UNIT - VI

Medium Access Control

UNIT - VI

- Channel allocation: Static and Dynamic
- Multiple Access Protocols: Pure and Slotted ALOHA, CSMA, WDMA
- IEEE 802.3 Standards and Frame Formats
- CSMA/CD, Binary Exponential Back-off algorithm
- Fast Ethernet, Gigabit Ethernet,
- IEEE 802.11a/b/g/n and IEEE 802.15 and IEEE 802.16 Standards, Frame formats, CSMA/CA.

CHANNEL ALLOCATION

- The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum.
- Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.
- Channel Allocation Schemes
- Channel Allocation may be done using two schemes −
- Static Channel Allocation
- Dynamic Channel Allocation

STATIC CHANNEL ALLOCATION

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- It is not suitable in case of a large number of users with variable bandwidth requirements.

DYNAMIC CHANNEL ALLOCATION

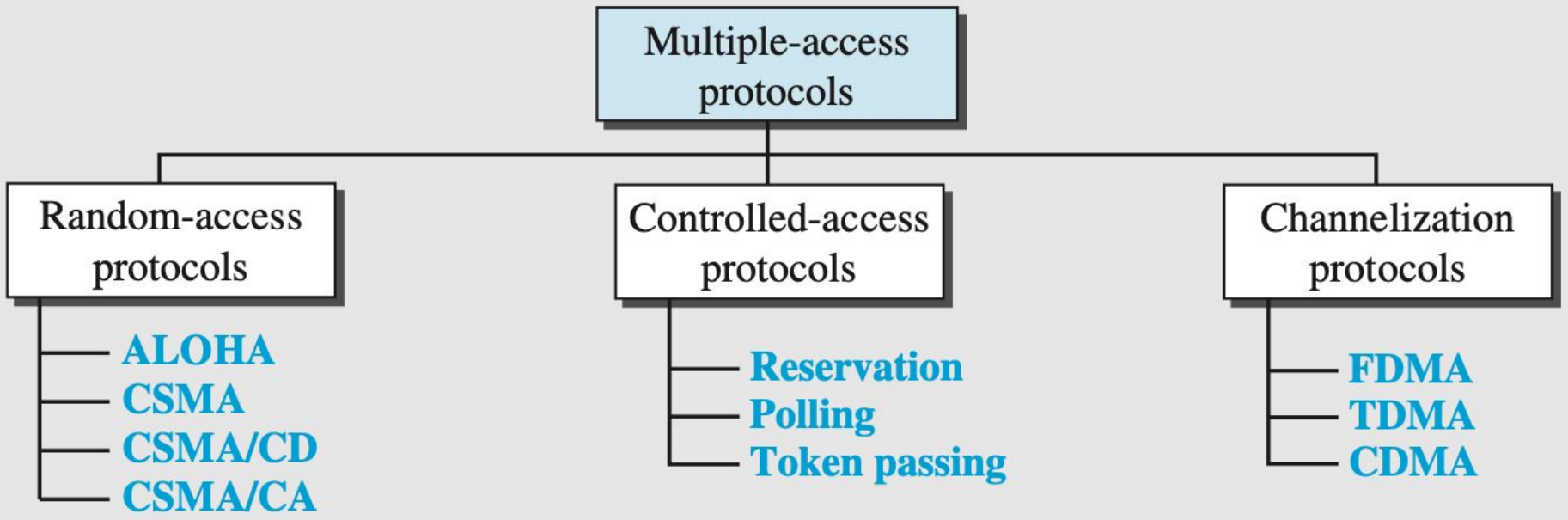
- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users.
- Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.
- This allocation scheme optimizes bandwidth usage and results in faster transmissions.
- Dynamic channel allocation is further divided into centralized and distributed allocation.

MULTIPLE-ACCESS PROTOCOLS

- Many protocols have been devised to handle access to a shared link.
- All of these protocols belong to a sublayer in the data-link layer called media access control (MAC).
- We categorize them into three groups.

MULTIPLE-ACCESS PROTOCOLS

Figure 12.1 *Taxonomy of multiple-access protocols*



RANDOM ACCESS

- In random-access or contention methods, no station is superior to another station and none is assigned control over another.
- 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.
- This decision depends on the state of the medium (idle or busy).
- Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access.
- Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.

RANDOM ACCESS

- In a random-access method, each station has the right to the medium without being controlled by any other station.
- However, if more than one station tries to send, there is an access conflict (collision) and the frames will be either destroyed or modified.
- To avoid access conflict or to resolve it when it happens, each station follows a procedure.

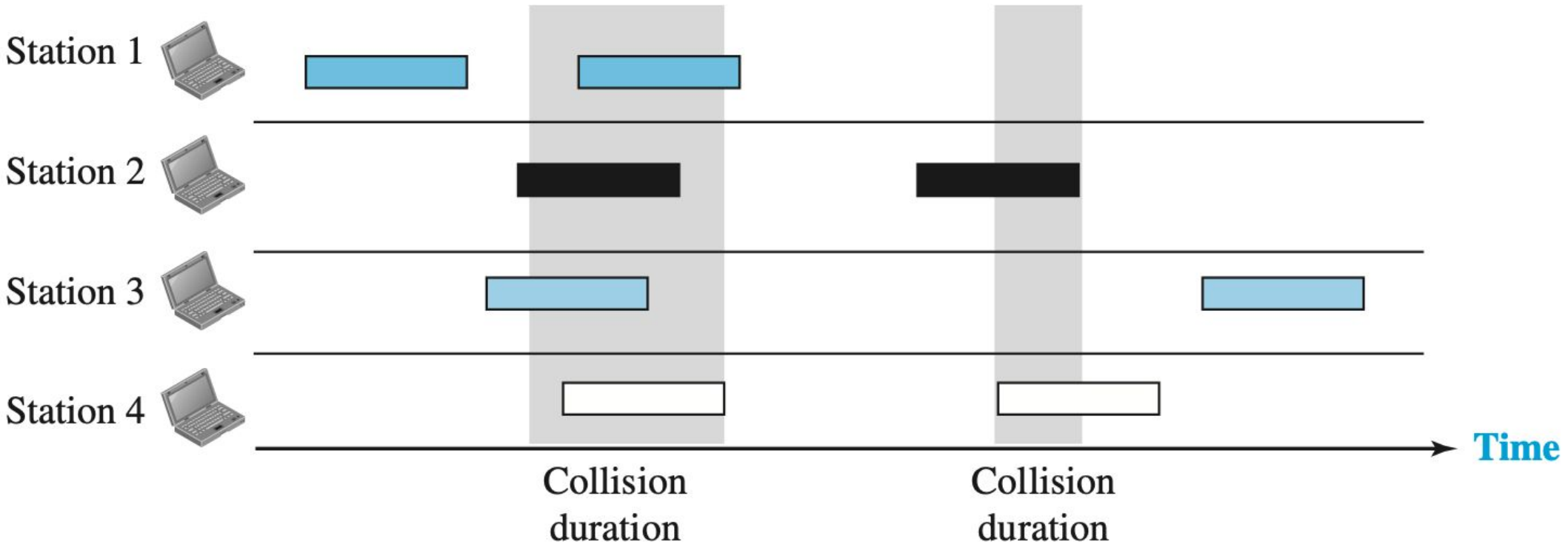
ALOHA

- ALOHA, the earliest random access method, was developed at the University of Hawaii in early 1970.
- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.
- It is obvious that there are potential collisions in this arrangement.
- The medium is shared between the stations.
- When a station sends data, another station may attempt to do so at the same time.
- The data from the two stations collide and become garbled.

PURE ALOHA

- The original ALOHA protocol is called pure ALOHA.
- This is a simple but elegant protocol.
- The idea is that each station sends a frame whenever it has a frame to send (multiple access).
- However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

Figure 12.2 *Frames in a pure ALOHA network*



PURE ALOHA

- The pure ALOHA protocol relies on acknowledgments from the receiver.
- When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.
- A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again.
- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame.
- The randomness will help avoid more collisions. We call this time the backoff time T_B.

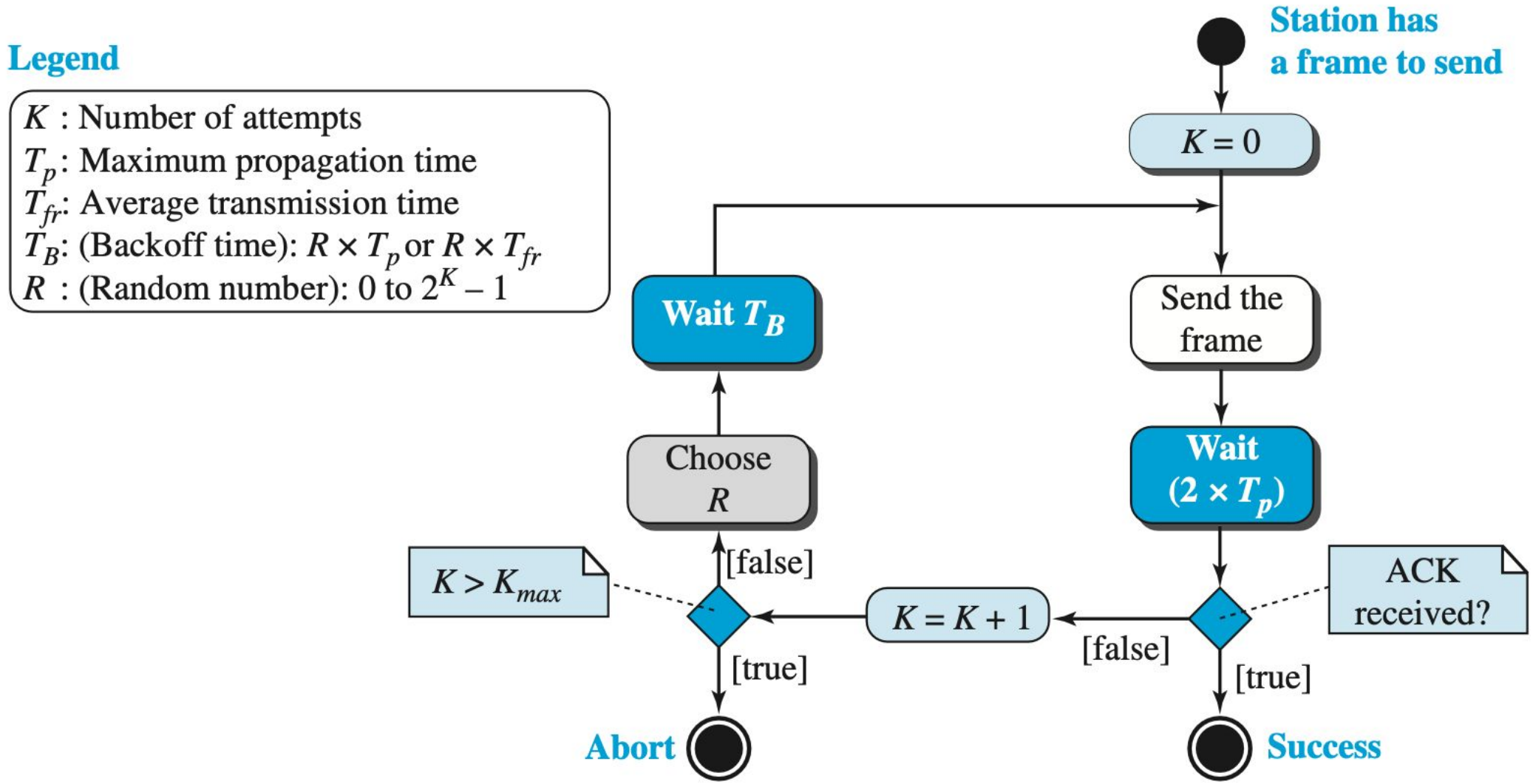
PURE ALOHA - BINARY EXPONENTIAL BACK-OFF ALGORITHM

- Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames.
- After a maximum number of retransmission attempts K_{max} a station must give up and try later.
- The time-out period is equal to the maximum possible round-trip propagation delay, which is twice the amount of time required to send a frame between the two most widely separated stations $(2 \times T_p)$.
- The backoff time T_B is a random value that normally depends on K (the number of attempted unsuccessful transmissions).

PURE ALOHA - BINARY EXPONENTIAL BACK-OFF ALGORITHM

- The formula for T_B depends on the implementation. One common formula is the binary exponential backoff.
- In this method, for each retransmission, a multiplier $R = 0$ *to* $2^K - 1$ is randomly chosen and multiplied by T_p (maximum propagation time) or T_{fr} (the average time required to send out a frame) to find T_B.
- Note that in this procedure, the range of the random numbers increases after each collision.
- The value of K_{max} is usually chosen as 15.

Figure 12.3 *Procedure for pure ALOHA protocol*



VULNERABLE TIME

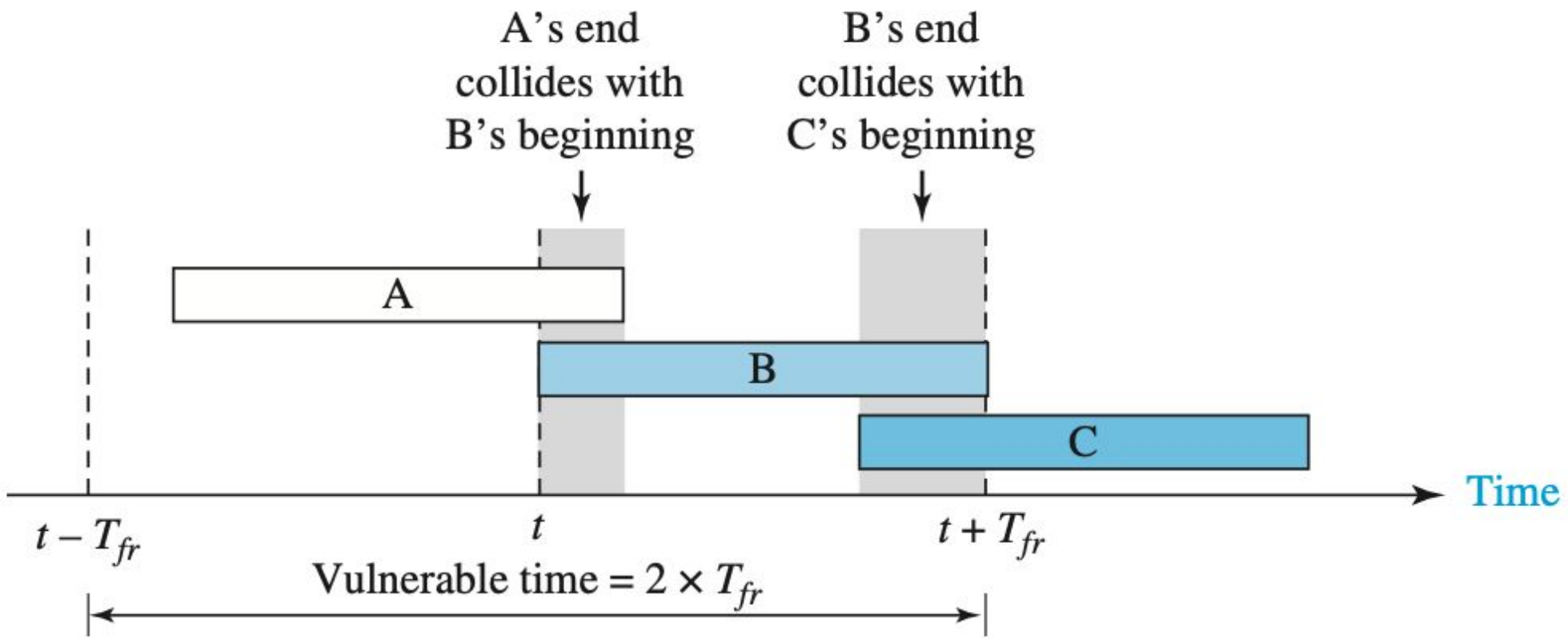
- Vulnerable time, the length of time in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking T_{fr} seconds to send.
- Station B starts to send a frame at time t. Now imagine station A has started to send its frame after $t - T_{fr}$.
- This leads to a collision between the frames from station B and station A.

VULNERABLE TIME

- On the other hand, suppose that station C starts to send a frame before time $t + T_{fr}$. Here, there is also a collision between frames from station B and station C.
- We see that the vulnerable time during which a collision may occur in pure ALOHA is 2 times the frame transmission time.

Pure ALOHA vulnerable time = $2 \times T_{fr}$

Figure 12.4 *Vulnerable time for pure ALOHA protocol*



THROUGHPUT

- Let us call ***G*** the average number of frames generated by the system during one frame transmission time.
- Then it can be proven that the average number of successfully transmitted frames for pure ALOHA is $S = G \times e^{-2G}$.
- The maximum throughput S_{max} is **0.184**, for $G = 1/2$.
- In other words, if one-half a frame is generated during one frame transmission time (one frame during two frame transmission times), then **18.4** percent of these frames reach their destination successfully.

SLOTTED ALOHA

- Pure ALOHA has a vulnerable time of $2 \times T_{fr}$. This is so because there is no rule that defines when the station can send.
- A station may send soon after another station has started or just before another station has finished.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA we divide the time into slots of T_{fr} seconds and force the station to send only at the beginning of the time slot.

Figure 12.5 *Frames in a slotted ALOHA network*

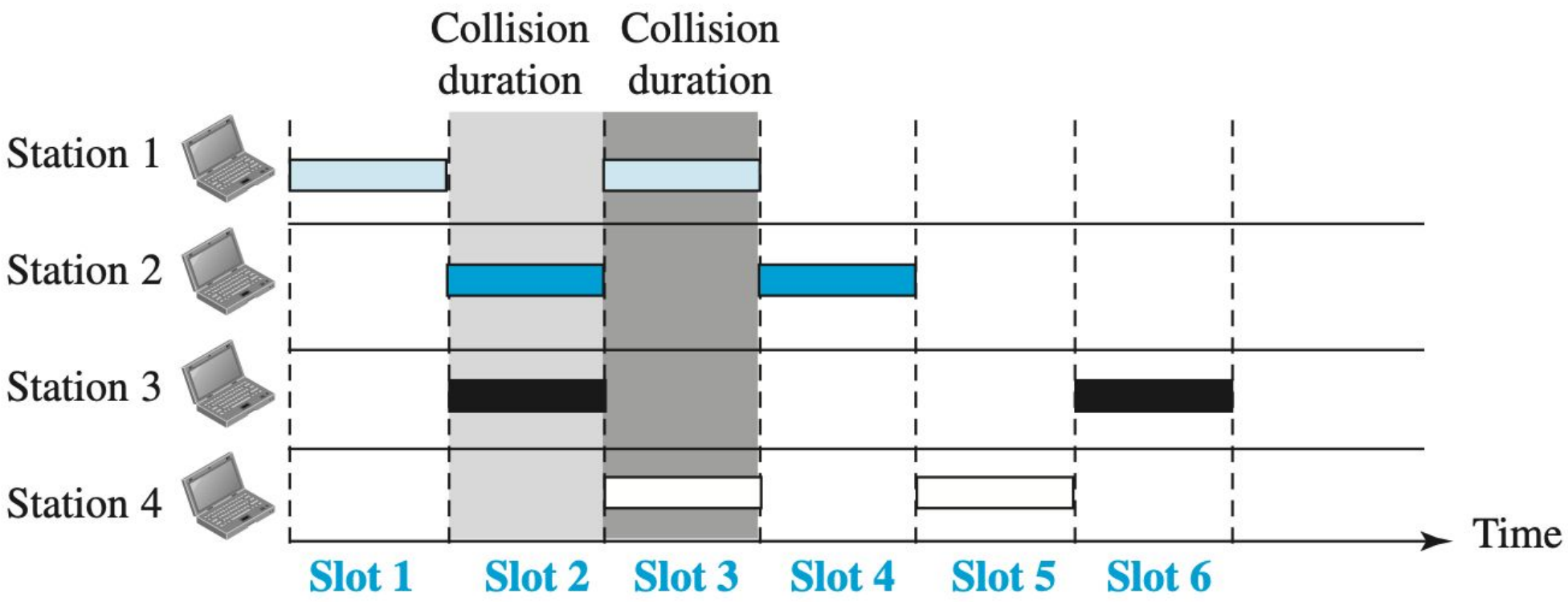
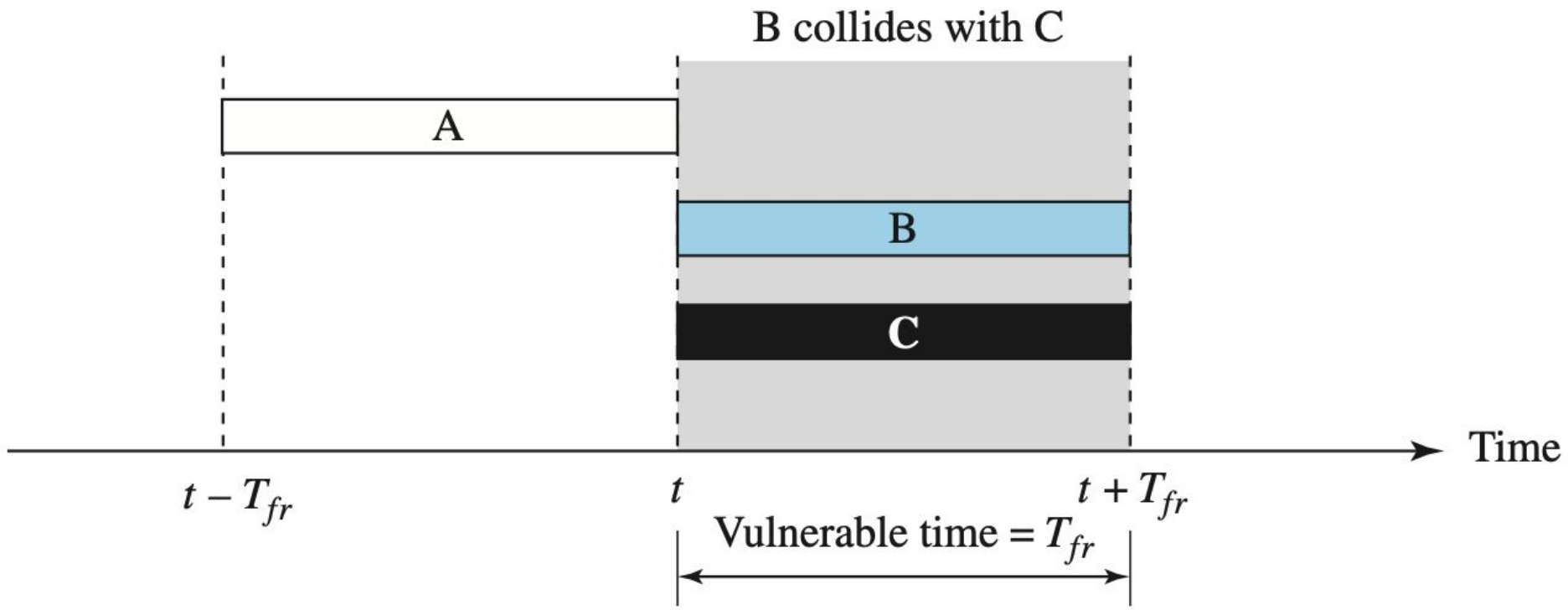


Figure 12.6 *Vulnerable time for slotted ALOHA protocol*



THROUGHPUT

- It can be proven that the average number of successful transmissions for slotted ALOHA is $S = G \times e^{-G}$.
- The maximum throughput S_{max} is **0.368**, when $G = 1$.
- In other words, if one frame is generated during one frame transmission time, then **36.8** percent of these frames reach their destination successfully.

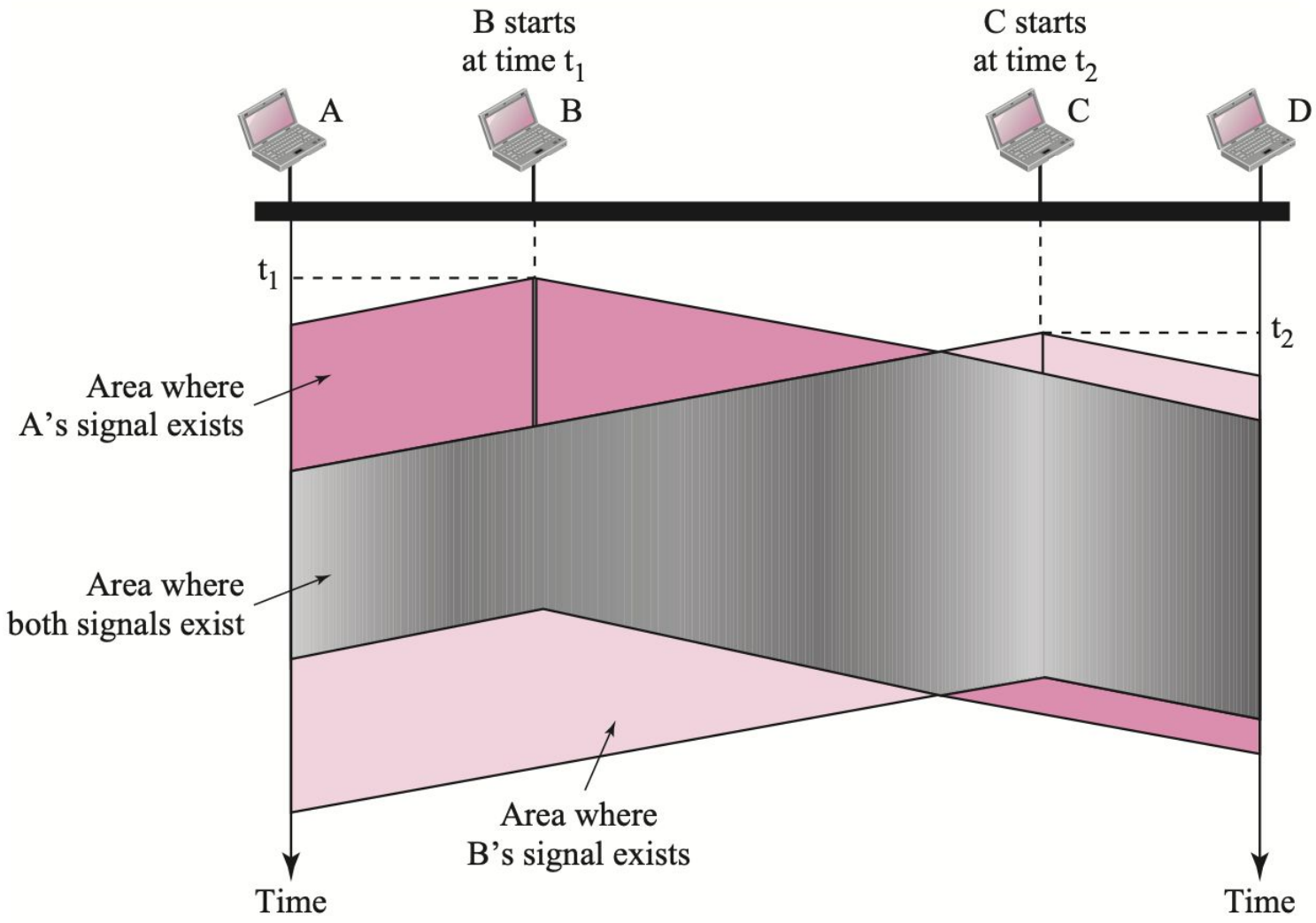
CSMA

- To minimize the chance of collision and increase the performance, the CSMA method was developed.
- The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium before sending.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.

CSMA

- The possibility of collision still exists because of propagation delay.
- When a station sends a frame, it still takes time for the first bit to reach every station and for every station to sense it.

Figure 3.7 *Space/time model of a collision in CSMA*



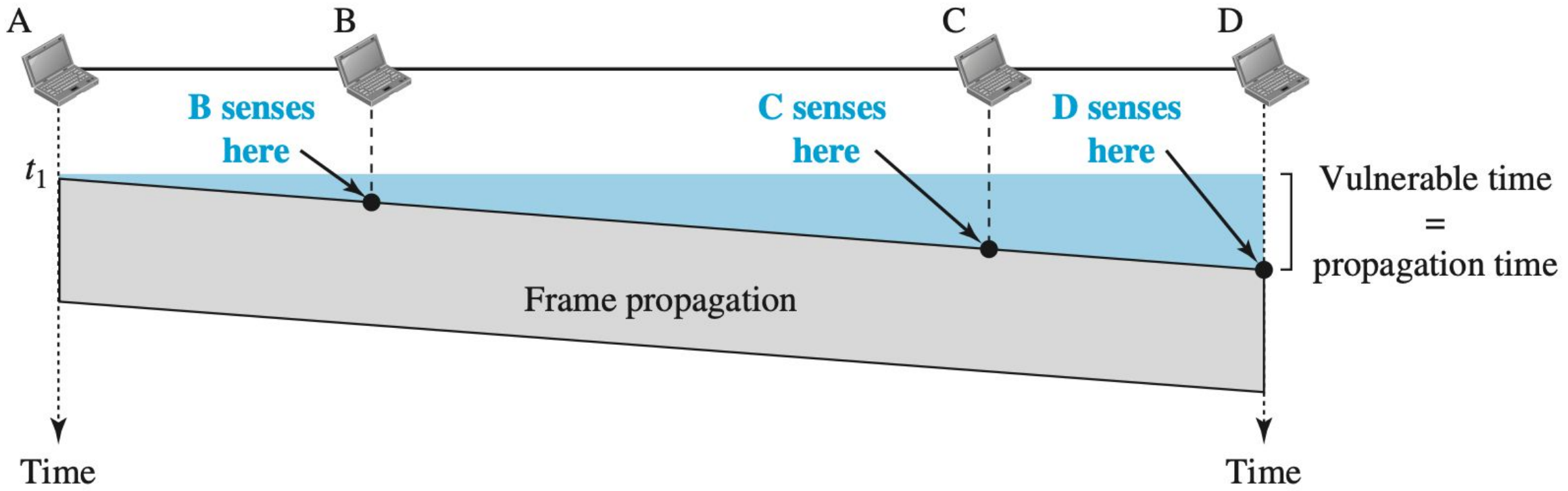
CSMA

- At time t1, station B senses the medium and finds it idle, so it sends a frame.
- At time t2 (t2 > t1), station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C.
- Station C also sends a frame.
- The two signals collide and both frames are destroyed.

VULNERABLE TIME

- The vulnerable time for CSMA is the propagation time T_p.
- This is the time needed for a signal to propagate from one end of the medium to the other.
- When a station sends a frame and any other station tries to send a frame during this time, a collision will result.
- But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

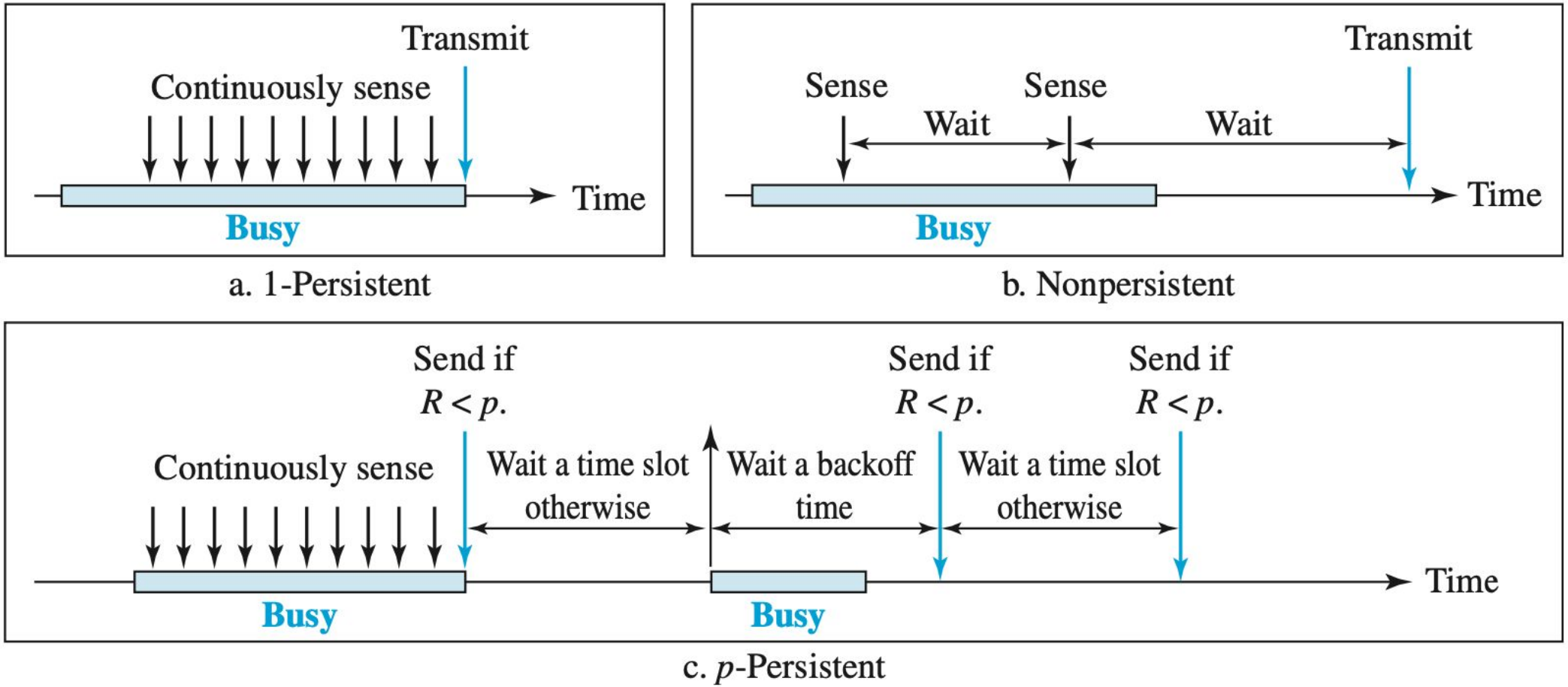
Figure 12.8 *Vulnerable time in CSMA*



PERSISTENCE METHODS

- 1-Persistent
- Nonpersistent
- p-Persistent

Figure 12.9 *Behavior of three persistence methods*



a. 1-Persistent

b. Nonpersistent

c. *p*-Persistent

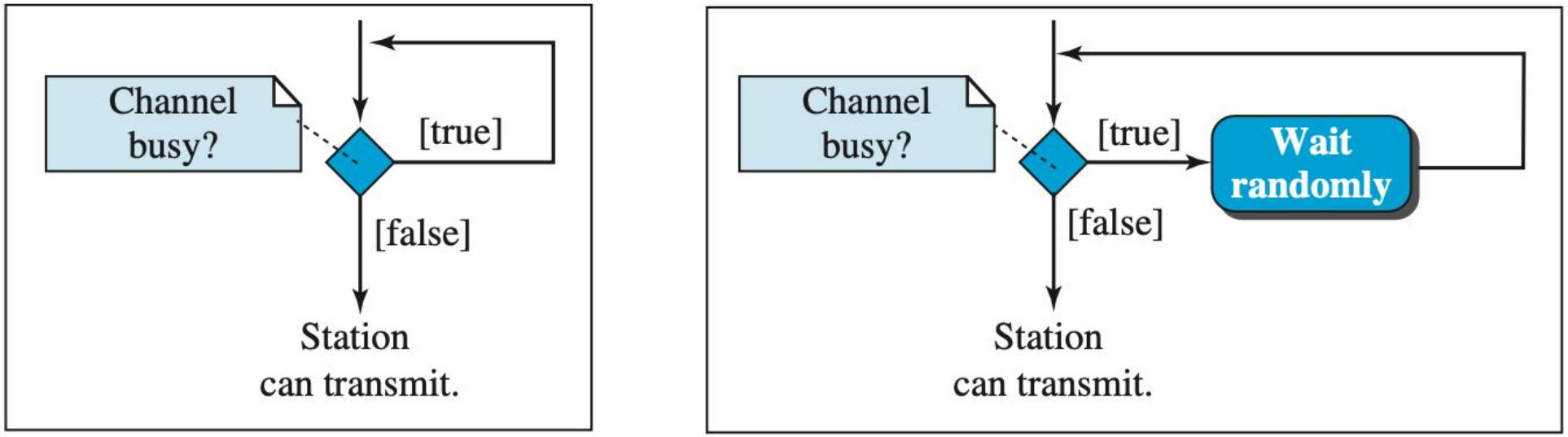
1-PERSISTENT

- In this method, after the station finds the line idle, it sends its frame immediately (with probability 1).
- This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

NONPERSISTENT

- In the nonpersistent method, a station that has a frame to send senses the line.
- If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
- The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Figure 12.10 *Flow diagram for three persistence methods*



a. 1-Persistent

b. Nonpersistent

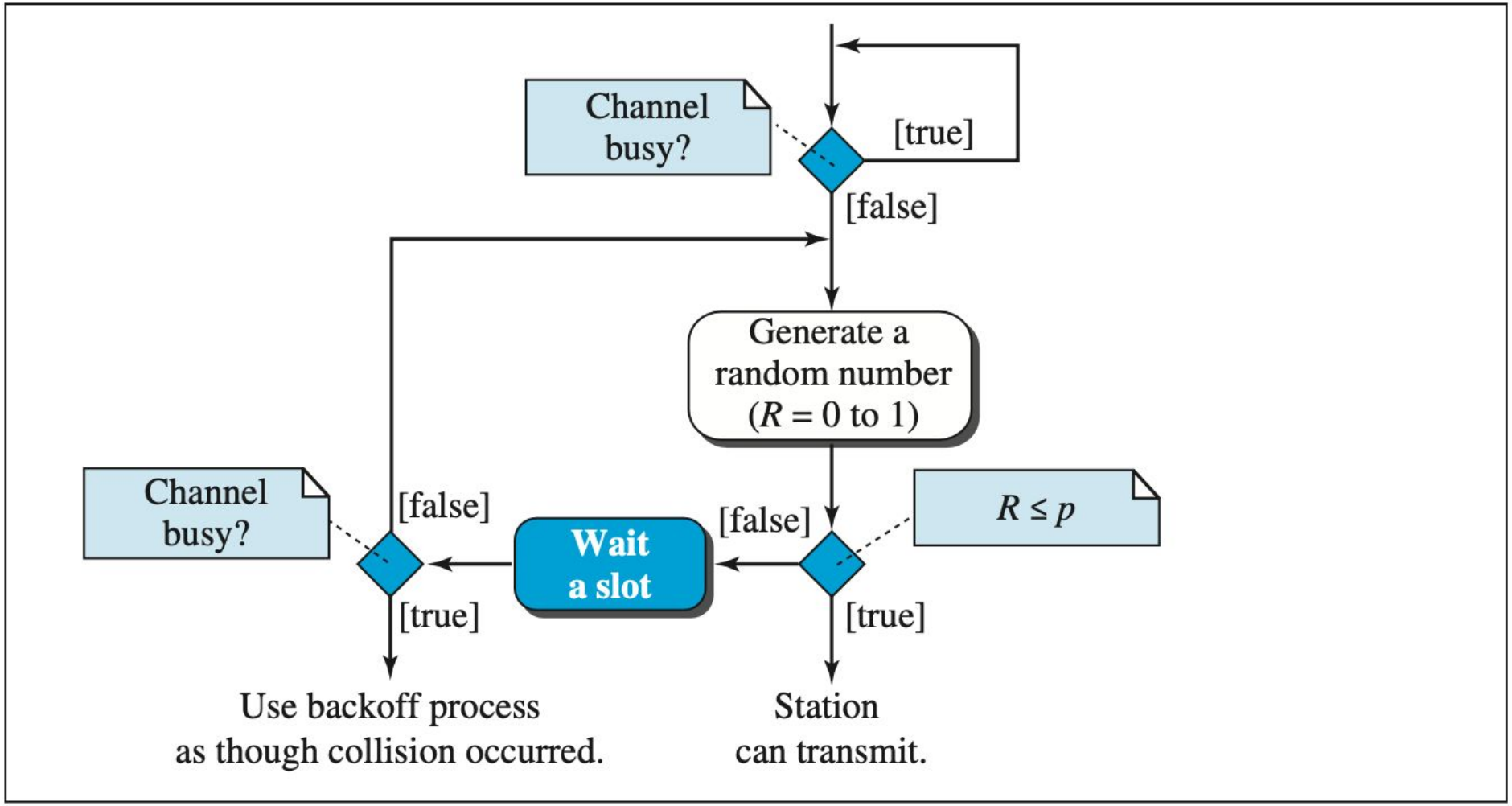
p-PERSISTENT

- The p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies.
- It reduces the chance of collision and improves efficiency.

p-PERSISTENT

- In this method, after the station finds the line idle it follows these steps:

1. With probability **p**, the station sends its frame.
2. With probability **q = 1 − p**, the station waits for the beginning of the next time slot and checks the line again.
   a. If the line is idle, it goes to step 1.
   b. If the line is busy, it acts as though a collision has occurred and uses the back-off procedure.



c. *p*-Persistent

CSMA/CD

- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If, however, there is a collision, the frame is sent again.

Figure 12.11 *Collision of the first bits in CSMA/CD*

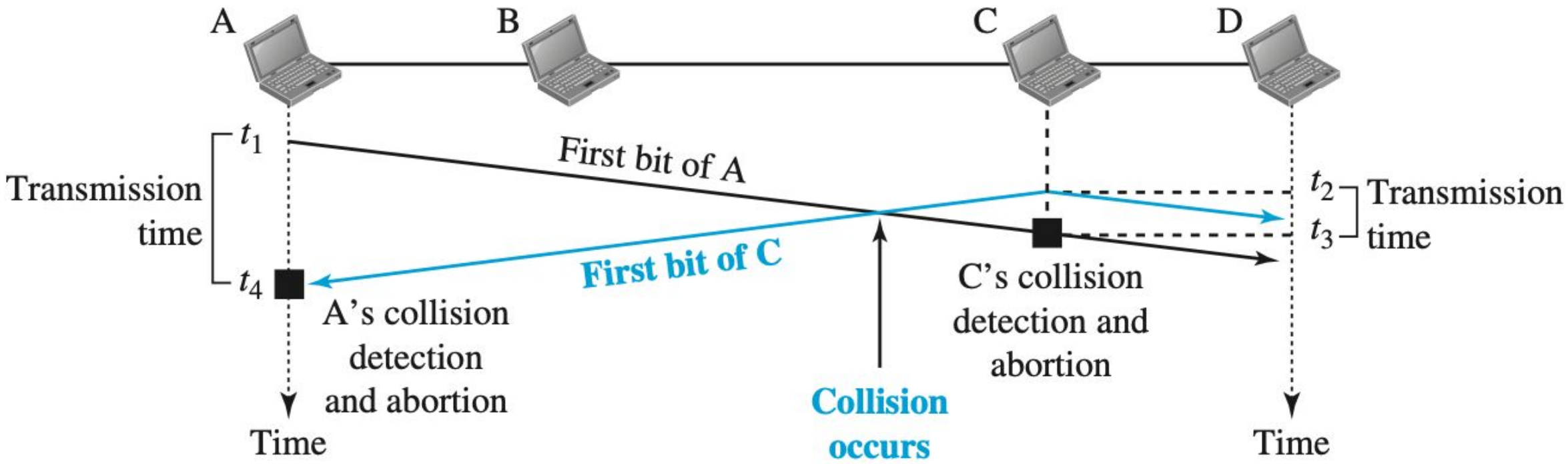


Figure 12.12 *Collision and abortion in CSMA/CD*

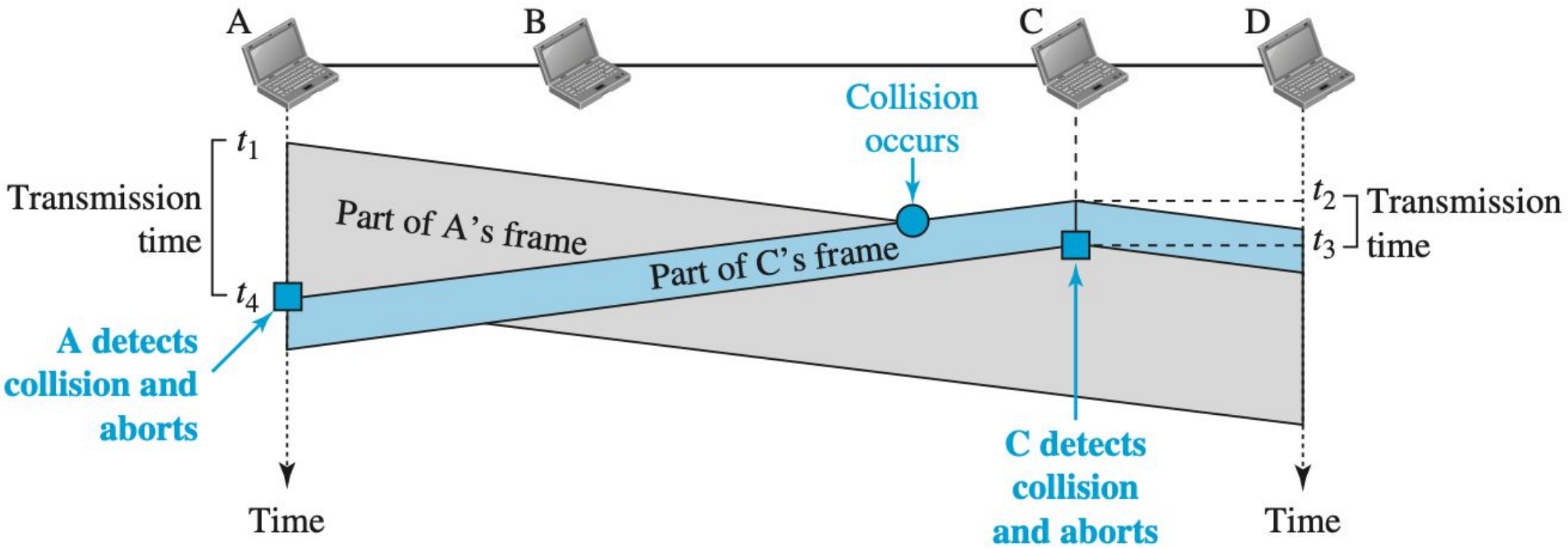
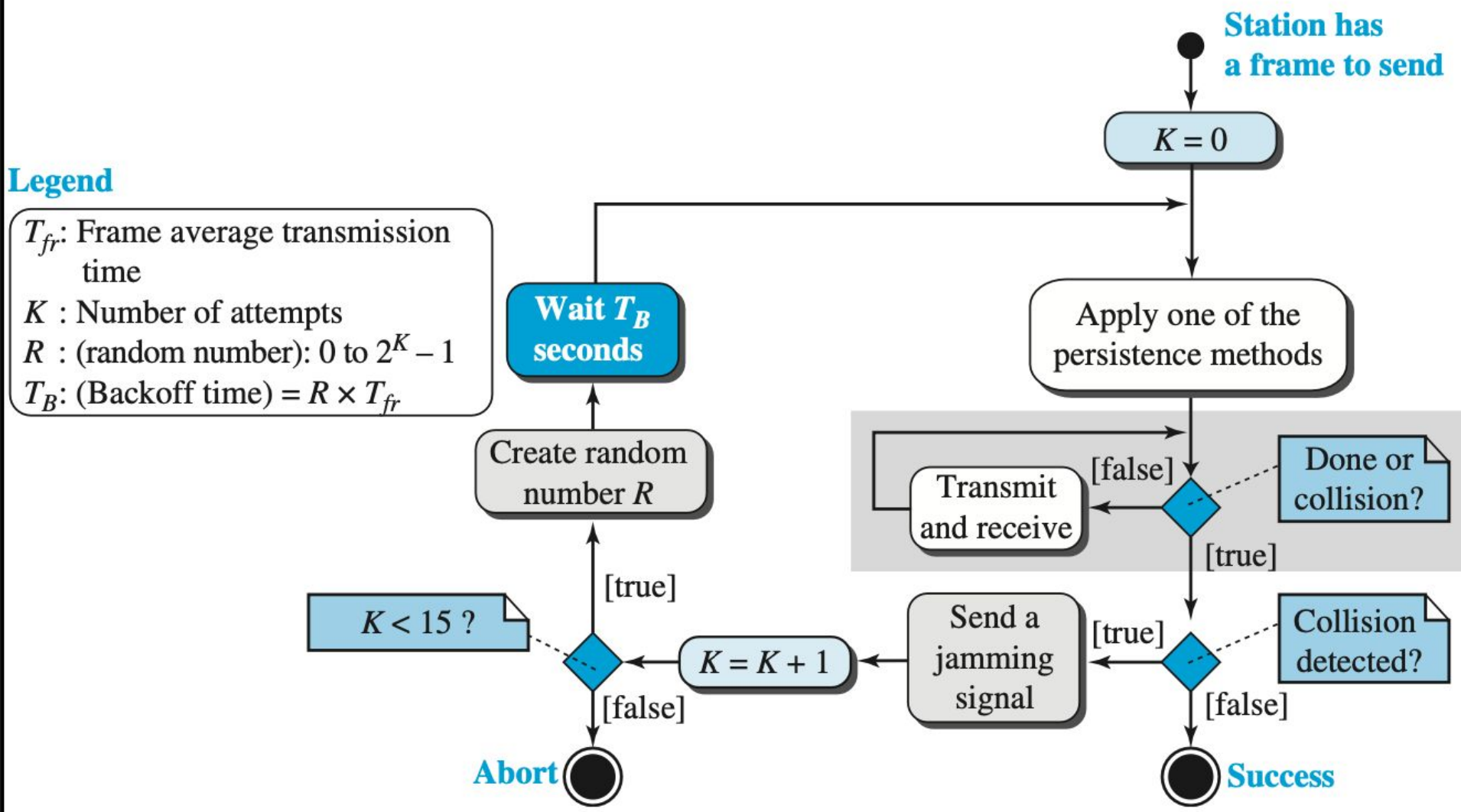


Figure 12.13 *Flow diagram for the CSMA/CD*



CSMA/CA

- Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.
- Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments.

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.
- Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.
- The distant station’s signal has not yet reached this station

INTERFRAME SPACE (IFS)

- After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention window.
- The IFS variable can also be used to prioritize stations or frame types.
- For example, a station that is assigned a shorter IFS has a higher priority.

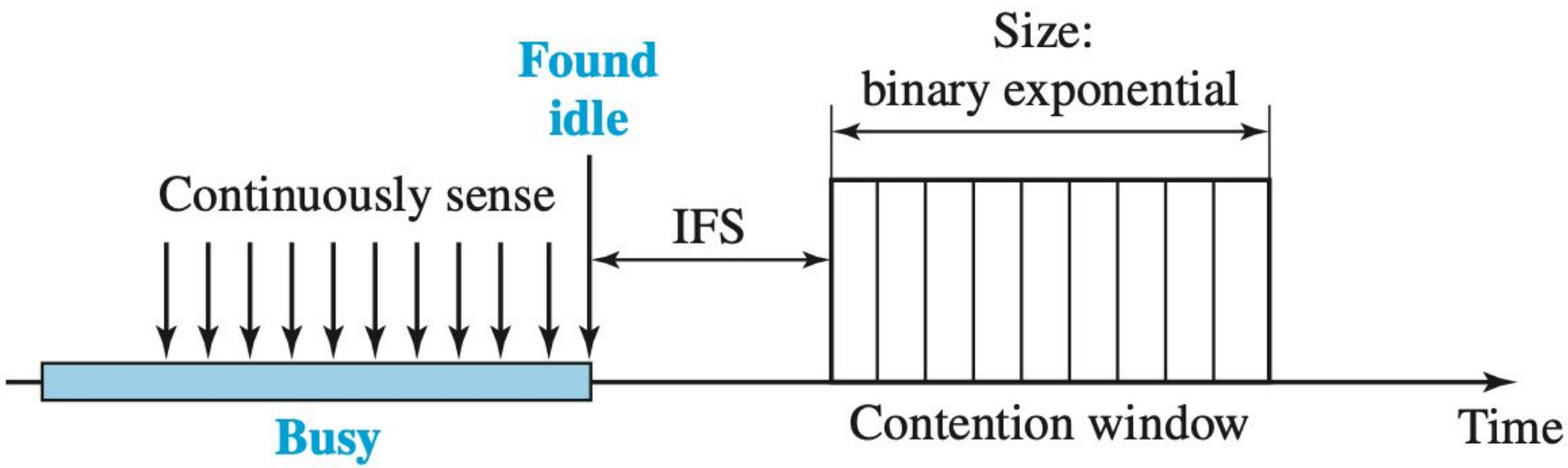
CONTENTION WINDOW

- 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 backoff strategy.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time.

CONTENTION WINDOW

- This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station.
- 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.

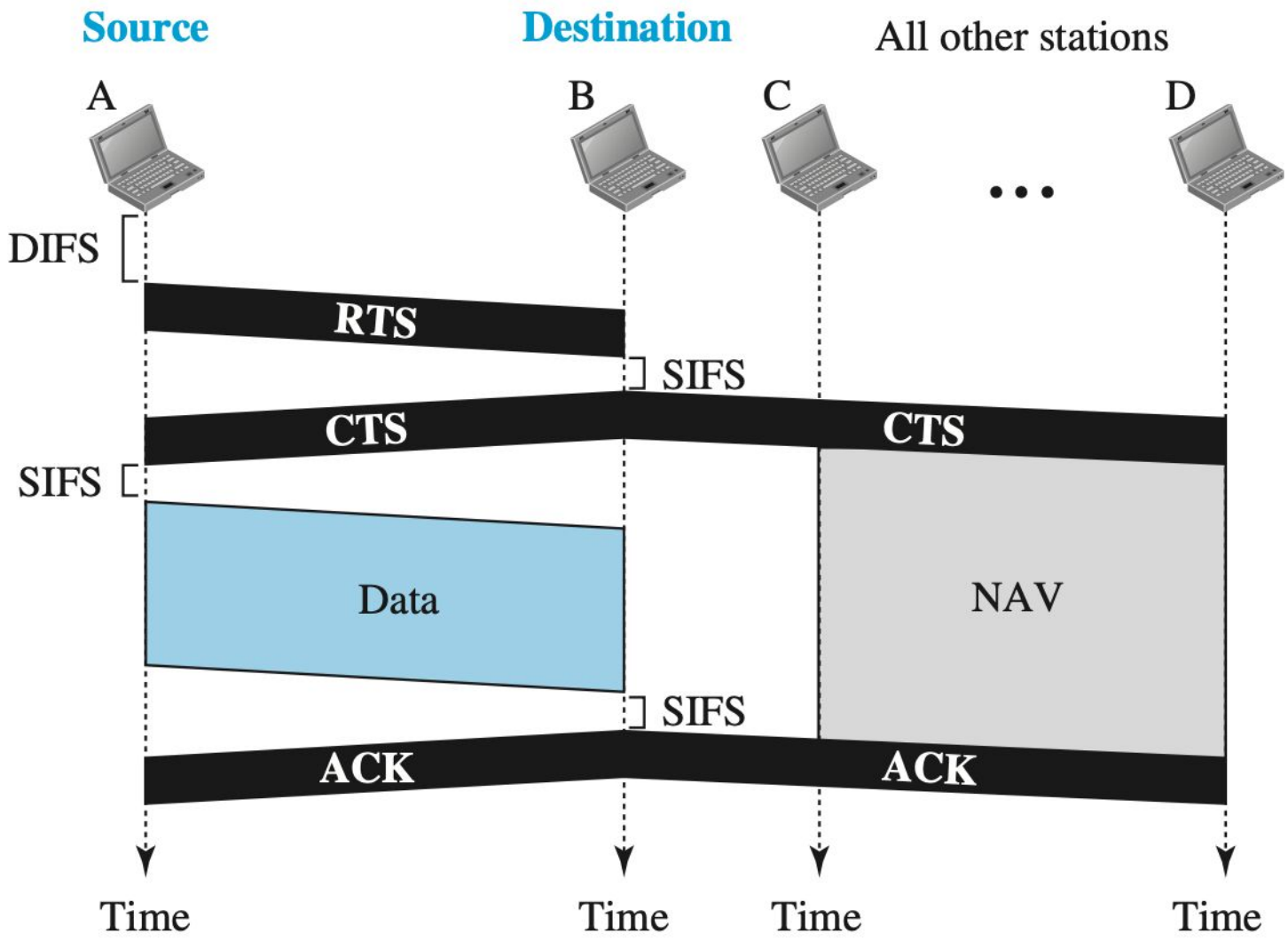
Figure 12.16 *Contention window*



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.

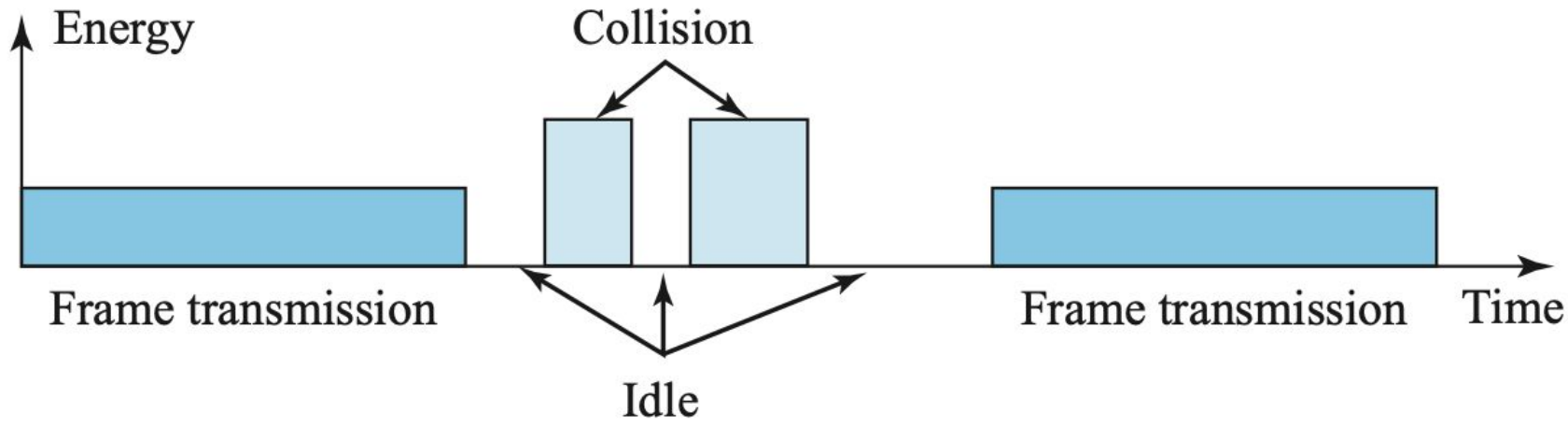
Figure 12.17 *CSMA/CA and NAV*



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.

Figure 12.14 *Energy level during transmission, idleness, or collision*



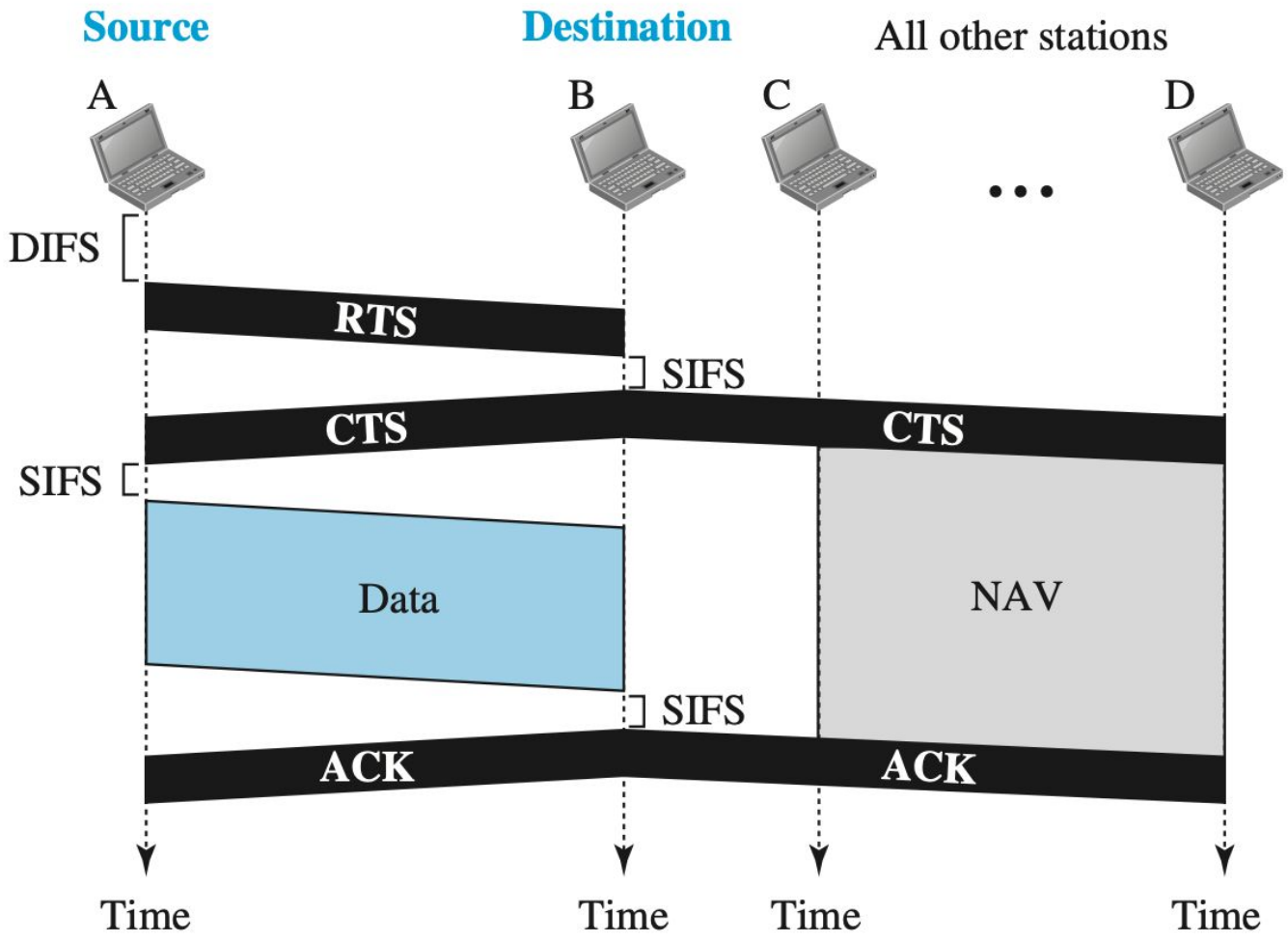
FRAME EXCHANGE TIME LINE

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency.
   a) The channel uses a persistence strategy with backoff until the channel is idle.
   b) After the station is found to be idle, the station waits for a period of time called the DCF interframe space (DIFS); then the station sends a control frame called the request to send (RTS).

FRAME EXCHANGE TIME LINE

2. After receiving the RTS and waiting a period of time called the short interframe space (SIFS), the destination station sends a control frame, called the clear to send (CTS), to the source station. This control frame indicates that the destination station is ready to receive data.
3. The source station sends data after waiting an amount of time equal to SIFS.
4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received.

Figure 12.17 *CSMA/CA and NAV*



NETWORK ALLOCATION VECTOR

- How do other stations defer (delay or postpone) sending their data if one station acquires access?
- The key is a feature called NAV.
- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness.
- Each time a station accesses the system and sends an RTS frame, other stations start their NAV.

COLLISION DURING HANDSHAKING

- Two or more stations may try to send RTS frames at the same time.
- These control frames may collide.
- However, because there is no mechanism for collision detection, the sender assumes there has been a collision if it has not received a CTS frame from the receiver.
- The backoff strategy is employed, and the sender tries again.

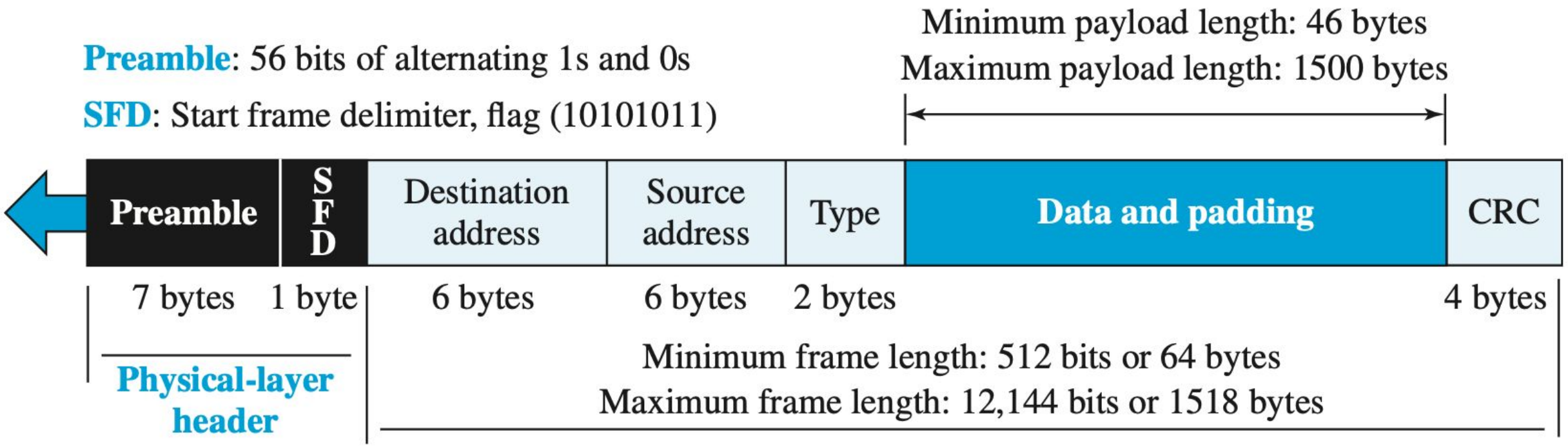
HIDDEN-STATION PROBLEM

- The solution to the hidden station problem is the use of the handshake frames (RTS and CTS).
- RTS message from B reaches A, but not C.
- However, because both B and C are within the range of A, the CTS message, which contains the duration of data transmission from B to A, reaches C.
- Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

ETHERNET EVOLUTION

- The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs.
- Since then, it has gone through four generations:
- Standard Ethernet (10 Mbps), IEE Standard **802.3i**
- Fast Ethernet (100 Mbps), IEE Standard **802.3u**
- Gigabit Ethernet (1 Gbps), IEE Standard **802.3z**
- 10 Gigabit Ethernet (10 Gbps) IEE Standard **802.3ae**

Figure 13.3 *Ethernet frame*



FAST ETHERNET (100 MBPS)

- IEEE 802.3u standard
- Upgrade the data rate to 100 Mbps.
- Make it compatible with Standard Ethernet.
- Keep the same 48-bit address.
- Keep the same frame format.

AUTONEGOTIATION

- A new feature added to Fast Ethernet is called autonegotiation.
- It allows a station or a hub a range of capabilities.
- Autonegotiation allows two devices to negotiate the mode or data rate of operation.
- It was designed particularly to allow incompatible devices to connect to one another.
- For example, a device with a maximum data rate of 10 Mbps can communicate with a device with a 100 Mbps data rate (but which can work at a lower rate).

Table 13.2 *Summary of Fast Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	UTP or STP	100 m	2	4B5B + MLT-3
100Base-FX	Fiber	185 m	2	4B5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

GIGABIT ETHERNET

- IEEE 802.3z standard
- Upgrade the data rate to 1 Gbps.
- Make it compatible with Standard or Fast Ethernet.
- Use the same 48-bit address.
- Use the same frame format.
- Keep the same minimum and maximum frame lengths.
- Support autonegotiation as defined in Fast Ethernet.

Table 13.3 *Summary of Gigabit Ethernet implementations*

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
1000Base-SX	Fiber S-W	550 m	2	8B/10B + NRZ
1000Base-LX	Fiber L-W	5000 m	2	8B/10B + NRZ
1000Base-CX	STP	25 m	2	8B/10B + NRZ
1000Base-T4	UTP	100 m	4	4D-PAM5

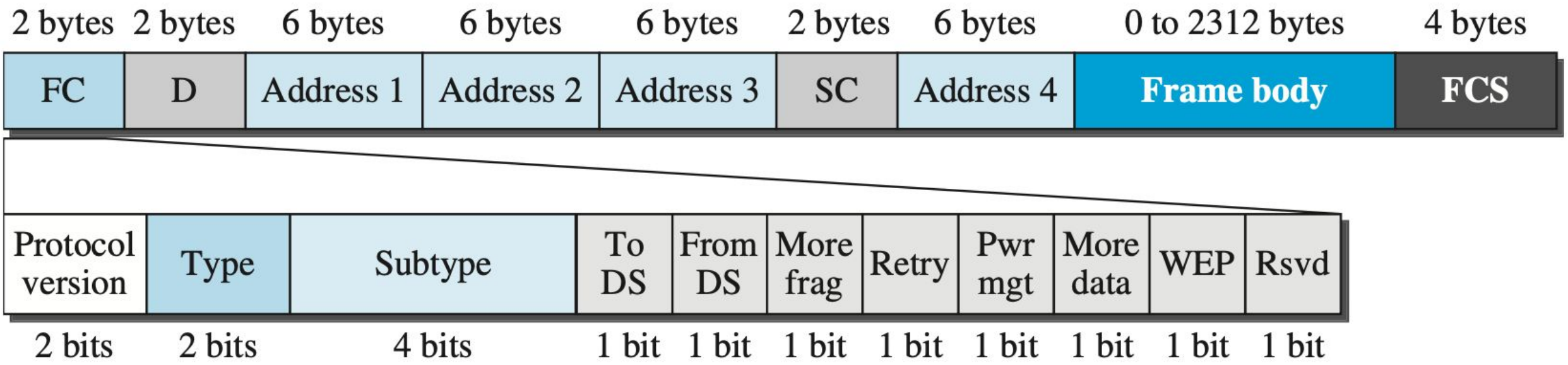
IEEE 802.11

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data-link layers. It is sometimes called wireless Ethernet.
- The public uses the term Wi-Fi (short for wireless fidelity) as a synonym for wireless LAN.

Table 1. Technology comparison.

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Frequency band	5.7 GHz	2.4 GHz	2.4 GHz	2.4 / 5 GHz
Average Theoretical speed	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Modulation	OFDM	CCK modulated with QPSK	DSSS, CCK, OFDM	OFDM
Channel bandwidth	20 MHz	20 MHz	20 MHz	20 / 40 MHz
Coverage radius	35 m	38 m	38 m	75 m
Unlicensed spectrum	Yes (it depends on countries)	Yes	Yes	Yes (it depends on countries)
Radio Interference	Low	High	High	Low
Introduction cost	Medium-Low	Low	Low	High-medium
Device cost	Medium-Low	Low	Low	Medium
Mobility	Yes	Yes	Yes	Yes
Current use	Medium	High	High	High
Security	Medium	Medium	Medium	High

Figure 15.9 *Frame format*



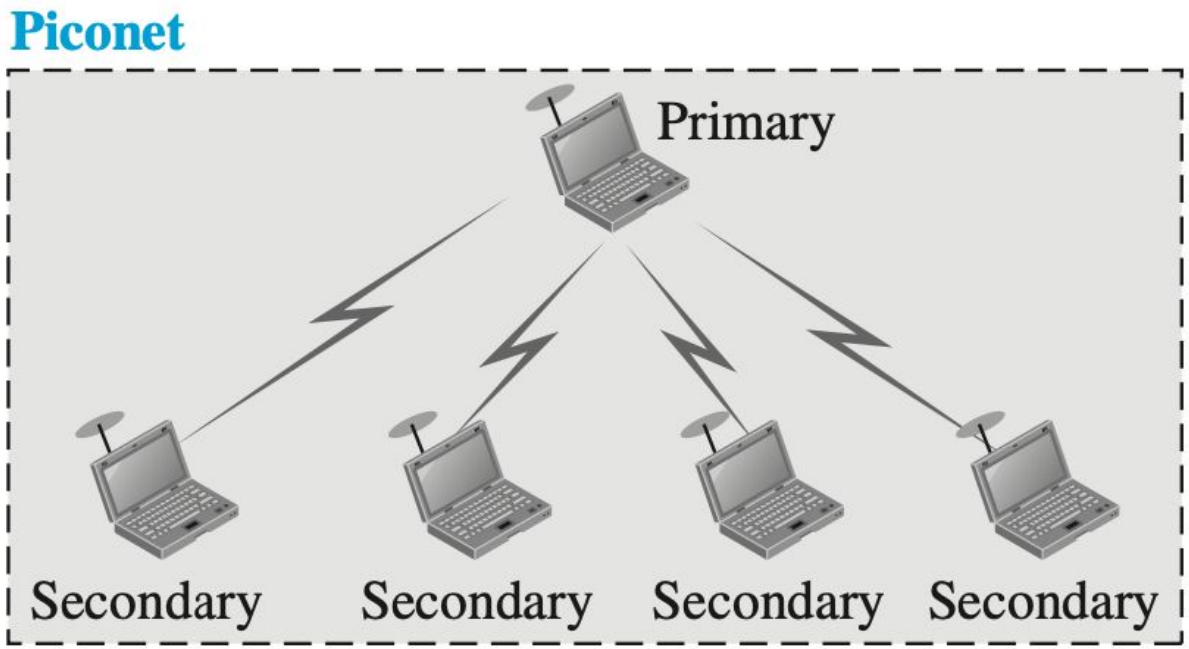
IEEE 802.15

- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.
- Bluetooth defines two types of networks: piconet and scatternet.

PICONET

- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- A piconet can have only one primary station.
- The communication between the primary and secondary stations can be one-to-one or one-to-many.

Figure 15.17 *Piconet*



SCATTERNET

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.

Figure 15.18 *Scatternet*

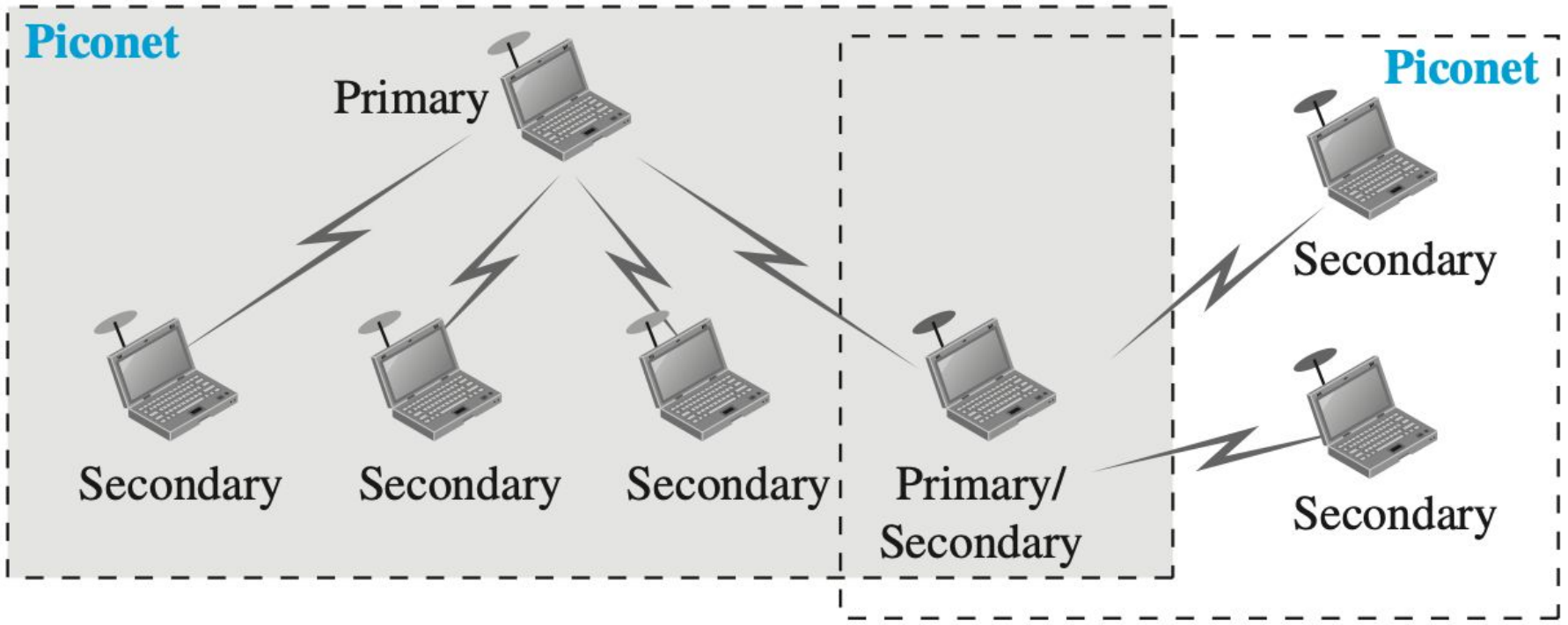
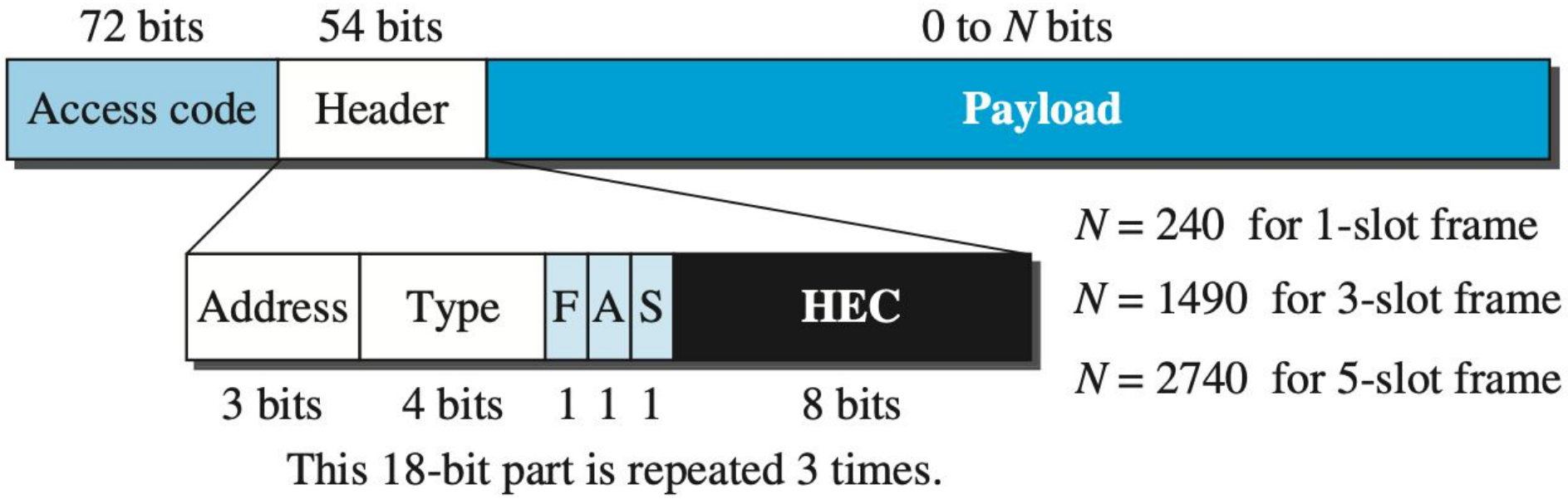


Figure 15.23 *Frame format types*



IEEE 802.16

- WiMAX is the result of the IEEE 802.16 project, which was an effort to standardize the proprietary broadband wireless system in 2002.
- The standard is sometimes referred to as wireless local loop, in contrast with wired local loop (dial-up, DLS, or cable).
- 802.11 is a standard for a wireless LAN; 802.16 is a standard for a wireless WAN (or MAN).
- The distance between a base station and a host in the first is very limited; the base station and subscriber station in the second may be separated by tens of kilometers.

Figure 16.4 *WiMAX MAC frame format*