest advantage of this method is since all stations agree on which station is next to transmit then there are no possible collisions.

The illustration below shows a scenario with five stations with a five-slot reservation frame. here, in the time interval stations 1,3,4 are the only stations with reservations, and in the second interval, station-1 is the only station with a reservation.



2) Polling in Computer Network

Recall your school or college classroom, what was the first thing the teacher does after entering the class? The answer is roll call or attendance. Let's compare the scenario. The teacher calls roll number 1 and gets a response if he/she is present then switches to the next roll number, say roll number two and roll number 2 is absent, so the teacher gets no response in return or say a negative response. Similarly, in a computer network, there is a primary station or controller (teacher) and all other stations are secondary (students), the primary station sends a message to each station. The message which is sent by the primary station consists of the address of the station which is selected for granting access.

The point to remember is that all the nodes receive the message but the addressed one responds and sends data in return, but if the station has no data to transmit then it sends a message called **Poll Reject or NAK** (negative acknowledgment).

But this method has some drawbacks like the high overhead of the polling messages and high dependence on the reliability of the primary station.

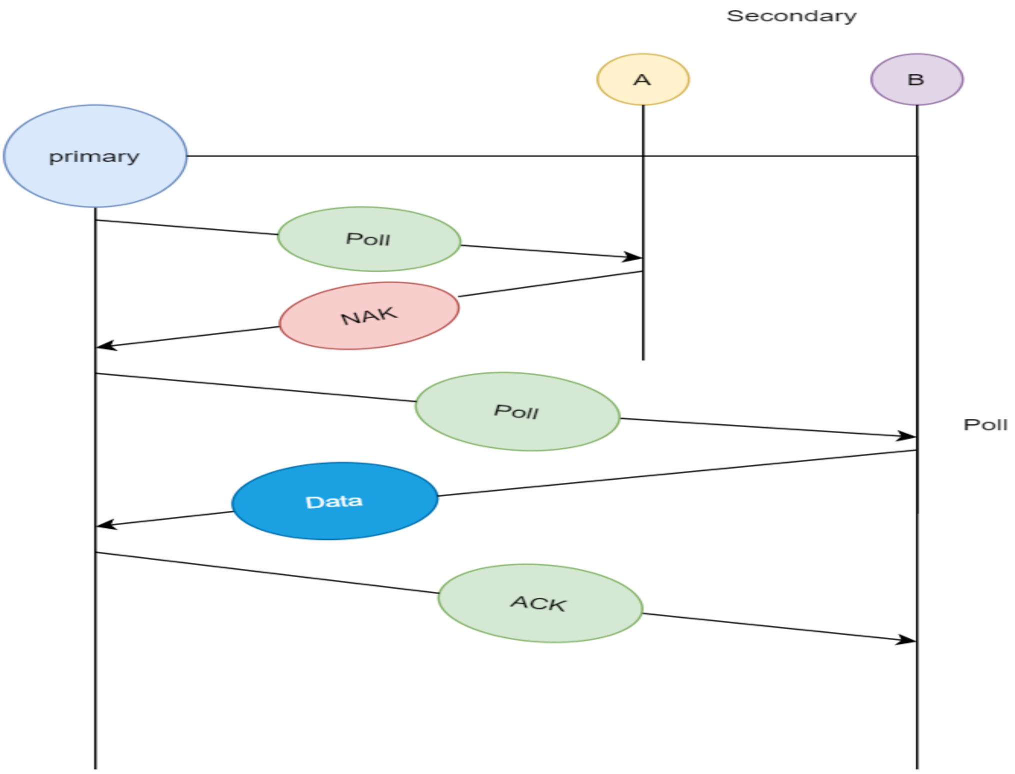
We calculate the efficiency of this method in terms of time for polling & time required for transmission of data.

Tpoll = time for polling

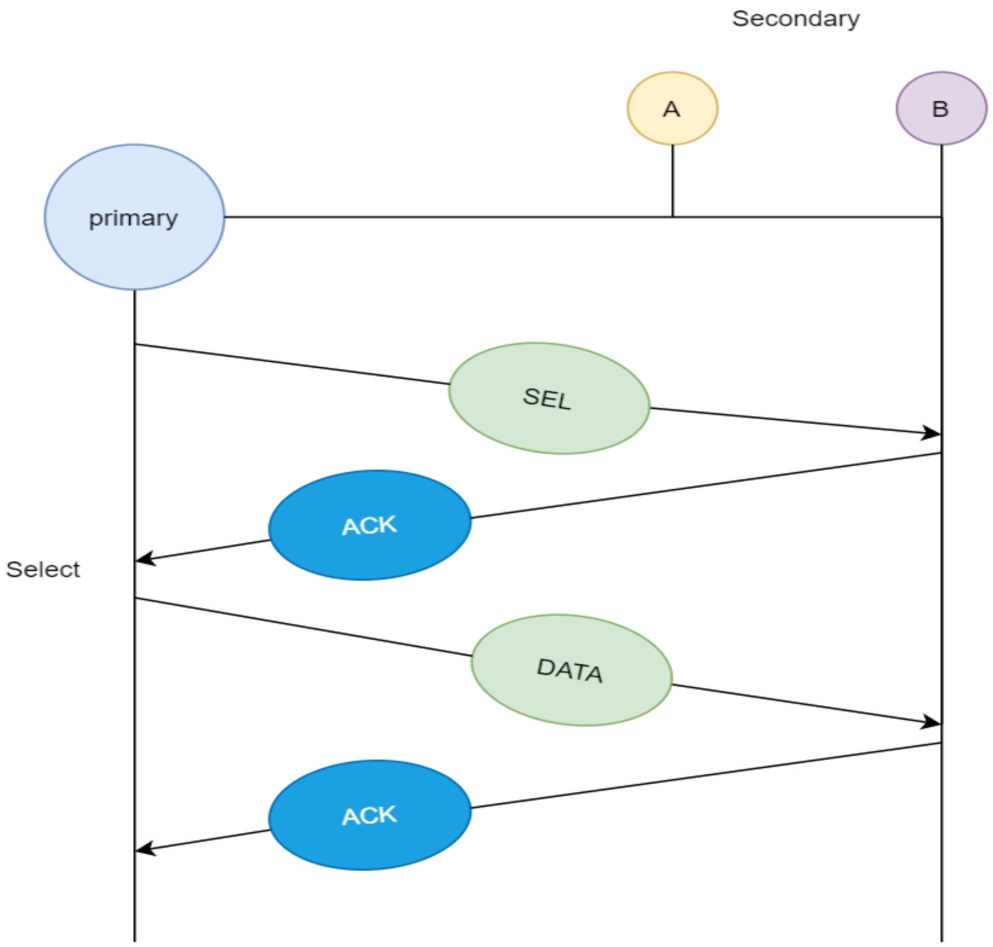
Tt = time required for transmission of data

So, **efficiency = Tt / (Tt + Tpoll)**

Whenever the primary station wants to receive the data, it asks the secondary stations present in its channel, this method is **polling**. In the first diagram, we see that the primary station asks station A if it has any data ready for transmission, since A does not have any data queued for transmission it sends NAK (negative acknowledgment), and then it asks station B since B has data ready for transmission, so it transmits the data and in return receives an acknowledgment from the primary station.



In the next case, if the primary station wants to send data to the secondary stations, it sends a select message, and if the secondary station accepts the request from the primary station, then it sends back an acknowledgment, and then the primary station transmits the data and in return receives an acknowledgment.



3) Token Passing in Computer Network

Now, say 4 people are sitting on a round table and only that person can speak who has the token. In computer networks, a token is a special bit pattern that allows the token-possessing system to send data or we can say that a token represents permission to transmit data. The token circulation around the table (or a network ring) is in a predefined order. A station can only pass the token to its adjacent station and not to any other station in the network. If a station has some data queued for transmission it can not transmit the data until it receives the token and makes sure it has transmitted all the data before passing on the received token.

This method has some drawbacks like duplication of tokens or sometimes the token being damaged or lost during circulation, or some times if we introduce a new station or remove an existing station from the network, this leads to a huge disturbance, which should be taken care of so that the efficiency of the method is not affected.

The performance of a token ring is governed by 2 parameters, which are delay and throughput.

Delay is a measure of the time; it is the time difference between a packet ready for transmission and when it is transmitted. Hence, the average time required to send a token to the next station is a/N.

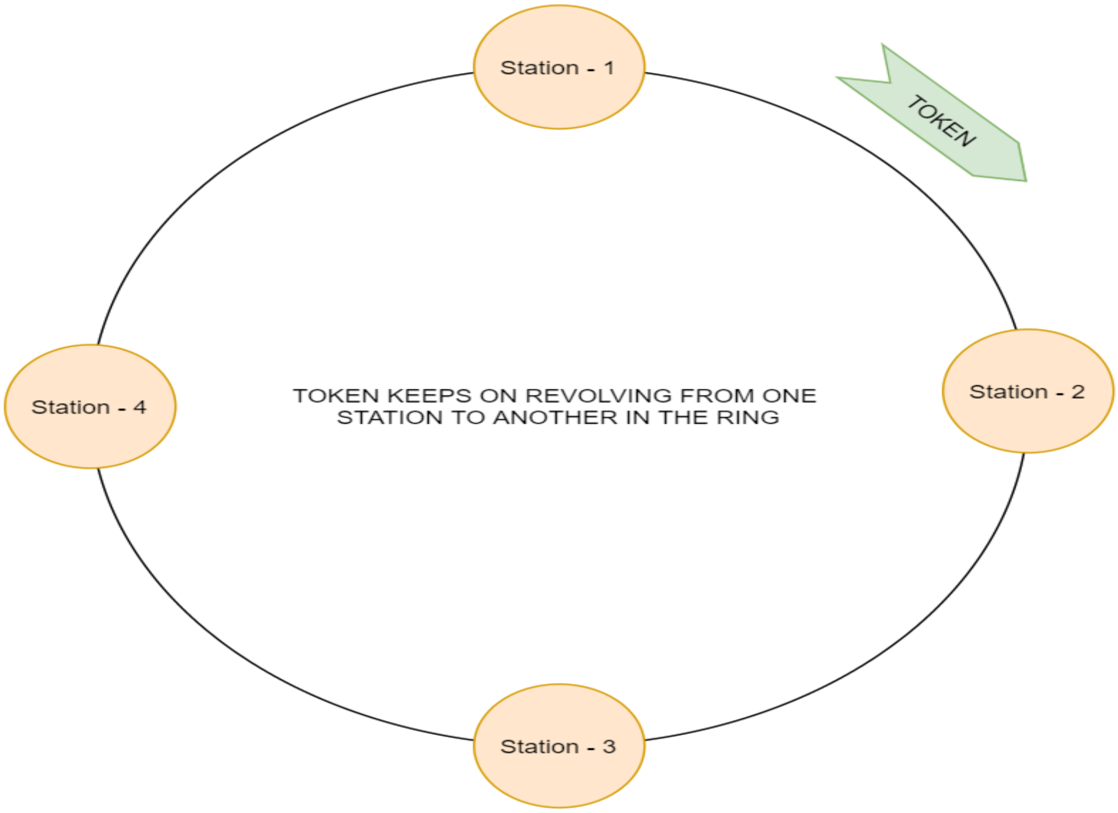
Throughput is a measure of the successful traffic in the communication channel.

Throughput, S = 1/ (1 + a/N) for a<1

S = 1/[a(1+1/N)] for a>1, here N = number of stations & a = Tp/Tt

Tp = propagation delay &Tt = transmission delay

In the diagram below when station-1 possesses the token it starts transmitting all the data frames which are in its queue. now after transmission, station-1 passes the token to station-2 and so on. Station-1 can now transmit data again, only when all the stations in the network have transmitted their data and passed the token.


Station - 1
TOKEN
Station - 4
TOKEN KEEPS ON REVOLVING FROM ONE STATION TO ANOTHER IN THE RING
Station - 2
Station - 3

Note: A token can only work in that channel, for which it is generated, and not for any other.

Conclusion

Controlled access protocols play a crucial role in managing access to shared resources in computer networks. Reservation, polling, and token passing are three widely used techniques for implementing controlled access protocols. While each of these techniques has its advantages and disadvantages, the choice of the protocol ultimately depends on the specific requirements and characteristics of the network.

By using these protocols effectively, network administrators can ensure fair and efficient access to shared resources while minimizing the risk of collisions and congestion.

1. What is a controlled access protocol?

A controlled access protocol is a technique used to manage access to shared resources in a network.

2. What is reservation in controlled access protocols?

Reservation is a technique in which a user reserves the resource before accessing it, ensuring exclusive access.

3. What is polling in controlled access protocols?

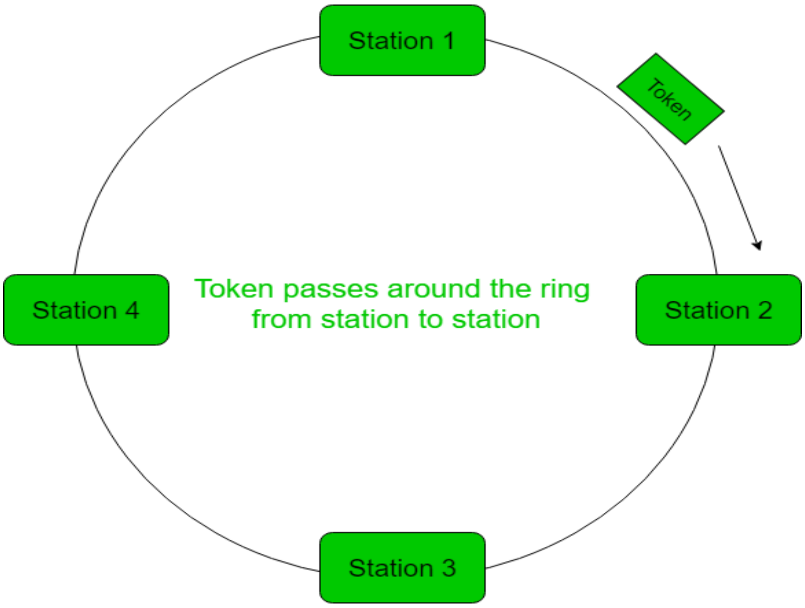
Polling is a technique where a device checks for the availability of the resource before accessing it.

4. What is token passing in controlled access protocols?

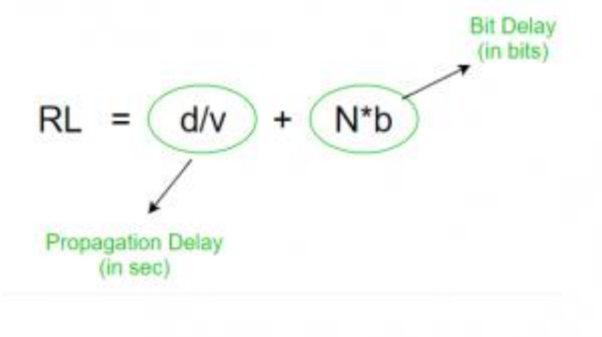
Token passing is a technique in which a token is passed from device to device, ensuring exclusive access to the resource.

14. Explain Token Ring technology

Token Ring protocol is a communication protocol used in Local Area Network (LAN). In a token ring protocol, the topology of the network is used to define the order in which stations send. The stations are connected to one another in a single ring. It uses a special three-byte frame called a **“token”** that travels around a ring. It makes use of Token Passing controlled access mechanism. Frames are also transmitted in the direction of the token. This way they will circulate around the ring and reach the station which is the destination.



Ring Latency –
The time taken by a single bit to travel around the ring is known as ring latency.



Where,
d = length of the ring
v = velocity of data in ring
N = no. of stations in ring
b = time taken by each station to hold the bit before transmitting it (bit delay)

Converting N*b into sec –

RL = d/v + (N*b)/B (B – bandwidth)

Converting d/v into bits –

RL = (d/v)*B + N*b (B – bandwidth)

Cycle Time –
The time taken by the token to complete one revolution of the ring is known as cycle time.

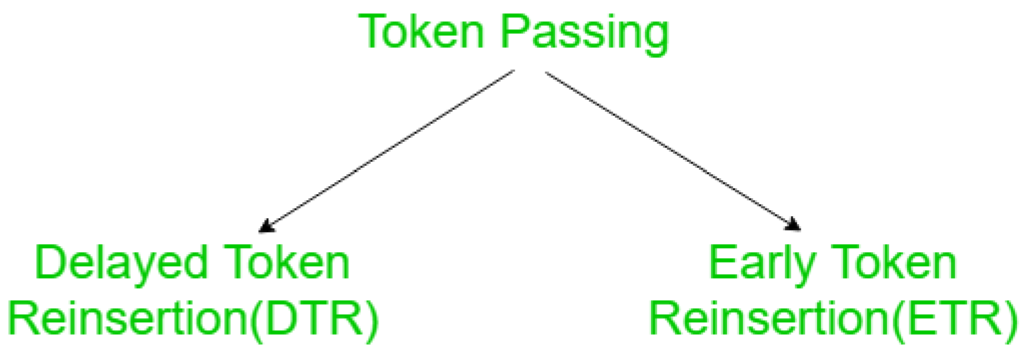
Cycle time = T_p + (THT*N)

Where, THT - Token Holding Time
T_p - Propagation delay(d/v)

Token Holding Time (THT) –

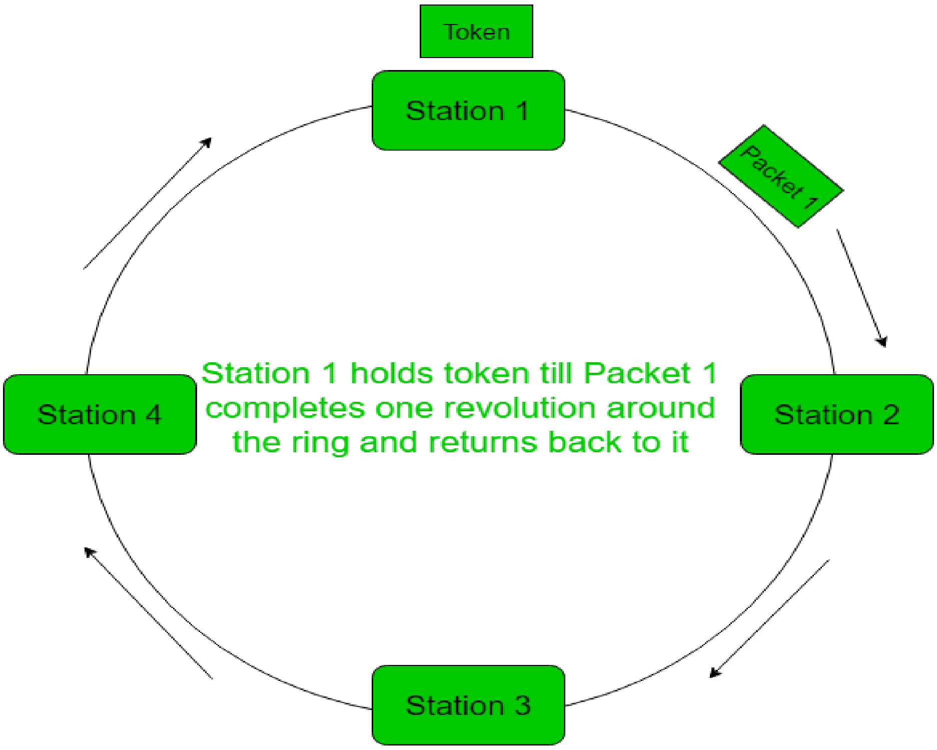
The maximum time a token frame can be held by a station is known as THT, by default it is set to 10msec. No station can hold the token beyond THT.

Calculating THT:



1. Delayed token reinsertion (DTR) –

- In this, the sender transmit the data packet and waits till the time the whole packet takes the round trip of the ring and return to it. When the whole packet is received by the sender, then it releases the token
- There is only one packet in the ring at an instance
- More reliable than ETR

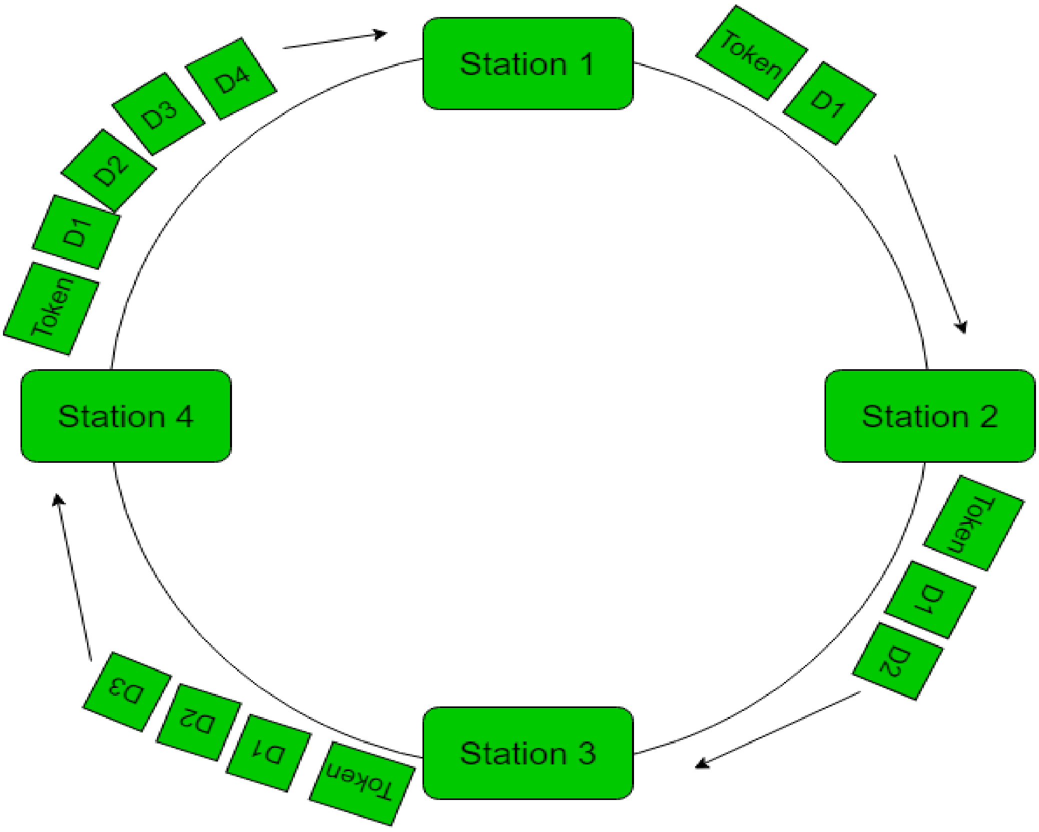

Token
Station 1
Packet 1
Station 4
Station 1 holds token till Packet 1 completes one revolution around the ring and returns back to it
Station 2
Station 3

In this case,

THT = T_t + RL
  = $T_t + T_p + N*b$ (In most cases, bit delay is 0)
So, THT = $T_t + T_p$
 where T_t = transmission delay
    T_p = propagation delay

2. Early token reinsertion (ETR) –

- Sender does not wait for the data packet to complete revolution before releasing the token. Token is released as soon as the data is transmitted
- Multiple packets present in the ring
- Less reliable than DTR



Station 1: Receives the token and transmits data D1 and then, releases the token.
Station 2: Receives D1 (puts it onto the other end) and the token and then, transmits data D2 and releases the token.
Station 3: Receives D1 –> transmits D1
Receives D2 –> transmits D2
Receives token –> transmits D3
Releases token.
Station 4: Receives D1 –> transmits D1
Receives D2 –> transmits D2

Receives D3 –> transmits D3
Receives token –> transmits D4
Releases token.

Station 1: Receives D1 –> discards D1 as D1 has completed its journey
Receives D2 –> transmits D2
Receives D3 –> transmits D3
Receives D4 –> transmits D4
Receives token –> transmits D1(new)
Releases token.
(and the cycle continues so on…..)
In this case,

THT = T_t
where T_t = transmission delay
T_p = propagation delay

Efficiency –

Efficiency, e = useful time/ total time
useful time = N*T_t
total time = cycle time = T_p + (THT*N)
So, e = (N*T_t)/(T_p + (THT*N))

1. Delayed token reinsertion –

In this case, THT = T_t + T_p
So, cycle time = T_p + N*(T_t + T_p)

Efficiency, e = (N*T$_{t)/(Tp + N*(Tt + Tp))}$

= 1/(1 + a*((N+1)/N))

where a = Tp/Tt

2. Early token reinsertion –

In this case, THT = T_t
So, cycle time = T_p + N*(T_t)

Efficiency, e = (N*T$_{t)/(Tp + N*(Tt))}$

= 1/(1 + a*(1/N))

where a = Tp/Tt