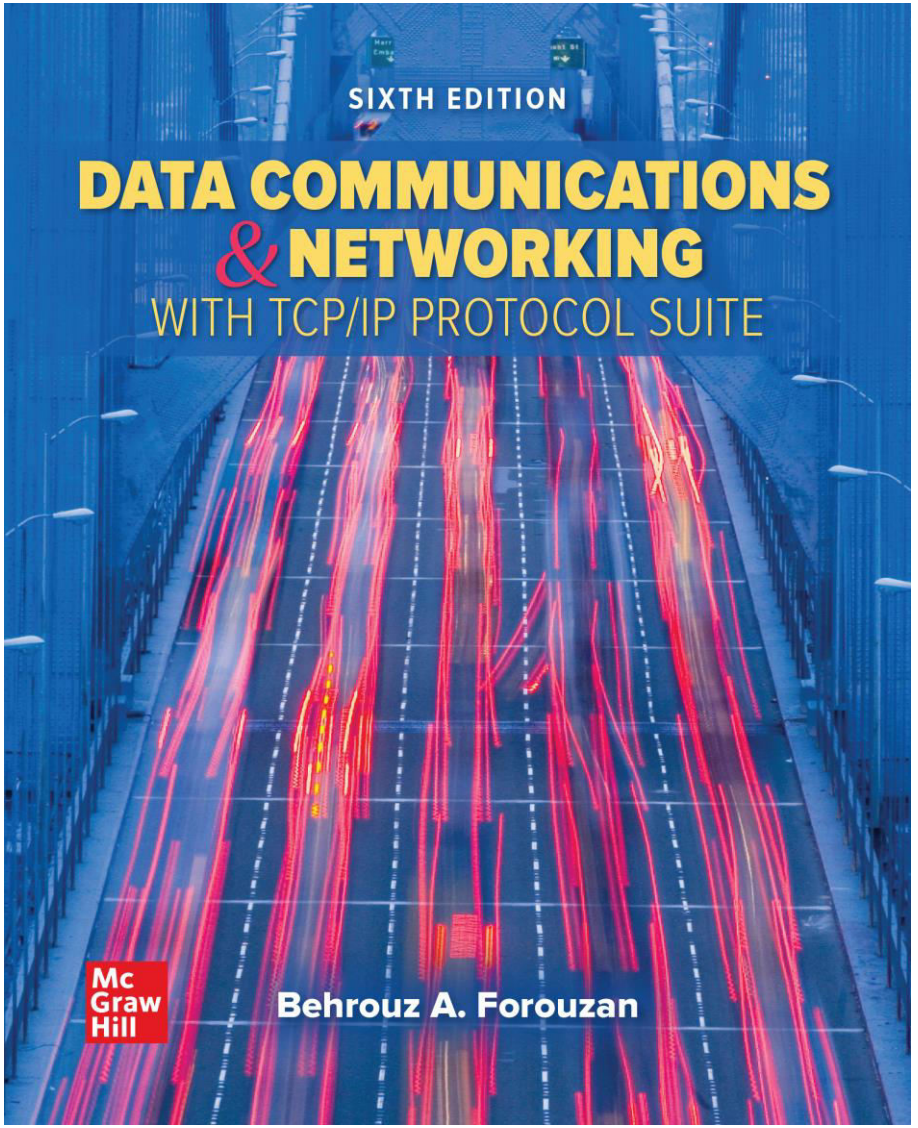
Because learning changes everything.®



Chapter 03

Data-Link Layer

Data Communications and Networking, With TCP/IP protocol suite
Sixth Edition
Behrouz A. Forouzan

Chapter 3: Outline

3.1 INTRODUCTION

3.2 DATA LINK CONTROL

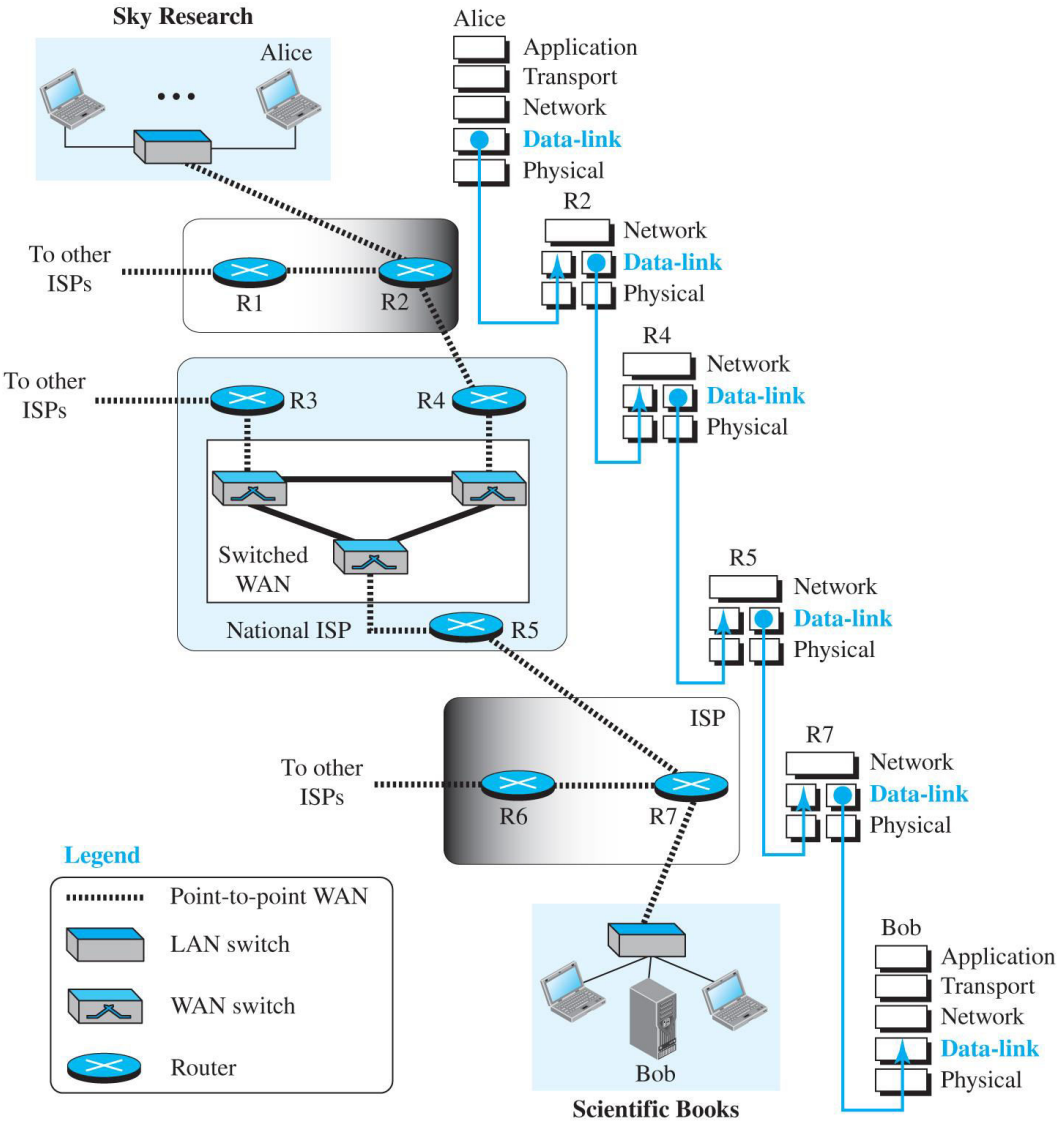
3.3 MEDIA ACCESS CONTROL

3.4 LINK-LAYER ADDRESSING

3-1 INTRODUCTION

The Internet is a combination of networks glued together by connecting devices (routers or switches). If a packet is to travel from a host to another host, it needs to pass through these networks. Figure 3.1 shows the same scenario we discussed in Chapter 2, but we are now interested in communication at the data-link layer.

Figure 3.1 Communication at the data-link layer

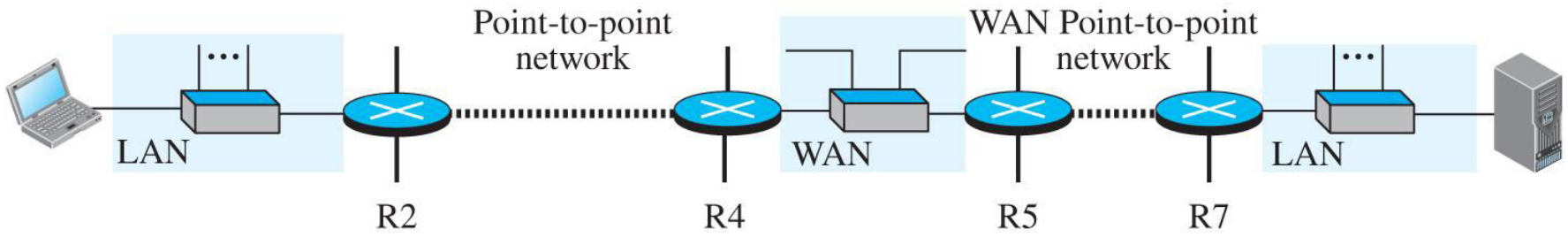


Access the text alternative for slide images.

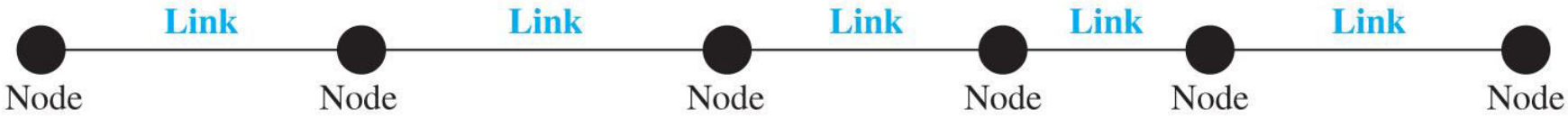
3.1.1 Nodes and Links

Communication at the data-link layer is node-to-node. A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point. Theses LANs and WANs are connected by routers. It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links. Figure 3.2 is a simple representation of links and nodes when the path of the data unit is only six nodes.

Figure 3.2 Nodes and Links



a. A small part of the Internet



b. Nodes and links

Access the text alternative for slide images.

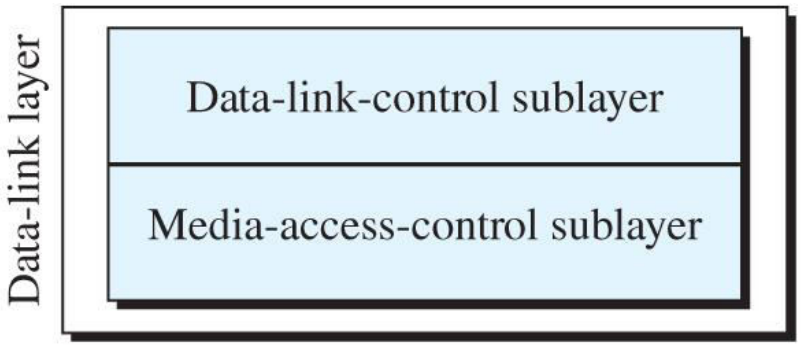
3.1.2 Two Types of Links

Although two nodes are physically connected by a transmission medium such as cable or air, we need to remember that the data-link layer controls how the medium is used. We can have a data-link layer that uses the whole capacity of the medium; we can also have a data-link layer that uses only part of the capacity of the link. In other words, we can have a point-to-point link or a broadcast link.

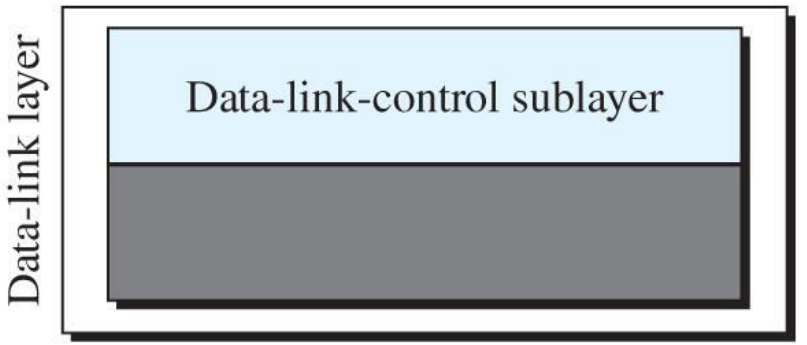
3.1.3 Two Sublayers

To better understand the functionality of and the services provided by the link layer, we can divide the data-link layer into two sublayers: data link control (DLC) and media access control (MAC). This is not unusual because, as we will see in later chapters, LAN protocols actually use the same strategy.

Figure 3.3 Dividing the data-link layer into two sublayers



a. Data-link layer of a broadcast link



b. Data-link layer of a point-to-point link

Access the text alternative for slide images.

3-2 Data Link Control (DLC)

The data link control (DLC) deals with procedures for communication between two adjacent nodes no matter whether the link is dedicated or broadcast. Data link control functions include framing and flow and error control.

3.2.1 Framing

The data-link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.

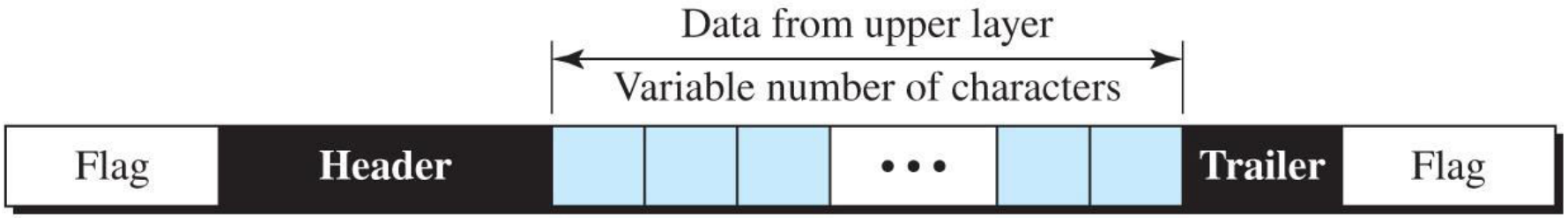
Frame Size

Frames can be fixed or variable size. In the first, there is no need to define the boundary of the frame; in the second, we need to do so.

Character-Oriented Framing

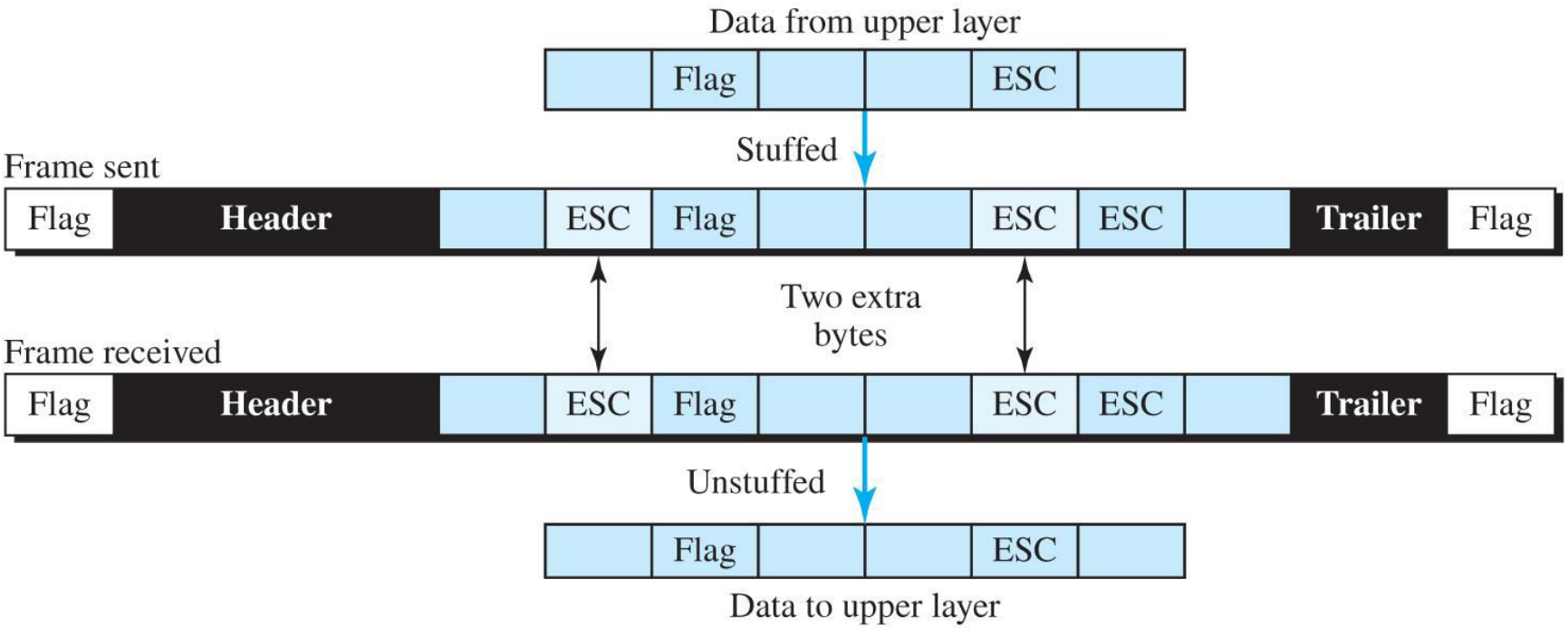
In this type of framing, data to be carried are 8-bit characters (Figure 3.4). In this type of framing, we need to do byte-stuffing to prevent a special character to be interpreted as beginning or end of the message.

Figure 3.4 A frame in a character-oriented protocol



Access the text alternative for slide images.

Figure 3.5 Byte stuffing and unstuffing

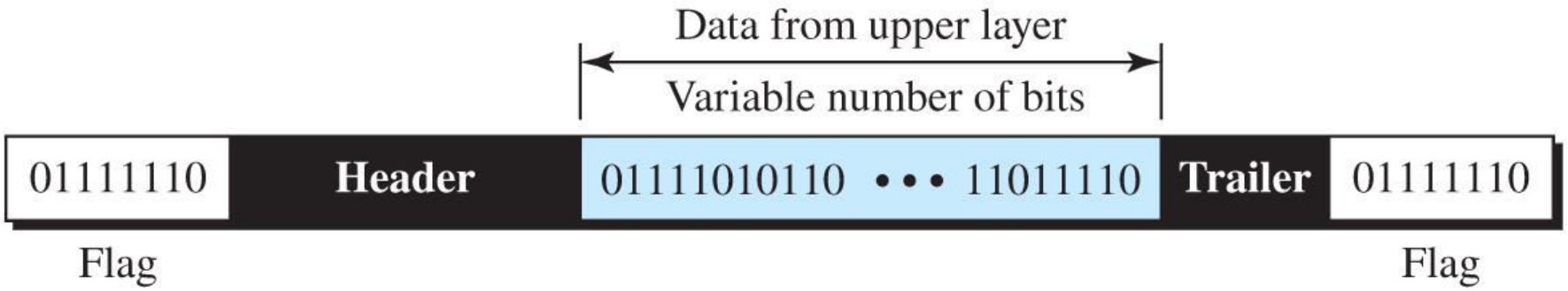


Access the text alternative for slide images.

Bit-Oriented Framing

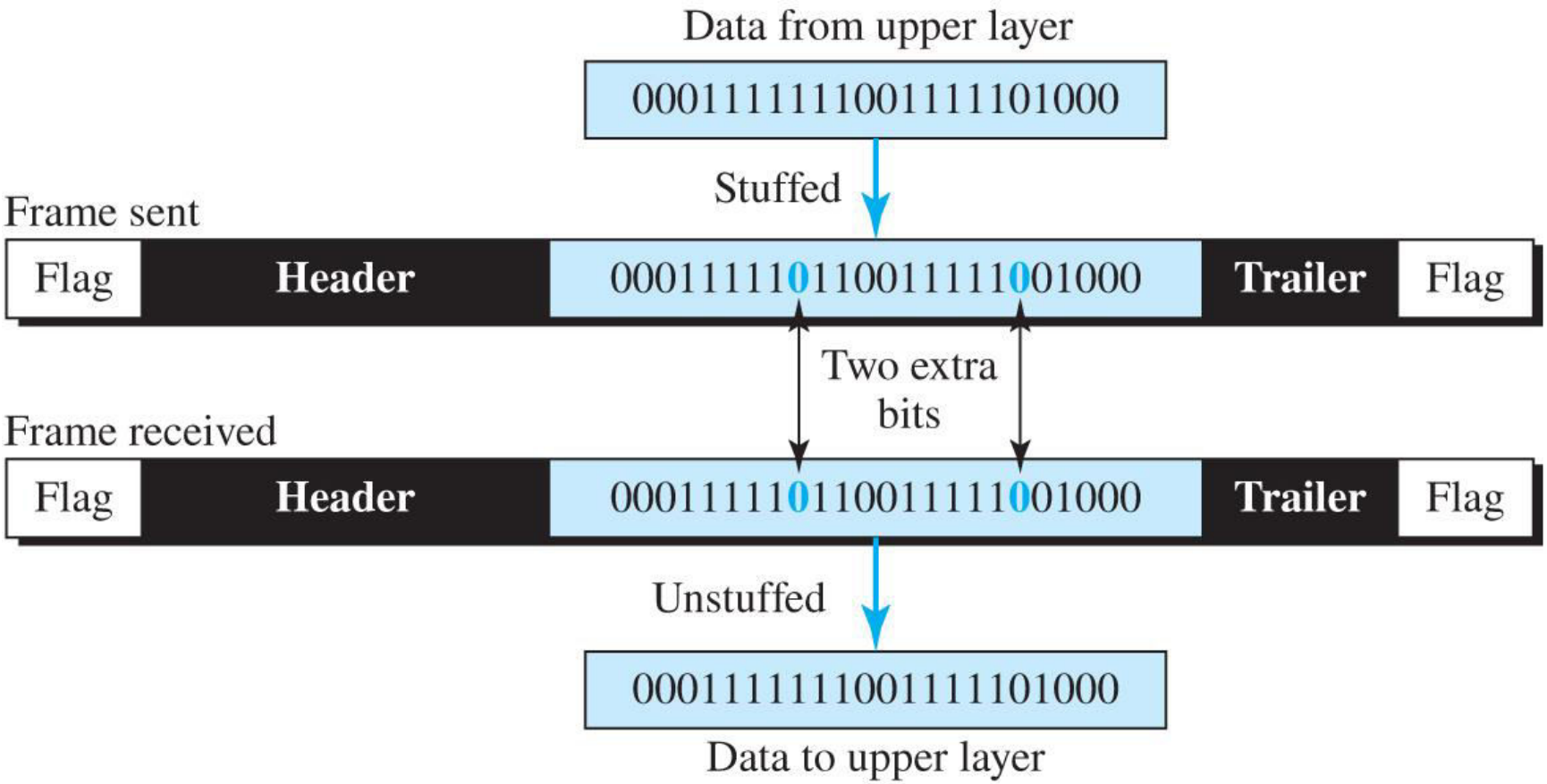
In bit-oriented framing data is a sequence of bits. To separate one frame from another, we normally use an 8-bit flag (01111110). To prevent that a byte to be interpreted as a flag, we do bit stuffing (Figure 3.7).

Figure 3.6 A frame in a bit-oriented protocol



Access the text alternative for slide images.

Figure 3.7 Bit stuffing and unstuffing



Access the text alternative for slide images.

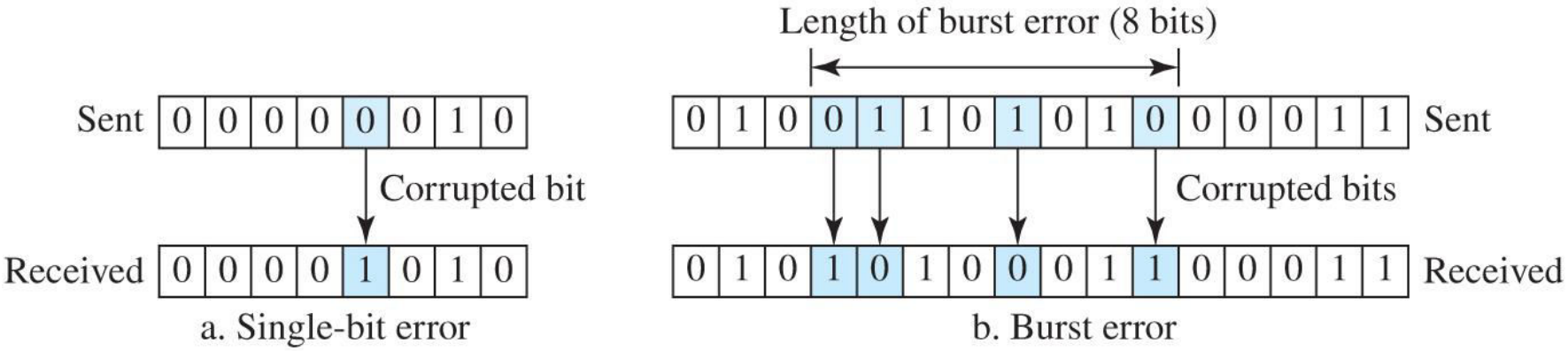
3.2.2 Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damage in transition and coordinates the retransmission of frames by the sender.

Types of Error

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1. The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1. Figure 3.8 shows the effect of a single-bit and a burst error on a data unit.

Figure 3.8 Single-bit and burst error

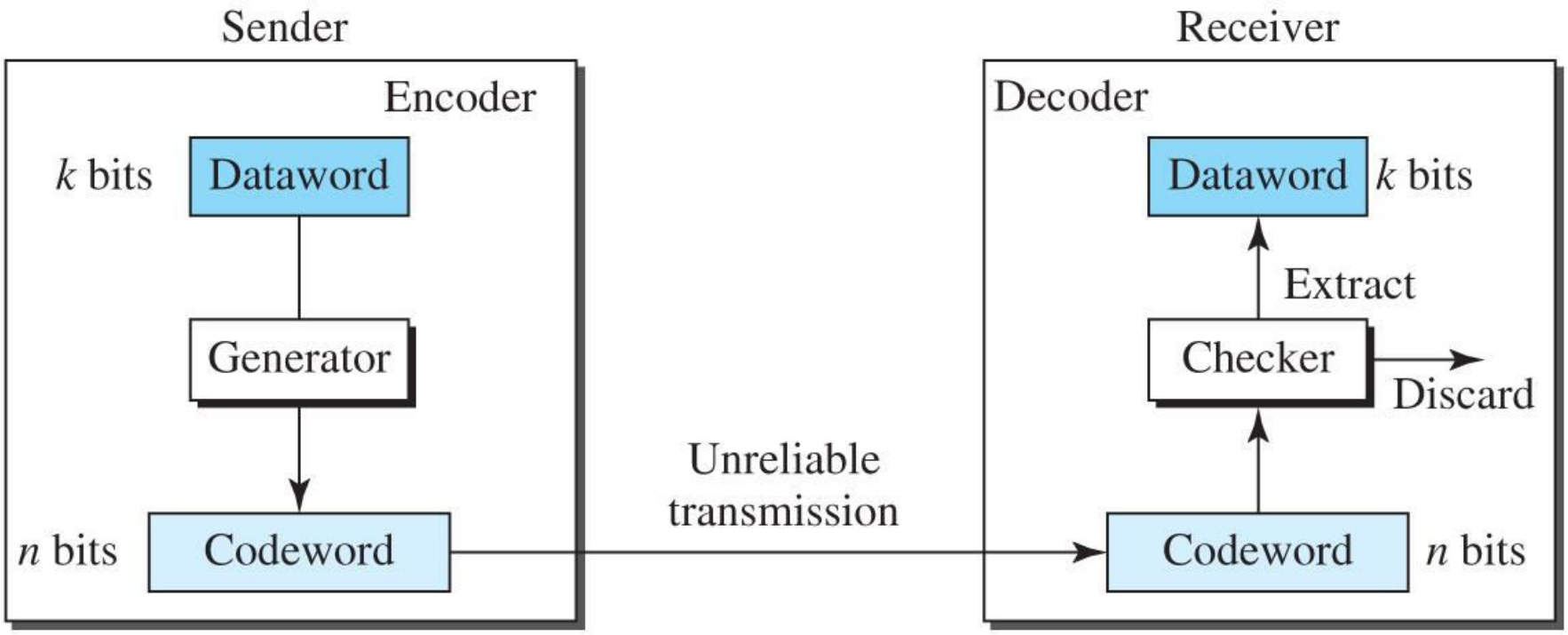


Access the text alternative for slide images.

Block Coding

In block coding, we divide our message into blocks, each of k bits, called data-words. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called codewords. How the extra r bits are chosen or calculated is something we will discuss later.

Figure 3.9 Process of error detection in block coding



Access the text alternative for slide images.

Example 3.1 (1)

Let us assume that k = 2 and n = 3. Table 3.1 shows the list of datawords and codewords. Later, we will see how to derive a codeword from a dataword.

Table 3.1 A code for error detection in Example 3.1

Datawords	*Codewords*	*Datawords*	*Codewords*
00	000	10	101
01	011	11	110

Example 3.1 (2)

1. The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it.

2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.

3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable.

Hamming Distance

One of the central concepts in coding for error control is the idea of the Hamming distance. The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. The Hamming distance can easily be found if we apply the XOR operation (Å) on the two words and count the number of 1s in the result. Note that the Hamming distance is a value greater than or equal to zero.

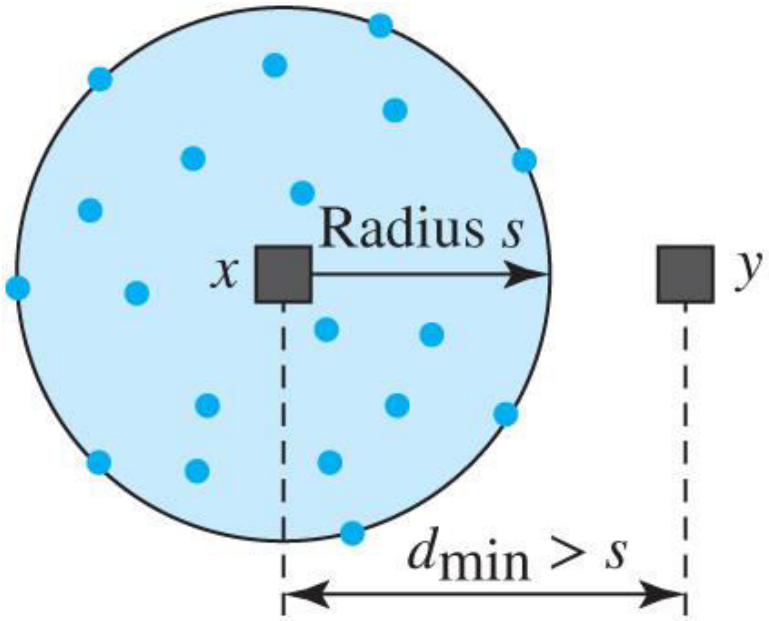
Example 3.2

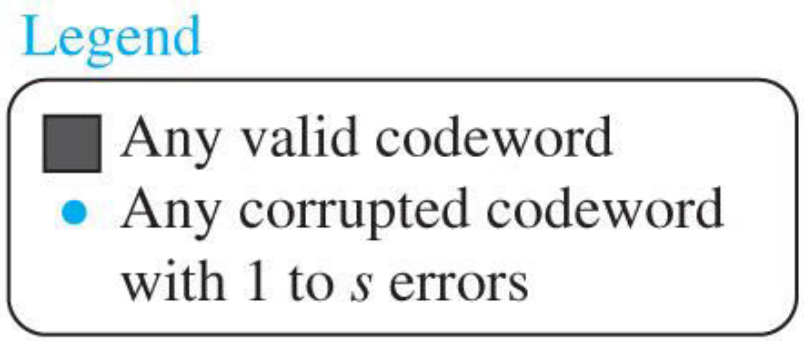
Let us find the Hamming distance between two pairs of words.

1. The Hamming distance ***d*** (000, 011) is 2 because (000 XOR 011) is 011 (two 1s).

2. The Hamming distance ***d*** (10101, 11110) is 3 because (10101 XOR 11110) is 01011 (three 1s).

Figure 3.10 Geometric concept explaining d_{min} in error detection





Access the text alternative for slide images.

Example 3.3

The minimum Hamming distance for our first code scheme (Table 3.1) is 2. This code guarantees detection of only a single error. For example, if the third codeword (101) is sent and one error occurs, the received codeword does not match any valid codeword. If two errors occur, however, the received codeword may match a valid codeword and the errors are not detected.

Example 3.4

A code scheme has a Hamming distance $\boldsymbol{d}_{min} = 4$. This code guarantees the detection of up to three errors ($\boldsymbol{d} = s + 1$ or $\boldsymbol{s} = 3$).

Linear Block Codes 1

- *Almost all block codes used today belong to subset of a block code called linear block code. For our purposes, a linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.*

- *It is simple to find the minimum Hamming distance for a linear block code. The minimum Hamming distance is the number of 1s in the nonzero valid codeword with the smallest number of 1s*

Example 3.5

The code in Table 3.1 is a linear block code because the result of XORing any codeword with any other codeword is a valid codeword. For example, the XORing of the second and third codewords creates the fourth one.

Linear Block Codes 2

Perhaps the most familiar error-detecting code is the parity-check code. This code is a linear block code. In this code, a k-bit dataword is changed to an n-bit codeword where n = k + 1. The extra bit, called the parity bit, is selected to make the total number of 1s in the codeword even.

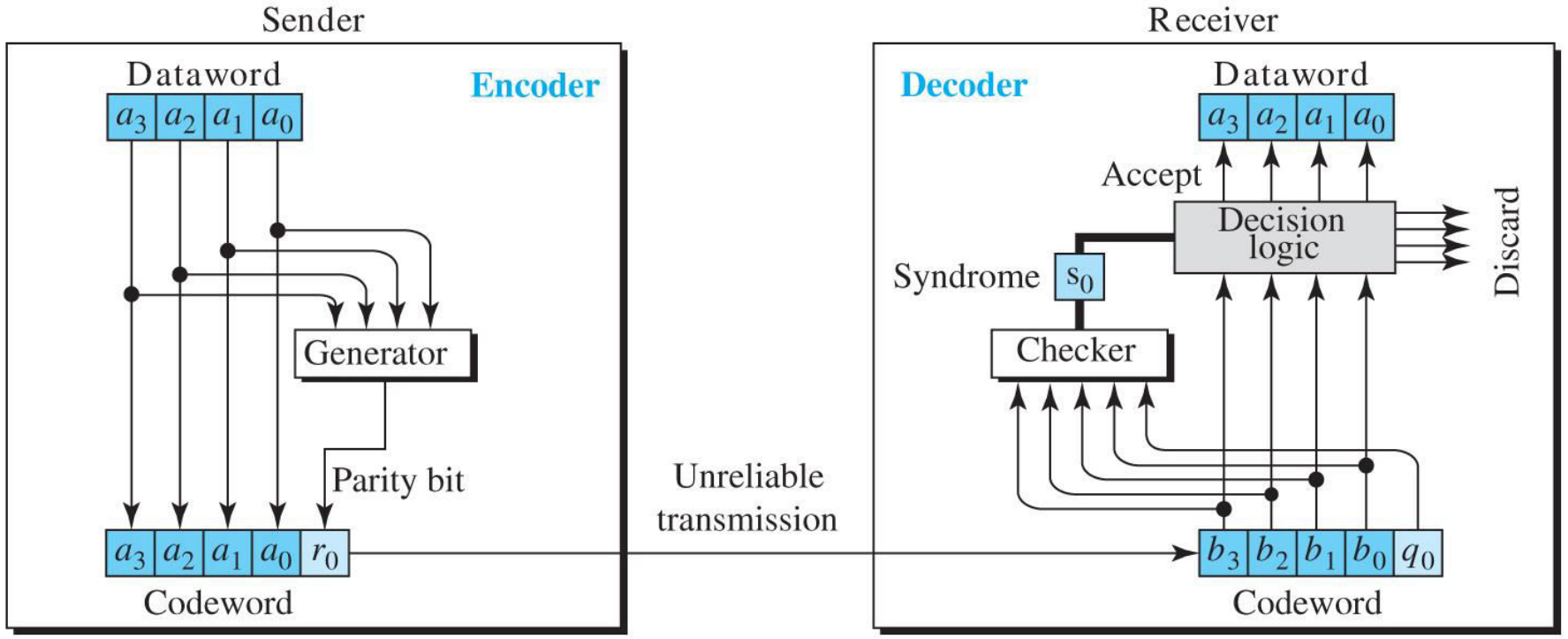
Example 3.6

In our first code (Table 3.1), the numbers of 1s in the nonzero codewords are 2, 2, and 2. So the minimum Hamming distance is $\boldsymbol{d}_{\text{min}} = 2$.

Table 3.2 Simple parity-check code C(5, 4)

Datawords	**Codewords**	*Datawords*	**Codewords**
0000	**00000**	1000	**10001**
0001	**00011**	1001	**10010**
0010	**00101**	1010	**10100**
0011	**00110**	1011	**10111**
0100	**01001**	1100	**11000**
0101	**01010**	1101	**11011**
0110	**01100**	1110	**11101**
0111	**01111**	1111	**11110**

Figure 3.11 Encoder and decoder for simple parity-check code



Access the text alternative for slide images.

Example 3.7 (1)

Let us look at some transmission scenarios. Assume the sender sends the dataword 1011. The codeword created from this dataword is 10111, which is sent to the receiver. We examine five cases:

1. No error occurs; the received codeword is 10111. The syndrome is 0. The dataword 1011 is created.

2. One single-bit error changes a_1. The received codeword is 10**0**11. The syndrome is 1. No dataword is created.

Example 3.7 (2)

3. One single-bit error changes r_0. The received codeword is 1011**0**. The syndrome is 1. No dataword is created. Note that although none of the dataword bits are corrupted, no dataword is created because the code is not sophisticated enough to show the position of the corrupted bit.

4. An error changes r_0 and a second error changes a_3. The received codeword is **0**011**0**. The syndrome is 0. The dataword 0011 is created at the receiver. Note that here the dataword is wrongly created due to the syndrome value. The simple parity-check decoder cannot detect an even number of errors. The errors cancel each other out and give the syndrome a value of 0.

Example 3.7 (3)

5. Three bits—a_3, a_2, and a_1—are changed by errors. The received codeword is **010**11. The syndrome is 1. The dataword is not created. This shows that the simple parity check, guaranteed to detect one single error, can also find any odd number of errors.

A parity-check code can detect an odd number of errors.

Cyclic Codes

- *Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword. For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword.*

- *We can create cyclic codes to correct errors. However, the theoretical background required is beyond the scope of this book. In this section, we simply discuss a subset of cyclic codes called the cyclic redundancy check (CRC), which is used in networks such as LANs and WANs.*

CRC introduced by Hamming

Used in high speed data networks

3 key aspects:

- *CRC supports Arbitrary length message*
- *Excellent error detection*
- *Fast Hardware implementation, CPU can do CRC computation fast*

Theory behind CRC

Given a from of k-bit

Transmitter generates n-bit sequence called FCS (frame check sequence)

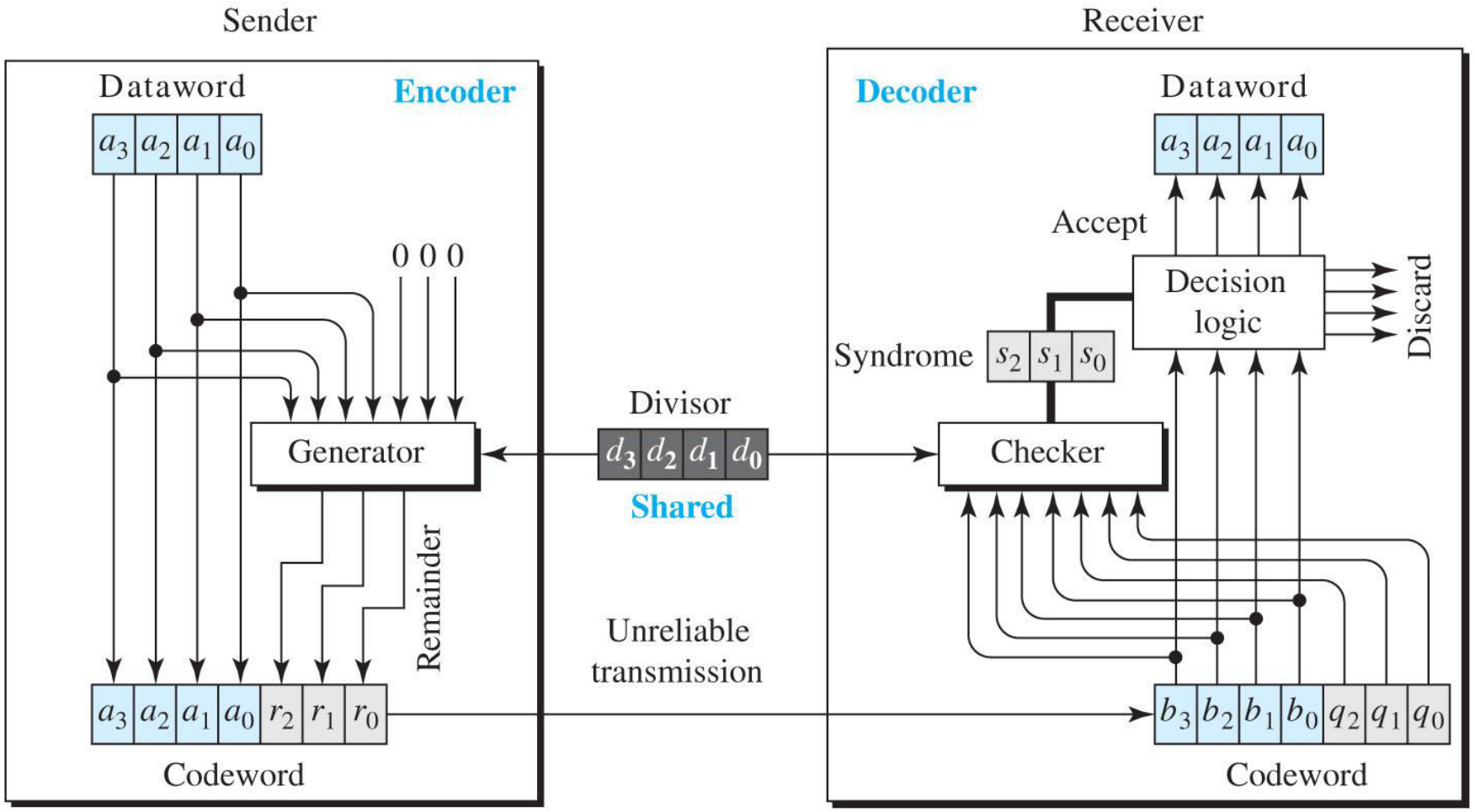
The k+n bit is divisible by some predetermined number.

The receiver divides the total by the predetermined number. If no remainder, then the block is fine.

Table 3.3 A CRC code with C(7, 4)

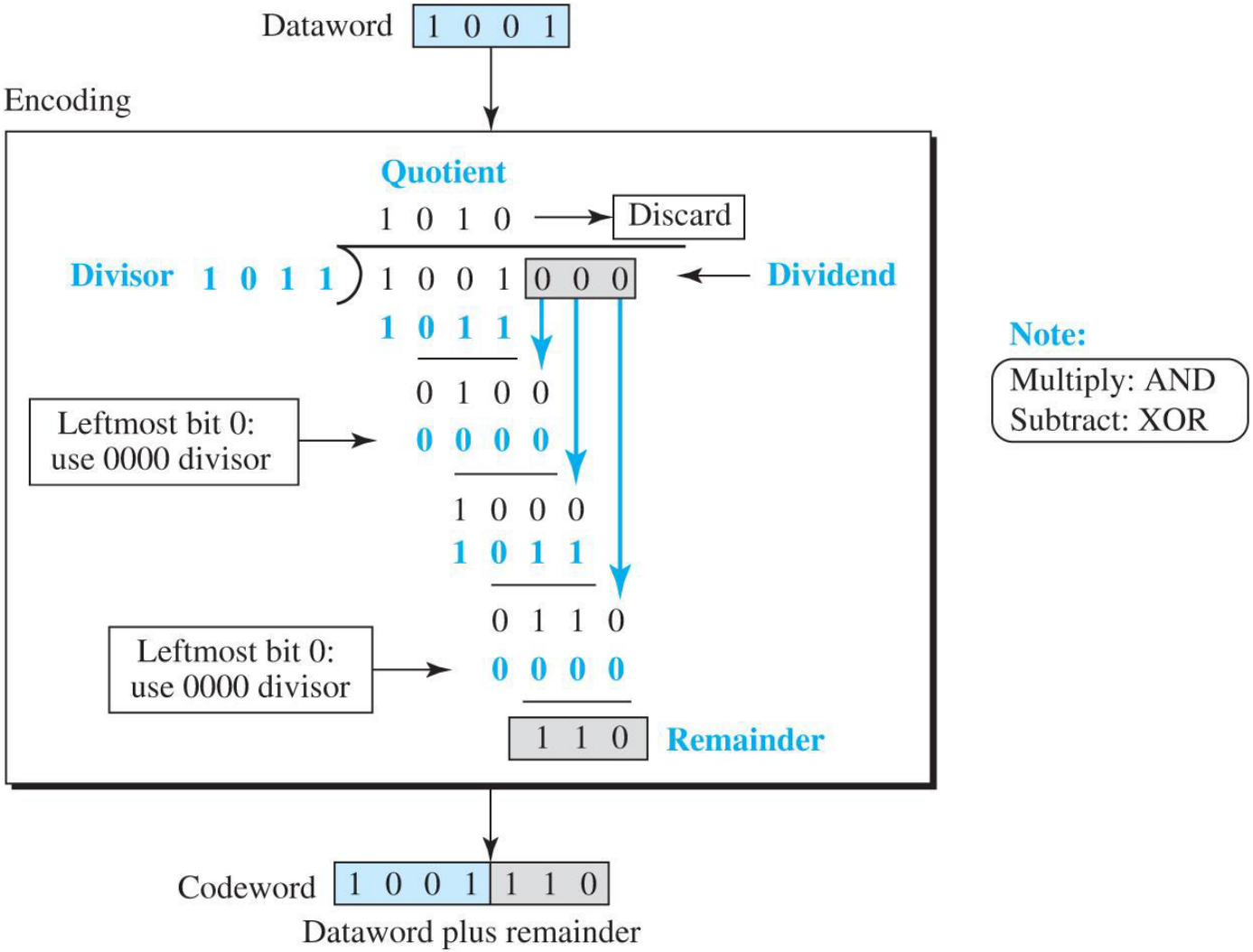
Datawords	*Codewords*	*Datawords*	*Codewords*
0000	**0000000**	1000	**1000101**
0001	**0001011**	1001	**1001110**
0010	**0010110**	1010	**1010011**
0011	**0011101**	1011	**1011000**
0100	**0100111**	1100	**1100010**
0101	**0101100**	1101	**1101001**
0110	**0110001**	1110	**1110100**
0111	**0111010**	1111	**1111111**

Figure 3.12 CRC encoder and decoder



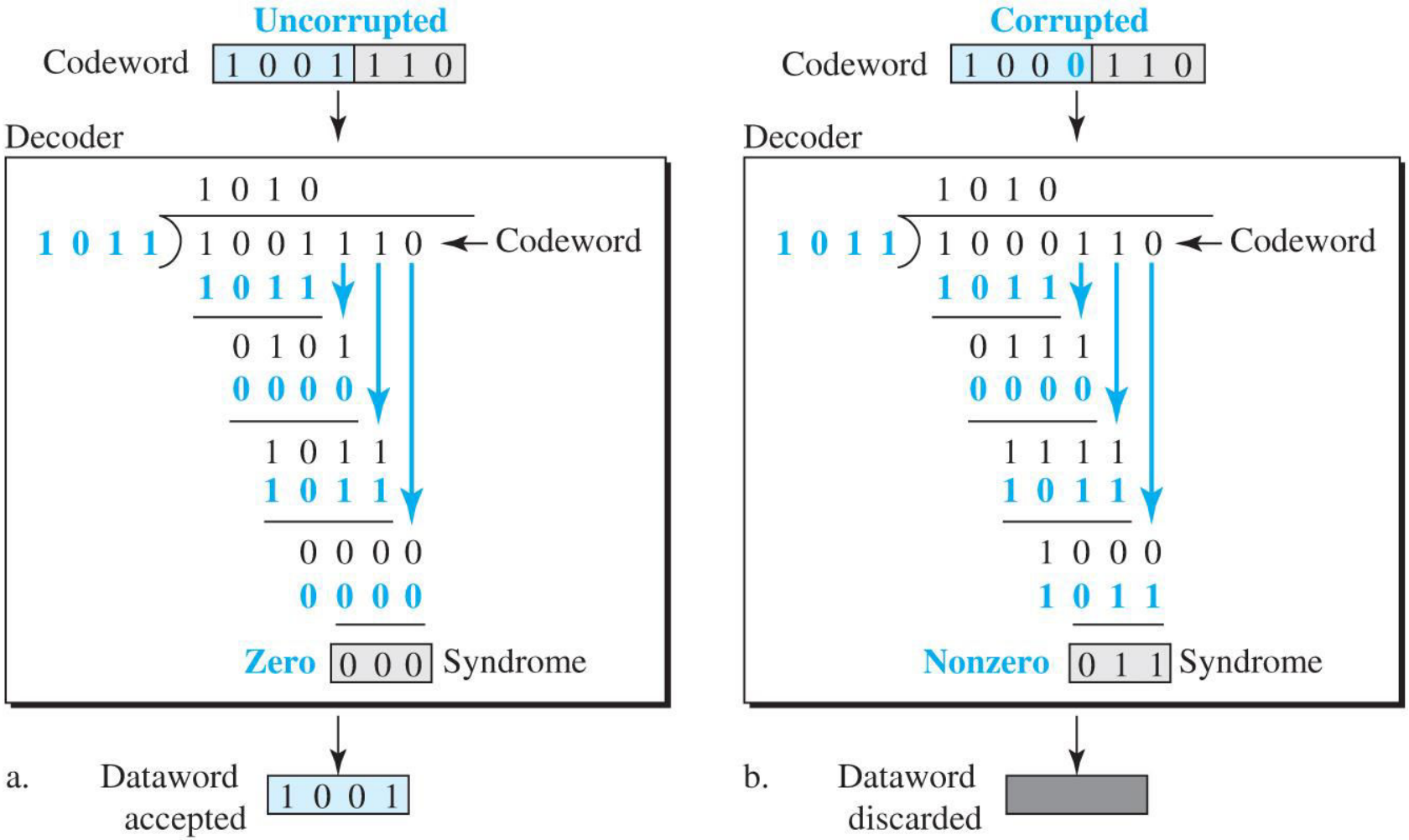
Access the text alternative for slide images.

Figure 3.13 Division in CRC encoder



Access the text alternative for slide images.

Figure 3.14 Division in the CRC decoder for two cases



Access the text alternative for slide images.

Table 3.4 Standard polynomials

Name	Binary	Application
CRC-8	100000111	ATM header
CRC-10	11000110101	ATM AAL
CRC-16	10001000000100001	HDLC
CRC-32	100000100110000010001110110110111	LANs

Checksum

Checksum is an error-detecting technique that can be applied to a message of any length. In the Internet, the checksum technique is mostly used at the network and transport layer rather than the data-link layer. We discuss it when we discuss the network layer.

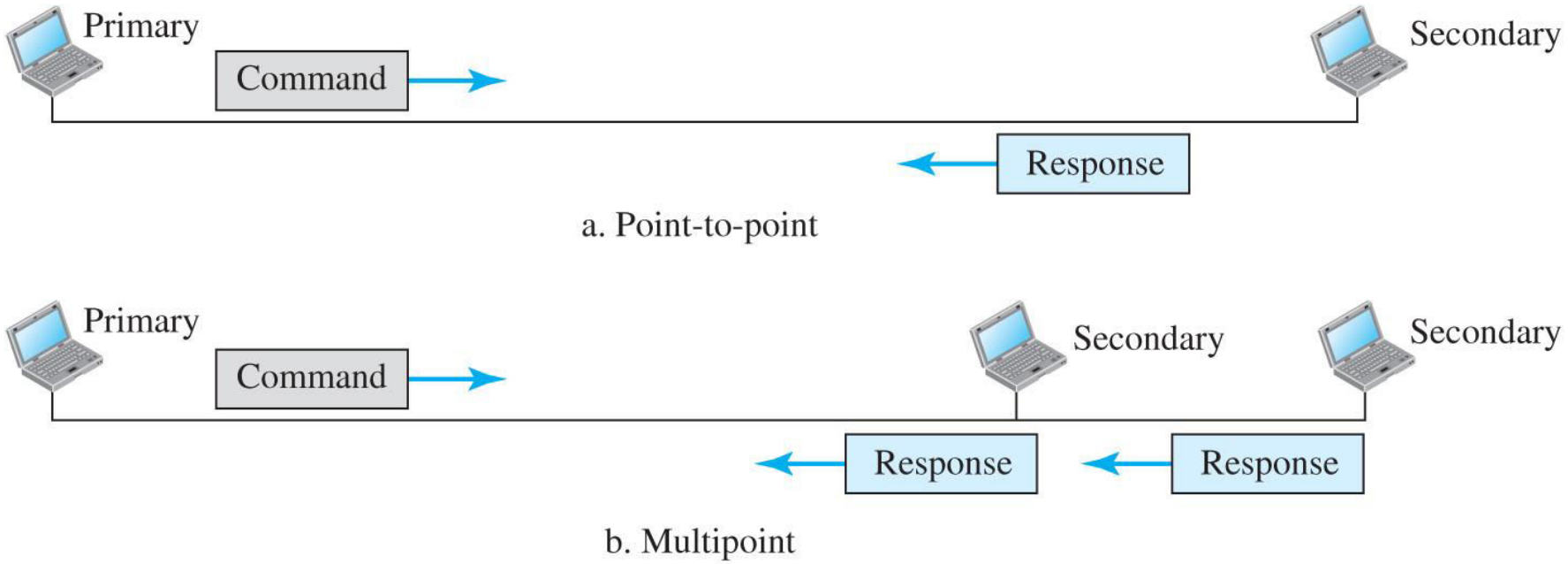
3.2.3 Two DLC Protocols

After finishing all issues related to DLC sublayer, we discuss two DCL protocols that actually implement these concepts: HDLC and Point-to-Point.

HDLC

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point-to-point and multipoint links. It implements the stop-and-wait protocol we discussed earlier.

Figure 3.15 Normal response mode

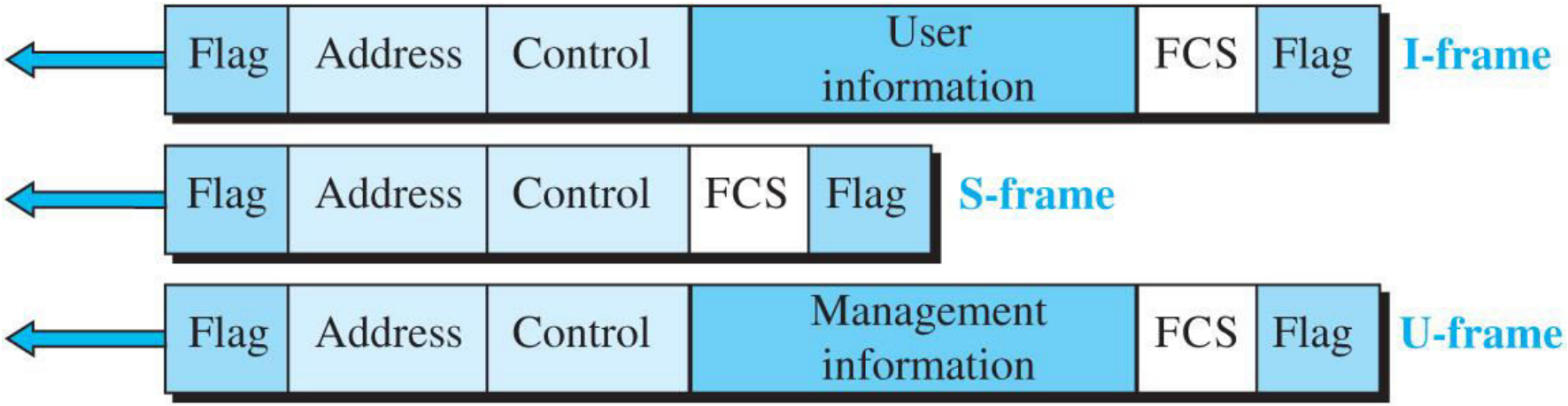


Access the text alternative for slide images.

Figure 3.16 Asynchronous balanced mode

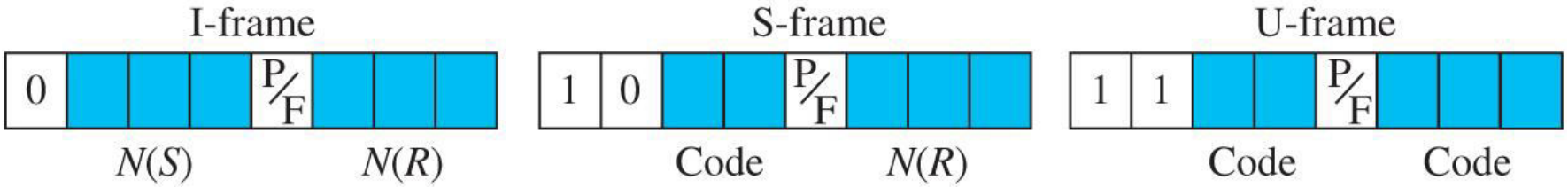
Access the text alternative for slide images.

Figure 3.17 HDLC frames



Access the text alternative for slide images.

Figure 3.18 Control field format for the different frame types

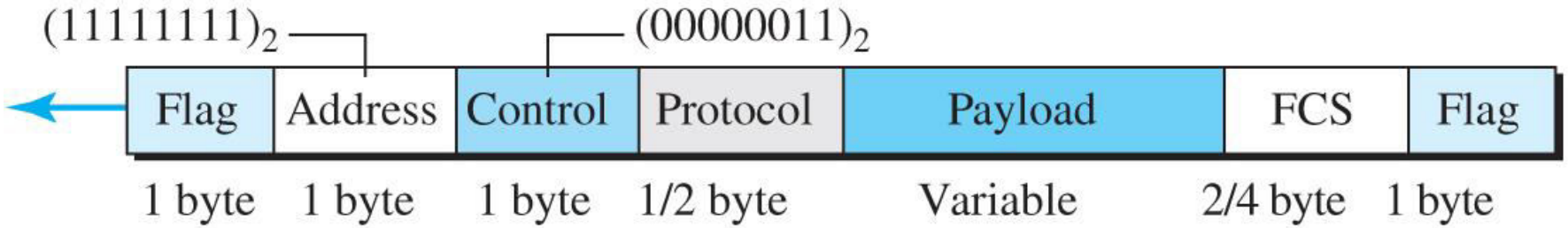


Access the text alternative for slide images.

Point-to-Point Protocol (PPP)

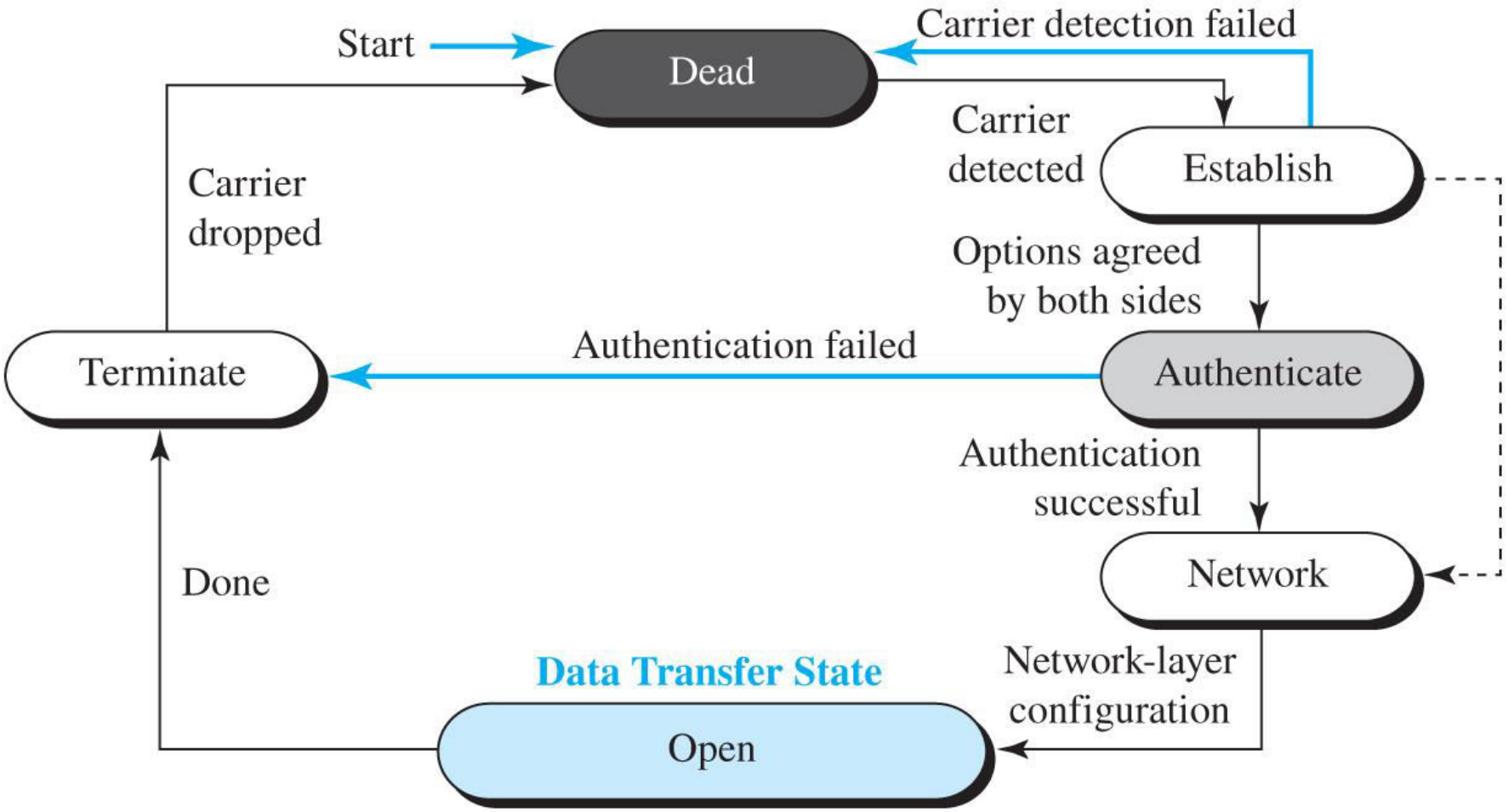
One of the most common protocols for point-to-point access is the point-to-point protocol.

Figure 3.19 PPP frame format



Access the text alternative for slide images.

Figure 3.20 Transition phases



Access the text alternative for slide images.

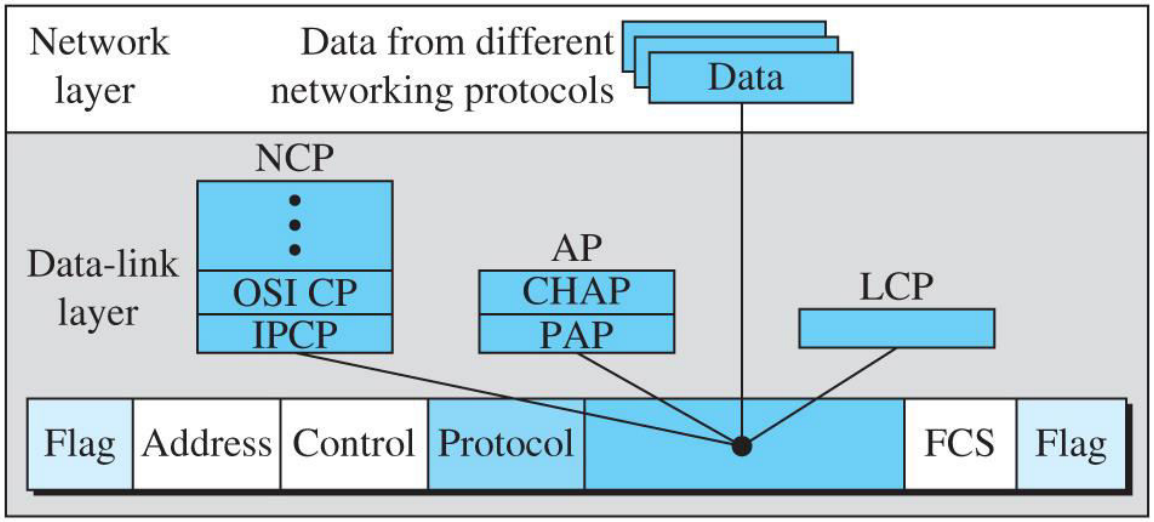
Figure 3.21 Multiplexing in PPP

Legend

LCP : Link control protocol
AP : Authentication protocol
NCP: Network control protocol

Protocol values:

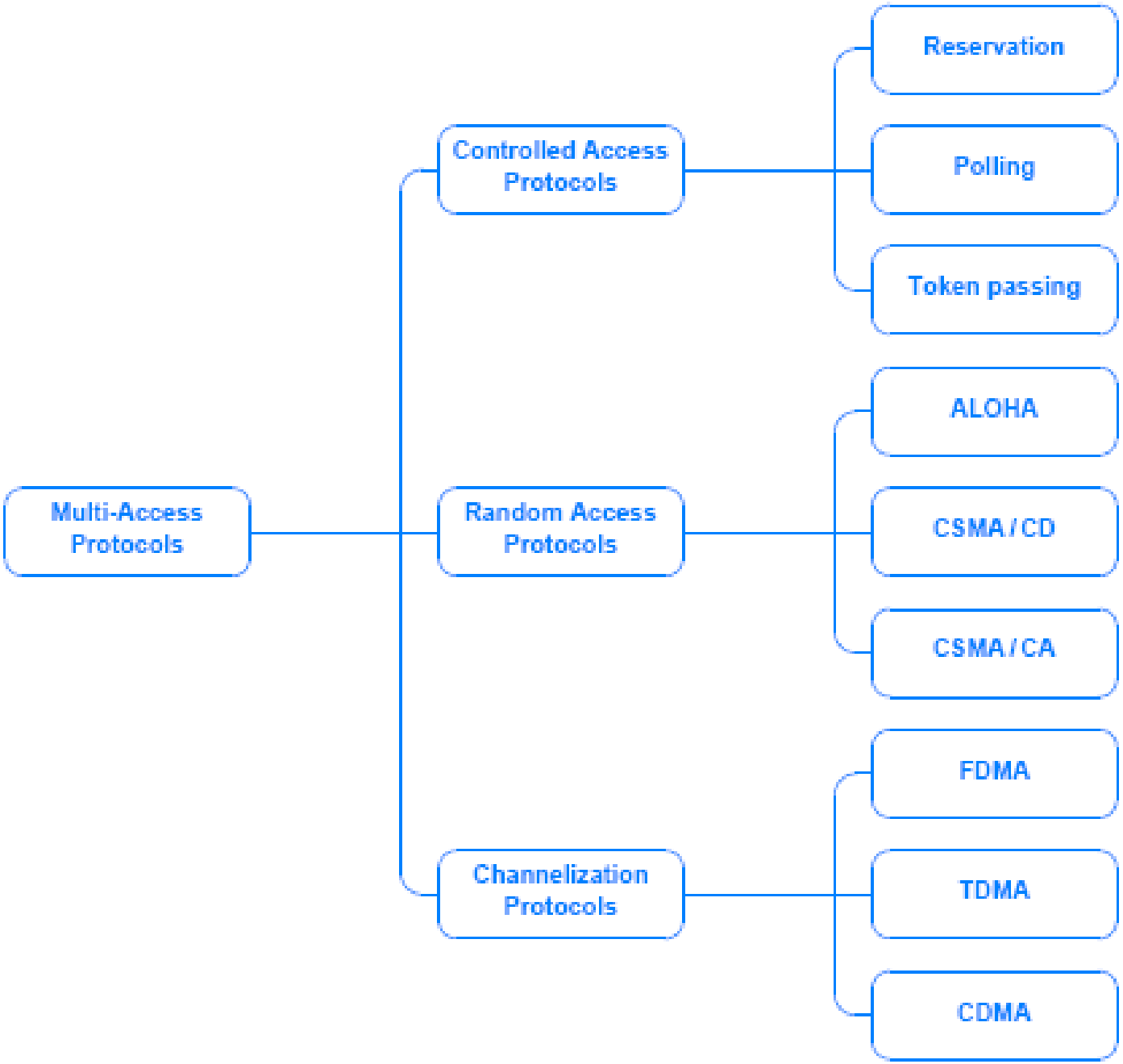
LCP : 0xC021
AP : 0xC023 and 0xC223
NCP: 0x8021 and ....
Data: 0x0021 and ....



Access the text alternative for slide images.

3-3 Media Access Protocols

We said that data link control is divided into two groups: data link control and media access control.


Multi-Access Protocols
Controlled Access Protocols
Random Access Protocols
Channelization Protocols
Reservation
Polling
Token passing
ALOHA
CSMA/CD
CSMA/CA
FDMA
TDMA
CDMA

Static and Dynamic Channel Allocation
Static is discussed below:

Channelization to refer to a mapping (between communication and a channel in the underlying transmission system).

Traditional way to allow more than one person to use the medium is to use FDM

In Frequency division multiplexing, the total bandwidth is divided among the total number of users, each pair is assigned to a unique frequency. This is known as 1-to-1 static.

FDM works well when there is a small number of users

When users grow a fast busy signal is issued

Channelization Protocols

FDMA

TDMA

Code Division Multi-Access

Already covered these

Controlled Access Protocols – Collision free

Polling: A centralized controller cycles through all stations on the network and gives each an opportunity to transmit a packet, either uses round robin order or priority order

.

Reservation – Collision free

Often used with satellite transmission, employs a two-step process. Each transmission is planned in advanced. In the first step, each potential sender specifies whether they have a packet to send during the next round and the controller transmits a list of stations that will be transmitting. In the second step, stations transmit upon their turn.

Bit-map protocol

- *A bit map with enough slots for all stations is passed around*
- *Each station wanting to send a frame and if the frame is ready in the queue, inserts a 1 bit into its reserved slot in the bit map.*
- *Once station numbers of all who want to send is known they take turns in order.*

Reservation – collision free. Binary count down

Each station is given a binary address

If a station wants to transmit a frame it broadcasts its address one bit at a time starting with the high order bit.

Bits from each station are Ored together the station address starting with the resulting 0 or 1 bit as agreed upon is allowed to go on. If two or more has the same bit then go to the next bit and so on.

Token Passing – collision free

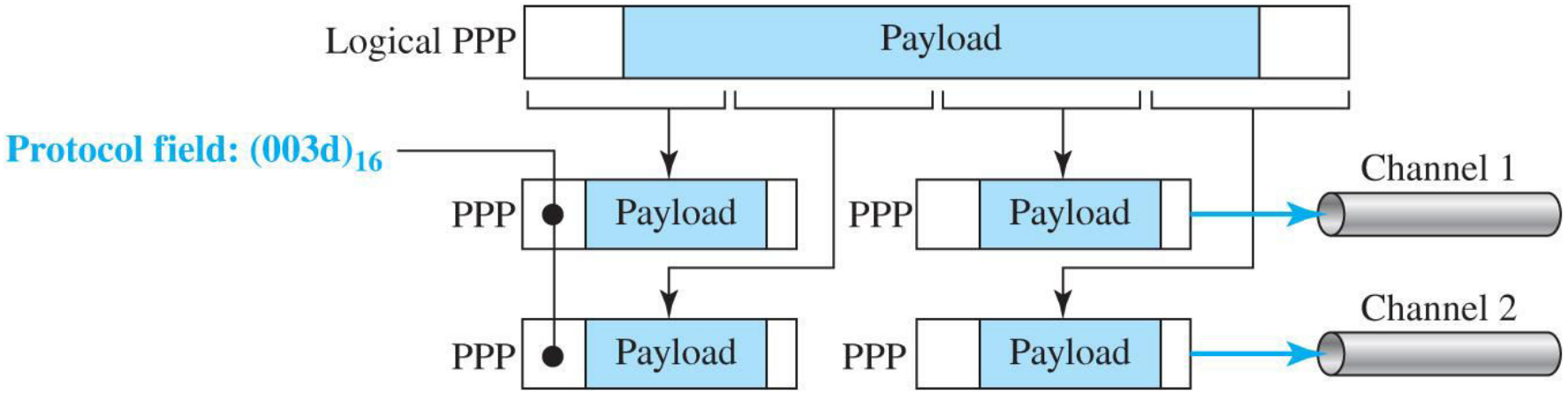
Token bus

- *Each station knows the address of the station to its left and right*
- *The highest numbered station may send the first frame*
- *Then it passes permission to its immediate neighbor by send a special frame called a token.*
- *The first station passes the token to the highest numbered one.*

Token Ring

- *Physical Ring*
- *Token circulates*

Figure 3.22 Multilink PPP



Access the text alternative for slide images.

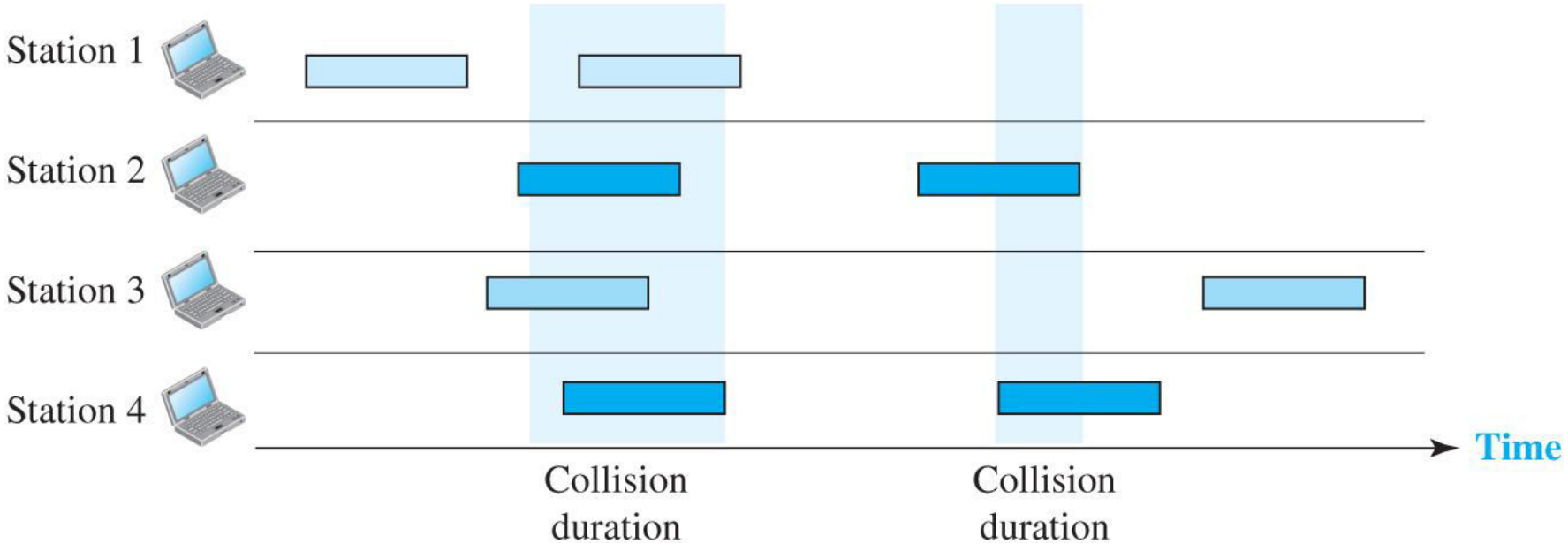
3.3.1 Random Access

In random access no station is superior to another station and none is assigned the control over another.

ALOHA

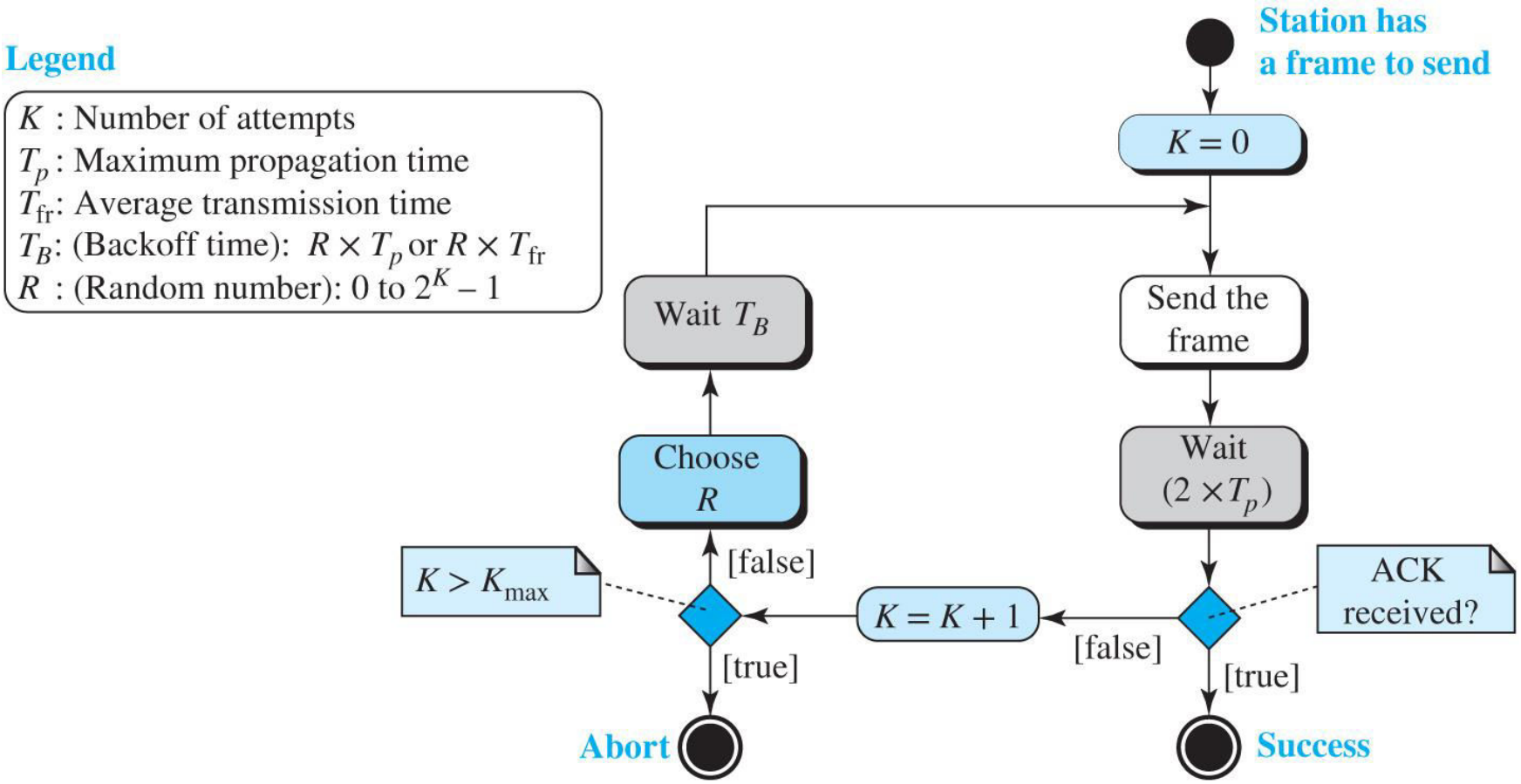
ALOHA, the earliest random access method, was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium. It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When 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.

Figure 3.24 Frames in a pure ALOHA network



Access the text alternative for slide images.

Figure 3.25 Procedure for pure ALOHA protocol

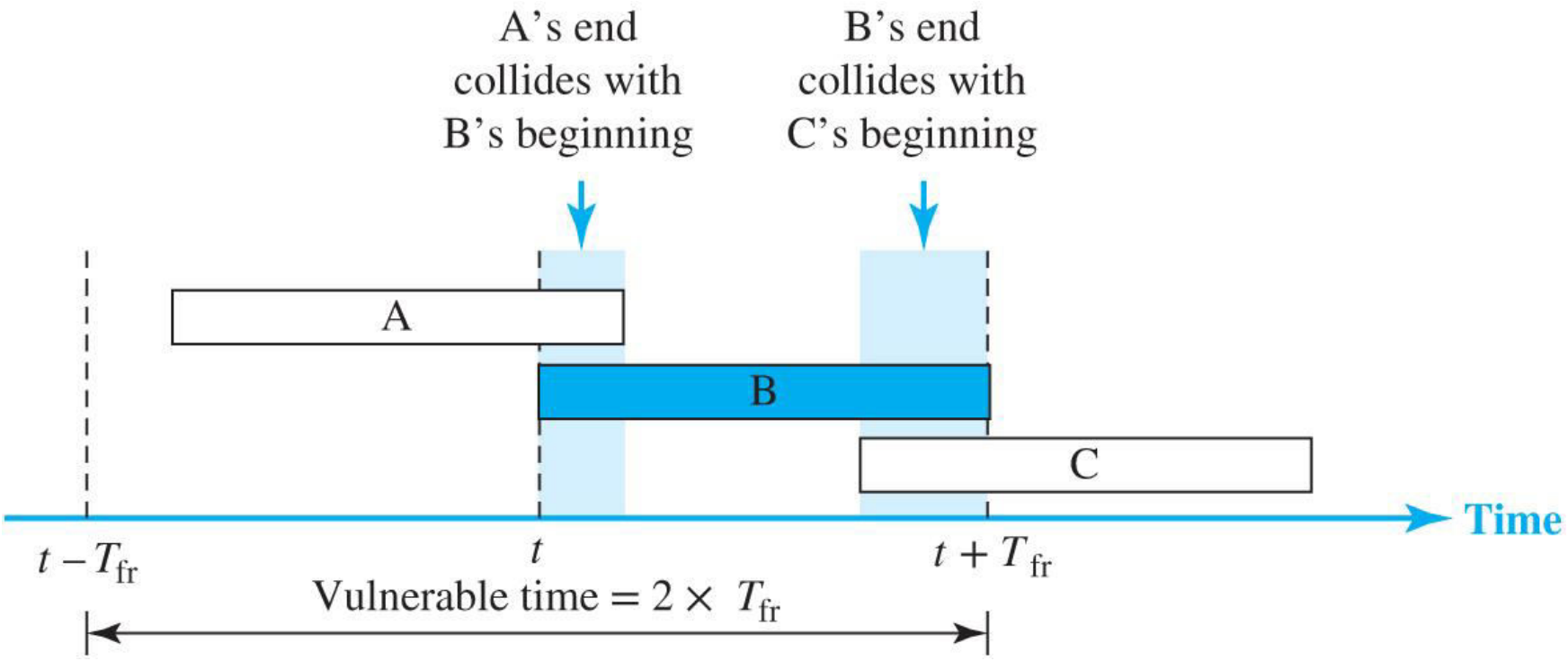


Access the text alternative for slide images.

Example 3.8

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 $T_p = (600 \times 10^3)/(3 \times 10^8) = 2$ ms. For K = 2, the range of R 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 R.

Figure 3.26 Vulnerable time for pure ALOHA protocol



Access the text alternative for slide images.

Example 3.9

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 period (1 ms) that this station is sending.

Example 3.10 (1)

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second?

b. 500 frames per second?

c. 250 frames per second?

Solution

The frame transmission time is 200/200 kbps or 1 ms.

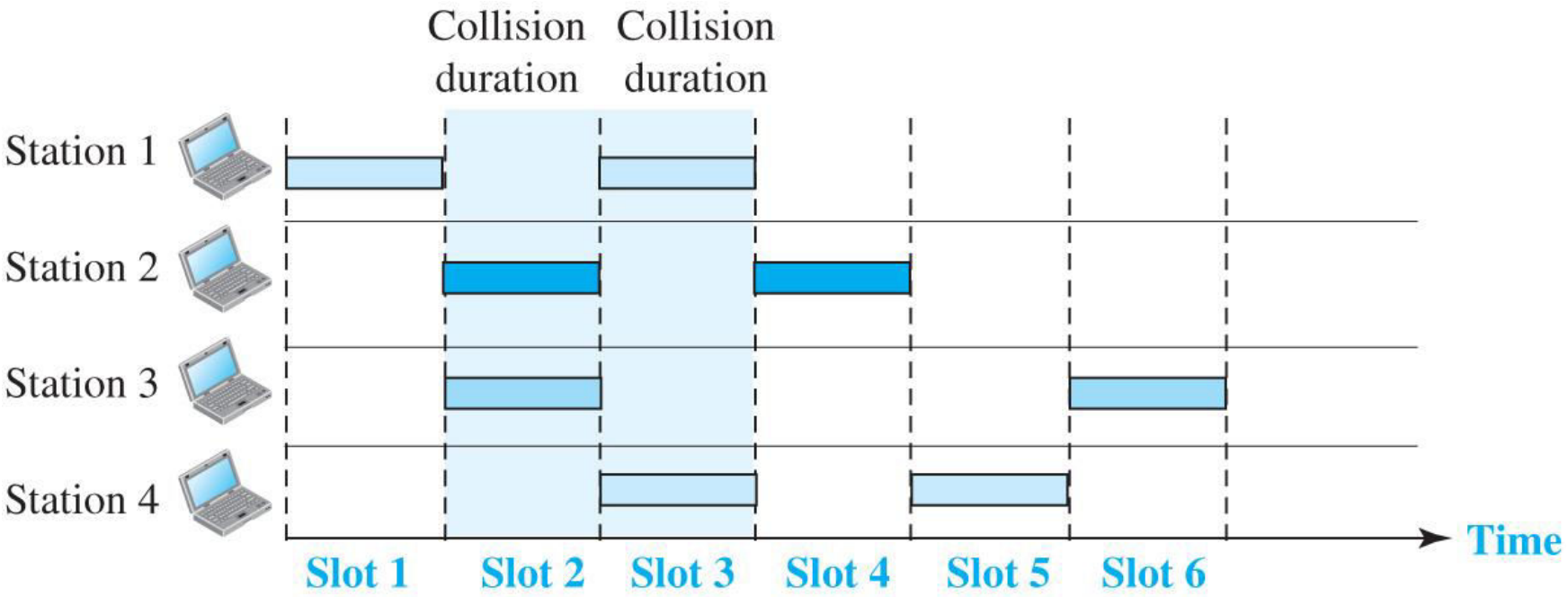
a. If the system creates 1000 frames per second, or 1 frame per millisecond, then G = 1. In this case $S = G \times e^{-2G} = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

Example 3.10 (2)

b. If the system creates 500 frames per second, or 1/2 frames per millisecond, then G = 1/2. In this case $S = G \times e^{-2G} = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the maximum throughput case, percentage-wise.

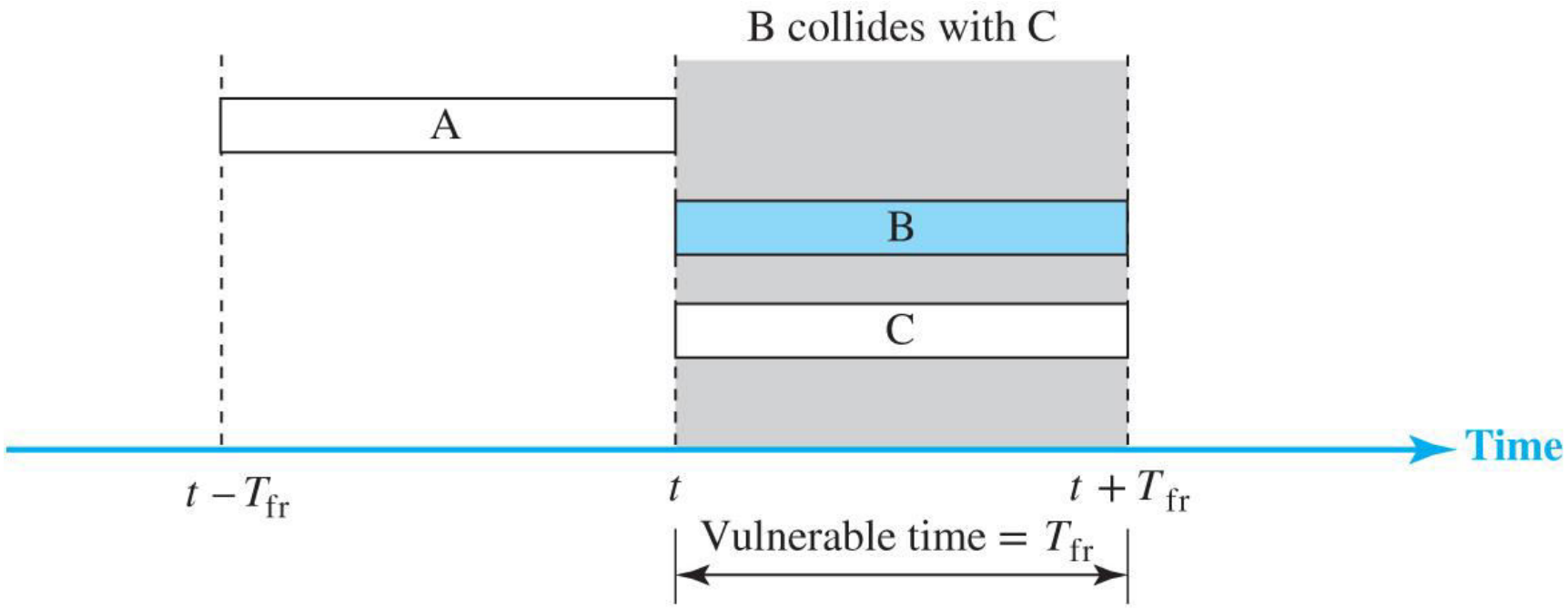
c. If the system creates 250 frames per second, or 1/4 frames per millisecond, then G = 1/4. In this case $S = G \times e^{-2G} = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive

Figure 3.27 Frames in a slotted ALOHA network



Access the text alternative for slide images.

Figure 3.28 Vulnerable time for slotted ALOHA protocol



Access the text alternative for slide images.

Example 3.11 (1)

A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second.

b. 500 frames per second.

c. 250 frames per second.

Solution

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms.

Example 3.11 *(2)*

a) In this case G is 1. So $S = G \times e^{-G} = 0.368$ (36.8 percent). This means that the throughput is $1000 \times 0.0368 =$ 368 frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentage-wise.

b) Here G is 1/2. In this case $S = G \times e^{-G} = 0.303$ (30.3 percent). This means that the throughput is $500 \times 0.0303 = 151$. Only 151 frames out of 500 will probably survive.

c) Now G is 1/4. In this case $S = G \times e^{-G} = 0.195$ (19.5 percent). This means that the throughput is $250 \times 0.195 = 49$. Only 49 frames out of 250 will probably survive.

Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, 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 (or check the state of the medium) before sending. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

Carrier Sense Multiple Access Protocols (CSMA)

Listen for a transmission

If the line is clear then transmit

Implementations:

- *Persistent, Non Persistent and p-persistent*
- *CSMA with collision detection*

Persistent

Listen, if busy wait until line is free

Transmit a frame

If collision occurred, wait for a random amount of time

Transmission time delay between two sending computers will cause the second computer not to hear the transmission.

Non-Persistent

Listen, if busy wait random amount of time and listen again until the line is free

This approach is less greedy than the Persistent one

This prevents two or more wanting to get on the line from doing so at the same time when the channel becomes free.

P-persistent CSMA

Slotted channels.

Listen, if free send at the beginning of the next slot

CSMA with Collision Detection (CSMA-CD)

Abort transmission as soon as collision is detected

Collision is detected by comparing received signal power to sent signal

If collision is detected, stop transmission and wait for random amount of time

CSMA/CD is used widely in LAN IEEE 802.3 is an example.

Binary Exponential Backoff

After a collision occurs, a computer must wait, but how long? In Aloha randomization was used.

In exponential backoff, the computer must wait twice the amount of time than the previous time. This is repeated if collision occur again.

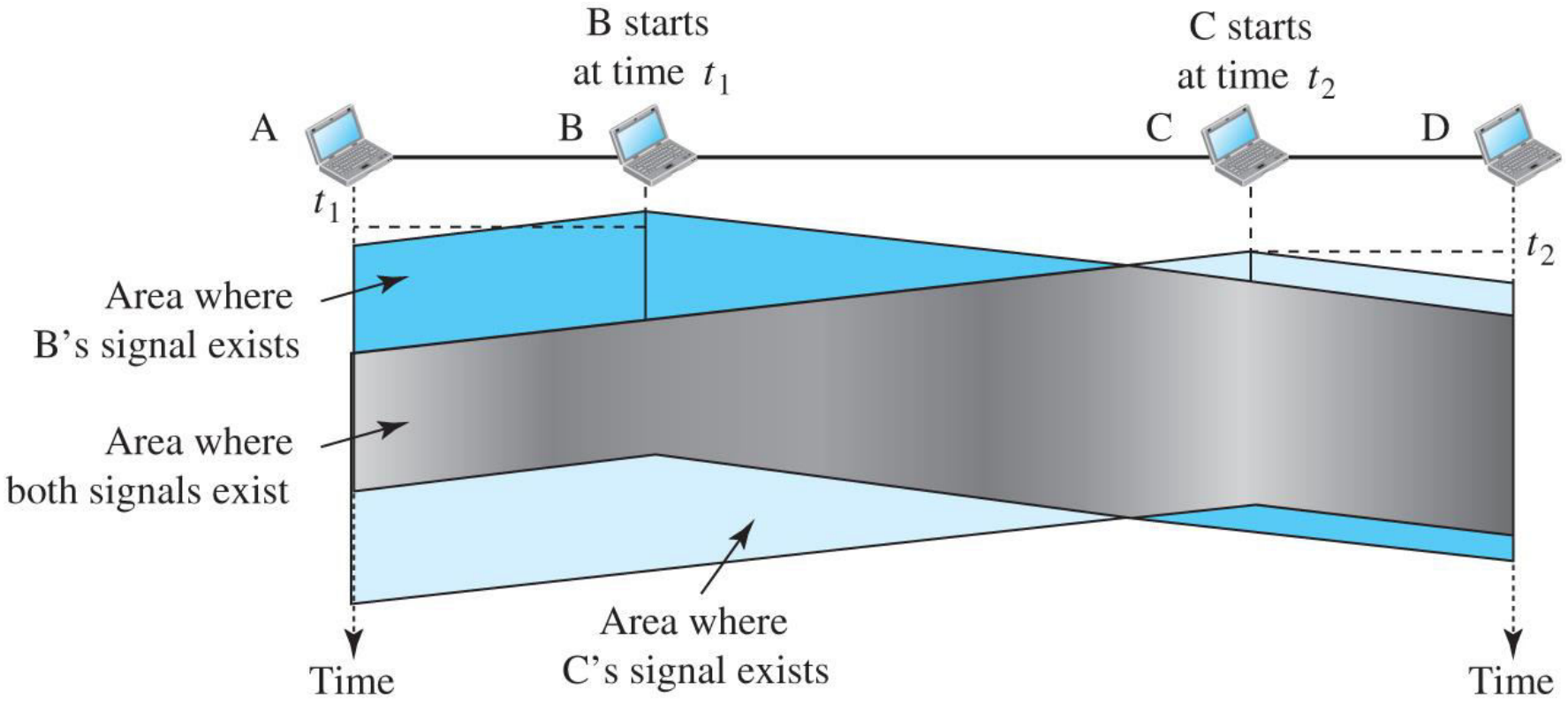
CSMA-CA

For wireless.

May not be able to hear computers outside the range, while the other party can hear. This is known as the hidden station problem.

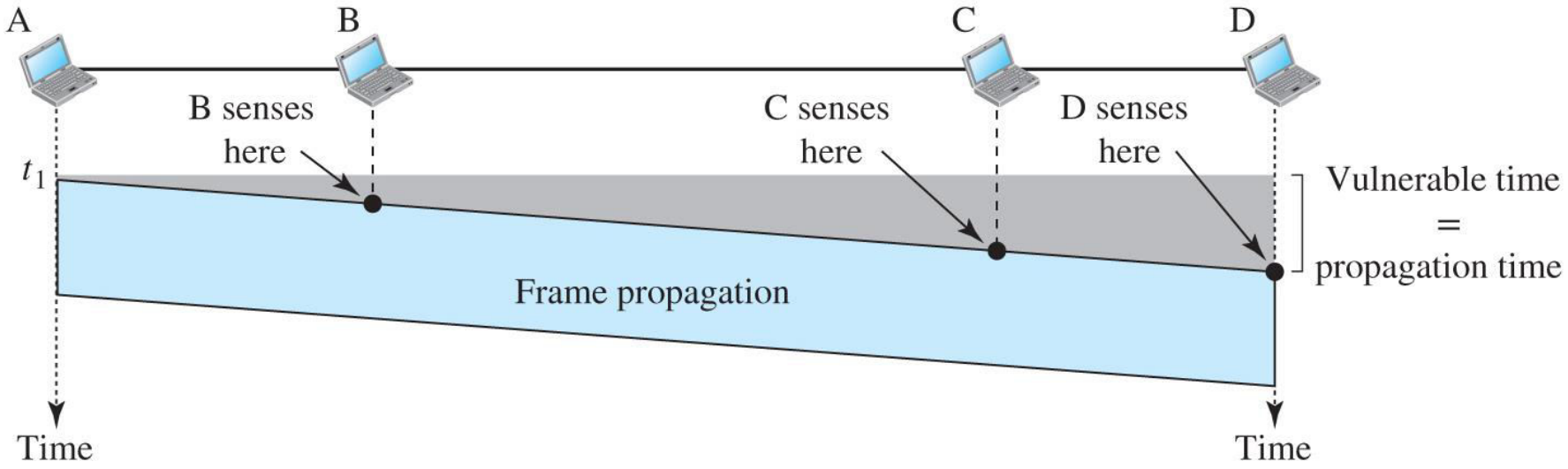
Ready to send and clear to send are transmitted first before transmitting packet. The clear to send or the ready to send will be heard by all within range.

Figure 3.29 Space and time model of a collision in CSMA



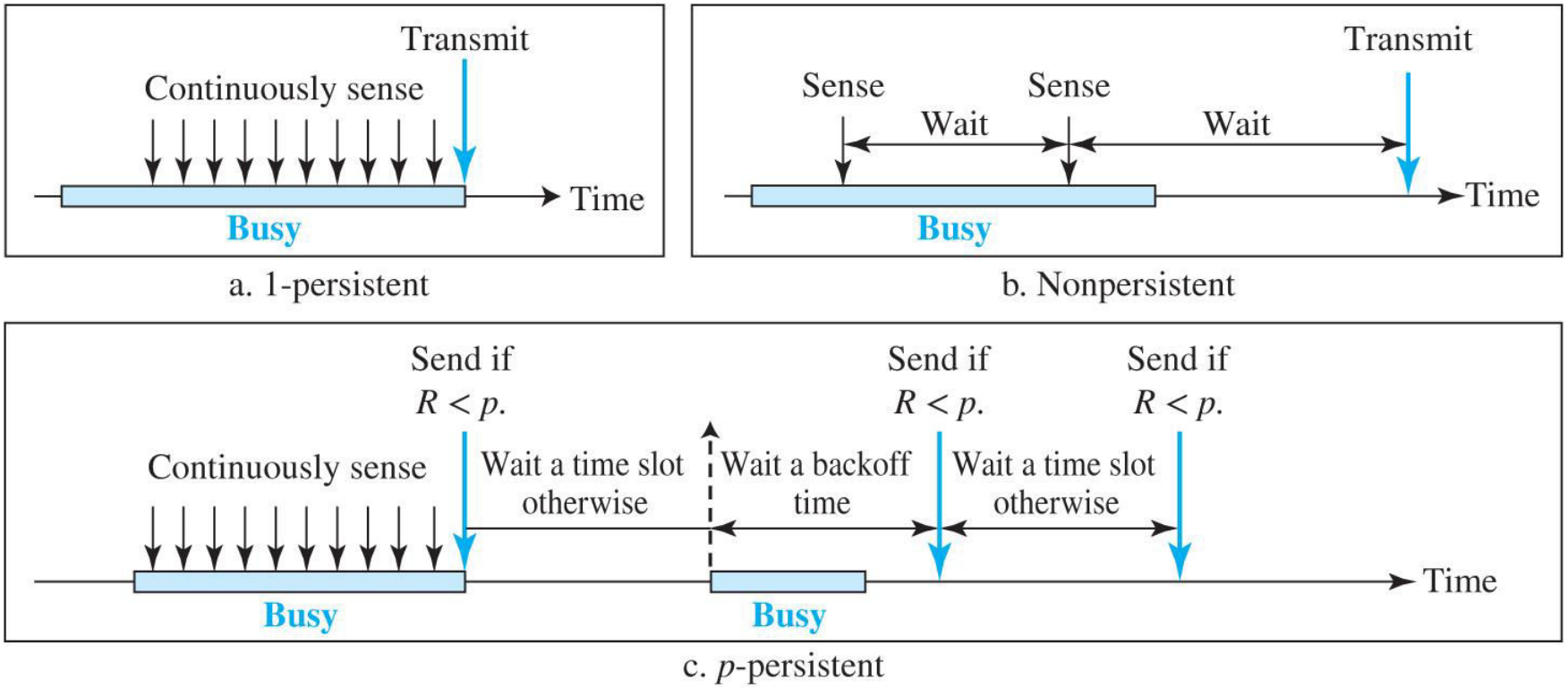
Access the text alternative for slide images.

Figure 3.30 Vulnerable time in CSMA



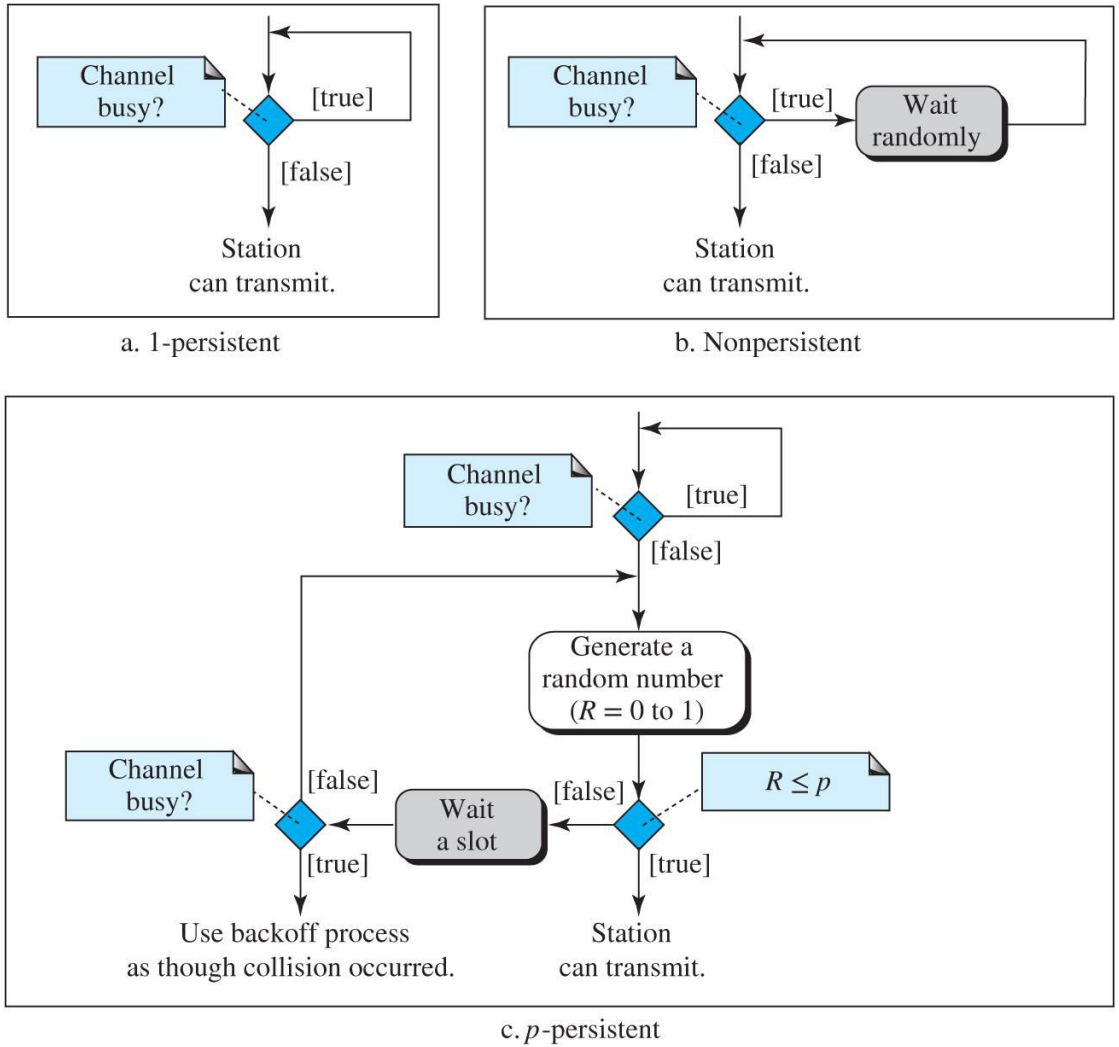
Access the text alternative for slide images.

Figure 3.31 Behavior of three persistence methods



Access the text alternative for slide images.

Figure 3.32 Flow diagram for three persistence methods



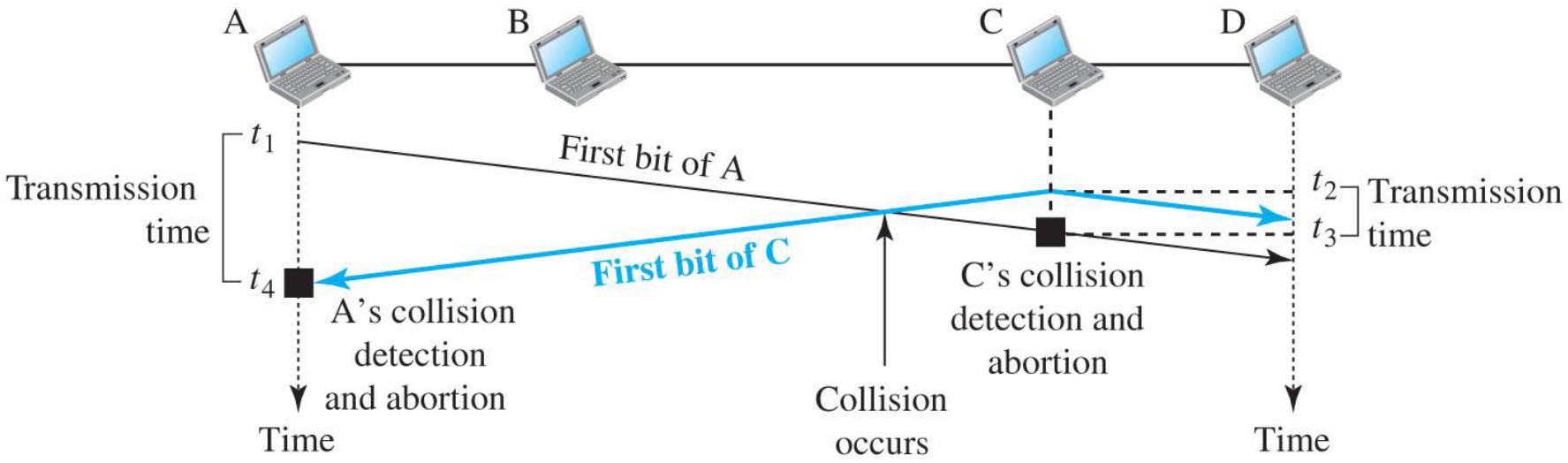
Access the text alternative for slide images.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

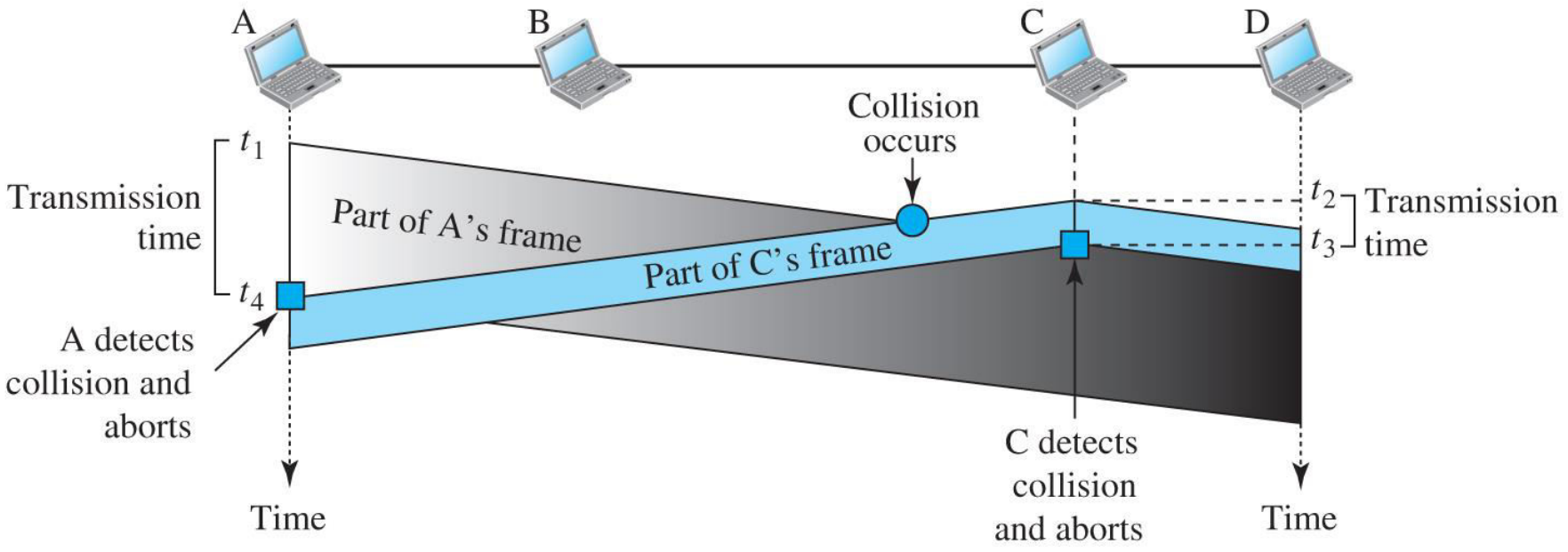
In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

Figure 3.33 Collision of the first bits in CSMA/CD



Access the text alternative for slide images.

Figure 3.34 Collision and abortion in CSMA/CD



Access the text alternative for slide images.

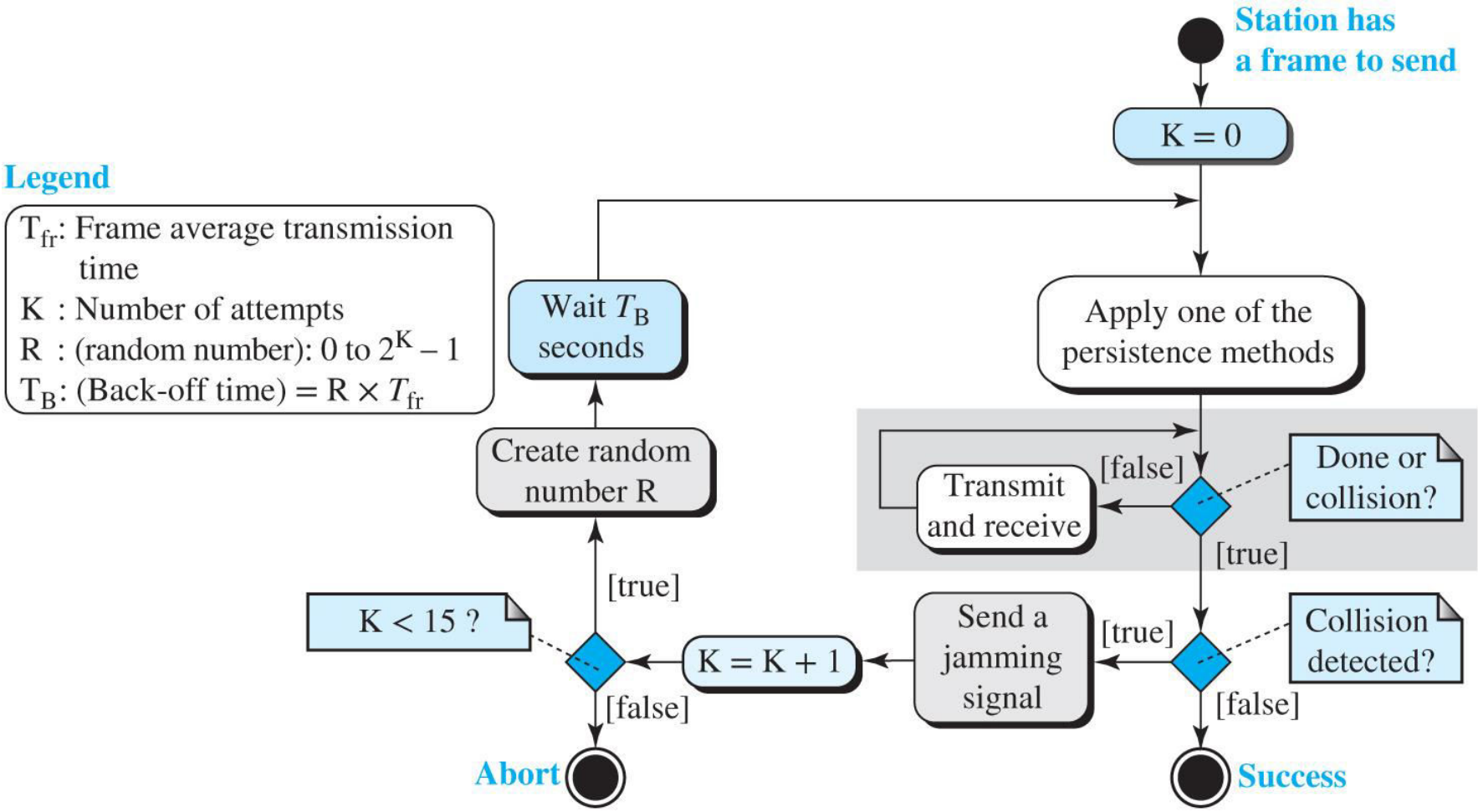
Example 3.12

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

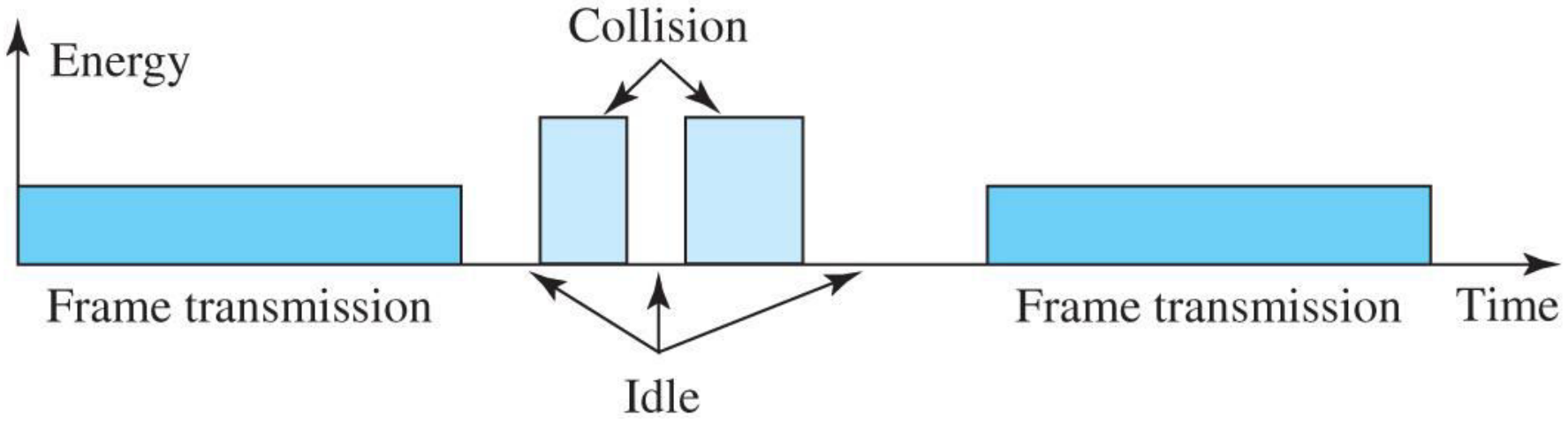
The minimum frame transmission time is $T_{fr} = 2 \times T_p = 51.2$ μs. This means, in the worst case, a station needs to transmit for a period of 51.2 μs to detect the collision. The minimum size of the frame is 10 Mbps × 51.2 μs = 512 bits or 64 bytes. This is actually the minimum size of the frame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

Figure 3.35 Flow diagram for the CSMA/CD



Access the text alternative for slide images.

Figure 3.36 Energy level during transmission, idleness, or collision



Access the text alternative for slide images.

CSMA/CA

Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for wireless networks.

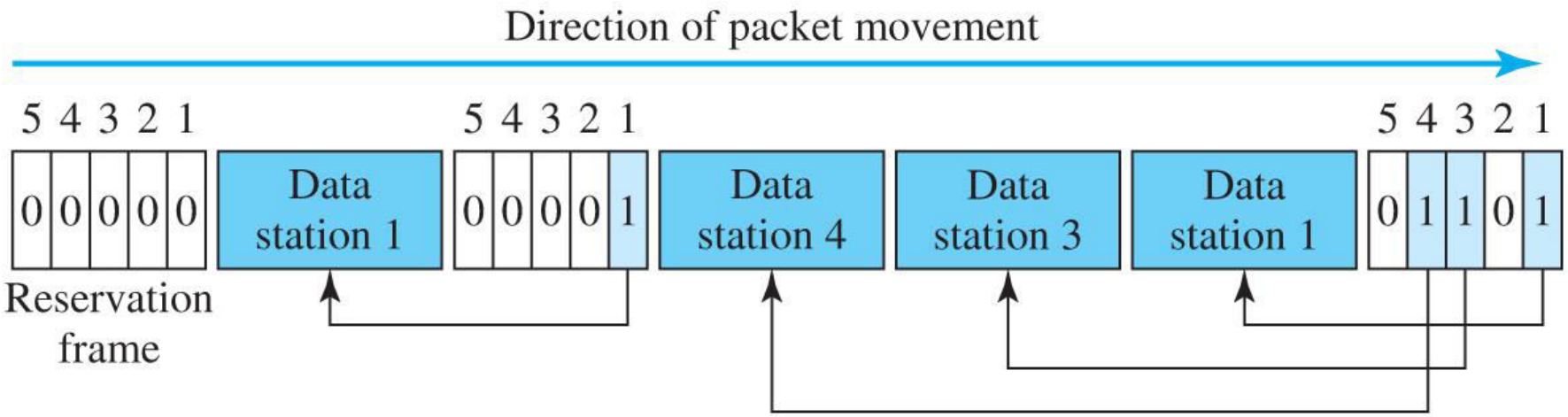
3.3.2 Controlled Access

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 controlled-access methods.

Reservation

In the reservation method, a station needs to make a reservation before sending data. Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

Figure 3.37 Reservation access method

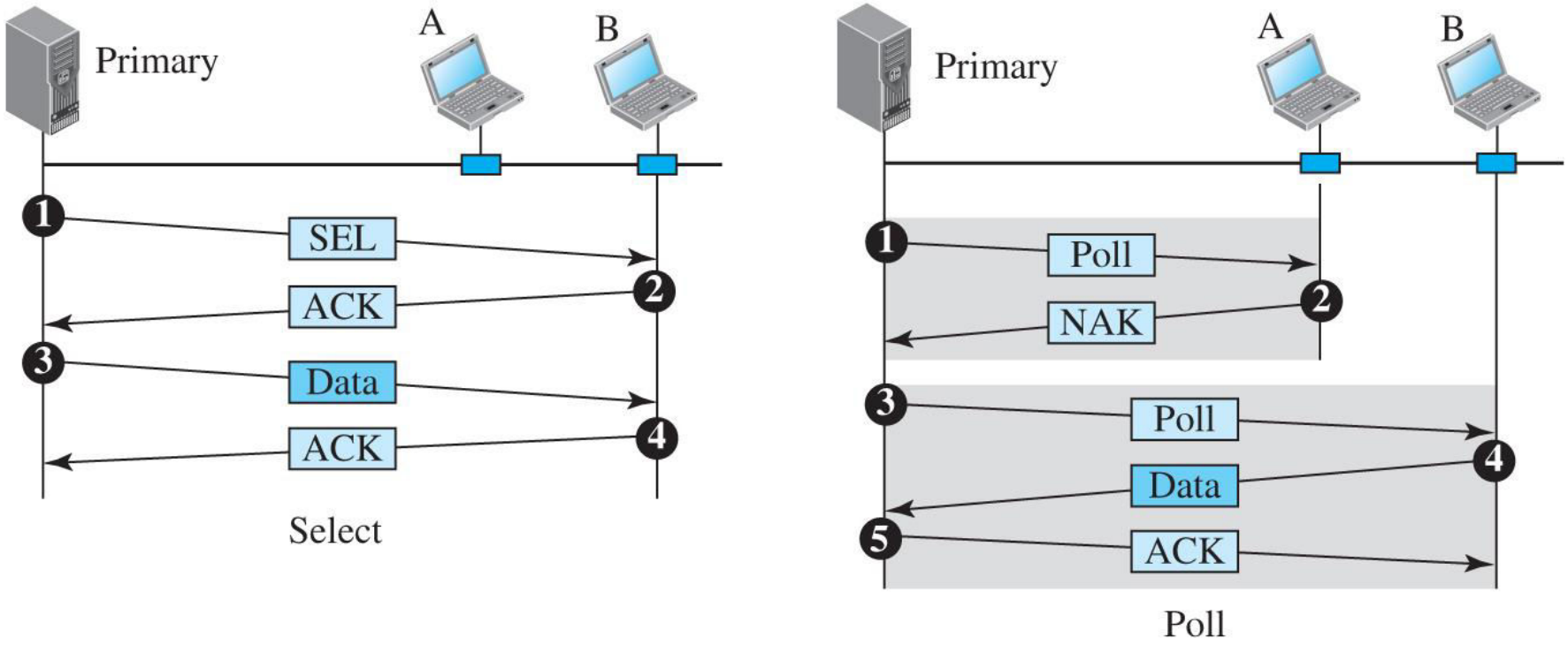


Access the text alternative for slide images.

Polling

Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations. All data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the link; the secondary devices follow its instructions. It is up to the primary device to determine which device is allowed to use the channel at a given time.

Figure 3.38 Select and poll functions in polling-access method

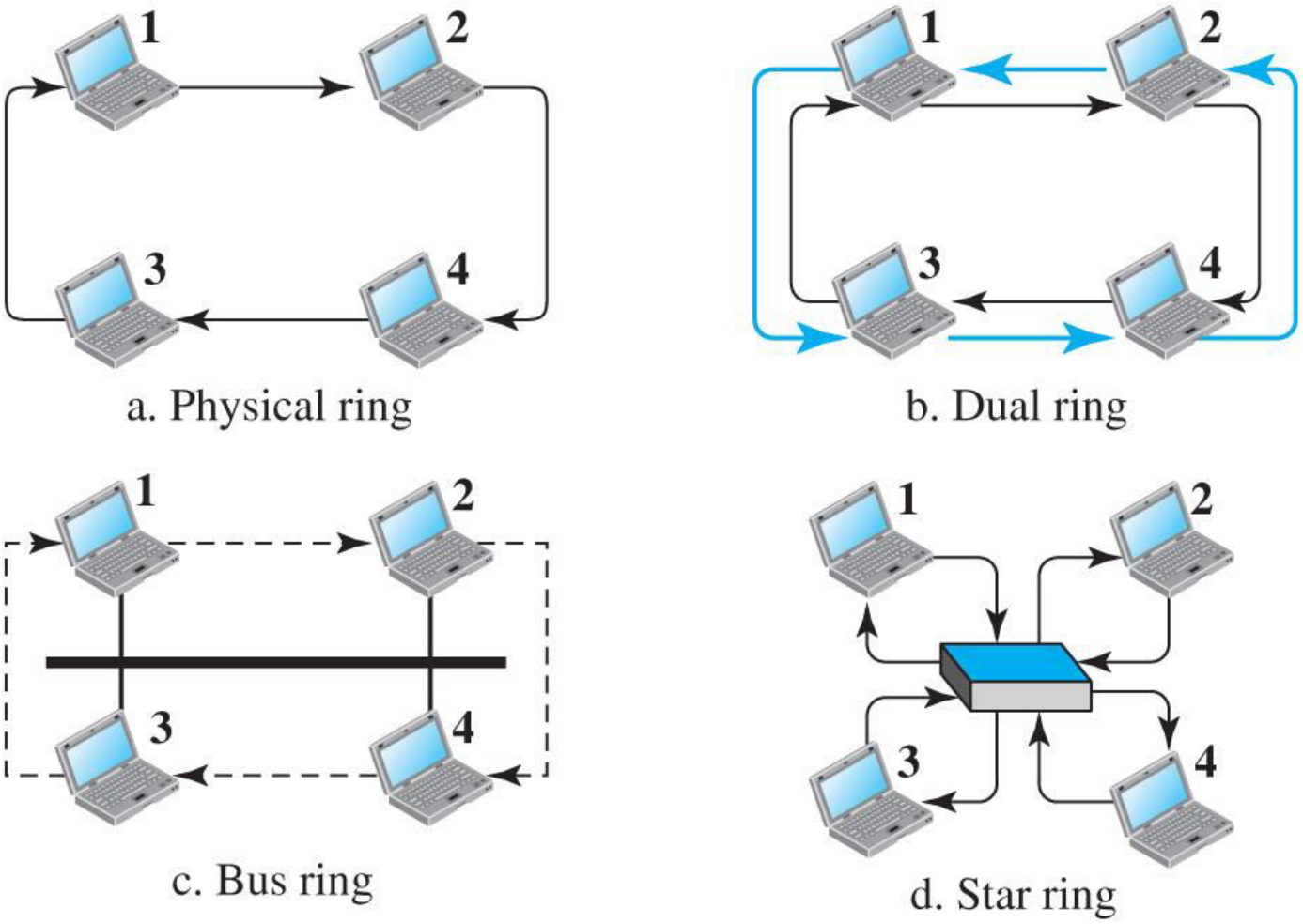


Access the text alternative for slide images.

Token Passing

In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a predecessor and a successor. The predecessor is the station that is logically before the station in the ring; the successor is the station that is after the station in the ring.

Figure 3.39 Logical ring and physical topology in token-passing access method



Access the text alternative for slide images.

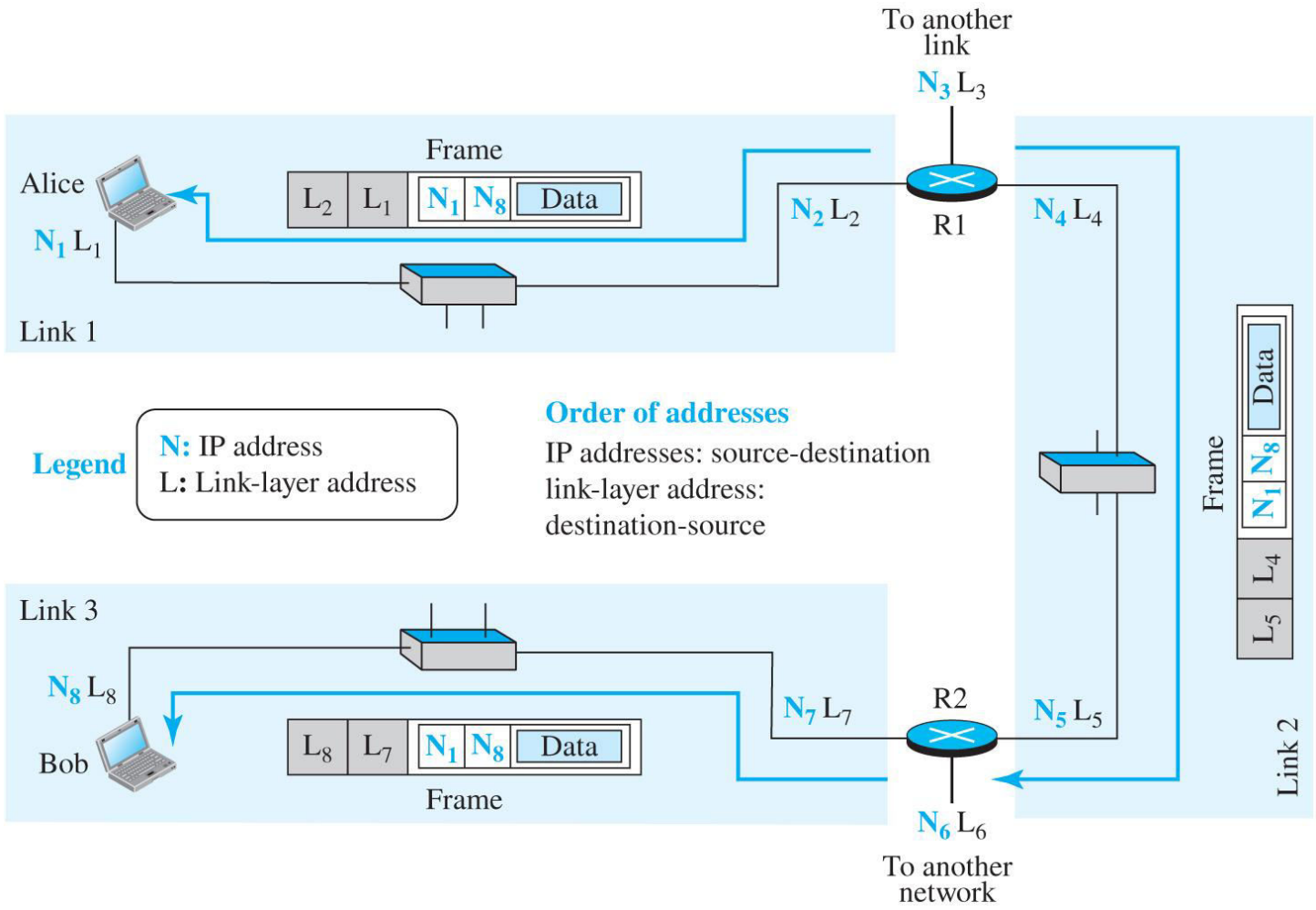
3.3.3 Channelization

Channelization (or channel partition, as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations. Since this method is normally used in wireless LAN, we postpone this discussion until Chapter 4.

3-4 LINK-LAYER ADDRESSING

In Chapter 7, we will discuss IP addresses as the identifiers at the network layer. However, in an internetwork such as the Internet we cannot make a datagram reach its destination using only IP addresses. The source and destination IP addresses define the two ends but cannot define which links the packet should pass through.

Figure 3.40 IP addresses and link-layer addresses in a small internet



Access the text alternative for slide images.

3.4.1 Three Types of Addresses

Some link-layer protocols define three types of addresses: unicast, multicast, and broadcast.

Unicast Address

Each host or interface is assigned a unicast address.

Example 3.13

As we discuss later in the chapter, the link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A2:34:45:11:92:F1

Multicast Address

Some link-layer protocols define multicast addresses. A multicast address means one-to-many communication.

Example 3.14

As we discuss later in the chapter, the link-layer addresses in the most common LAN, Ethernet, are 48 bits (six bytes) that are presented as 12 hexadecimal digits separated by colons; for example, the following is a link-layer address of a computer.

A2:34:45:11:92:F1

Broadcast Address

A broadcast address means one-to-all address.

Example 3.15

A broadcast address is made of 48 bits of 1's.

FF:FF:FF:FF:FF:FF

3.4.2 Address Resolution Protocol (ARP)

Any time a node has a packet to send to another node, it has the IP address (network-layer address of the next node); it needs the link-layer address of the next node. This is done by a protocol called ARP located in the network layer. We discuss it when we discuss the network layer.

Because learning changes everything.®

www.mheducation.com