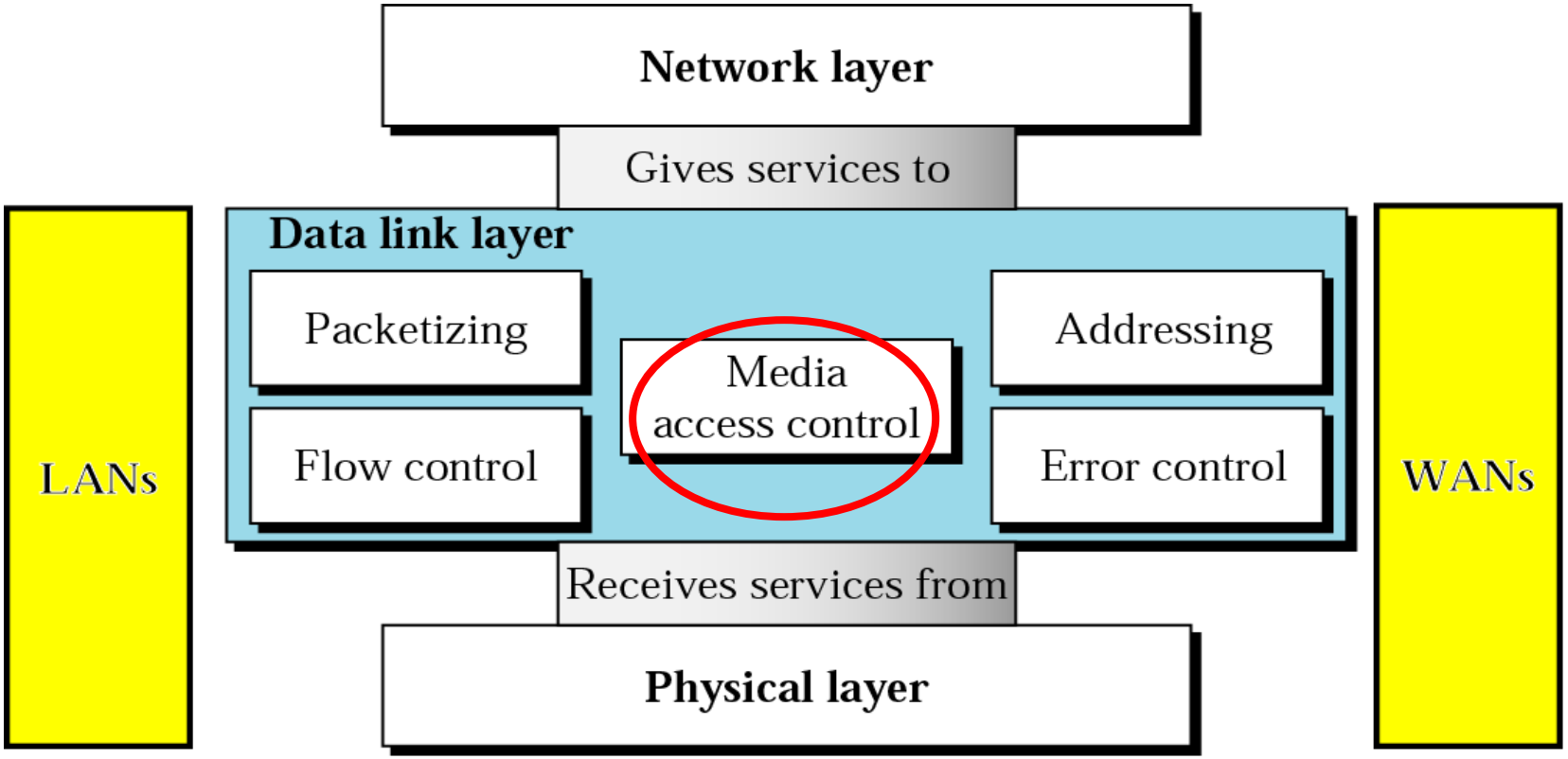
Chapter 4

Media Access Control (MAC)

Prepared by :

Dr. Adel Soudani & Dr. Mznah Al-Rodhaan

Data Link Layer

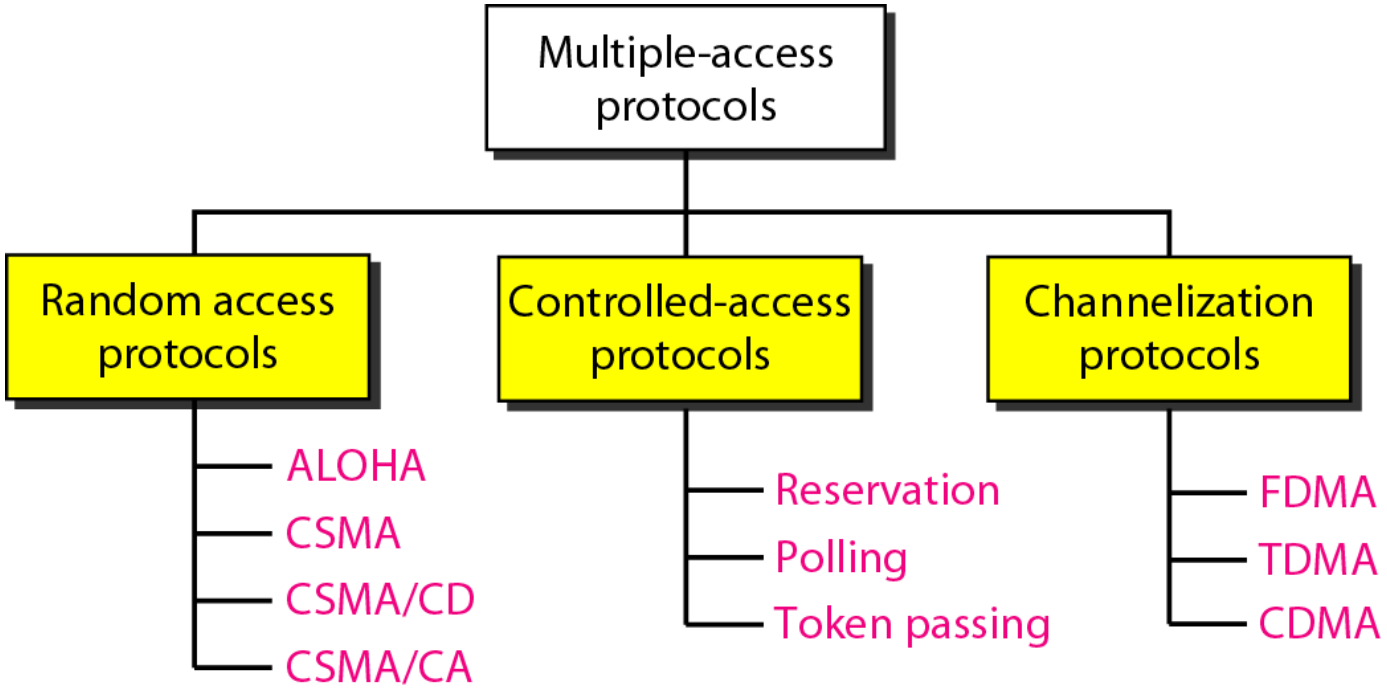


Multiple access problem

Human communication protocols:

- Give everyone a chance to speak
- Raise your hand if you have a question
- Don’t speak until you are spoken to
- Don’t interrupt when someone is speaking
- Don’t monopolize the conversation
- Don’t fall asleep when someone else is talking

Taxonomy of Multiple-Access Protocols



Lecture 1

Random Access Protocols

Random Access Protocols

In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits another station to send.

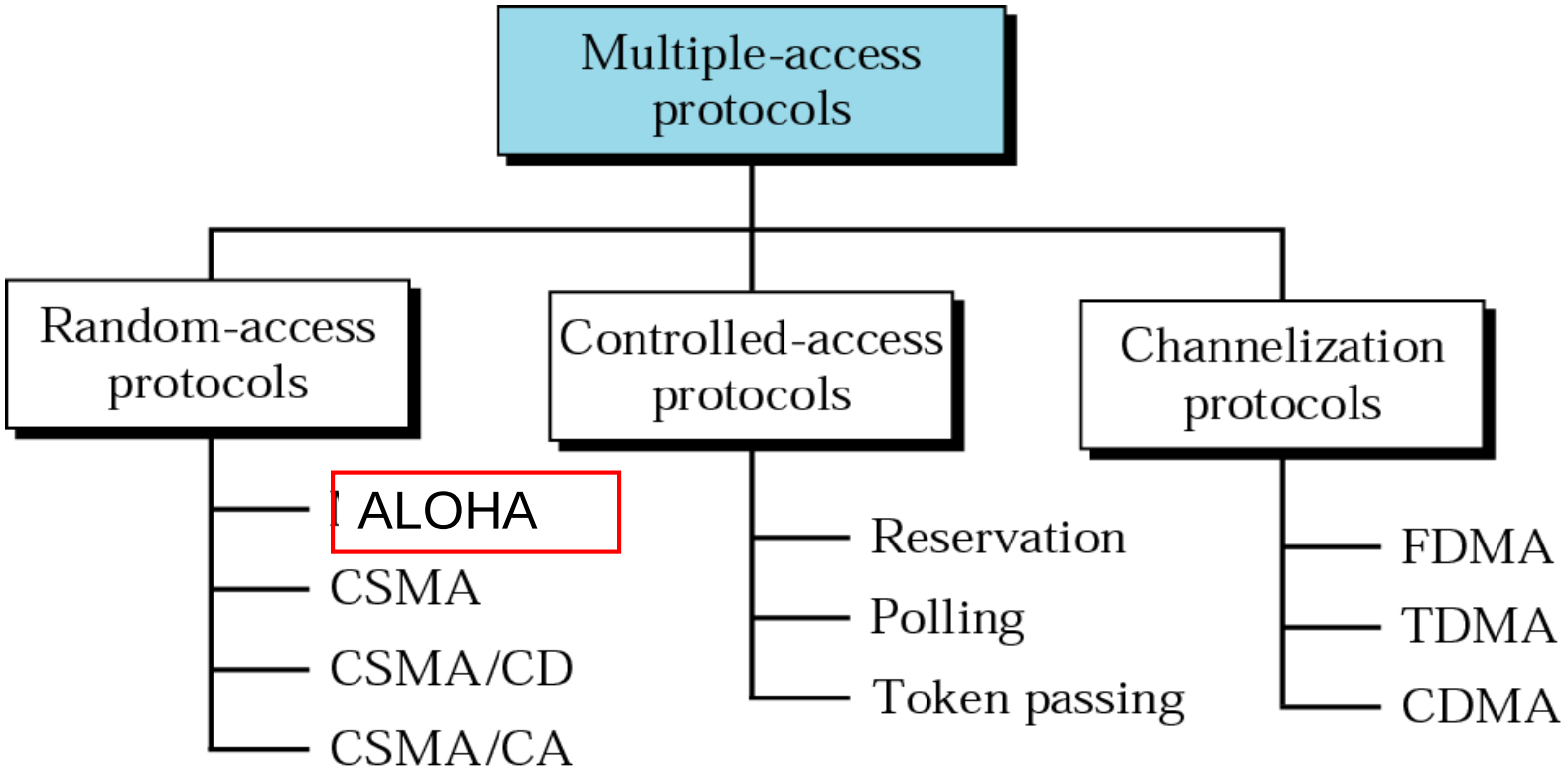
At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

Random Access Protocols

Topics discussed in this section:

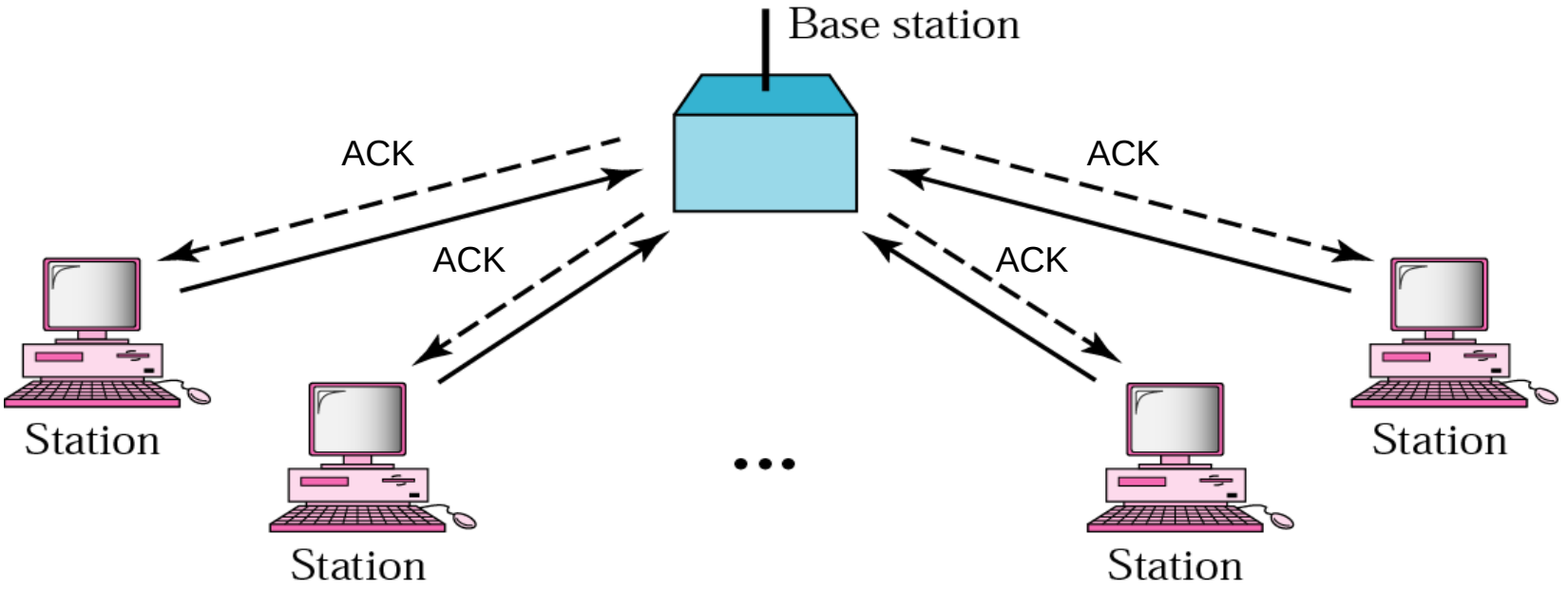
- ALOHA
- Carrier Sense Multiple Access (CSMA)
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Multiple Access Protocols



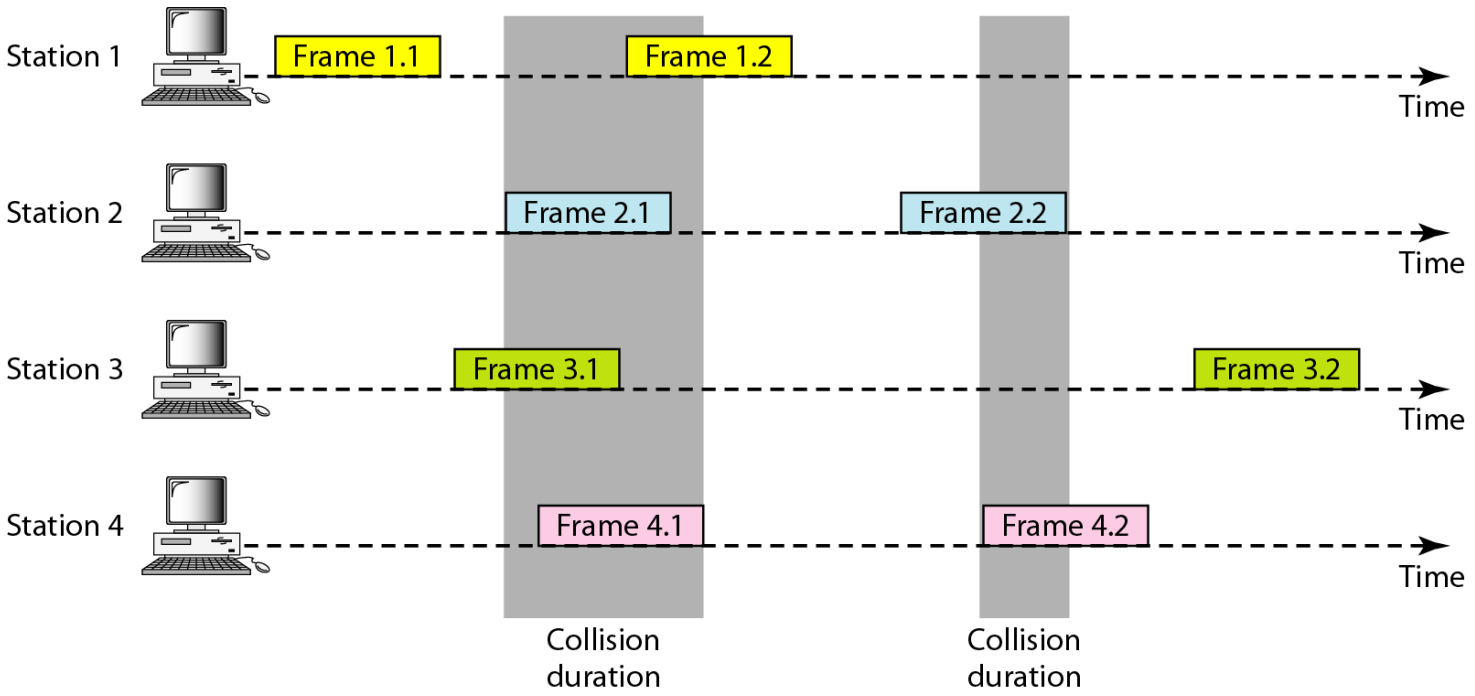
ALOHA Network

Developed at the Univ. of Hawaii

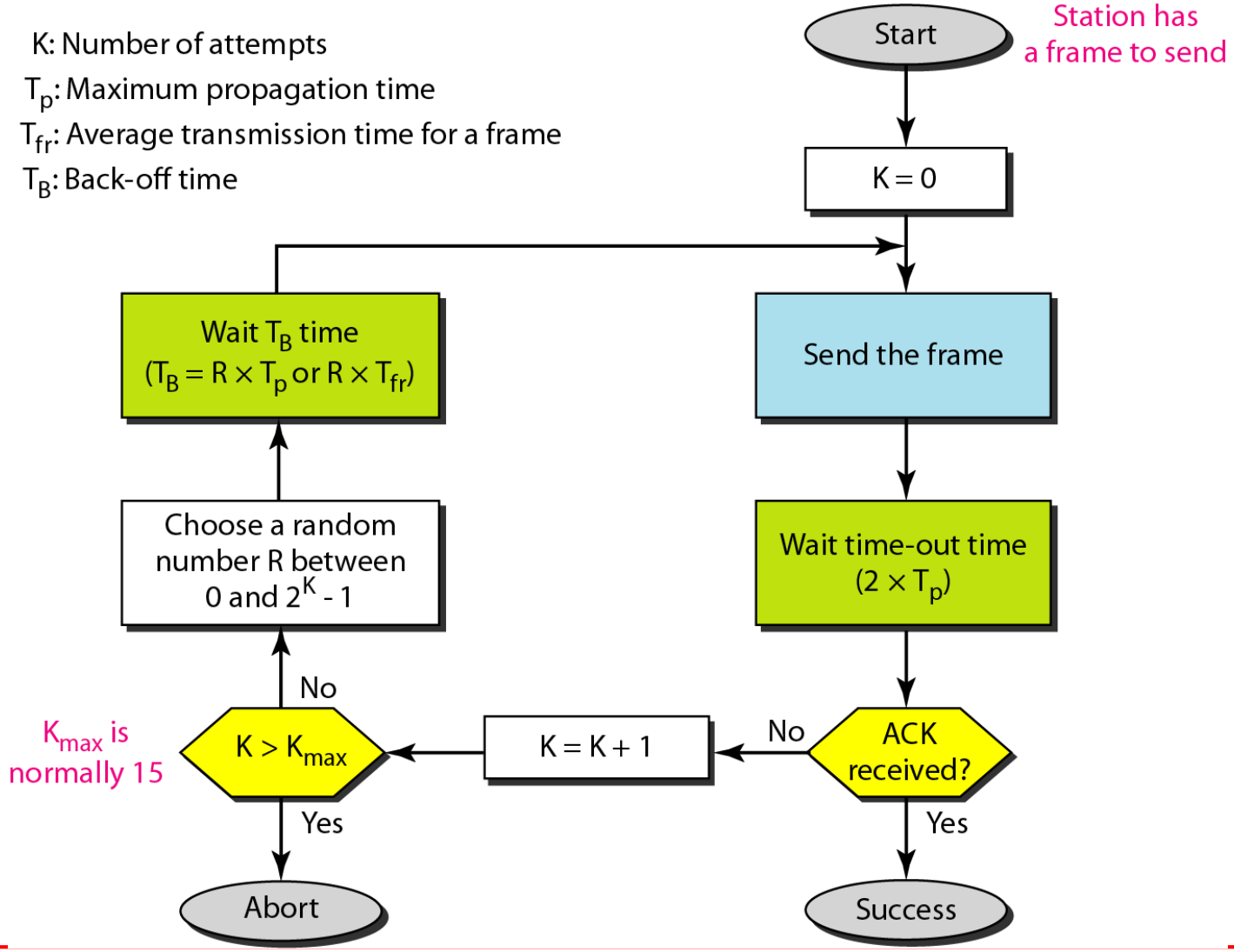


Pure Aloha

The node immediately transmits its frame completely
If the frame is collided it retransmits the frame again with the probability *p.*



Procedure for pure ALOHA protocol



Example 1

The stations on a wireless ALOHA network are a maximum of 600 km apart. If we assume that signals propagate at 3×10^8 m/s, we find

$$T_p = (600 \times 10^3) / (3 \times 10^8) = 2 \text{ ms}.$$

Now we can find the value of T_B for different values of K .

a. For K = 1, the range is {0, 1}. The station needs to generate a random number with a value of 0 or 1. This means that T_B is either 0 ms (0 × 2) or 2 ms (1 × 2), based on the outcome of the random variable.

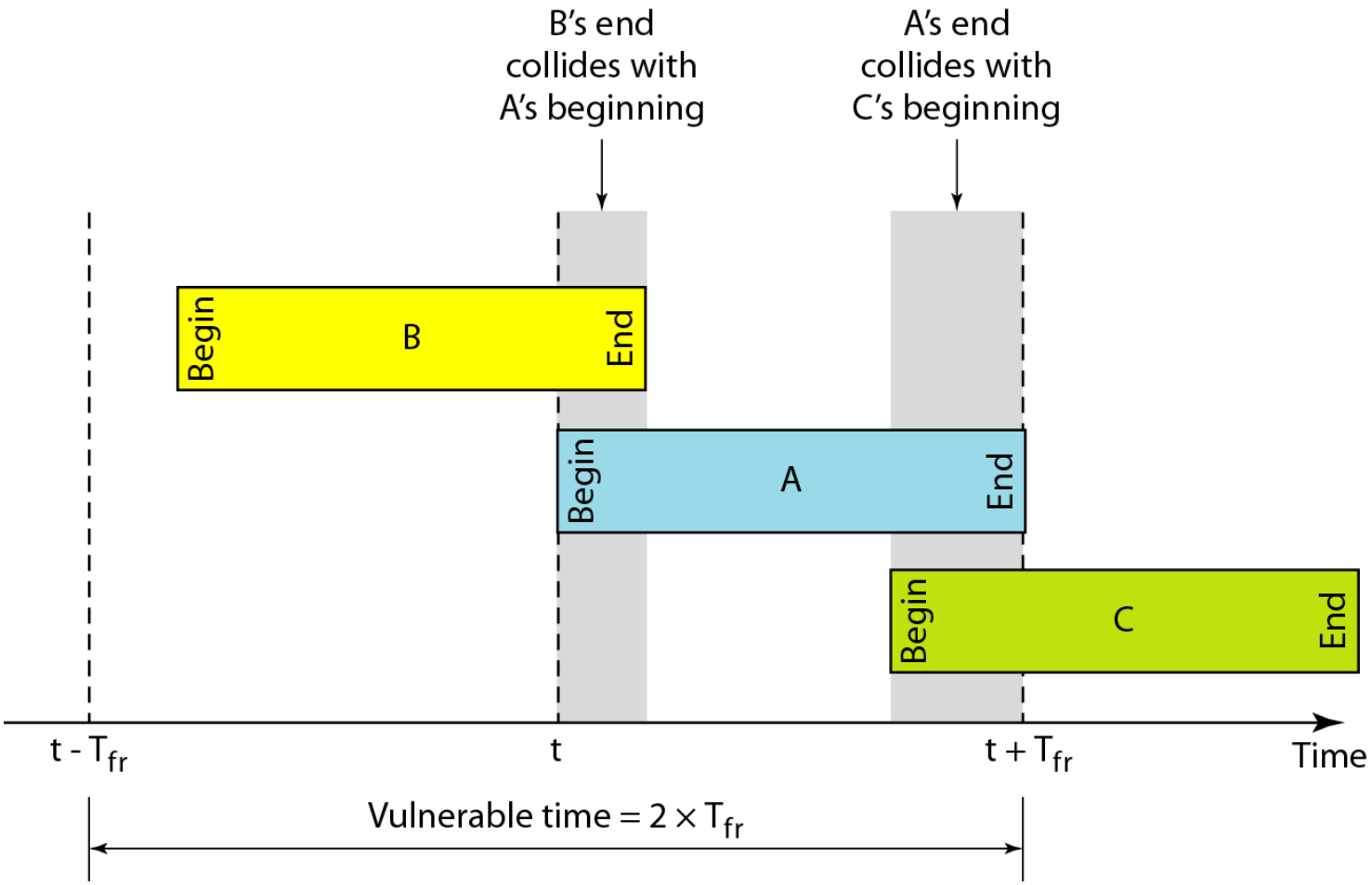
Example 1 (continued)

b. For K = 2, the range is {0, 1, 2, 3}. This means that T_B can be 0, 2, 4, or 6 ms, based on the outcome of the random variable.

c. For K = 3, the range is {0, 1, 2, 3, 4, 5, 6, 7}. This means that T_B can be 0, 2, 4, . . . , 14 ms, based on the outcome of the random variable.

d. We need to mention that if K > 10, it is normally set to 10.

Vulnerable time for pure ALOHA protocol



Example 2

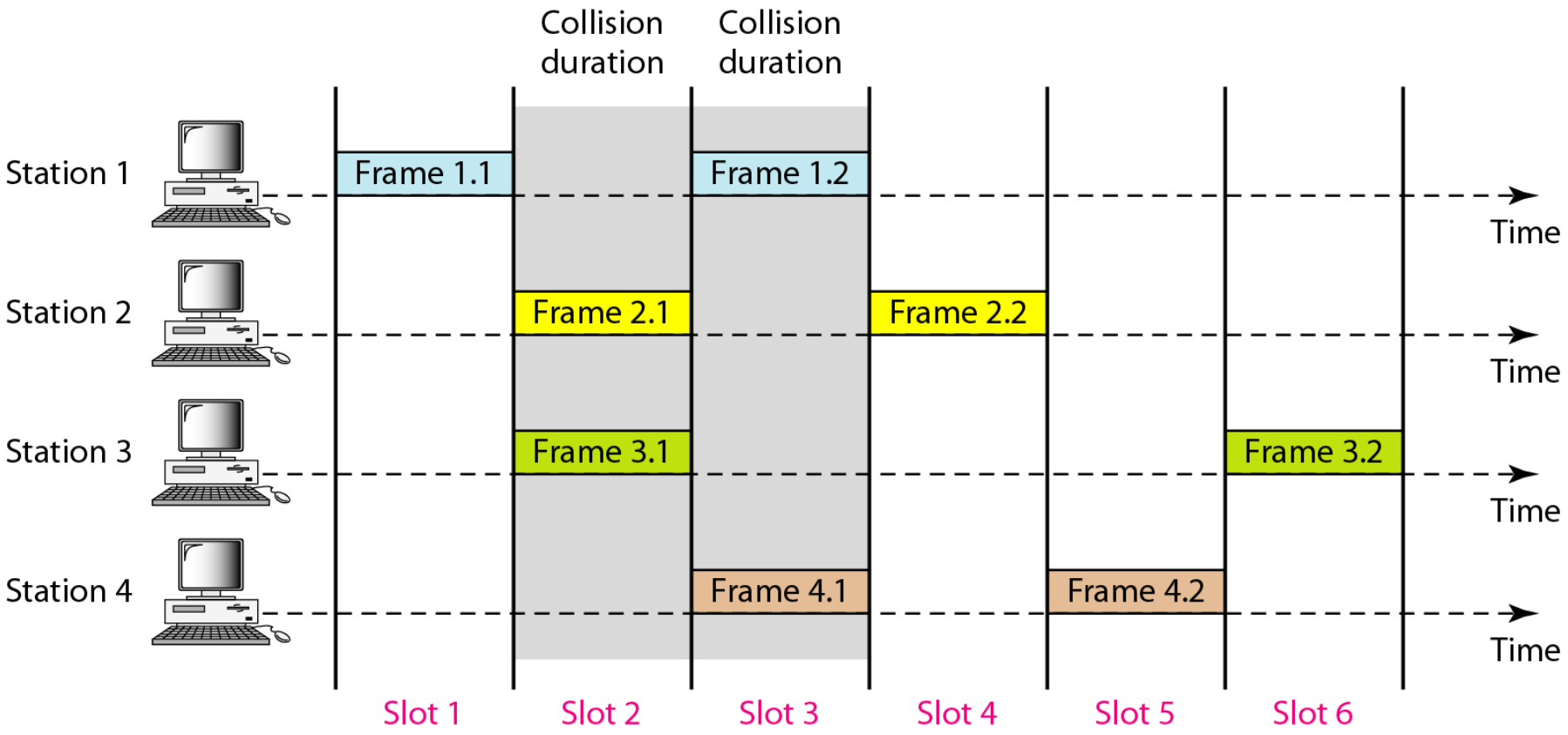
A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms = 2 ms.

- This means no station should send later than 1 ms before this station starts transmission
- and no station should start sending during the one 1-ms period that this station is sending.

Frames in a slotted ALOHA network



Slotted Aloha

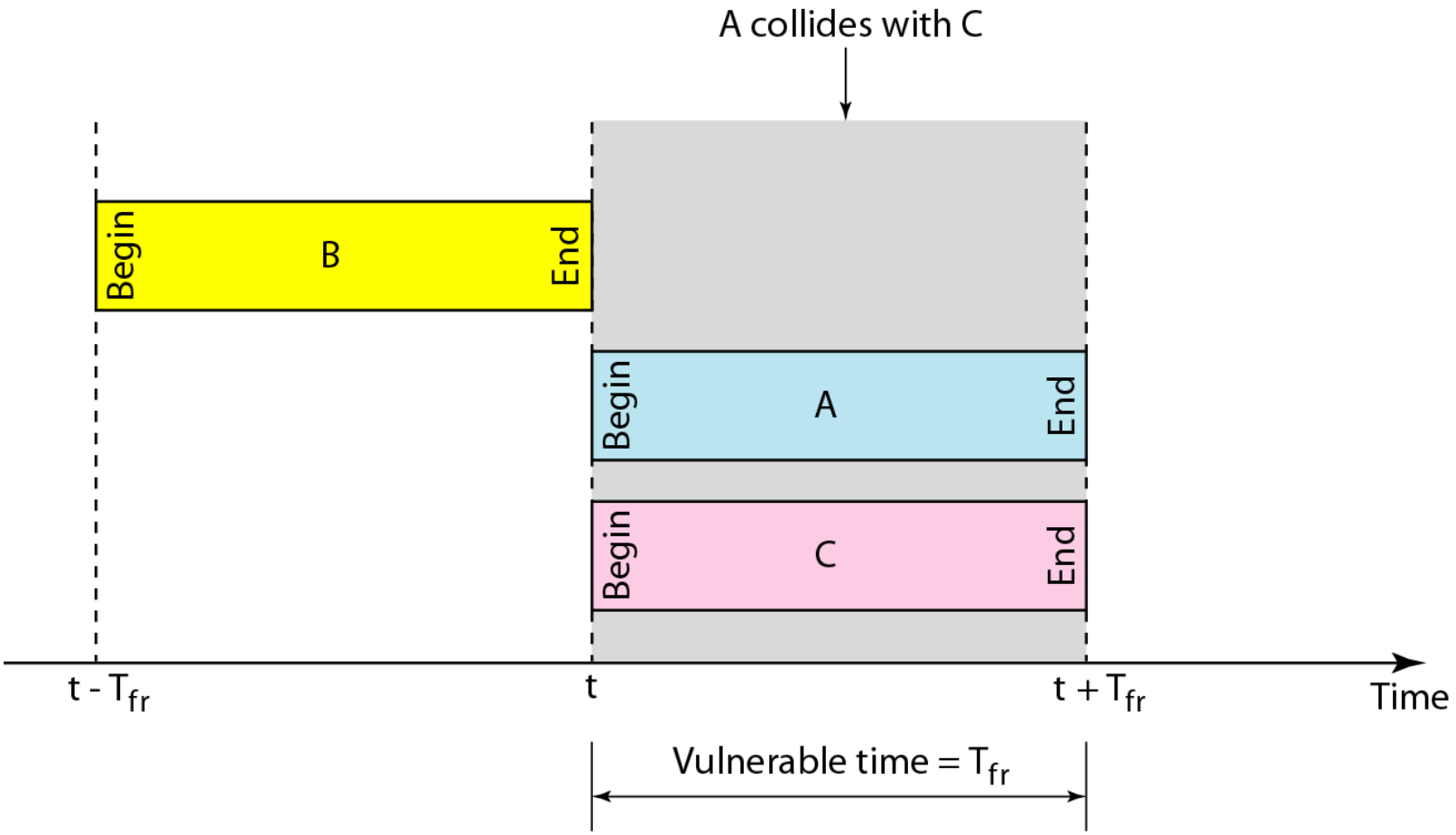
Assumptions

Frames are of the same size
time is divided into equal size slots, time to transmit 1 frame
nodes start to transmit frames only at beginning of slots
nodes are synchronized
if 2 or more nodes transmit in slot, all nodes detect collision

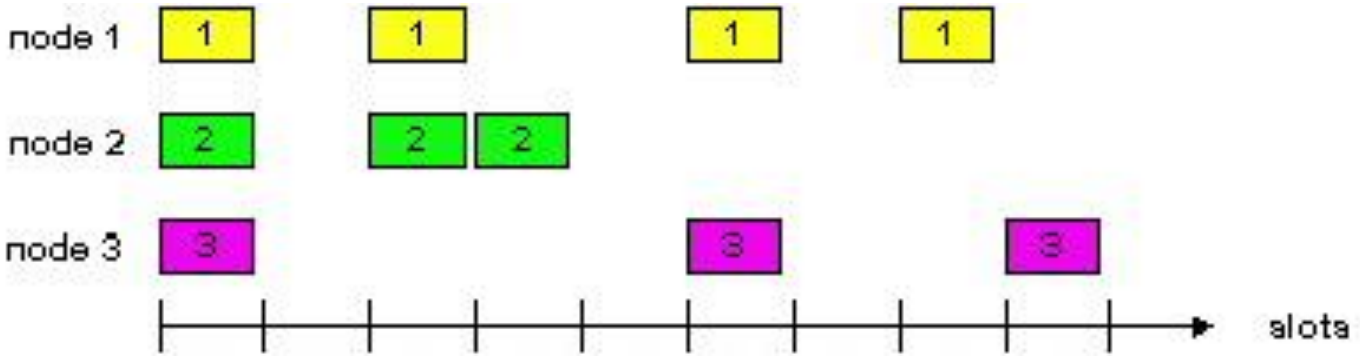
Operation

- when node obtains fresh frame, it transmits in next slot
- no collision, node can send new frame in next slot
- if collision, node retransmits frame in each subsequent slot with prob. p until success

Vulnerable time for slotted ALOHA protocol



Slotted Aloha



Pros

- single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- simple

Cons

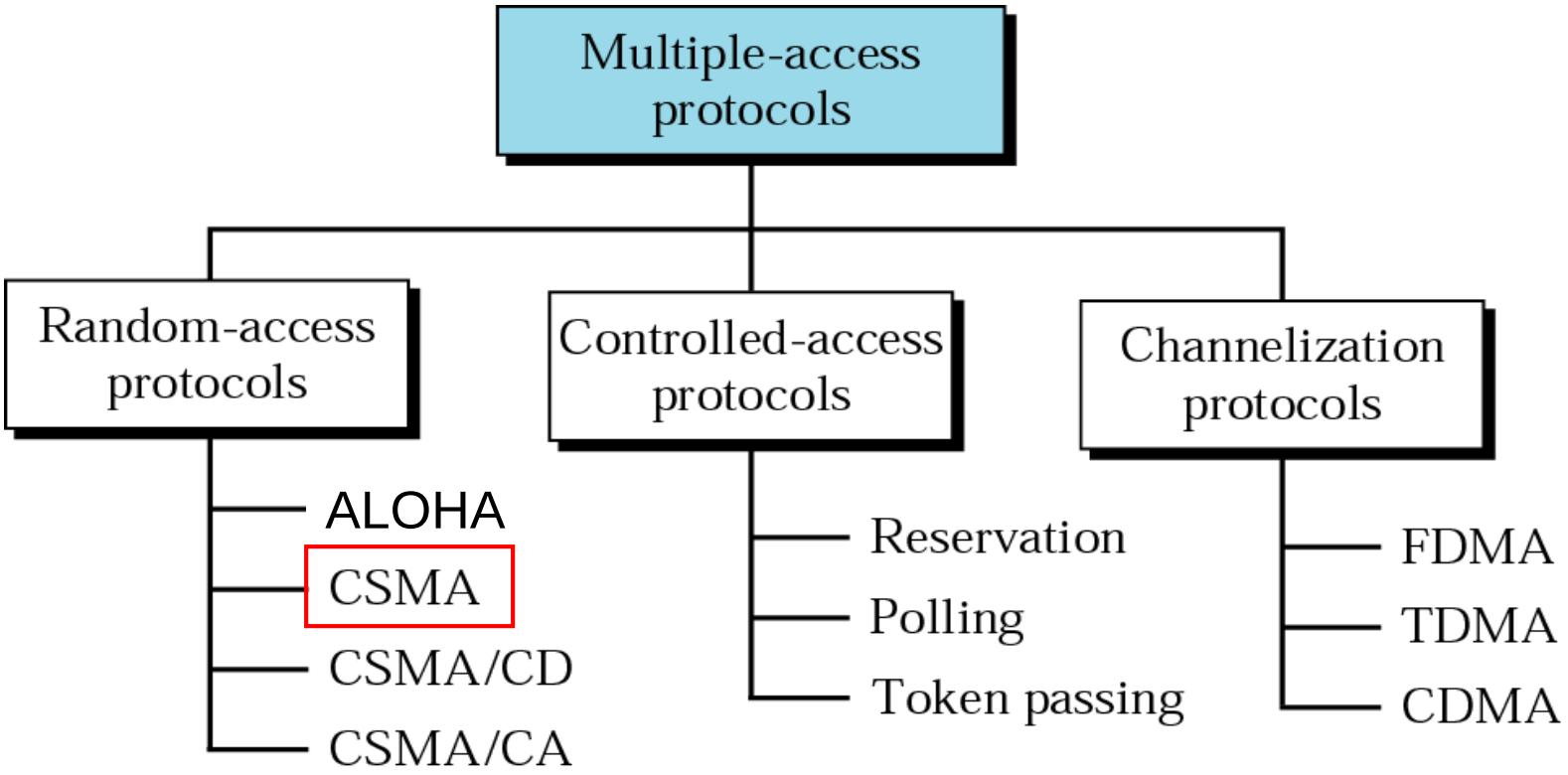
- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less time than to transmit packet
- clock synchronization

Lecture 2

Random Access Protocols

Carrier Sense Multiple Access

Multiple Access Protocols



Carrier Sense Multiple Access

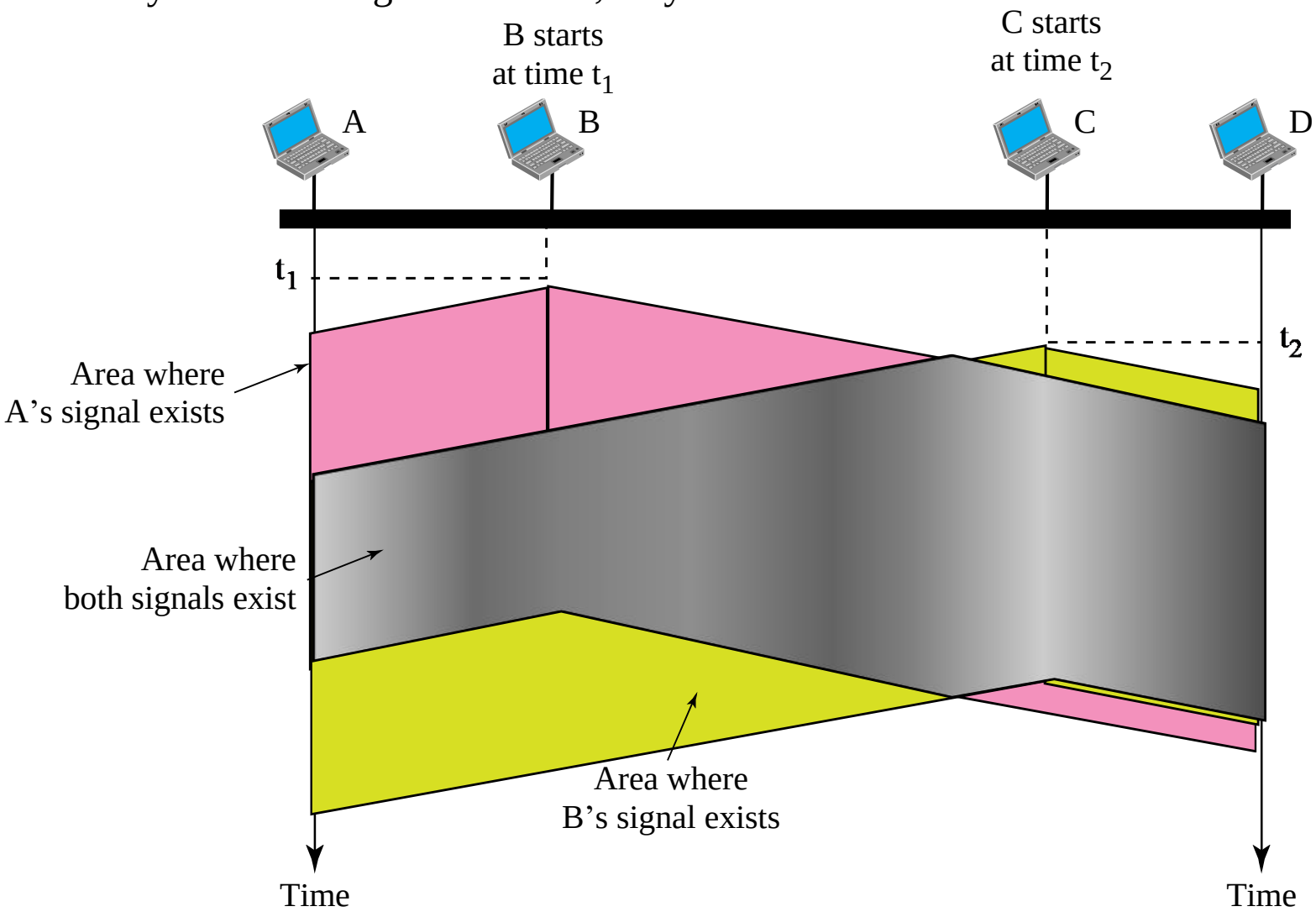
- Invented to minimize collisions and increase the performance
- A station now "follows" the activity of other stations
- Simple rules for a polite human conversation
  - Listen before talking
  - If someone else begins talking at the same time as you, stop talking

- CSMA
  - A node should not send if another node is already sending → carrier sensing

  - CD (collision detection) a node should stop transmission if there is interference → collision detection

Space/time model of the collision in CSMA

If everyone is sensing the medium, why collisions still occur?



CSMA

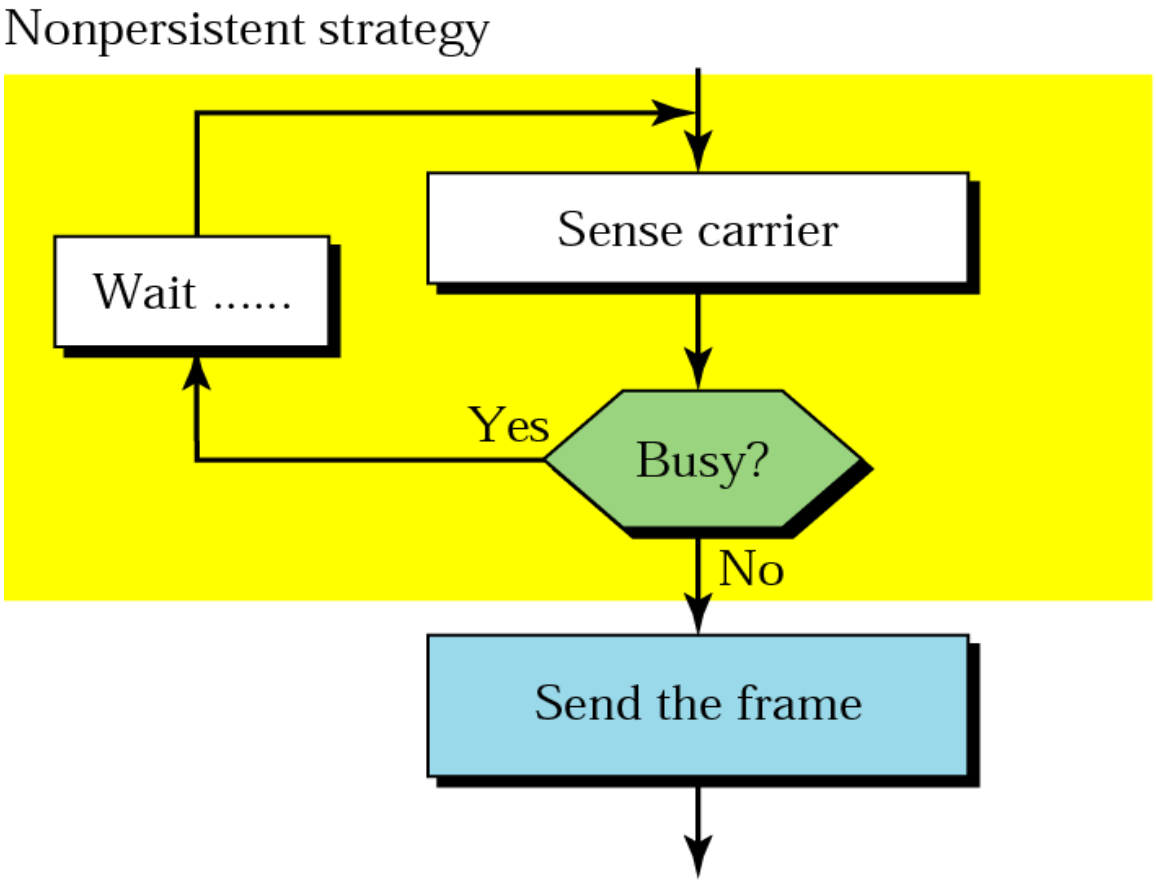
Persistence methods:

1. Nonpersistent strategy

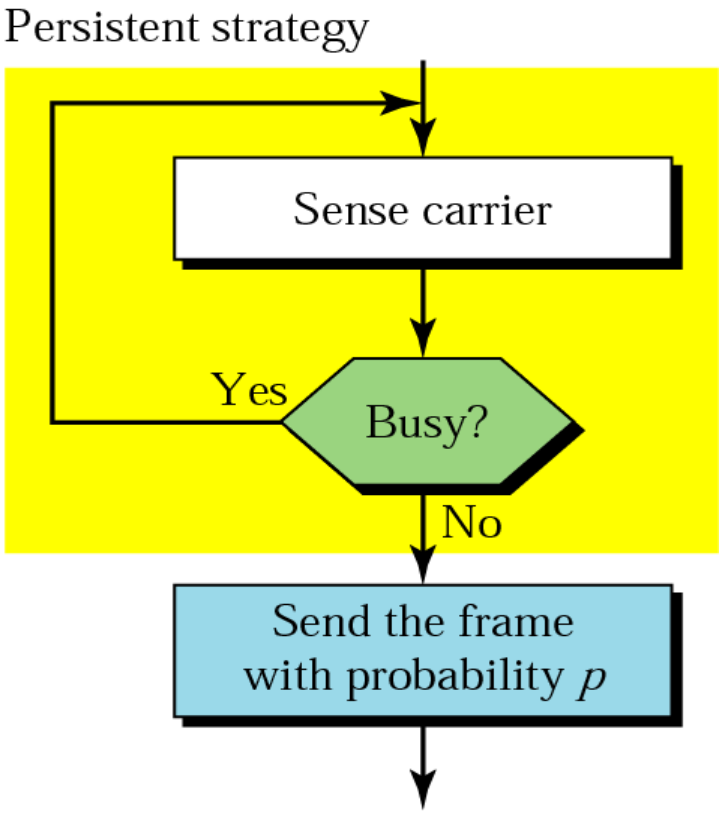
2. Persistent strategy

3. P-persistent strategy

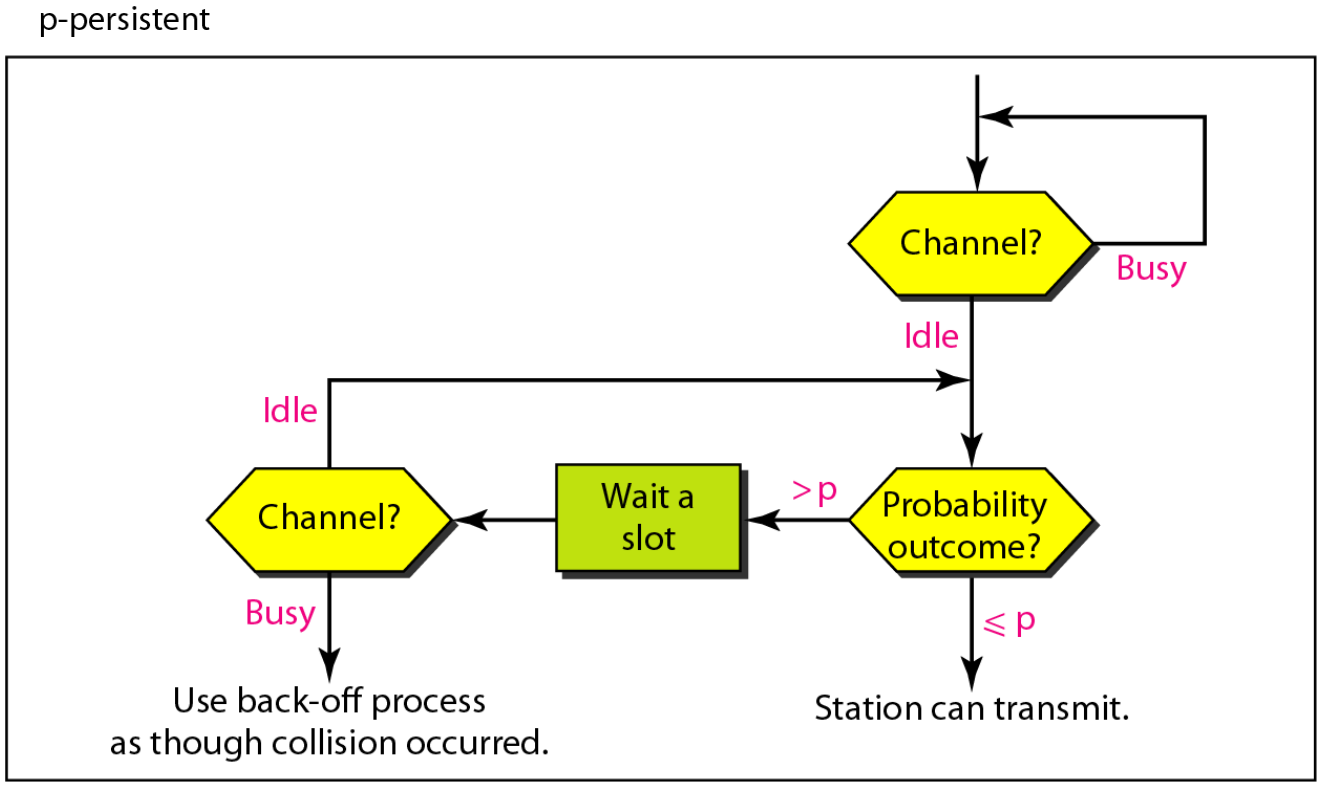
Flow diagram for three persistence methods



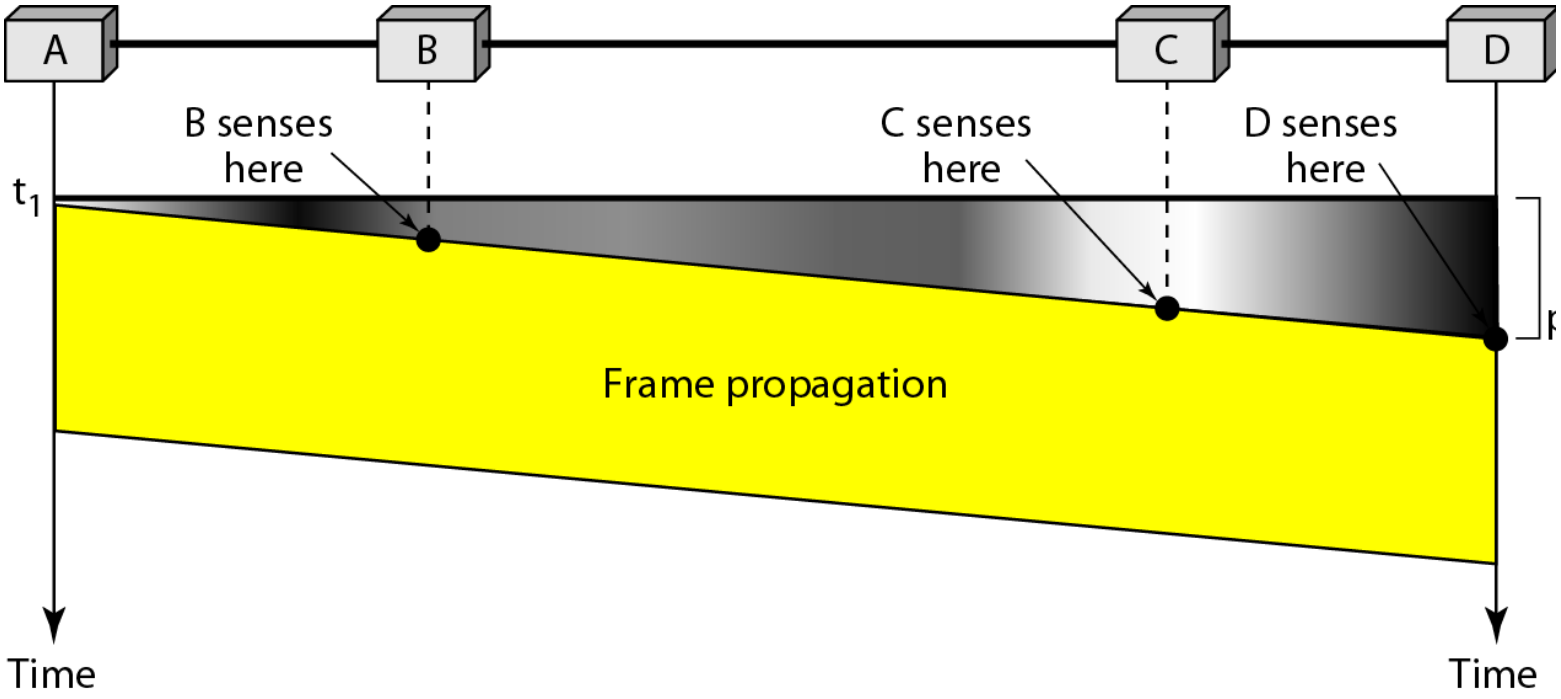
Flow diagram for three persistence methods



Flow diagram for three persistence methods

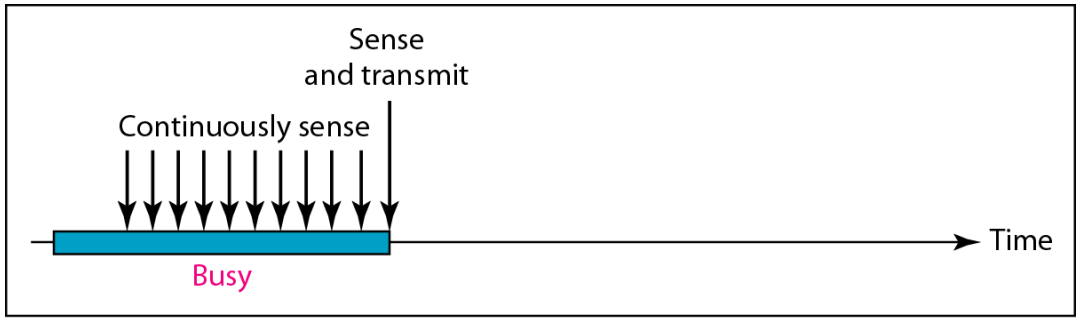


Vulnerable time in CSMA

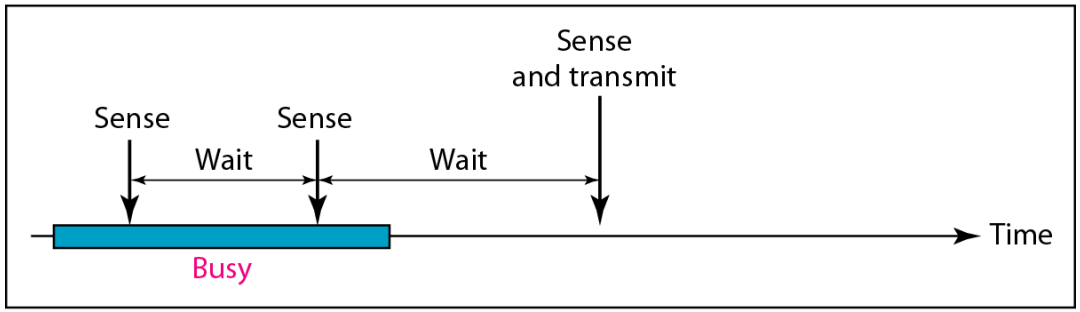


Vulnerable time = propagation time

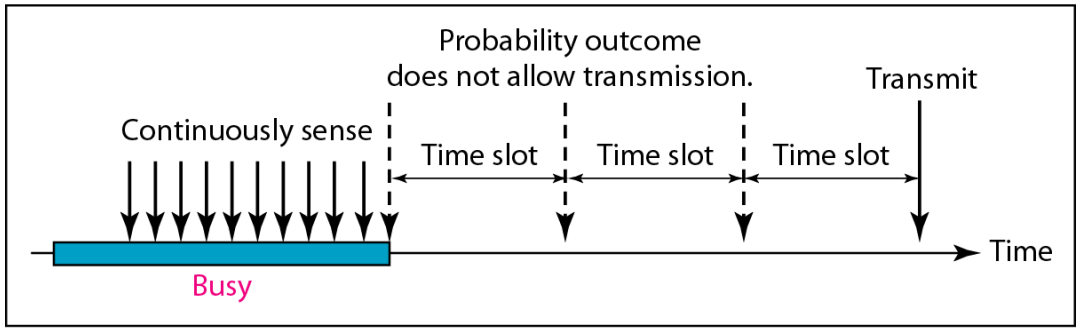
Behavior of three persistence methods



a. 1-persistent

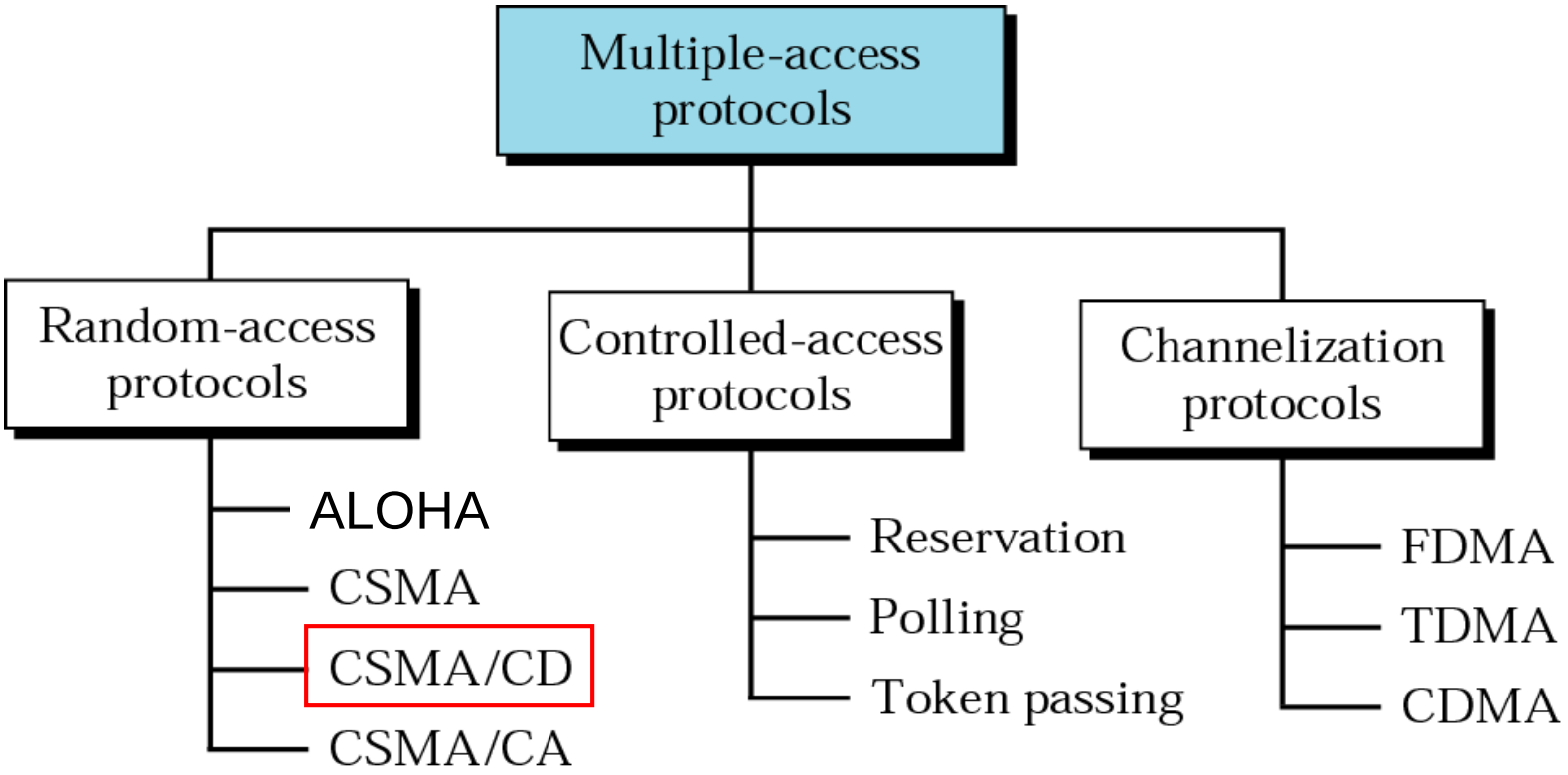


b. Nonpersistent

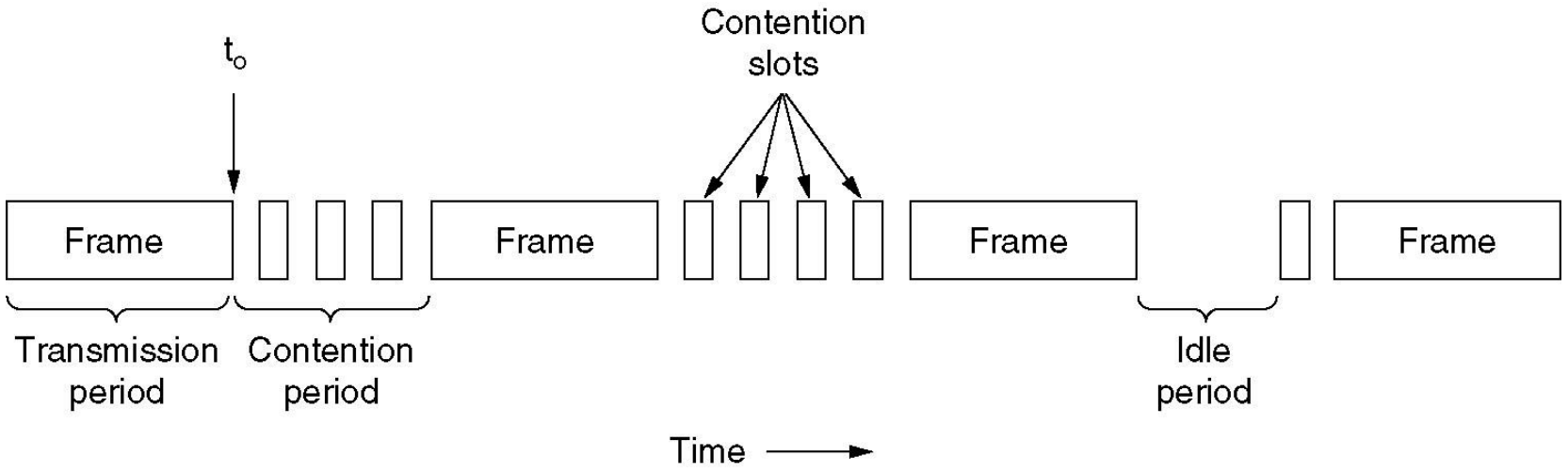


c. p-persistent

Multiple Access Protocols



CSMA with Collision Detection (CSMA/CD)



CSMA/CD can be in one of the three states: contention, transmission, or idle.
Example of CSMA/CD: Ethernet

How long does it take before stations realize that there has been a collision?

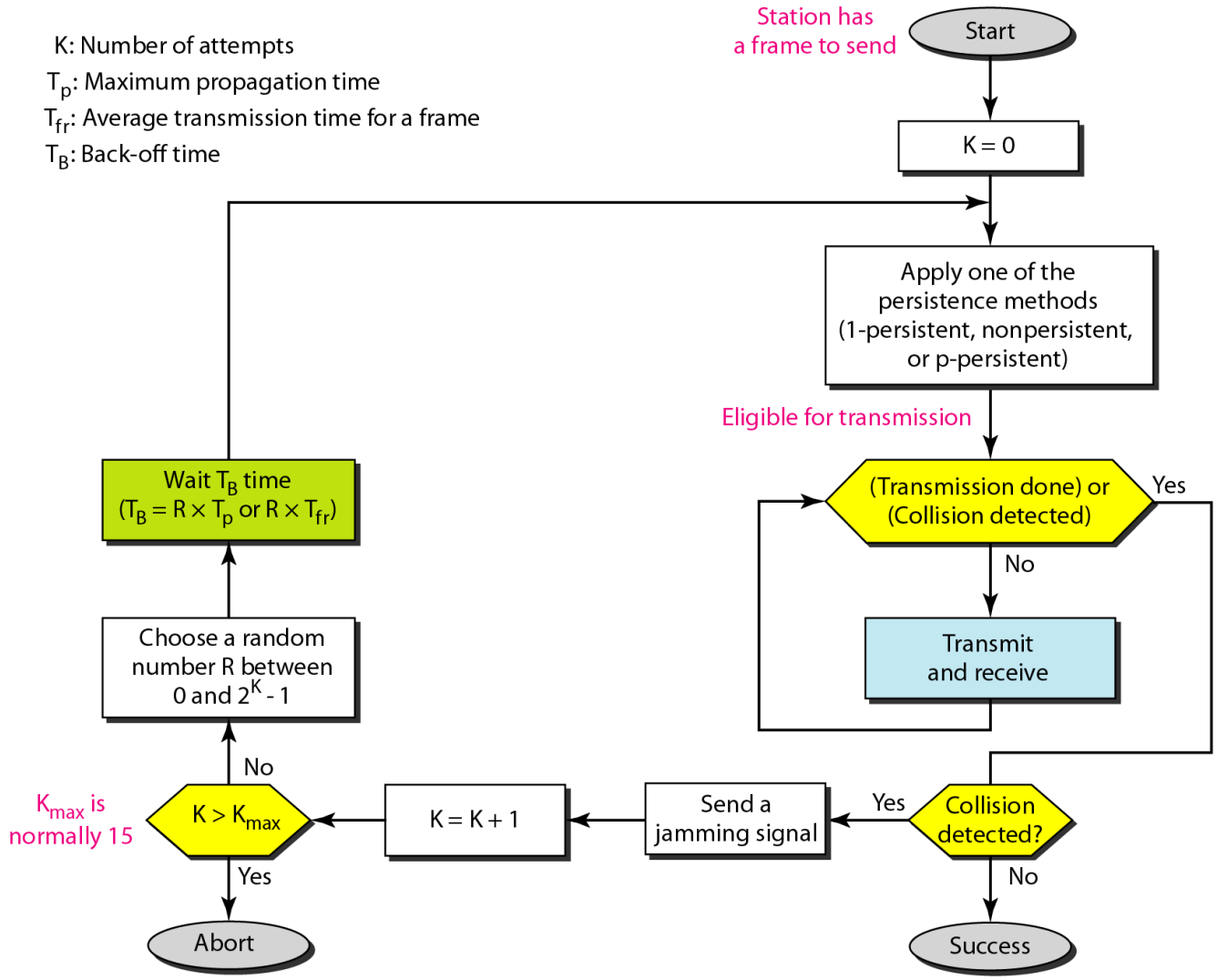
Collision Detection

How the station detects a collision?
There are many collision detection methods!
Most of them are analog processes.

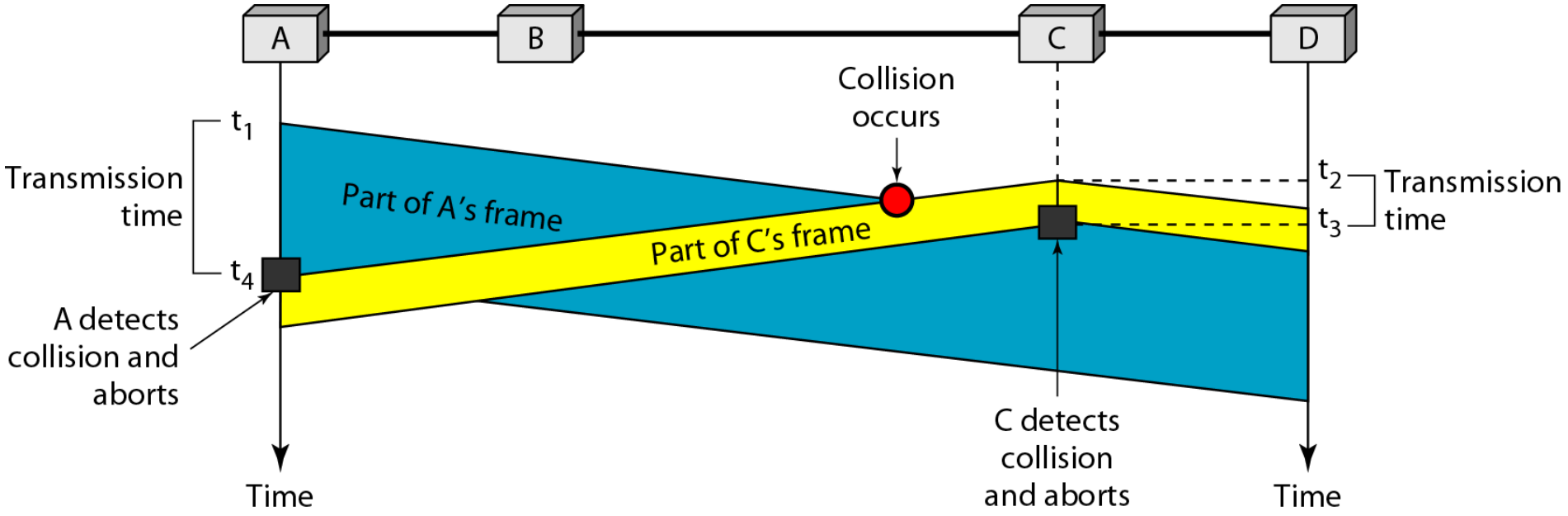
Examples:

- detecting voltage level on the line
- detecting power level
- detecting simultaneous transmission & reception

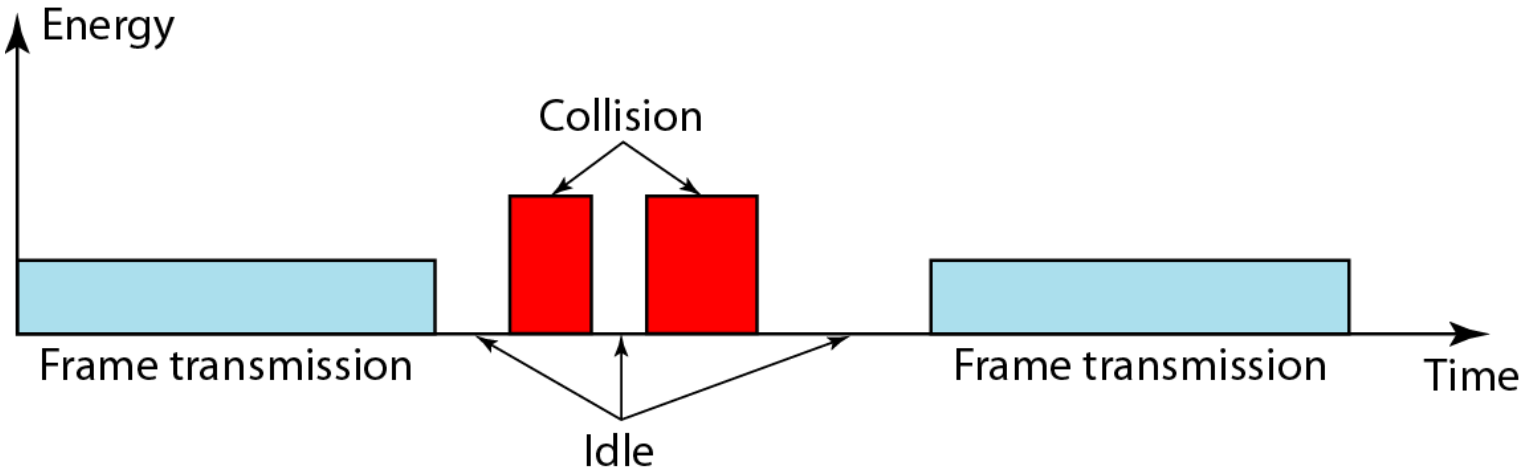
Flow diagram for the CSMA/CD



Collision and abortion in CSMA/CD



Energy level during transmission, idleness, or collision



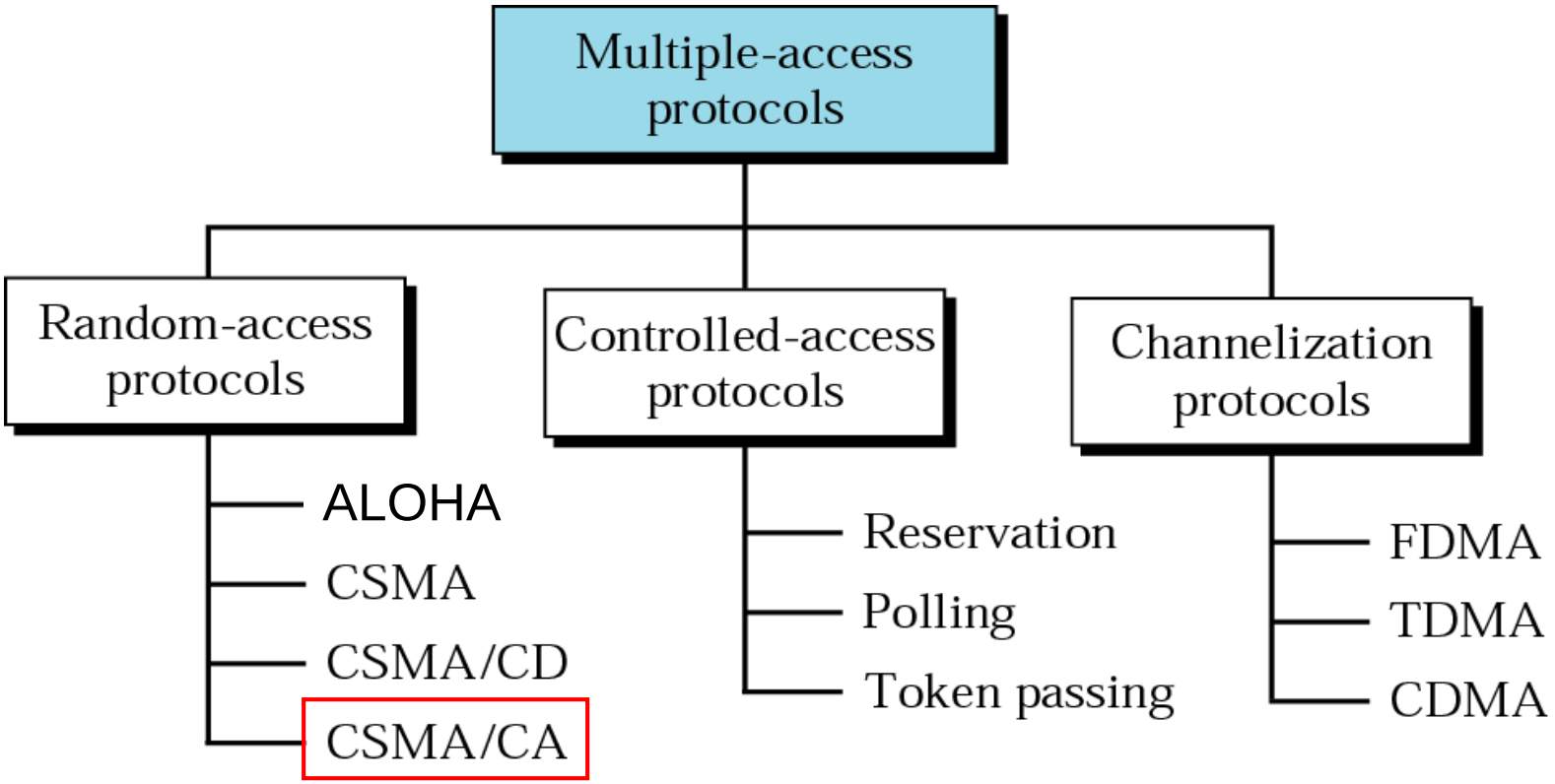
Example 5

A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 μs, what is the minimum size of the frame?

Solution

The frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame for Standard Ethernet.

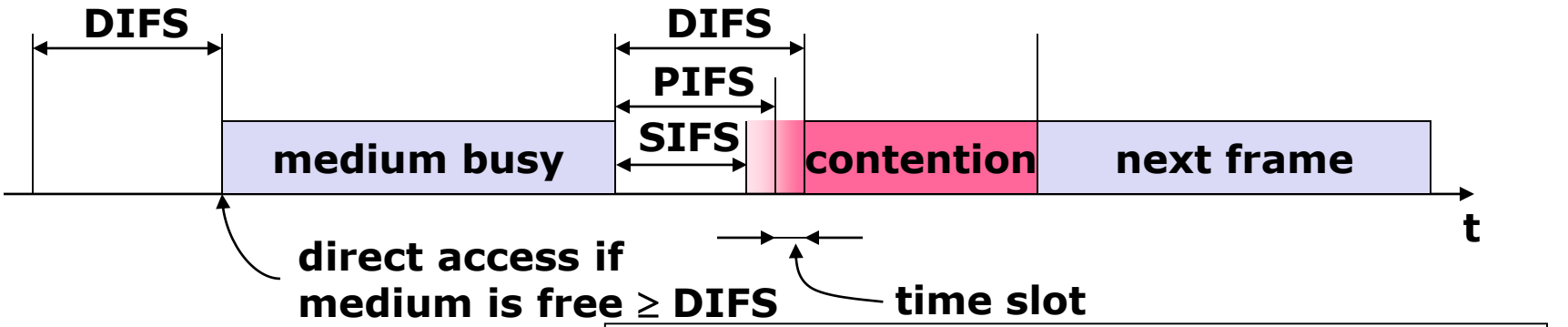
Multiple Access Protocols



CSMA/CA

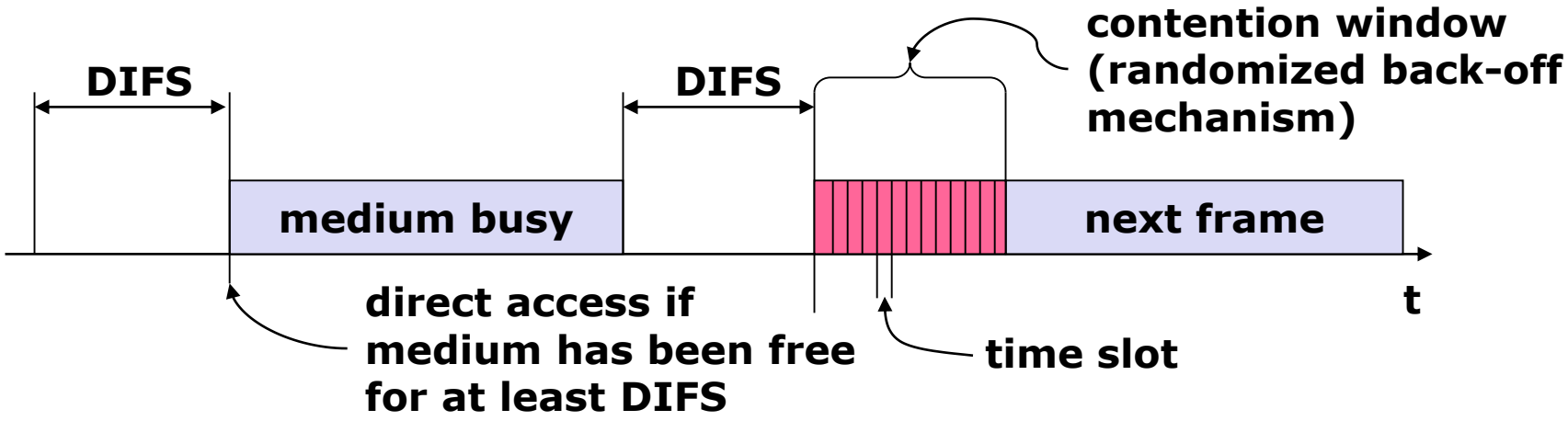
CSMA/CA - MAC layer principles

- **Priorities**
  - **defined through different inter frame spaces**
  - **no guaranteed, hard priorities**
  - **SIFS (Short Inter Frame Spacing)**
    - **highest priority, for ACK, CTS, polling response**
  - **PIFS (PCF IFS)**
    - **medium priority, for time-bounded service using PCF**
  - **DIFS (DCF, Distributed Coordination Function IFS)**
    - **lowest priority, for asynchronous data service**



Note : IFS durations are specific to each PHY

802.11 - CSMA/CA principles

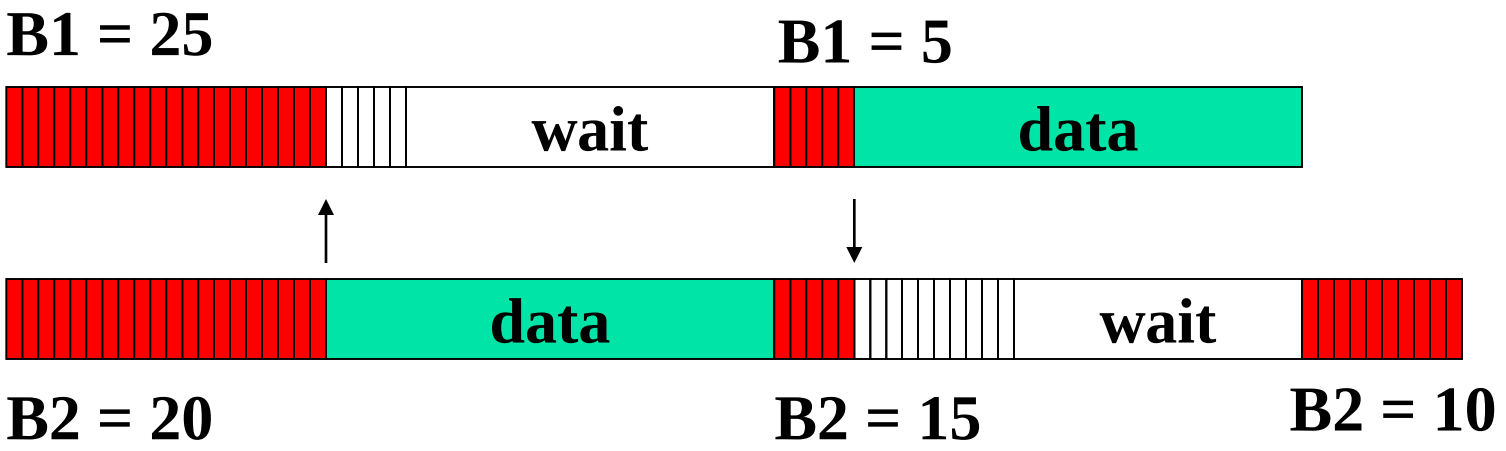


- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (to increase fairness)

Random Contention Access

- Slotted contention period
  - Used by all carrier sense variants
  - Provides random access to the channel
- Operation
  - Each node selects a random back off number
  - Waits that number of slots monitoring the channel
  - If channel stays idle and reaches zero then transmit
  - If channel becomes active wait until transmission is over then start counting again

DCF Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

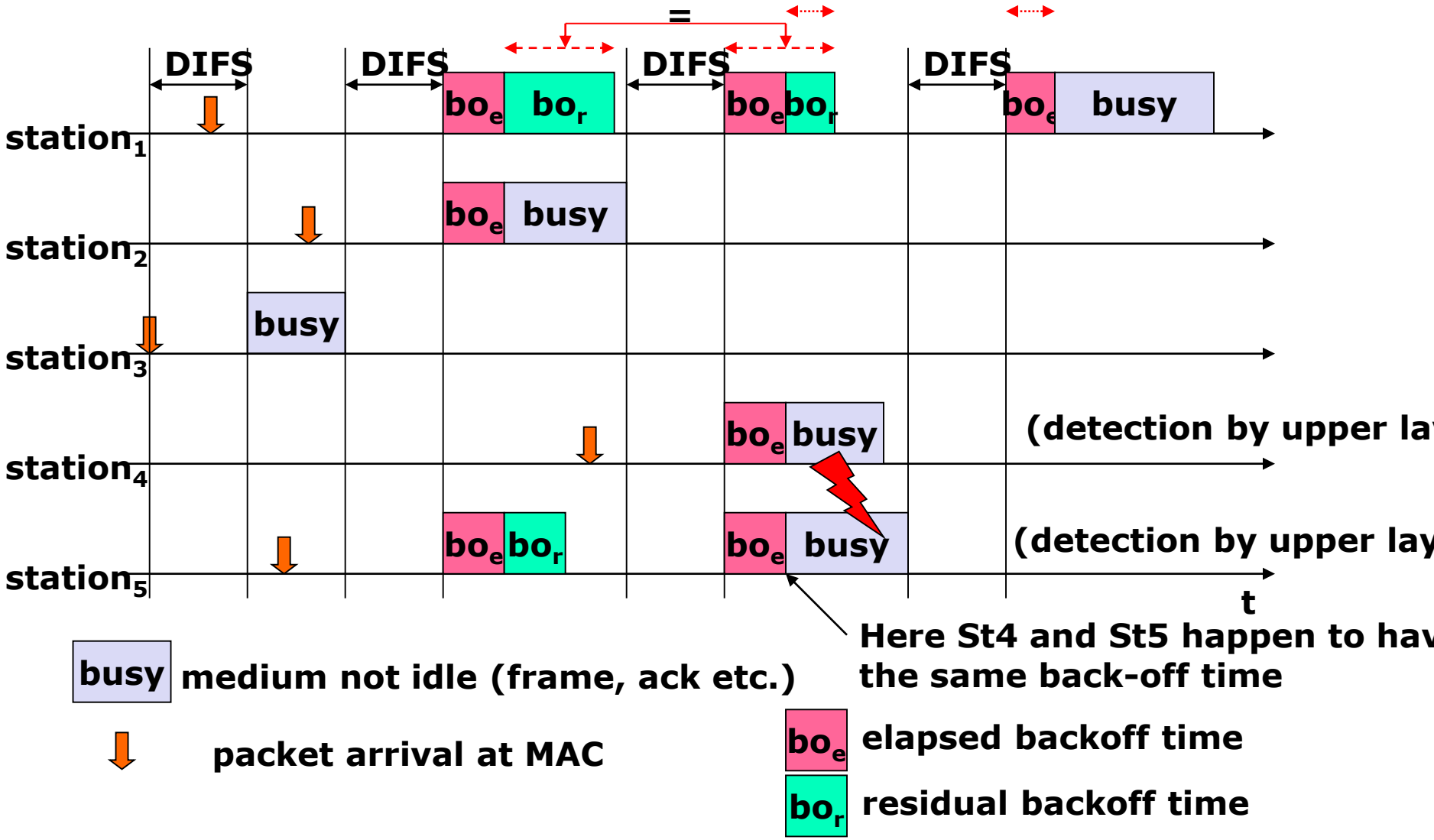
Contention Window

- Random number selected from [0,cw]
- Small value for cw
  - Less wasted idle slots time
  - Large number of collisions with multiple senders (two or more stations reach zero at once)
- Optimal cw for known number of contenders & know packet size
  - Computed by minimizing expected time wastage (by both collisions and empty slots)
  - Tricky to implement because number of contenders is difficult to estimate and can be VERY dynamic

Adaptive Contention Window

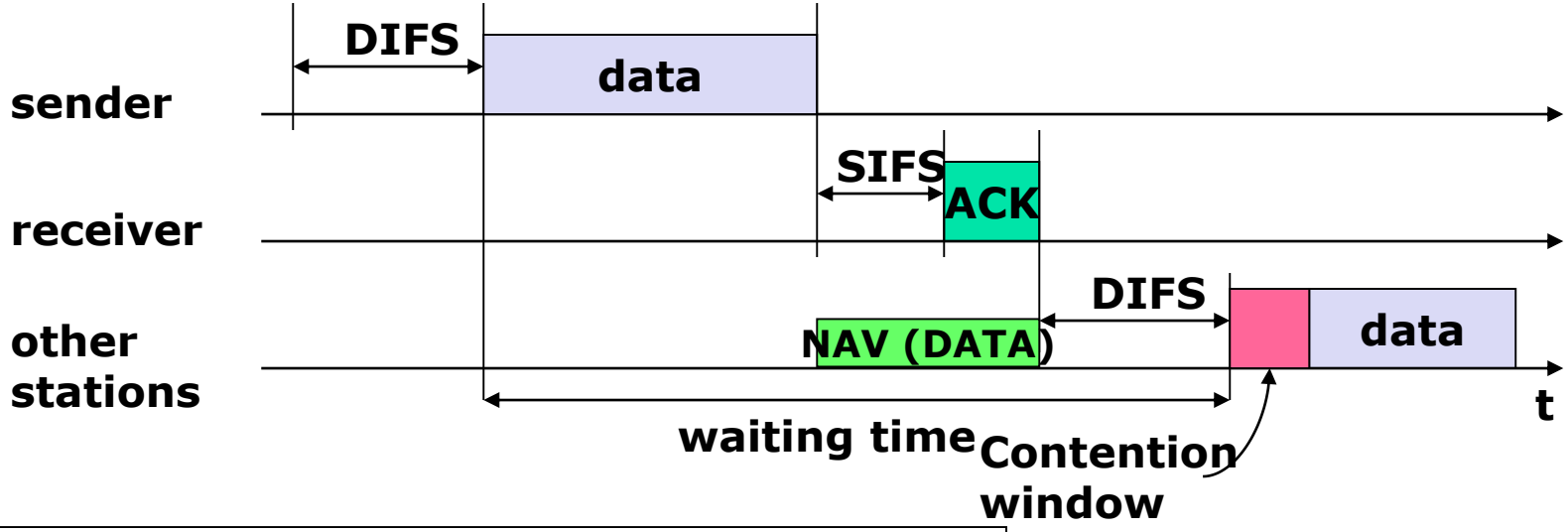
- 802.11 adaptively sets cw
  - Starts with cw = 31
  - If no CTS or ACK then increase to 2*cw+1 (63, 127, 255)
  - Reset to 31 on successful transmission
- 802.11 adaptive scheme is unfair
  - Under contention, unlucky nodes will use larger cw than lucky nodes (due to straight reset after a success)
  - Lucky nodes may be able to transmit several packets while unlucky nodes are counting down for access
- Fair schemes should use same cw for all contending nodes (better for high congestion too)

802.11 – CSMA/CA broadcast



802.11 - CSMA/CA unicast

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receiver acknowledges at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



The ACK is sent right at the end of SIFS (no contention)

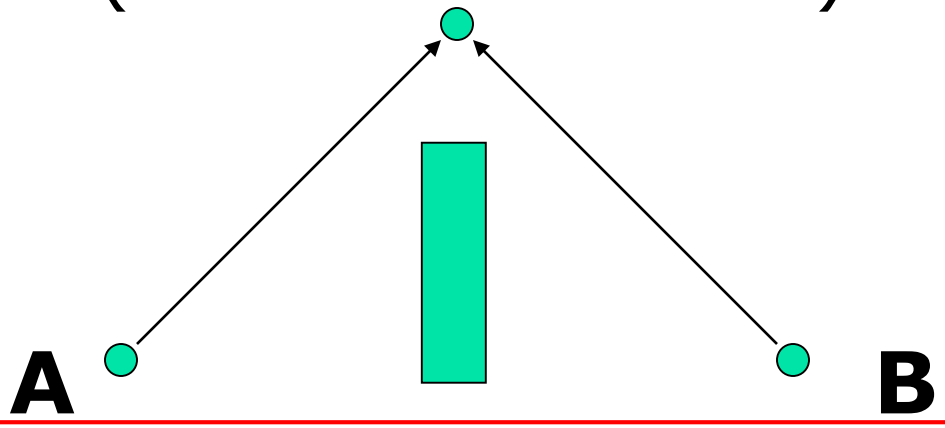
NAV: Net Allocation Vector

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

- Procedure
  - Similar to CSMA but instead of sending packets control frames are exchanged
  - RTS = request to send
  - CTS = clear to send
  - DATA = actual packet
  - ACK = acknowledgement

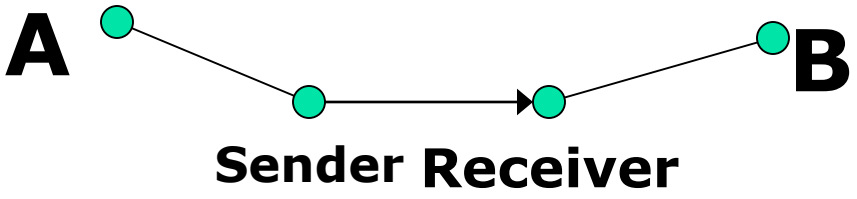
Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

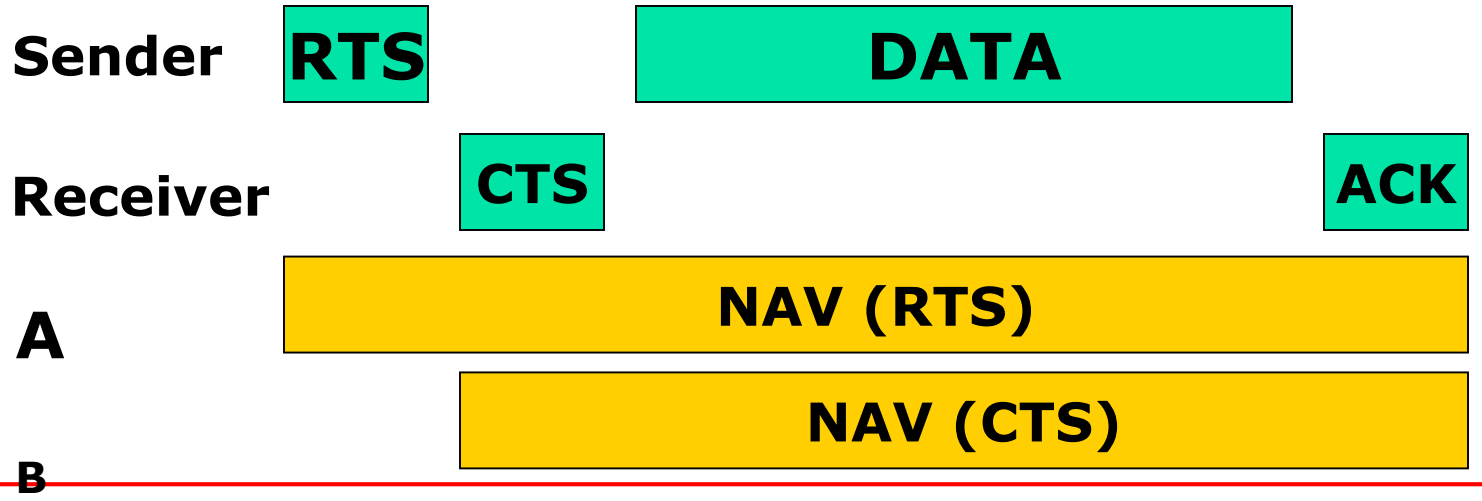
- Advantages
  - Small control frames lessen the cost of collisions (when data is large)
  - RTS + CTS provide "virtual" carrier sense which protects against hidden terminal collisions (where A can't hear B)



802.11 DCF (CSMA-CA)

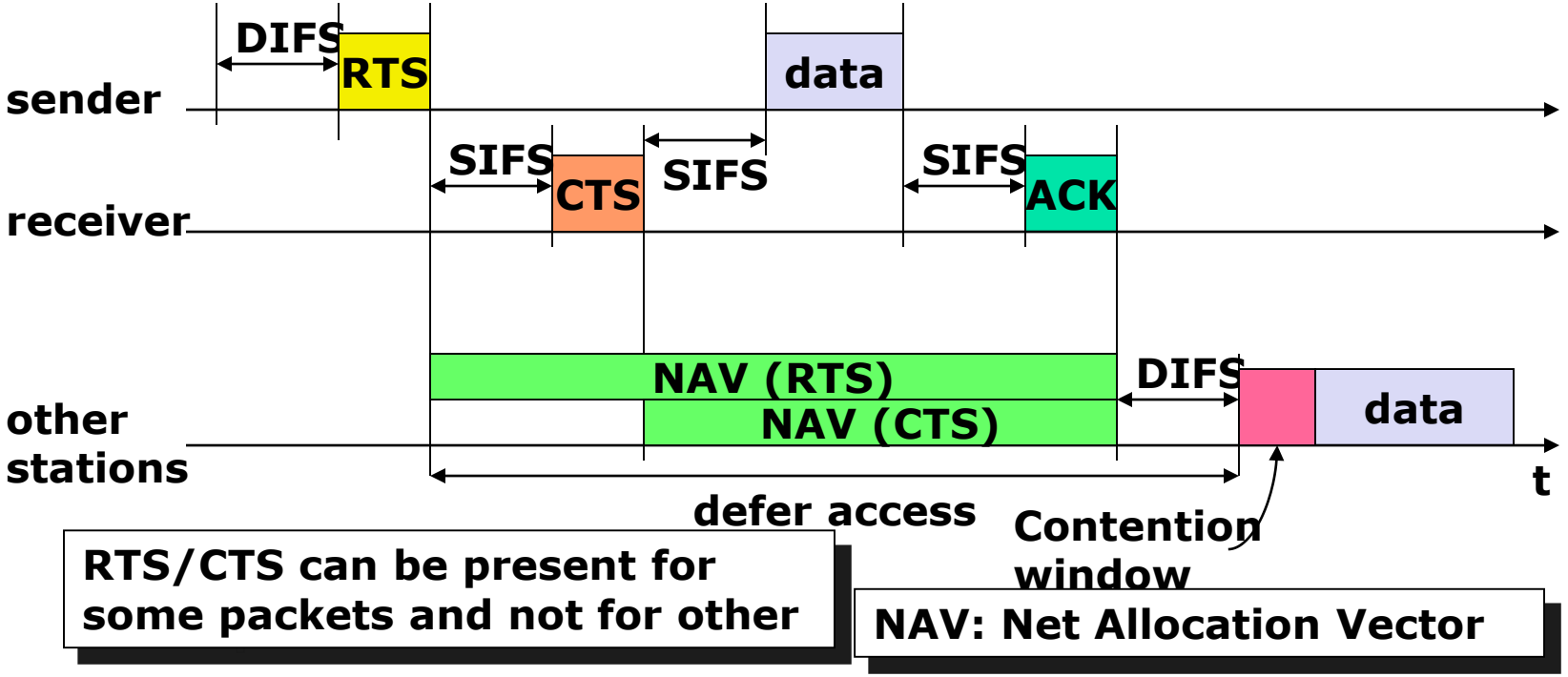
- Full exchange with "virtual" carrier sense (called the Network Allocation Vector)





802.11 – DCF with RTS/CTS

- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement via ACK
  - other stations store medium reservations distributed via RTS and CTS

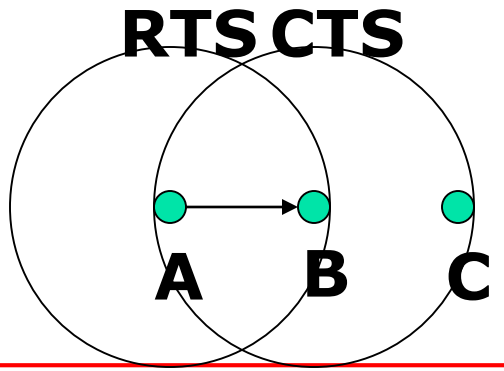


Carrier Sense Multiple Access (CSMA)

- Procedure
  - Listen to medium and wait until it is free (no one else is talking)
  - Wait a random back off time then start talking
- Advantages
  - Fairly simple to implement
  - Functional scheme that works
- Disadvantages
  - Can not recover from a collision (inefficient waste of medium time)

Virtual Carrier Sense

- Provided by RTS & CTS
- Designed to protect against hidden terminal collisions (when C can't receive from A and might start transmitting)
- However this is unnecessary most of the time due to physical carrier sense



Lecture 3

Controlled Access Protocols

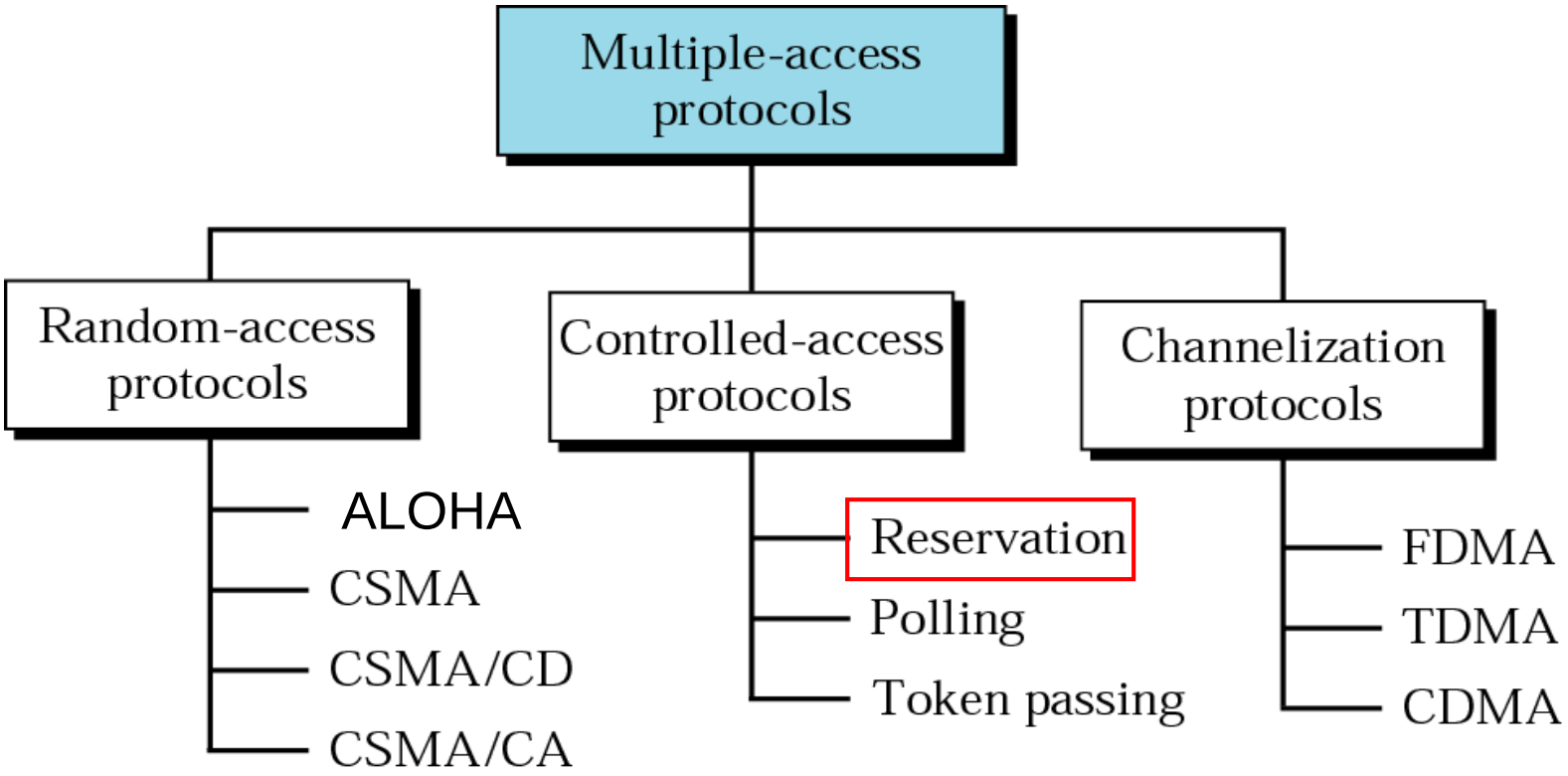
2- CONTROLLED ACCESS

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. We discuss three popular controlled-access methods.

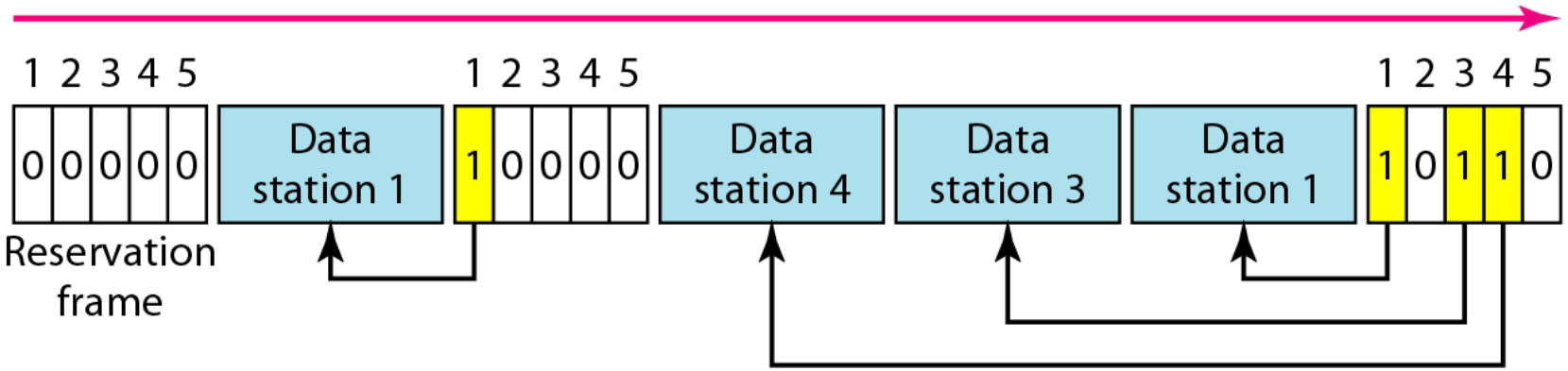
Topics discussed in this section:

- Reservation
- Polling
- Token Passing

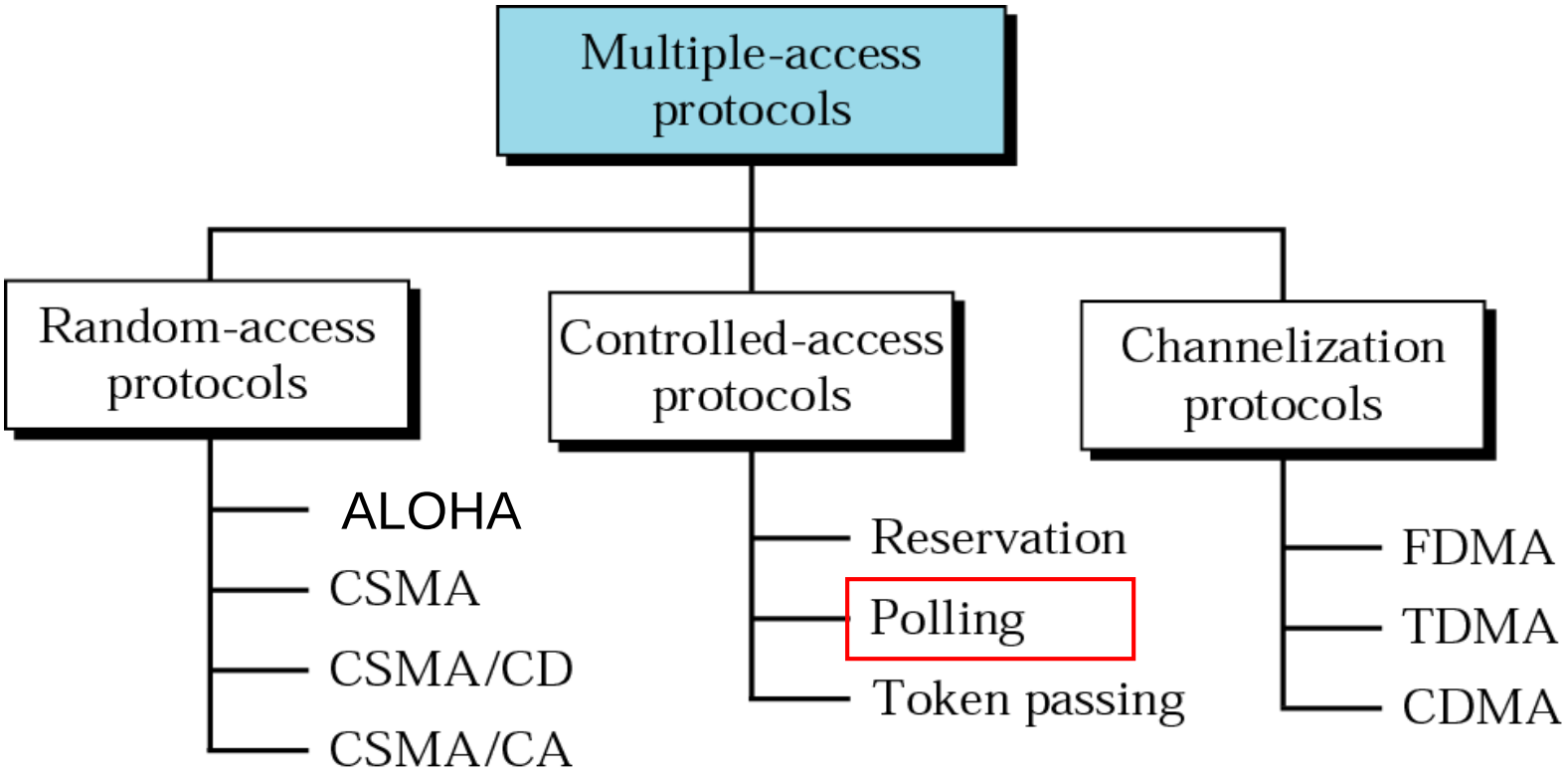
Multiple Access Protocols



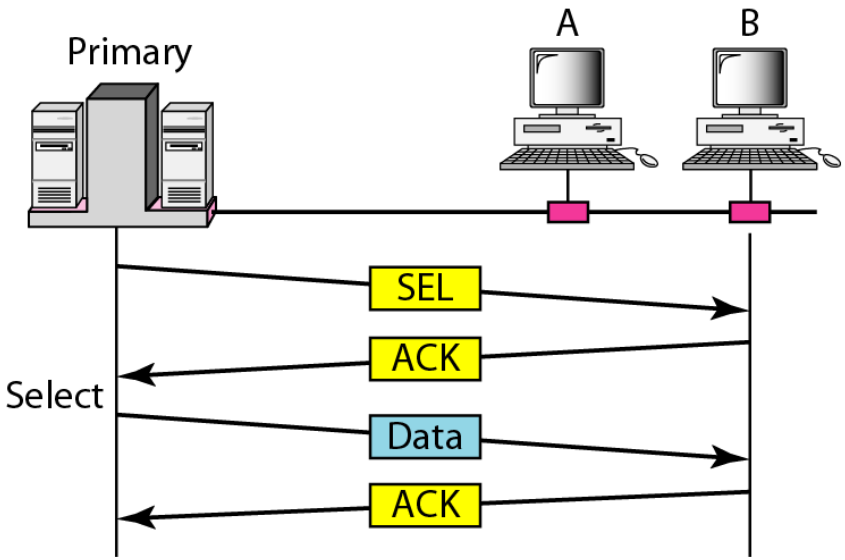
Reservation access method

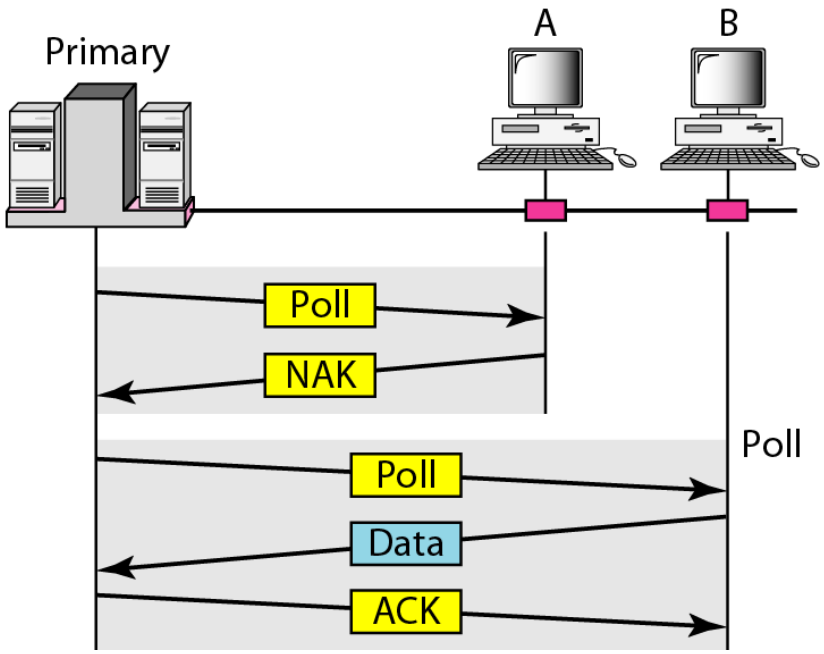


Multiple Access Protocols

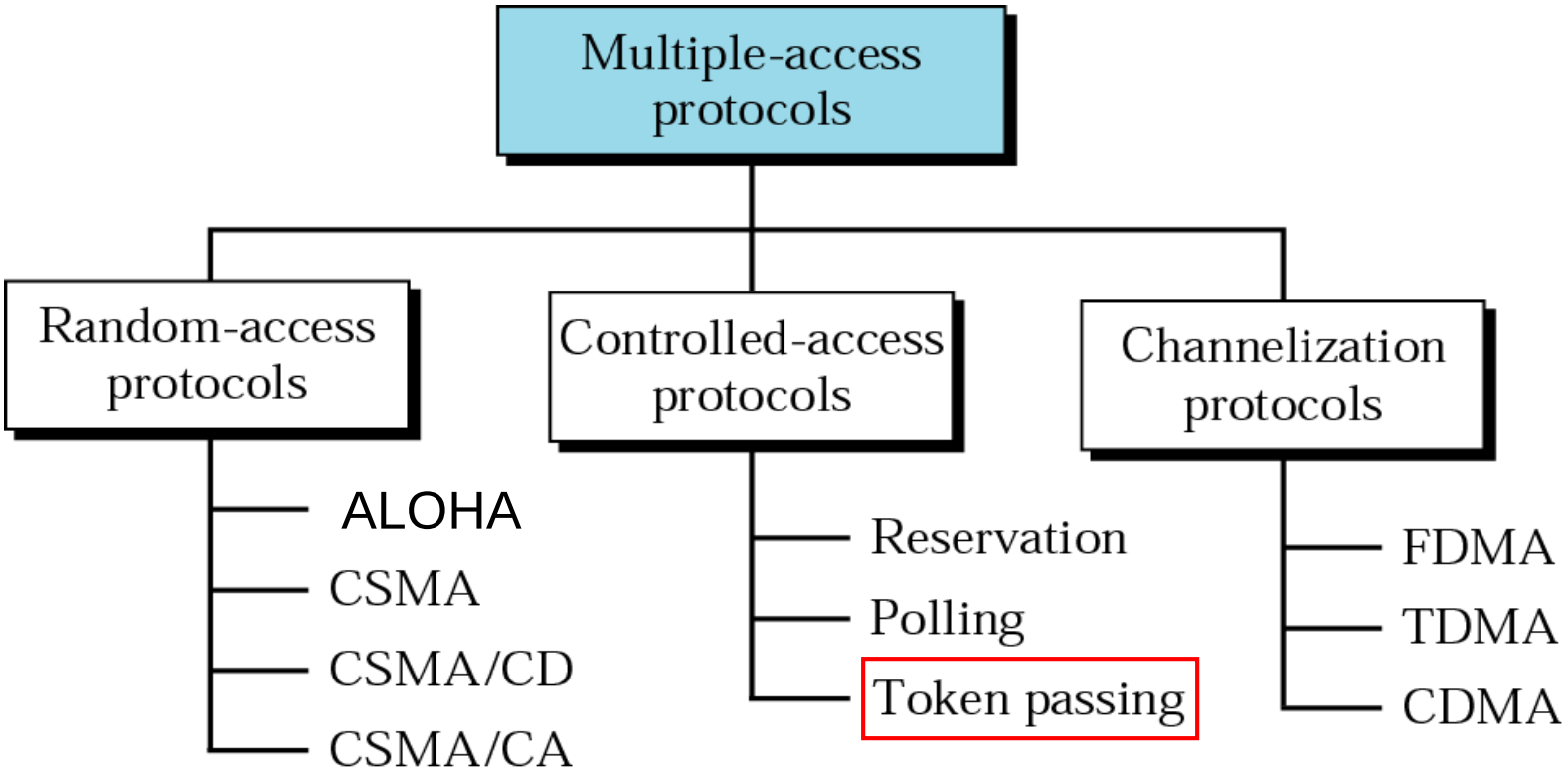


Select and poll functions in polling access method

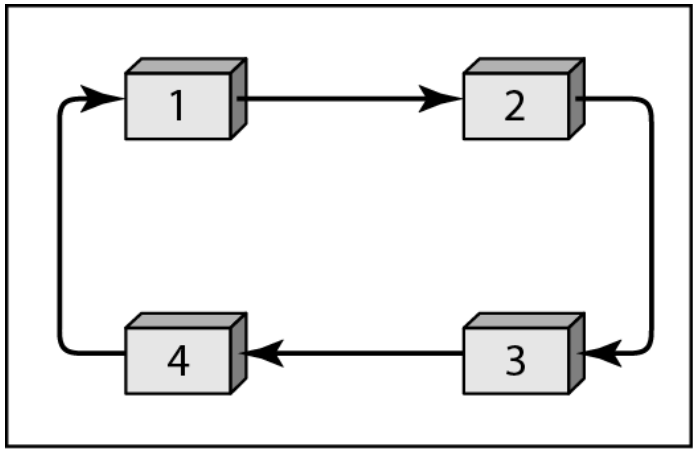




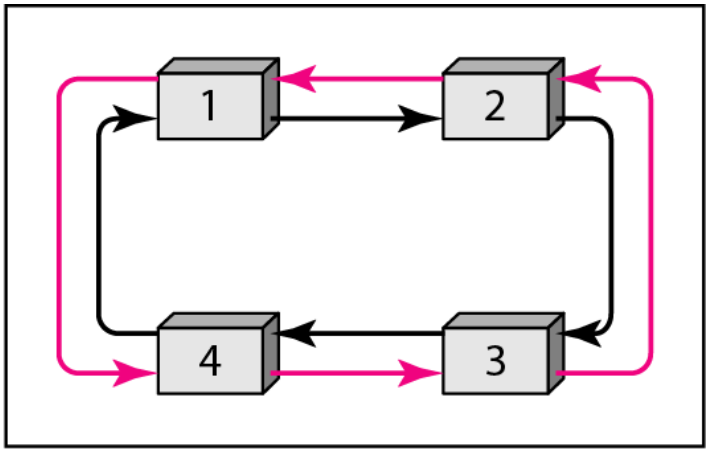
Multiple Access Protocols



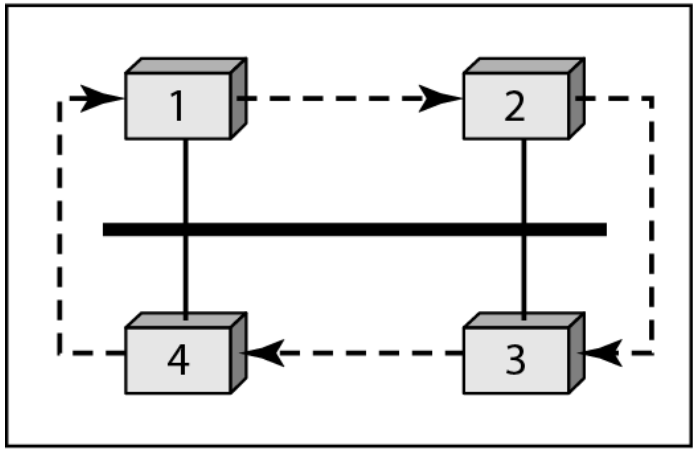
Logical ring and physical topology in token-passing access method



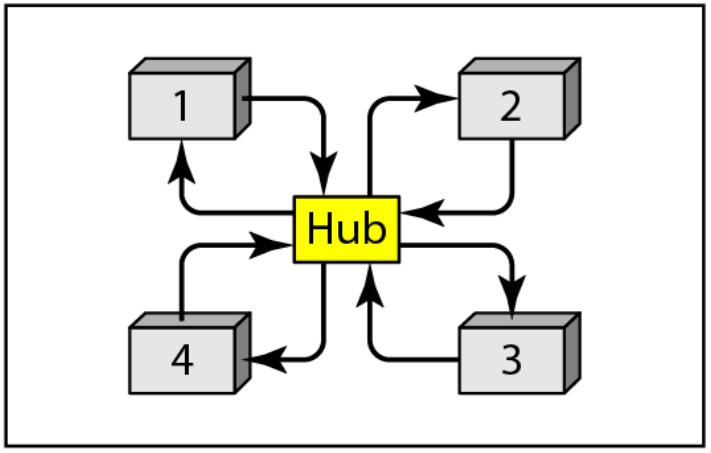
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

Lecture 4

Channelization Protocols

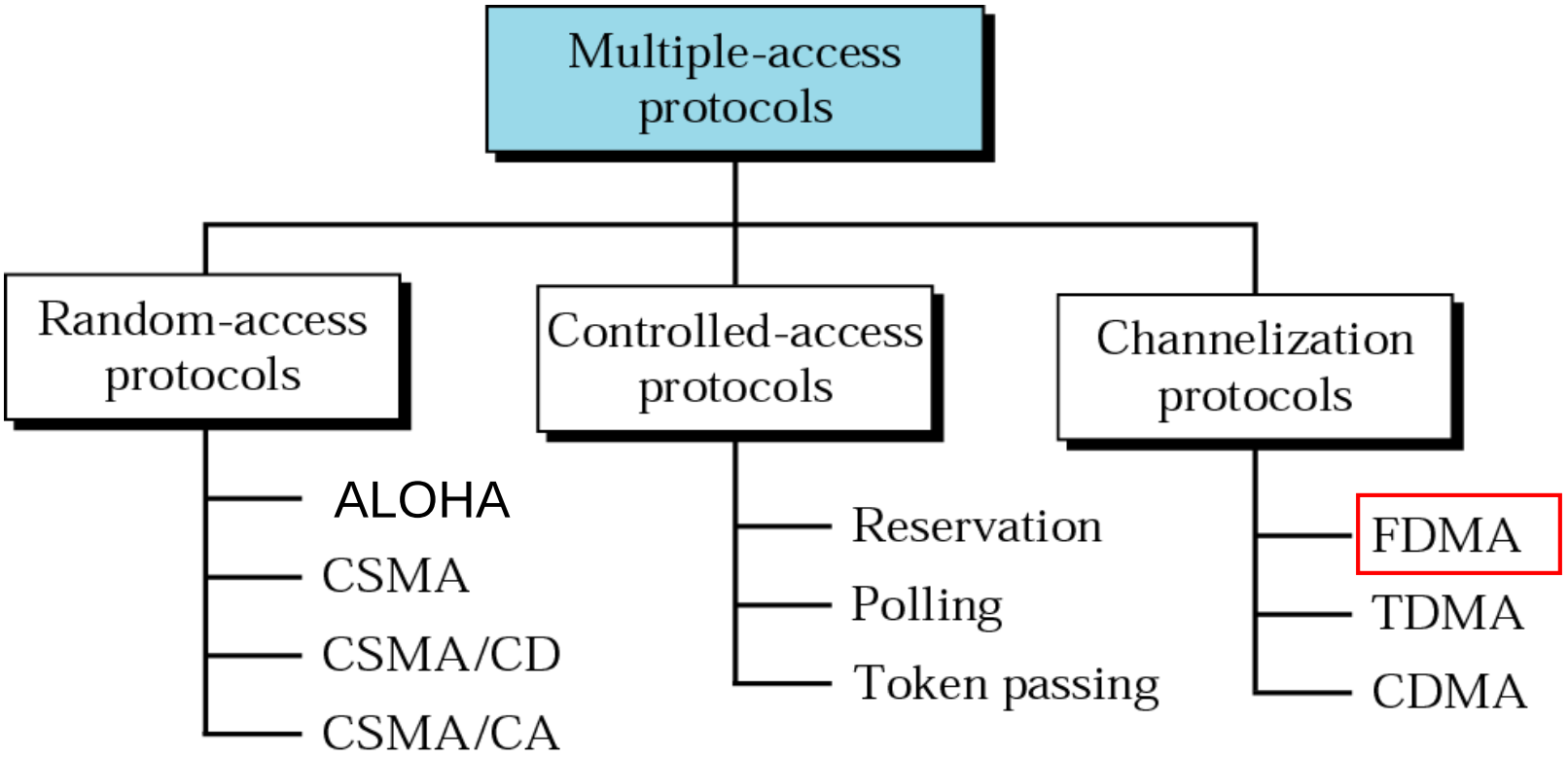
3- CHANNELIZATION

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. In this section, we discuss three channelization protocols.

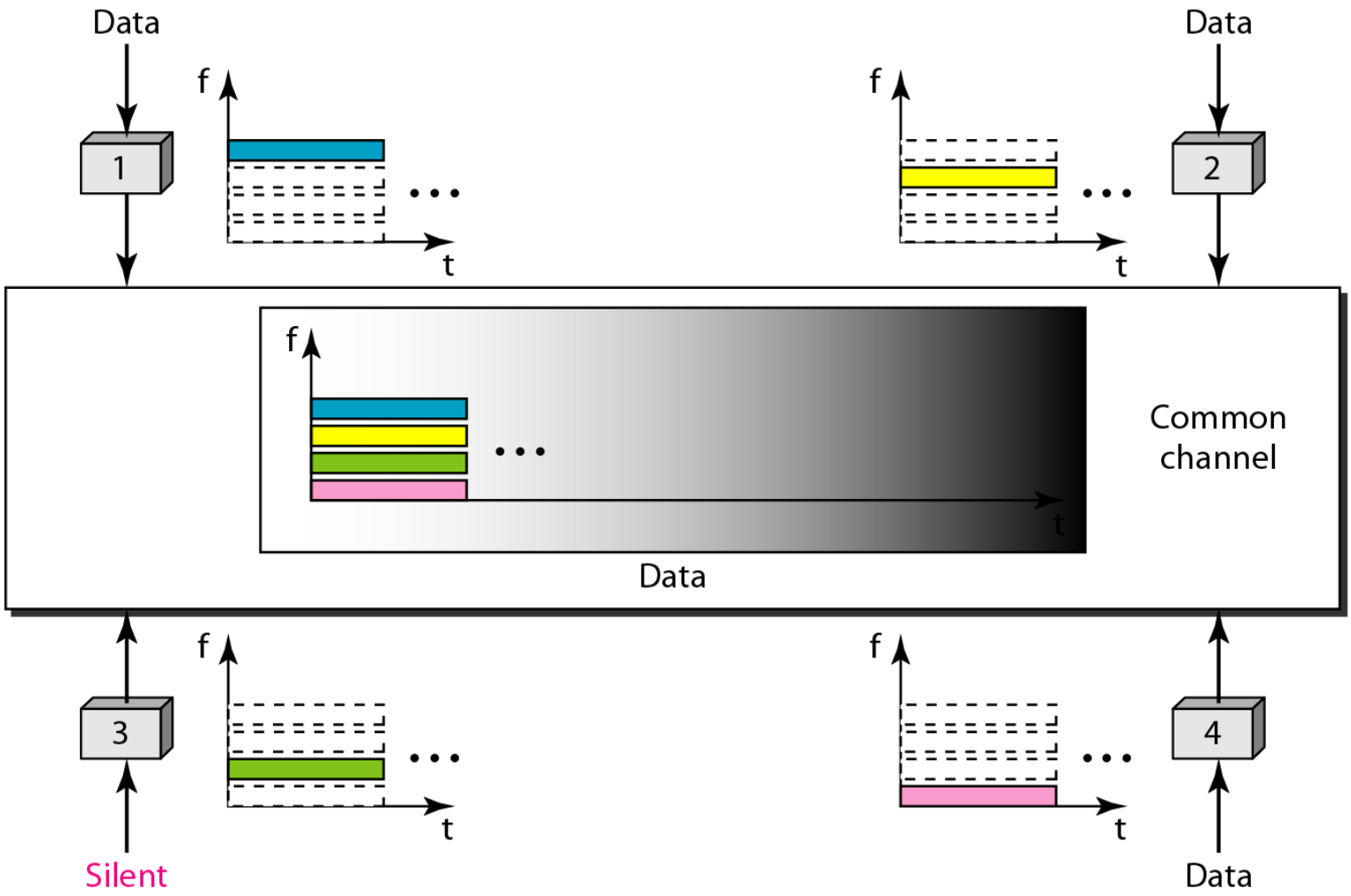
Topics discussed in this section:

- Frequency-Division Multiple Access (FDMA)
- Time-Division Multiple Access (TDMA)
- Code-Division Multiple Access (CDMA)

Multiple Access Protocols



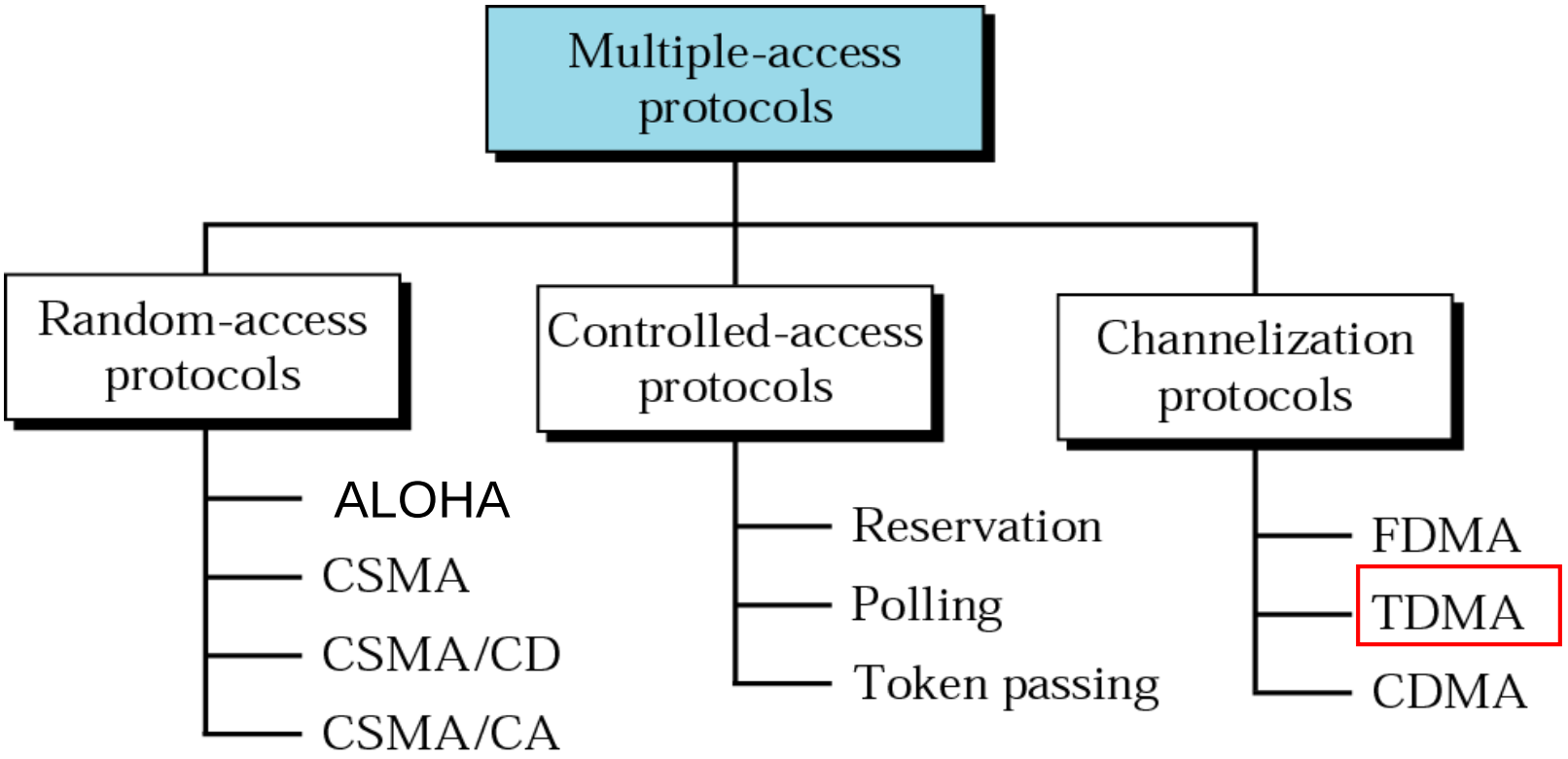
Frequency-division multiple access (FDMA)



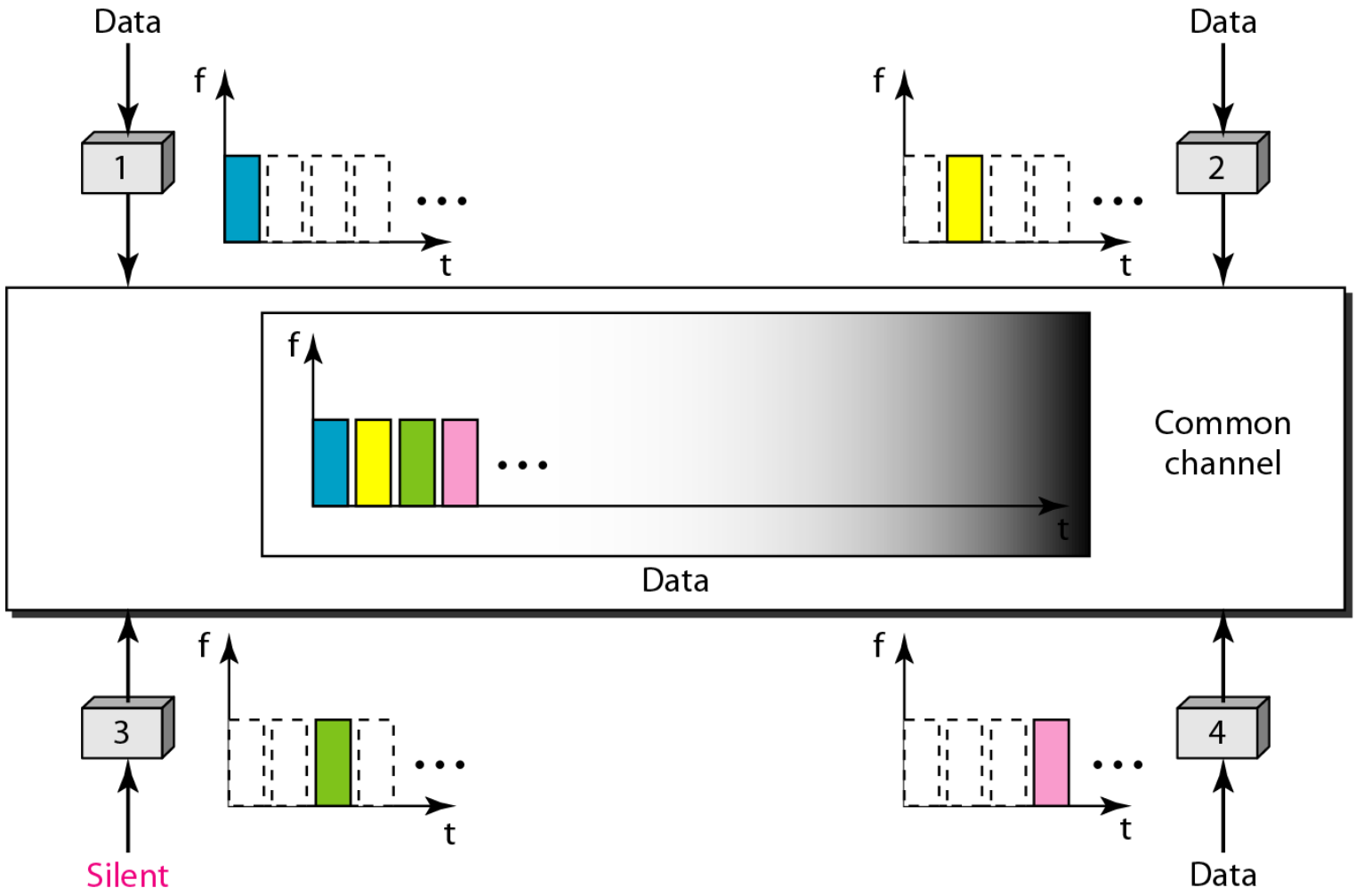
Frequency-Division Multiple Access (FDMA)

In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.

Multiple Access Protocols



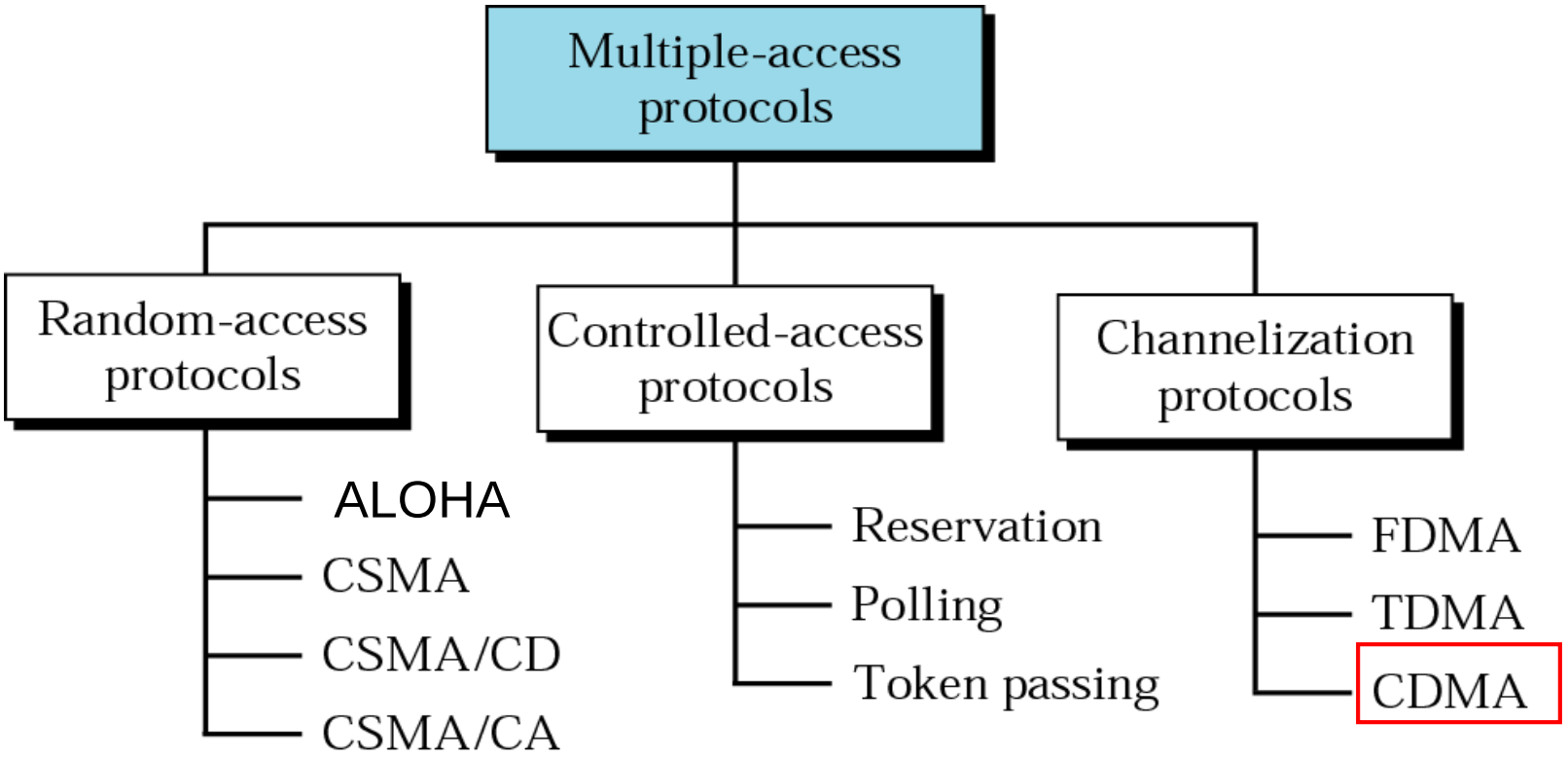
Time-division multiple access (TDMA)



Time-Division Multiple Access (TDMA)

In TDMA, the bandwidth is just one channel that is timeshared between different stations.

Multiple Access Protocols

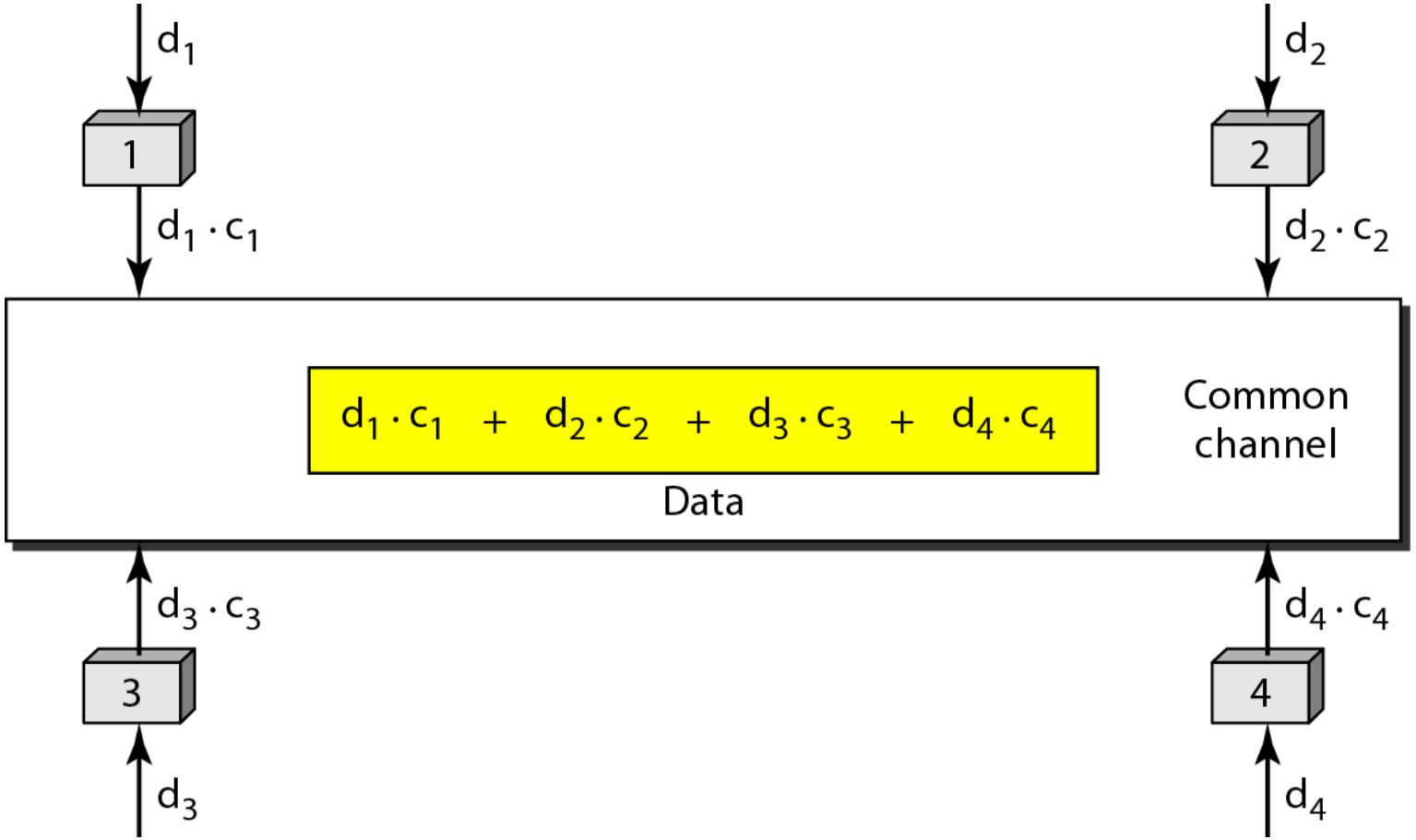


Code-Division Multiple Access (CDMA)

In CDMA, one channel carries all transmissions simultaneously.

Code-Division Multiple Access (CDMA)

Simple idea of communication with code

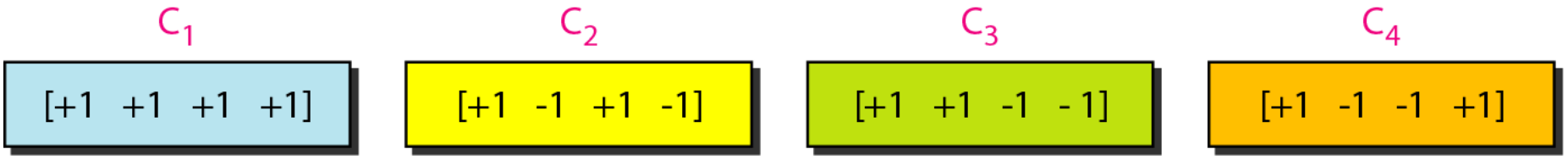


Code-Division Multiple Access (CDMA)

$C_x * C_y = 0$

$C_x * C_x = N$

Example: **Chip sequences**



Lecture 5

Local Area Network (Ethernet)

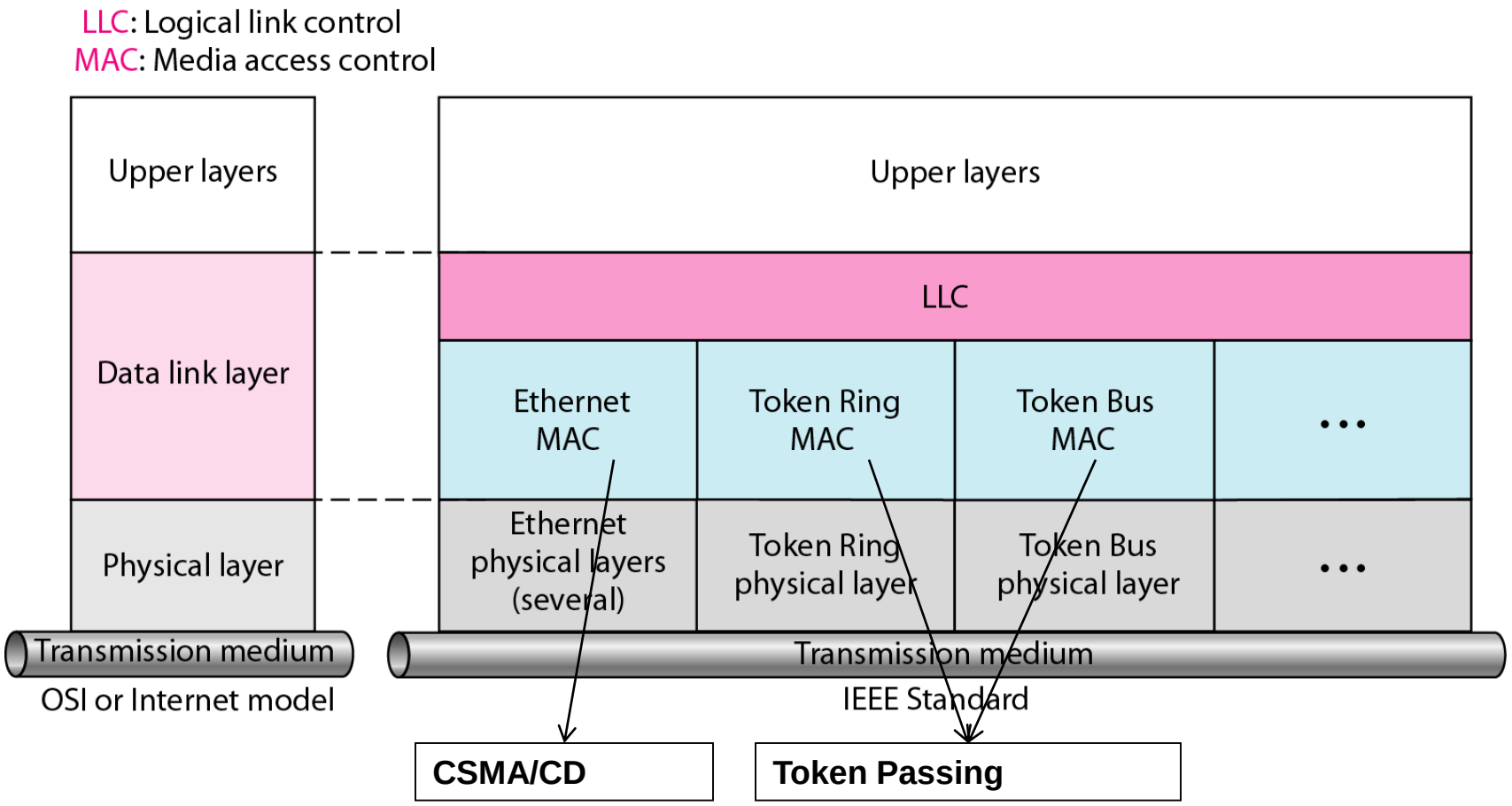
IEEE Standards

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

Topics discussed in this section:

Data Link Layer (LLC and MAC)
Framing
Physical Layer

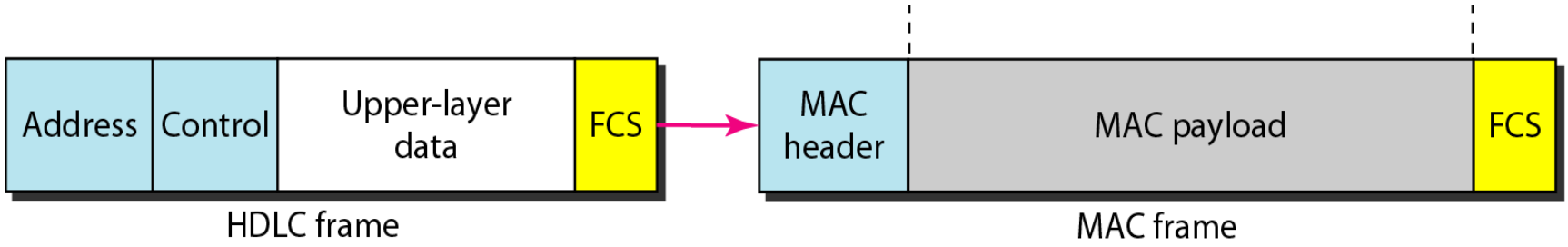
IEEE standard for LANs



IEEE 802 Series of LAN Standards

name	description
IEEE 802.3	Ethernet
IEEE 802.4	Token bus
IEEE 802.11 a/b/g/n	Wireless LAN & Mesh (Wi-Fi certification)
IEEE 802.15.1	Bluetooth
IEEE 802.16	Broadband Wireless Access (WiMAX certification)

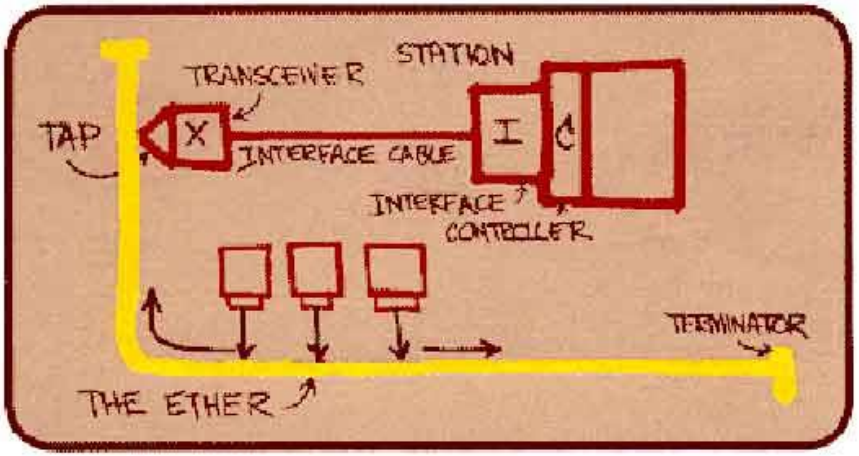
HDLC frame compared with MAC frames



Ethernet

It is the dominant LAN technology.

- **Cheap**
- **First widely used LAN technology**
- **Simpler and cheaper than token LANs**
- **Kept up with speed race: 10, 100, 1000 Mbps**

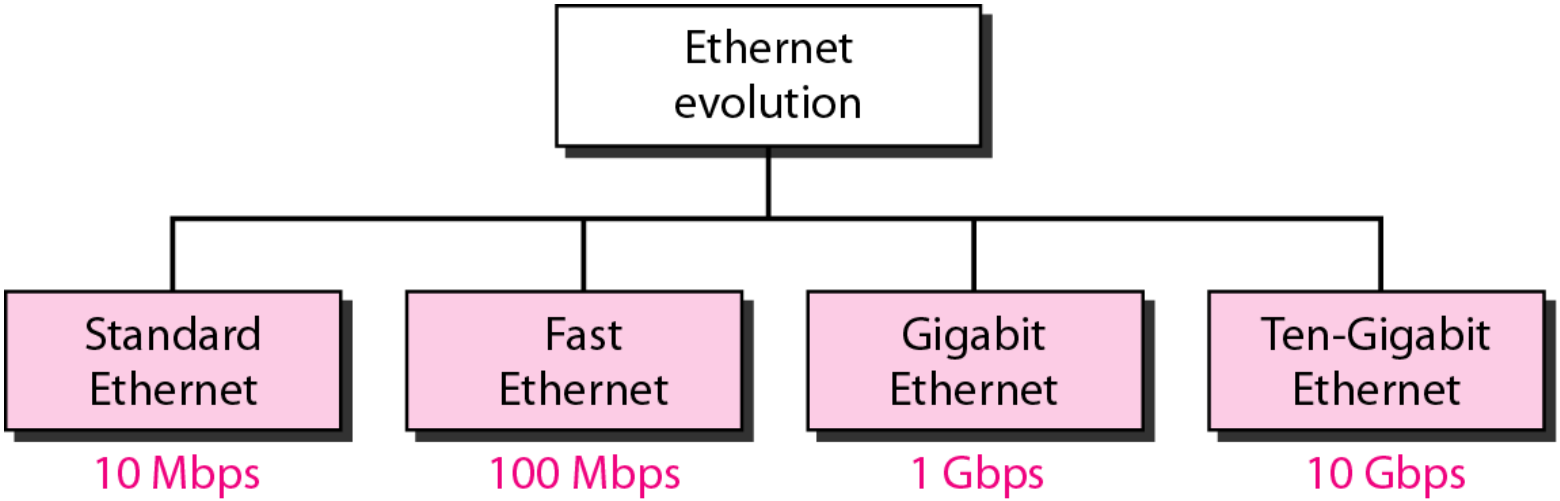


Metcalfe's Ethernet sketch
(http://www.digibarn.com/collections/diagrams/ethernet/index.html)

Physical layer

- Physical layer is dependent on the implementation and type of the physical media used.
- IEEE define detailed specifications for each LAN implementation.
- For example, although there is only one MAC sublayer for Standard Ethernet(CSMA/CD), there is a different physical layer specifications for each
- Ethernet implementations.

Ethernet evolution

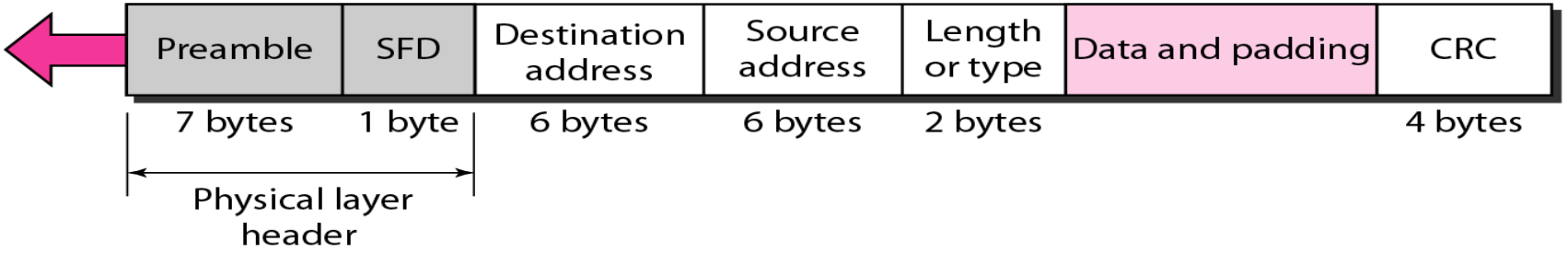


Ethernet Frame Format

- **Sending adapter encapsulates network layer protocol packet such as IP datagram in Ethernet frame**

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

SFD: Start frame delimiter, flag (10101011)



Preamble:

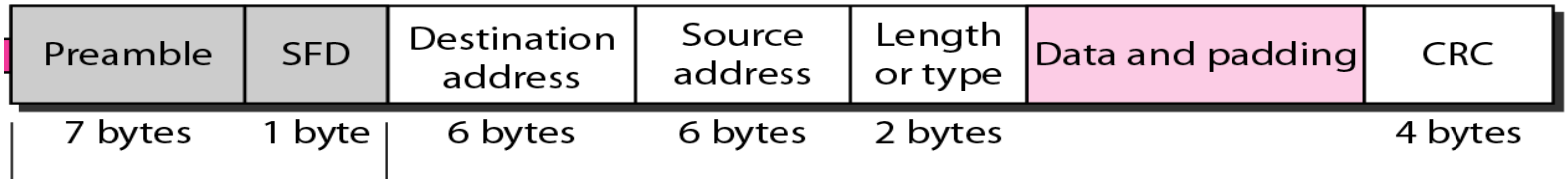
- **7 bytes with pattern 10101010.**
- **Used to synchronize receiver, sender clock rates.**

SFD:

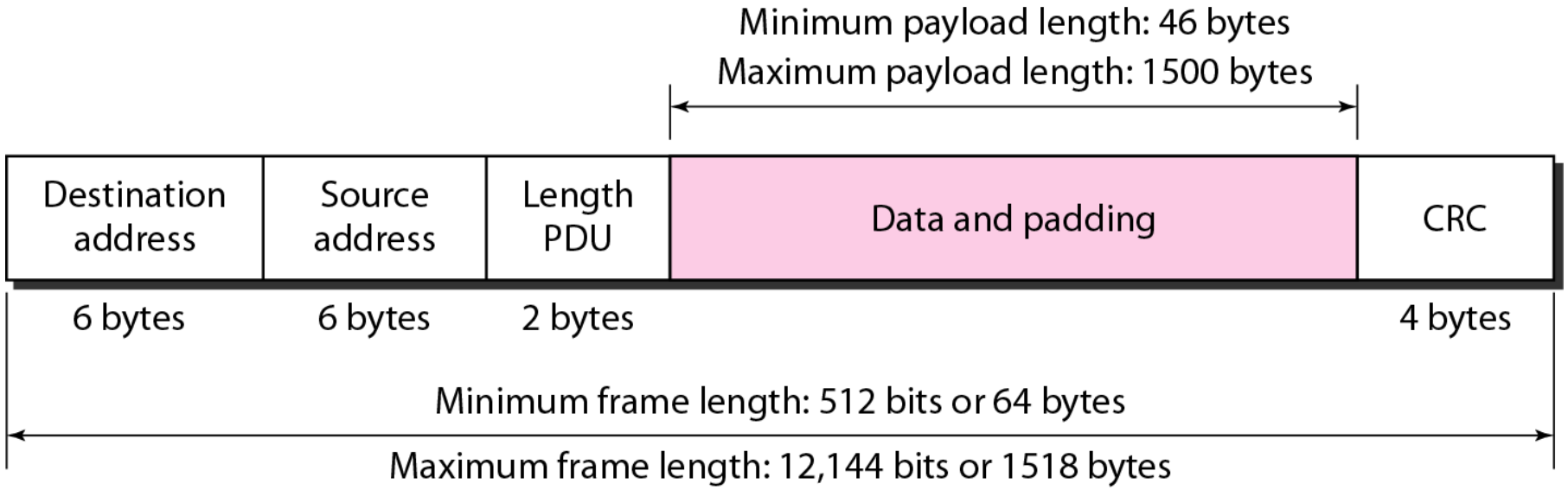
- **One byte with pattern 10101011 to signal the start of the frame.**

Ethernet Frame Format

- **Addresses:** **6 bytes, frame is received by all adapters on a LAN and dropped if address does not match**
- **Length/Type:** **indicates the higher layer protocol or the number of bytes in the data field.**
- **CRC:** **checked at receiver, if error is detected, the frame is simply dropped**



Minimum and Maximum Lengths



Frame length:

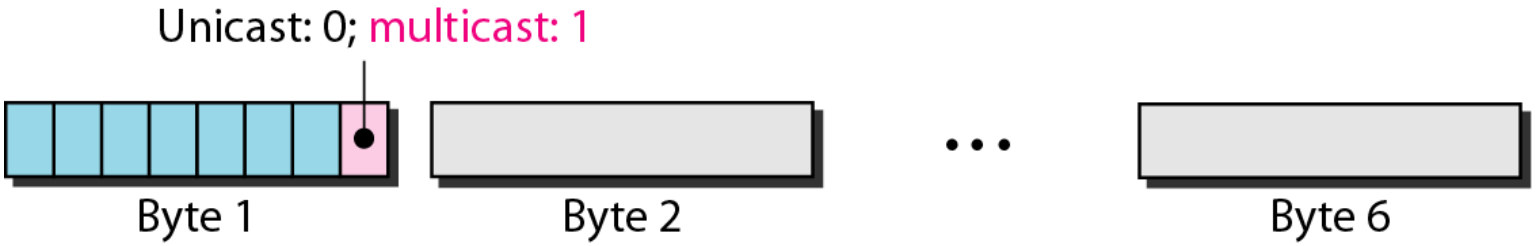
Minimum: 64 bytes (512 bits)

Maximum: 1518 bytes (12,144 bits)

Addressing

Example of an Ethernet address in hexadecimal notation

Unicast and multicast addresses



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 or broadcast.

The broadcast destination address is a special case of the multicast address in which all bits are 1s. (*FF:FF:FF:FF:FF:FF*)

Example 1

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A ***b. 47:20:1B:2E:08:EE***

c. FF:FF:FF:FF:FF:FF

Solution

a. This is a unicast address because A in binary is 1010.

b. This is a multicast address because 7 in binary is 0111.

c. This is a broadcast address because all digits are F's.

Example 2

Show how the address 47:20:1B:2E:08:EE is sent out on line.

Solution

The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit, as shown below:

47→20→1B→2E→08→EE

47 is 0100 0111 ⊂ 1110 0010

Slot time

Access method is CSMA/CD.

- Ethernet dose not provide any mechanism for acknowledging received frames(unreliable medium).
- Acknowledgments must be implemented at the higher layer.

Slot time = round-trip time+ jam sequence time.
It is defined in bits time.
It is the time required for a station to send 512 bits depending on the data rate, for traditional 10-Mbps Ethernet it is 51.2 microseconds.

Max Length = propagation speed * (slot time/2)

Max Length

Max Length = propagation speed * (Slot time/2)

Max Length=$(2 \times 10^{8}) \times (51.2 \times 10^{-6}/2)$=5120 m
Consider the delay times in repeaters and interfaces, and the jam sequence.

Max Length= 2500m (48 % of the theoretical)

WIRELESS LANS

Wireless communication is one of the fastest growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas. In this section, we concentrate on two wireless technologies for LANs:

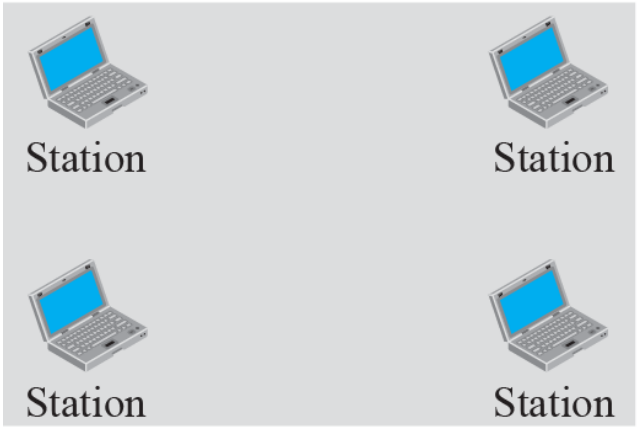
- IEEE 802.11 wireless LANs
- Bluetooth as technology for small wireless LANs.

Topics Discussed in the Section

- ✓ **IEEE 802.11**
- ✓ **MAC Sublayer**
- ✓ **Hidden and Expose Terminal problems**
- ✓ **Bluetooth**

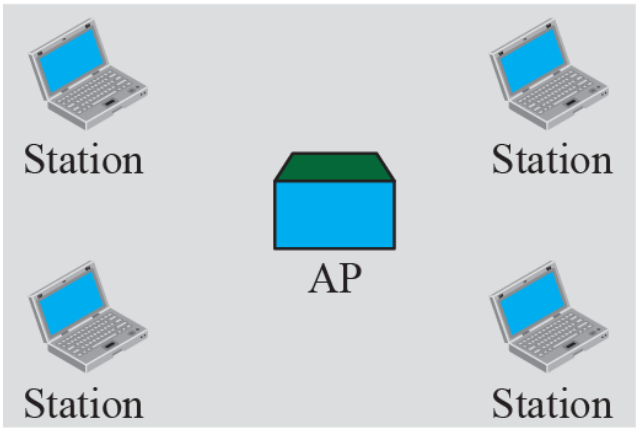
Basic service sets (BSSs)

BSS: Basic service set



Ad hoc network (BSS without an AP)

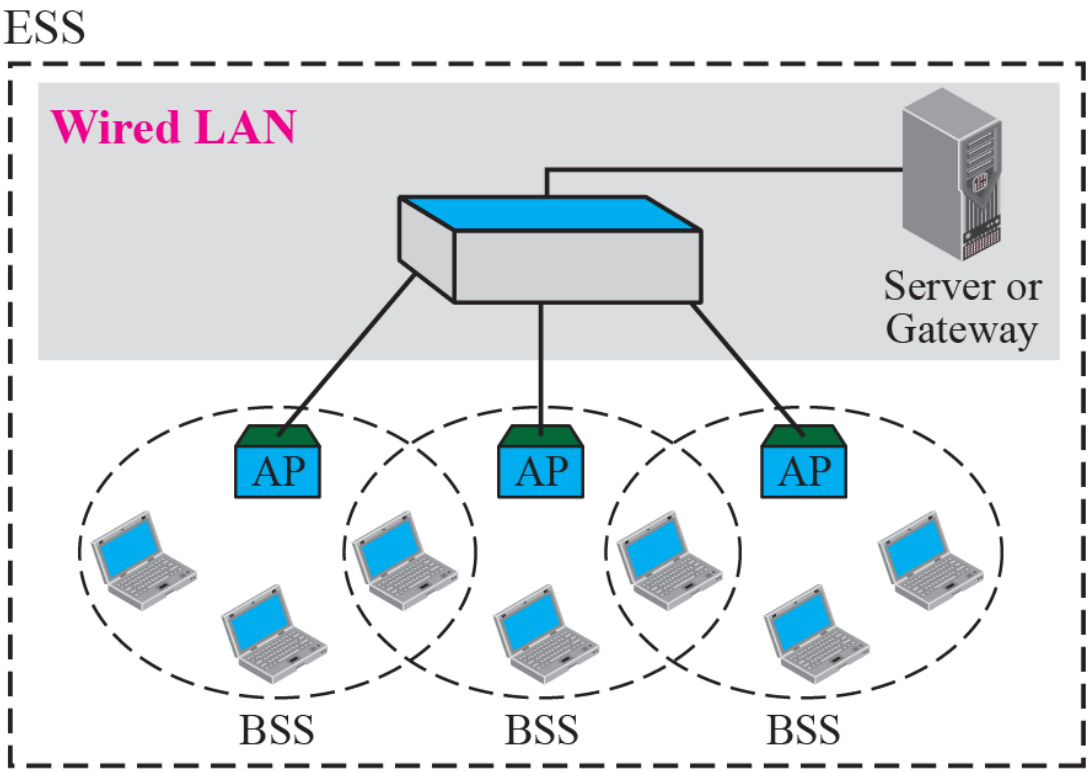
AP: Access point



Infrastructure (BSS with an AP)

Extended service sets (ESSs)

ESS: Extended service set
BSS: Basic service set
AP: Access point



802.11 Wireless LAN

- **Range (Distance between Access Point and WLAN client) depends on structural hindrances and RF gain of the antenna at the Access Point**
- **To service larger areas, multiple APs may be installed with a 20-30% overlap**
- **A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off)**
- **Variations:**
  - 802.11b (1999)
  - 802.11a (1999)
  - 802.11g (2003)
  - 802.11n (2009)

WLAN : 802.11b

- The most popular 802.11 standard currently in deployment.
- Supports 1, 2, 5.5 and 11 Mbps data rates in the 2.4 GHz ISM (Industrial-Scientific-Medical) band

WLAN : 802.11a

- Operates in the 5 GHz UNII (Unlicensed National Information Infrastructure) band
- Incompatible with devices operating in 2.4GHz
- Supports Data rates up to 54 Mbps.

WLAN : 802.11g

- Supports data rates as high as 54 Mbps on the 2.4 GHz band
- Provides backward compatibility with 802.11b equipment

WLAN : 802.11n

- Has rated 600Mbit/s bandwidth
- Introduces MIMO (Multiple-Input Multiple-Output)

Wireless LAN Protocols

Wireless has complications compared to wired.

Nodes may have different coverage regions

- Leads to hidden and exposed terminals

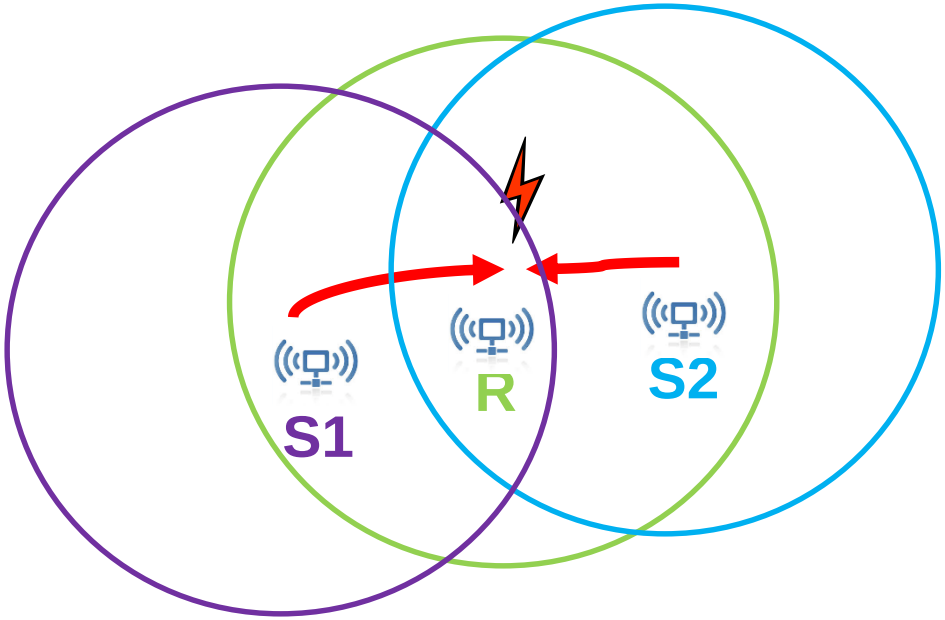
Nodes can't detect collisions, i.e., sense while sending

- Makes collisions expensive and to be avoided

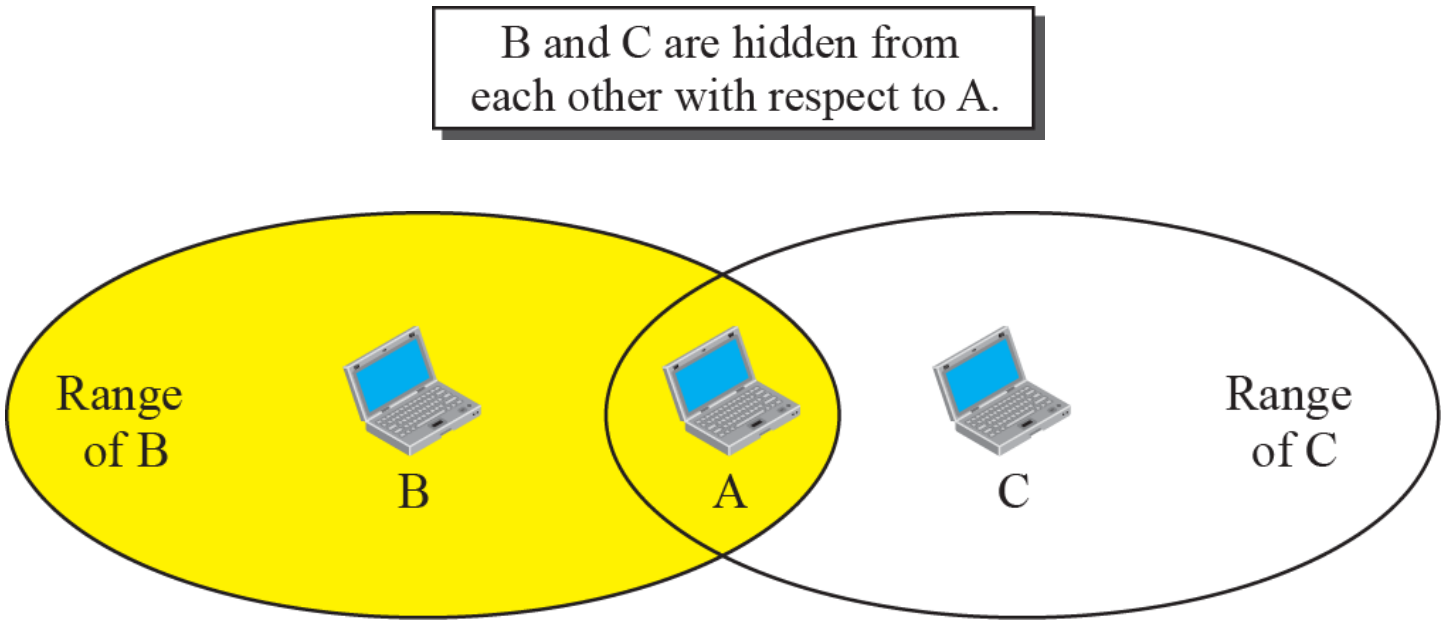
Wireless LANs – Hidden terminals

Hidden terminals are senders that cannot sense each other but nonetheless collide at intended receiver

- Want to prevent; loss of efficiency
- S1 and S2 are hidden terminals when sending to R



Hidden Terminal problem



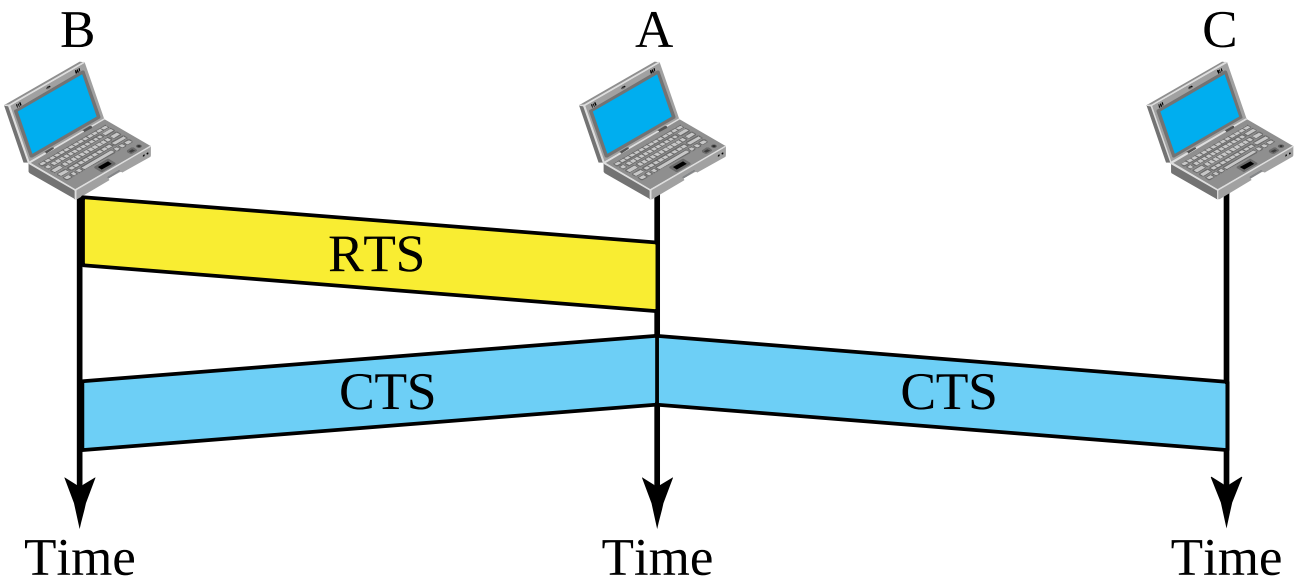
Wireless LANs – Hidden terminals

Before every data transmission

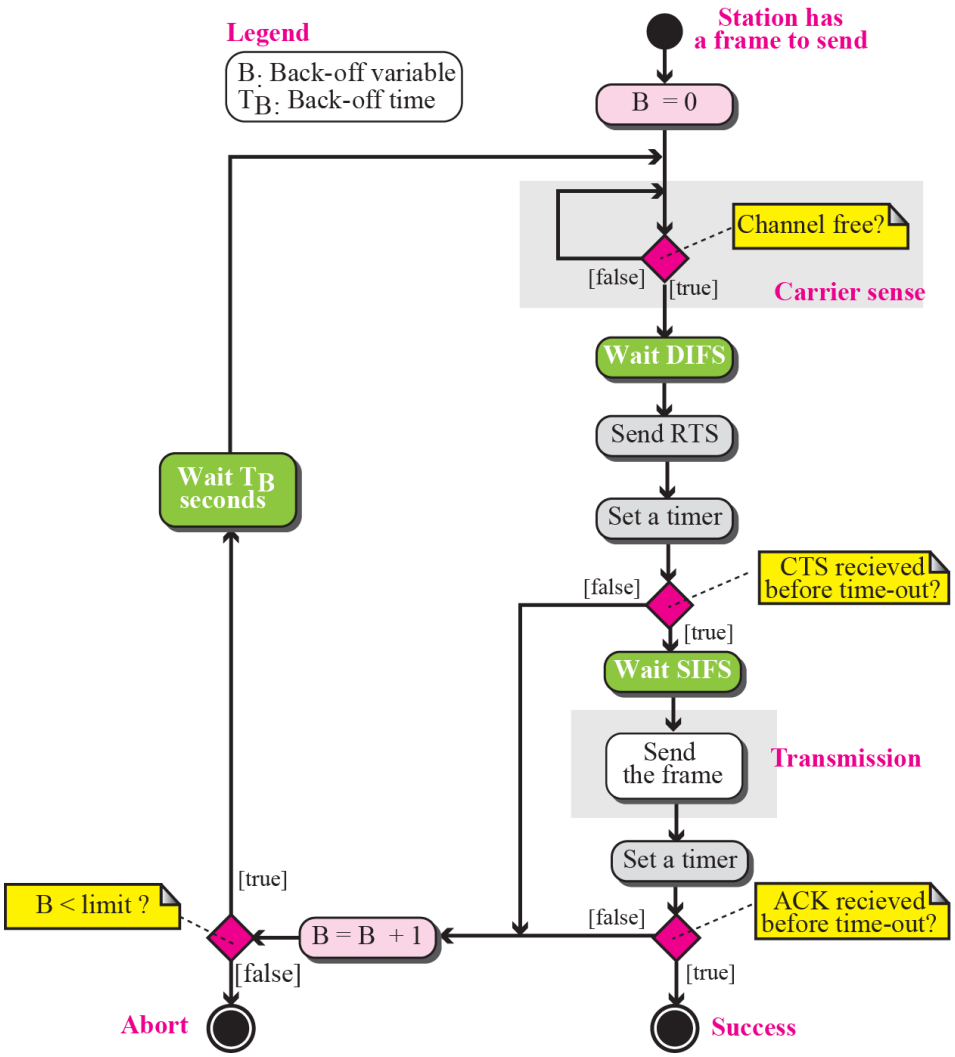
- **Sender sends a Request to Send (RTS) frame containing the length of the transmission**
- **Receiver respond with a Clear to Send (CTS) frame**
- **Sender sends data**
- **Receiver sends an ACK; now another sender can send data**

When sender doesn't get a CTS back, it assumes collision

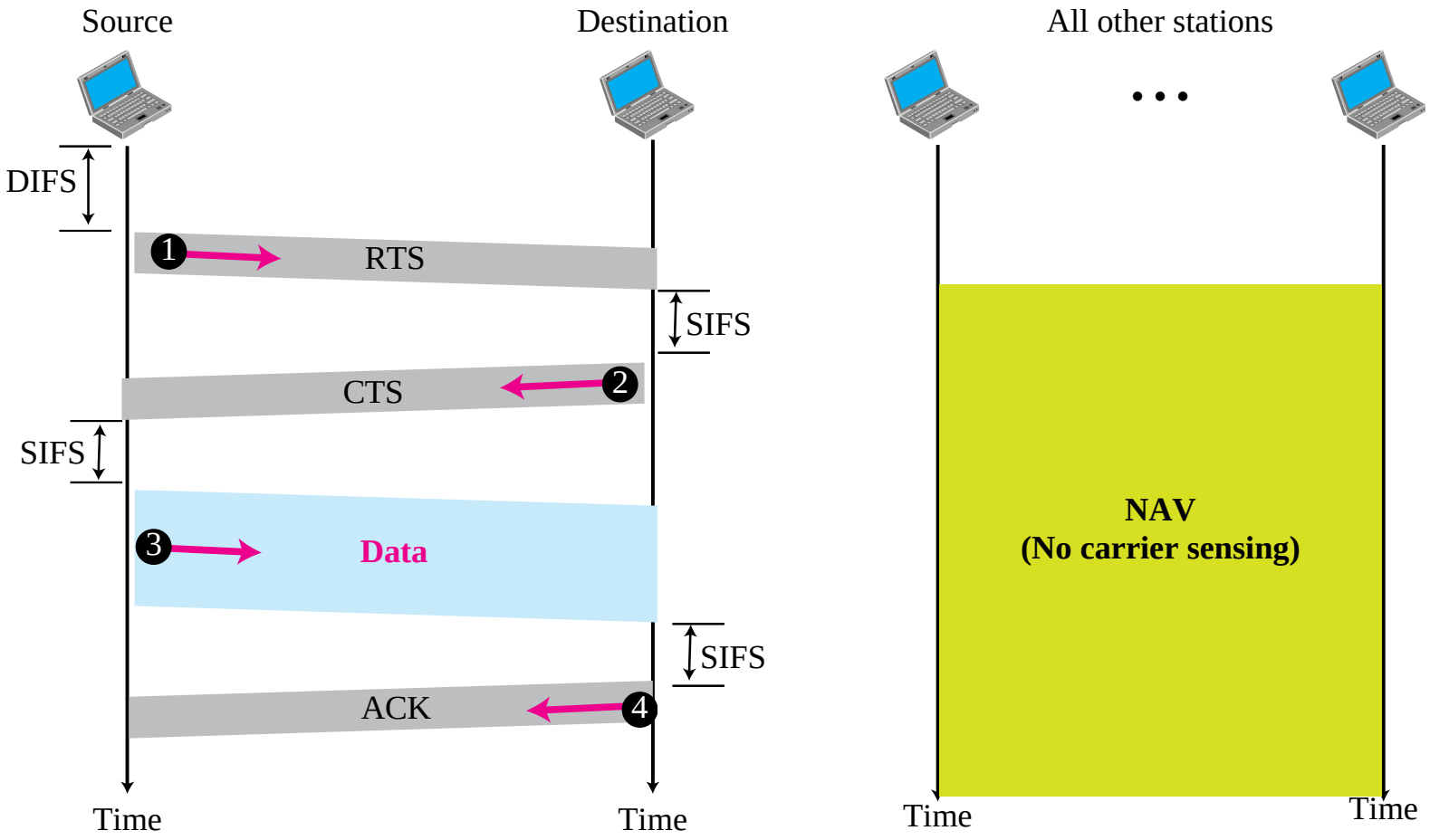
Use of handshaking to prevent hidden Terminal problem



CSMA/CA flow diagram

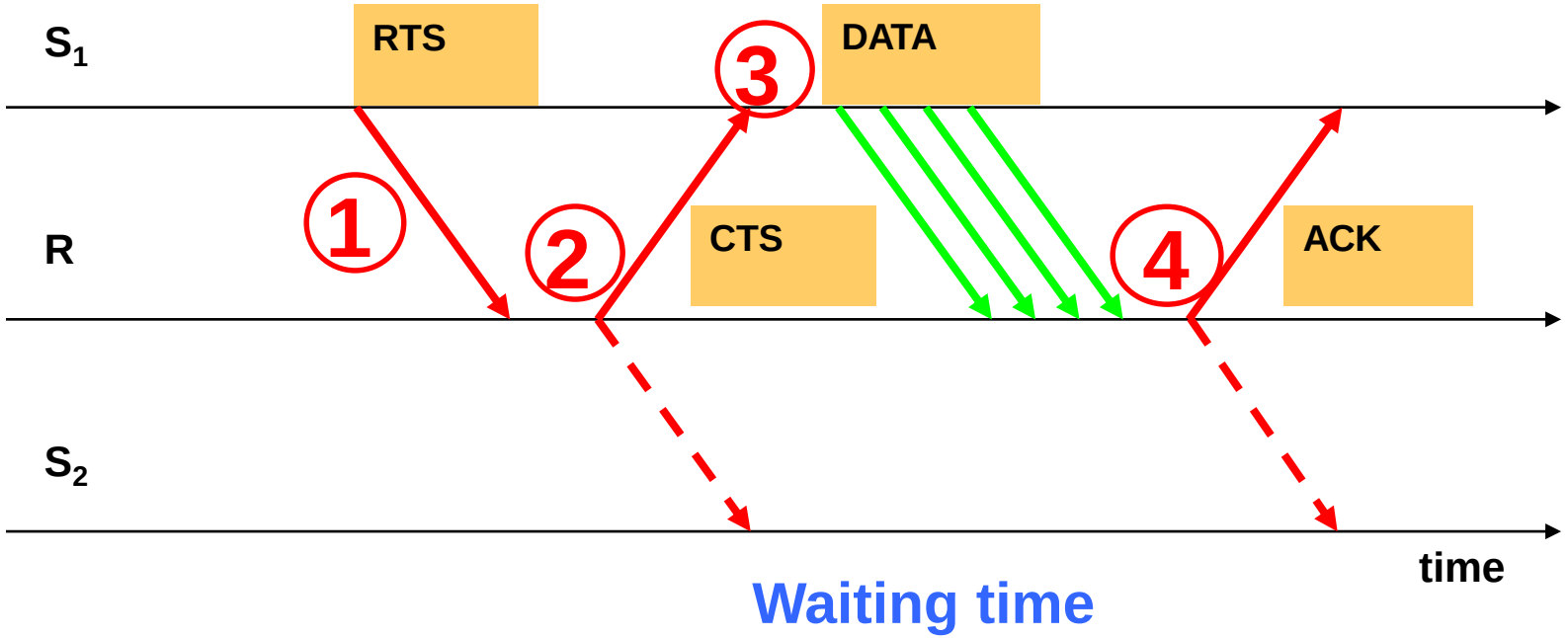


CSMA/CA and NAV



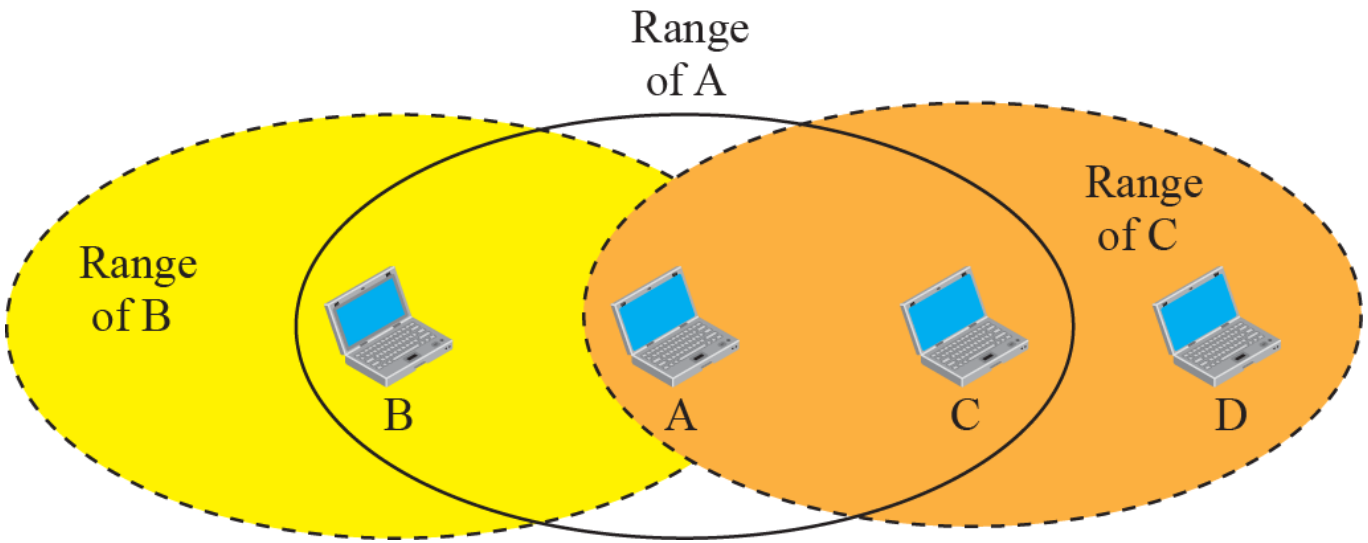
The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

Wireless LANs – Hidden terminals



Exposed Terminal problem

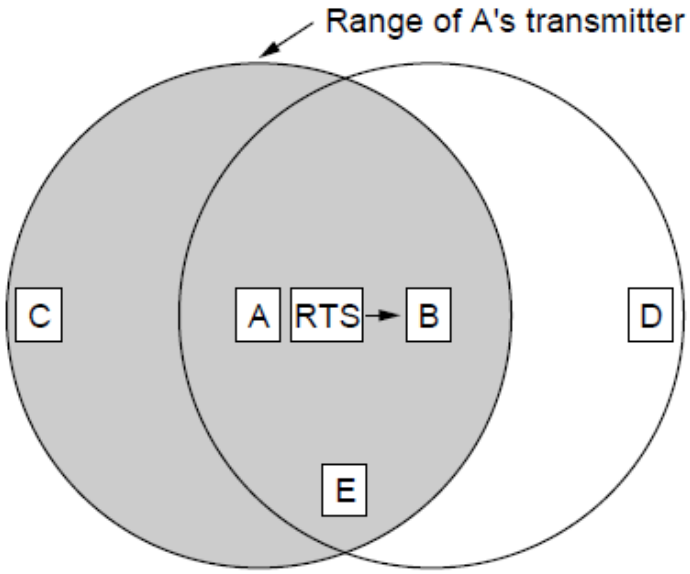
C is exposed to transmission from A to B.



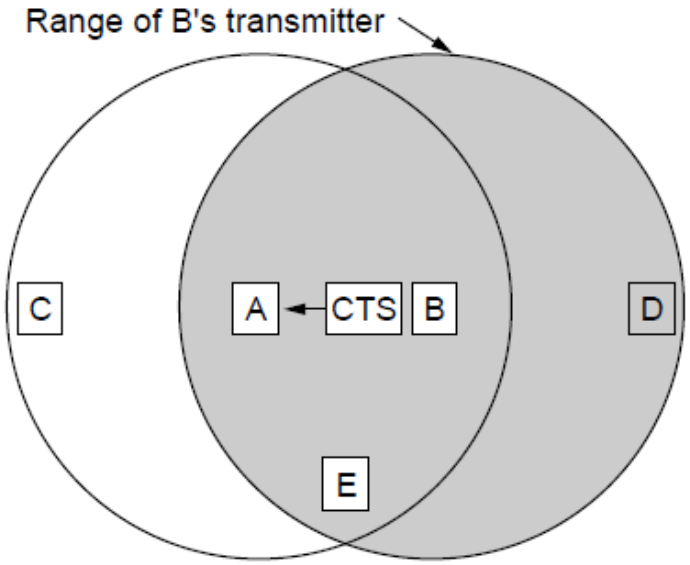
Wireless LANs – MACA

MACA protocol grants access for A to send to B:

- A sends RTS to B [left]; B replies with CTS [right]
- A can send with exposed but no hidden terminals



A sends RTS to B; C and E hear and defer for CTS

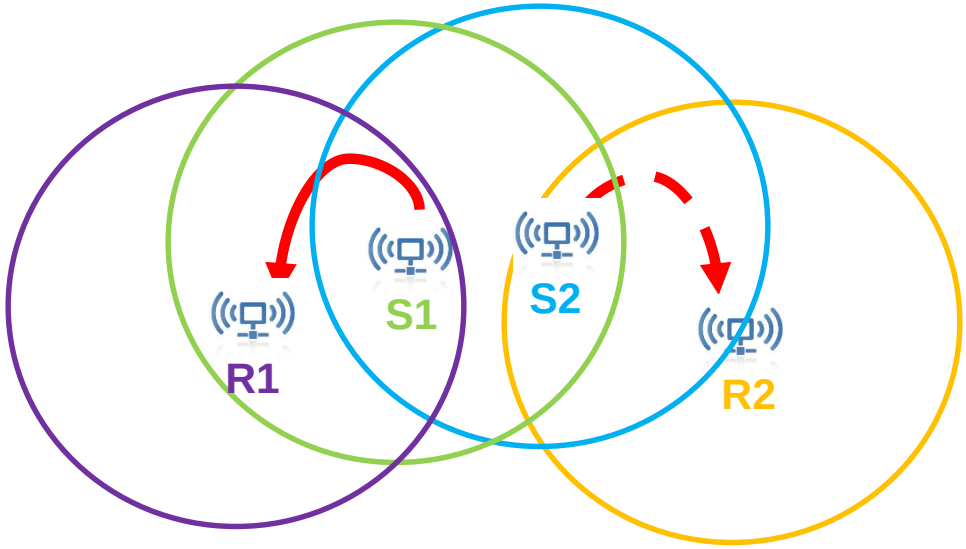


B replies with CTS; D and E hear and defer for data

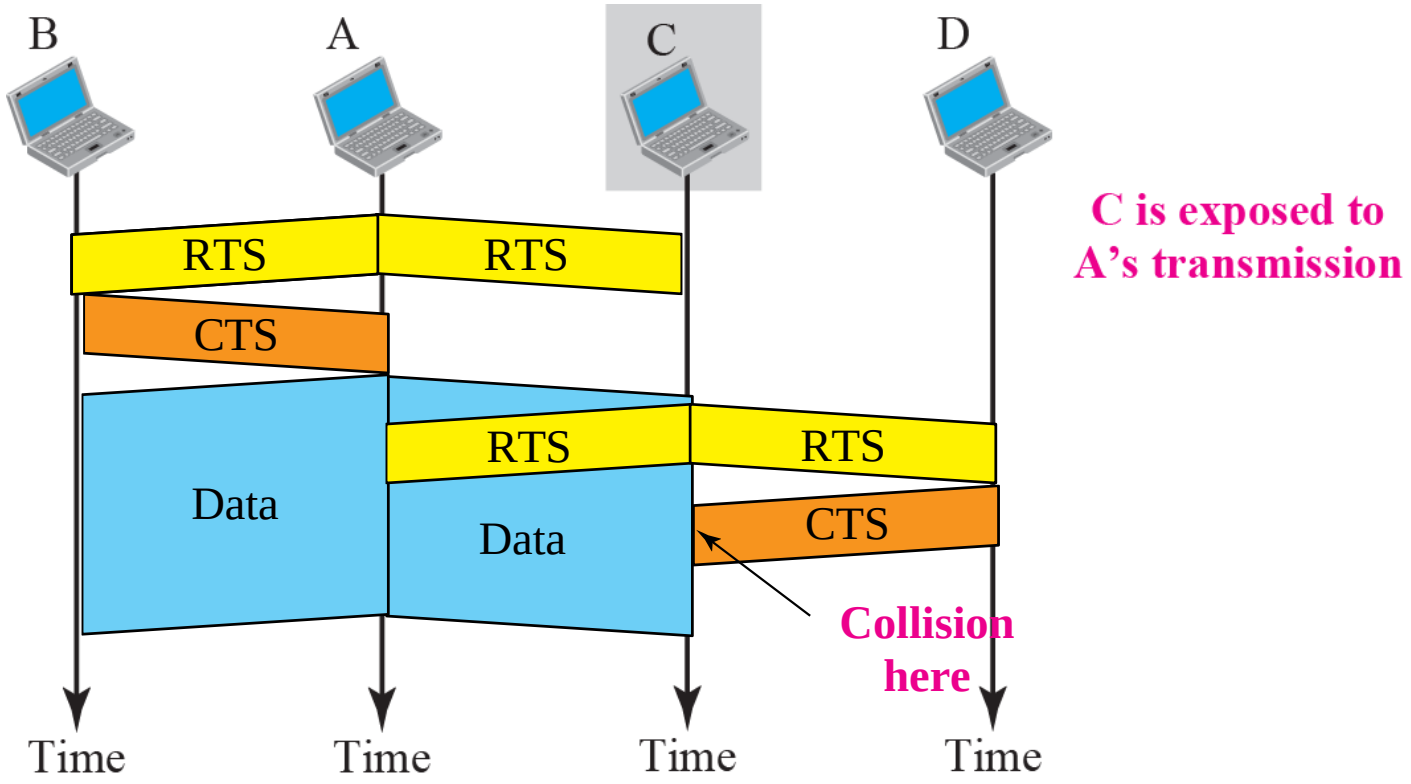
Wireless LANs – Exposed terminals

Exposed terminals are senders who can sense each other but still transmit safely (to different receivers)

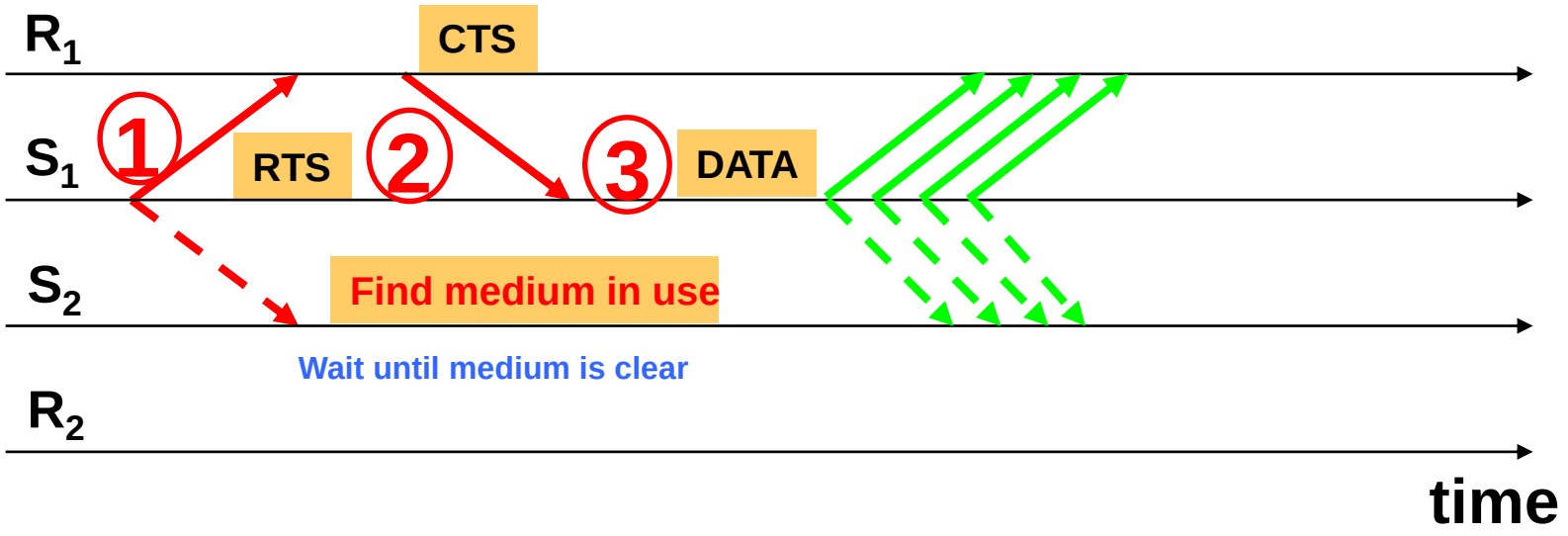
- Desirably concurrency; improves performance
- S1 → R1 and S2→ R2 are exposed terminals



Use of handshaking in exposed terminal problem



Wireless LANs – Exposed terminals



Wireless LANs – Exposed terminals