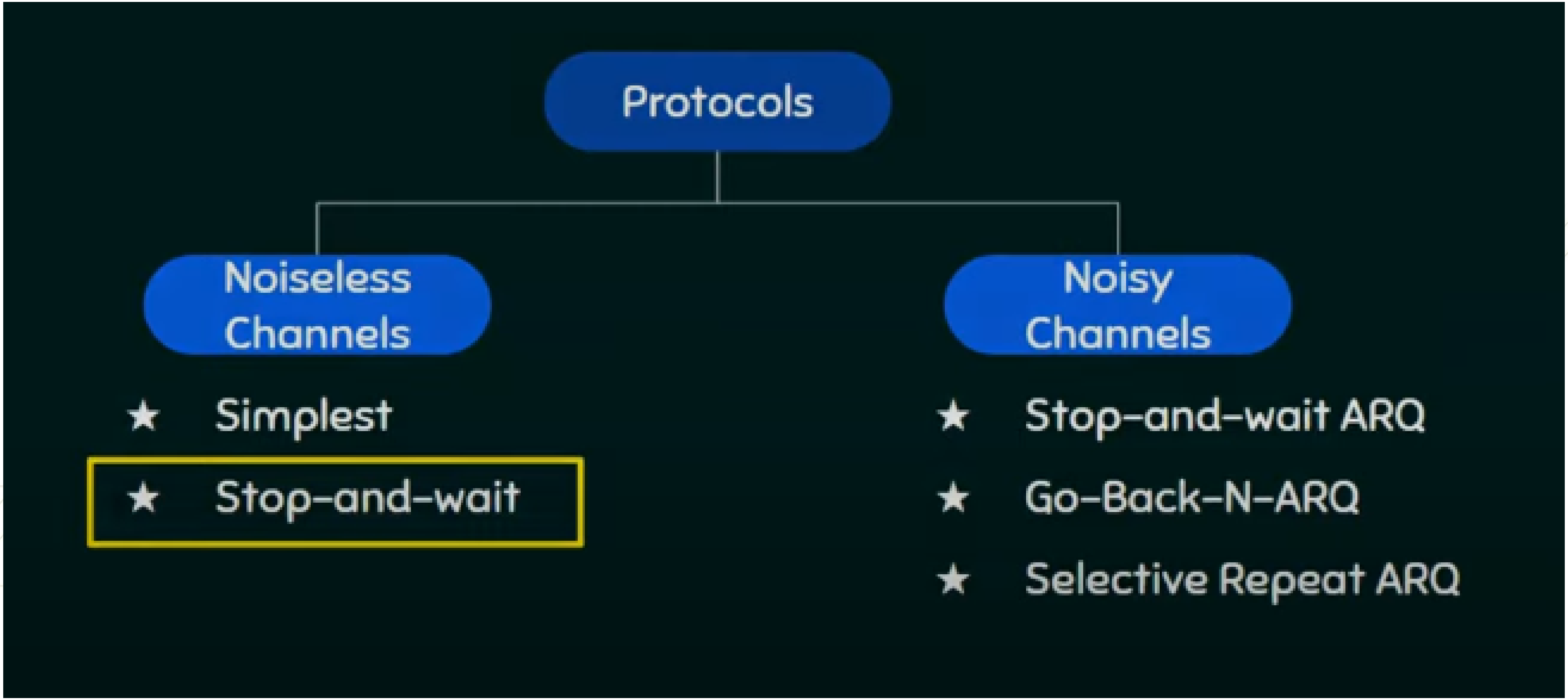
Flow Control Protocols



Protocols

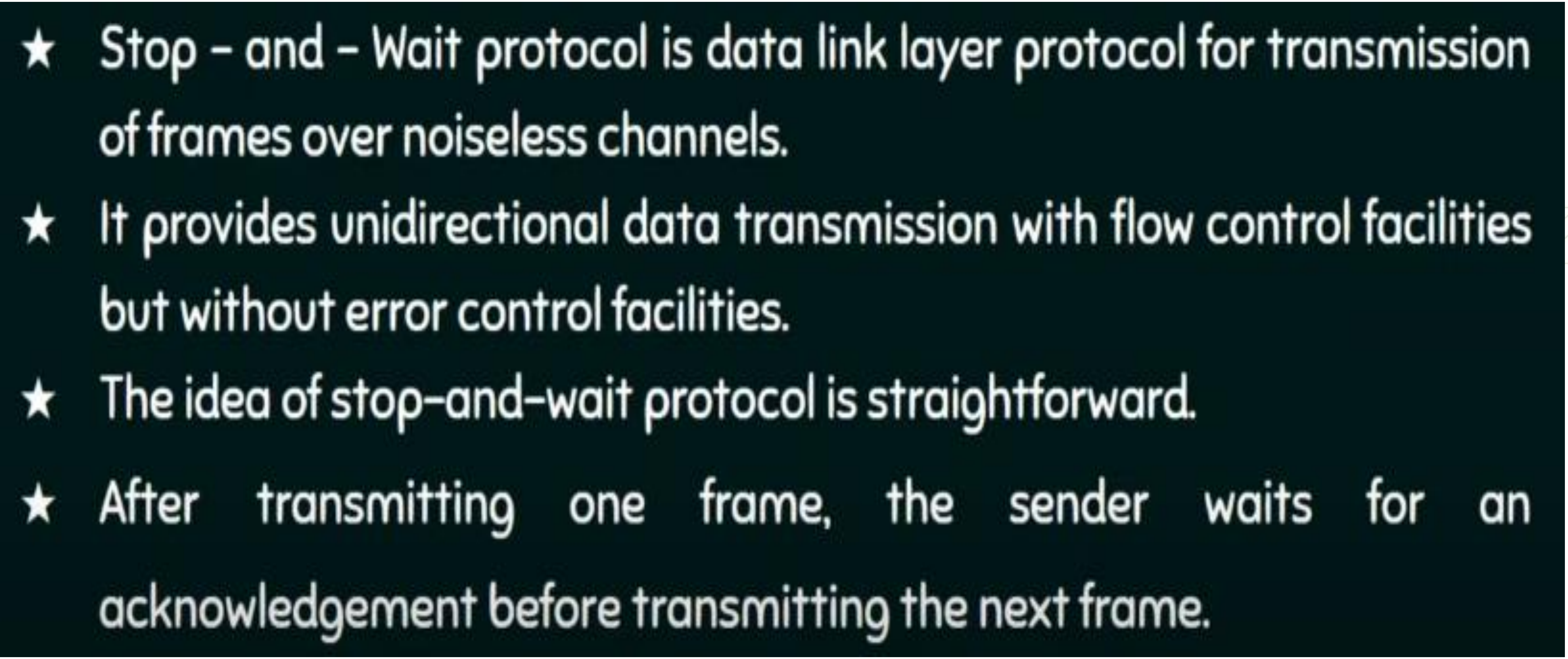
Noiseless Channels

- ★ Simplest
- ★ Stop-and-wait

Noisy Channels

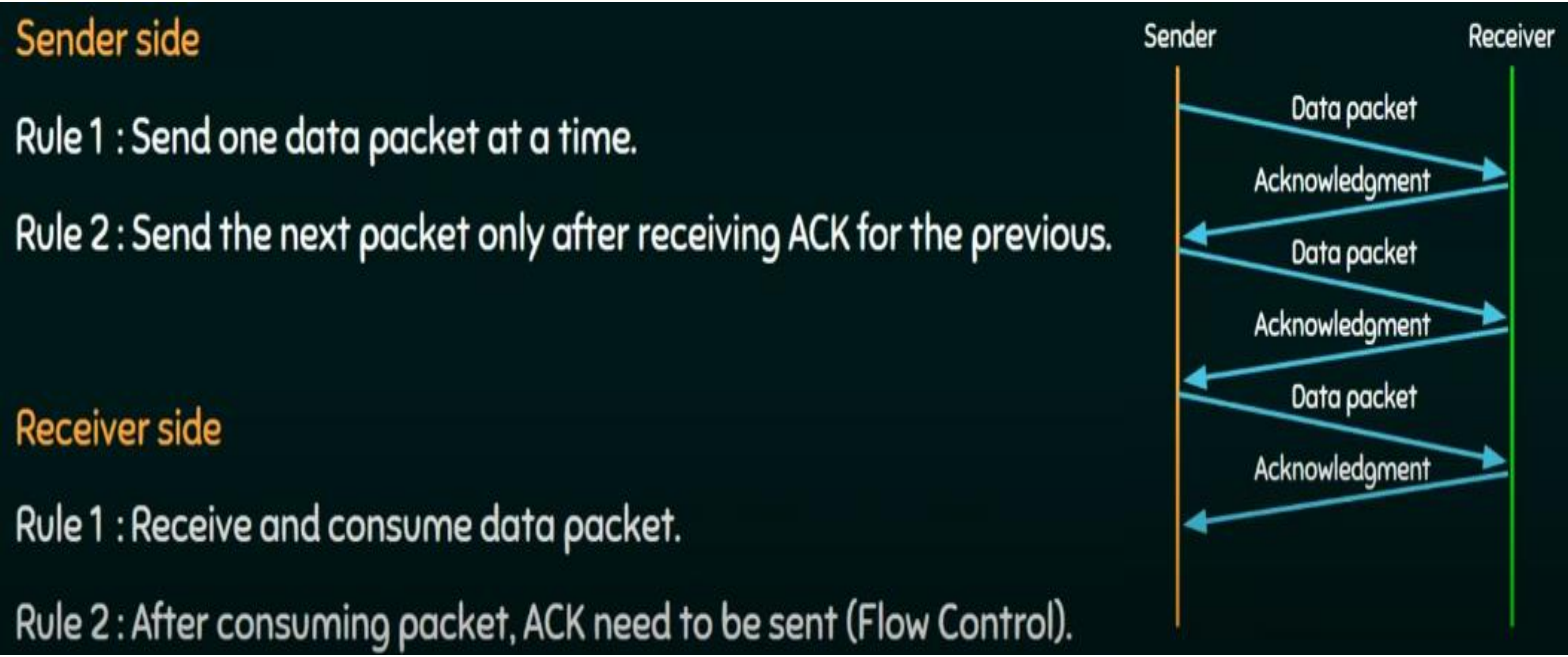
- ★ Stop-and-wait ARQ
- ★ Go-Back-N-ARQ
- ★ Selective Repeat ARQ

Stop and Wait Protocol



- ★ Stop – and – Wait protocol is data link layer protocol for transmission of frames over noiseless channels.
- ★ It provides unidirectional data transmission with flow control facilities but without error control facilities.
- ★ The idea of stop-and-wait protocol is straightforward.
- ★ After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.

Stop and Wait Protocol



Sender side

Rule 1 : Send one data packet at a time.

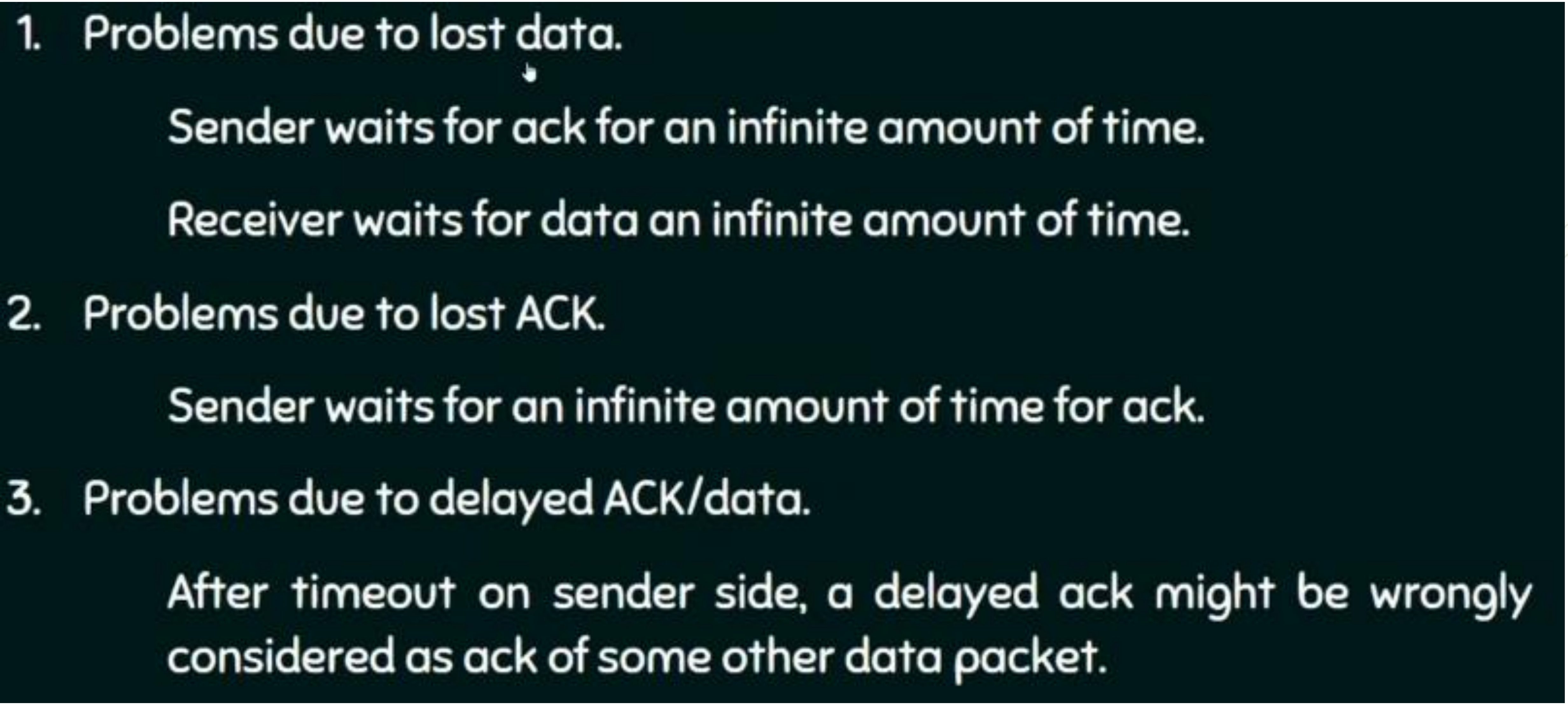
Rule 2 : Send the next packet only after receiving ACK for the previous.

Receiver side

Rule 1 : Receive and consume data packet.

Rule 2 : After consuming packet, ACK need to be sent (Flow Control).

Problems in Stop and Wait Protocol



1. Problems due to lost data.

   Sender waits for ack for an infinite amount of time.

   Receiver waits for data an infinite amount of time.

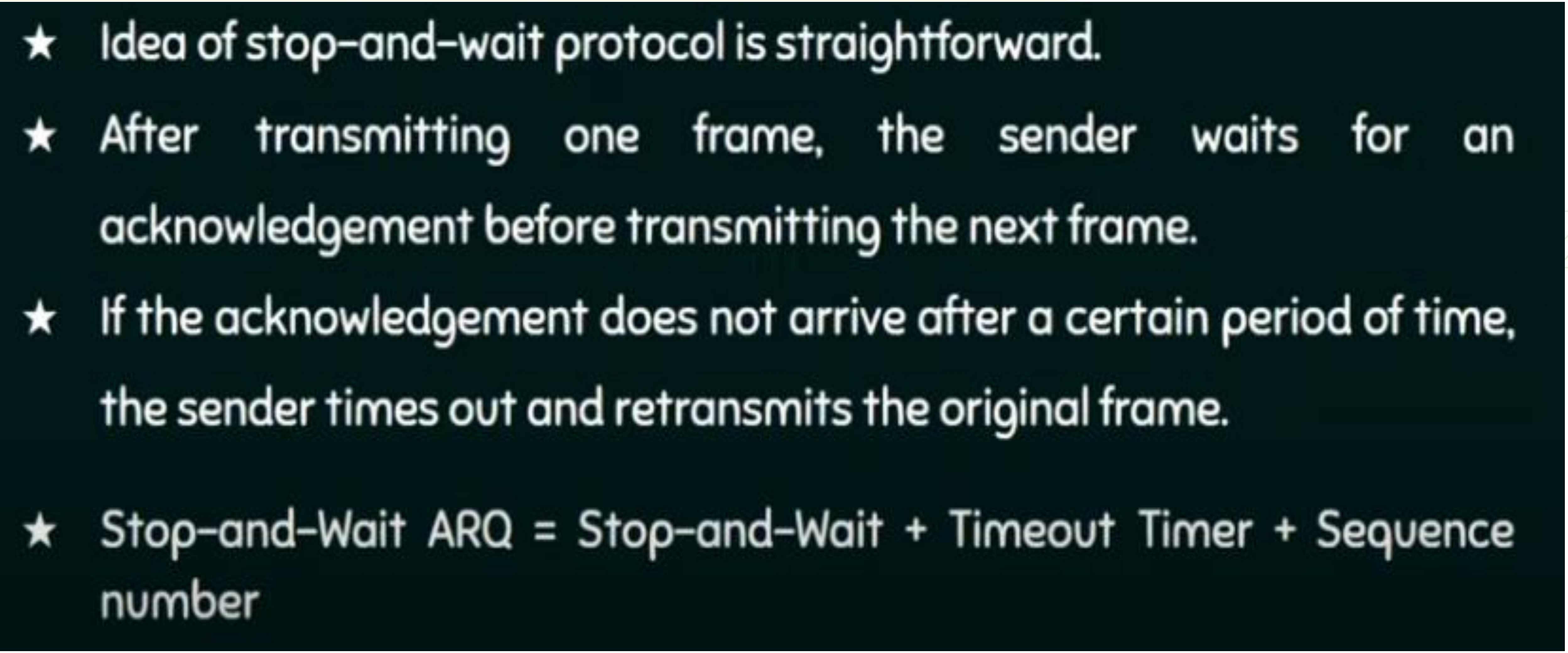
2. Problems due to lost ACK.

   Sender waits for an infinite amount of time for ack.

3. Problems due to delayed ACK/data.

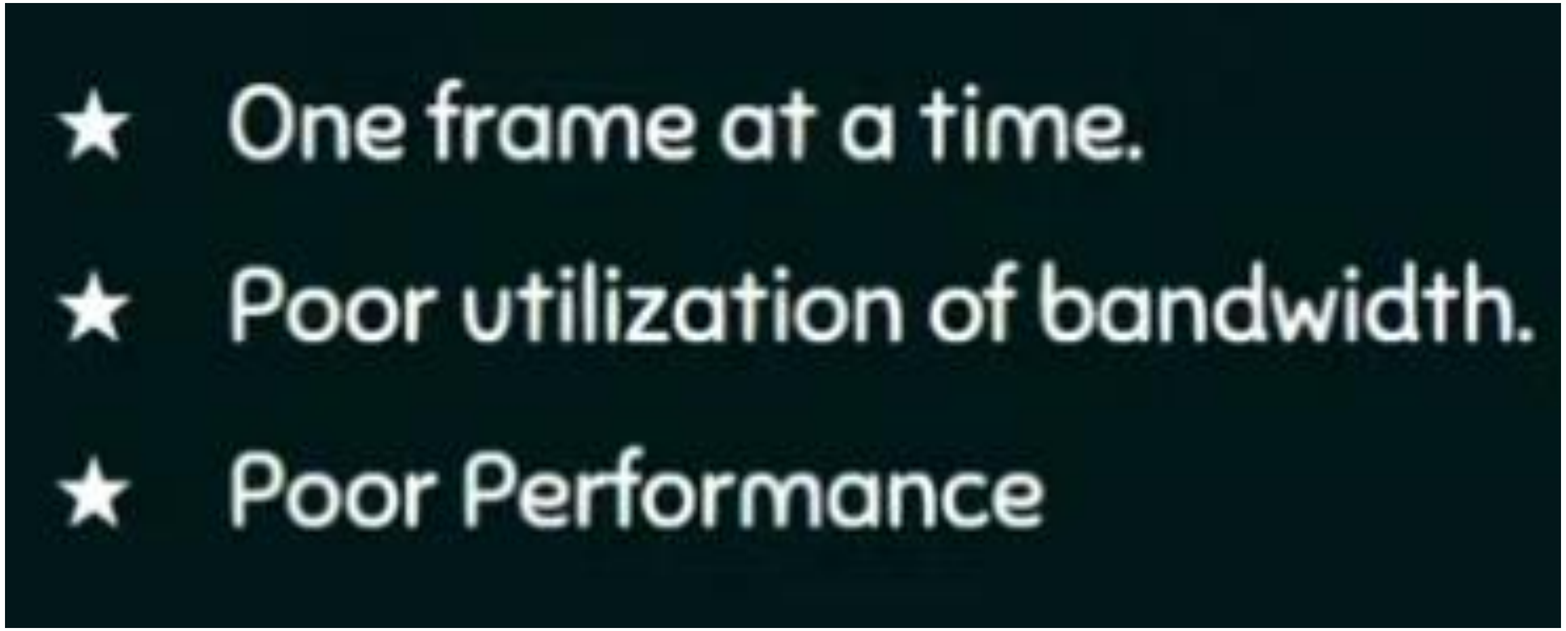
   After timeout on sender side, a delayed ack might be wrongly considered as ack of some other data packet.

Stop and Wait ARQ Protocol



- ★ Idea of stop-and-wait protocol is straightforward.
- ★ After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
- ★ If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.
- ★ Stop-and-Wait ARQ = Stop-and-Wait + Timeout Timer + Sequence number

Drawbacks of Stop and Wait ARQ Protocol

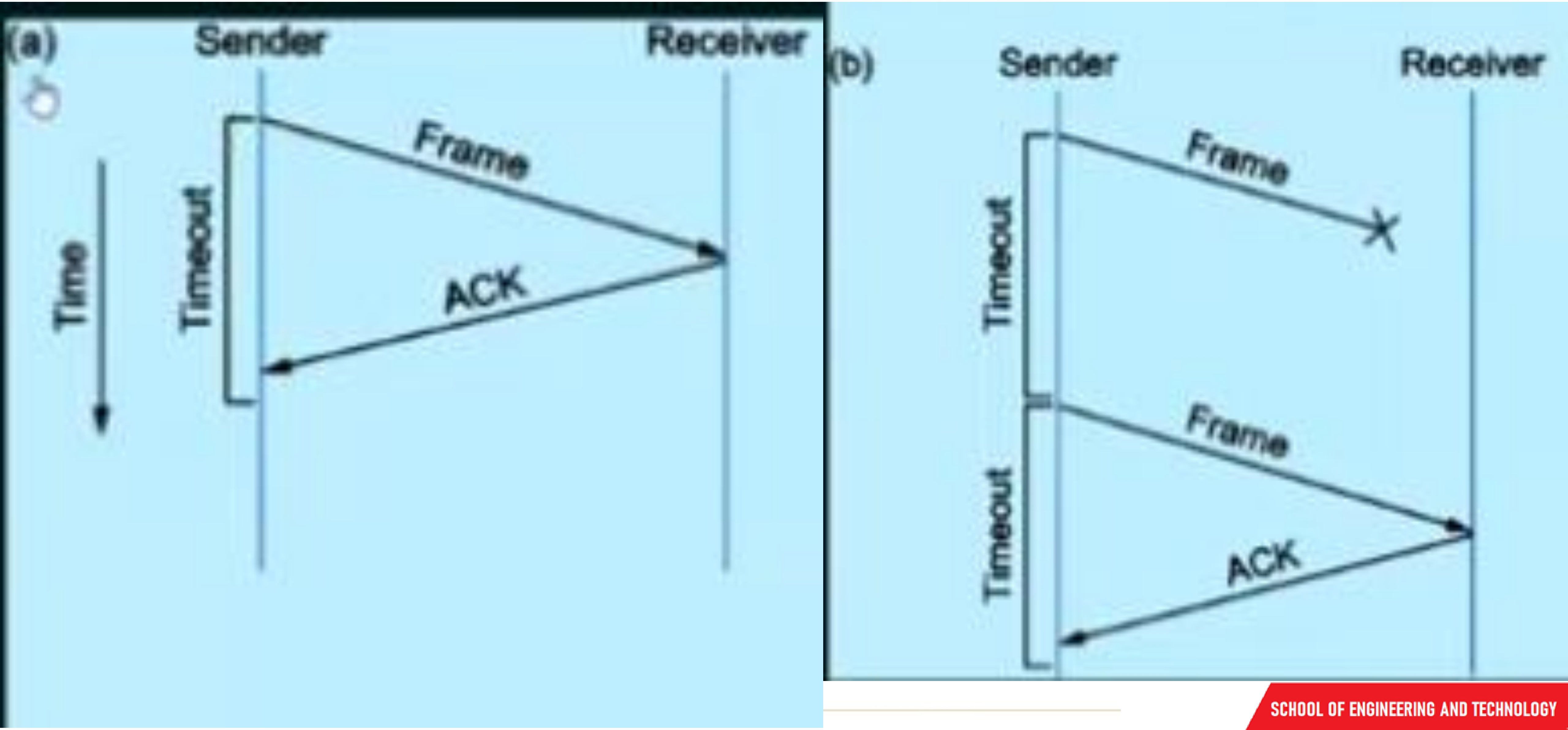


★ One frame at a time.

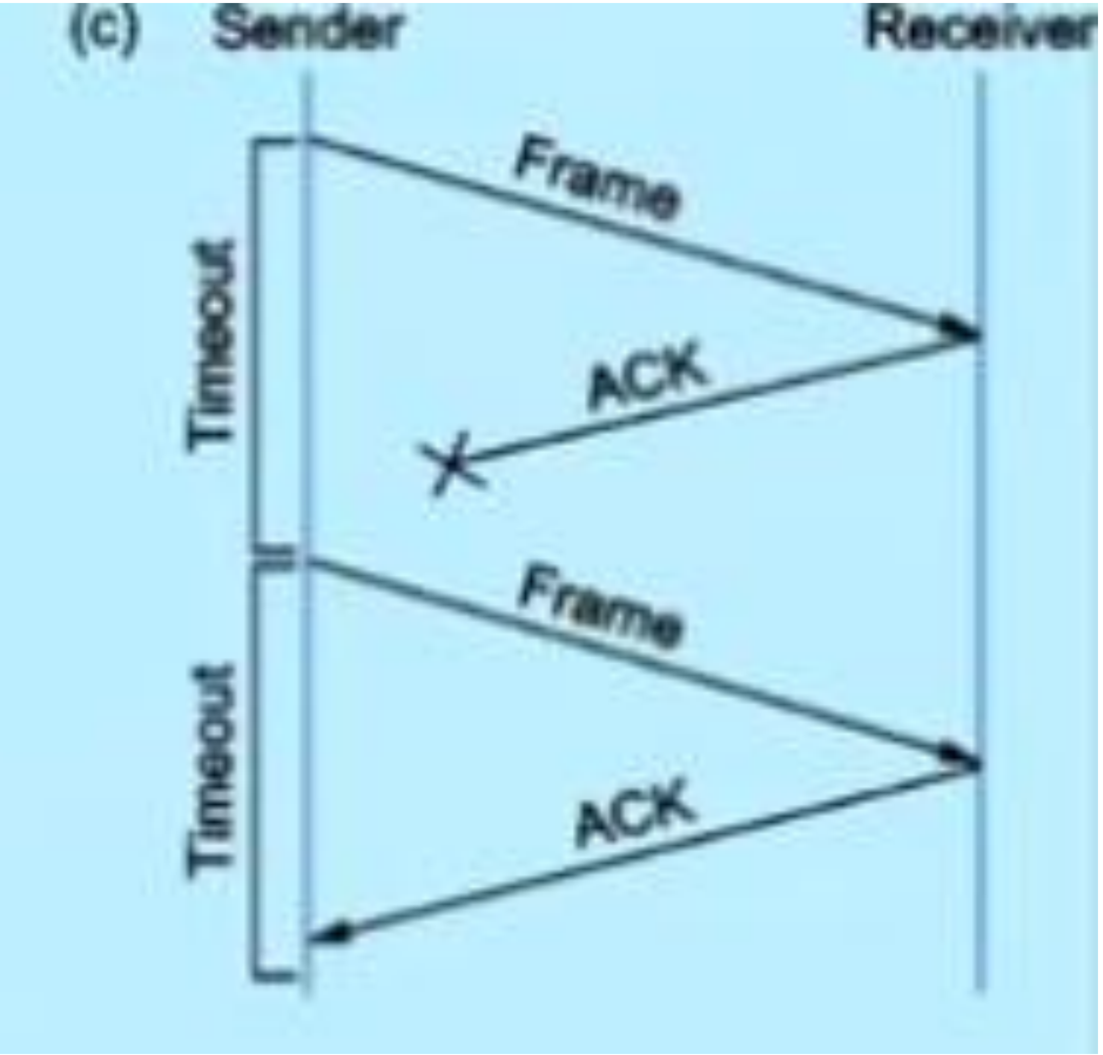
★ Poor utilization of bandwidth.

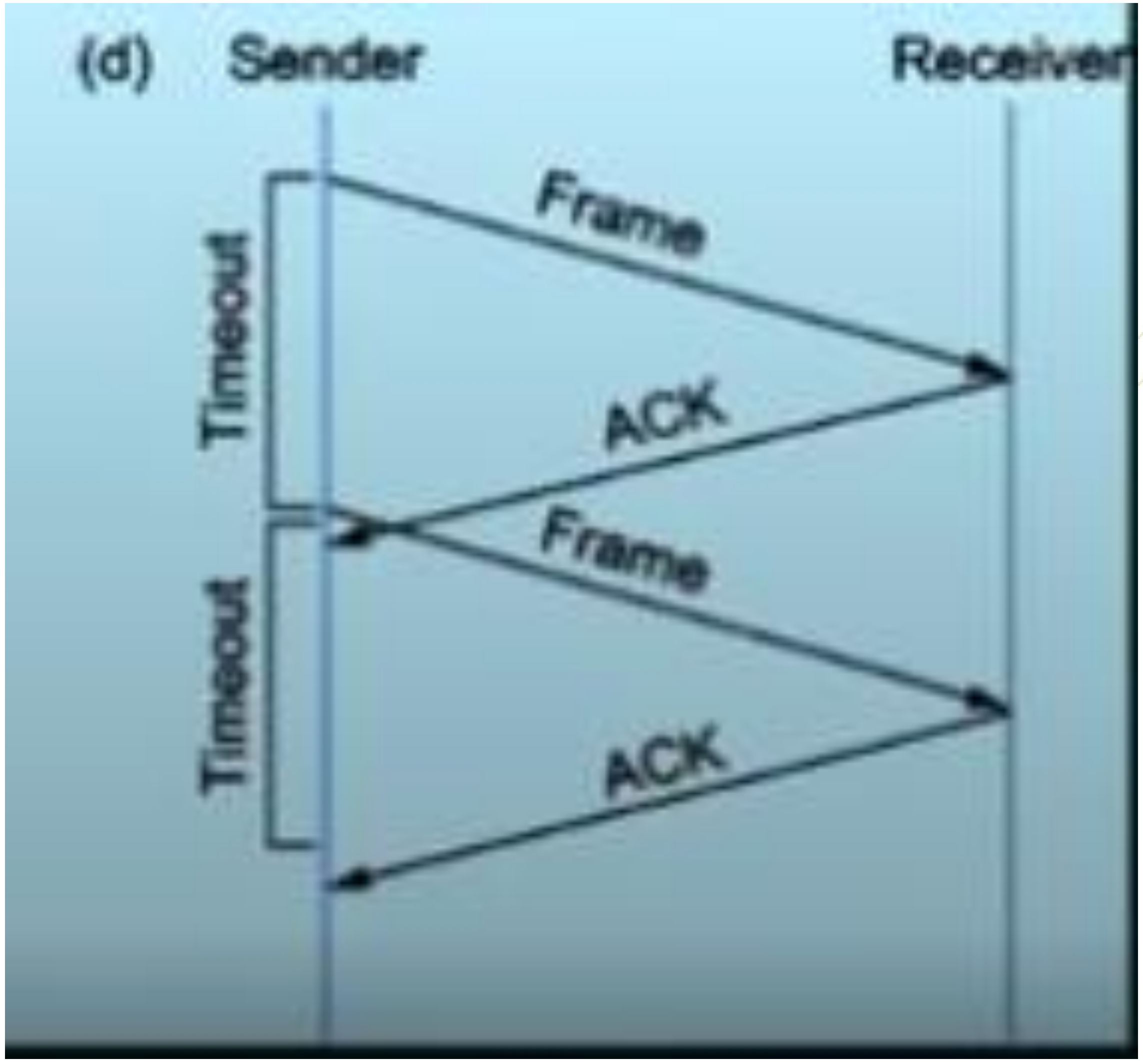
★ Poor Performance

Example- Stop and Wait ARQ Protocol

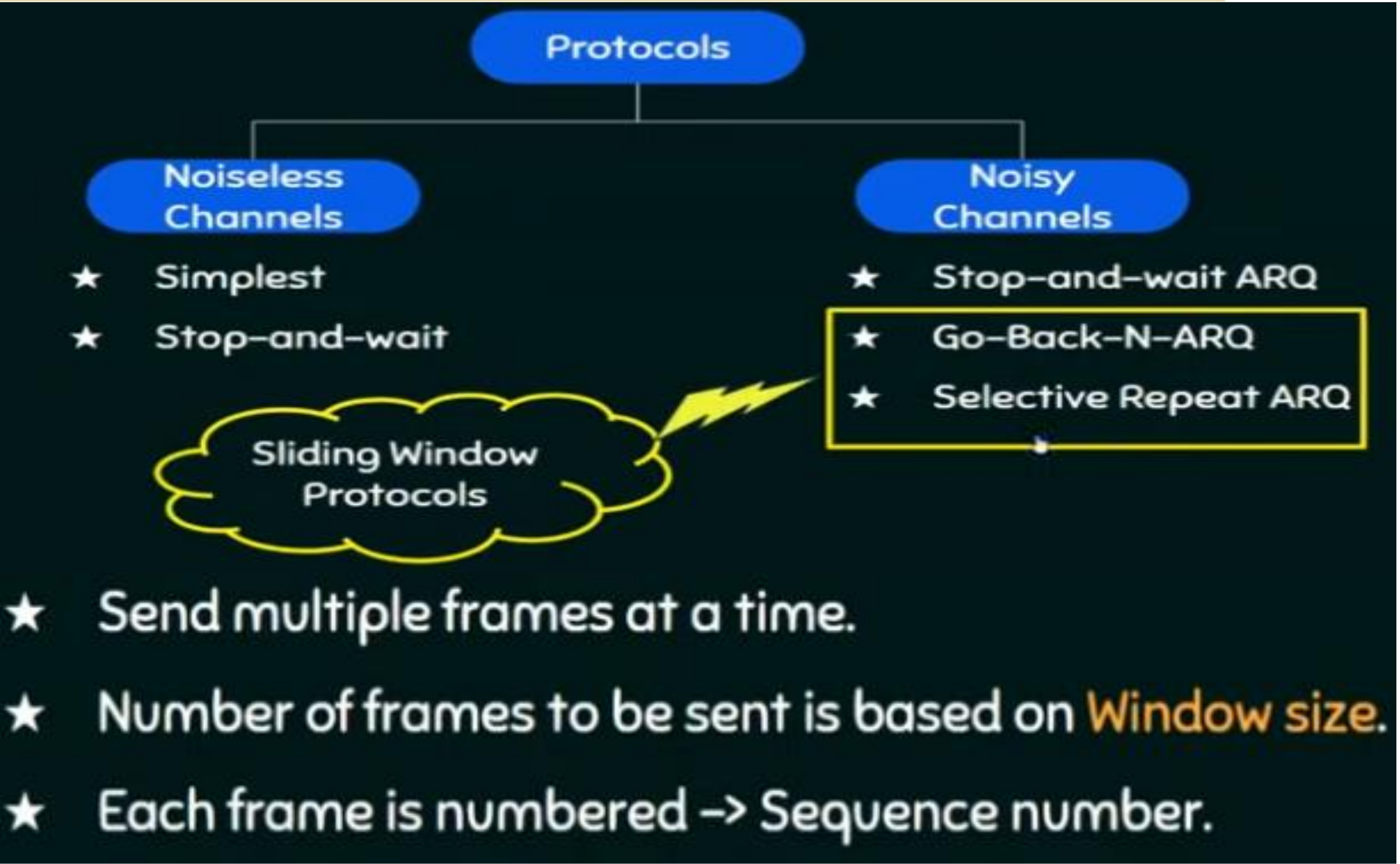


Example- Stop and Wait ARQ Protocol





Sliding Window Protocols



Protocols

Noiseless Channels

- ★ Simplest
- ★ Stop–and–wait

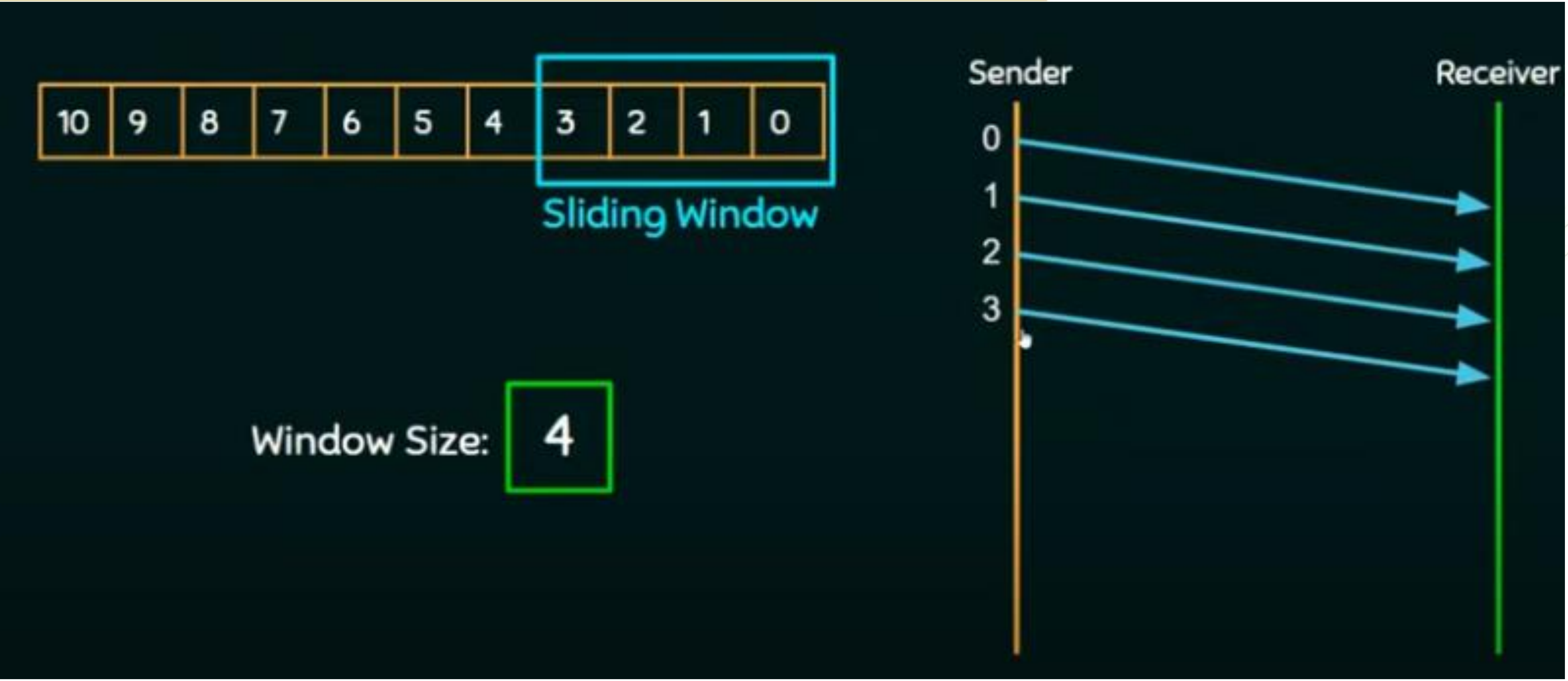
Noisy Channels

- ★ Stop–and–wait ARQ
- ★ Go–Back–N–ARQ
- ★ Selective Repeat ARQ

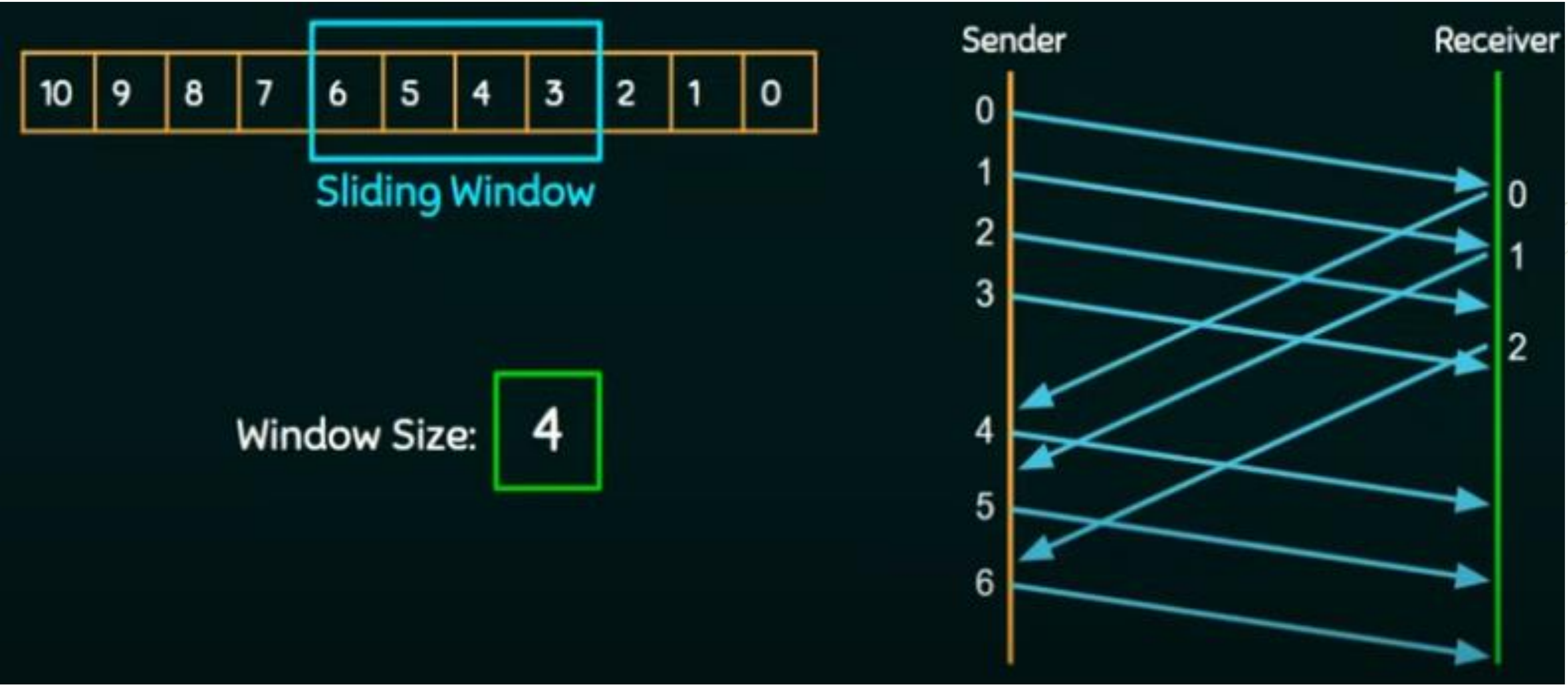
Sliding Window Protocols

- ★ Send multiple frames at a time.
- ★ Number of frames to be sent is based on Window size.
- ★ Each frame is numbered –> Sequence number.

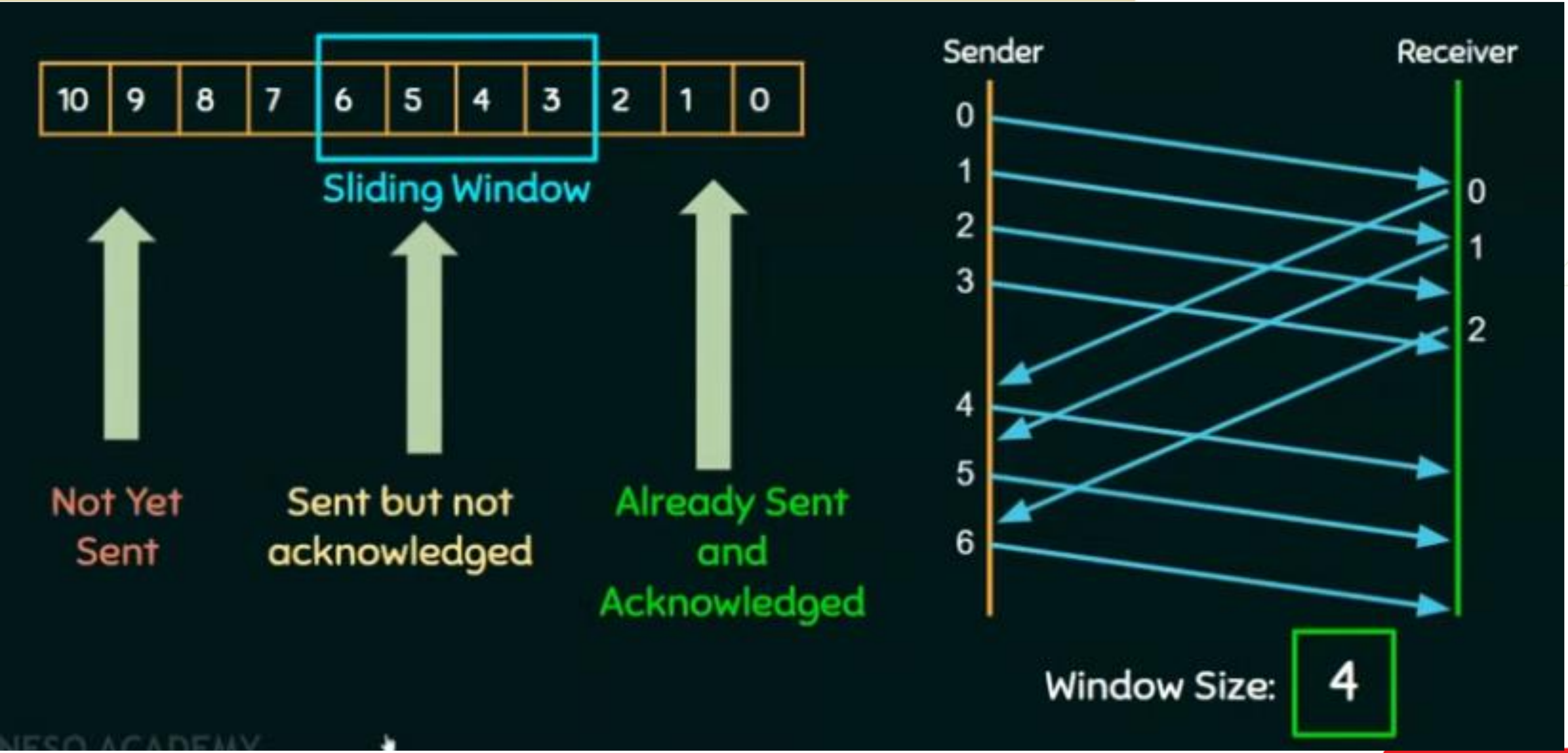
Example- Sliding Window Protocols



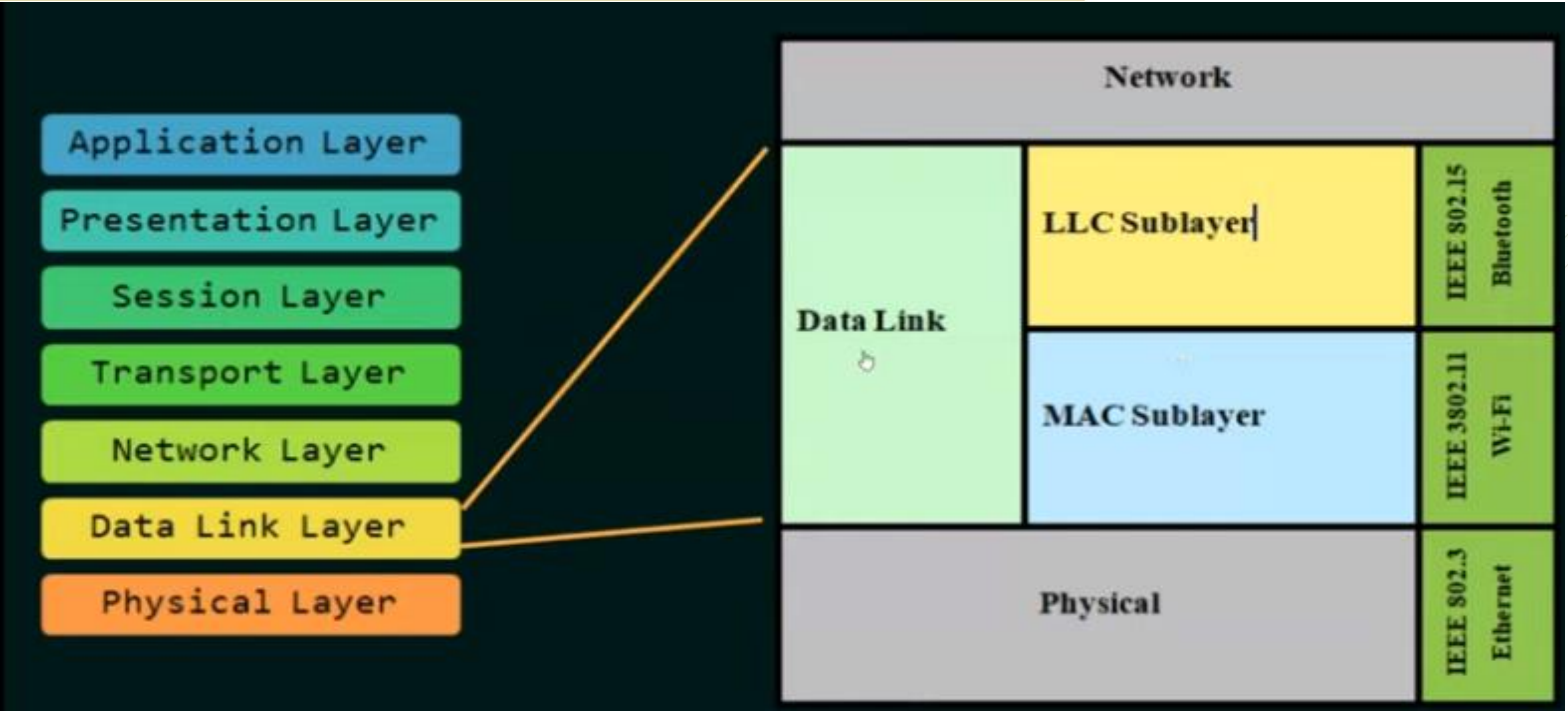
Example- Sliding Window Protocols



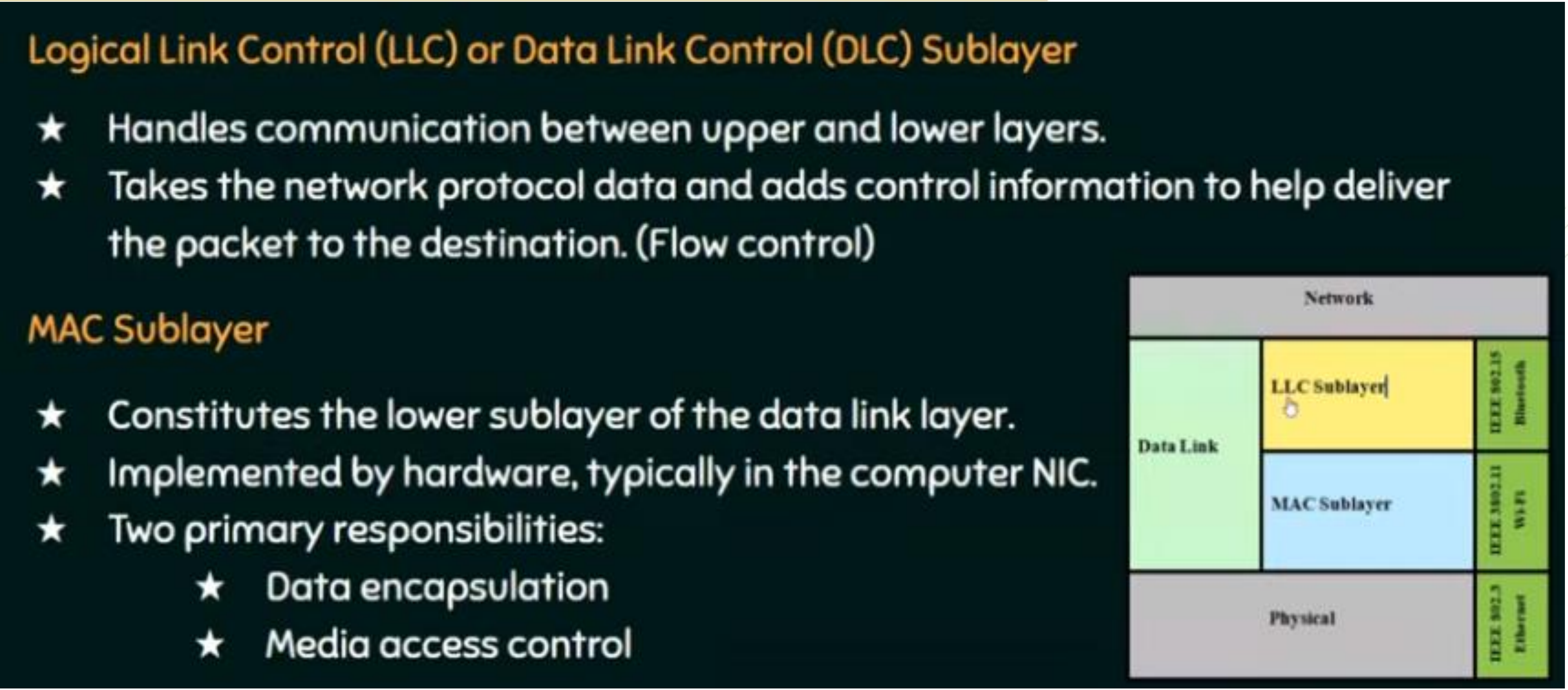
Example- Sliding Window Protocols



MAC Sublayer



MAC Sublayer



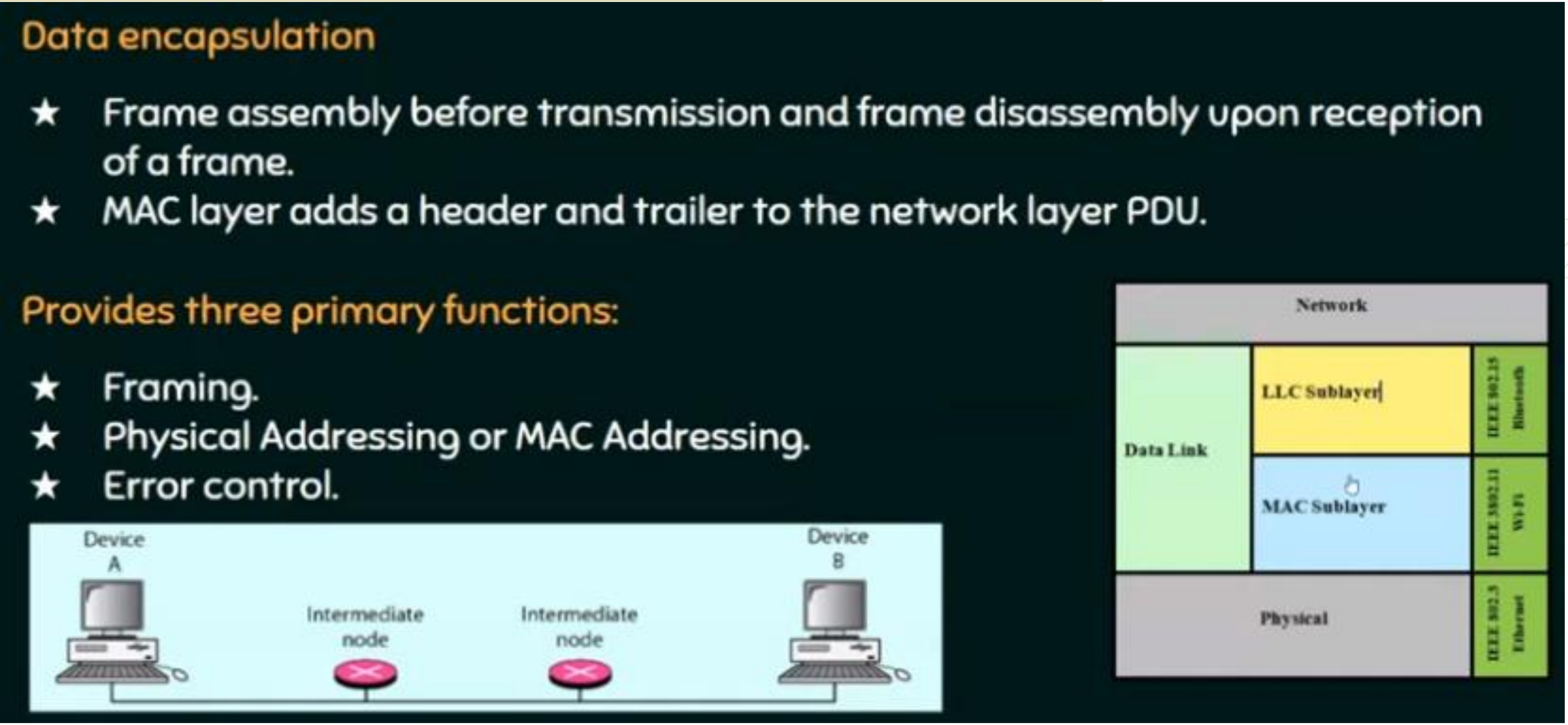
Logical Link Control (LLC) or Data Link Control (DLC) Sublayer

- ★ Handles communication between upper and lower layers.
- ★ Takes the network protocol data and adds control information to help deliver the packet to the destination. (Flow control)

MAC Sublayer

- ★ Constitutes the lower sublayer of the data link layer.
- ★ Implemented by hardware, typically in the computer NIC.
- ★ Two primary responsibilities:
    - ★ Data encapsulation
    - ★ Media access control

MAC Sublayer



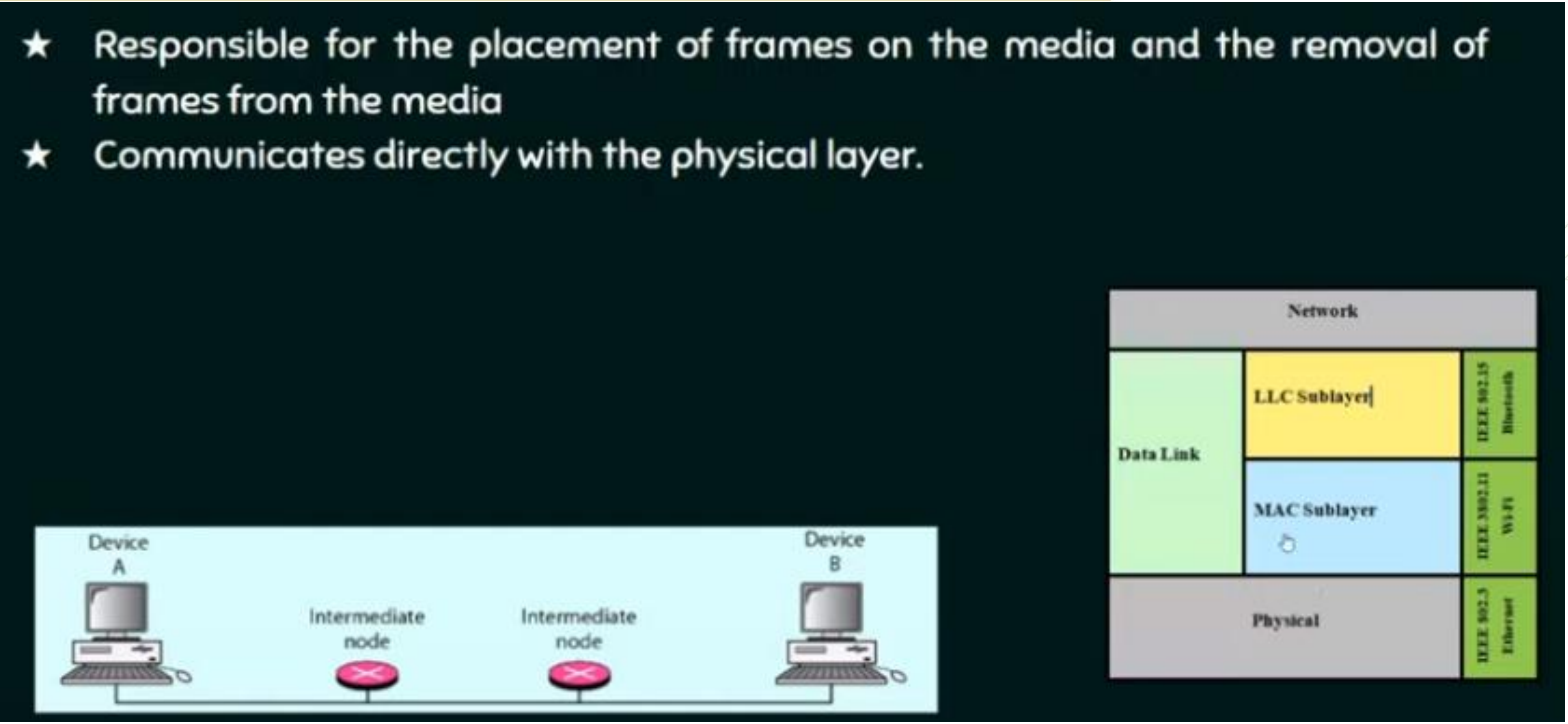
Data encapsulation

- ★ Frame assembly before transmission and frame disassembly upon reception of a frame.
- ★ MAC layer adds a header and trailer to the network layer PDU.

Provides three primary functions:

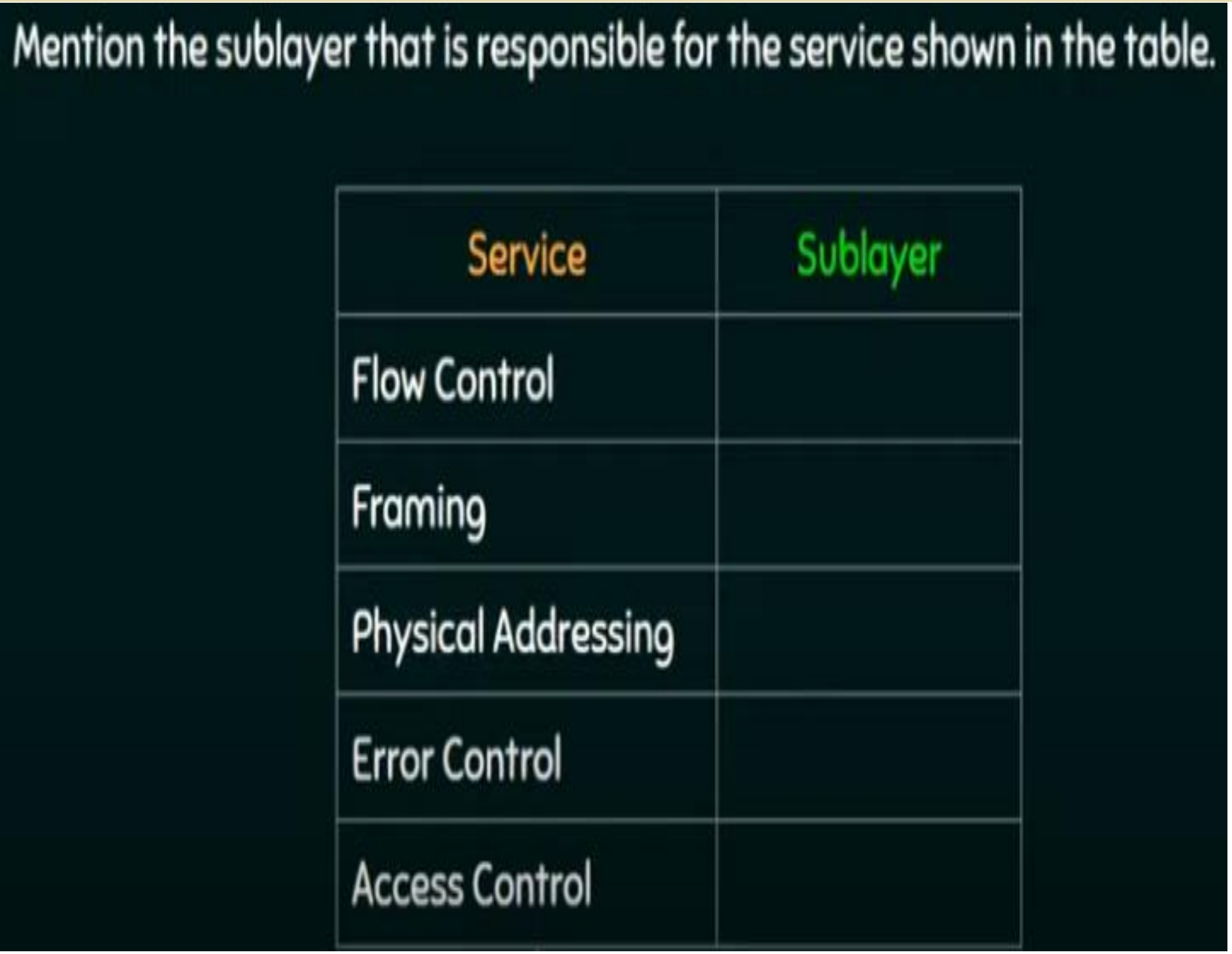
- ★ Framing.
- ★ Physical Addressing or MAC Addressing.
- ★ Error control.

MAC Sublayer



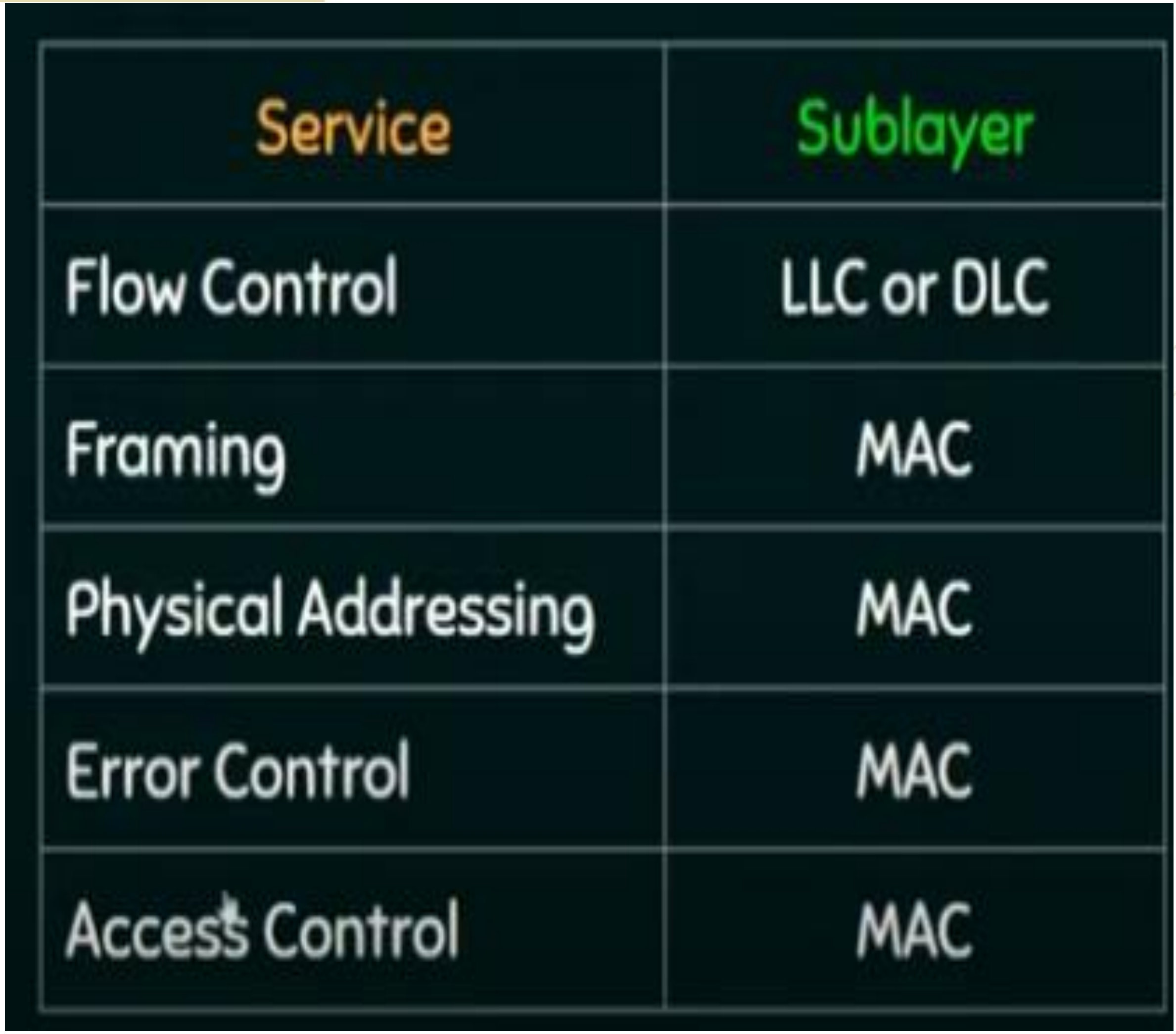
- ★ Responsible for the placement of frames on the media and the removal of frames from the media
- ★ Communicates directly with the physical layer.

Example of MAC Layer



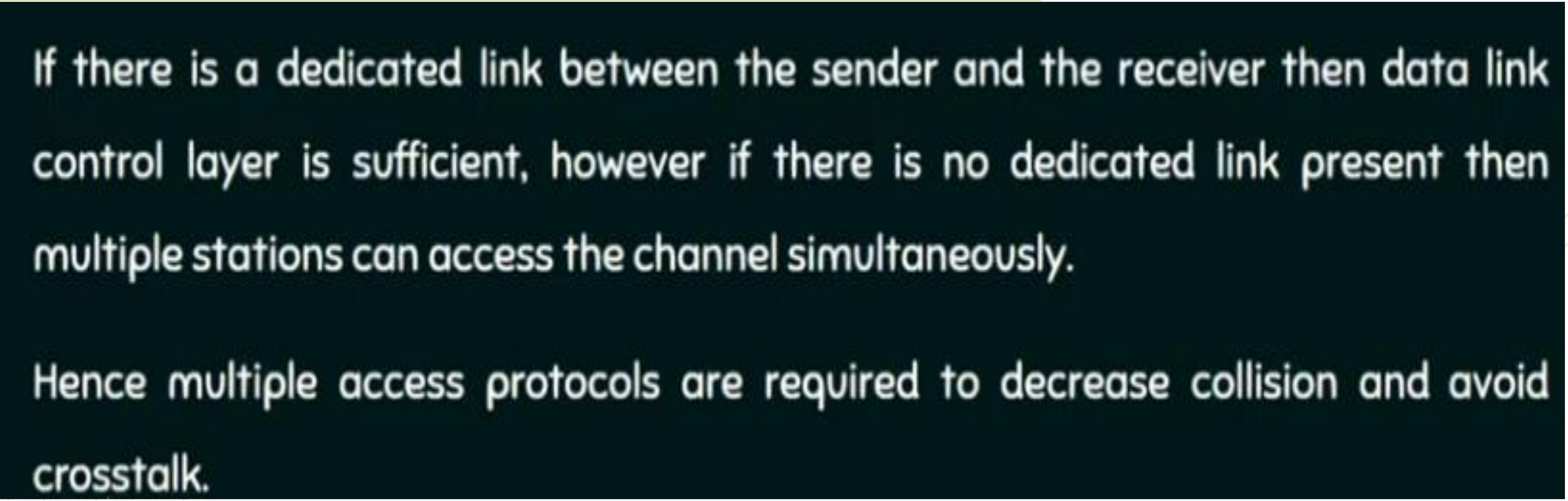
Mention the sublayer that is responsible for the service shown in the table.

Service	Sublayer
Flow Control	
Framing	
Physical Addressing	
Error Control	
Access Control	



Service	Sublayer
Flow Control	LLC or DLC
Framing	MAC
Physical Addressing	MAC
Error Control	MAC
Access Control	MAC

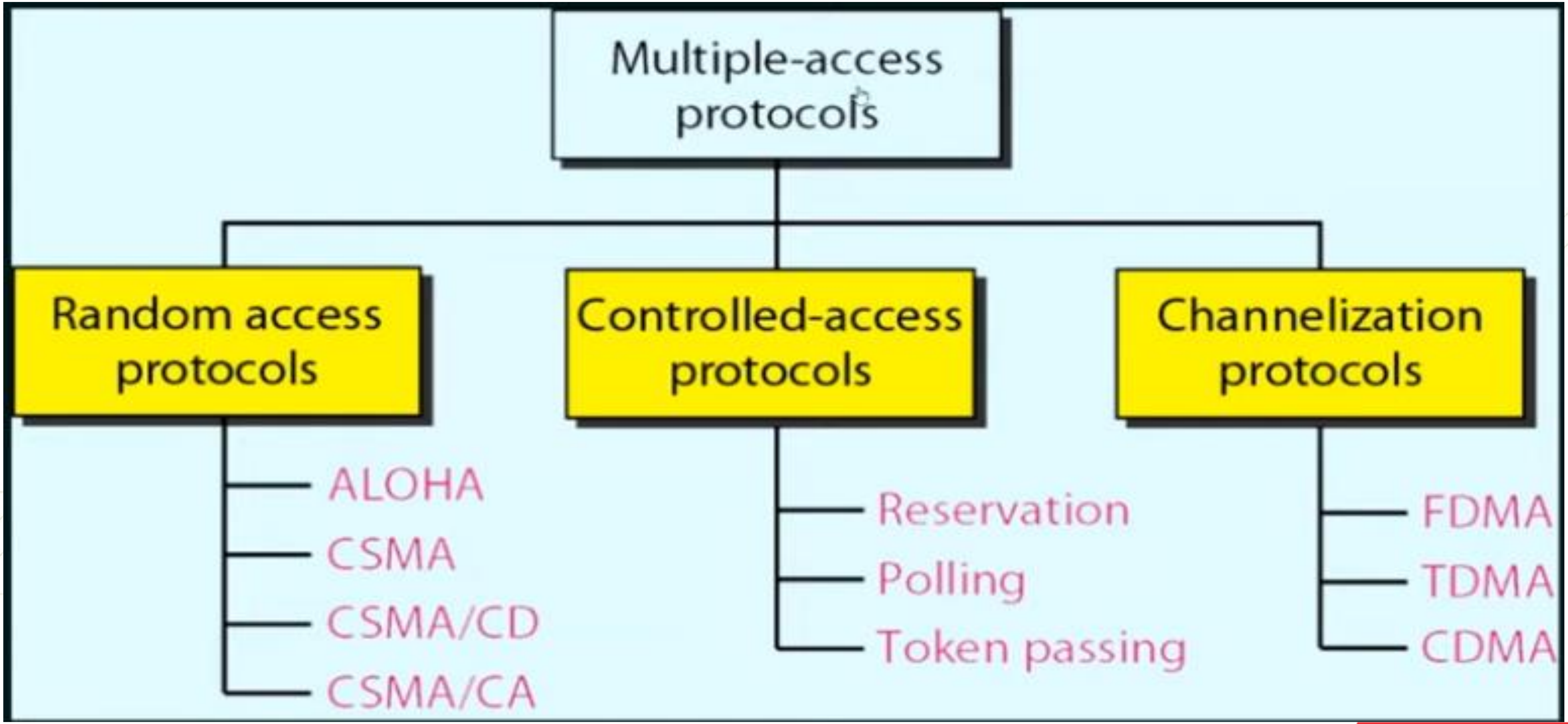
Multiple Access Protocol



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 Protocol



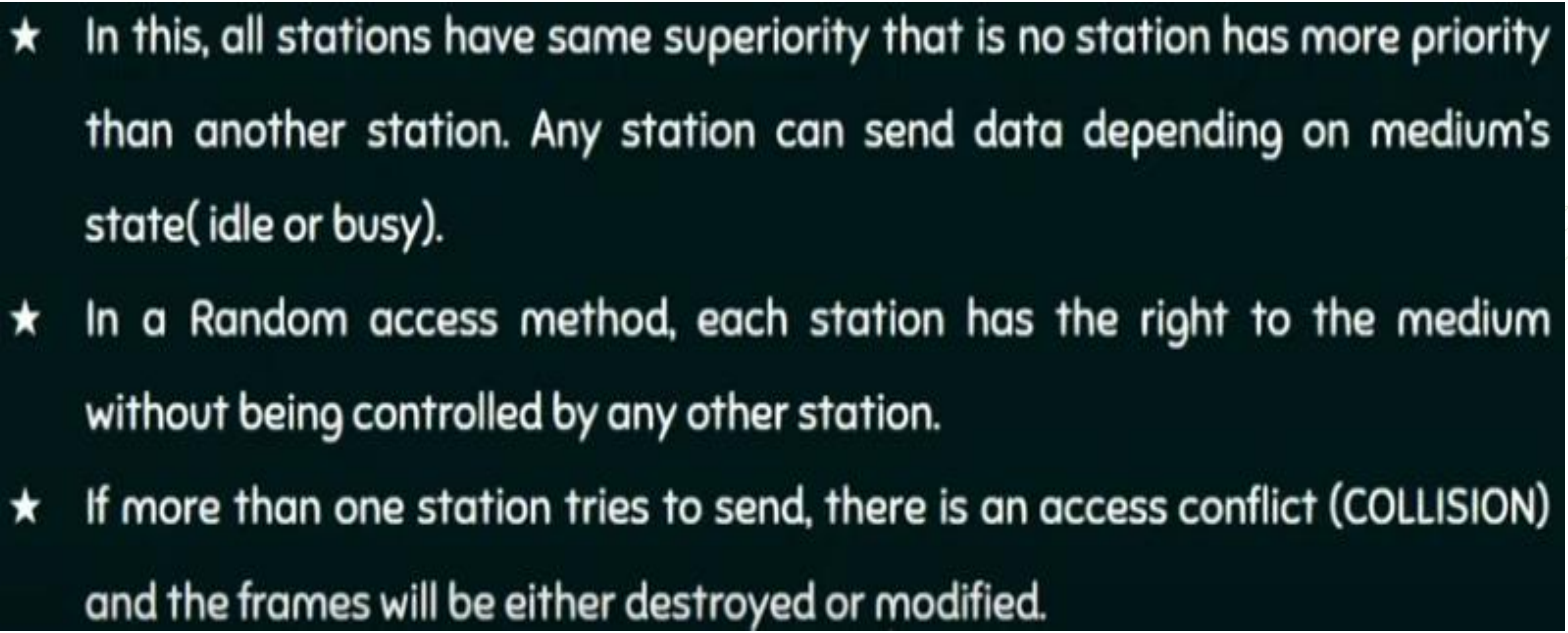
Multiple-access protocols

Random access protocols
- ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

Controlled-access protocols
- Reservation
- Polling
- Token passing

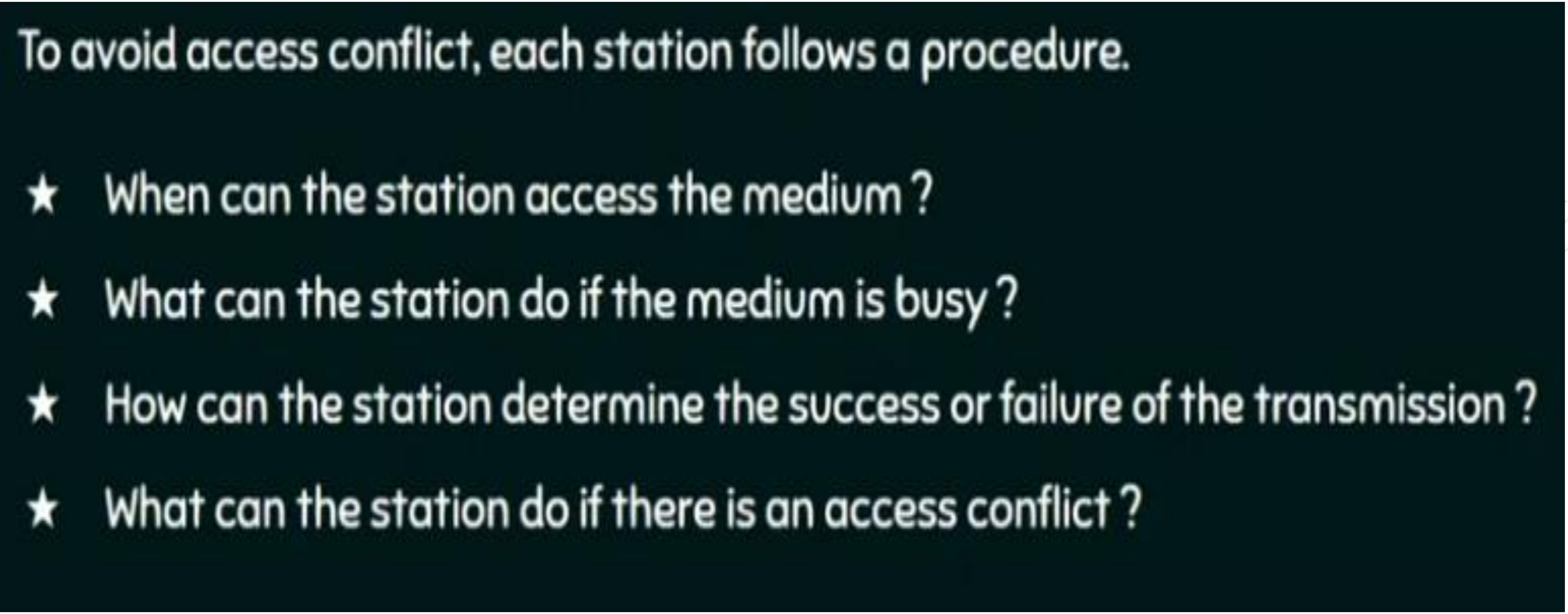
Channelization protocols
- FDMA
- TDMA
- CDMA

Random Access Protocol



- ★ 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.

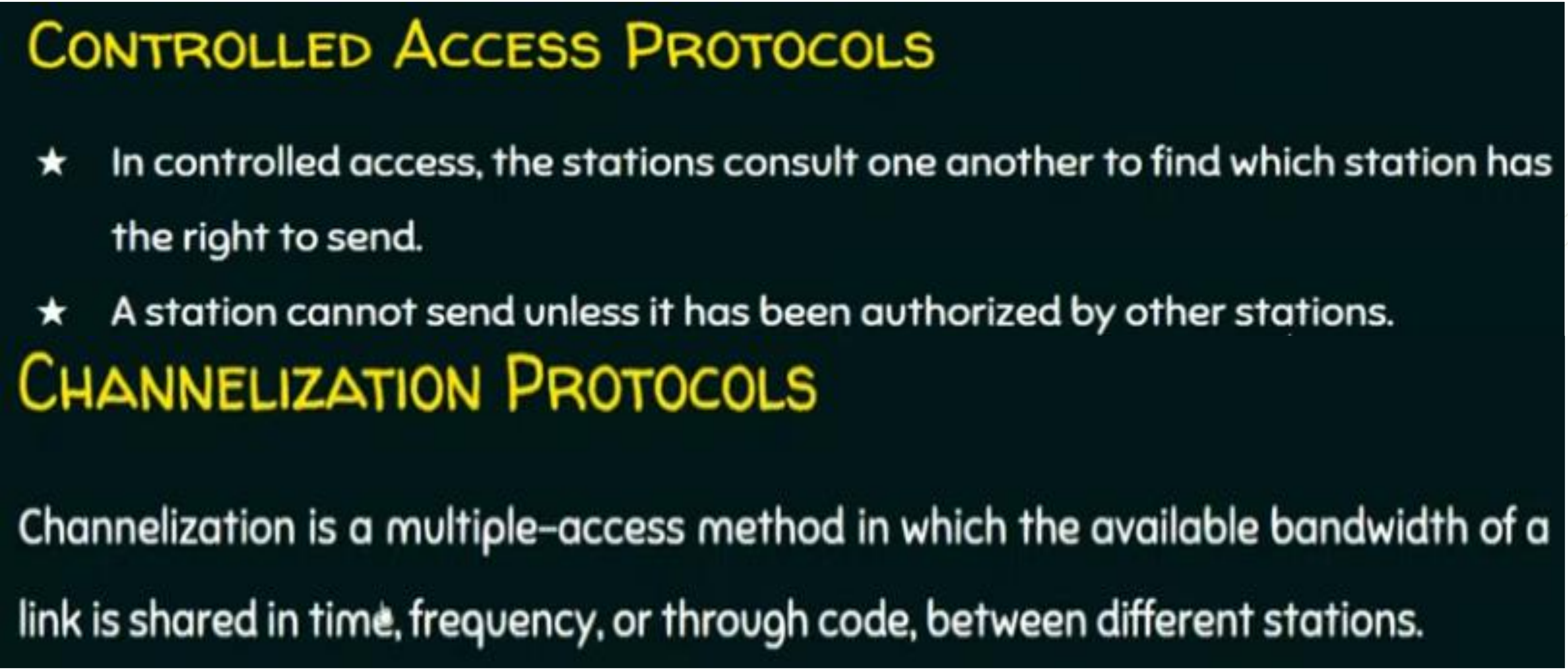
Random Access Protocol



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 ?

Multiple Access Protocol



Controlled Access Protocols

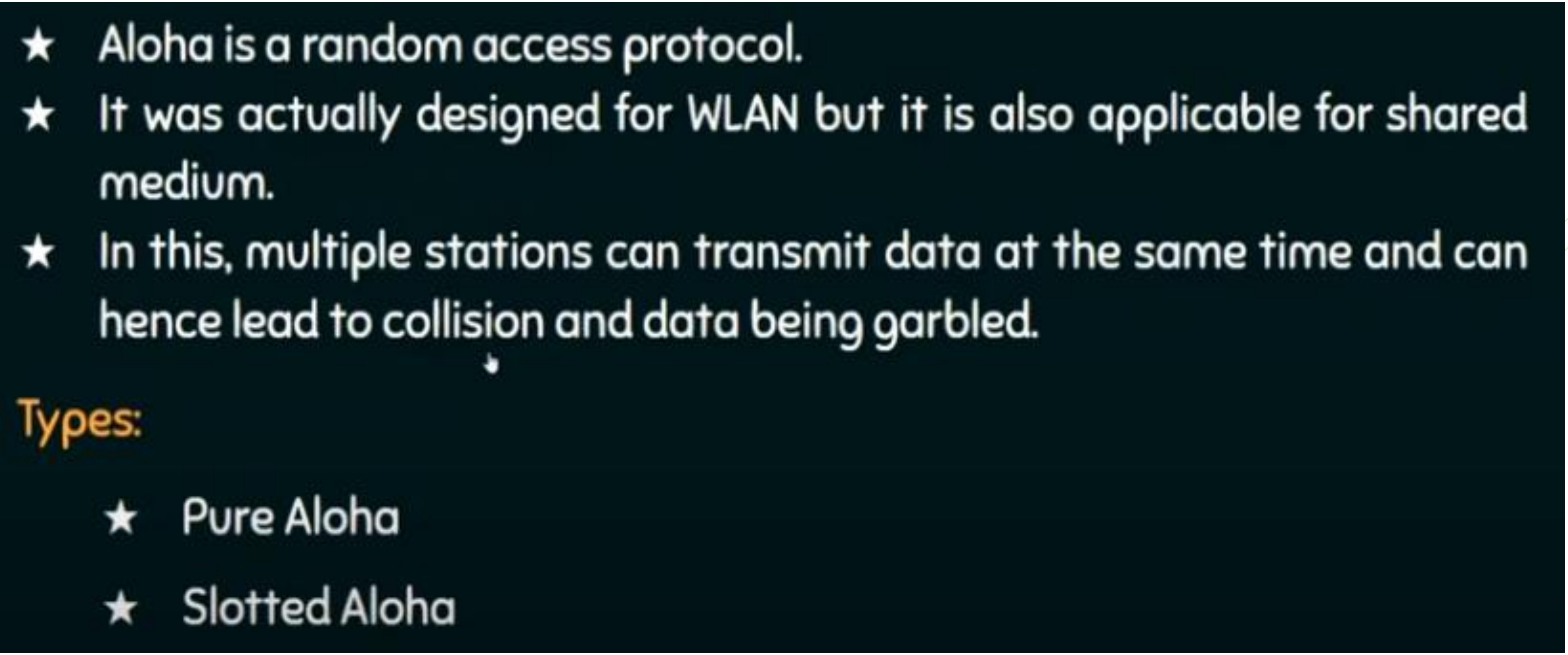
★ In controlled access, the stations consult one another to find which station has the right to send.

★ 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.

ALOHA- Random Access Protocol

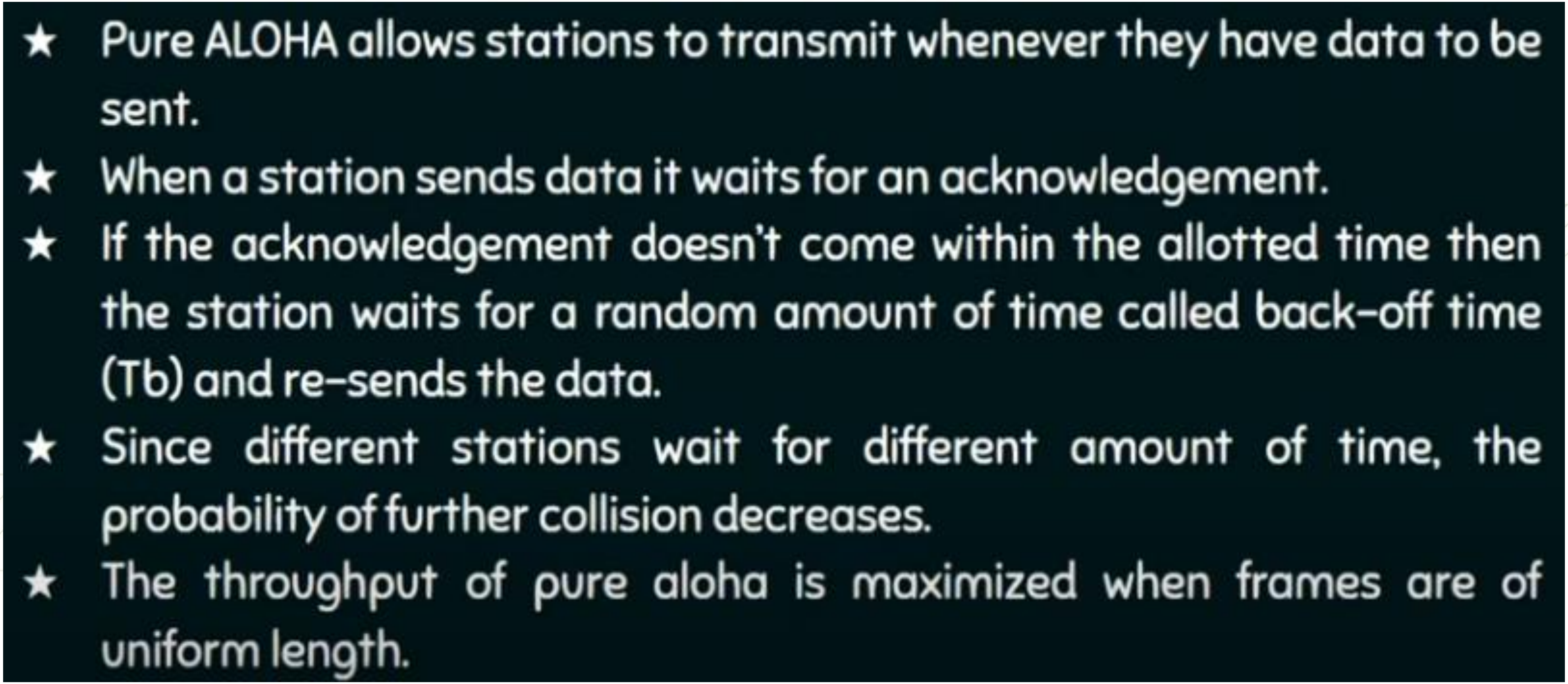


- ★ Aloha is a random access protocol.
- ★ It was actually designed for WLAN but it is also applicable for shared medium.
- ★ In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

Types:

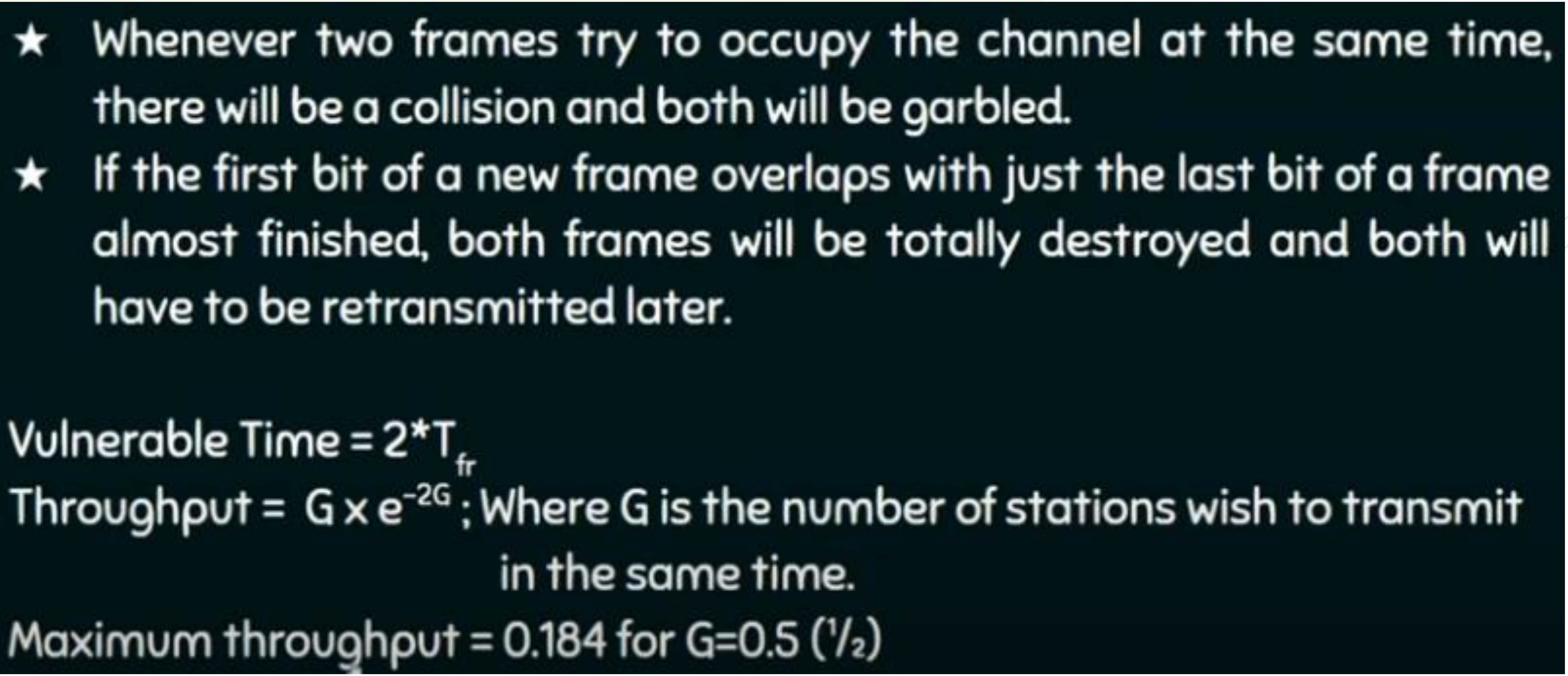
- ★ Pure Aloha
- ★ Slotted Aloha

ALOHA- Random Access Protocol



- ★ 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.

ALOHA- Random Access Protocol



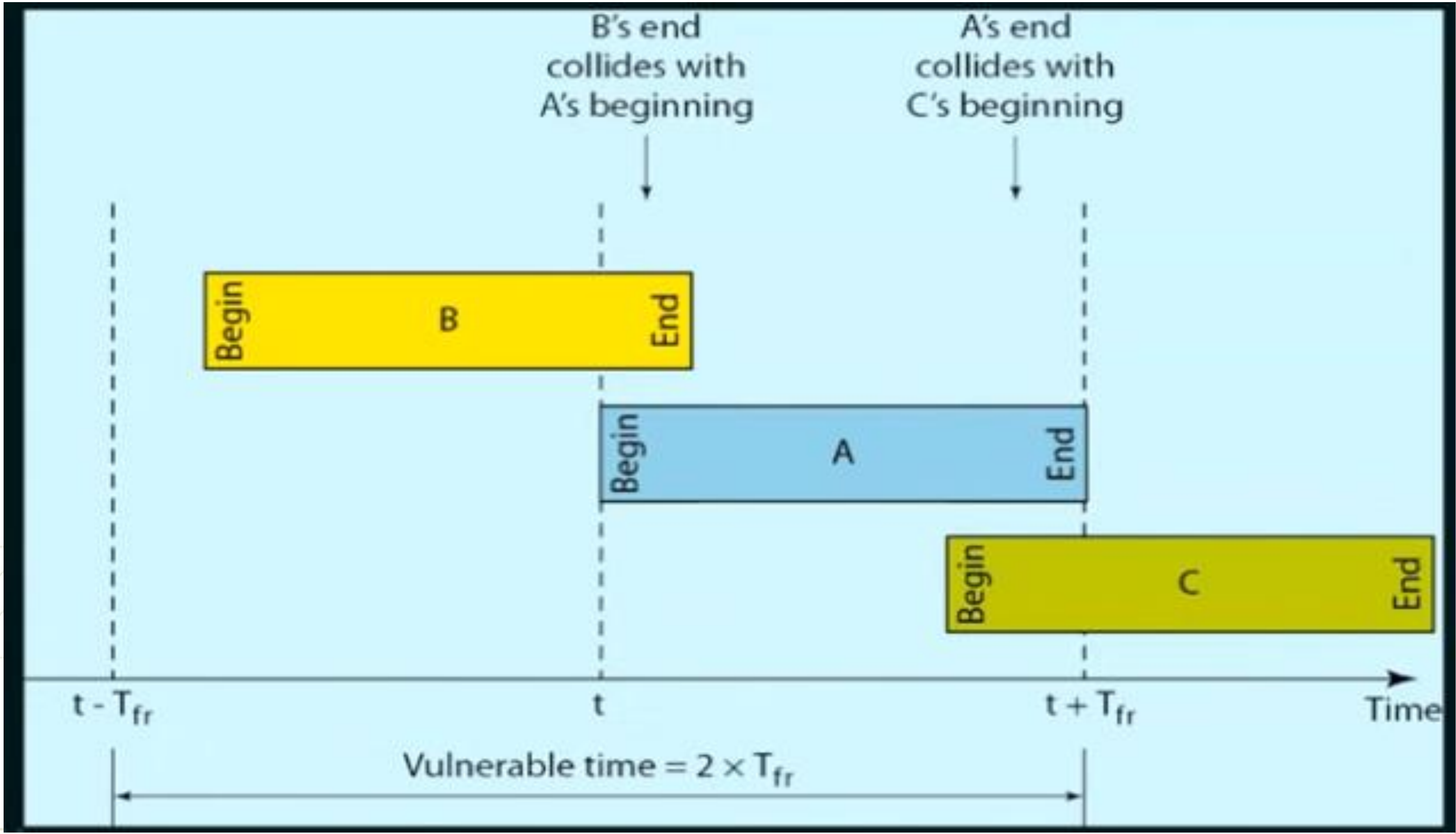
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
- If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

Vulnerable Time = $2*T_{fr}$

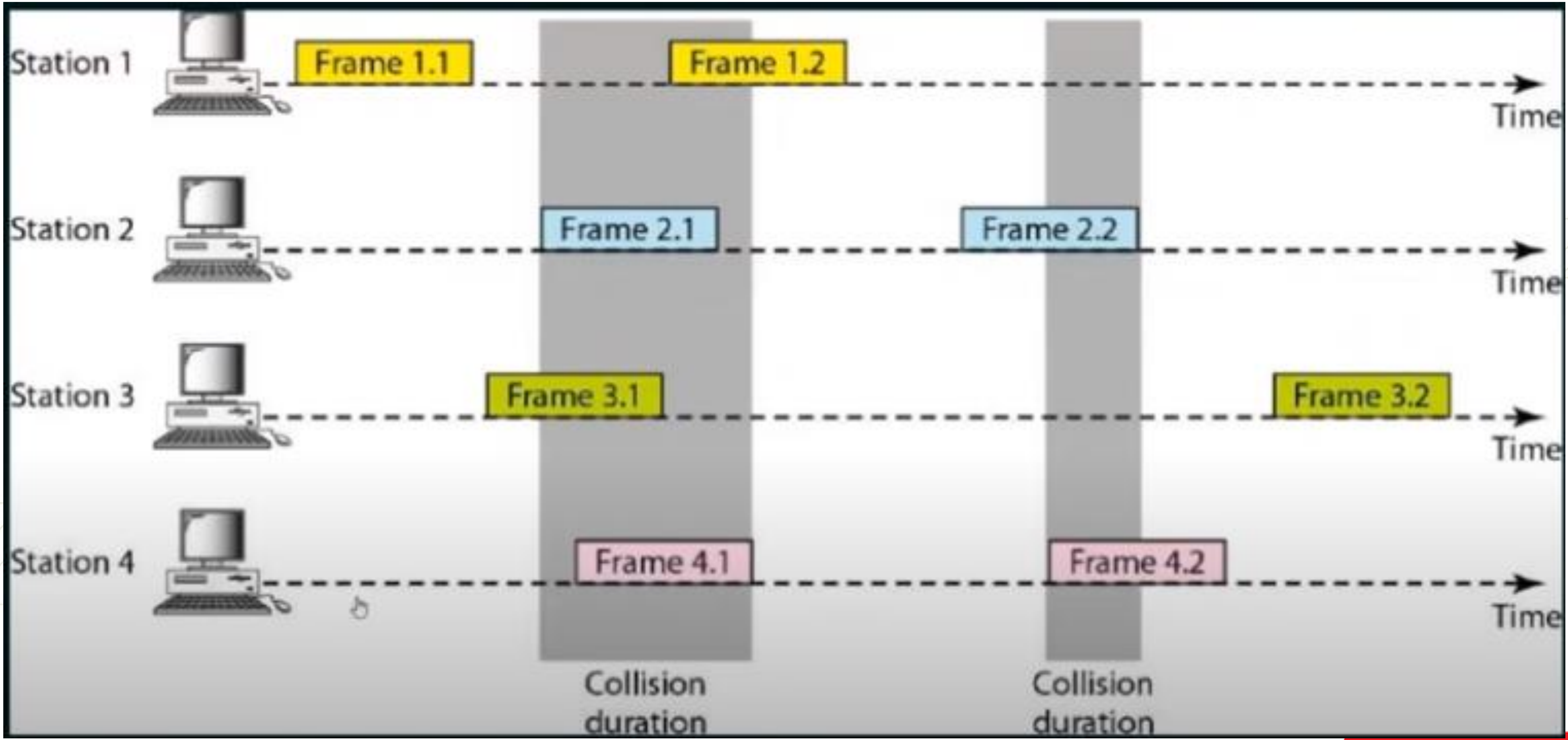
Throughput = $G \times e^{-2G}$; Where G is the number of stations wish to transmit in the same time.

Maximum throughput = 0.184 for G=0.5 (½)

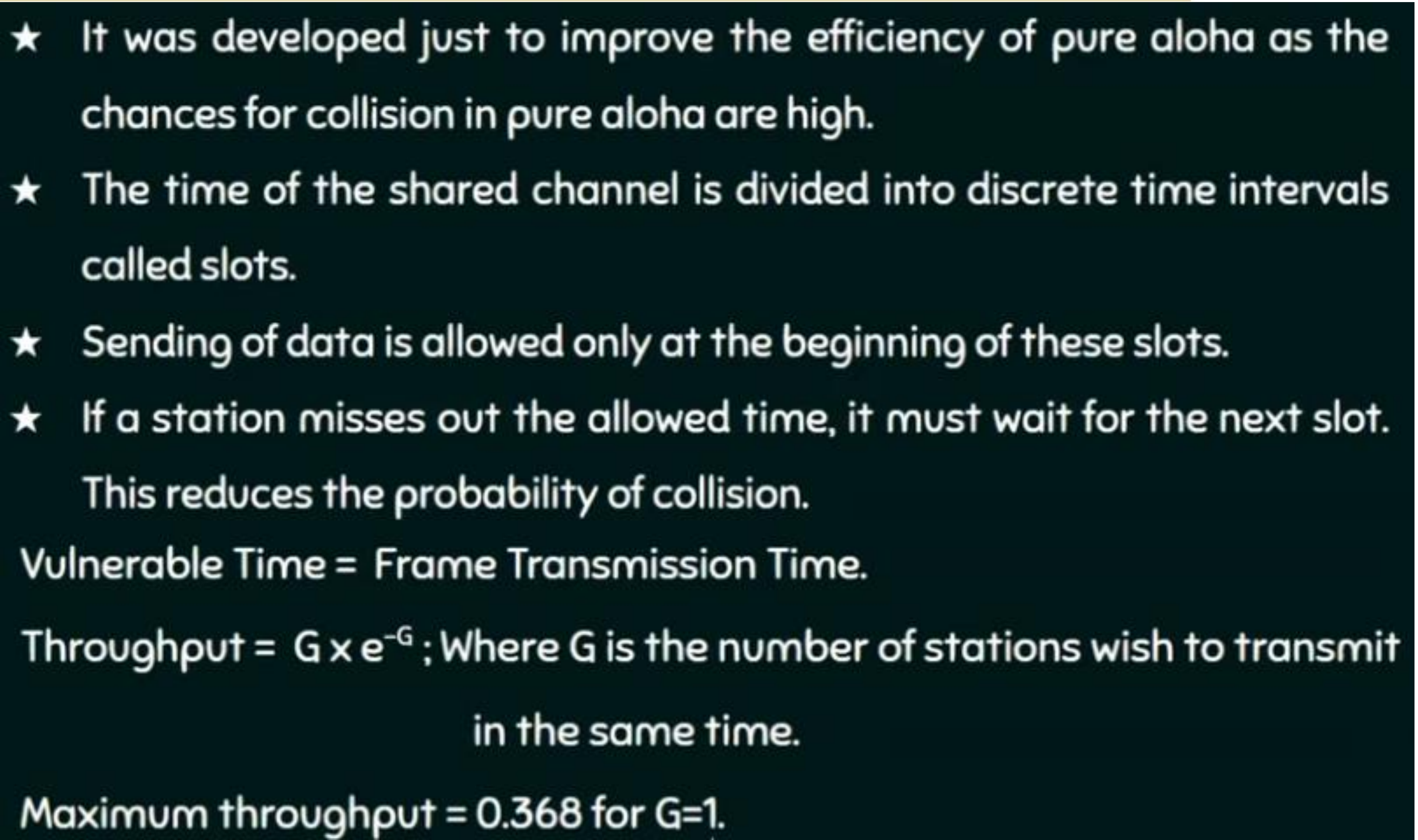
Example- Pure ALOHA


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 = $2 \times T_{fr}$

Example- Pure ALOHA



Slotted ALOHA



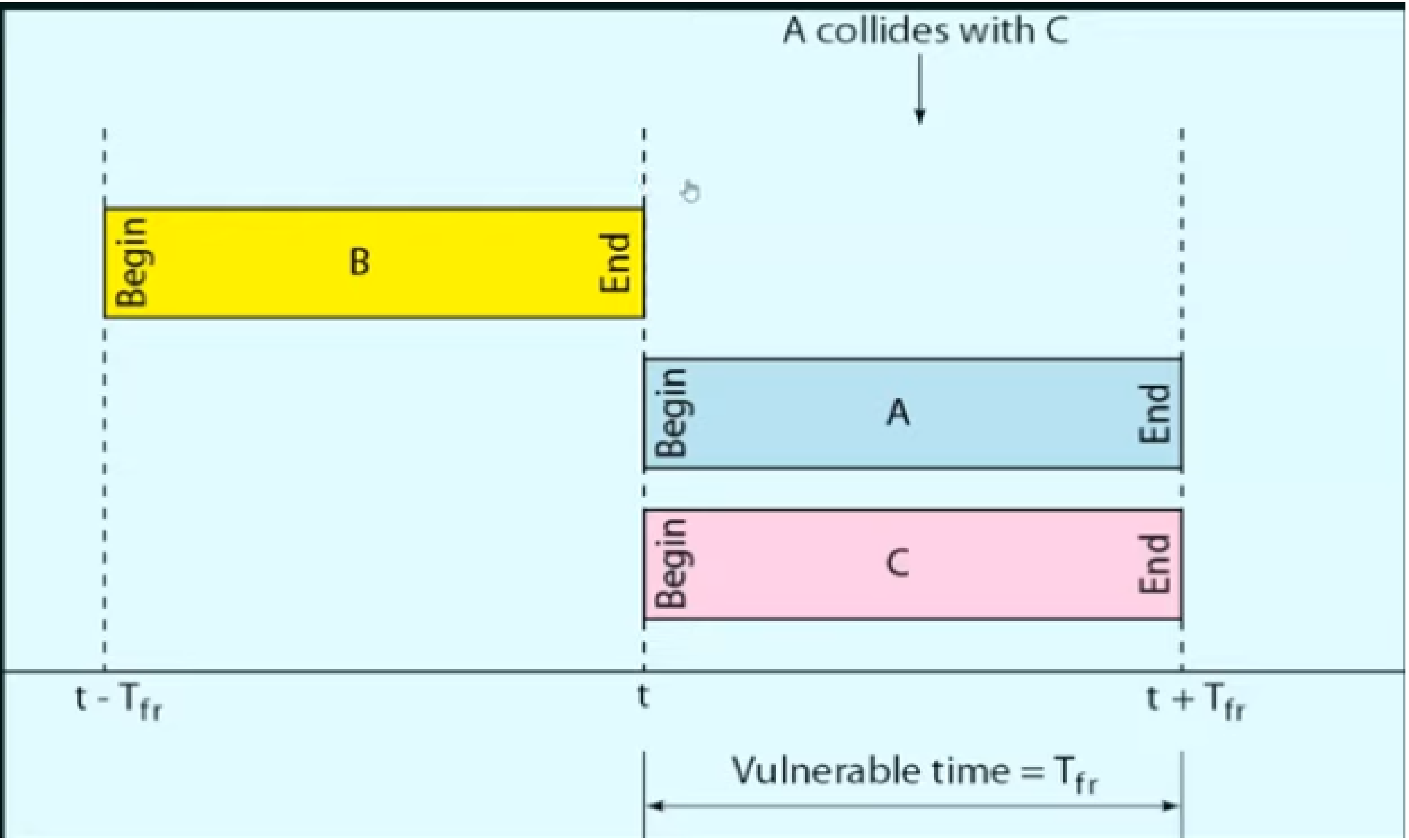
- ★ It was developed just to improve the efficiency of pure aloha as the chances for collision in pure aloha are high.
- ★ The time of the shared channel is divided into discrete time intervals called slots.
- ★ Sending of data is allowed only at the beginning of these slots.
- ★ If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame Transmission Time.

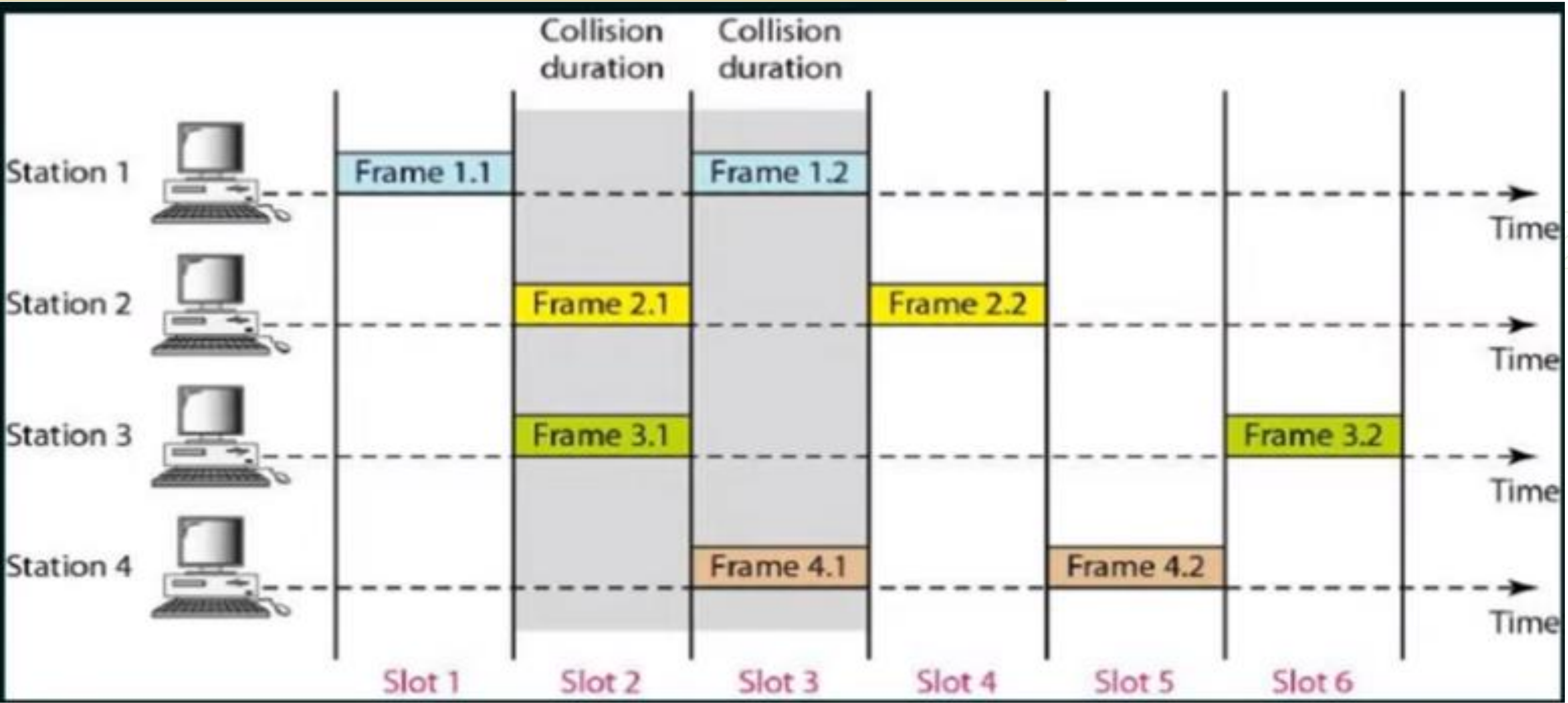
Throughput = $G \times e^{-G}$; Where G is the number of stations wish to transmit in the same time.

Maximum throughput = 0.368 for G=1.

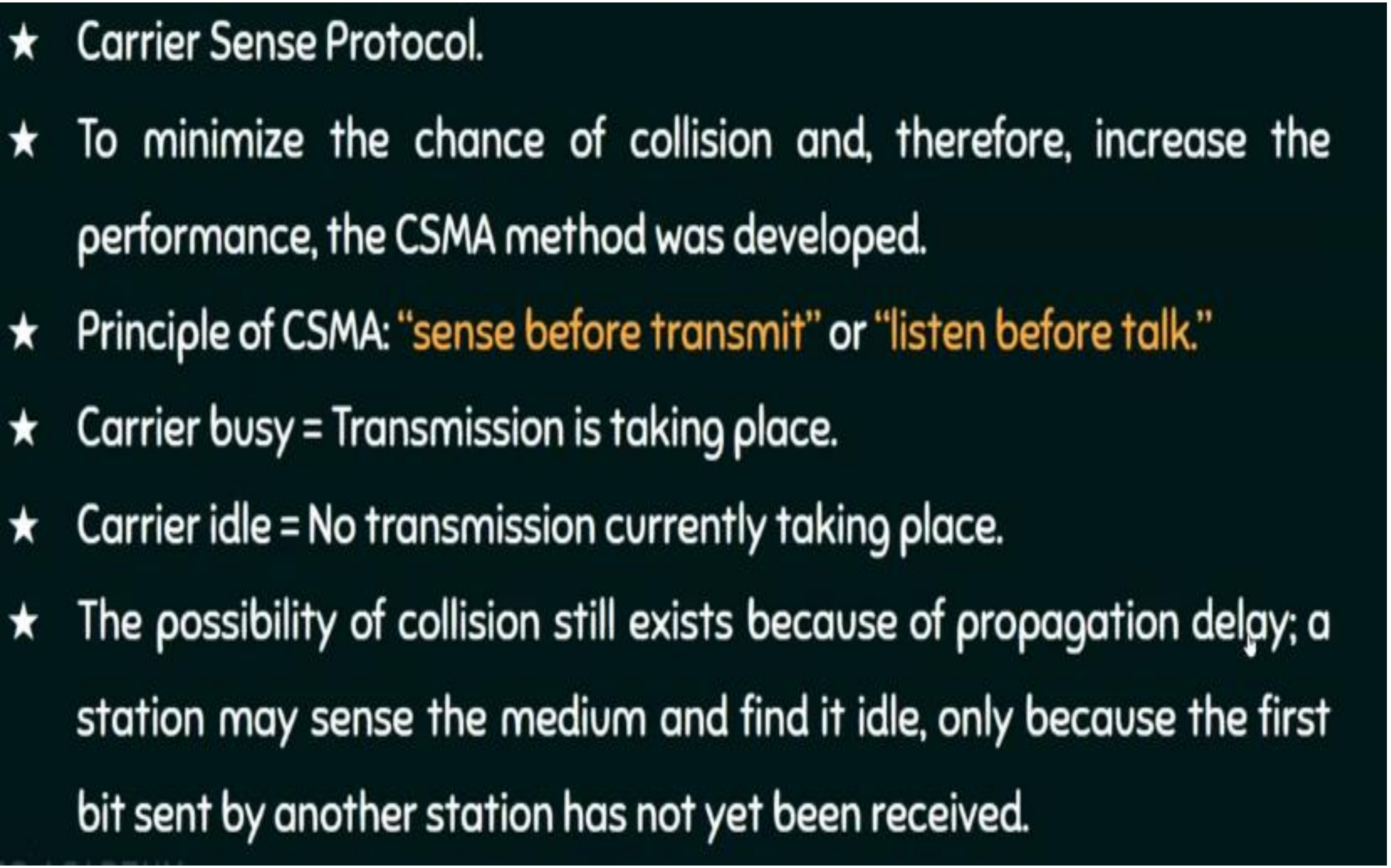
Example- Slotted ALOHA



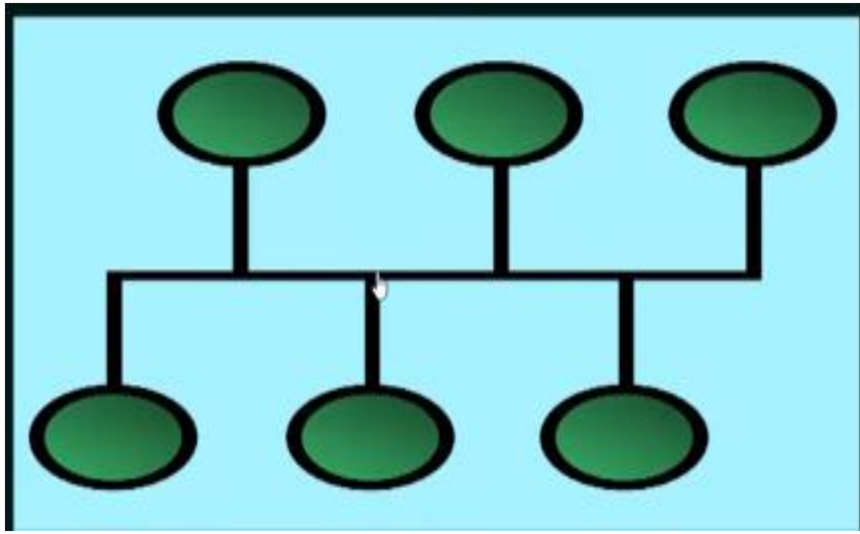
Example- Slotted ALOHA



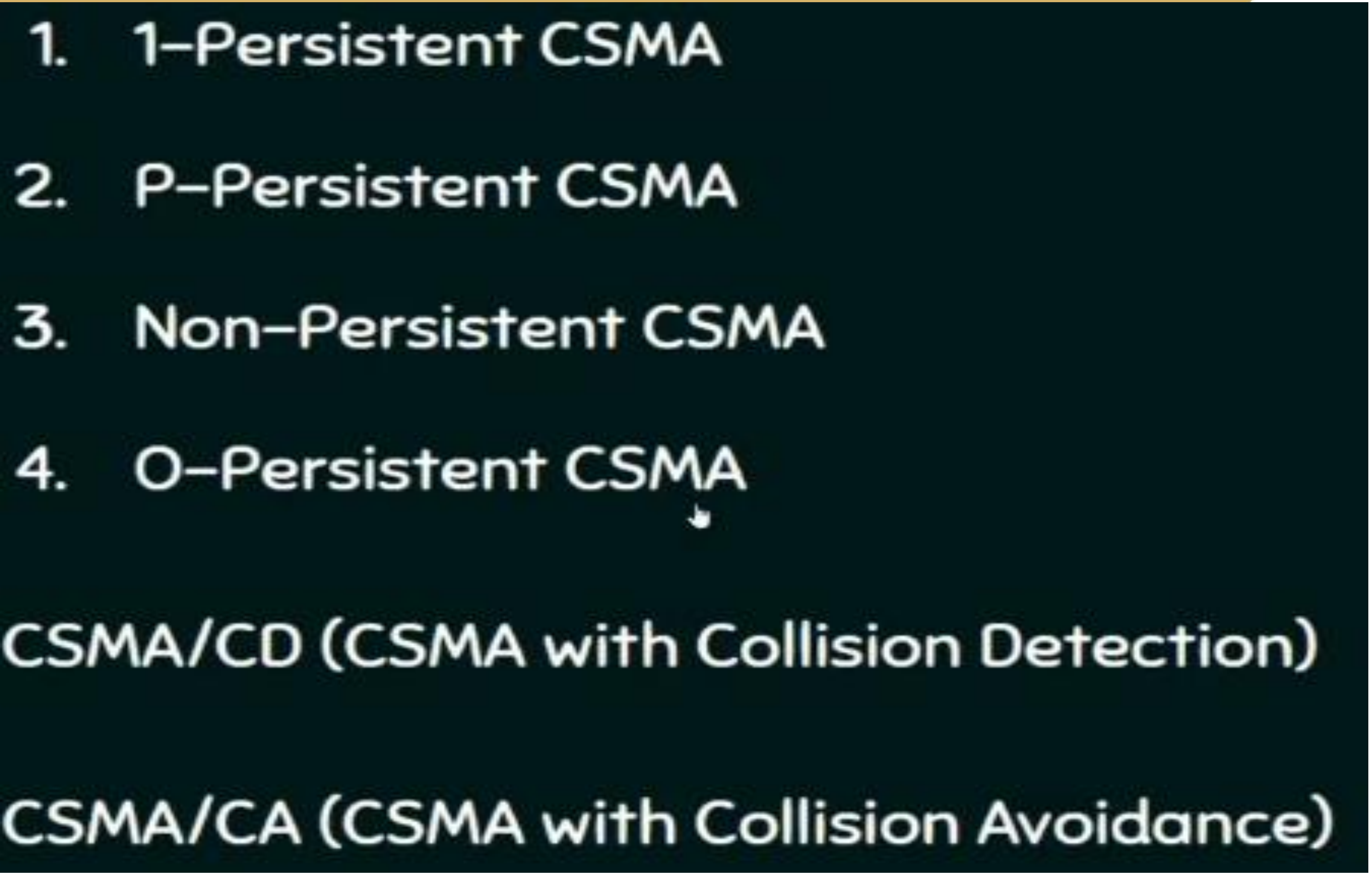
CSMA Protocol



- ★ Carrier Sense Protocol.
- ★ To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
- ★ Principle of CSMA: “sense before transmit” or “listen before talk.”
- ★ Carrier busy = Transmission is taking place.
- ★ Carrier idle = No transmission currently taking place.
- ★ The possibility of collision still exists because of propagation delay; a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.



Types of CSMA Protocol

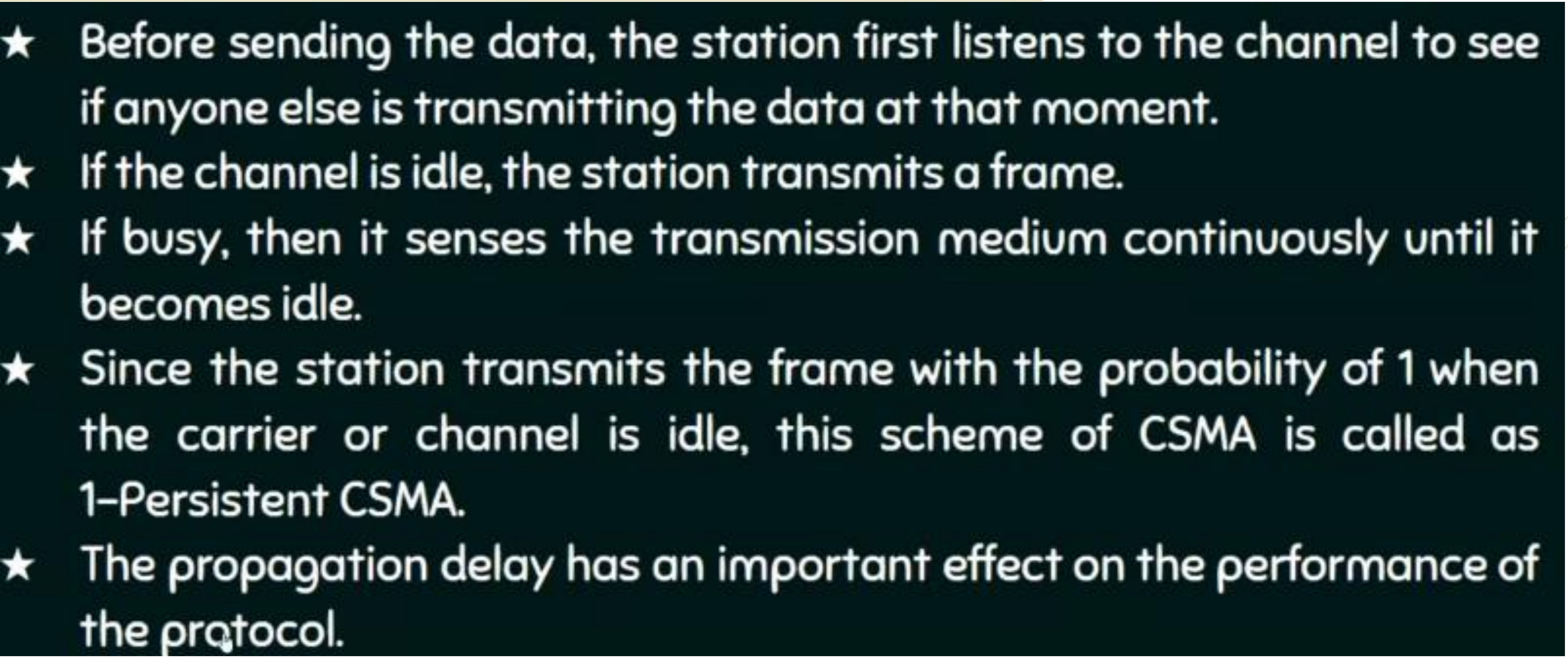


1. 1–Persistent CSMA
2. P–Persistent CSMA
3. Non–Persistent CSMA
4. O–Persistent CSMA

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.

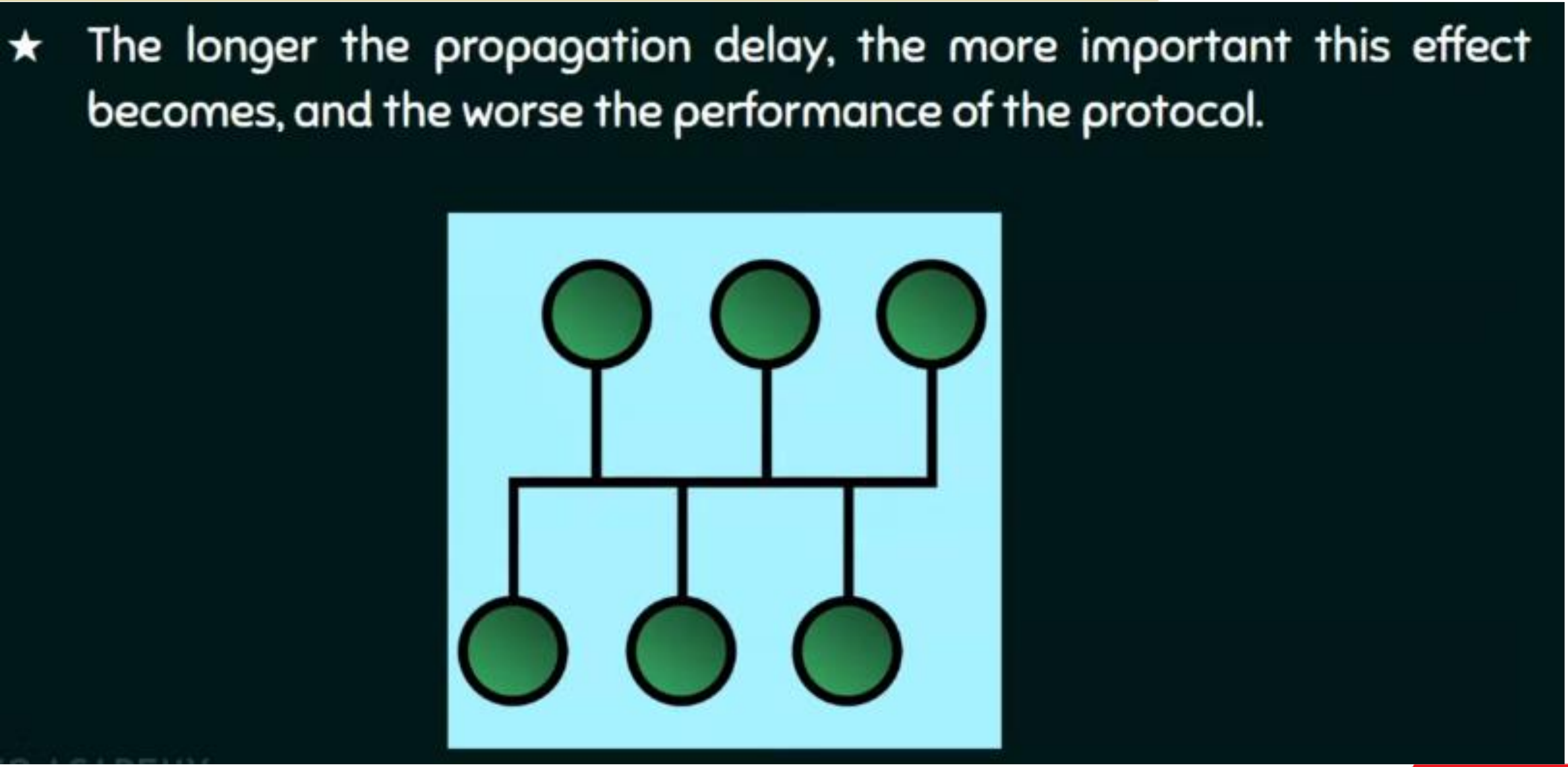
★ If the channel is idle, the station transmits a frame.

★ 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.

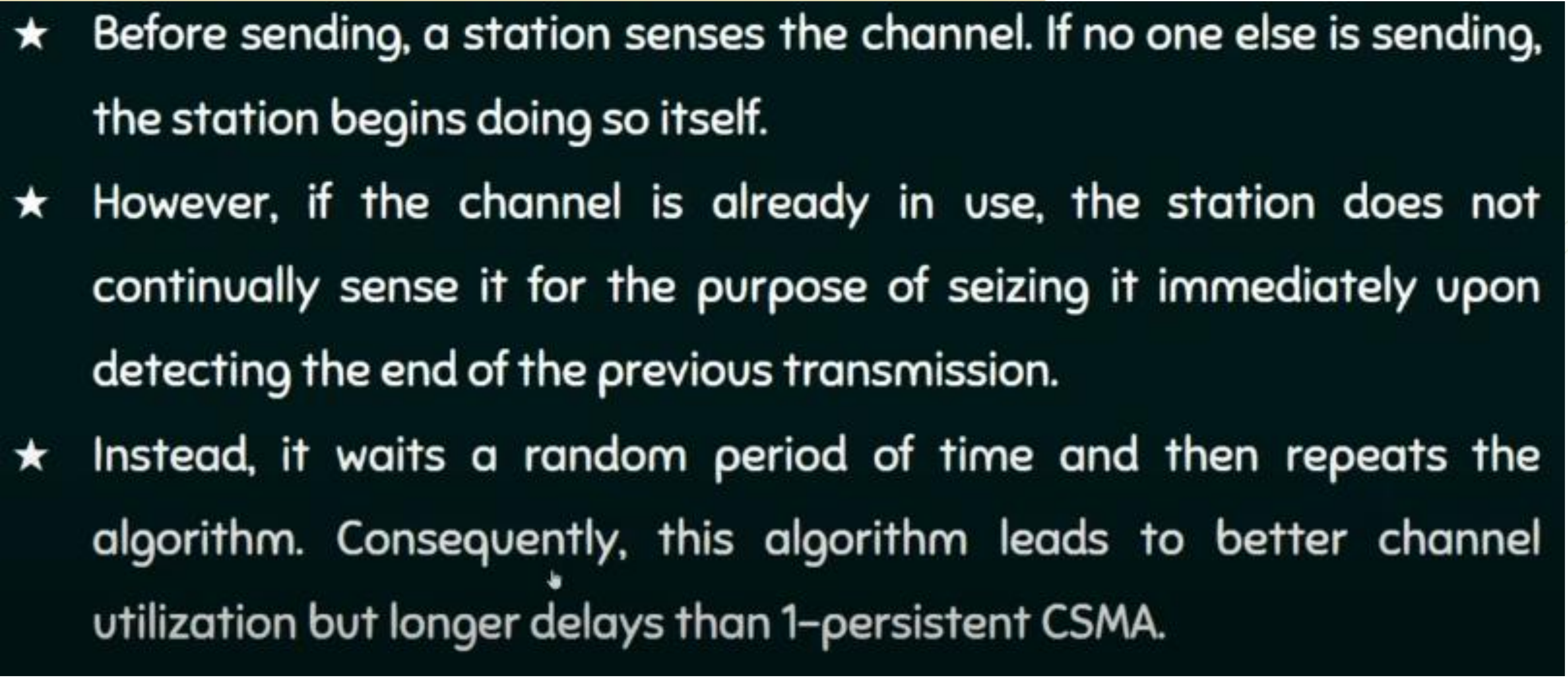
★ The propagation delay has an important effect on the performance of the protocol.

1 Persistent CSMA



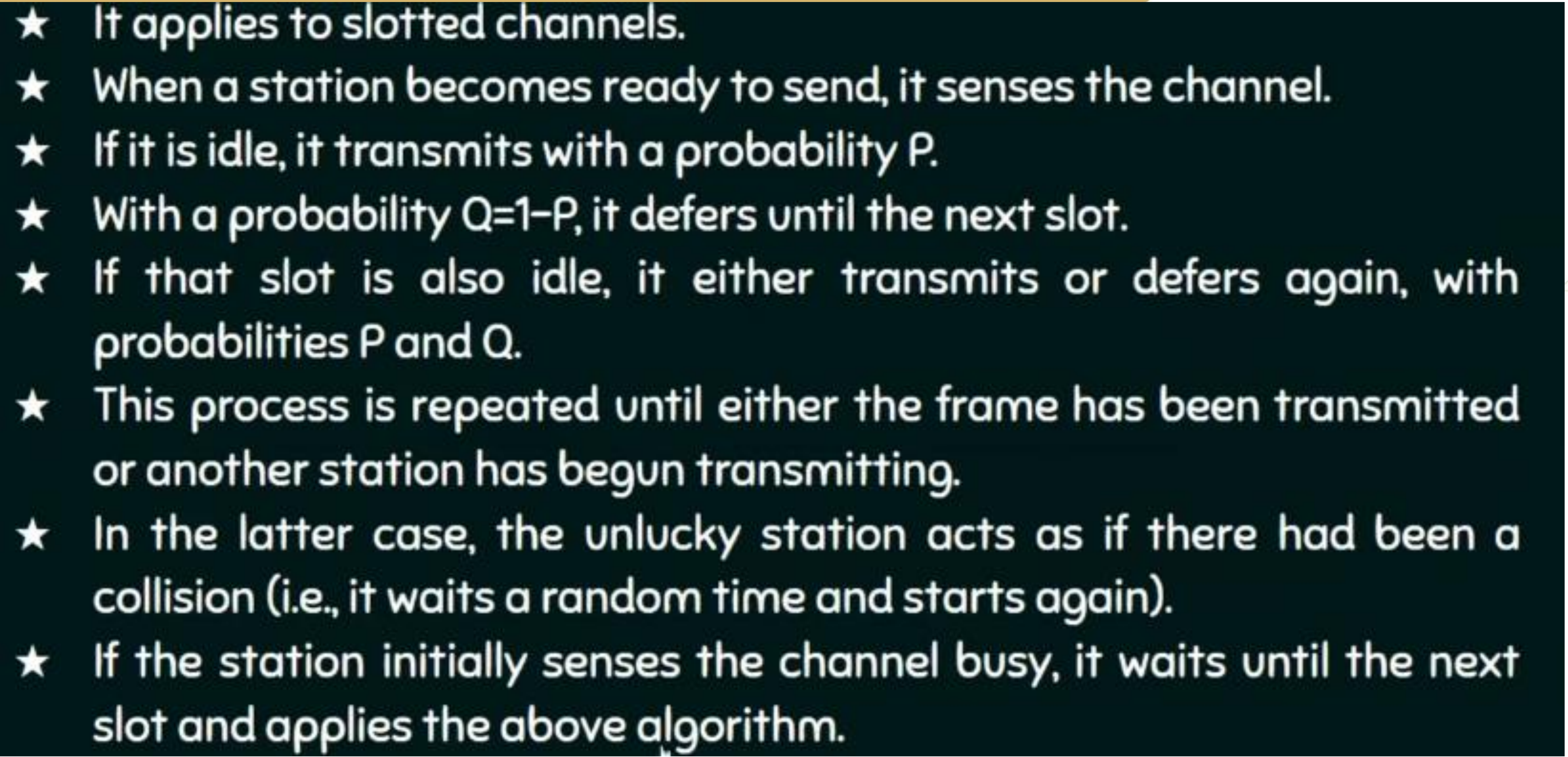
★ The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.

Non- Persistent CSMA



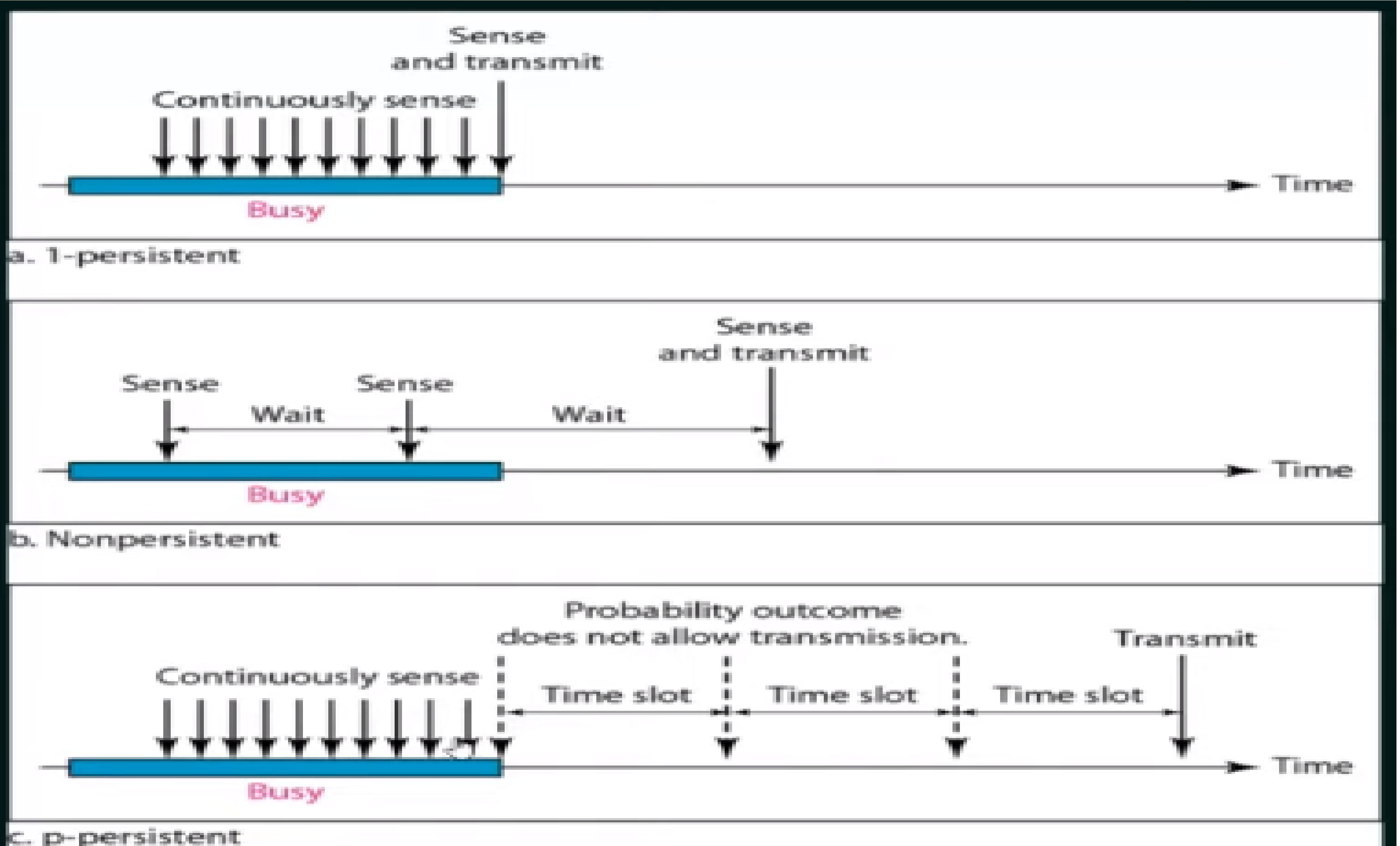
- Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself.
- However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- Instead,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

P- Persistent CSMA

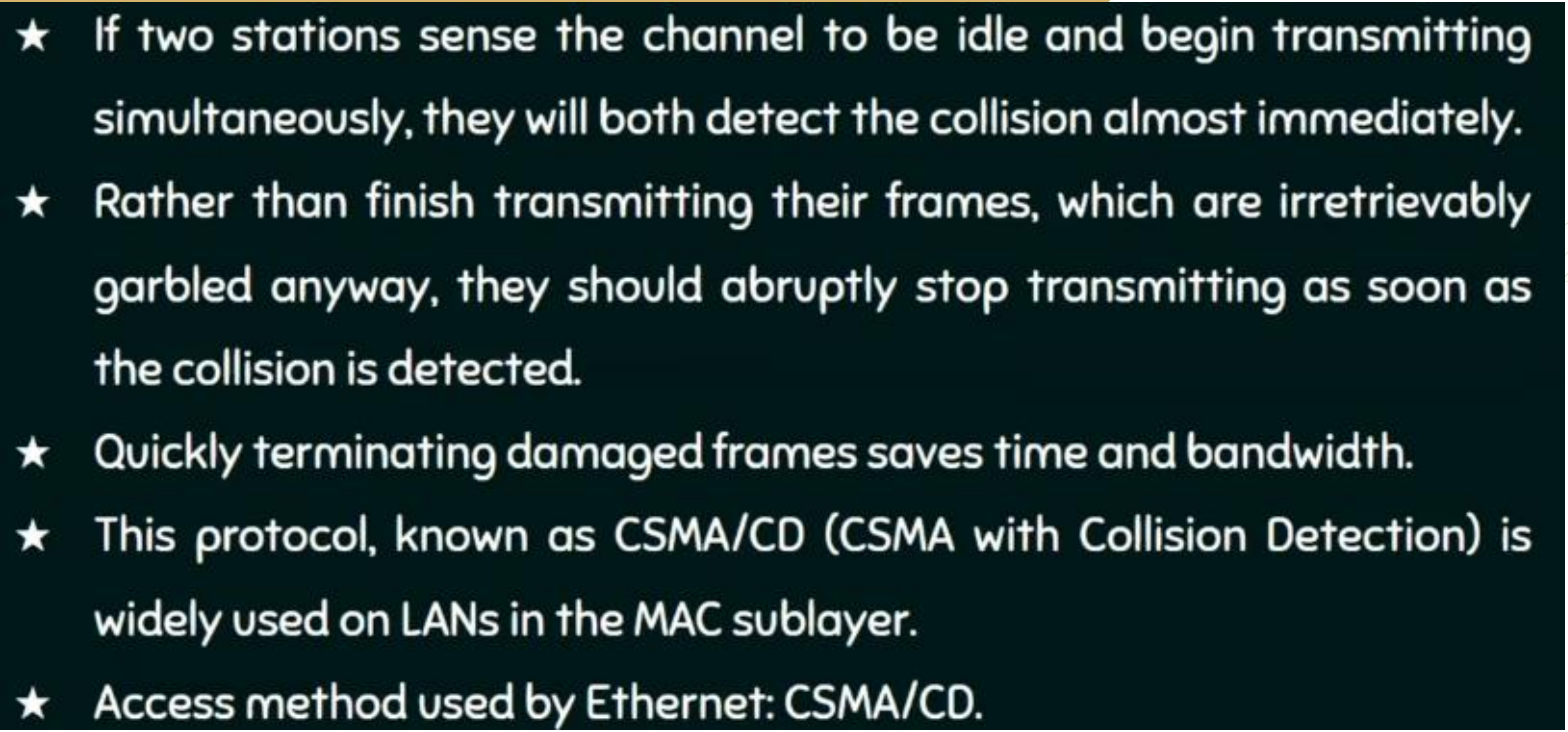


- ★ It applies to slotted channels.
- ★ When a station becomes ready to send, it senses the channel.
- ★ If it is idle, it transmits with a probability P.
- ★ With a probability Q=1–P, it defers until the next slot.
- ★ If that slot is also idle, it either transmits or defers again, with probabilities 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.

Behaviour of Three Presistent Methods

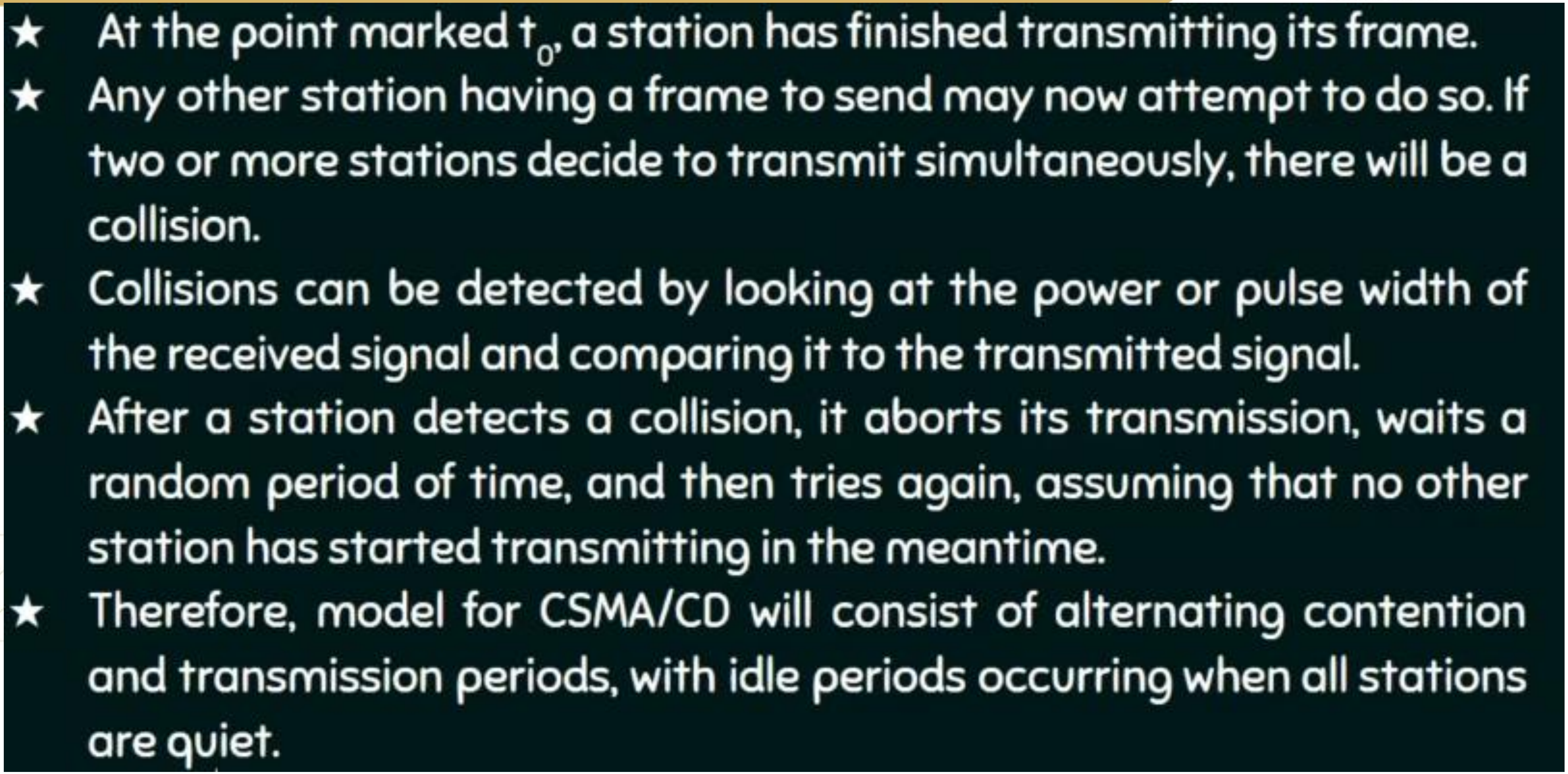


CSMA/CD



- ★ 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.

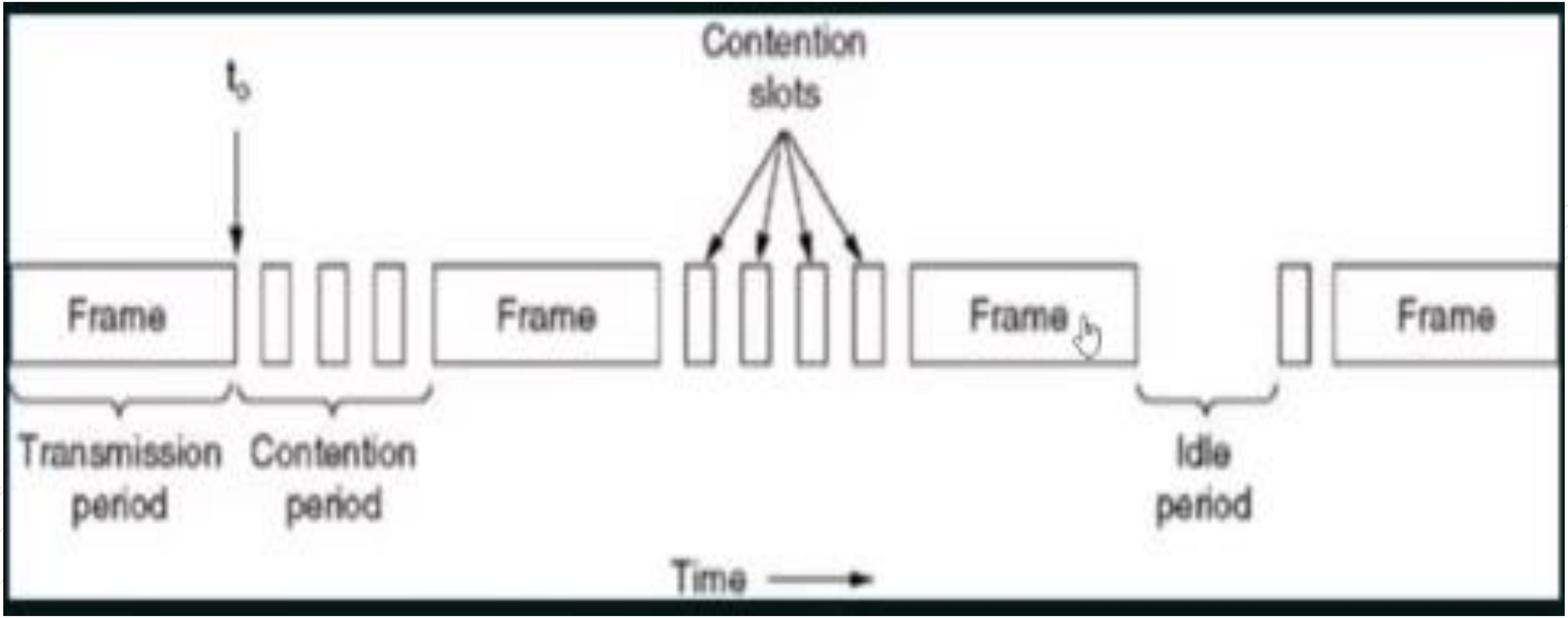
★ Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision.

★ Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

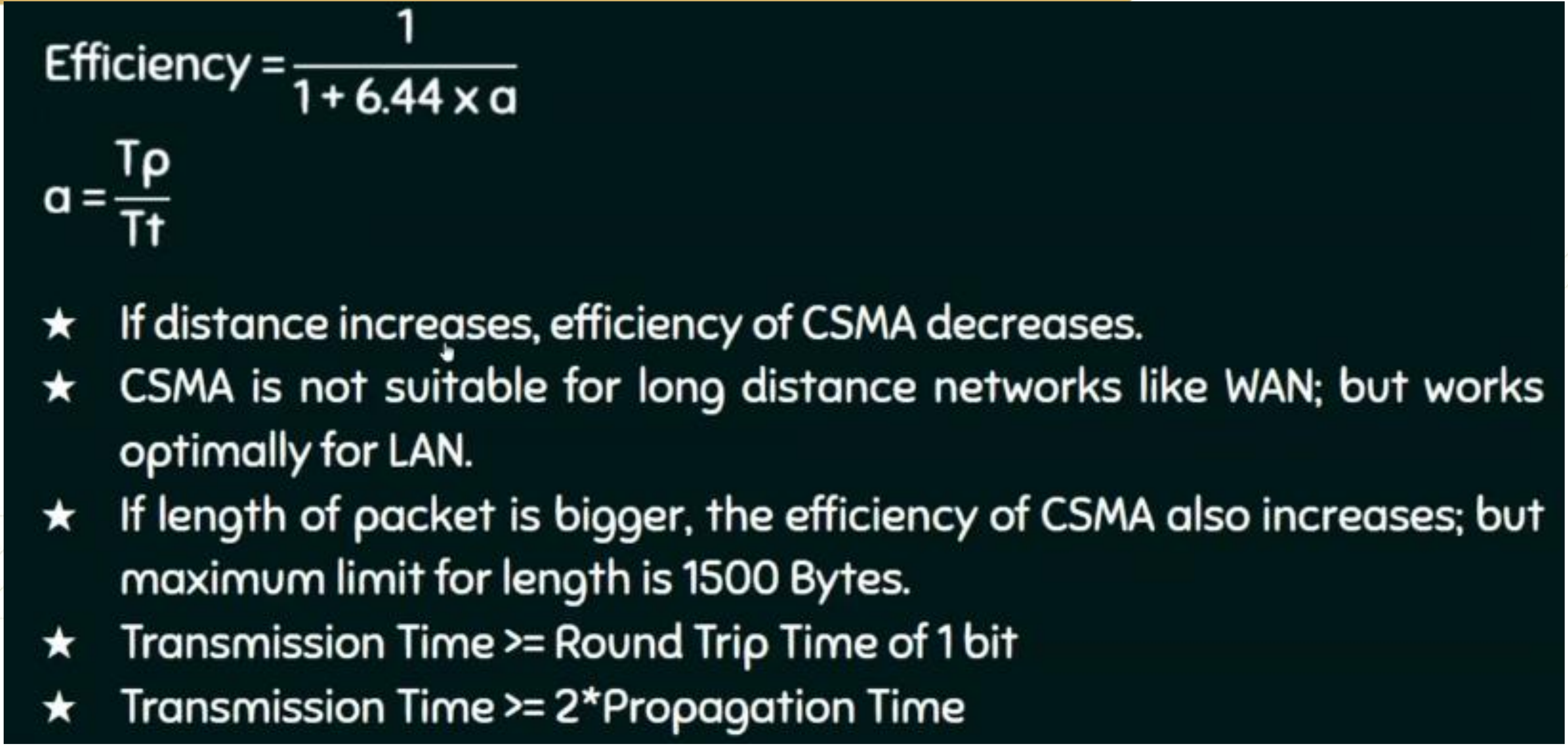
★ After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.

★ Therefore, model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

Example- CSMA/CD



Example- CSMA/CD



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

$$a = \frac{Tp}{Tt}$$

★ If distance increases, efficiency of CSMA decreases.

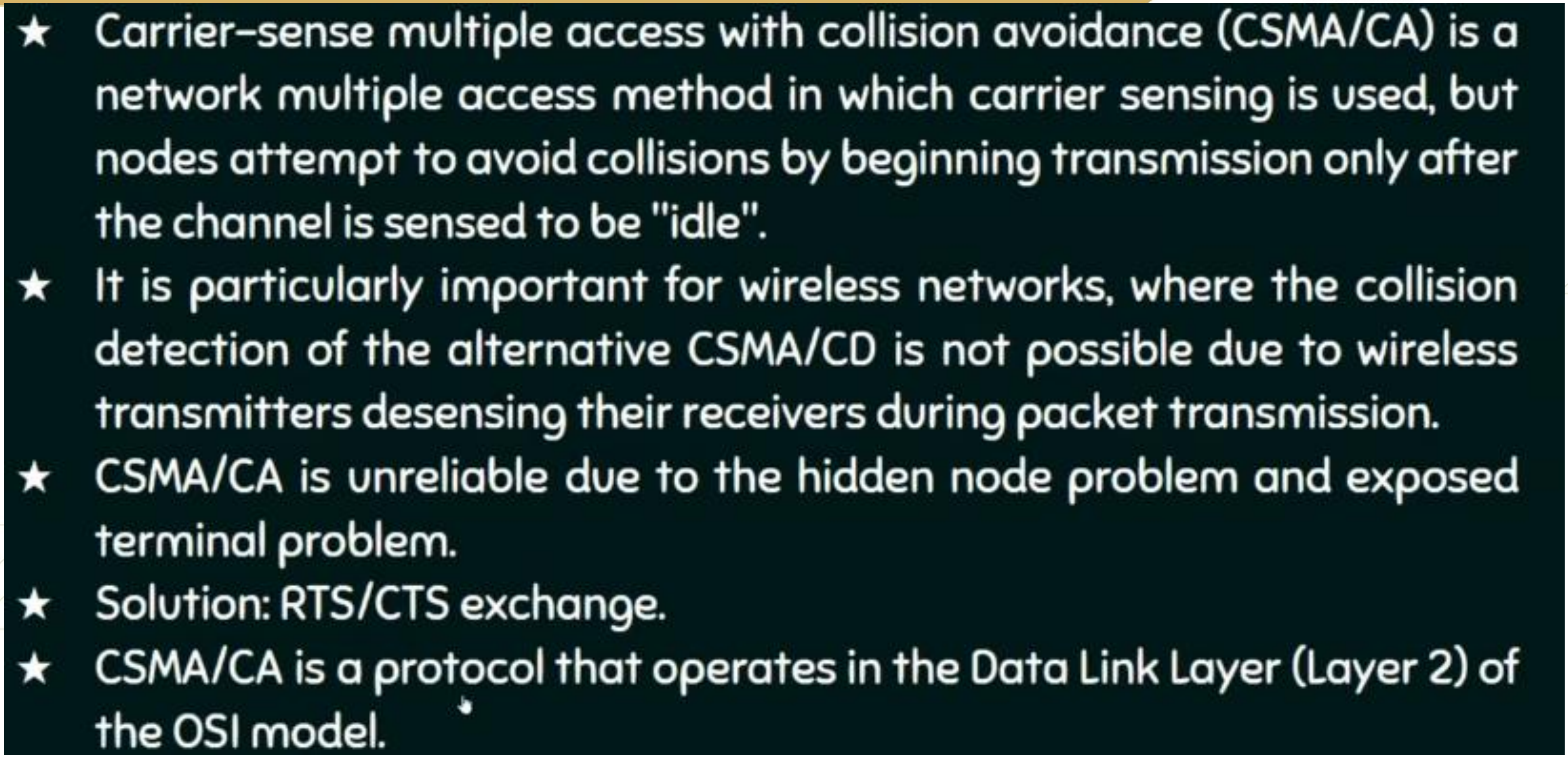
★ CSMA is not suitable for long distance networks like WAN; but works optimally for LAN.

★ 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

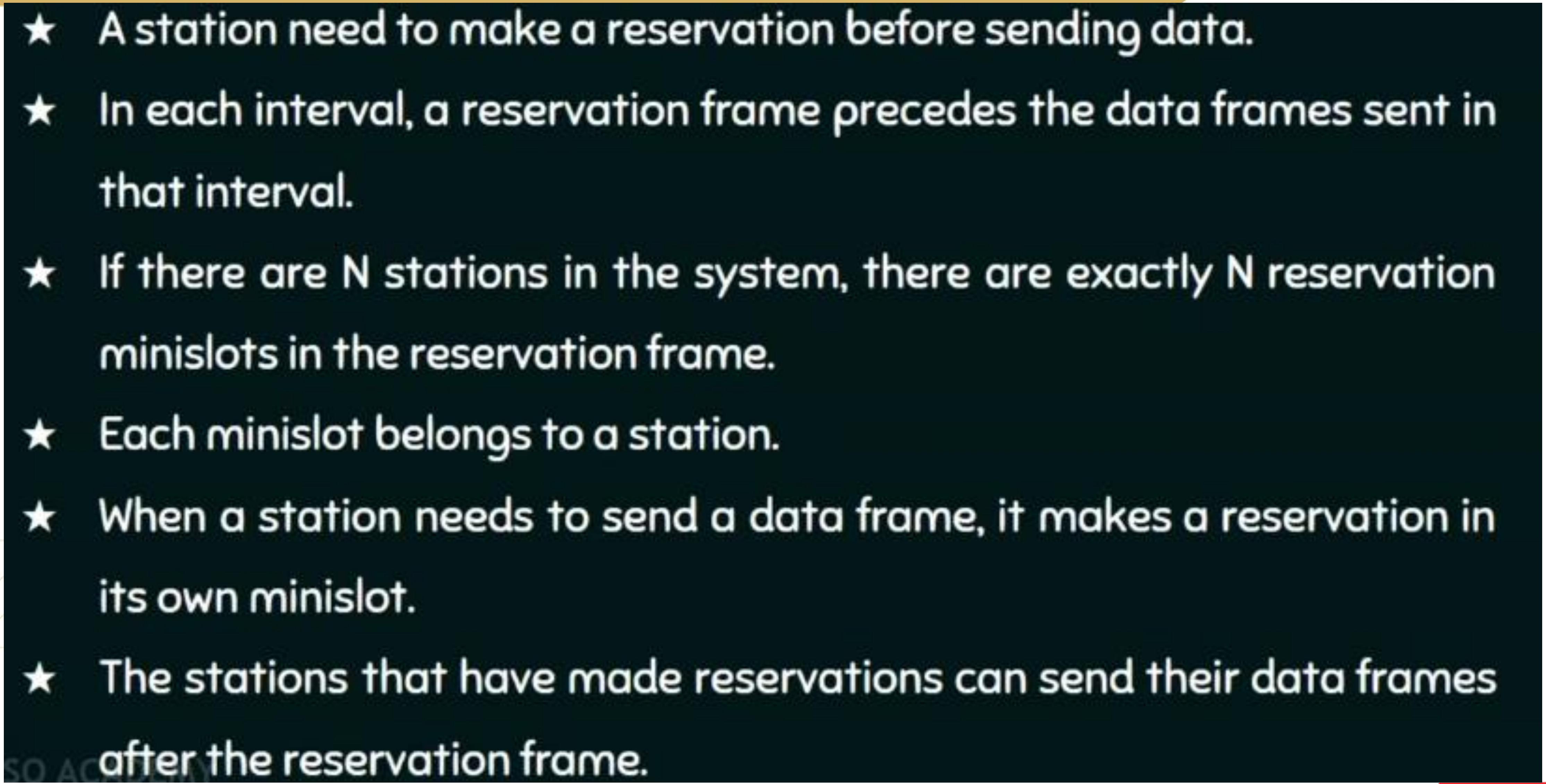
★ Transmission Time >= 2*Propagation Time

CSMA/CA



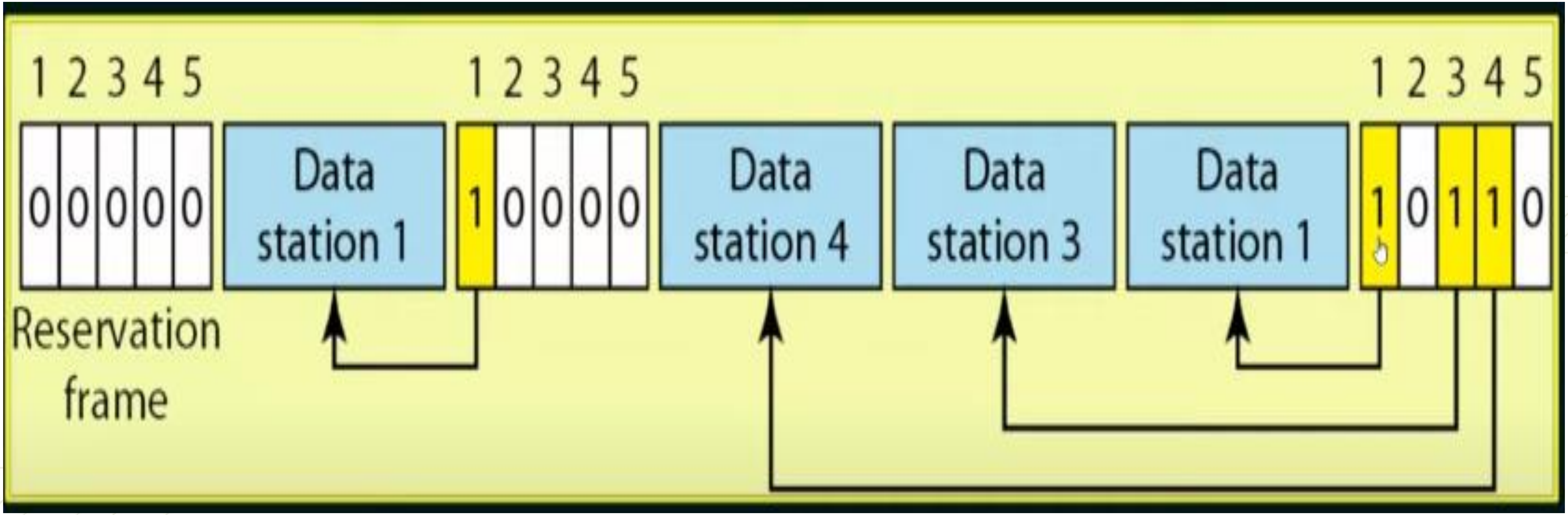
- ★ Carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".
- ★ It is particularly important for wireless networks, 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.

Controlled Access Protocol - Reservation

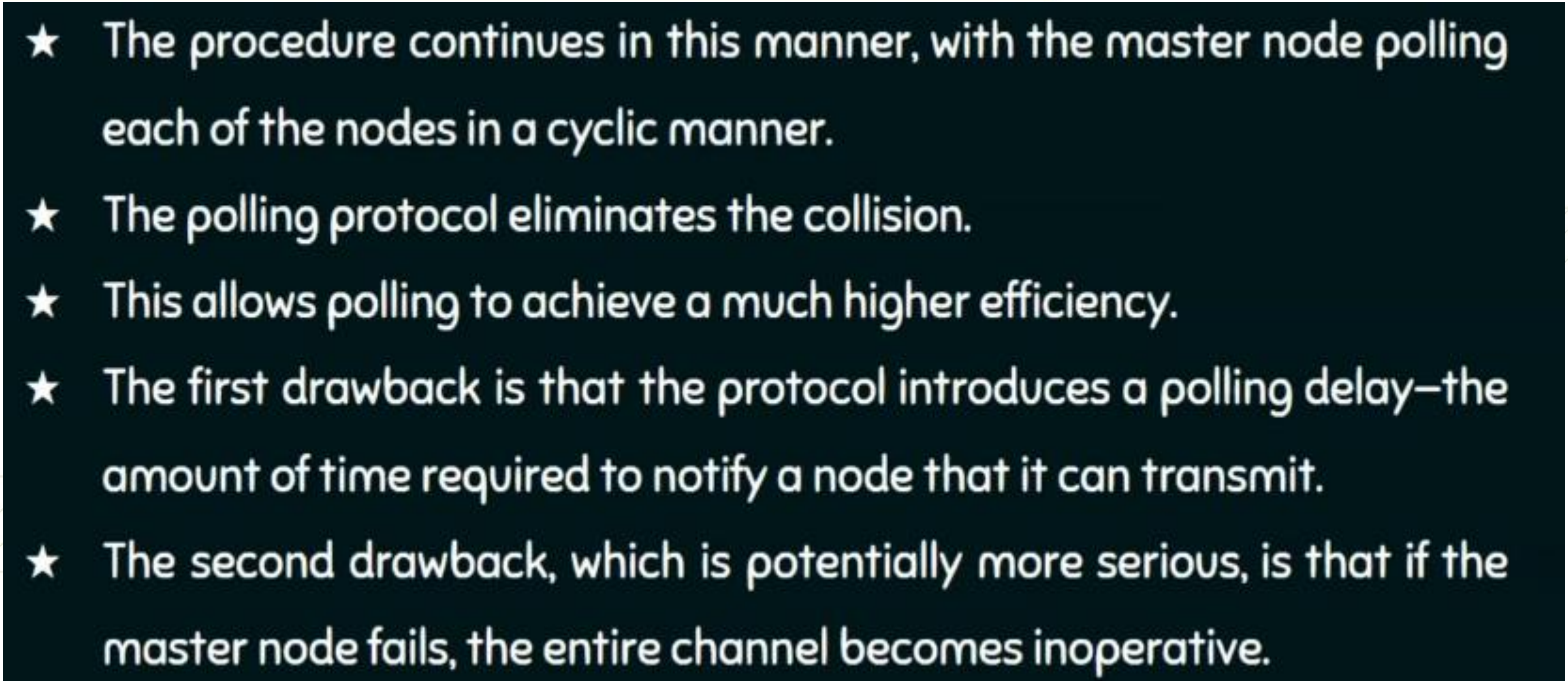


- ★ A station need to make a reservation before sending data.
- ★ In each interval, a reservation frame precedes the data frames sent in that interval.
- ★ If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.
- ★ Each minislot belongs to a station.
- ★ 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.

Controlled Access Protocol - Reservation

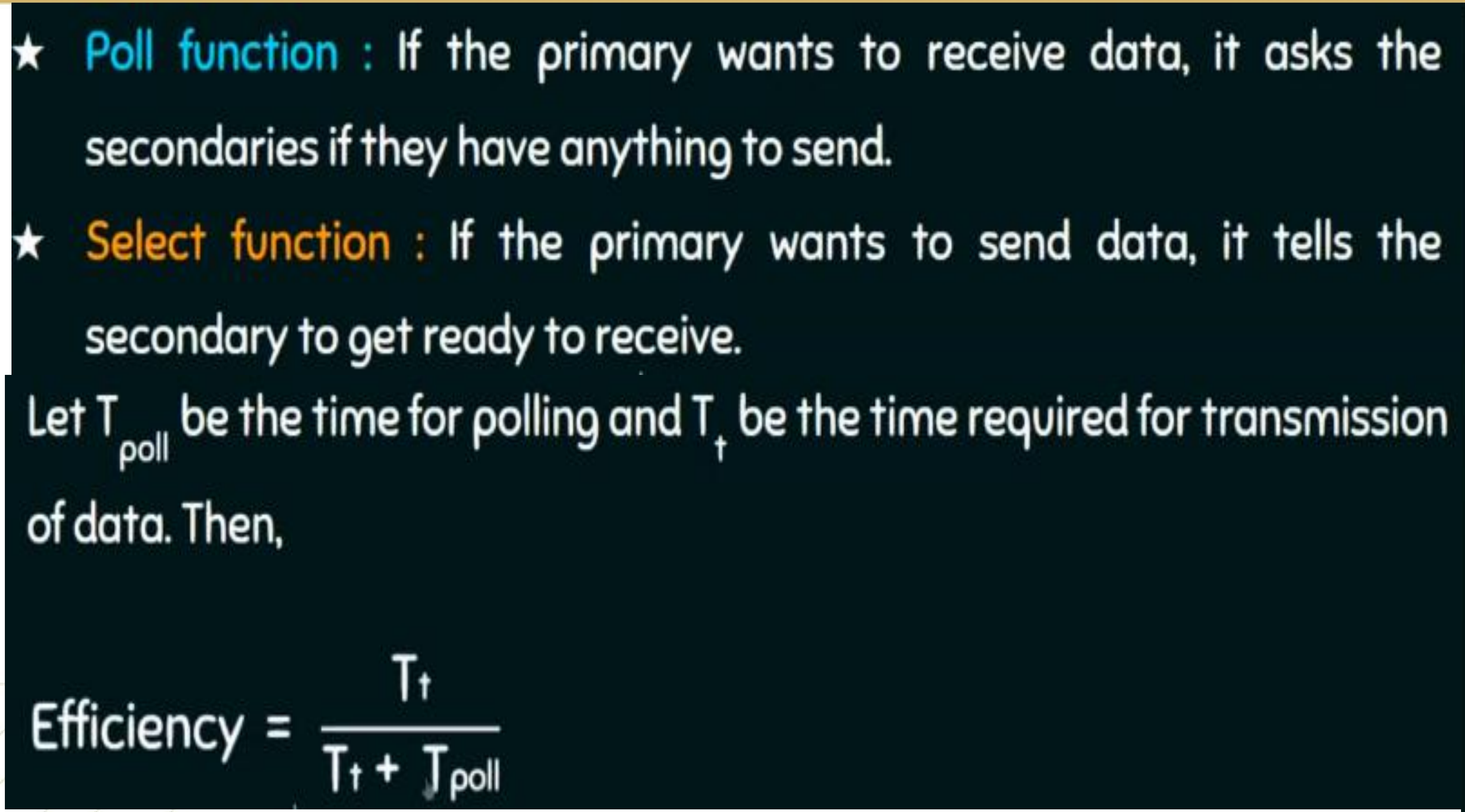


Controlled Access Protocol - Polling



- ★ 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.

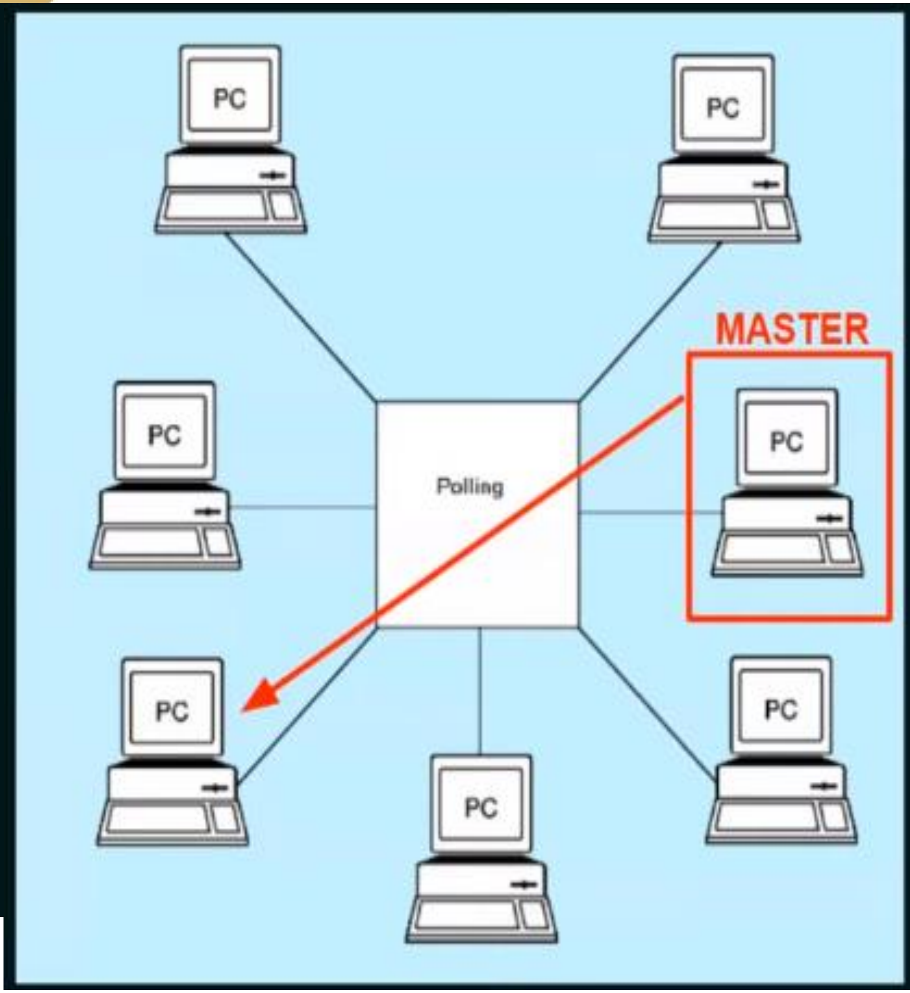
Polling Function and Efficiency



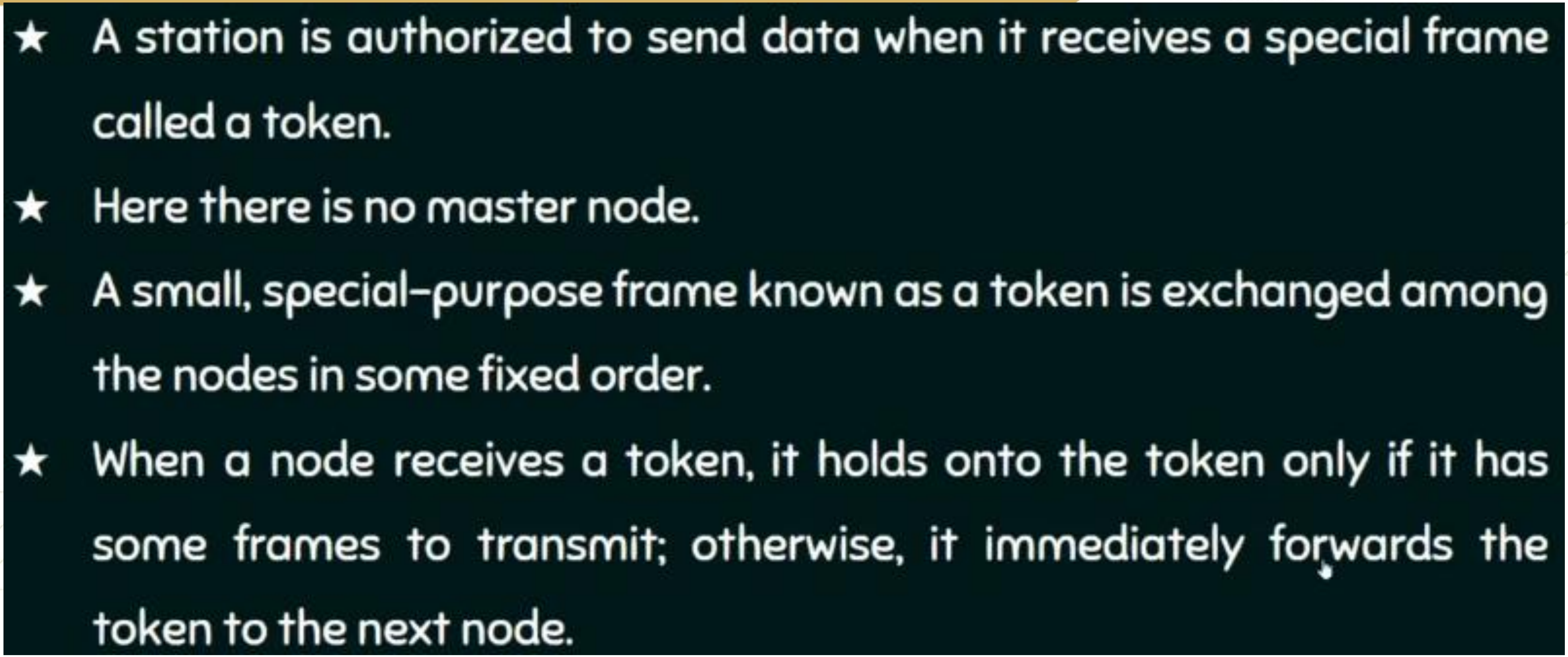
- ★ Poll function : If the primary wants to receive data, it asks the secondaries if they have anything to send.
- ★ Select function : If the primary wants to send data, it tells the secondary to get ready to receive.

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

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



Controlled Access Protocol- Token Passing



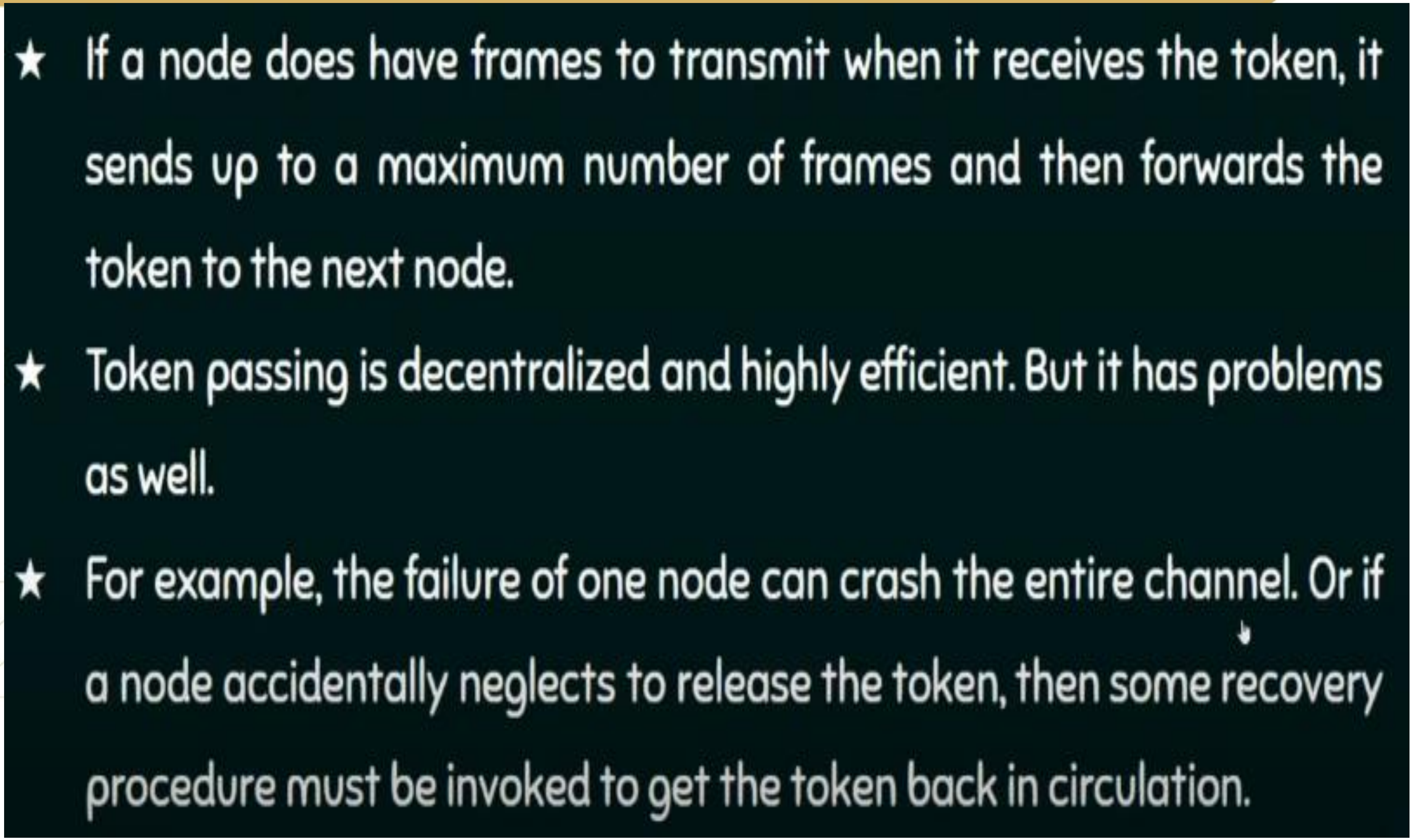
★ A station is authorized to send data when it receives a special frame called a token.

★ Here there is no master node.

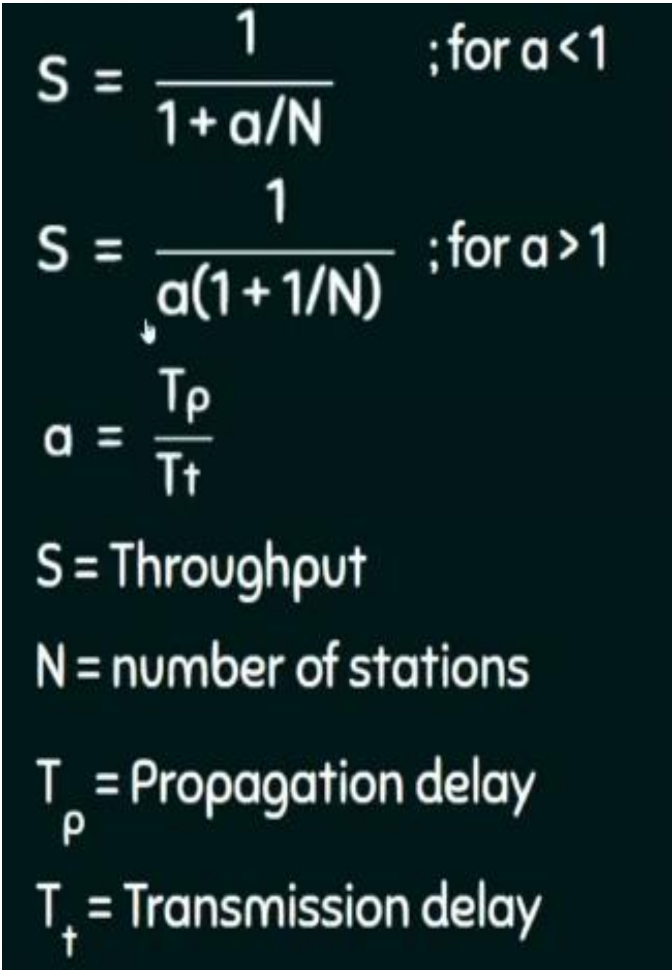
★ A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.

★ 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.

Performance and Efficiency of 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.



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

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

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

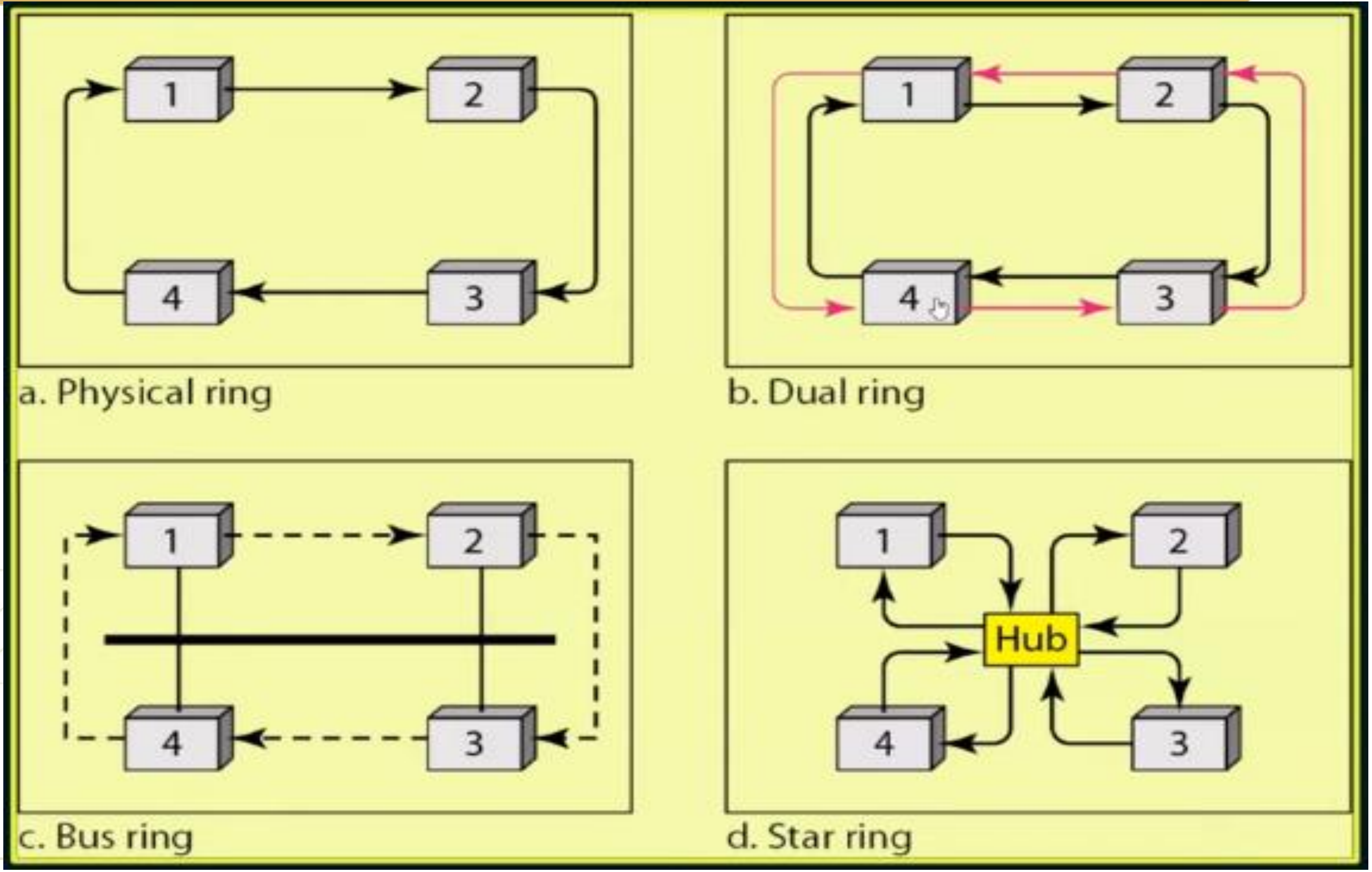
S = Throughput

N = number of stations

T_p = Propagation delay

T_t = Transmission delay

Example- Token Passing



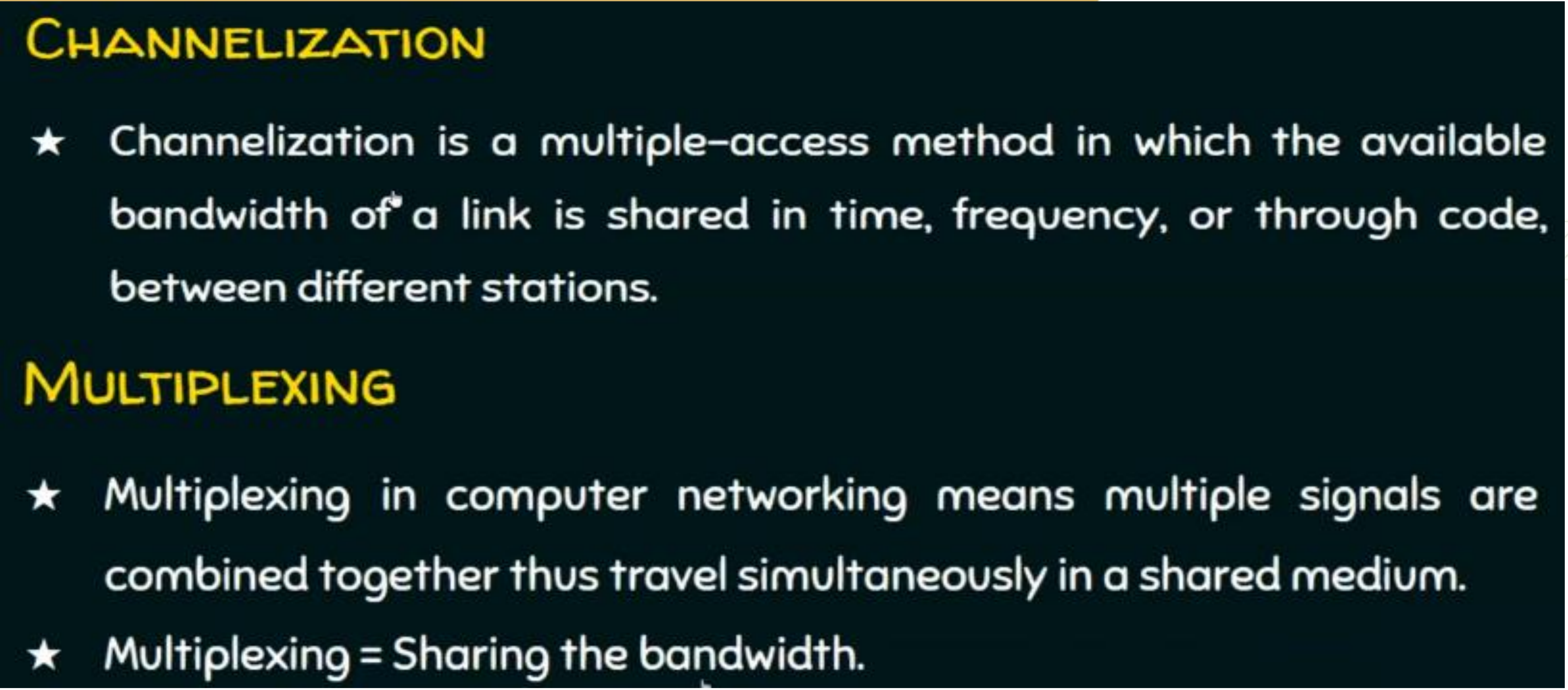
a. Physical ring

b. Dual ring

c. Bus ring

d. Star ring

Channelization Protocols



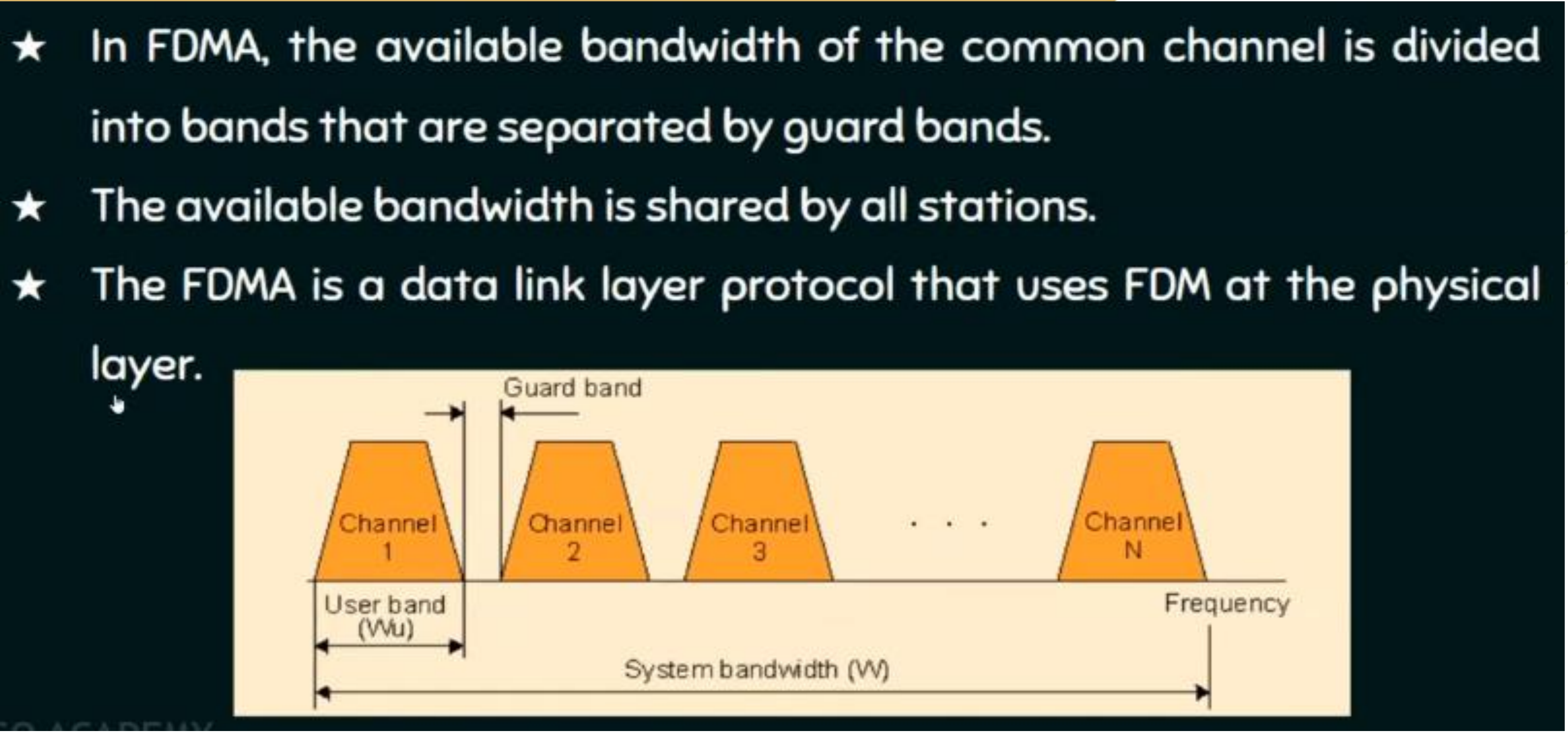
Channelization

- ★ 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.

Multiplexing

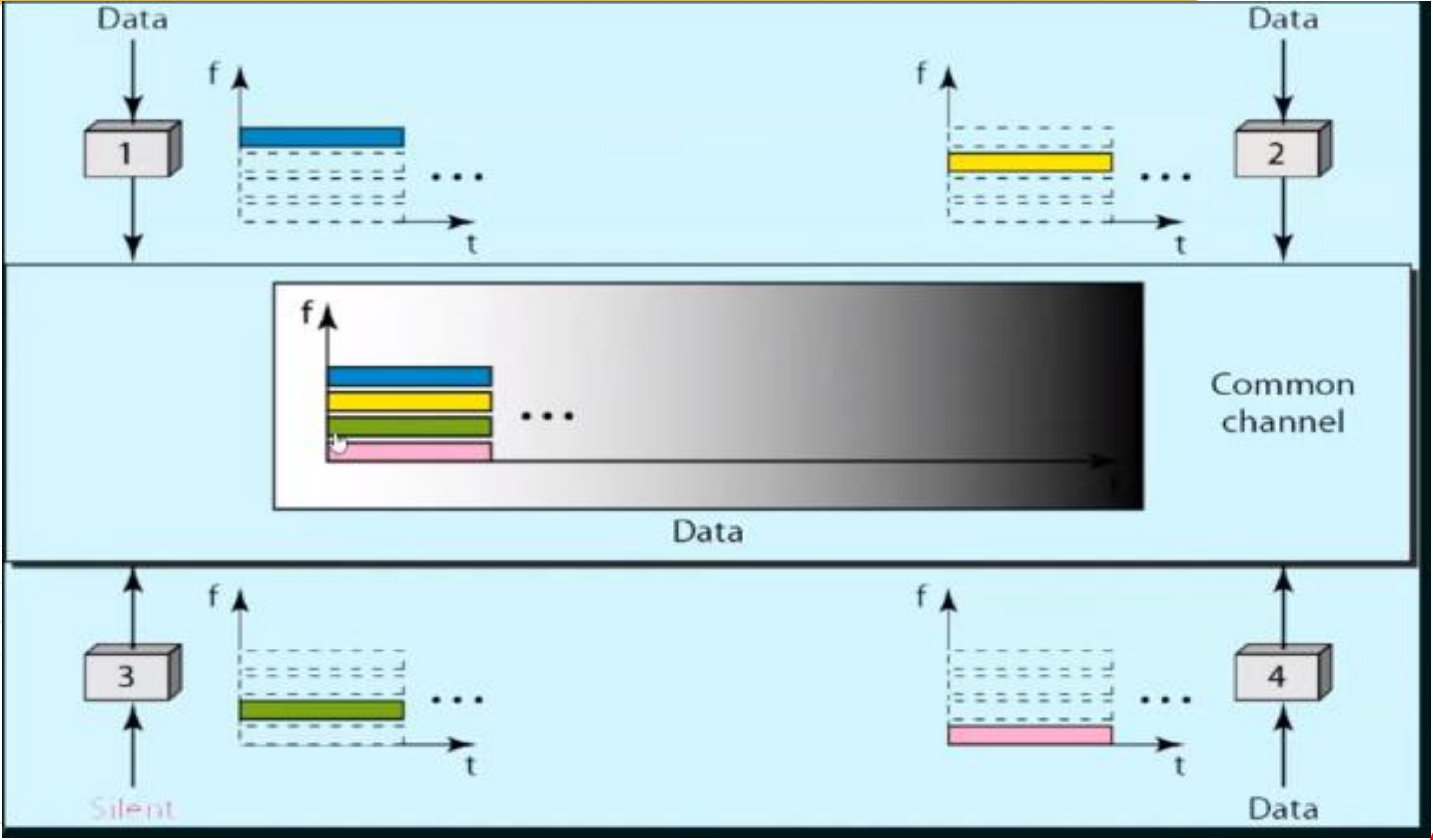
- ★ Multiplexing in computer networking means multiple signals are combined together thus travel simultaneously in a shared medium.
- ★ Multiplexing = Sharing the bandwidth.

Frequency Divison Multiple Access- FDMA

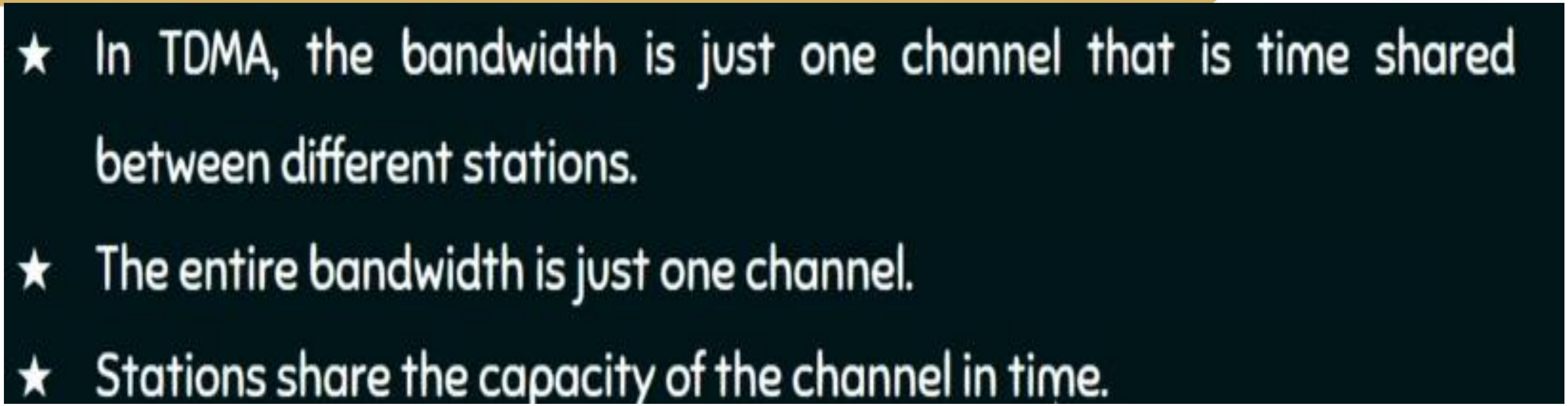


- ★ In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.
- ★ The available bandwidth is shared by all stations.
- ★ The FDMA is a data link layer protocol that uses FDM at the physical layer.

Example- FDMA



Time Divison Multiple Access-TDMA

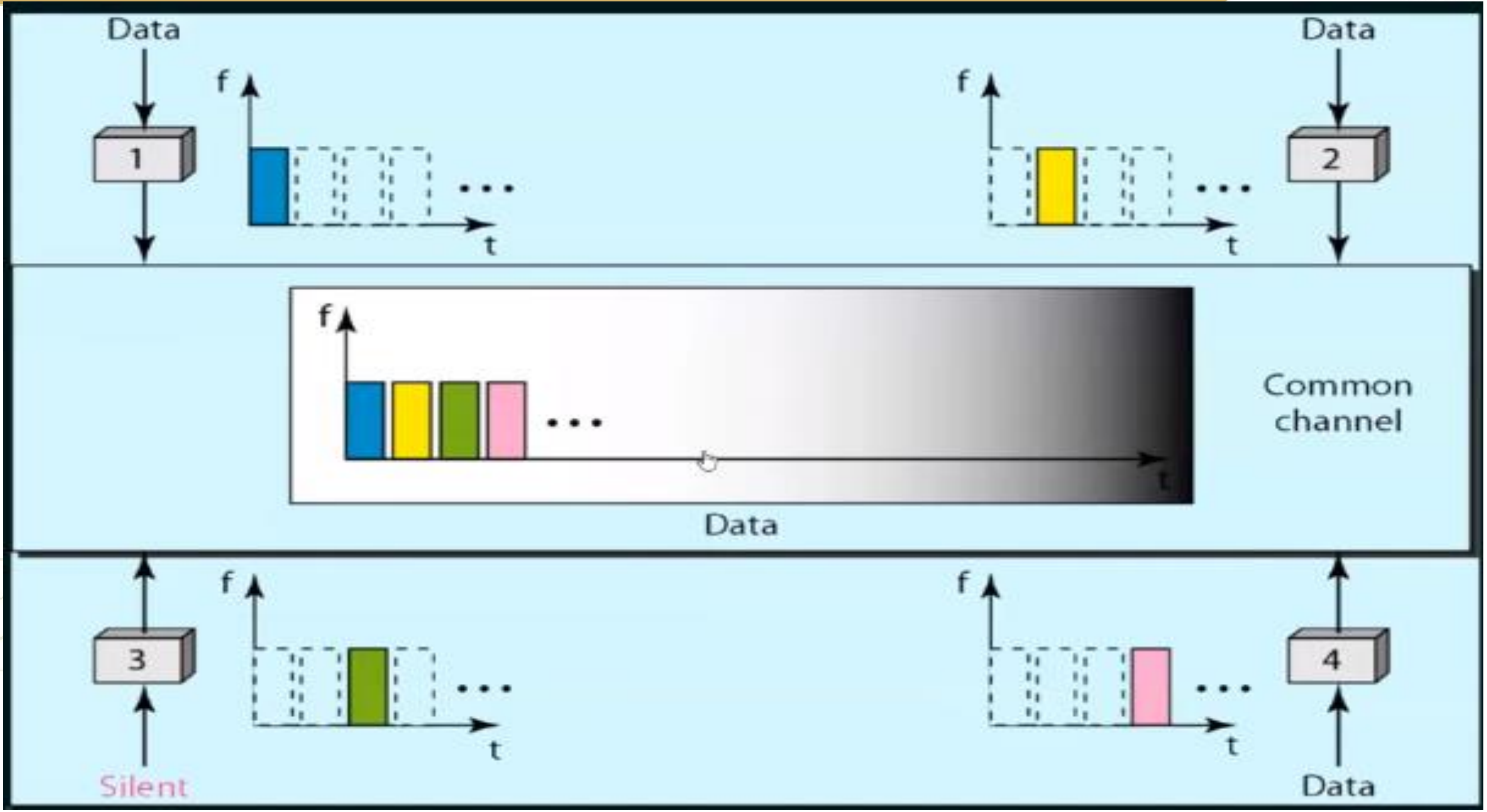


★ In TDMA, the bandwidth is just one channel that is time shared between different stations.

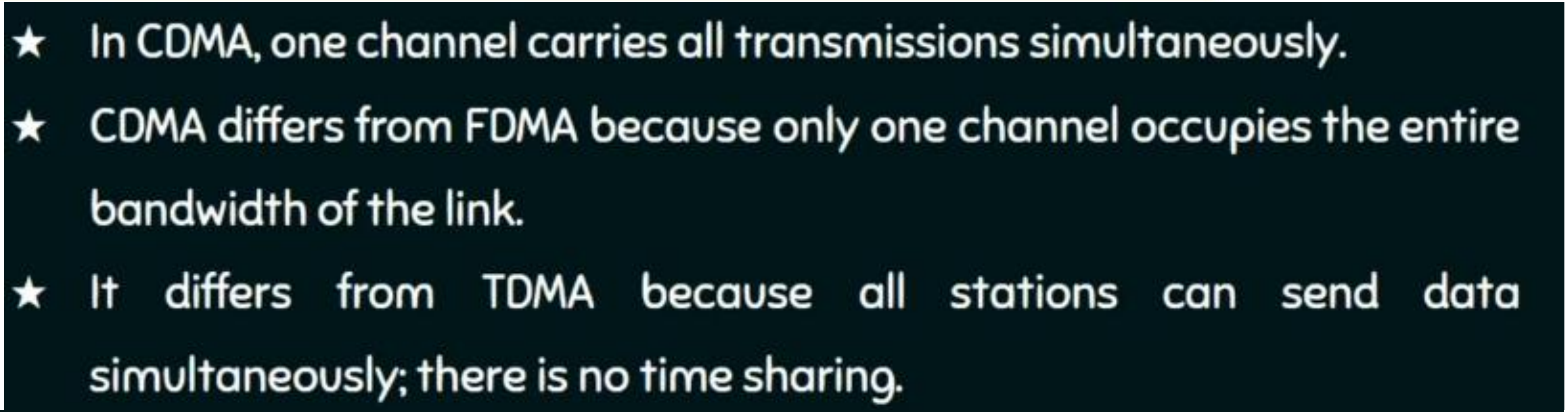
★ The entire bandwidth is just one channel.

★ Stations share the capacity of the channel in time.

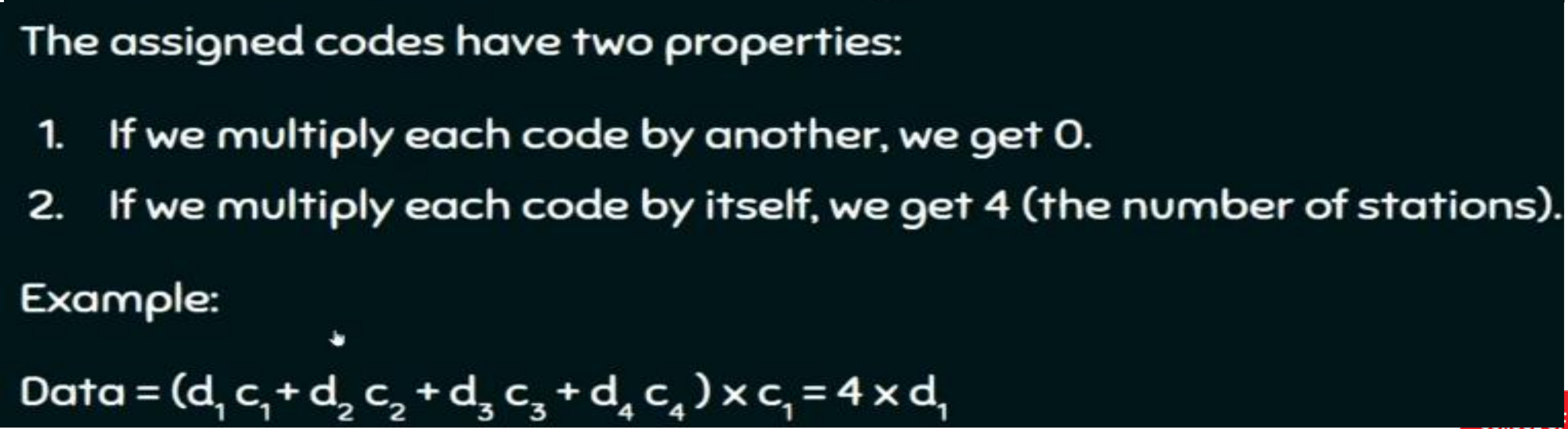
Example- TDMA



Code Divison Multiple Access-CDMA



- ★ In CDMA, one channel carries all transmissions simultaneously.
- ★ CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.
- ★ It differs from TDMA because all stations can send data simultaneously; there is no time sharing.



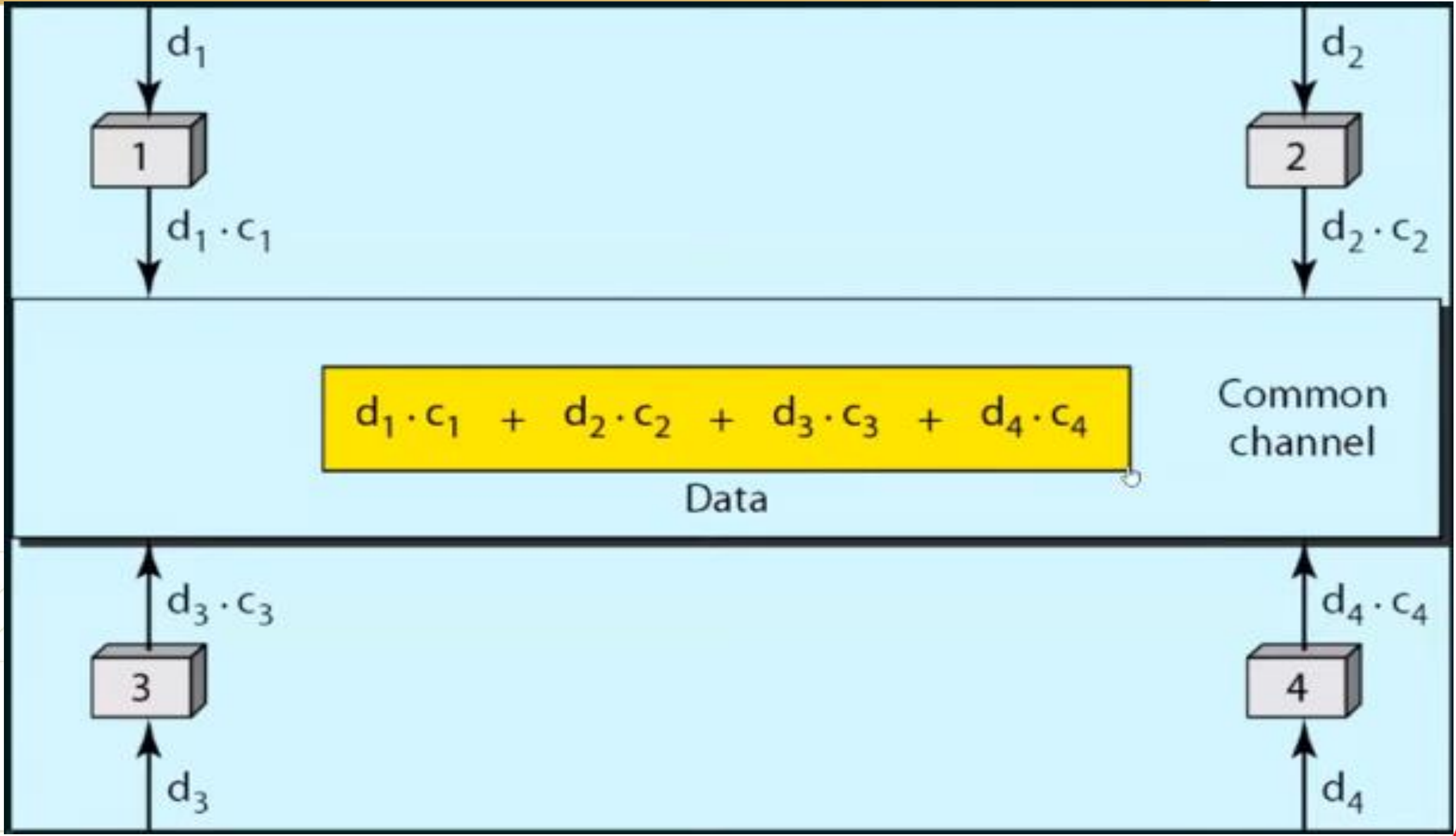
The assigned codes have two properties:

1. If we multiply each code by another, we get 0.
2. If we multiply each code by itself, we get 4 (the number of stations).

Example:

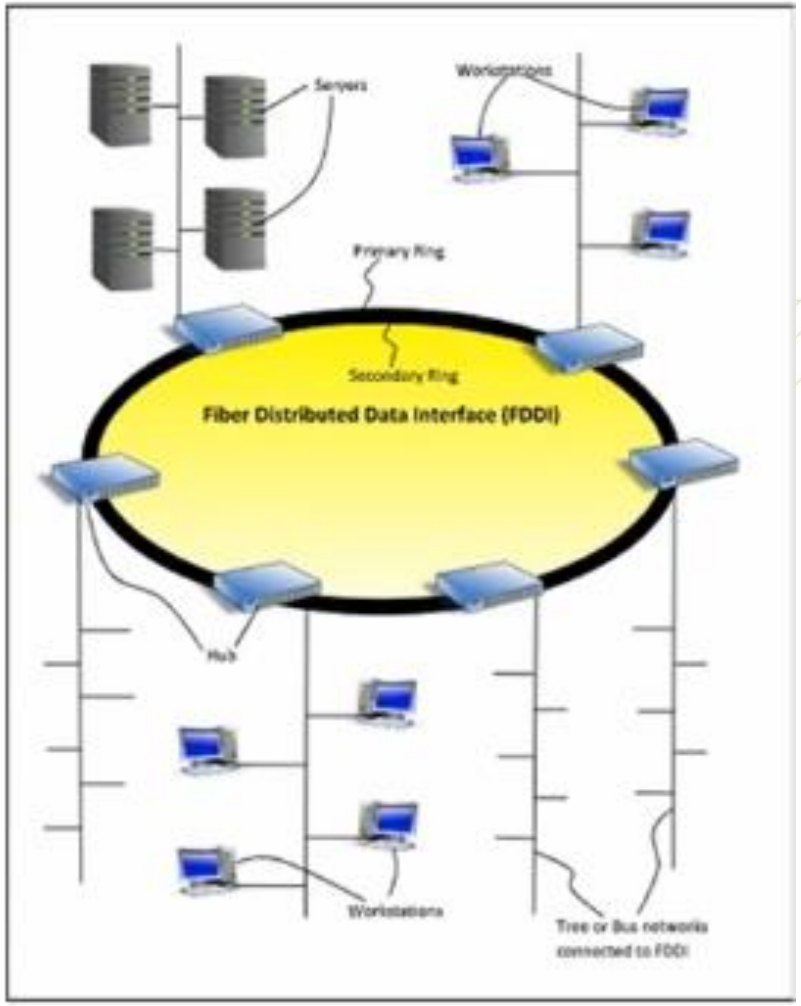
$$\text{Data} = (d_1 c_1 + d_2 c_2 + d_3 c_3 + d_4 c_4) \times c_1 = 4 \times d_1$$

Example-CDMA

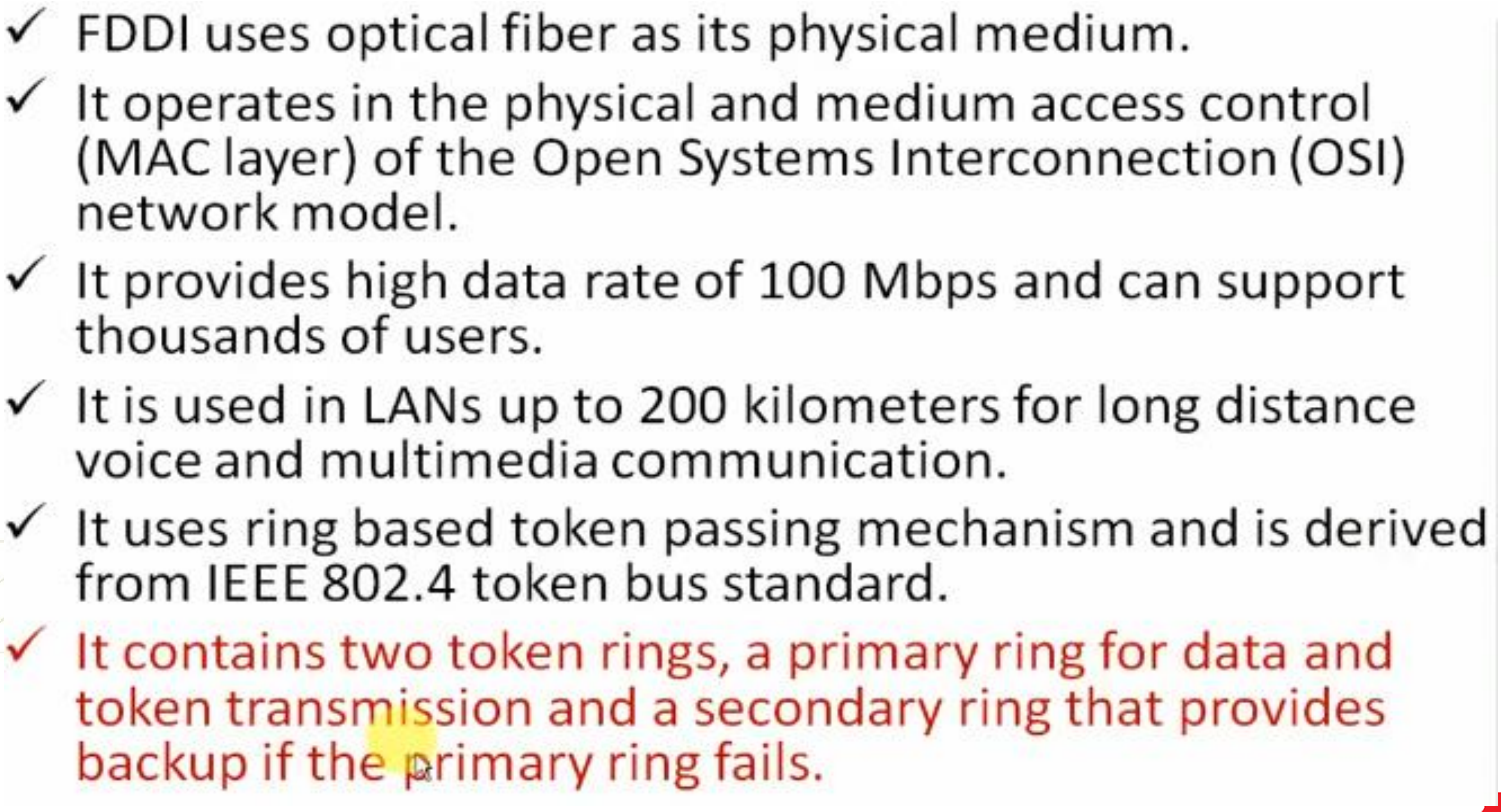


Fiber Distributed Data Interface (FDDI)

- ✓ Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables.
- ✓ It is applicable in large LANs that can extend up to 200 kilometers in diameter.

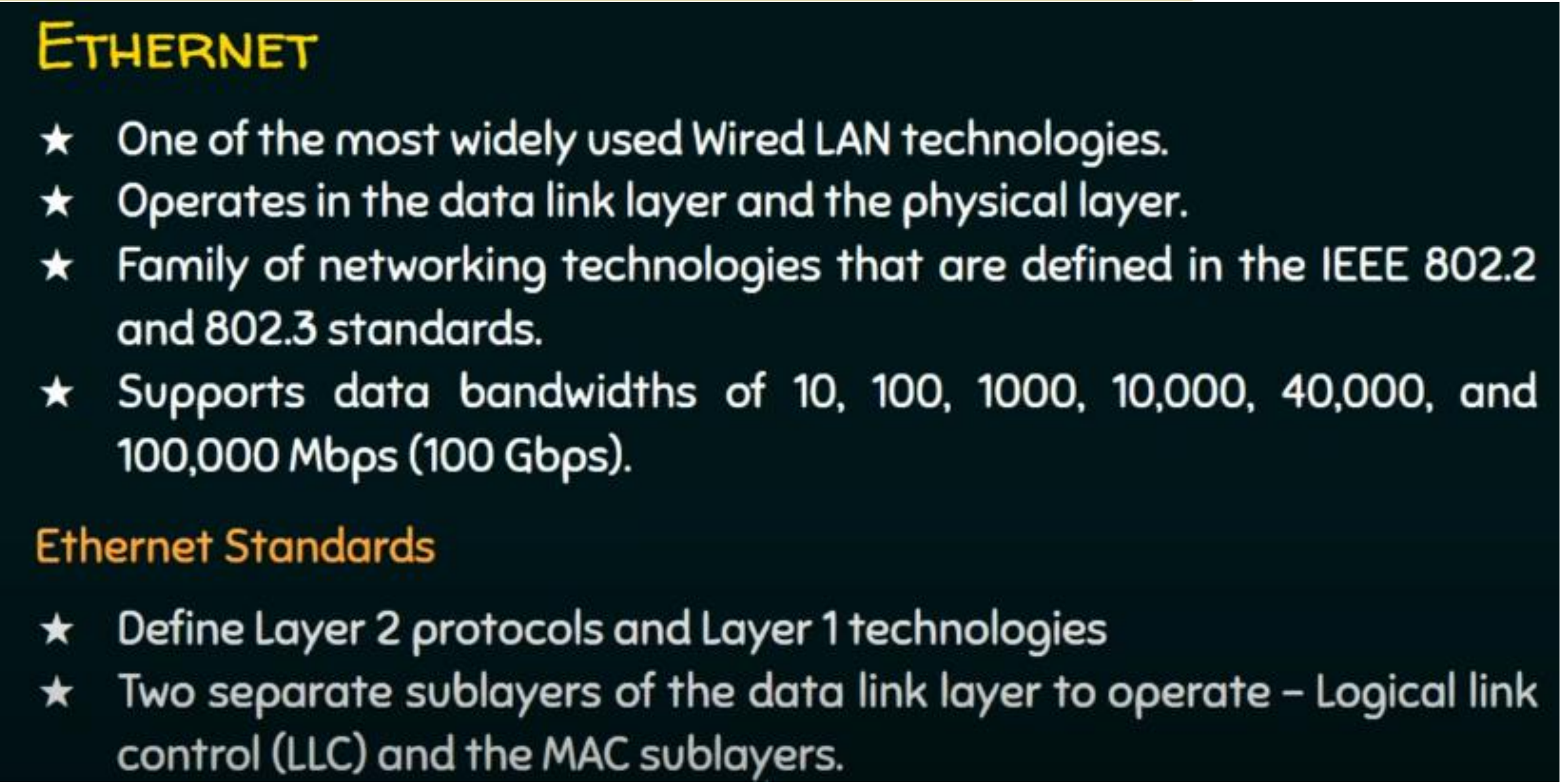


Features of FDDI



- ✓ FDDI uses optical fiber as its physical medium.
- ✓ It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- ✓ It provides high data rate of 100 Mbps and can support thousands of users.
- ✓ It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- ✓ It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- ✓ It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.

FDDI- Ethernet



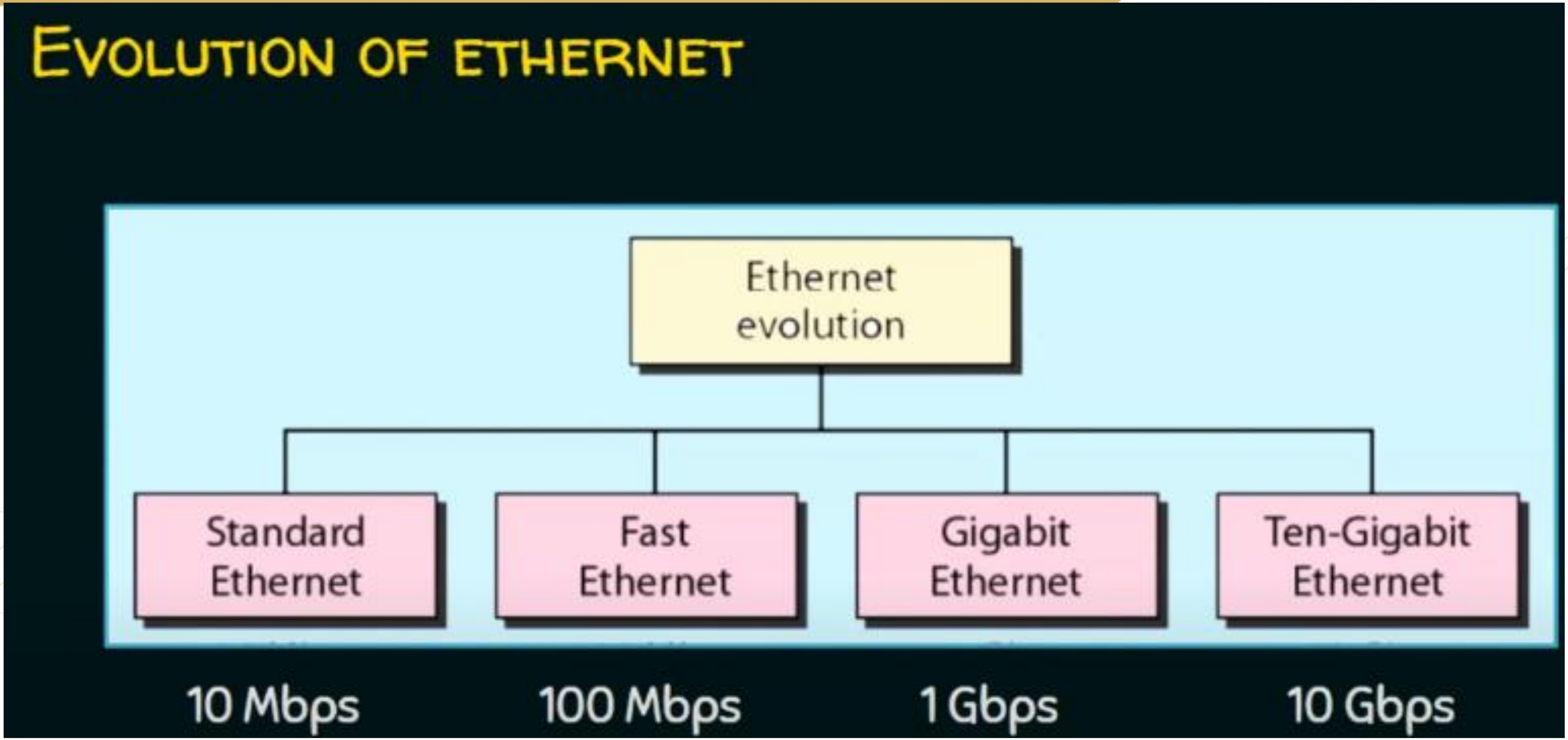
Ethernet

- ★ One of the most widely used Wired LAN technologies.
- ★ Operates in the data link layer and the physical layer.
- ★ Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards.
- ★ Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps).

Ethernet Standards

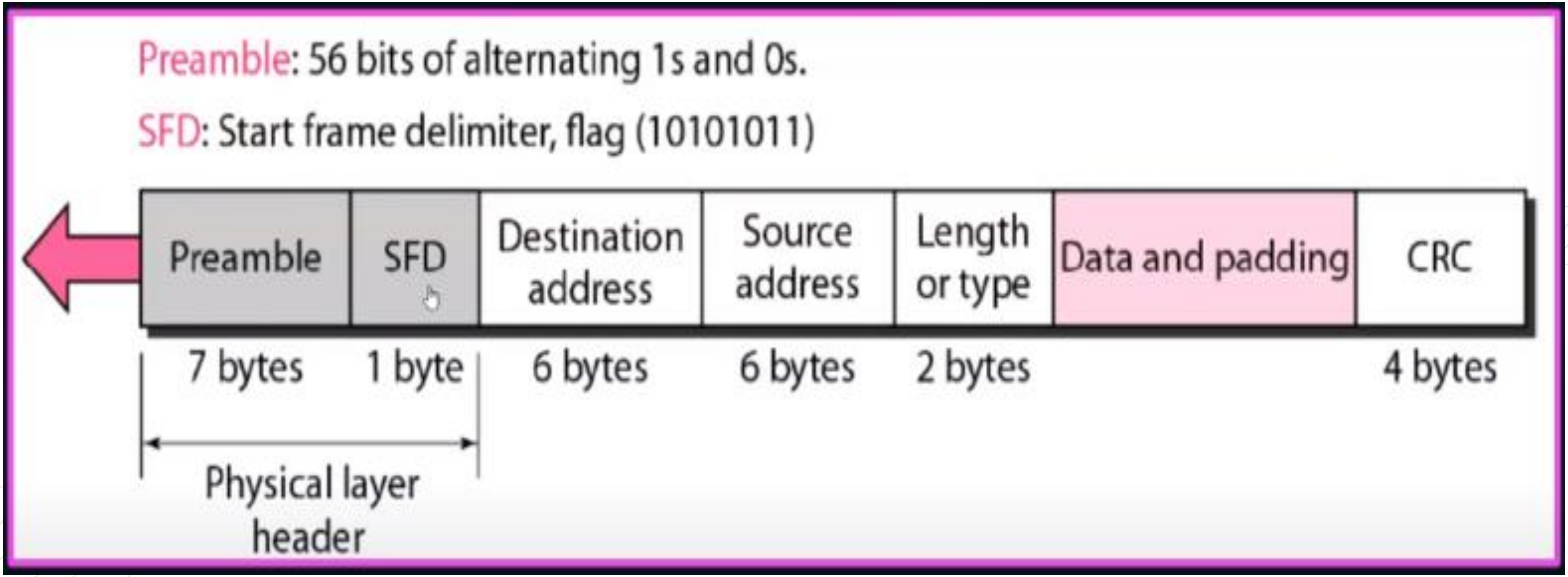
- ★ Define Layer 2 protocols and Layer 1 technologies
- ★ Two separate sublayers of the data link layer to operate – Logical link control (LLC) and the MAC sublayers.

FDDI- Ethernet



Evolution of Ethernet

FDDI- Ethernet Frame Format

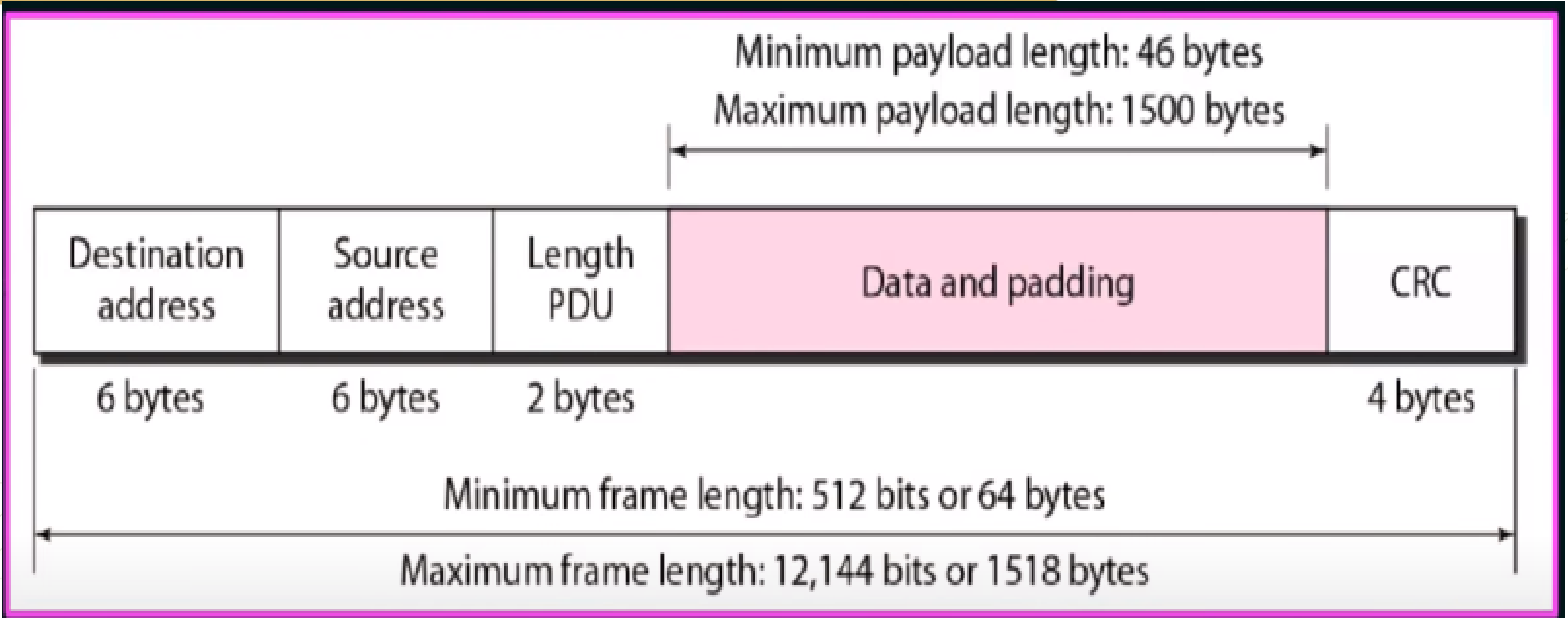


Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)

Preamble	SFD	Destination address	Source address	Length or type	Data and padding	CRC
7 bytes	1 byte	6 bytes	6 bytes	2 bytes		4 bytes

FDDI- Ethernet Frame – Min and Max Length



Minimum payload length: 46 bytes

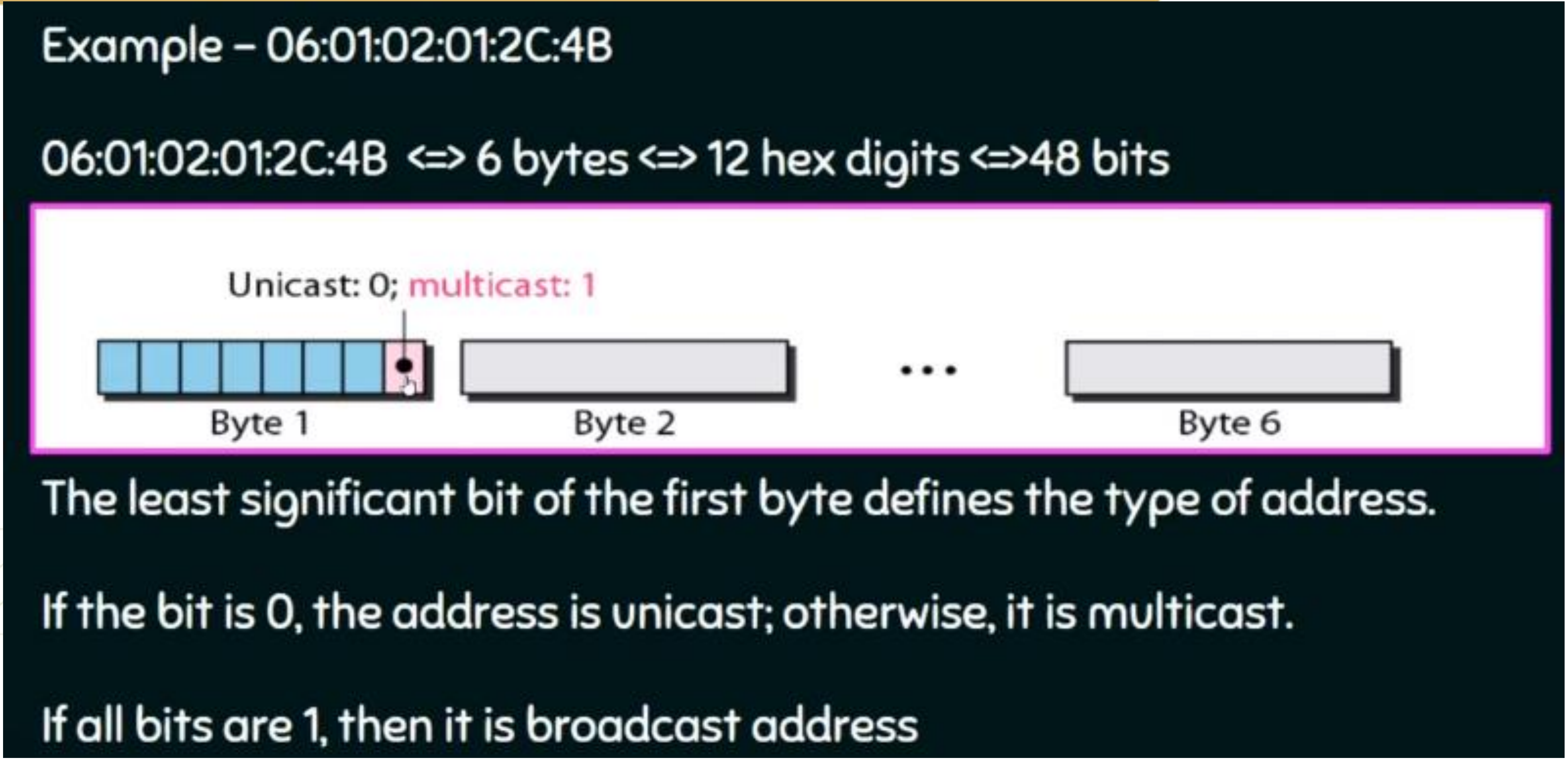
Maximum payload length: 1500 bytes

Destination address	Source address	Length PDU	Data and padding	CRC
6 bytes	6 bytes	2 bytes		4 bytes

Minimum frame length: 512 bits or 64 bytes

Maximum frame length: 12,144 bits or 1518 bytes

Example- Ethernet Address



Example – 06:01:02:01:2C:4B

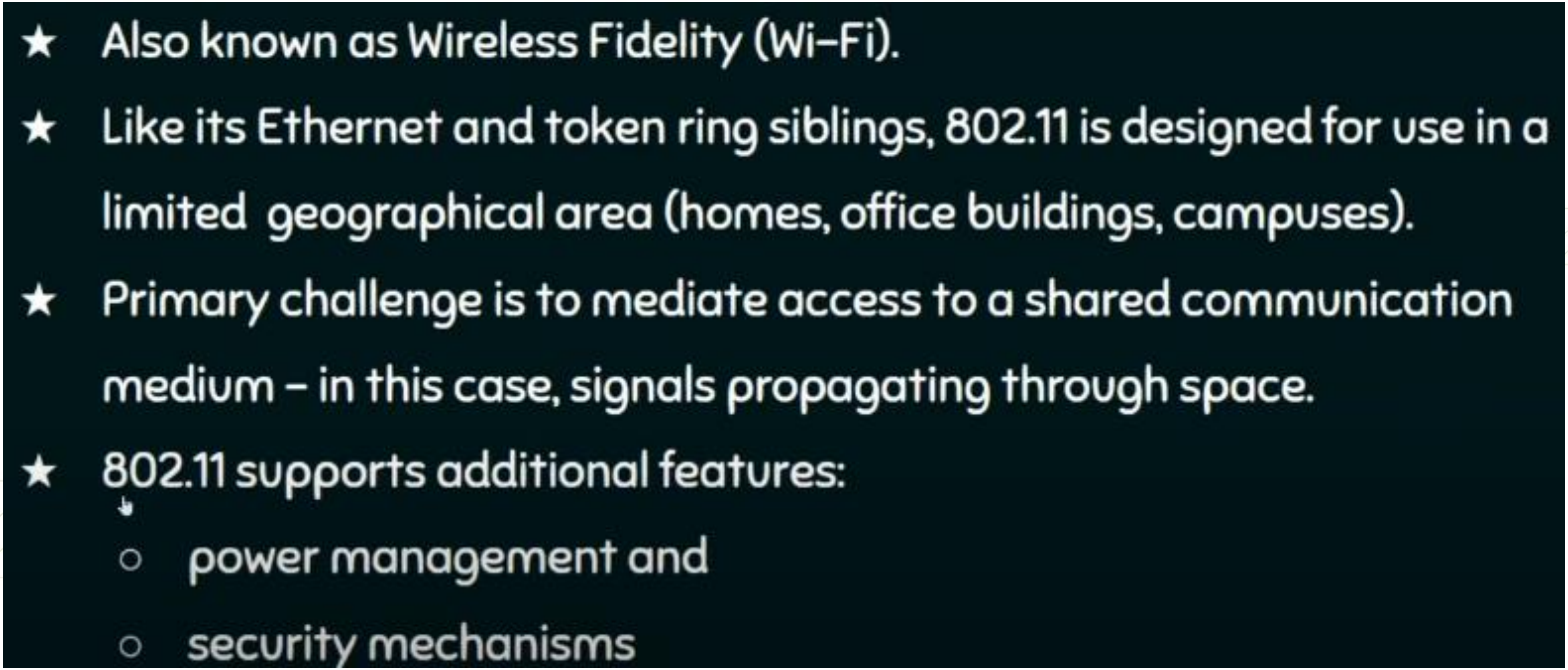
06:01:02:01:2C:4B <=> 6 bytes <=> 12 hex digits <=>48 bits

The least significant bit of the first byte defines the type of address.

If the bit is 0, the address is unicast; otherwise, it is multicast.

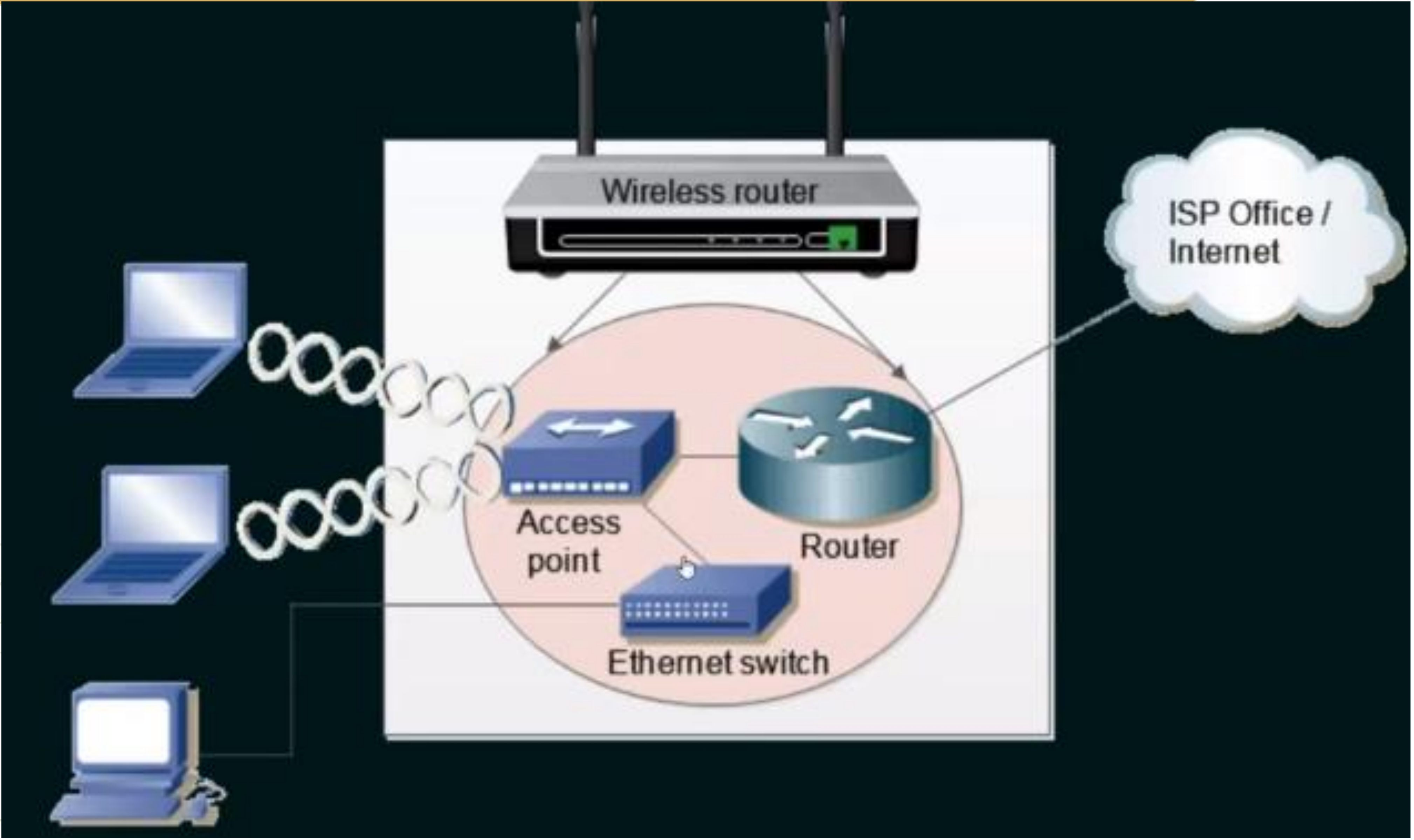
If all bits are 1, then it is broadcast address

IEEE 802.11 Wireless- Fidelity (Wi-Fi)

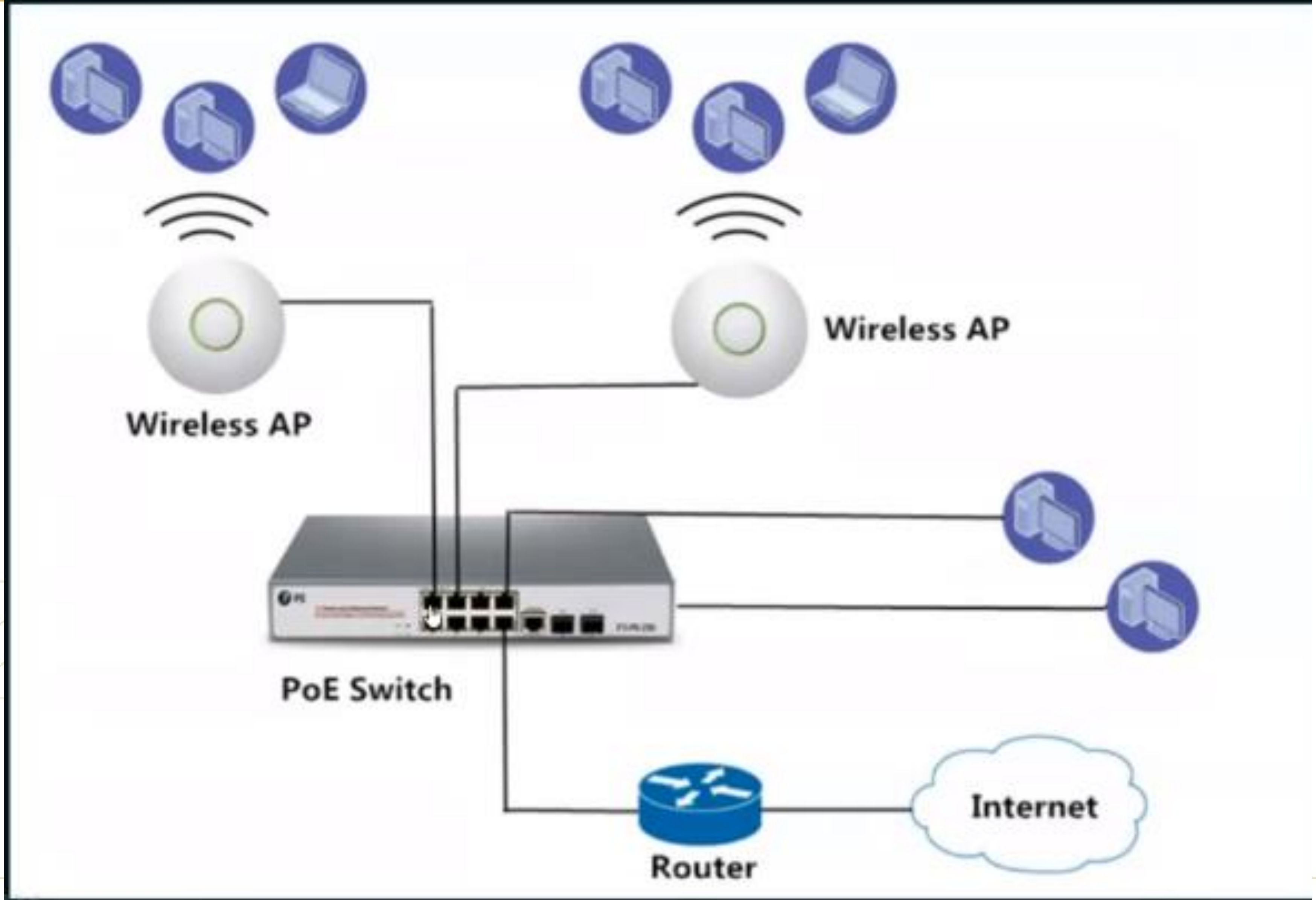


- ★ Also known as Wireless Fidelity (Wi-Fi).
- ★ Like its Ethernet and token ring siblings, 802.11 is designed for use in a limited geographical area (homes, office buildings, campuses).
- ★ Primary challenge is to mediate access to a shared communication medium – in this case, signals propagating through space.
- ★ 802.11 supports additional features:
  - ○ power management and
  - ○ security mechanisms

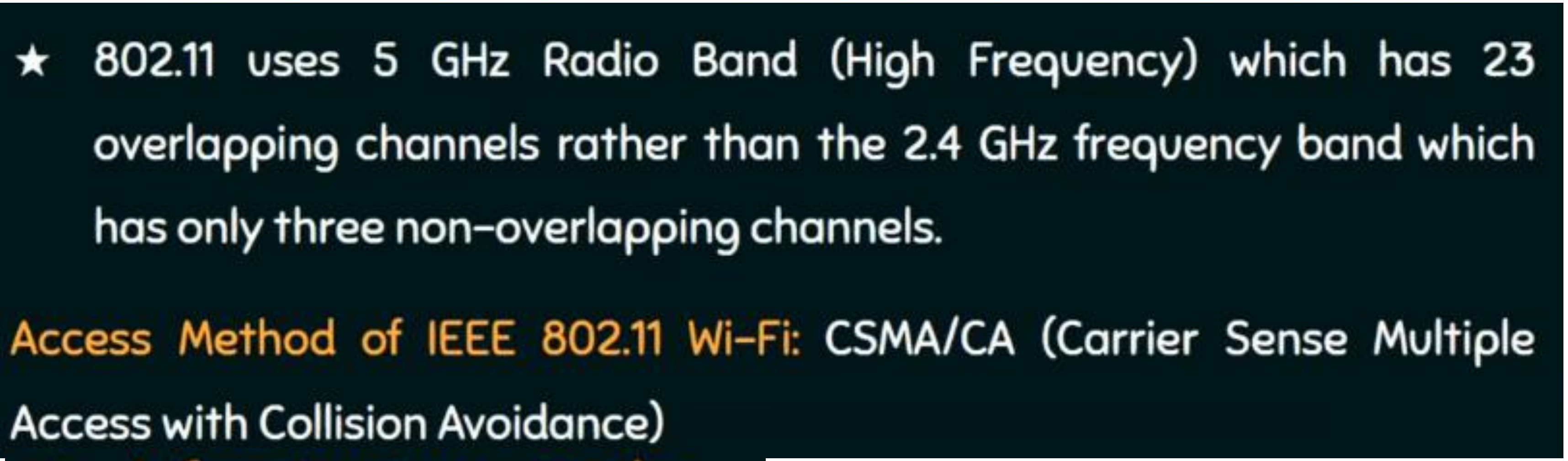
Example-IEEE 802.11 Wireless- Fidelity (Wi-Fi)



Example-IEEE 802.11 Wireless- Fidelity (Wi-Fi)

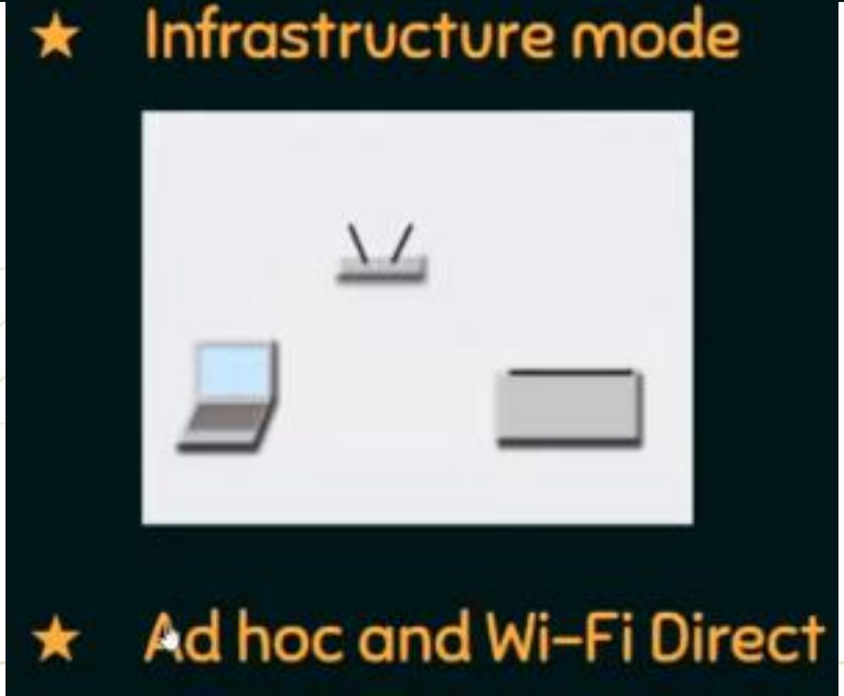


IEEE 802.11and its Modes



★ 802.11 uses 5 GHz Radio Band (High Frequency) which has 23 overlapping channels rather than the 2.4 GHz frequency band which has only three non-overlapping channels.

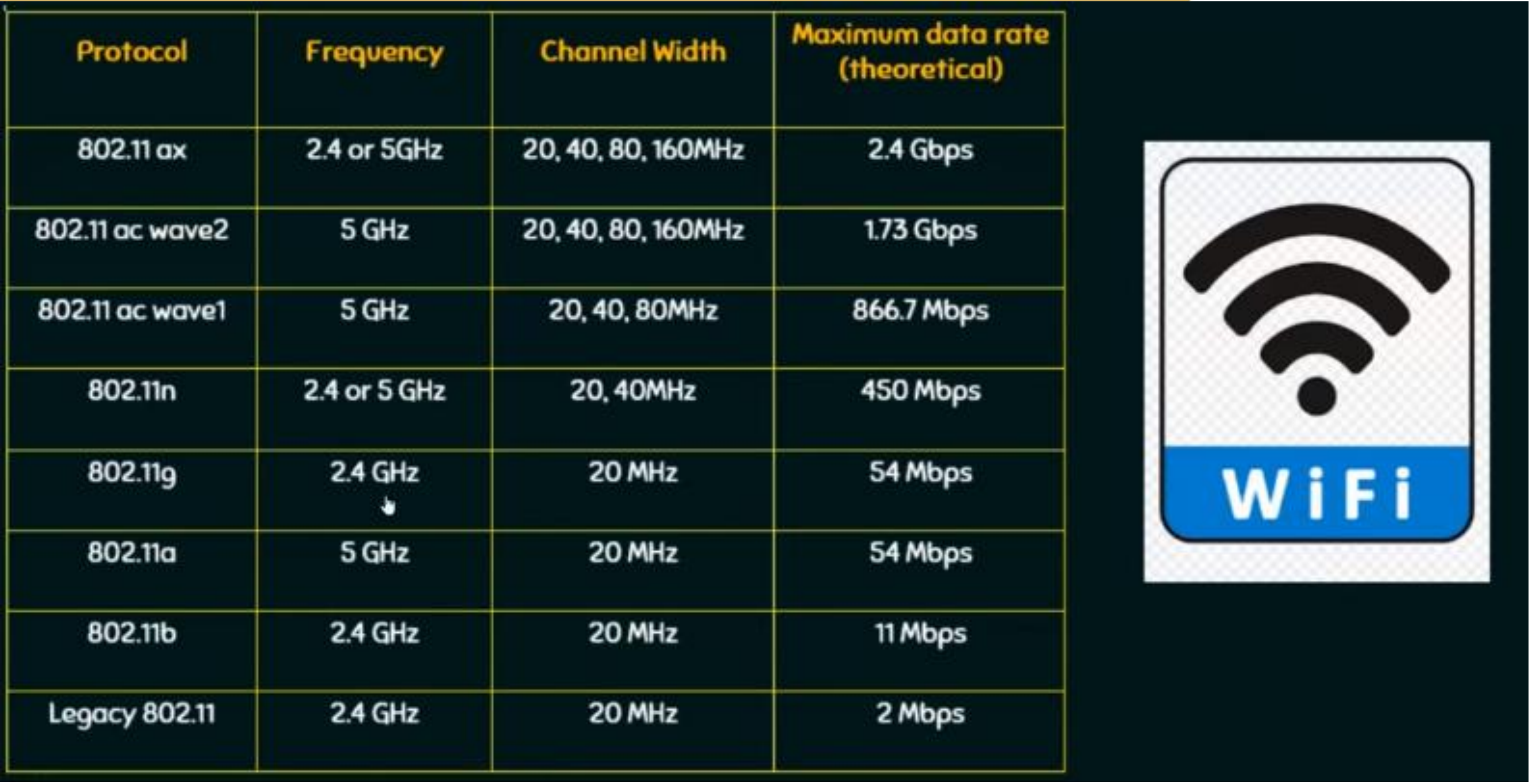
Access Method of IEEE 802.11 Wi-Fi: CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)



★ Infrastructure mode

★ Ad hoc and Wi-Fi Direct

Different Types of Wi-Fi Protocols



Protocol	Frequency	Channel Width	Maximum data rate (theoretical)
802.11 ax	2.4 or 5GHz	20, 40, 80, 160MHz	2.4 Gbps
802.11 ac wave2	5 GHz	20, 40, 80, 160MHz	1.73 Gbps
802.11 ac wave1	5 GHz	20, 40, 80MHz	866.7 Mbps
802.11n	2.4 or 5 GHz	20, 40MHz	450 Mbps
802.11g	2.4 GHz	20 MHz	54 Mbps
802.11a	5 GHz	20 MHz	54 Mbps
802.11b	2.4 GHz	20 MHz	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	2 Mbps