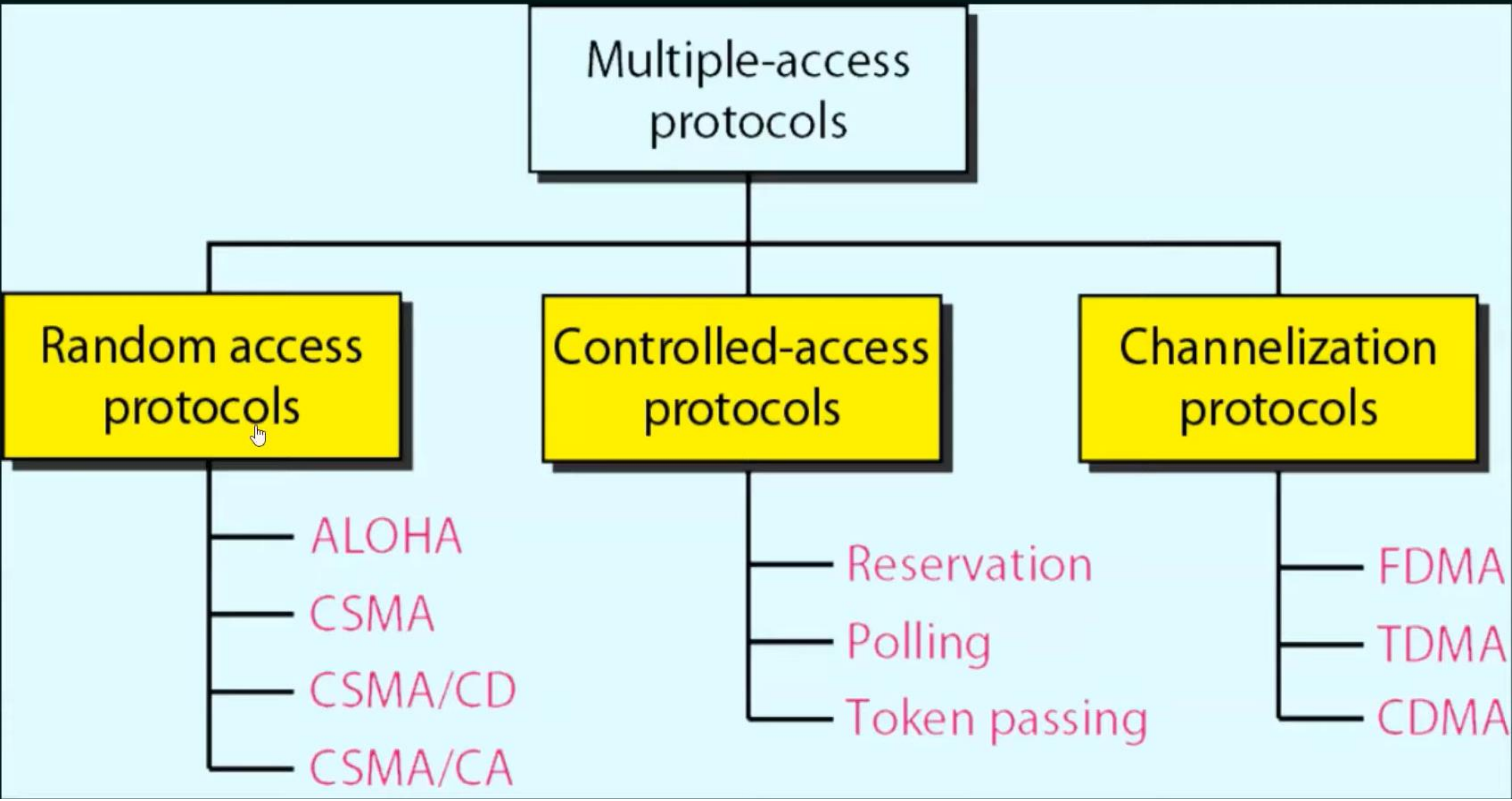
Why Multiple Access Protocols?

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

Hence multiple access protocols are required to decrease collision and avoid crosstalk.



Multiple-access protocols
Random access protocols
Controlled-access protocols
Channelization protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token passing
FDMA
TDMA
CDMA

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.

Channelization Protocols

Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.

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

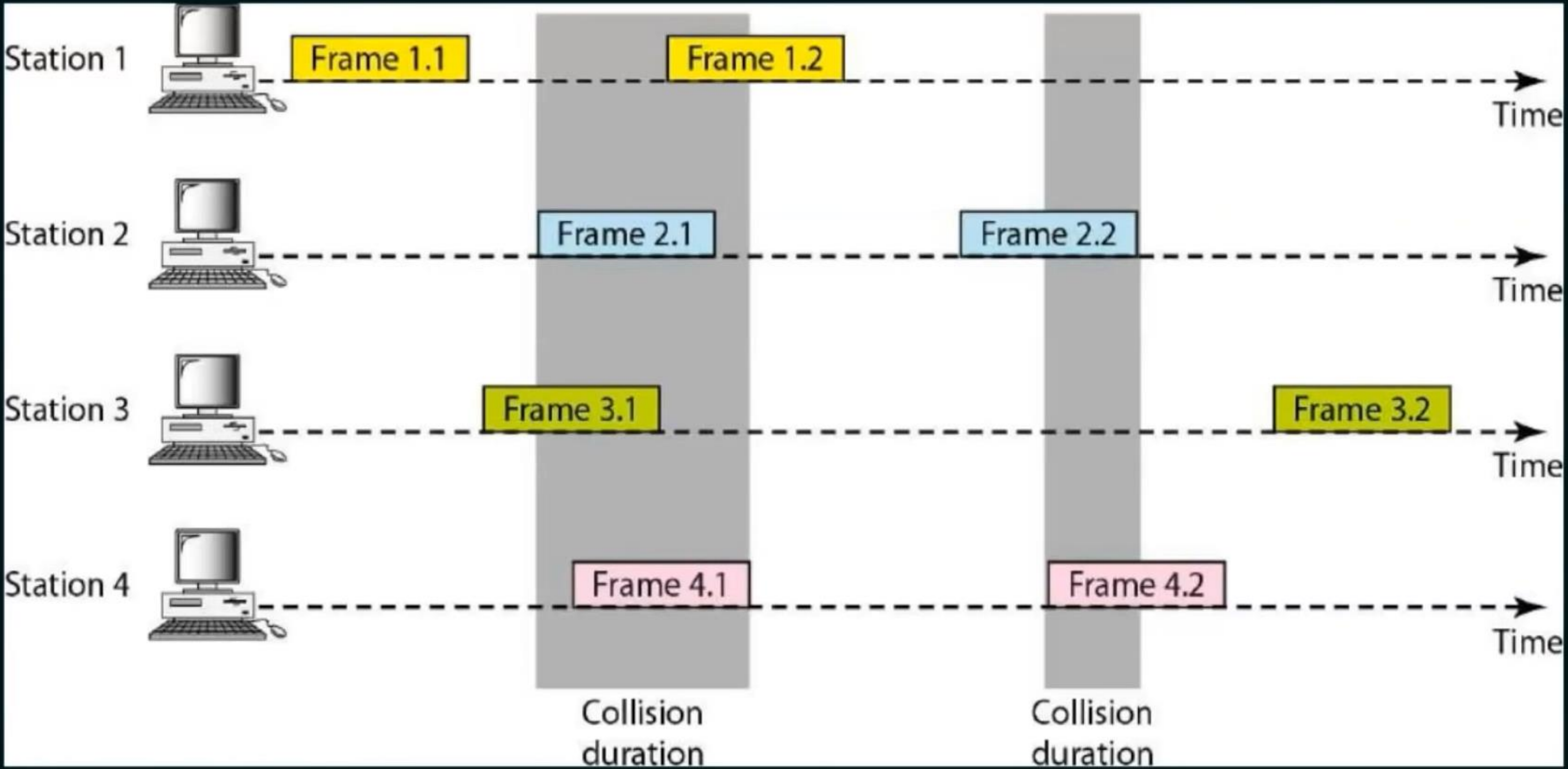
ALOHA

- ★ 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.

Types:

- ★ Pure Aloha
- ★ Slotted Aloha

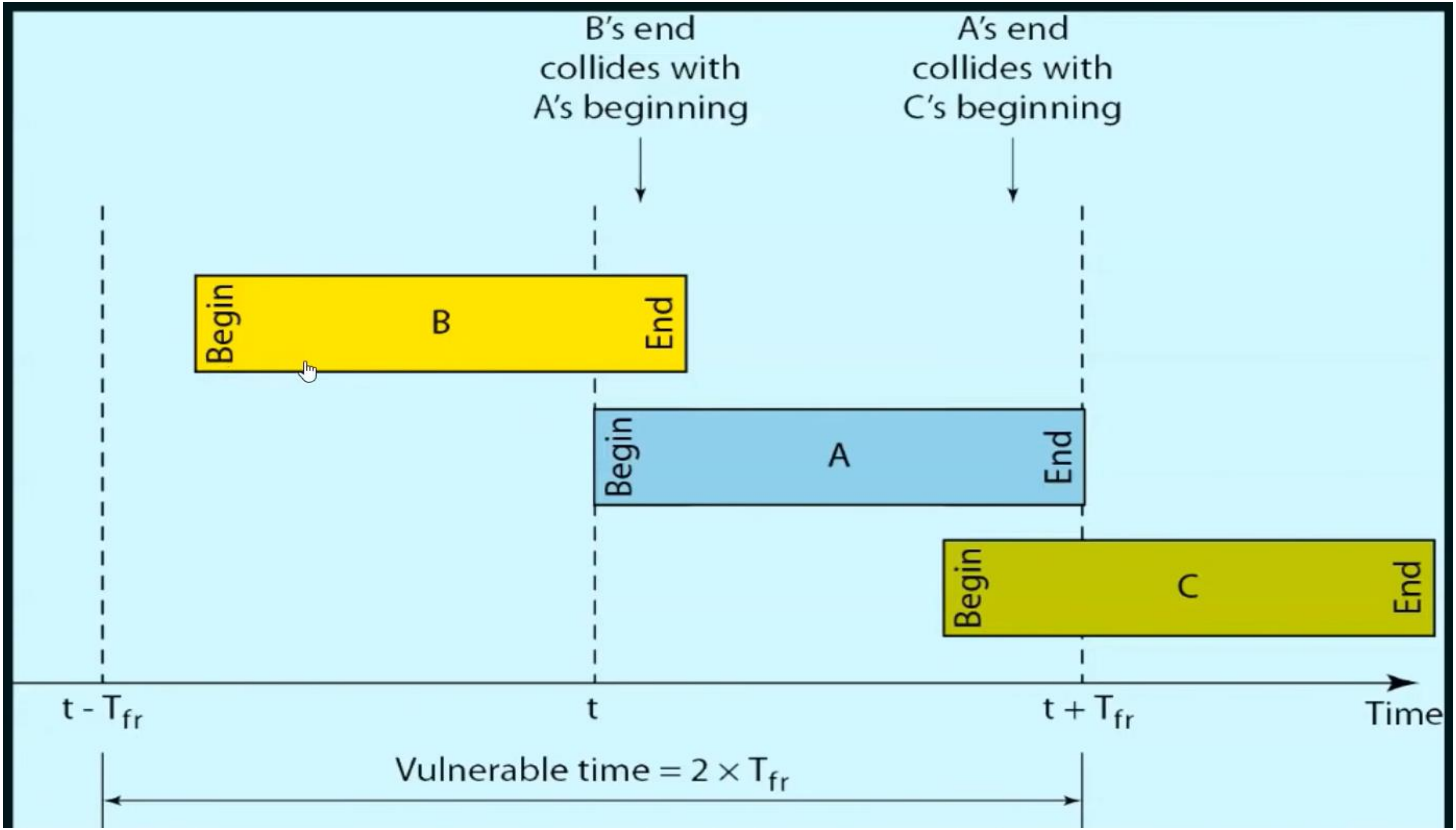
Pure aloha



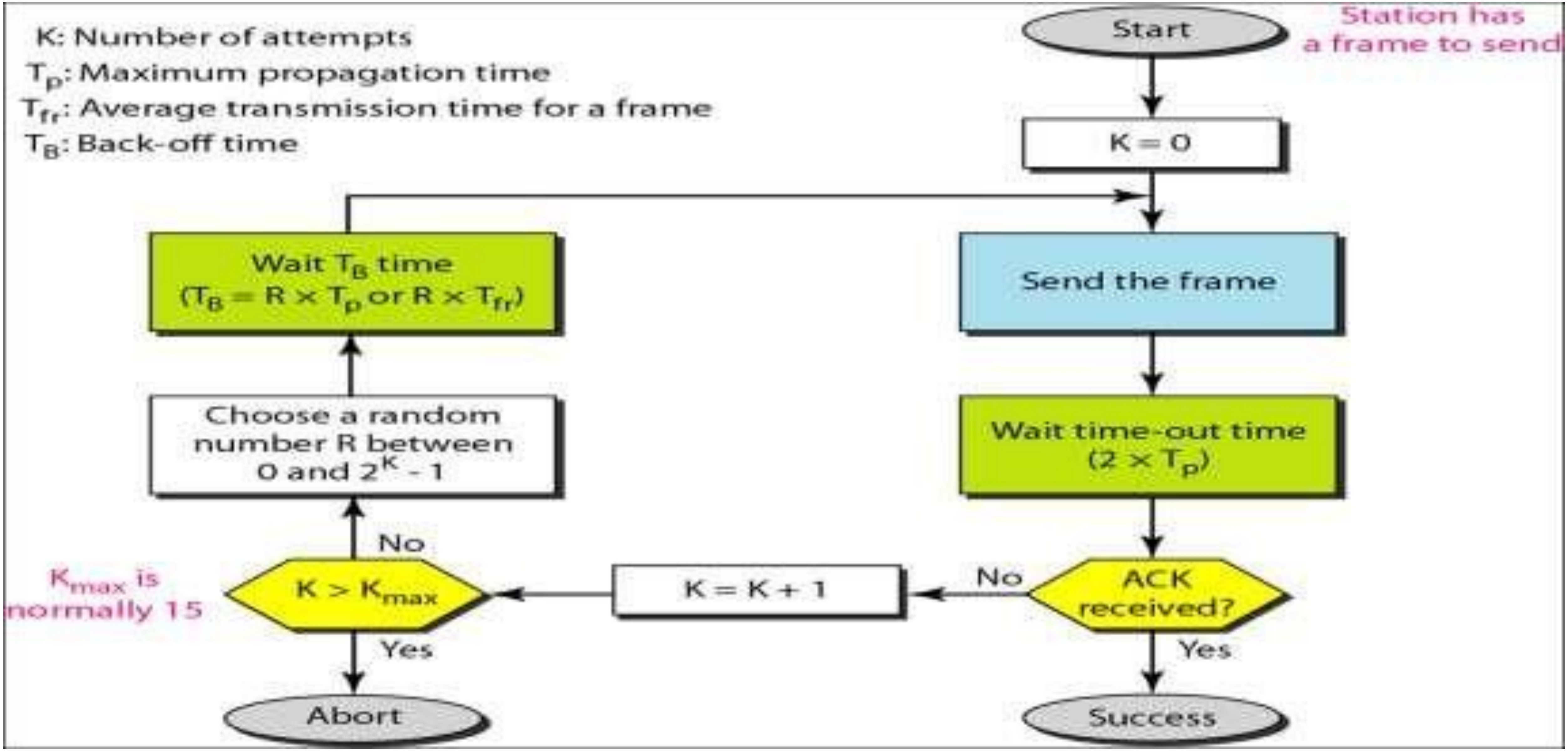
Station 1
Frame 1.1
Frame 1.2
Time
Station 2
Frame 2.1
Frame 2.2
Time
Station 3
Frame 3.1
Frame 3.2
Time
Station 4
Frame 4.1
Frame 4.2
Time
Collision duration
Collision duration

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.
- ★ The throughput of pure aloha is maximized when frames are of uniform length.


B's end collides with A's beginning
A's end collides with C's beginning
Begin
B
End
Begin
A
End
Begin
C
End
t - T_{fr}
t
t + T_{fr}
Time
Vulnerable time = $2 \times T_{fr}$

FLOW DIAGRAM FOR PURE ALOHA



Pure ALOHA

- 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.

Maximum throughput = 0.184 for G=0.5 (½)

Throughput of Pure ALOHA

$$\boxed{S = G \times e^{-2G}}$$

G = No. of frames generated by n/w in one Frame transmission time

- For maximum Throughput
- We put $\frac{ds}{dG} = 0$
- Maximum value of s occurs at $\boxed{G = \frac{1}{2}}$
- Substituting G = 1/2 in the above equation we get
- Maximum throughput of pure alone

$= \frac{1}{2} \times e^{-2\times\frac{1}{2}}$

$= \frac{1}{2e}$

$= 0.184$

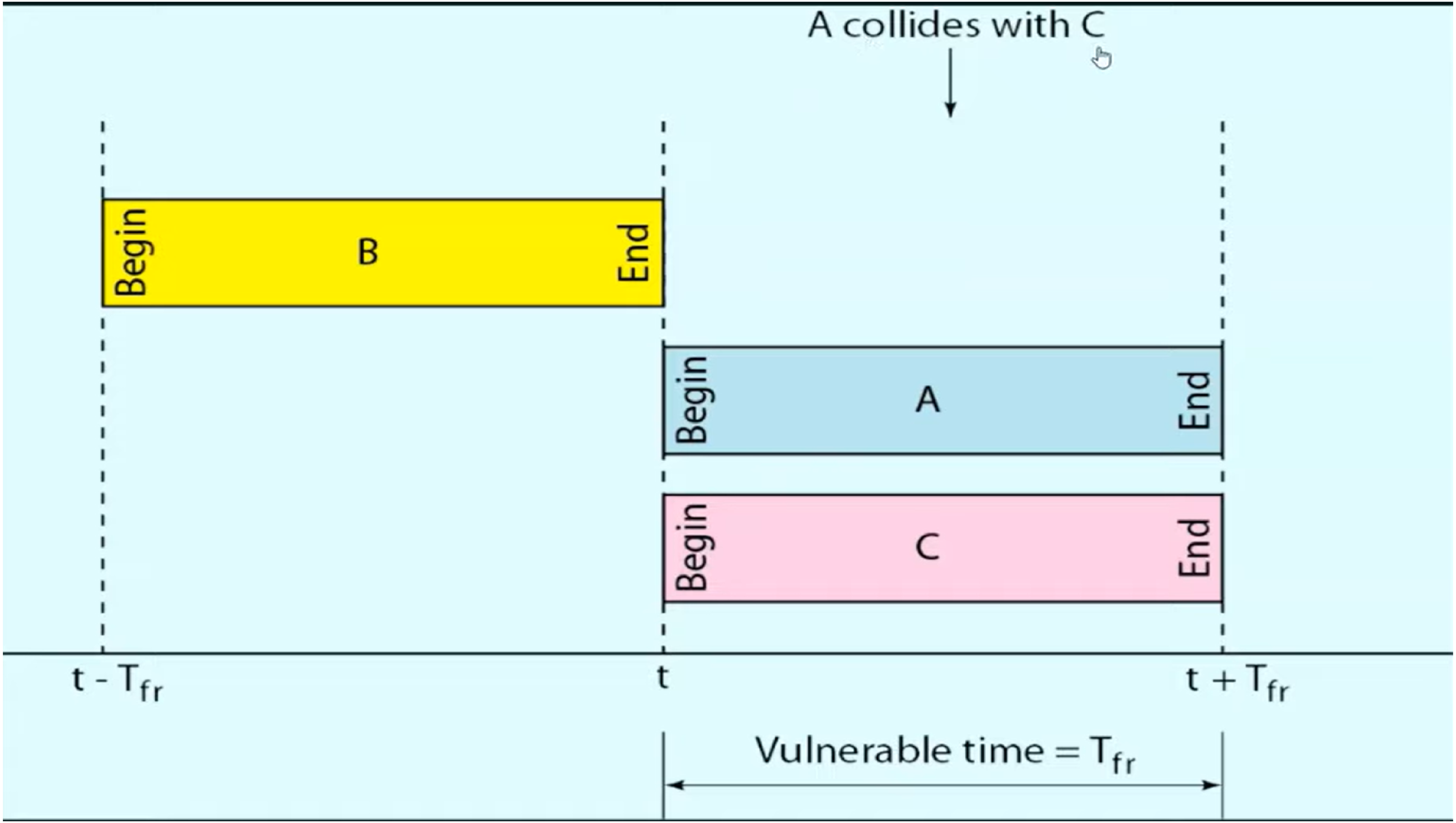
So maximum throughput of pure aloha = 18.4%

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.

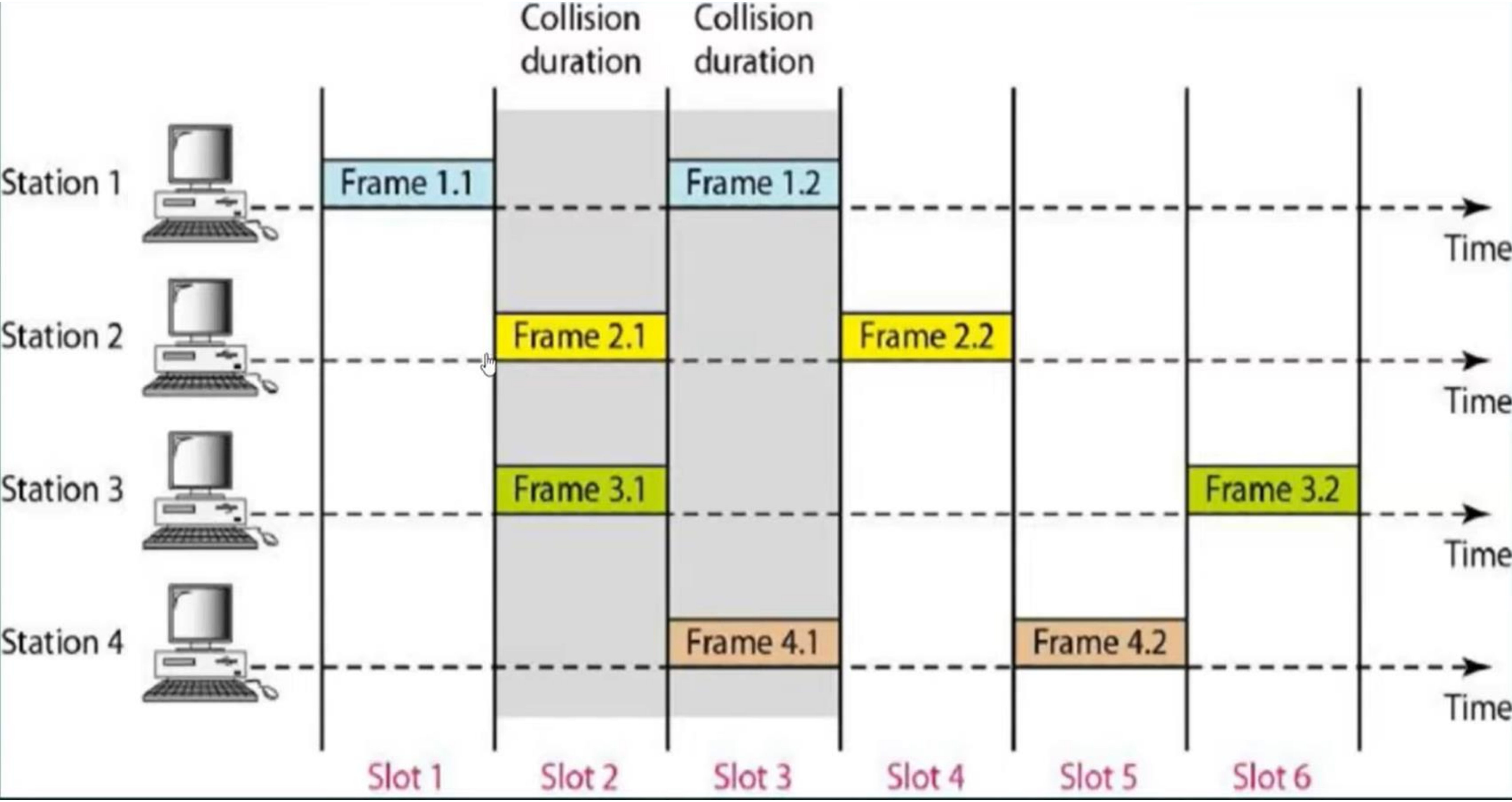
Types:

- Pure Aloha
- $\boxed{\star \text{ Slotted Aloha}}$


A collides with C
Begin
B
End
Begin
A
End
Begin
C
End
t - T_{fr}
t
t + T_{fr}
Vulnerable time = T_{fr}

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.


Collision duration
Collision duration
Station 1
Frame 1.1
Frame 1.2
Time
Station 2
Frame 2.1
Frame 2.2
Time
Station 3
Frame 3.1
Frame 3.2
Time
Station 4
Frame 4.1
Frame 4.2
Time
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5
Slot 6

Slotted aloha

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.

Throughput of Slotted ALOHA

$\boxed{S = G \times e^{-G}}$

G = No. of frames generated by n/w in one Frame transmission time

For maximum Throughput

- We put $\frac{ds}{dG} = 0$
- Maximum value of s occurs at $G = 1$
- Substituting G = 1 in the above equation we get
- Maximum throughput of pure alone

$= 1 \times e^{-1}$

$= \frac{1}{e}$

$= 0.368$

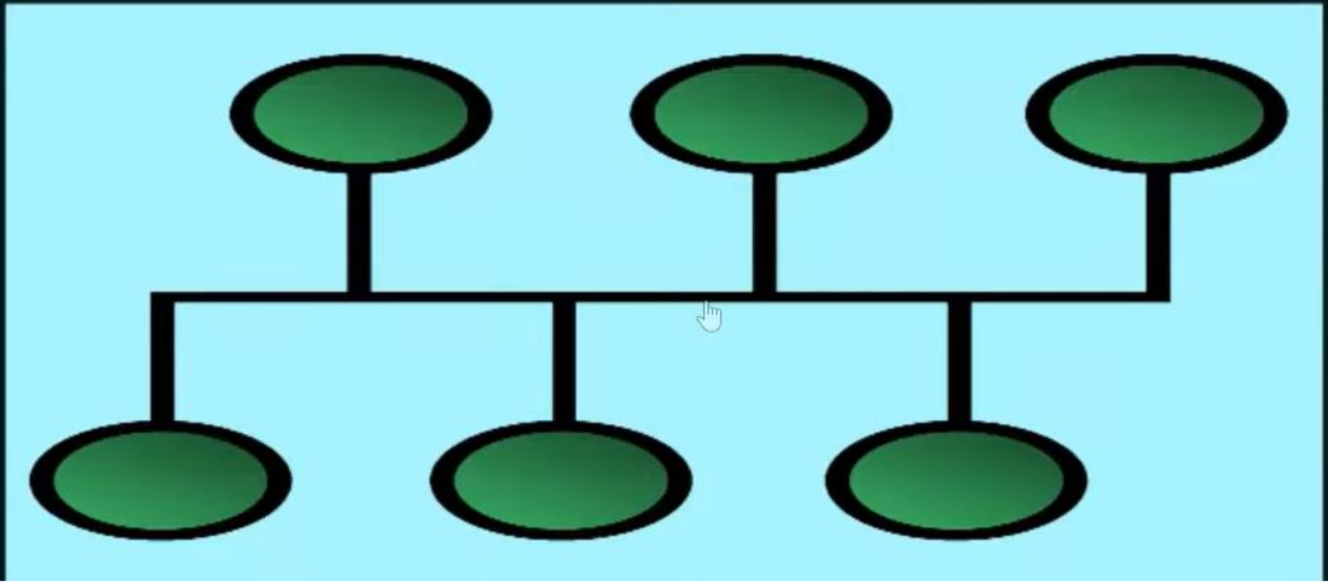
So maximum throughput of Slotted aloha = 36.8%

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 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."



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)

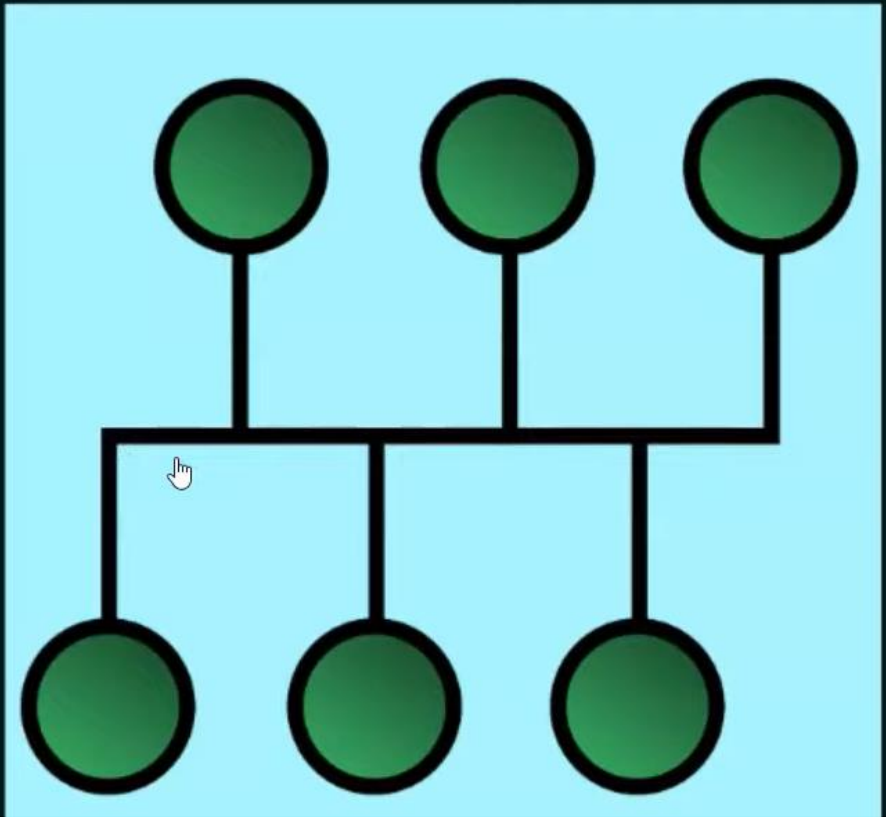
CSMA/CA (CSMA with Collision Avoidance)

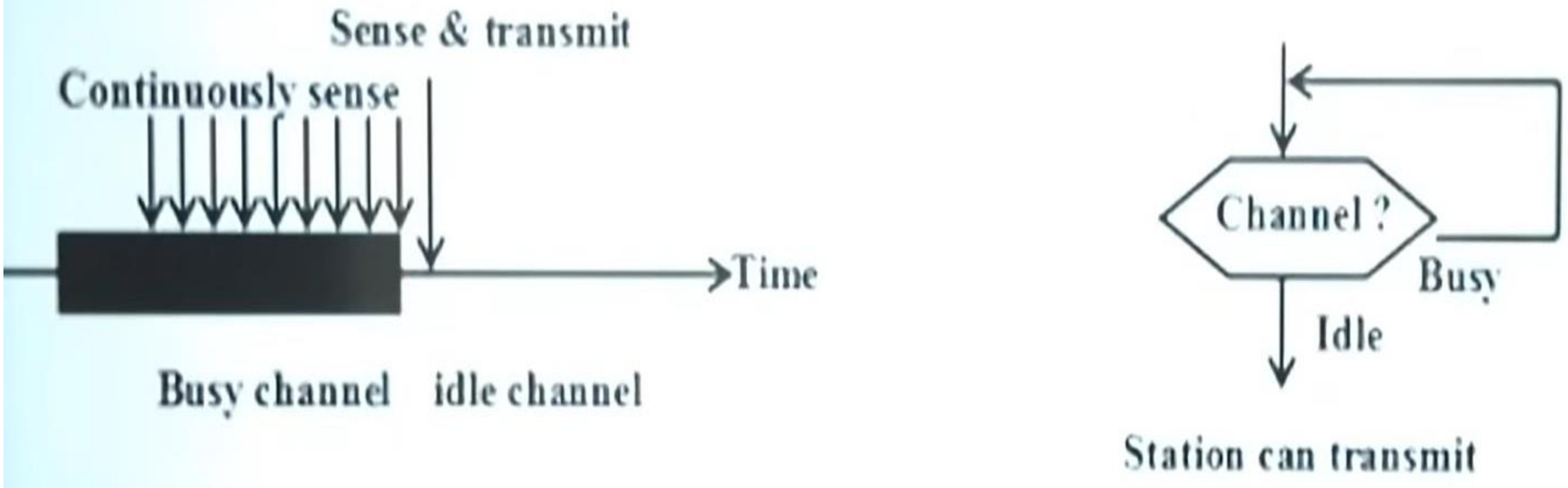
1-Persistent CSMA

- 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.
- The propagation delay has an important effect on the performance of the protocol.

1-Persistent CSMA

★ The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.

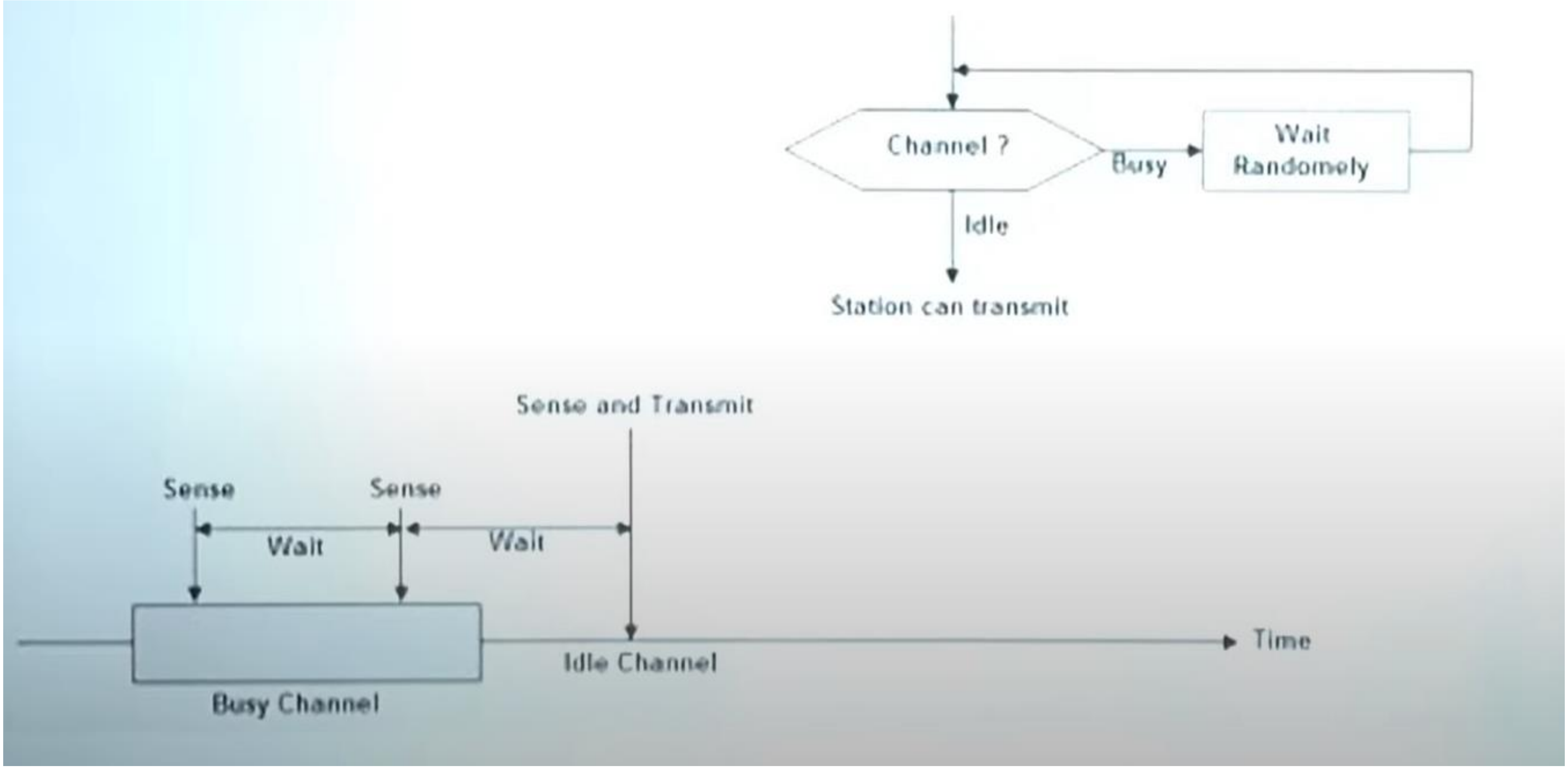




1-persistent CSMA

Non-Persistent CSMA

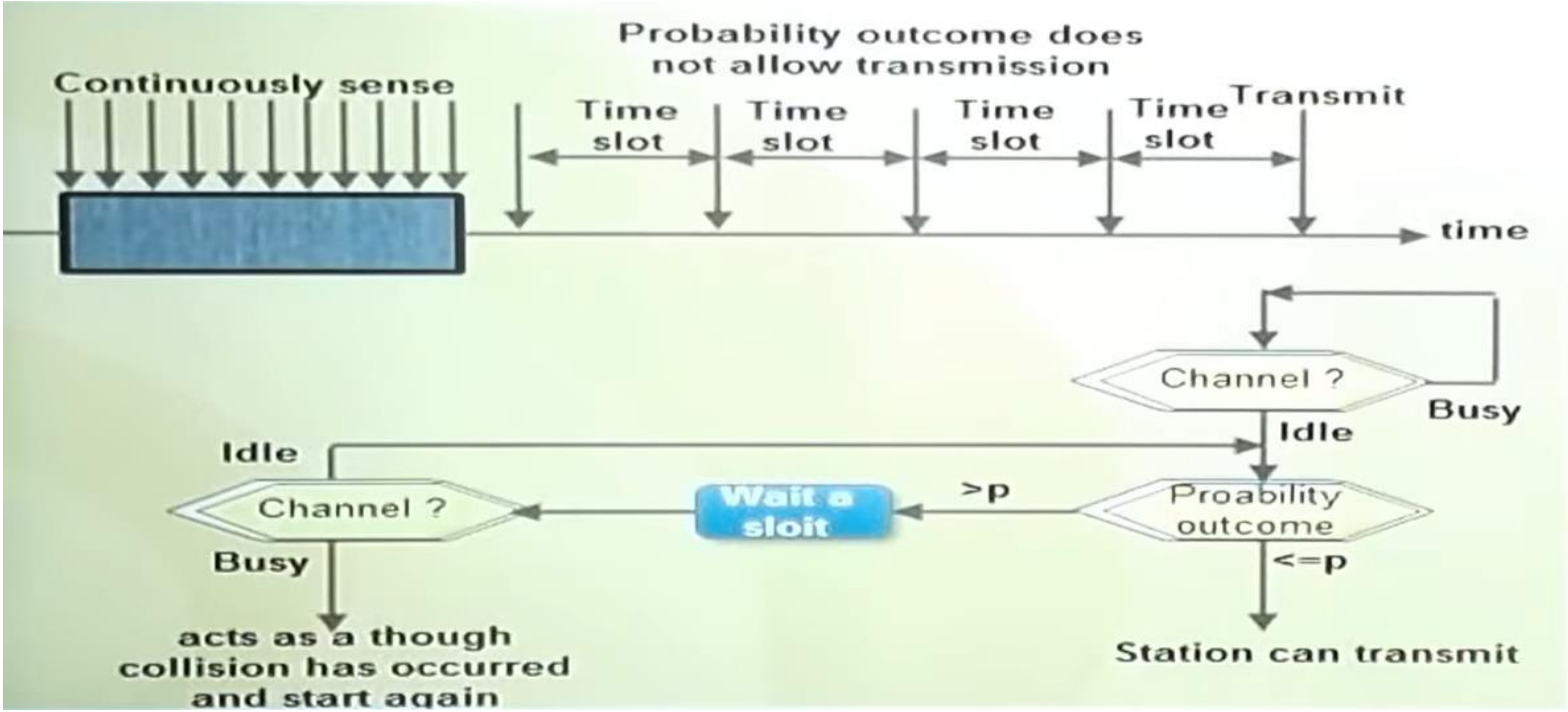
- ★ Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself.
- ★ However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- ★ 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.



NON PERSISTENT

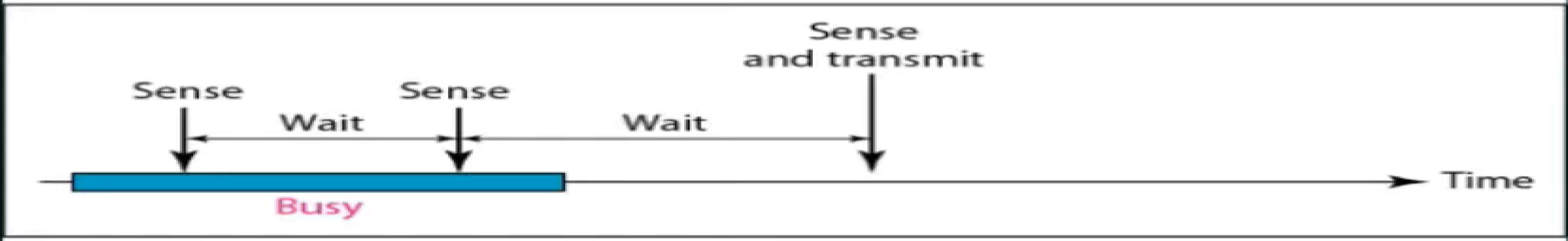
P-Persistent CSMA

- ★ 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 as 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.

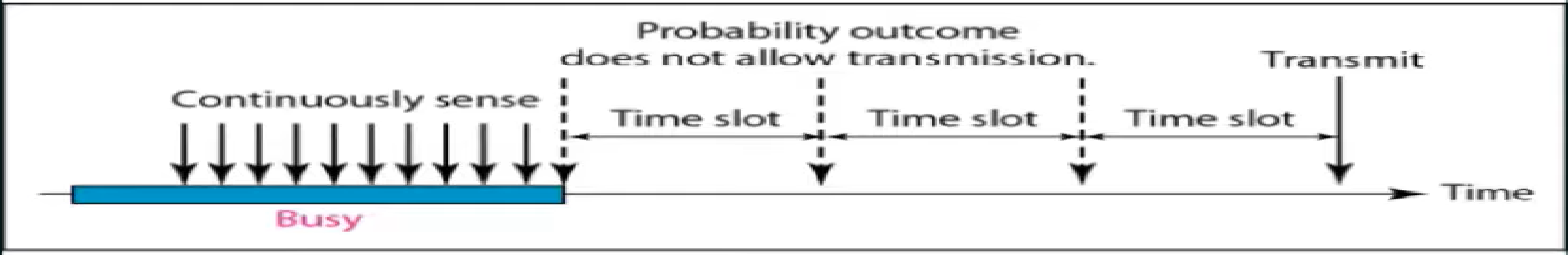


P-Persistent

a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/CD

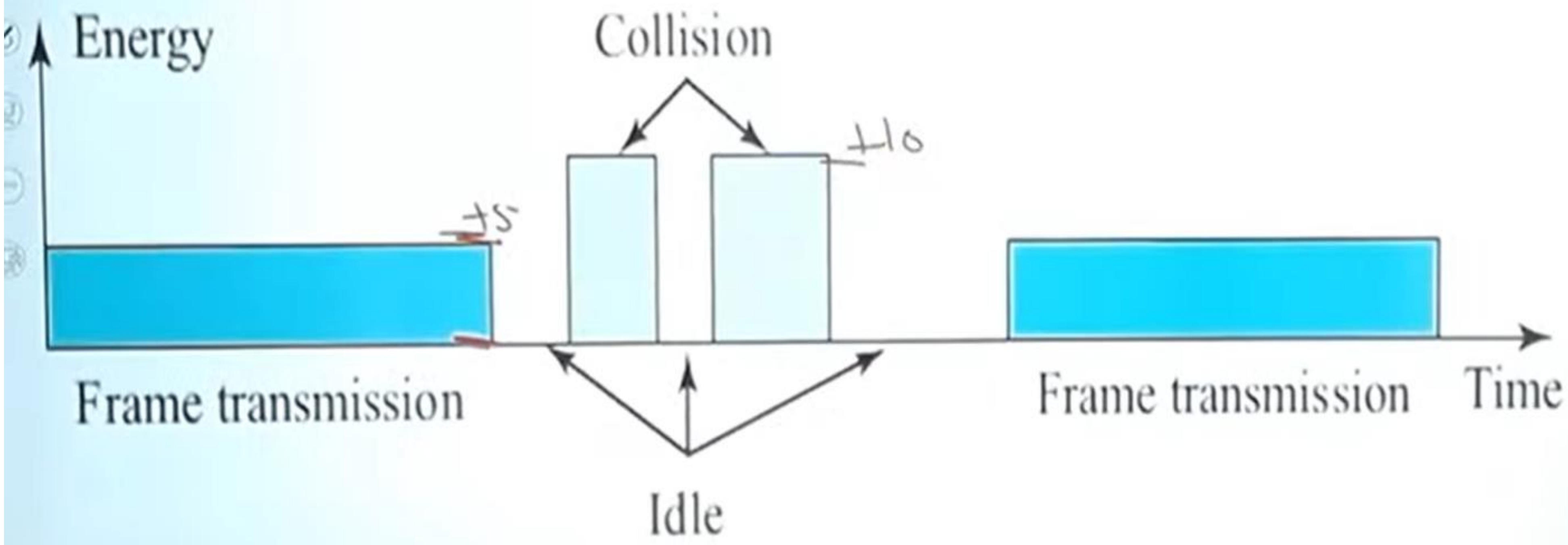
- ★ If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
- ★ Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collision is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

CSMA/CD

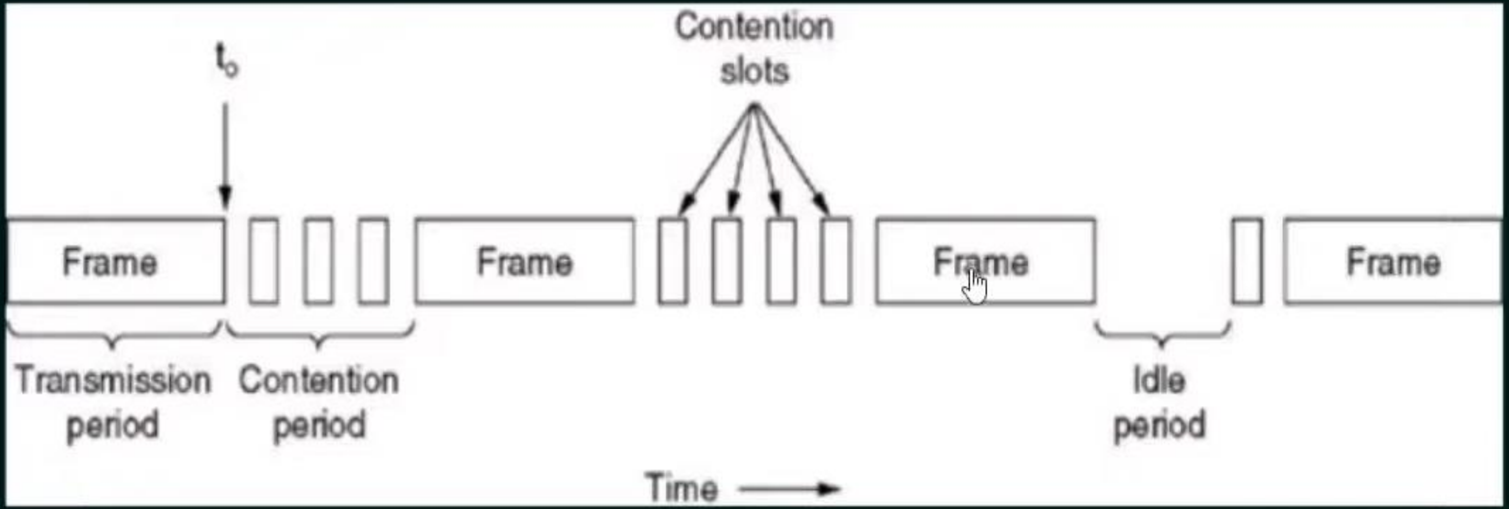
- ★ At the point marked t_0, a station has finished transmitting its frame.
- ★ Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision.
- ★ Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.
- ★ After a station detects 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 meantime.
- ★ Therefore, model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

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.

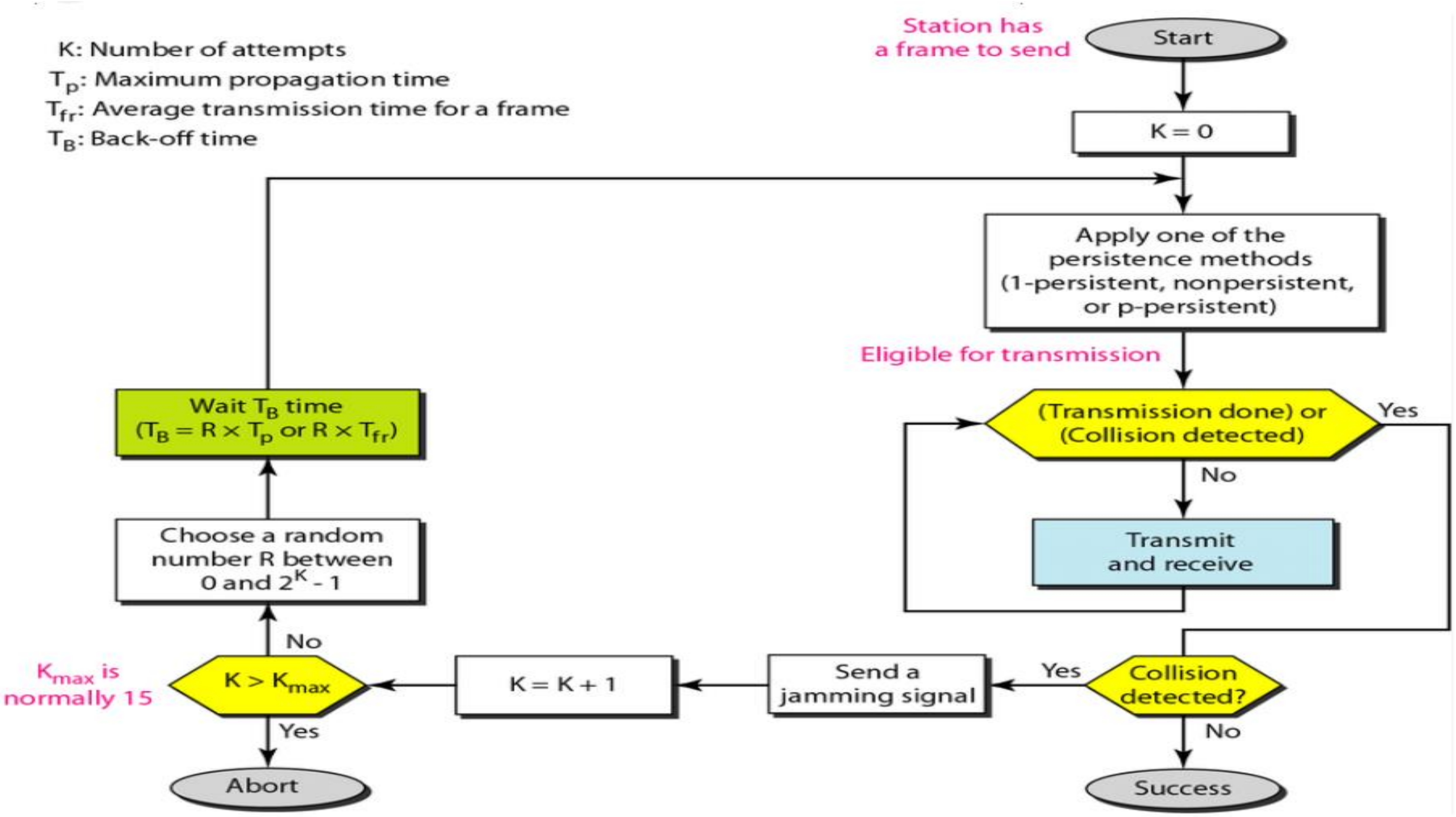


CSMA/CD



Contention slots
t_0
Frame
Frame
Frame
Frame
Transmission period
Contention period
Idle period
Time

Flow Diagram for CSMA/CD



1. Minimum size of frame to detect the collision in Ethernet (CSMA/CD

$$T_{d(frame)} \geq \underbrace{2 * P_d}_{RTT} + T_d(\text{Jam signal})$$

OR

$$T_d(F) \geq RTT + T_d($$

2. Backoff Algorithm

Waiting time = K * Slot duration

= K * RTT

= K * 2 * Pd

K is any random number in between 0 to $2^n - 1$

n is collision number (Collision number in respect to data packet).

Building a CSMA/CD network running at 1 Gbps over a I-km cable with no repeaters. The signal speed in the cable is200,000 km/sec. The minimum frame size is ____bits.

CSMA/CA

- ★ Carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but 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.
- ★ Solution: RTS/CTS exchange.
- ★ CSMA/CA is a protocol that operates in the Data Link Layer (Layer 2) of the OSI model.

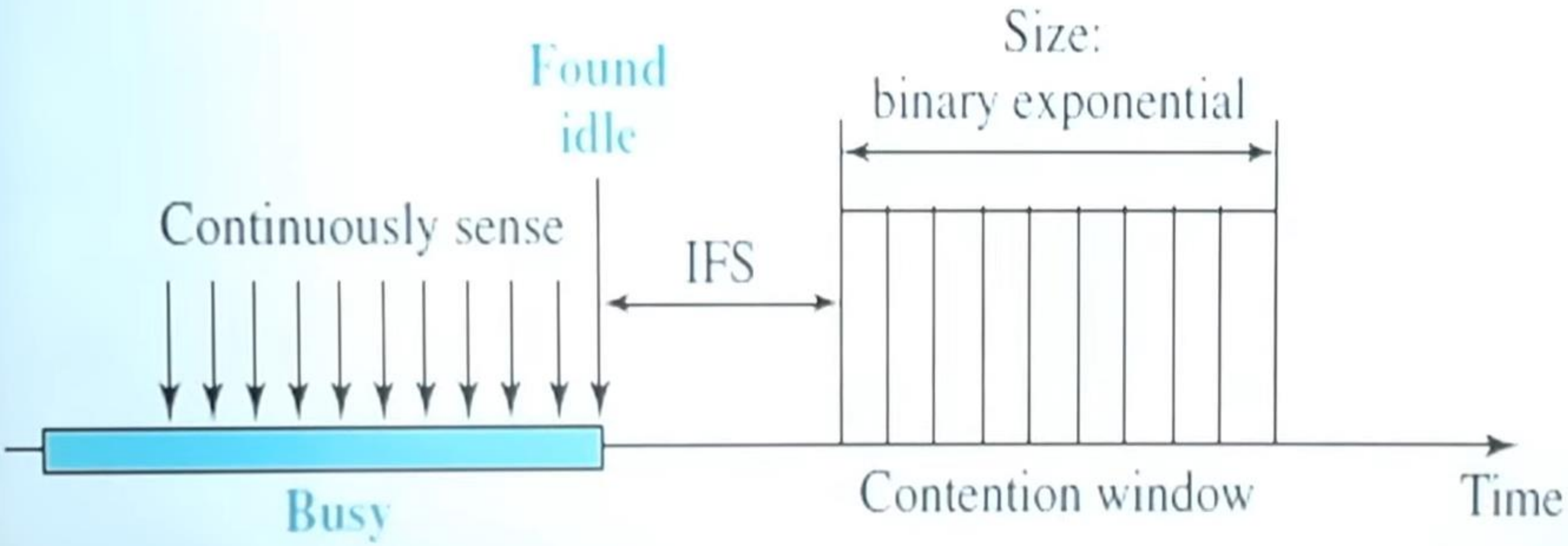
CSMA/CA

- ★ The Access method used by IEEE 802.11 Wi-Fi is CSMA/CA.

Interframe Space (IFS)

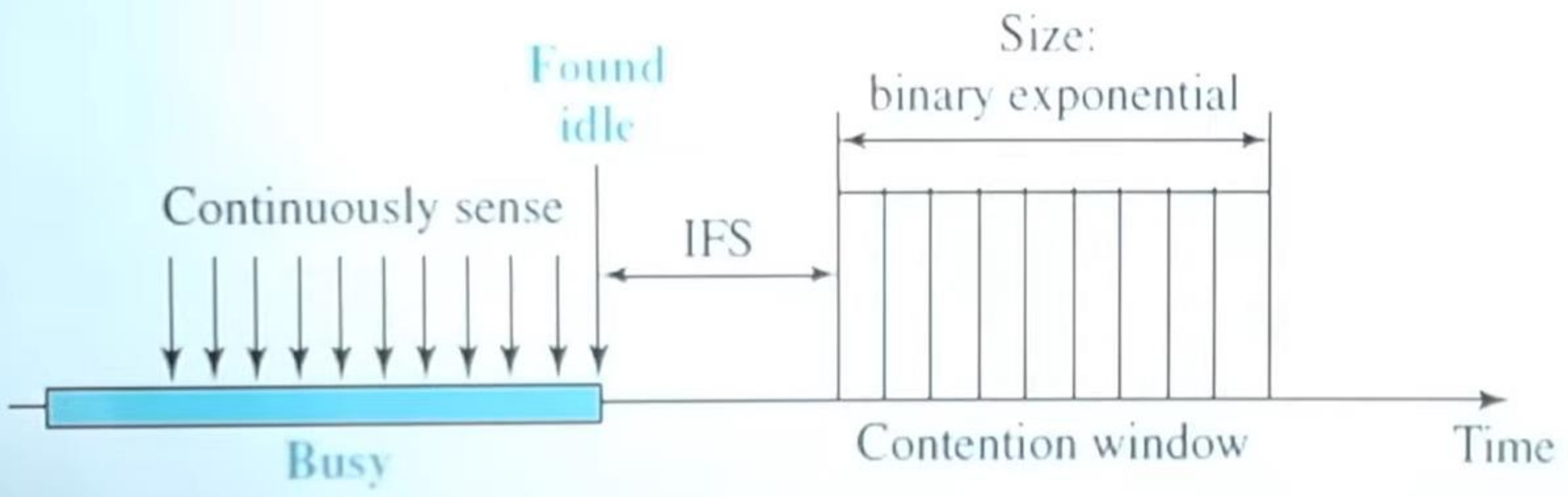
- First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.

- The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time. The IFS variable can also be used to prioritize stations or frame types.



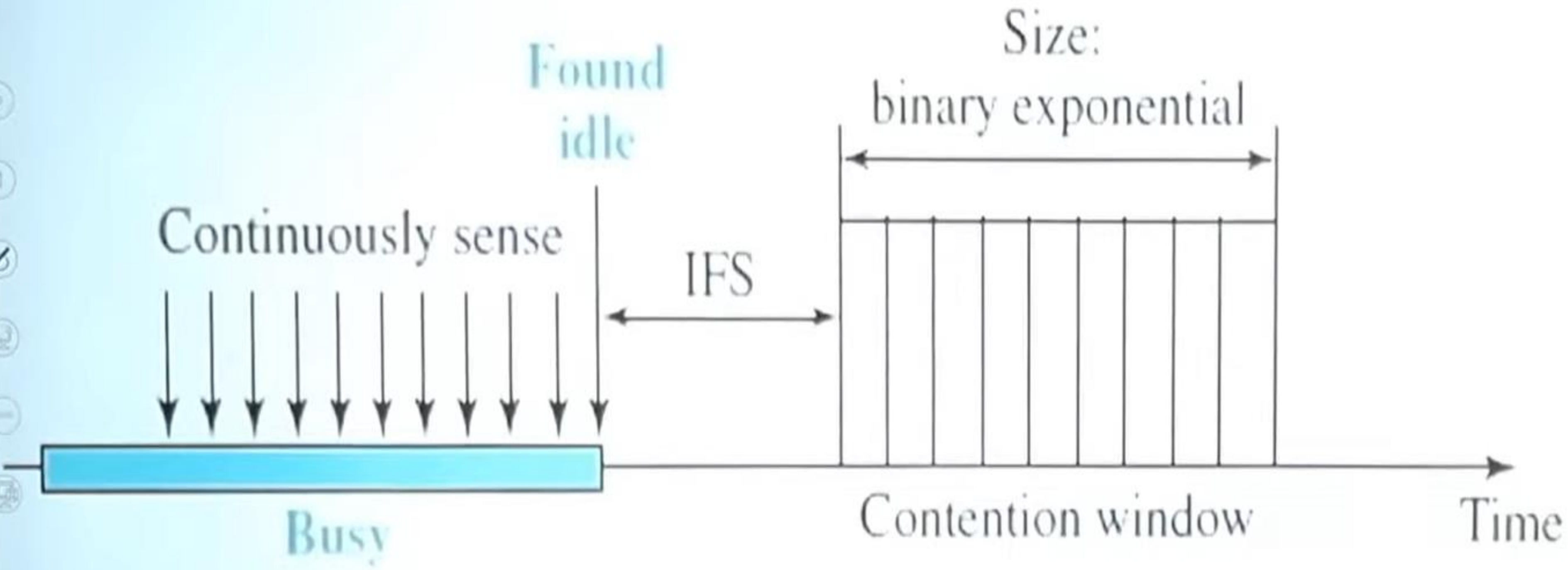
Contention Window

- The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.
- The number of slots in the window changes according to the binary exponential back-off strategy.
- This means that it is set to one slot the first time and then doubles each time.
- One interesting point about the contention window is that the station needs to sense the channel after each time slot.
- However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

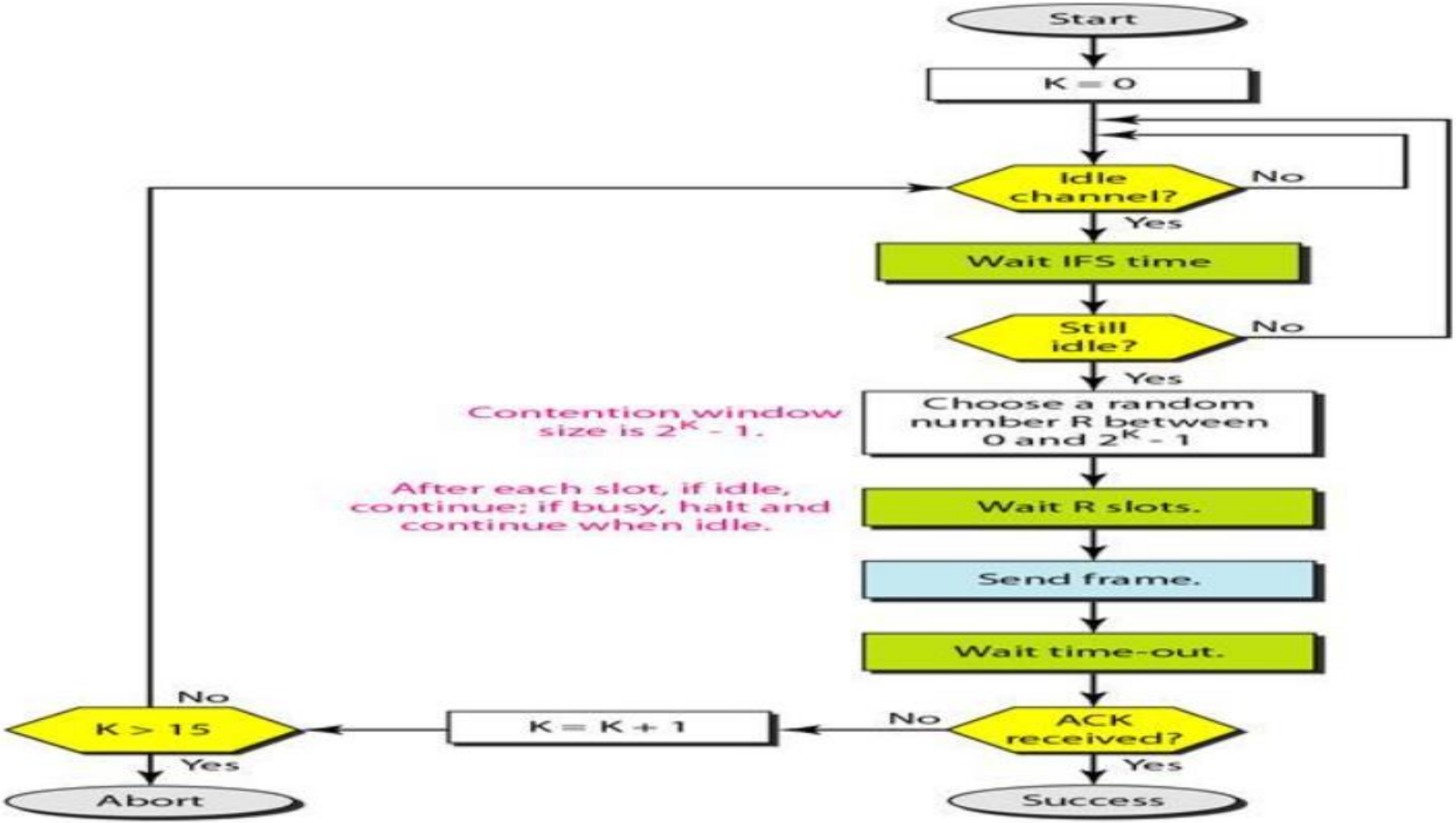


Acknowledgment

- With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.



FLOW DIAGRAM FOR CSMA/CA

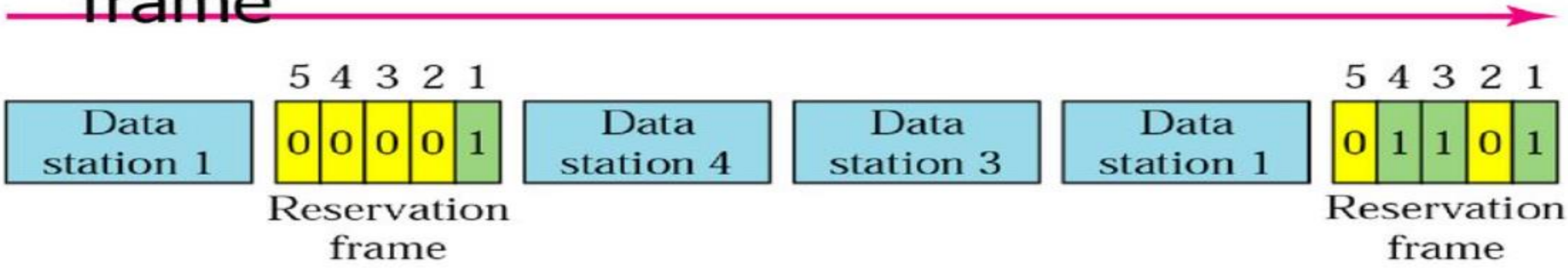


Controlled Access

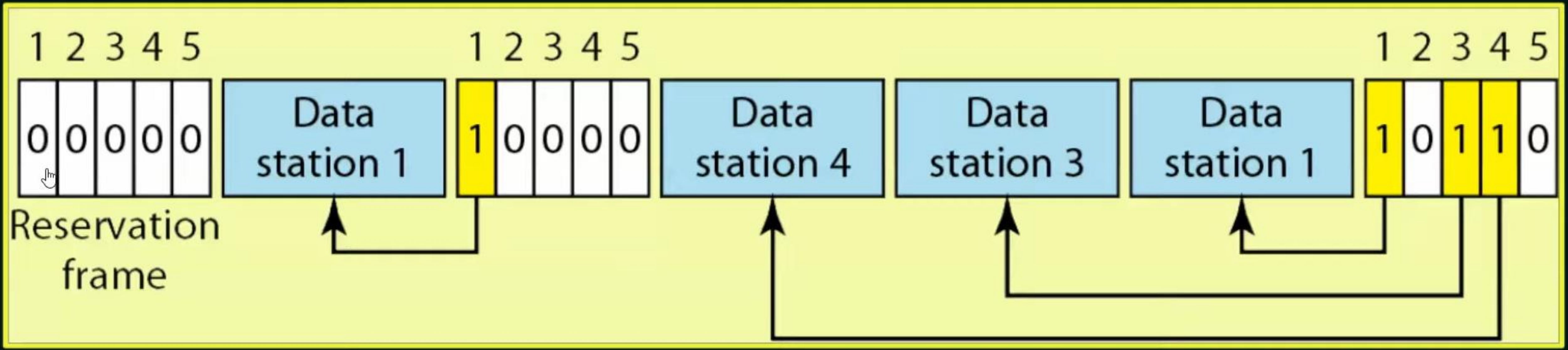
- The stations consult one another to find which station has the right to send
- A station cannot send unless it has been authorized by other stations
- 3 popular methods:
  - Reservation
  - Polling
  - Token Passing

Reservation

- A station needs to make a reservation before sending data
- Time is divided into intervals
- In each interval, a reservation frame precedes the data frames sent in that interval
- If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.
- The stations that have made reservation can send their data frames after the reservation frame



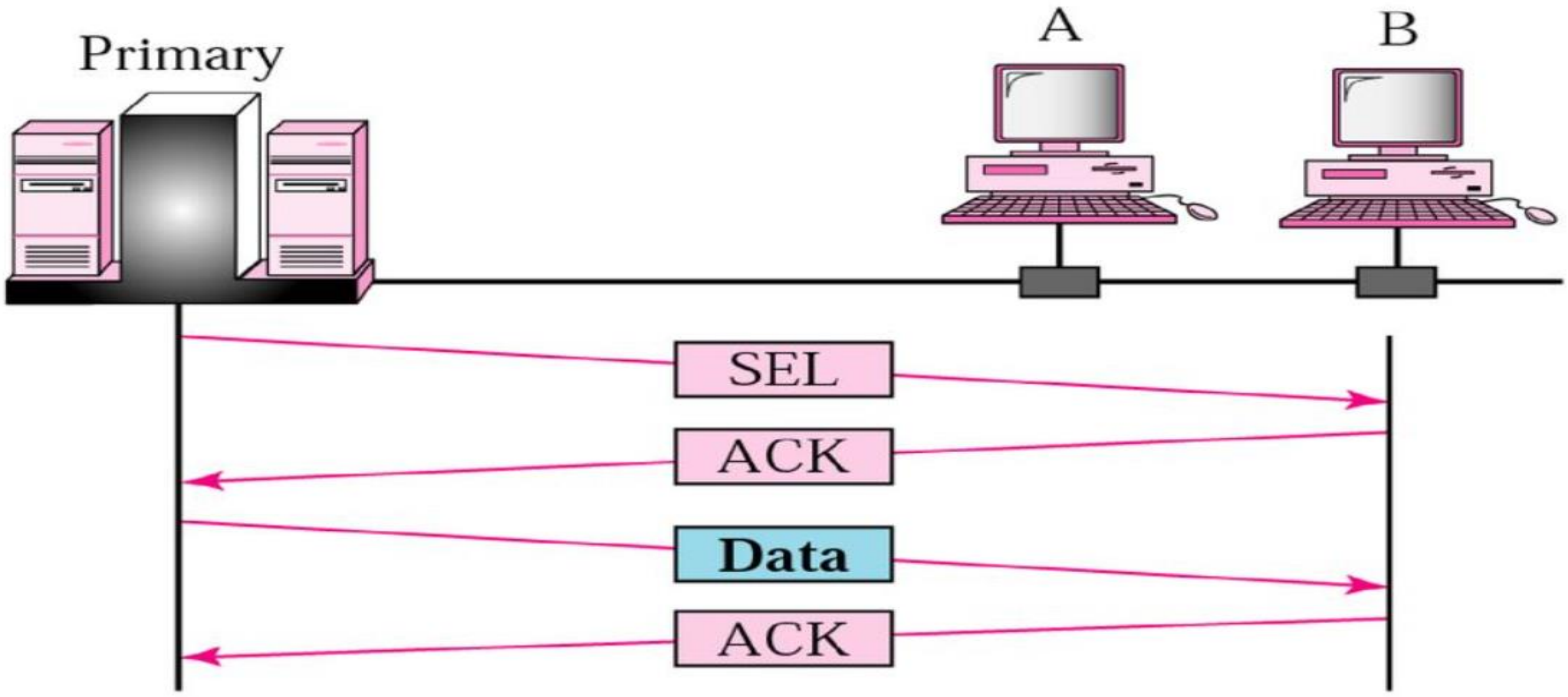
Reservation



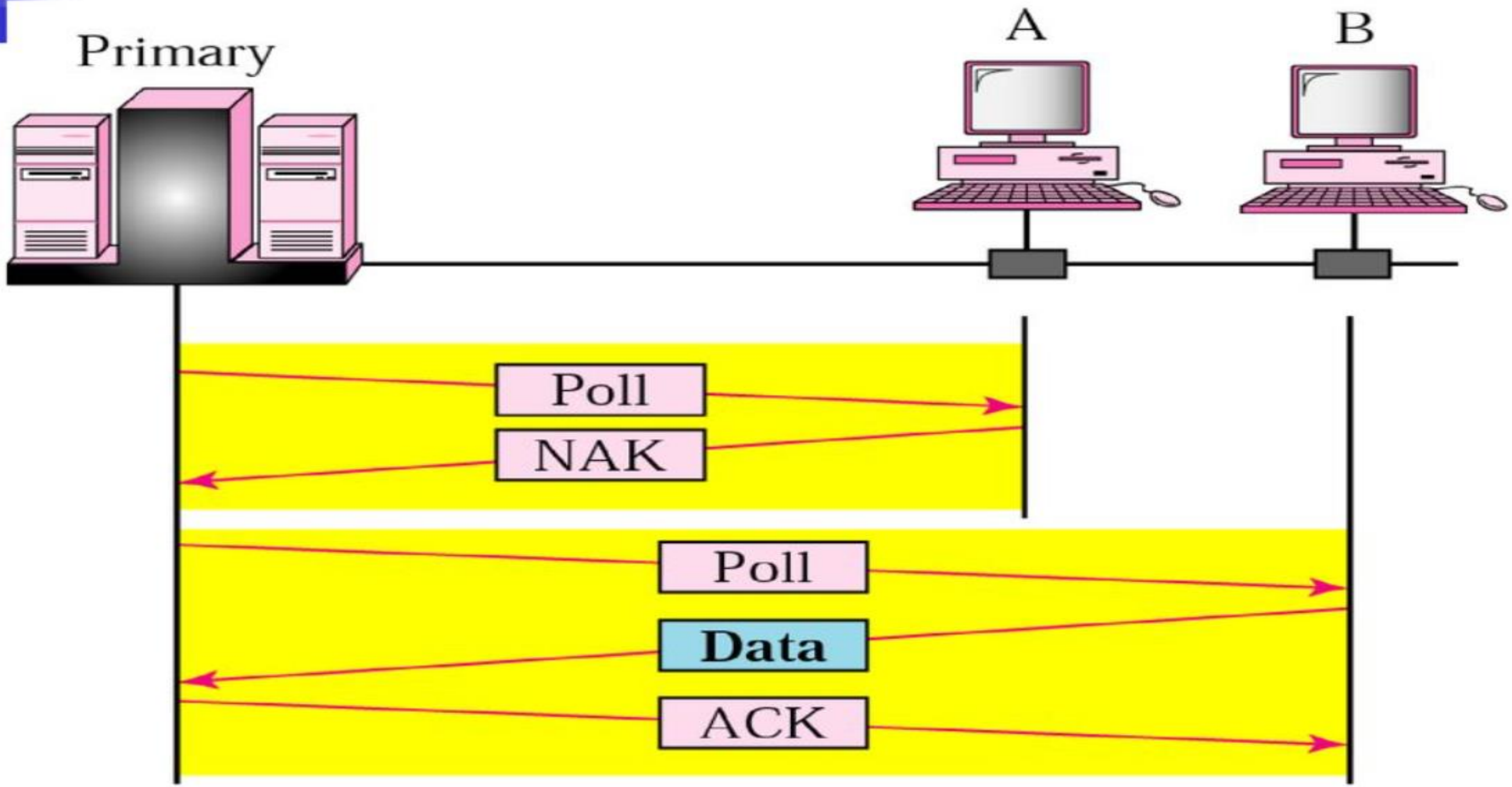
Polling

- Works with topologies in which one device is designated as a primary station and others as secondary stations.
- All data exchanges must be made through the primary station.
- Primary station controls the link.
- If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function
- If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function

Selecting process



Polling process



Efficiency of Polling

Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

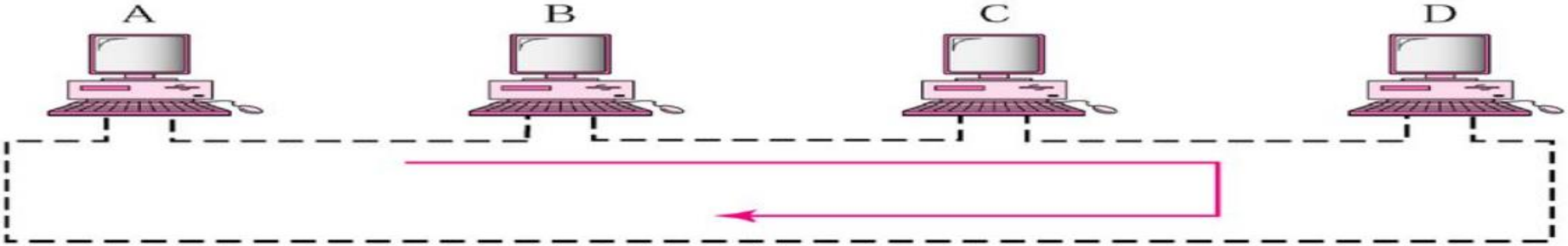
$$\text{Efficiency} = \frac{T_t}{T_t + T_{poll}}$$

Token Passing

- A Station is allowed to send data when it receives a special packet called token
- In this method, the stations in a network are organized in a logical ring
- For each station, there is a *predecessor* and a *successor*
- Packet received from *predecessor* and sent to *successor*

Token Passing

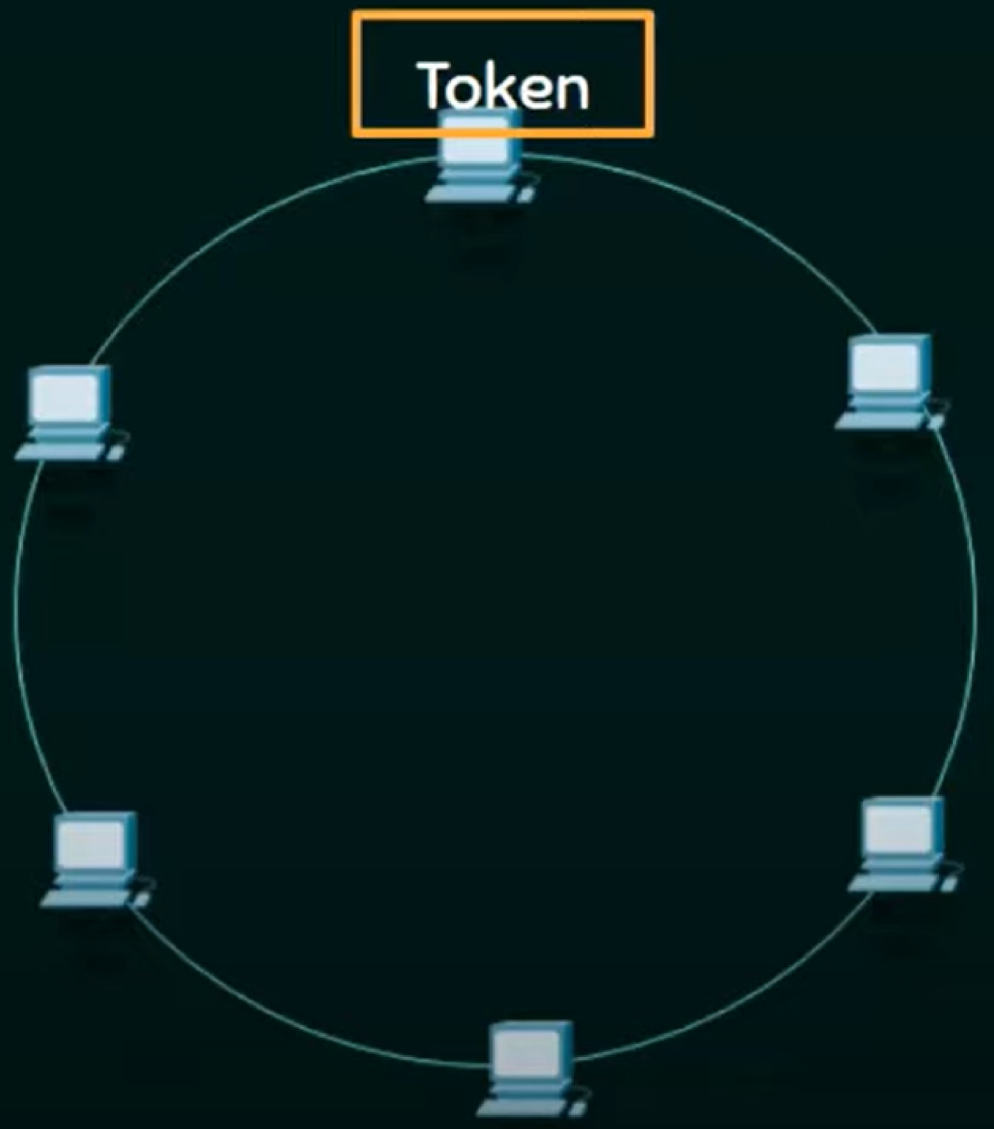
- When data is sent, token circulates through the ring
- When a station has some data to send, it waits until it receives the token from its predecessor. It then holds the token and sends its data.
- When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.
- The station cannot send data until it receives the token again in the next round.
- If a station receives the token and has no data to send, it just passes the data to the next station

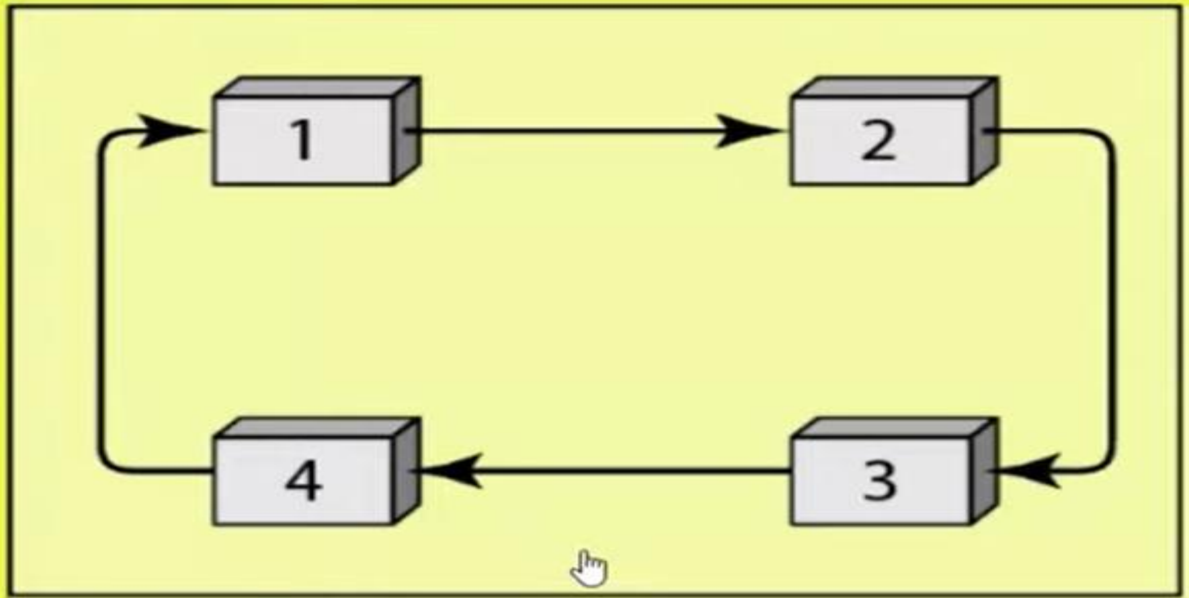


TOKEN PASSING

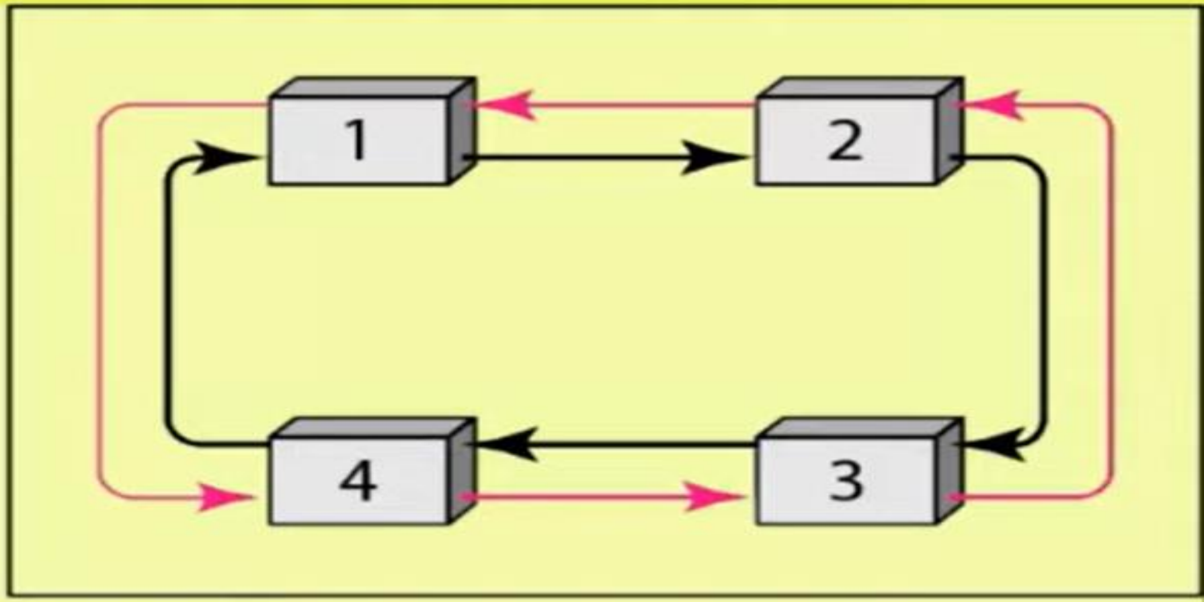
- ★ If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node.
- ★ Token passing is decentralized and highly efficient. But it has problems as well.
- ★ For example, the failure of one node can crash the entire 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.

Token Passing

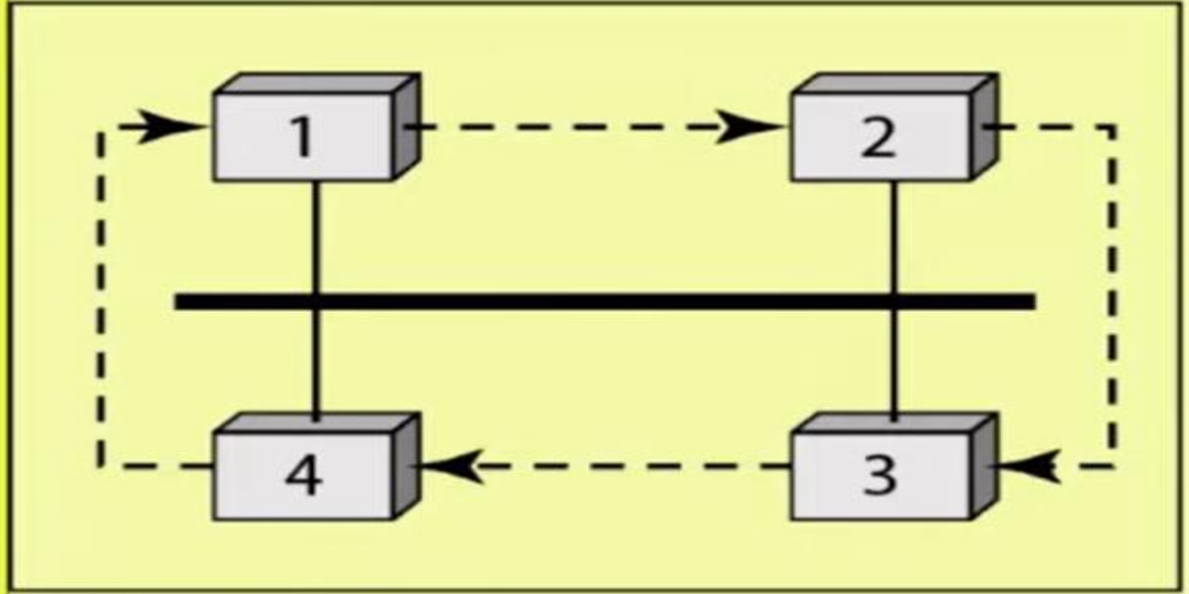




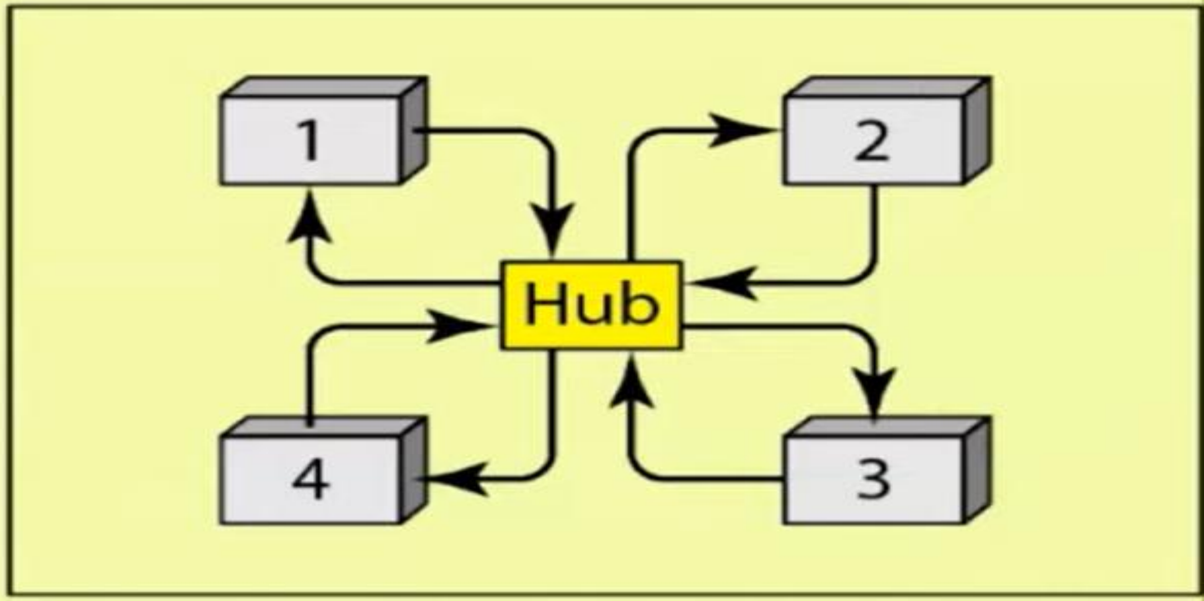
a. Physical ring



b. Dual ring

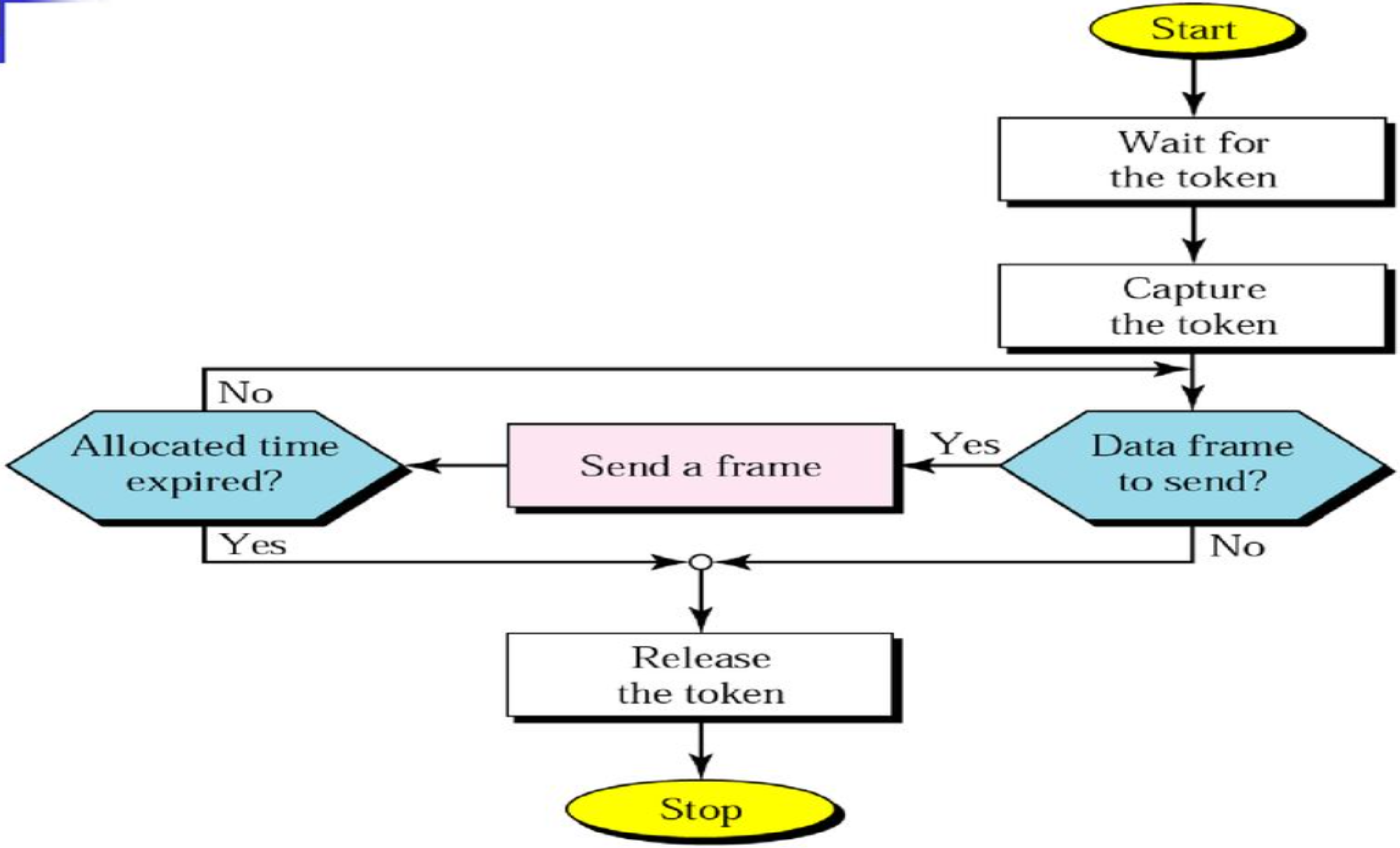


c. Bus ring



d. Star ring

Token Passing procedures



Performance of Token passing

$$S = \frac{1}{1 + a/N} \quad ; \text{for } a < 1$$

$$S = \frac{1}{a(1 + 1/N)} \quad ; \text{for } a > 1$$

$$a = \frac{T_p}{T_t}$$

S = Throughput

N = number of stations

T_p = Propagation delay

T_t = Transmission delay

Channelization

- Multiple access method in which the available bandwidth of a link is shared in time, frequency or code between different stations.
- 3 popular channelization protocol:
  - FDMA – the available bandwidth is divided into frequency bands
  - TDMA – the stations share the bandwidth of the channel in time
  - CDMA – differs from FDMA because only one channel occupies the entire bandwidth of the link; differs from TDMA because all stations can send data simultaneously, no time sharing

CDMA

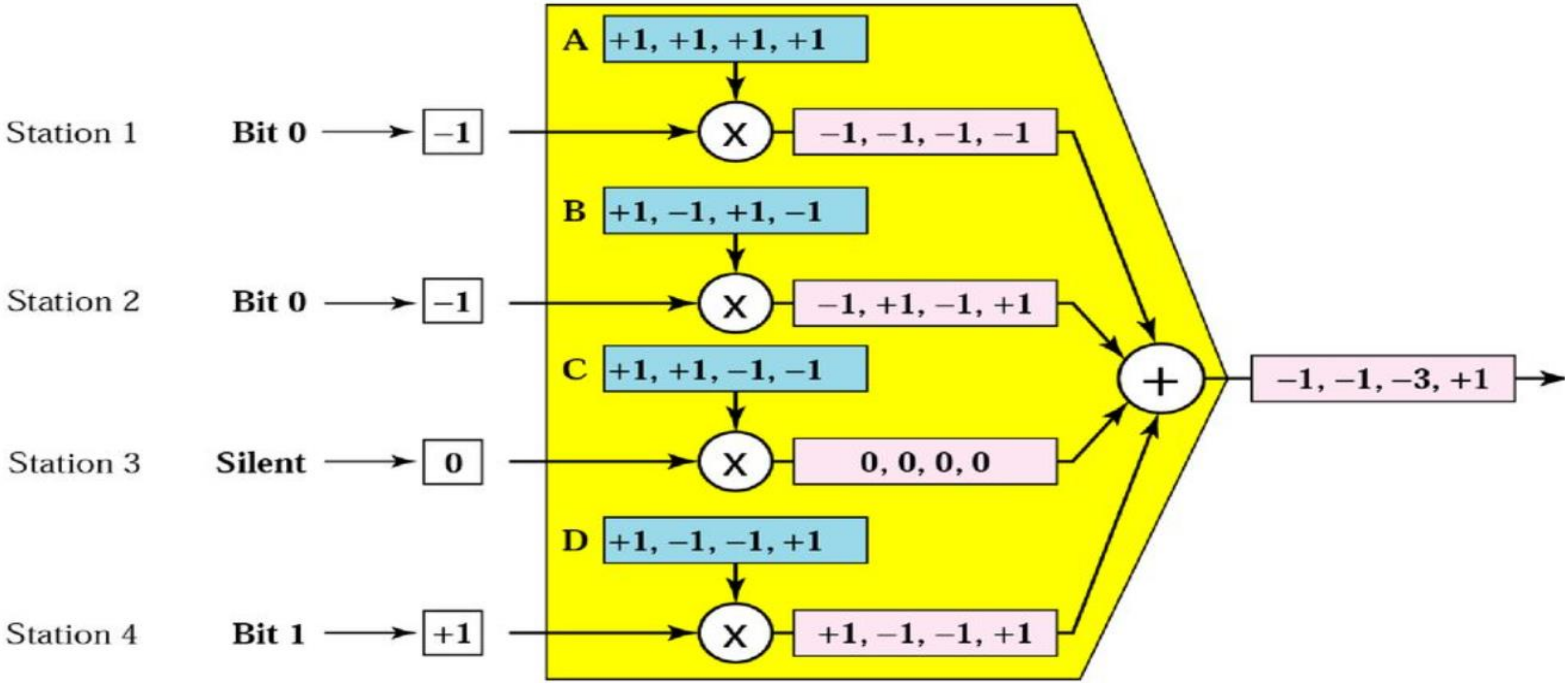
- Still new in implementation
- A channel carry all data transmission simultaneously
- Based on coding theory . Each station is assigned a code, which is a sequence of numbers called chips

+1, +1, +1, +1	+1, −1, +1, −1	+1, +1, −1, −1	+1, −1, −1, +1
A	B	C	D

Data representation

Data bit 0 → −1 Data bit 1 → +1 Silence → 0

CDMA multiplexing



CDMA demultiplexing