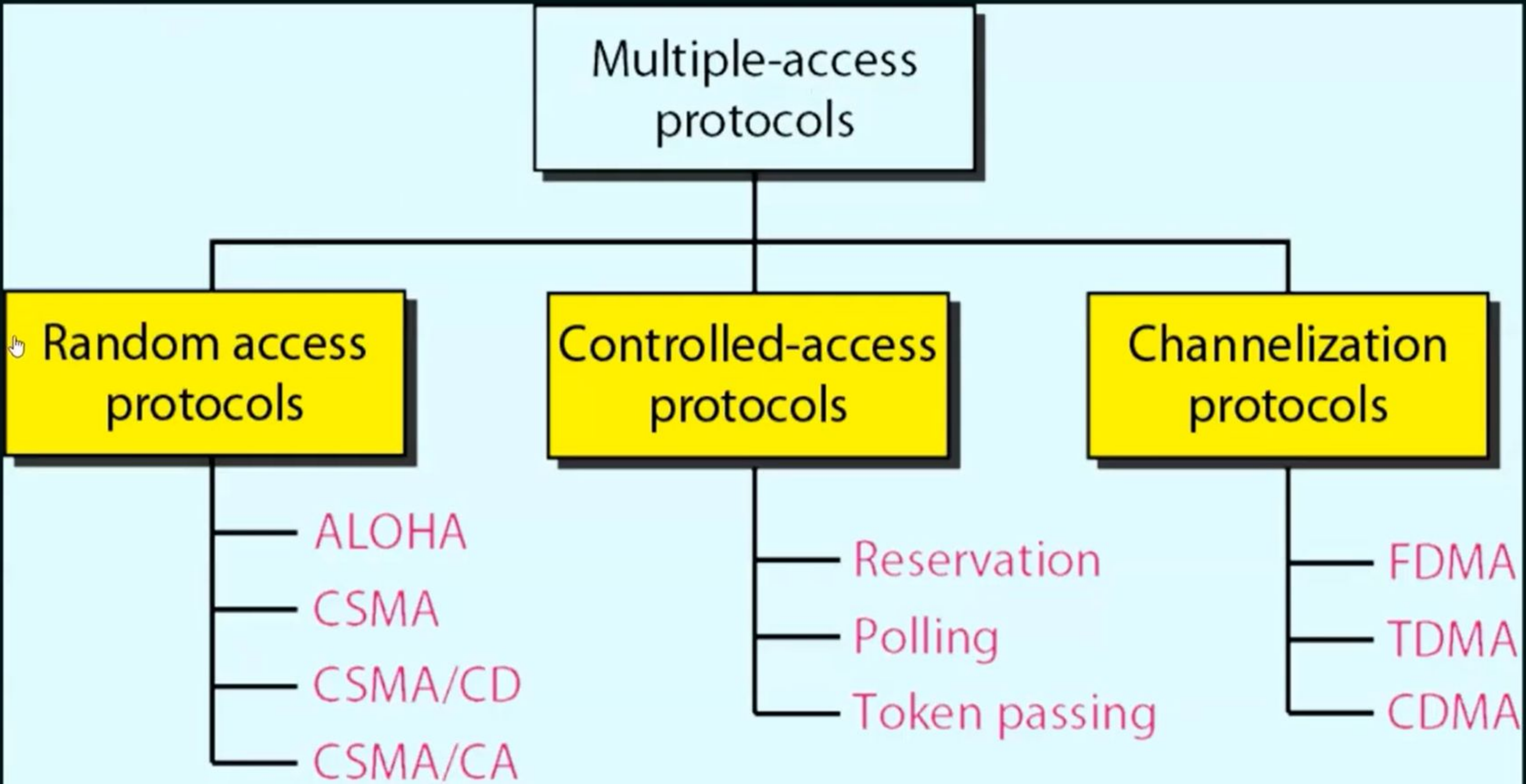
Multiple Access protocols

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

- ★ 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 ?

Controlled Access Protocols

- ★ In 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.

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.

Frequency Division Multiple Access (FDMA)

Time Division Multiple Access (TDMA)

Code Division Multiple Access (CDMA)

ALOHA

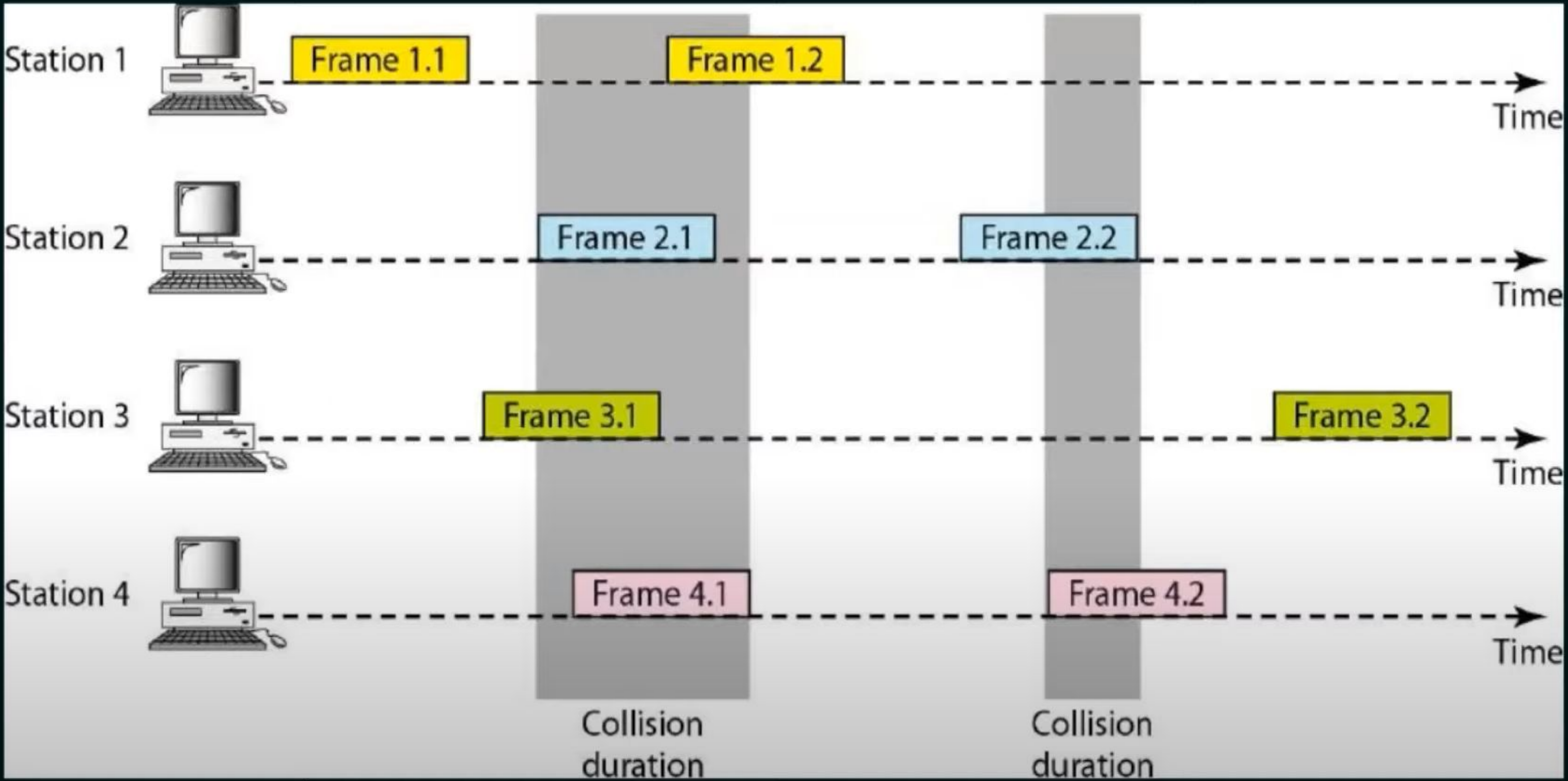
- ★ Aloha is a random access protocol.
- ★ It was actually designed for WLAN but it is also applicable for shared medium.
- ★ In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

Types:

- ★ Pure Aloha
- ★ Slotted Aloha

COLLISION

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.

PURE ALOHA

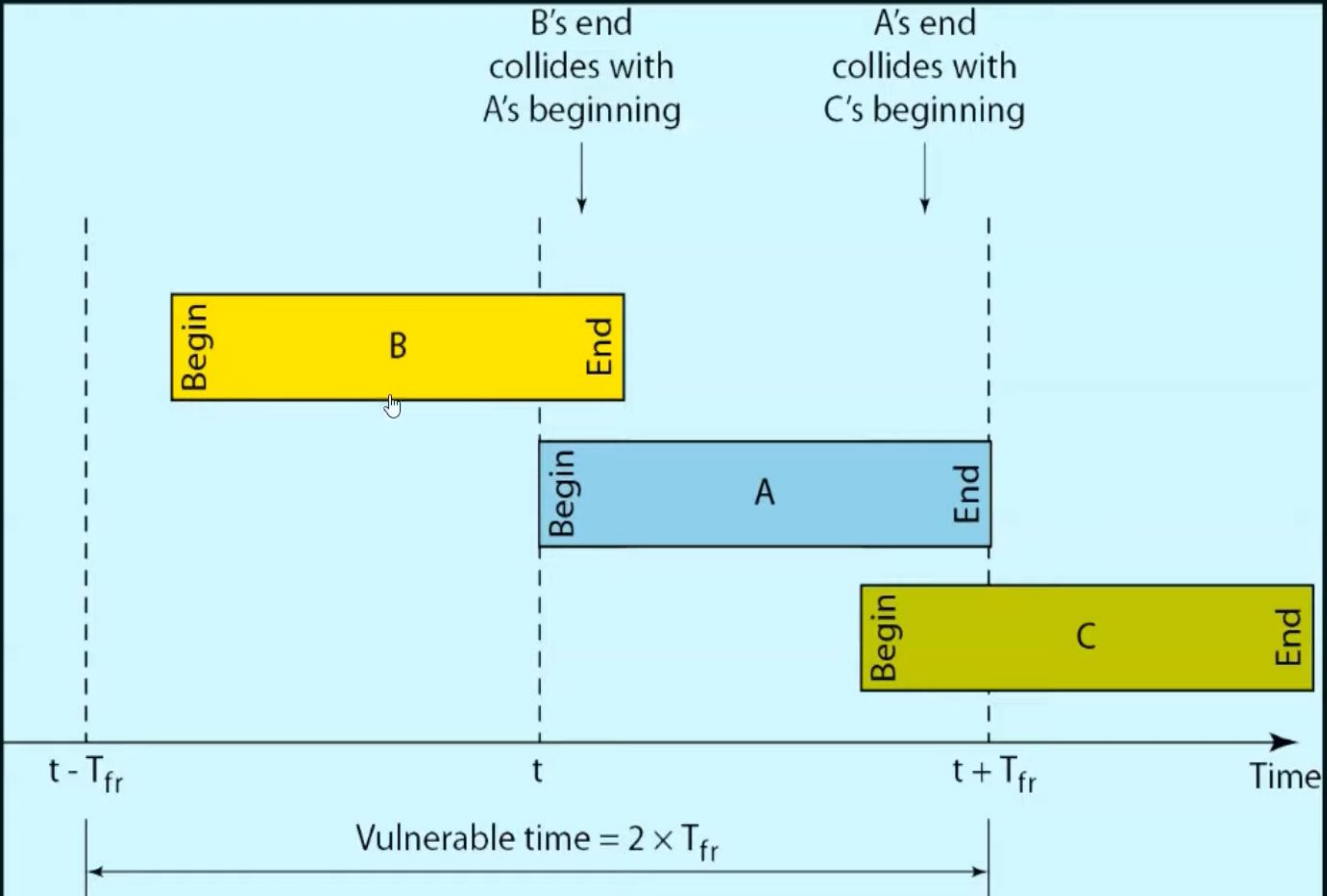
- ★ Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
- ★ If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

Vulnerable Time = $2 * T_{fr}$

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

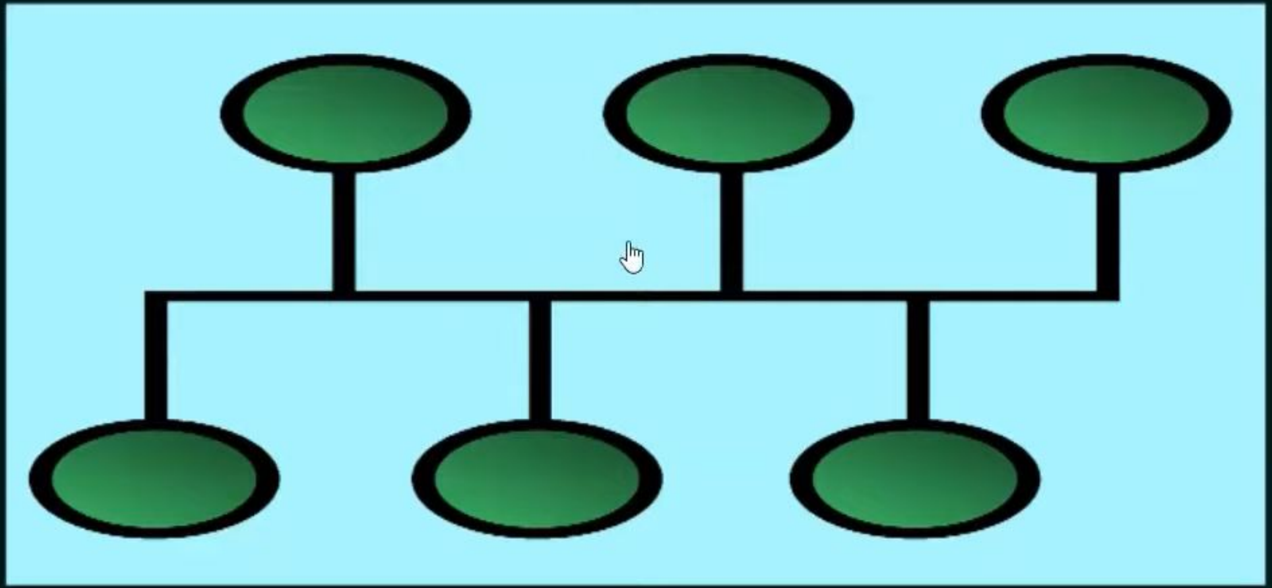
Maximum throughput = 0.184 for G=0.5 (½)

Pure aloha


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 × T_{fr}

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.

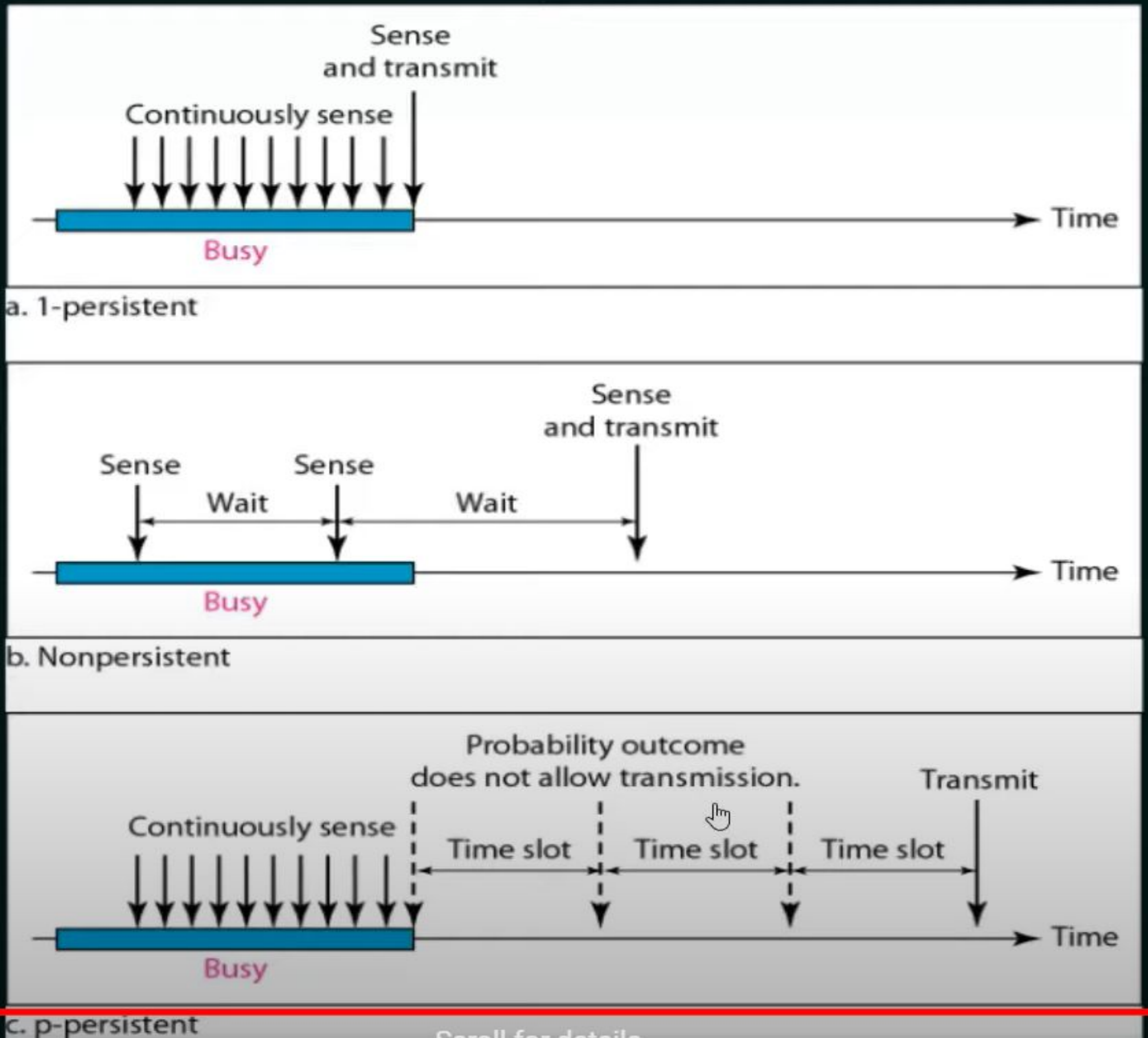
Non-Persistent CSMA

- ★ 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 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.

BEHAVIOUR OF THREE PERSISTENT METHODS

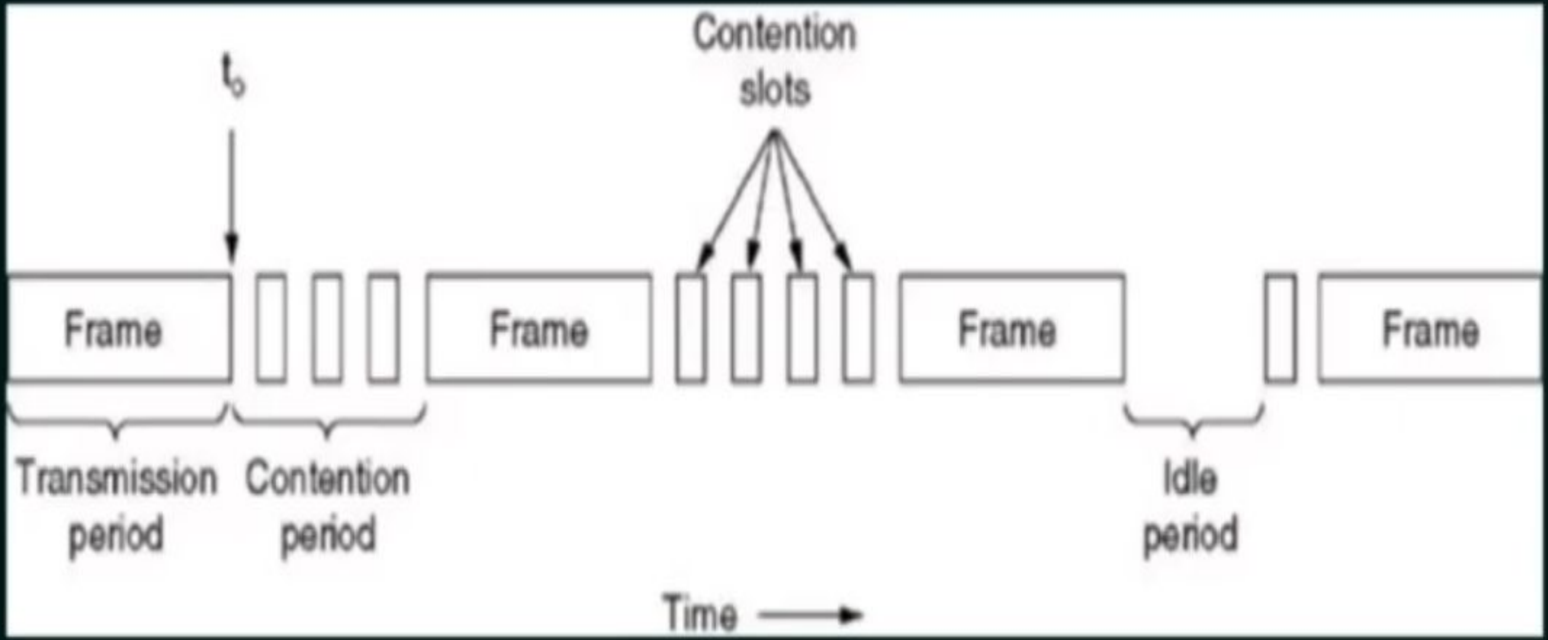


CSMA/CD

- ★ 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.



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.

CSMA/CD – For GATE aspirants

$$\text{Efficiency} = \frac{1}{1 + 6.44 \times a}$$

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

★ If distance increases, efficiency of CSMA decreases.

★ CSMA is not suitable for long distance networks like WAN; but works optimally for LAN.

★ If length of packet is bigger, the efficiency of CSMA also increases; but maximum limit for length is 1500 Bytes.

★ Transmission Time >= Round Trip Time of 1 bit

★ Transmission Time >= 2*Propagation Time

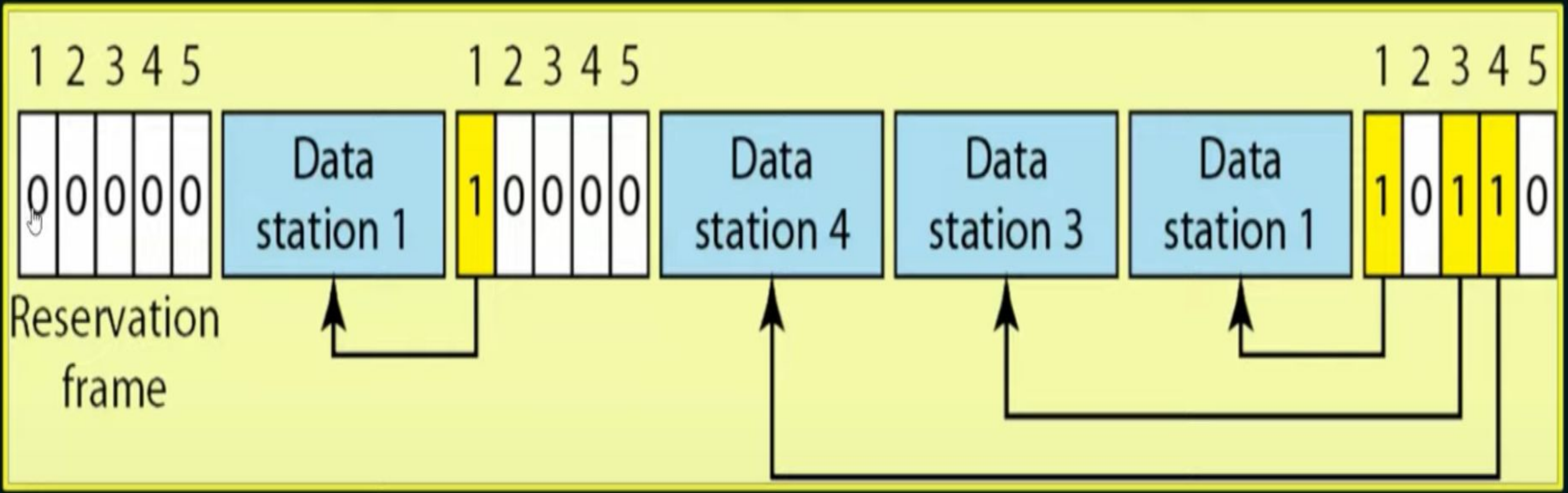
CSMA/CA

- ★ 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.

Reservation

- A station need to make a reservation before sending data.
- 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.
- Each minislot belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own minislot.
- The stations that have made reservations can send their data frames after the reservation frame.

Reservation



POLLING

- The polling protocol requires one of the nodes to be designated as a Master node (Primary station).
- The master node polls each of the nodes in a round-robin fashion.
- In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames.
- After node 1 transmits some frames, the master node tells node 2 it (node 2) can transmit up to the maximum number of frames.
- The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.

POLLING

- ★ The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.
- ★ The polling protocol eliminates the collision.
- ★ This allows polling to achieve a much higher efficiency.
- ★ The first drawback is that the protocol introduces a polling delay—the amount of time required to notify a node that it can transmit.
- ★ The second drawback, which is potentially more serious, is that if the master node fails, the entire channel becomes inoperative.

Polling – Functions

- ★ **Poll function** : If the primary wants to receive data, it asks the secondaries if they have anything to send.
- ★ **Select function** : If the primary wants to send data, it tells the secondary to get ready to receive.

Controlled Access Protocol – Polling

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 authorized to send data when it receives a special frame called a token.
- Here there is no master node.
- A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.
- When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node.

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.

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