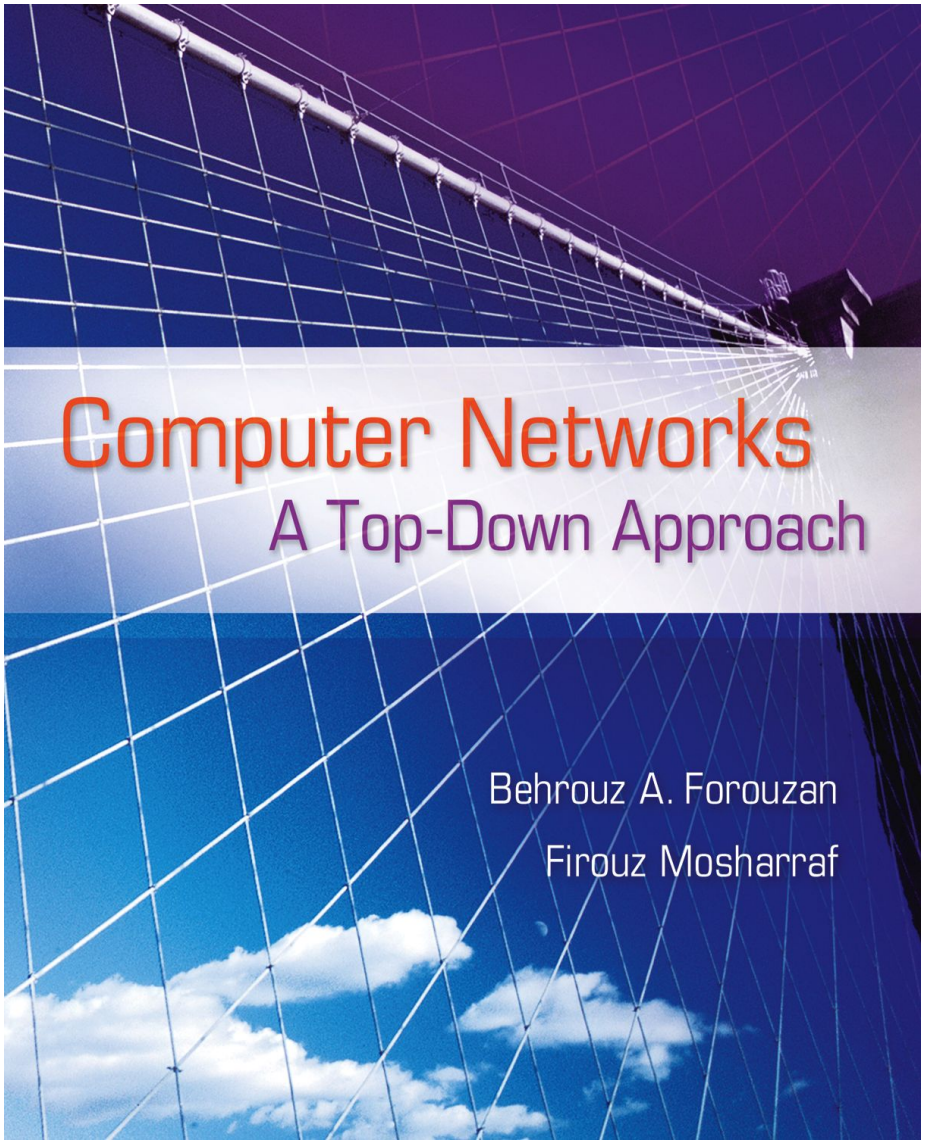
Chapter 5

Data-Link Layer: Wired Networks



Chapter 5: Outline

5.1 INTRODUCTION

5.2 DATA LINK CONTROL (DLC)

5.3 MULTIPLE ACCESS PROTOCOLS

5.4 LINK-LAYER ADDRESSING

5.5 WIRED LANS: ETHERNET PROTOCOL

5.6 OTHER WIRED NETWORKS

5.7 CONNECTING DEVICES

Chapter 5: Objective

- *We introduce the concept of nodes and links and the types of links, and show how the data-link layer is actually divided into two sublayers: data link control and media access control.*

- *We discuss data link control (DLC) of the data-link layer and explain services provided by this layer, such as framing, flow and error control, and error detection.*

- *We discuss the media access control (MAC) sublayer of the data-link layer. We explain different approaches such as random access, controlled access, and channelization.*

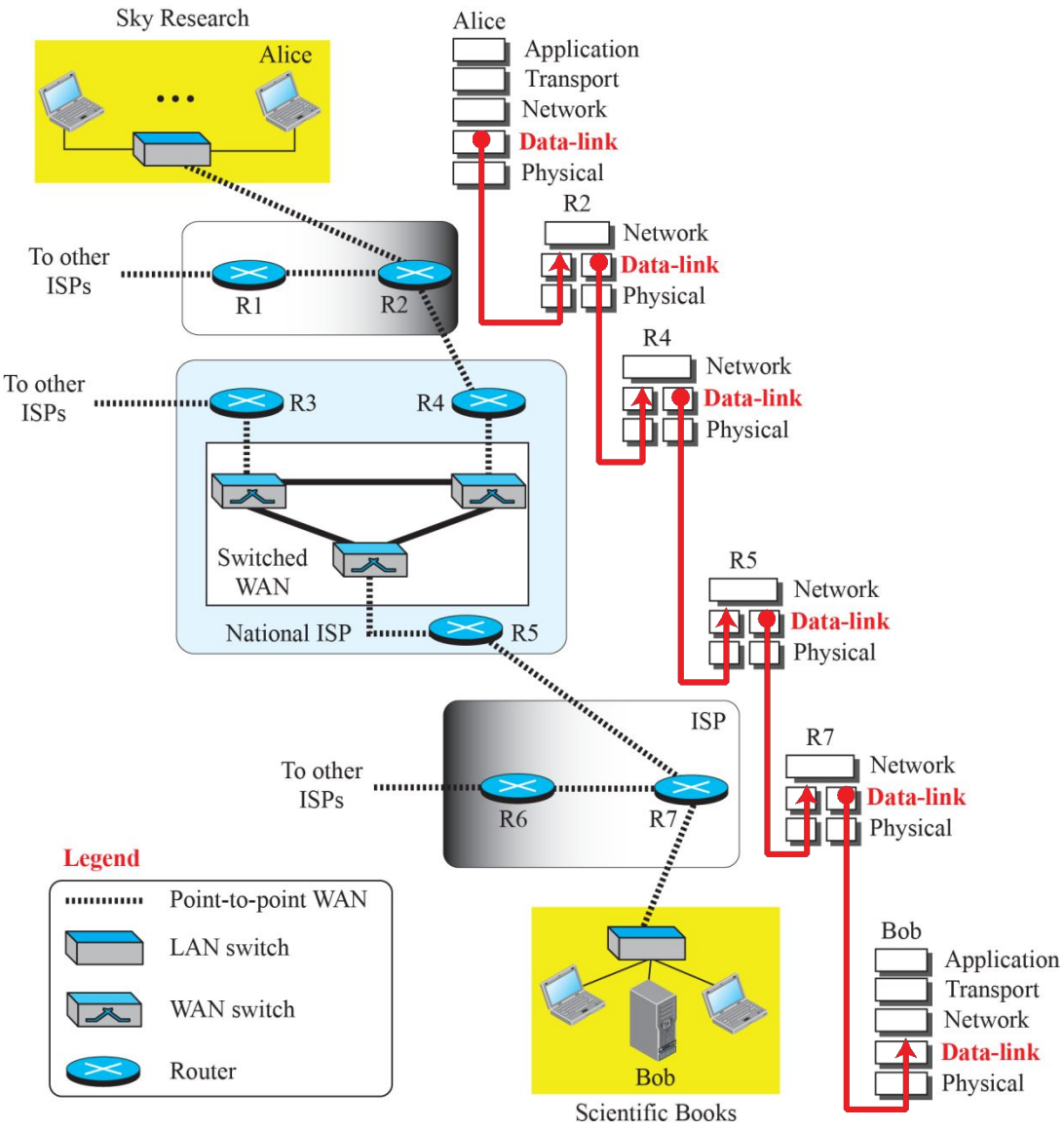
Chapter 5: Objective (continued)

- *We discuss link-layer addressing and how the link-layer address of a node can be found using the Address Resolution Protocol (ARP).*
- *We introduce the wired LANs and in particular Ethernet, the dominant LAN protocol today. We move through different generations of Ethernet and show how it has evolved.*
- *We discuss other wired networks that we encounter in the Internet today, such as point-to-point networks and switched networks.*
- *We discuss connecting devices used in the lower three layers of the TCP/IP protocol such as hubs, link-layer switches, and routers.*

5-1 INTRODUCTION

The Internet is a combination of networks glued together by connecting devices (routers or switches). If a datagram is to travel from a host to another host, it needs to pass through these networks. Figure 5.1 shows communication between Alice and Bob, using the same scenario we followed in the last three chapters.

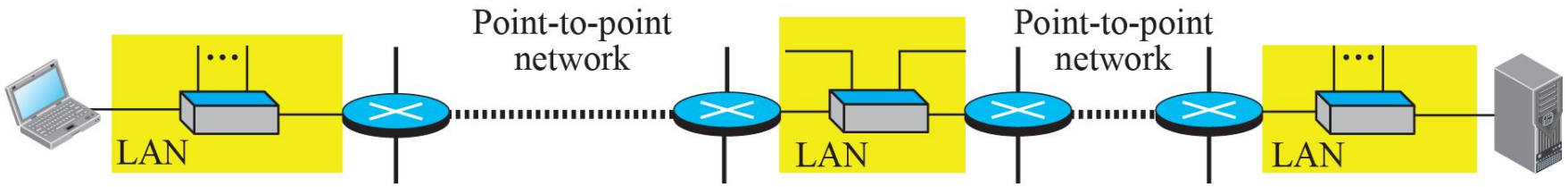
Figure 5.1: Communication at the data-link layer



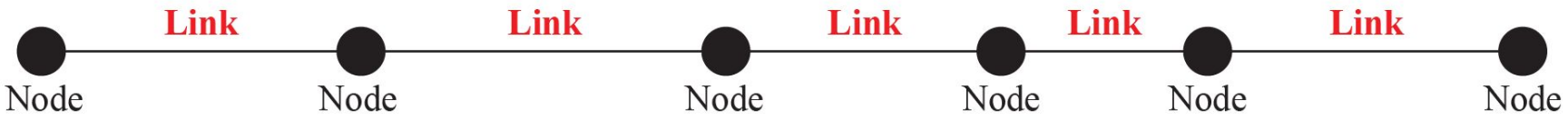
5.1.1 Nodes and Links

Although communication at the application, transport, and network layers is end-to-end, communication at the data-link layer is node-to node. As we have learned in the previous chapters, 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 5.2: Nodes and Links



a. A small part of the Internet



b. Nodes and links

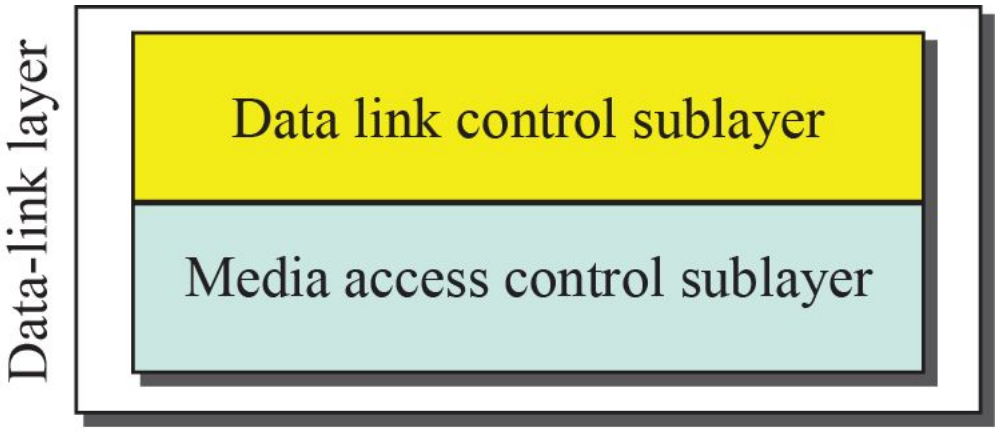
5.1.2 Two Types of Links

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.

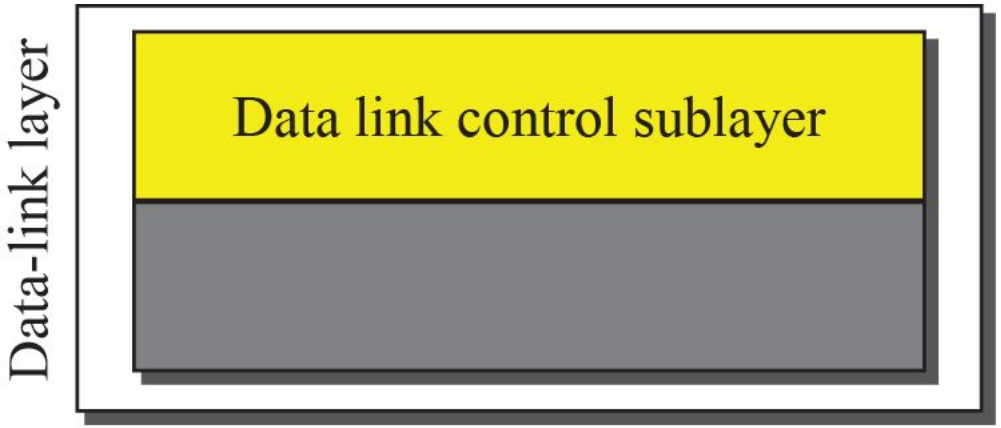
5.1.3 Two Sublayers

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 later in this chapter and in the next chapter, LAN protocols actually use the same strategy. The data link control sublayer deals with all issues common to both point-to-point and broadcast links; the media access control sublayer deals only with issues specific to broadcast links.

Figure 5.3: ***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

5-2 DATA LINK CONTROL (DLC)

The data link control deals with procedures for communication between two adjacent nodes. Data link control (DLC) functions include framing, flow and error control, and error detection and correction. In this section, we first discuss framing, or how to organize the bits that are carried by the physical layer. We then discuss flow and error control. Techniques for error detection are discussed at the end of this section.

5.2.1 Framing

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The data-link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.

- **Frame Size**
  - Character-Oriented Framing
  - Bit-Oriented Framing

Figure 5.4: A frame in a character-oriented protocol

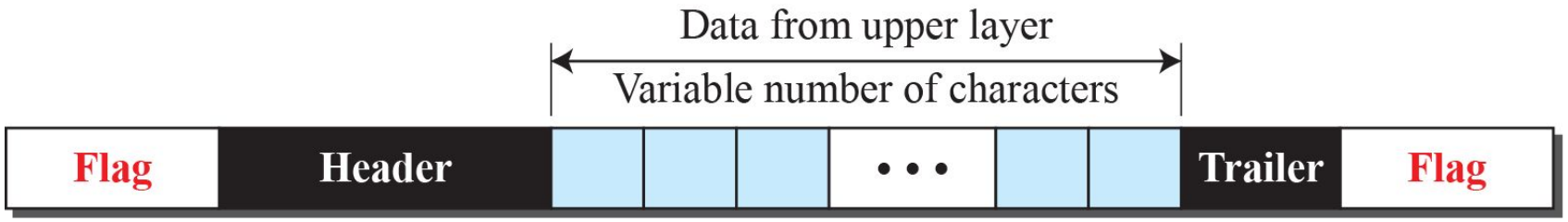


Figure 5.5: Byte stuffing and unstuffing

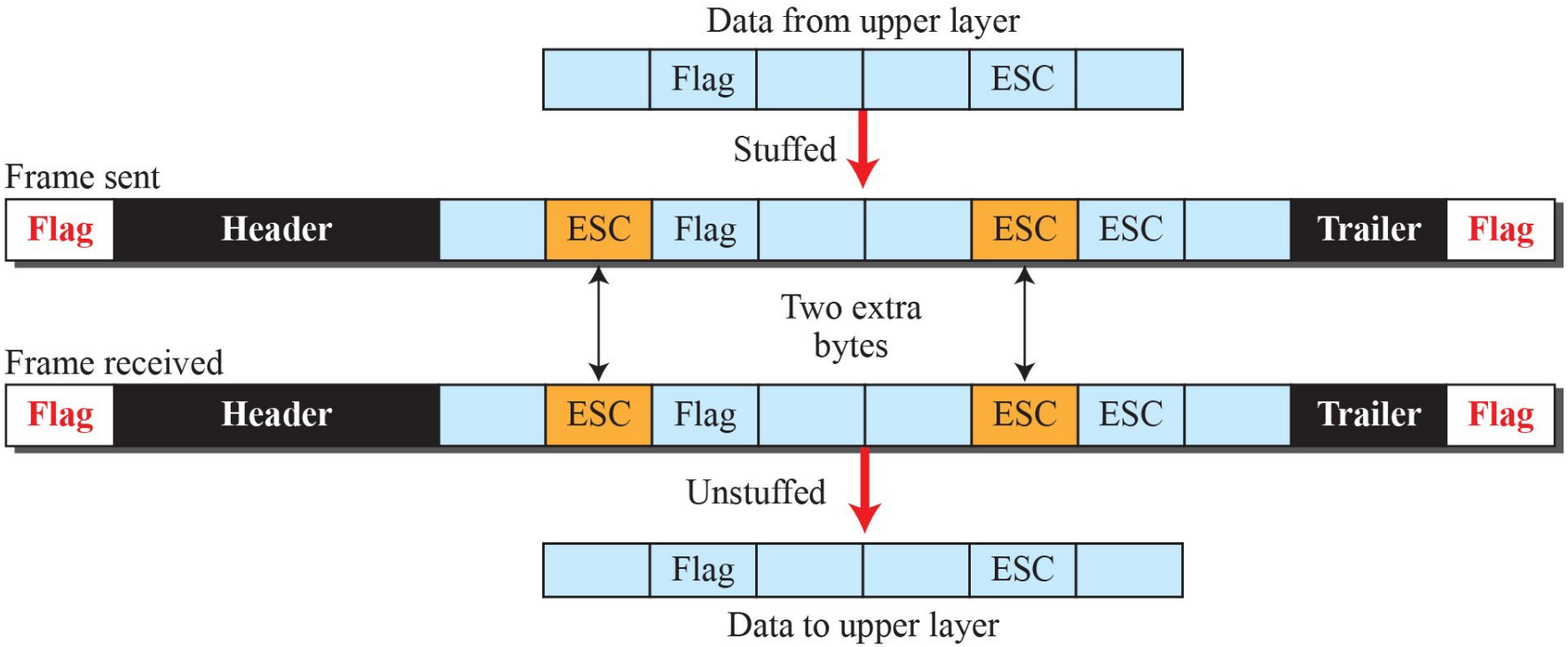


Figure 5.6: A frame in a bit-oriented protocol

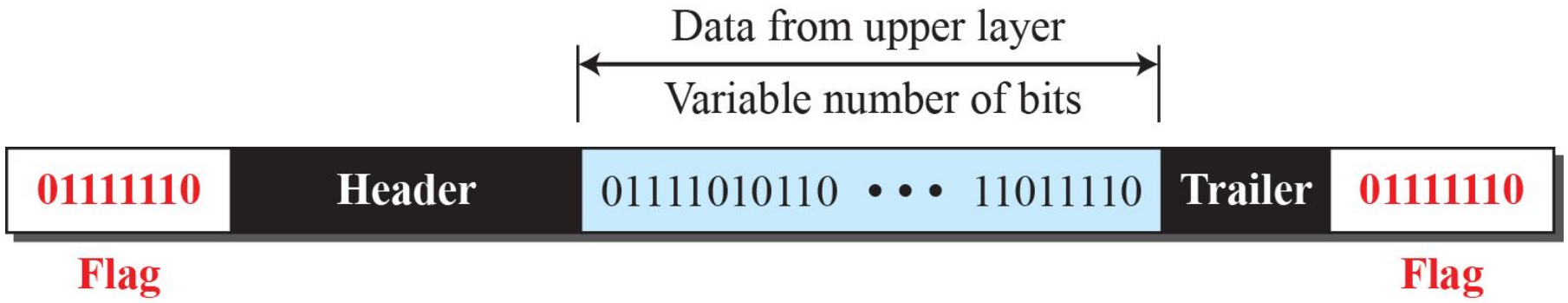
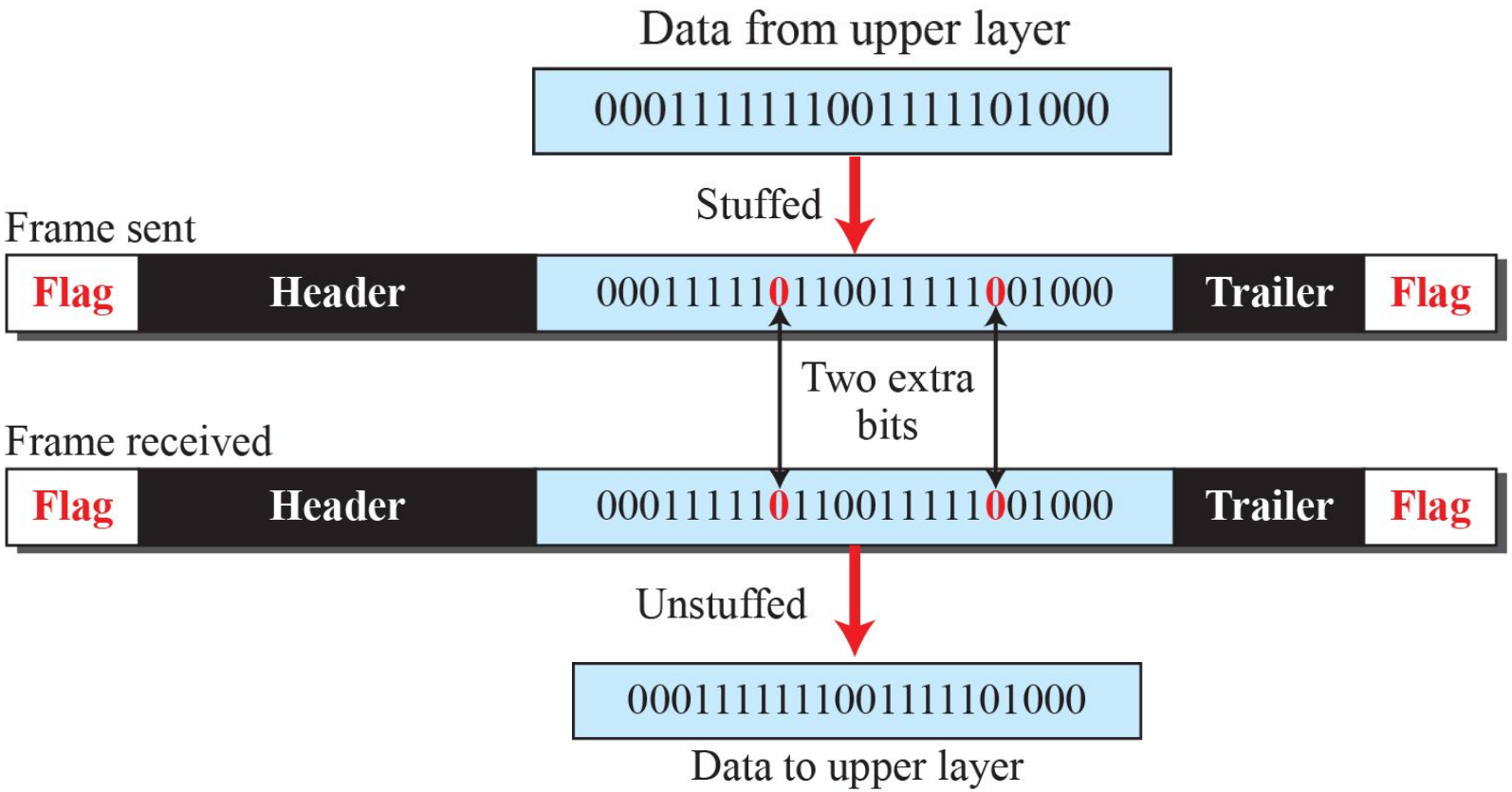


Figure 5.7: Bit stuffing and unstuffing



5.2.2 Flow and Error Control

We defined flow and error control in Chapter 3. One of the responsibilities of the data-link control sublayer is flow and error control at the data-link layer.

- *Flow Control*
- *Error Control*

5.2.3 Error Detection and Correction

At the data-link layer, if a frame is corrupted between the two nodes, it needs to be corrected before it continues its journey to other nodes. However, most link-layer protocols simply discard the frame and let the upper-layer protocols handle the retransmission of the frame. Some wireless protocols, however, try to correct the corrupted frame.

5.2.3 (continued)

- Introduction
  - Types of Errors
  - Redundancy
  - Detection versus Correction
  - Coding
- Block Coding
  - Error Detection
  - Hamming Distance
  - Minimum Hamming Distance for Error Detection

5.2.3 (continued)

- **Linear Block Codes**
  - Minimum Distance for Linear Block Codes
  - Parity-Check Code
- **Cyclic Codes**
  - Cyclic Redundancy Check
  - Polynomials
  - Requirement
  - Performance
  - Advantages of Cyclic Codes

5.2.3 (continued)

Checksum

- *Concept*
- *Internet Checksum*
- *Algorithm*
- *Other Approaches to the Checksum*

Figure 5.8: Single-bit and burst error

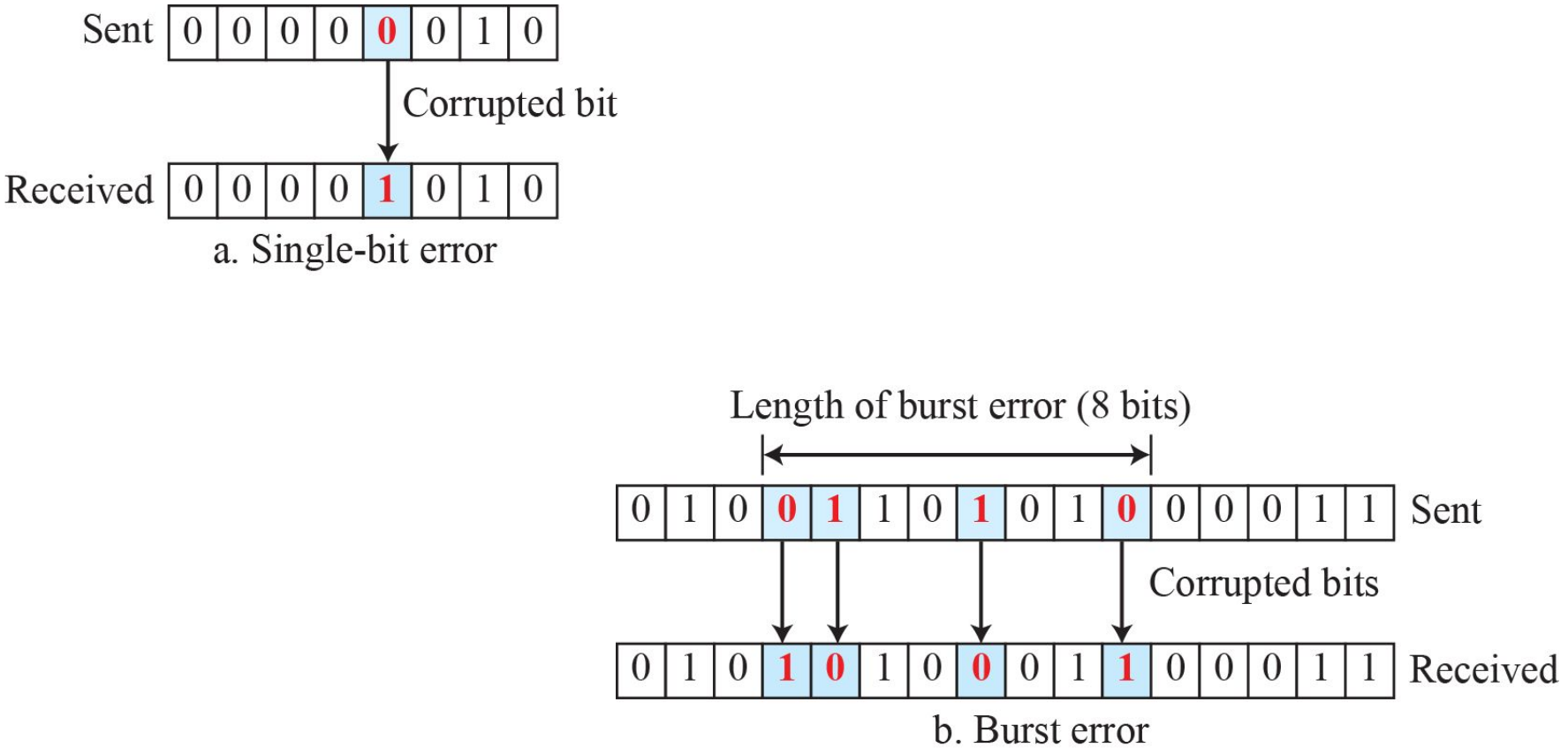
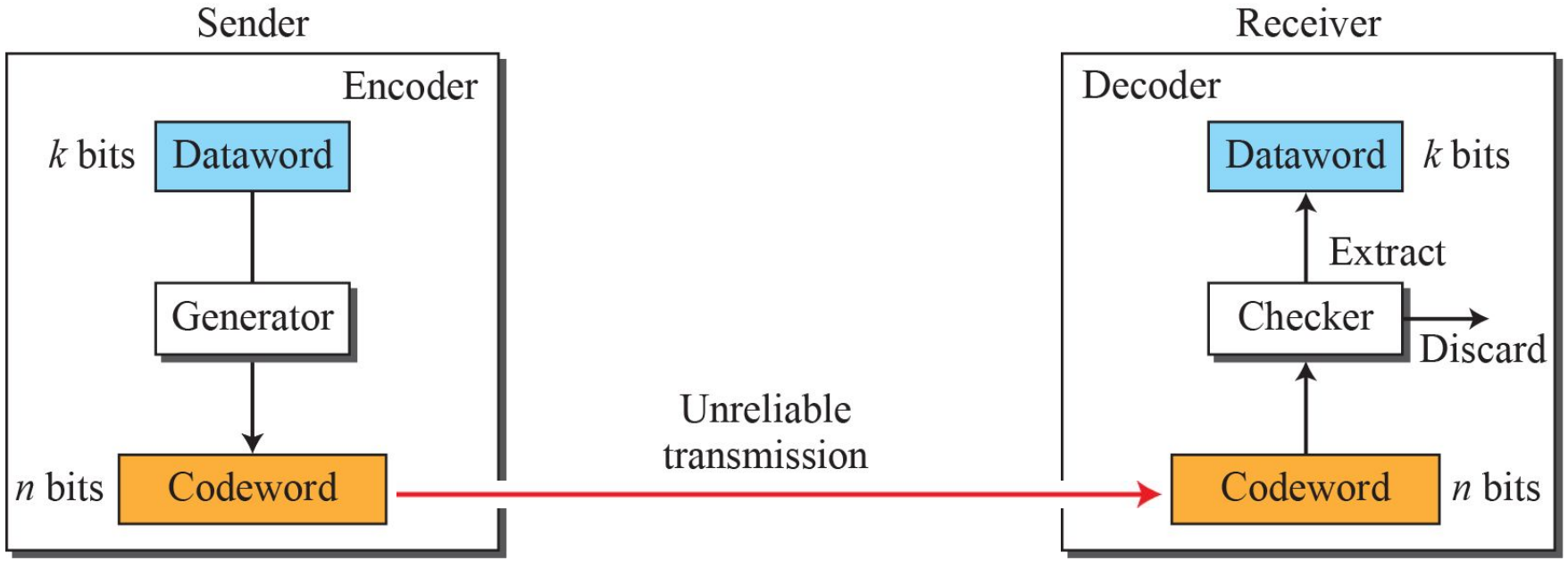


Figure 5.9: Process of error detection in block coding



Example 5.1

Let us assume that k = 2 and n = 3. Table 5.1 shows the list of datawords and codewords. Later, we will see how to derive a codeword from a dataword.

Table 5.1: A code for error detection in Example 5.1

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

Assume the sender encodes the dataword 01 as 011 and sends it to the receiver. Consider the following cases:

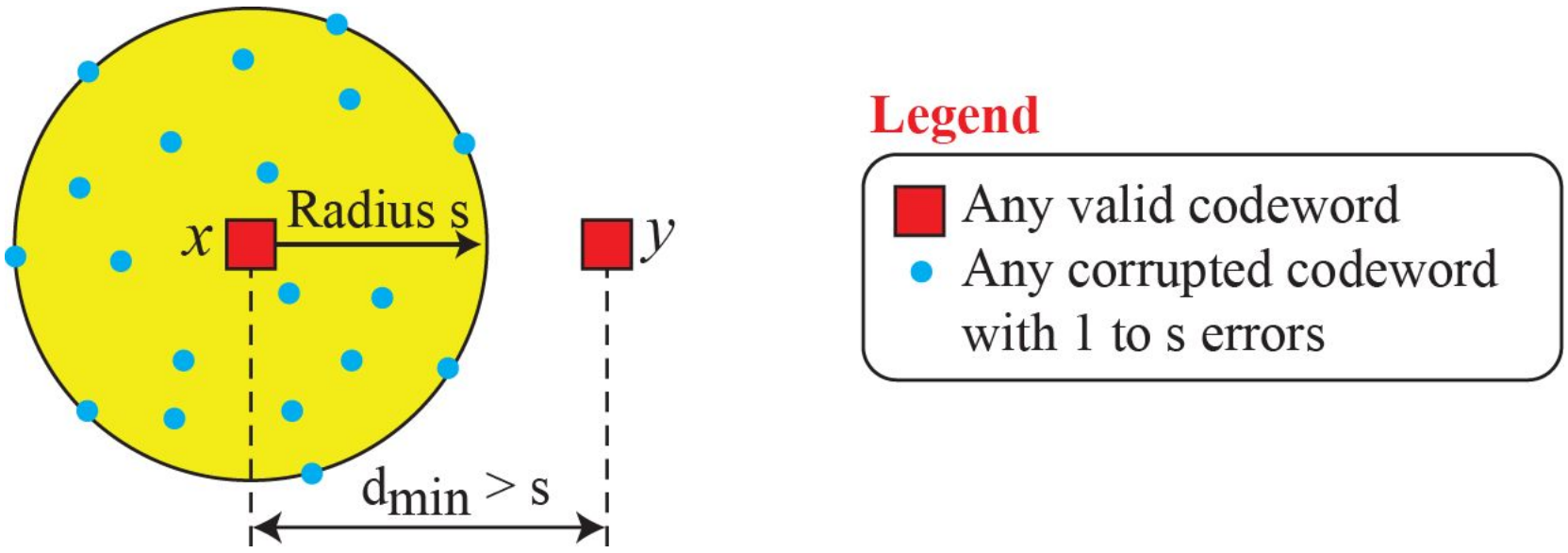
1. The receiver receives 011. It is a valid codeword. The receiver extracts the dataword 01 from it.
2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, 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.

Example 5.2

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

1. The Hamming distance $d(000, 011)$ is 2 because $(000 \oplus 011)$ is 011 (two 1s).
2. The Hamming distance $d(10101, 11110)$ is 3 because $(10101 \oplus 11110)$ is 01011 (three 1s).

Figure 5.10: Geometric concept explaining d_{min} in error detection



Example 5.3

The minimum Hamming distance for our first code scheme (Table 5.1) 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 5.4

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

Example 5.5

The code in Table 5.1 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.

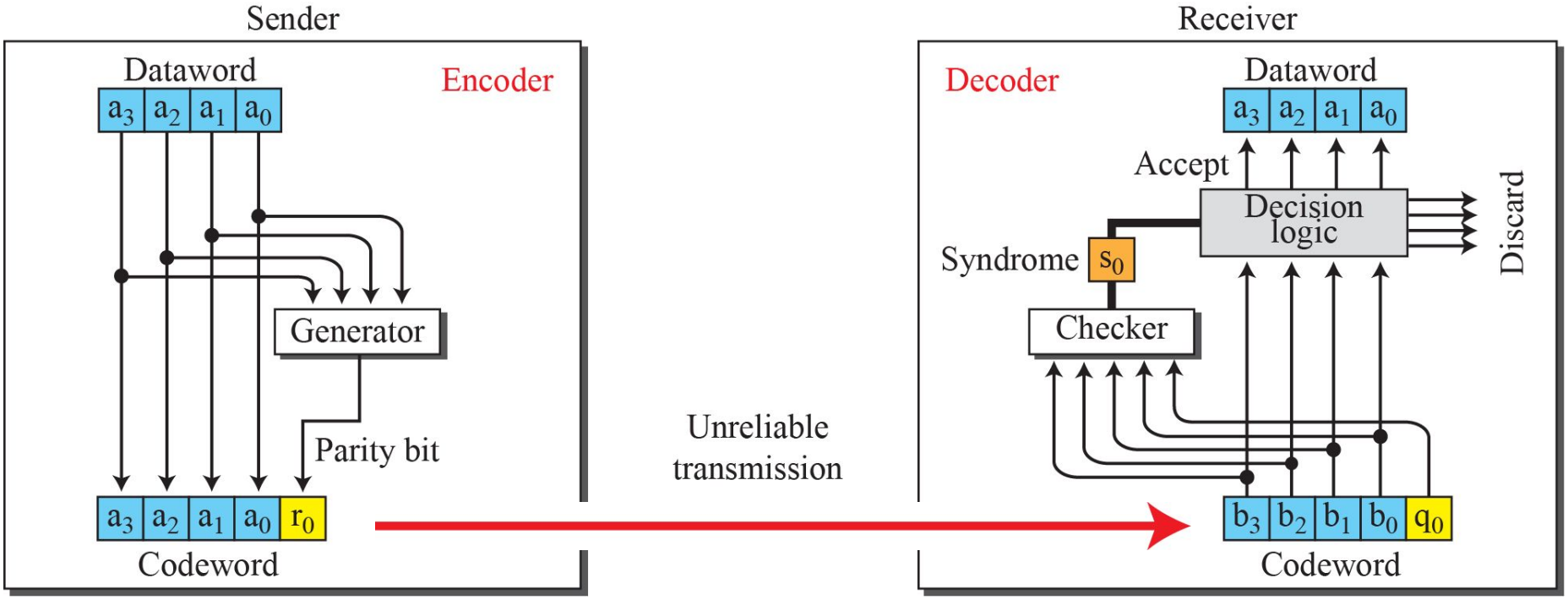
Example 5.6

In our first code (Table 5.1), 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 5.2: 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 5.11: Encoder and decoder for simple parity-check code



Example 5.7

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.
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.
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.

Table 5.3: A CRC code with C(7, 4)

Dataword	*Codeword*	*Dataword*	*Codeword*
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 5.12: CRC encoder and decoder

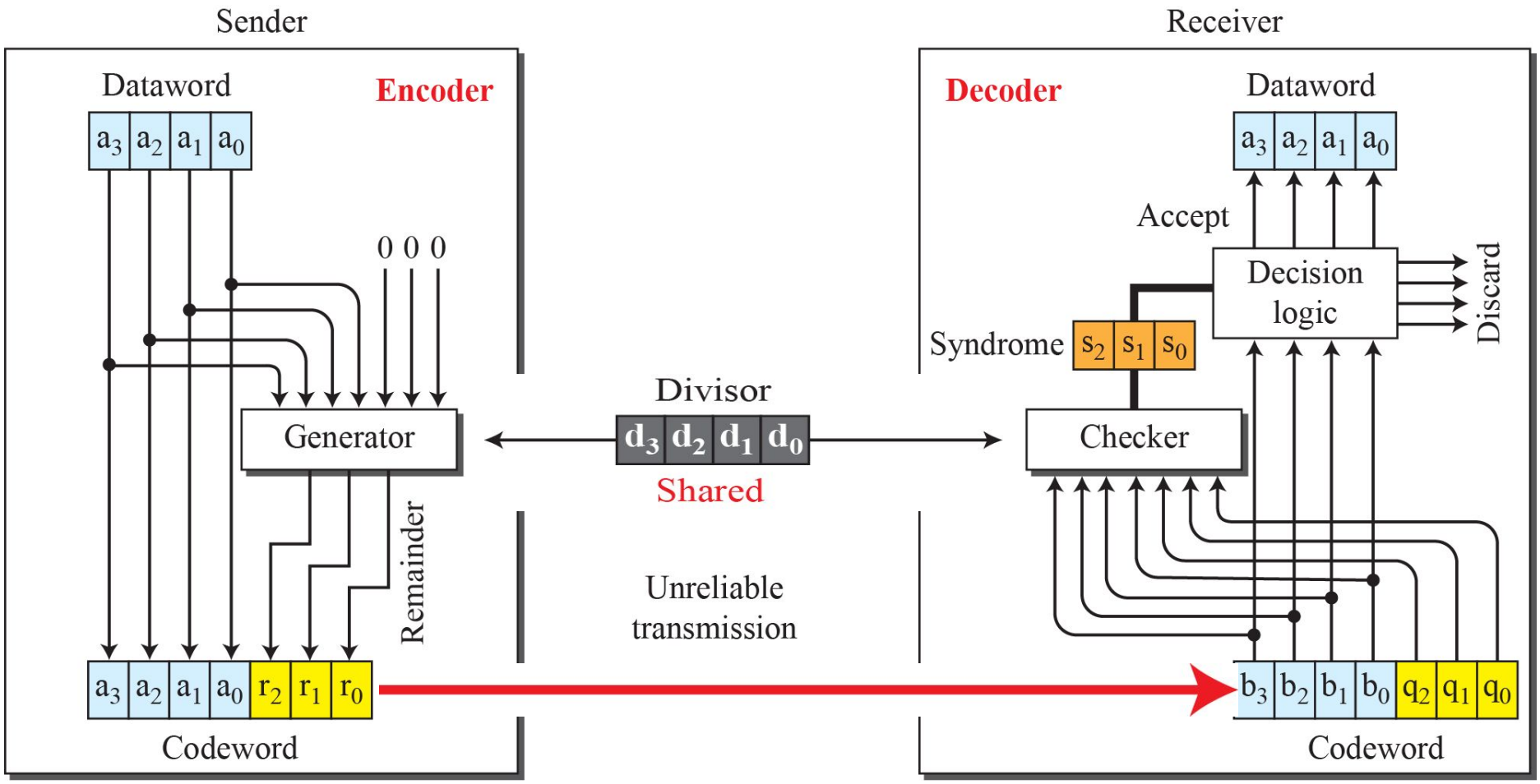


Figure 5.13: Division in CRC encoder

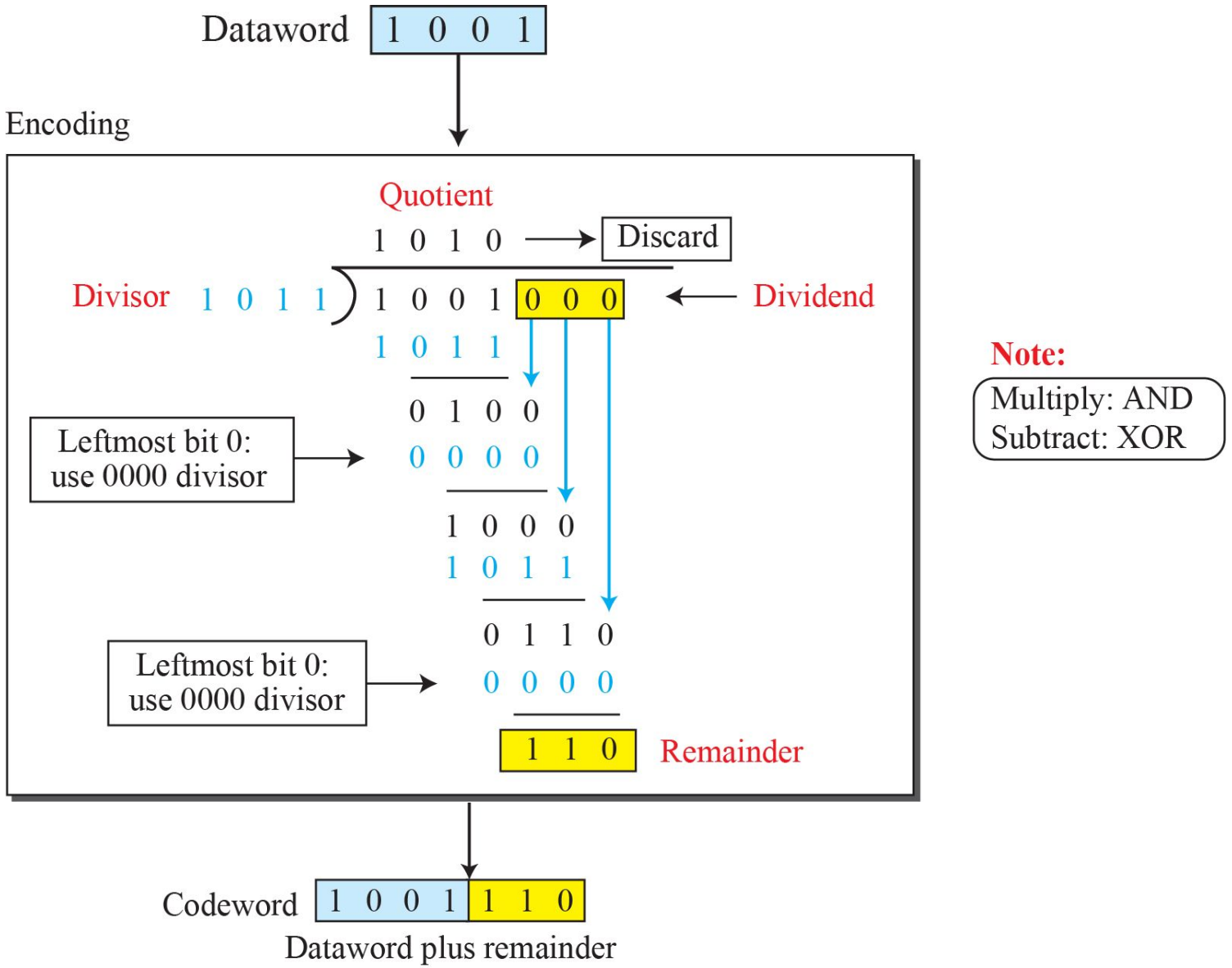


Figure 5.14: Division in the CRC decoder for two cases

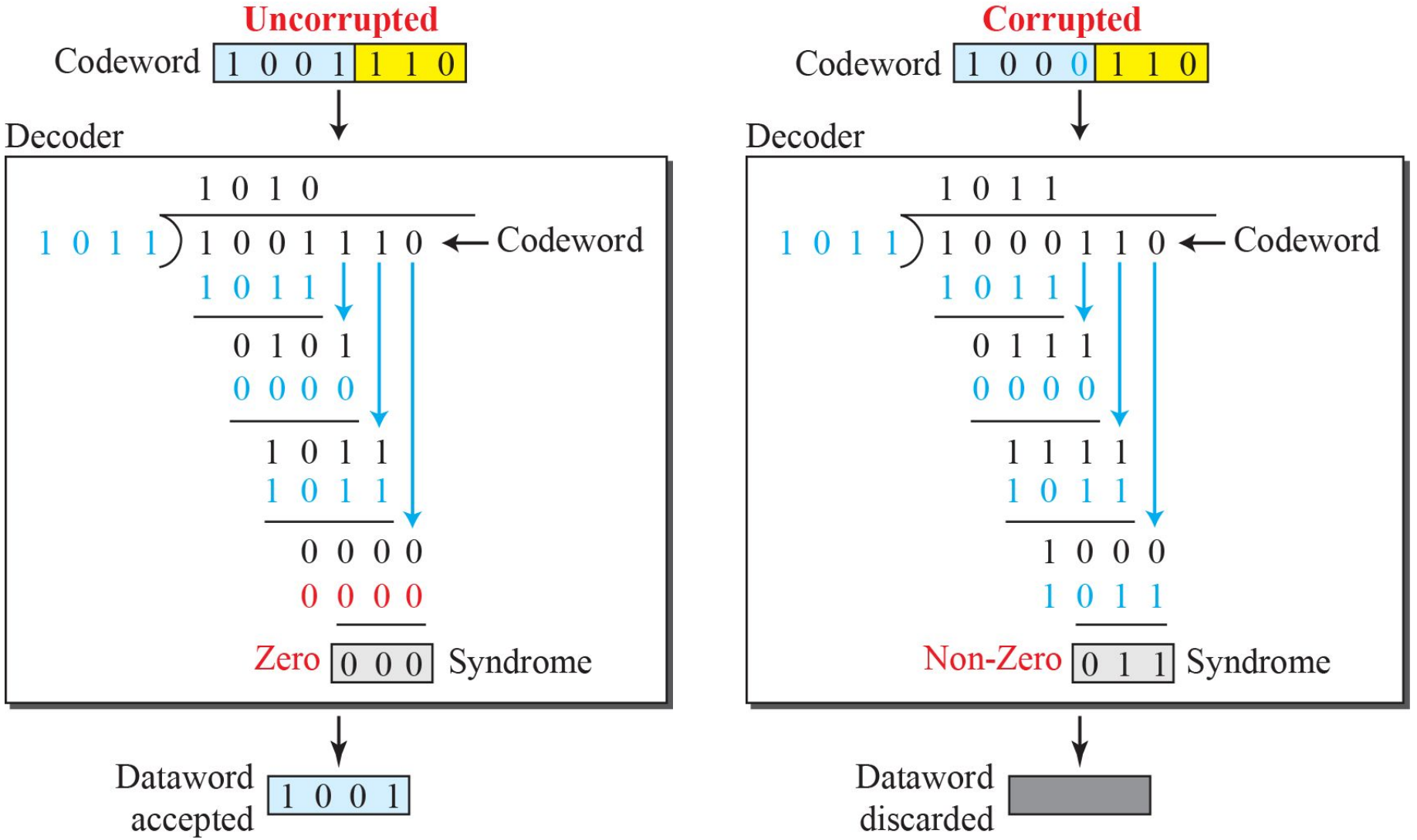
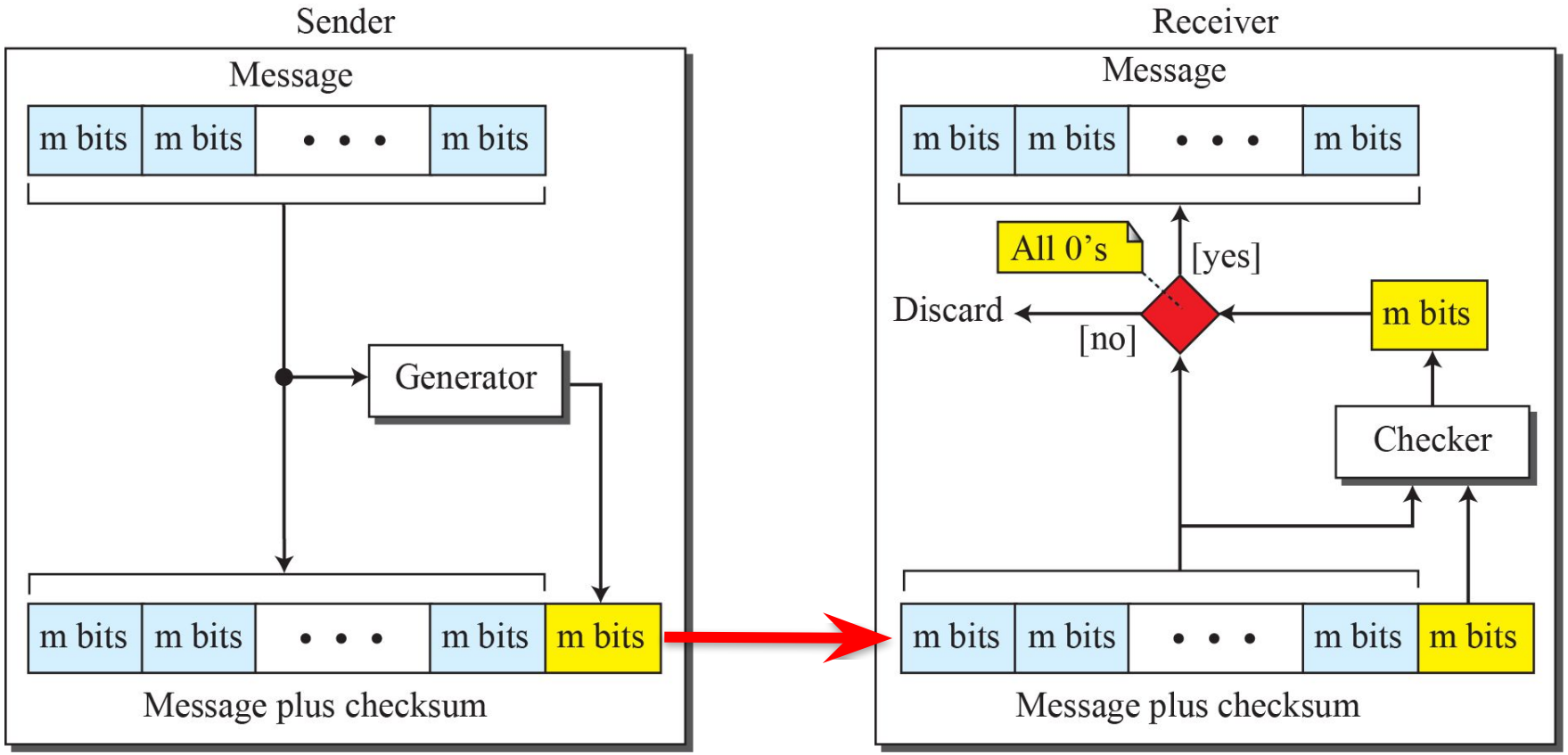


Table 5.4: Standard polynomials

Name	*Binary*	*Application*
CRC-8	100000111	ATM header
CRC-10	11000110101	ATM AAL
CRC-16	1000100000100001	HDLC
CRC-32	10000010011000001000111011011011	LANs

Figure 5.15: Checksum



Example 5.8

Suppose the message is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, **36**), where **36** is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the message not accepted.

Example 5.9

In the previous example, the decimal number 36 in binary is (100100)2. To change it to a 4-bit number we add the extra leftmost bit to the right four bits as shown below.

$$(10)_2 + (0100)_2 = (0110)_2 \rightarrow (6)_{10}$$

Instead of sending 36 as the sum, we can send 6 as the sum (7, 11, 12, 0, 6, 6). The receiver can add the first five numbers in one's complement arithmetic. If the result is 6, the numbers are accepted; otherwise, they are rejected.

Example 5.10

Let us use the idea of the checksum in Example 5.9. The sender adds all five numbers in one's complement to get the sum = 6. The sender then complements the result to get the checksum = **9**, which is 15 − 6. Note that 6 = (0110)2 and **9**= (1001)2; they are complements of each other. The sender sends the five data numbers and the checksum (7, 11, 12, 0, 6, **9**). If there is no corruption in transmission, the receiver receives (7, 11, 12, 0, 6, **9**) and adds them in one's complement to get 15.

Figure 5.16: Example 5.10

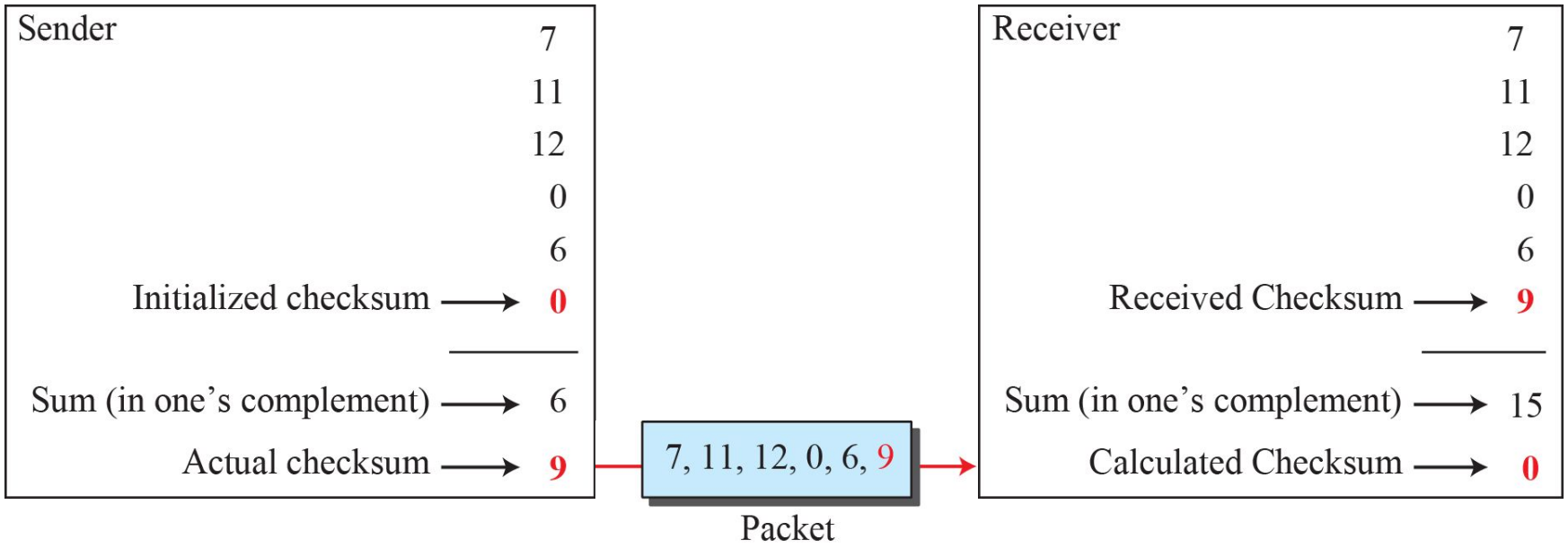


Table 5.5: Procedure to calculate the traditional checksum

Sender	*Receiver*
1. The message is divided into 16-bit words.	1. The message and the checksum is received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words are added using one's complement addition.
4. The sum is complemented and becomes the checksum.	4. The sum is complemented and becomes the new checksum.
5. The checksum is sent with the data.	5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.

Figure 5.17: Algorithm to calculate a traditional checksum

Notes:

a. Word and Checksum are each 16 bits, but Sum is 32 bits.
b. Left(Sum) can be found by shifting Sum 16 bits to the right.
c. Right(Sum) can be found by ANDing Sum with $(0000FFFF)_{16}$.
d. After Checksum is found, truncate it to 16 bits.

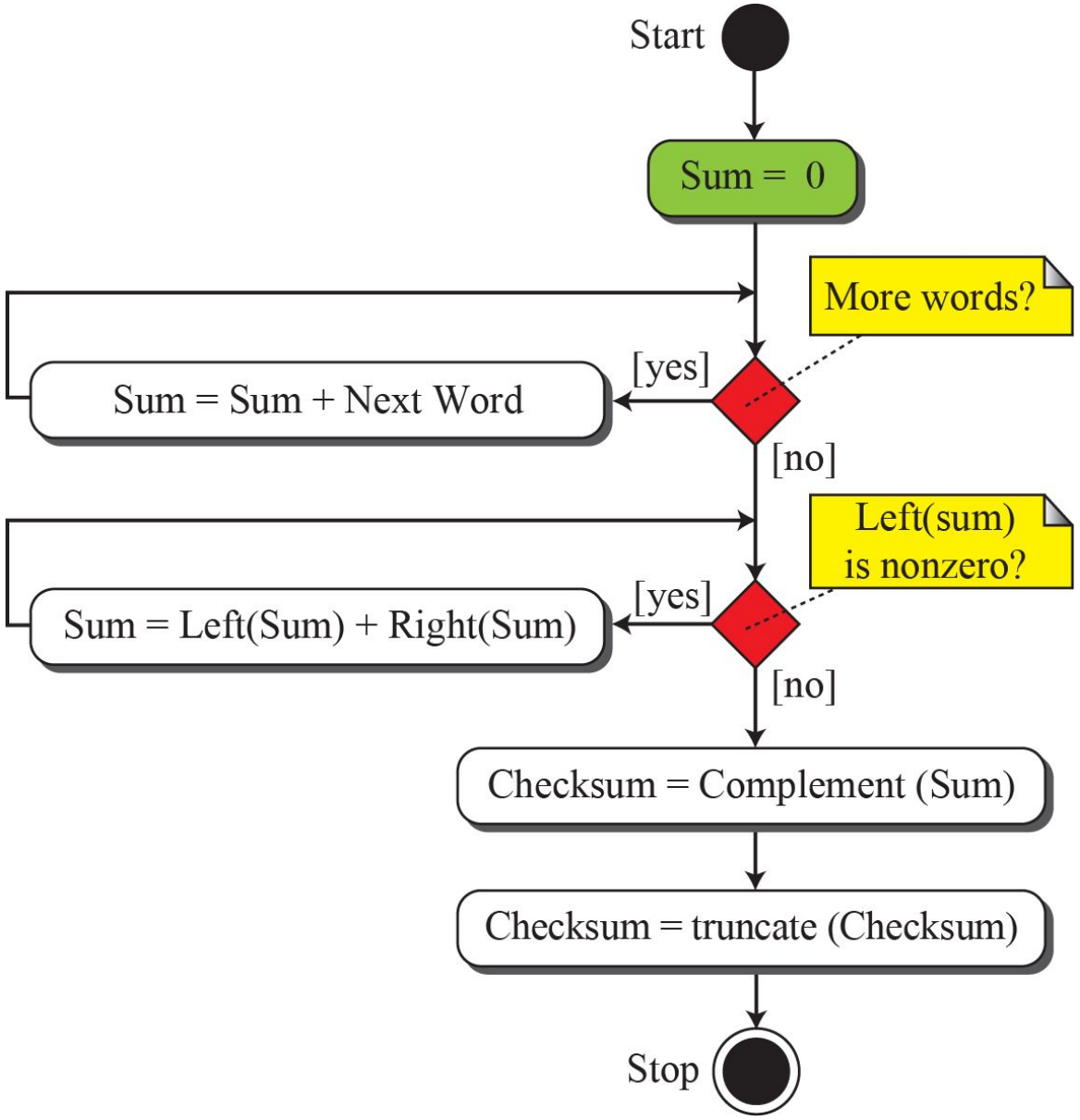


Figure 5.18: Algorithm to calculate an 8-bit Fletcher checksum

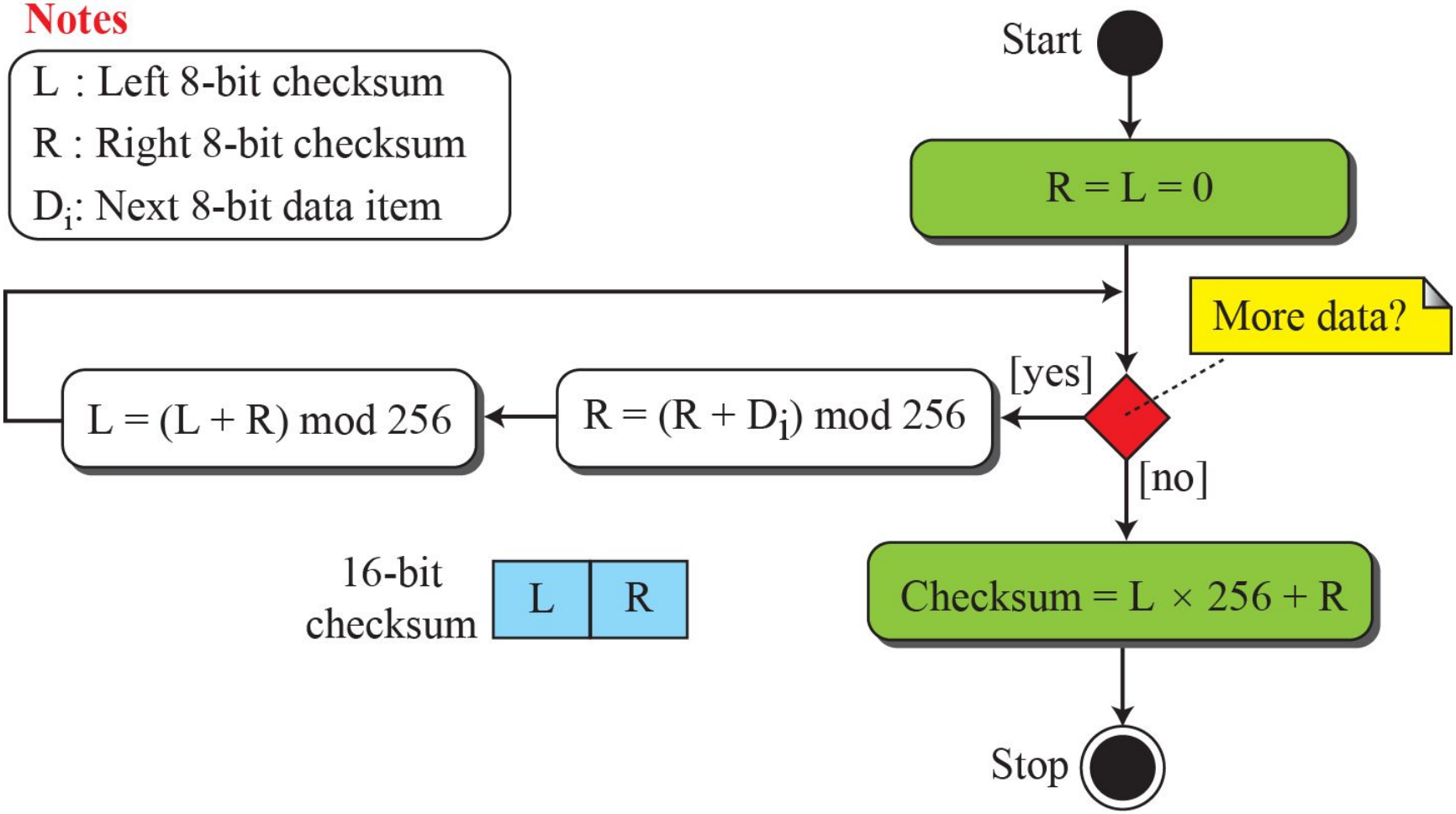
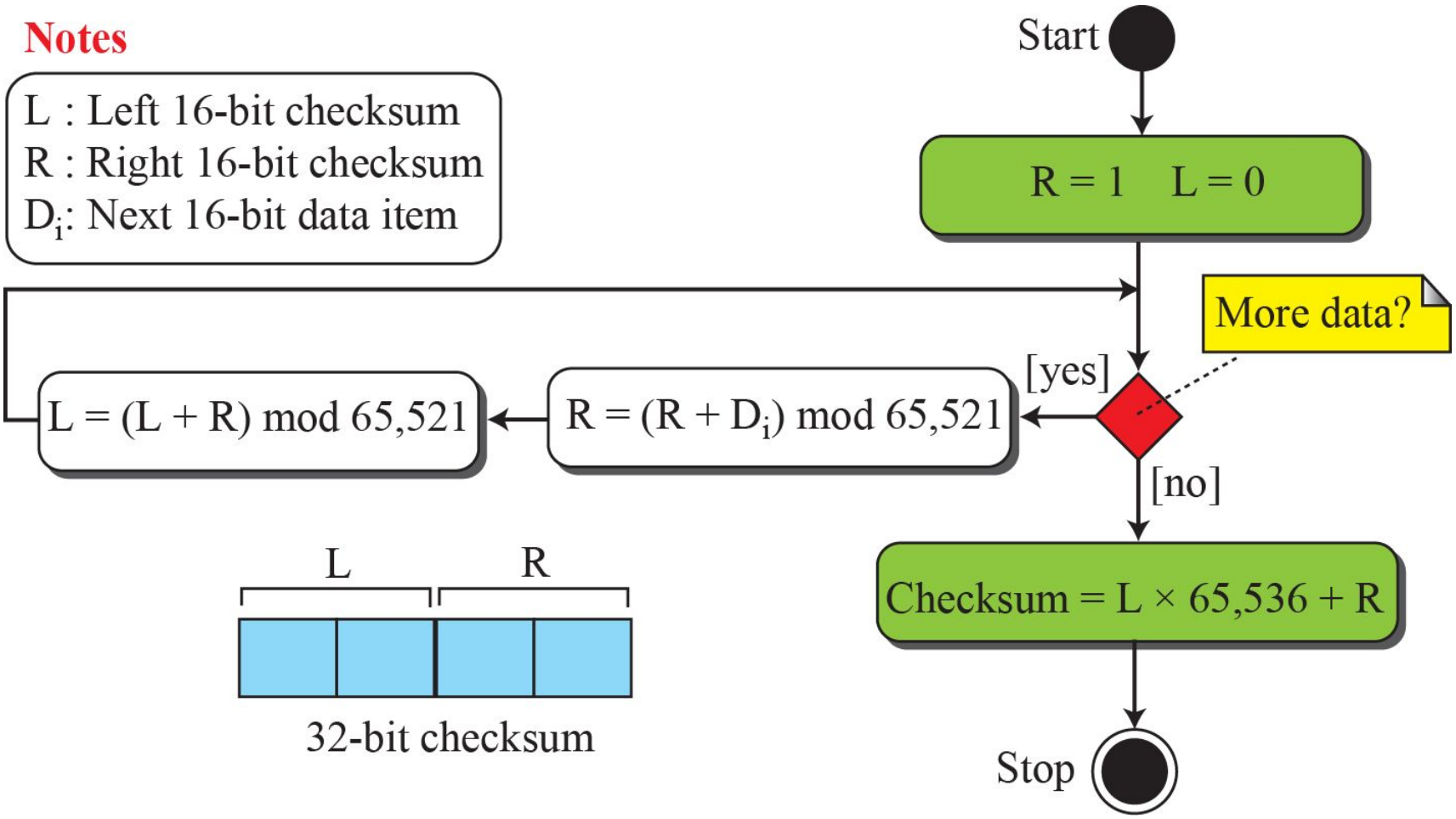


Figure 5.19: Algorithm to calculate an Adler checksum



5.2.4 Two DLC Protocols

After finishing all issues related to the DLC sublayer, we discuss two DLC protocols that actually implemented those concepts. The first, HDLC, is the base of many protocols that have been designed for LANs. The second, Point to-Point, is a protocol derived from HDLC and is used for point-to-point links.

5.2.4 (continued)

- **HDLC**
  - *Configuration and Transfer Modes*
  - *Frames*
- **Point-to-Point Protocol (PPP)**
  - *Services*
  - *Framing*
  - *Transition Phases*
  - *Multiplexing*
  - *Multilink PPP*

Figure 5.20: Normal response mode

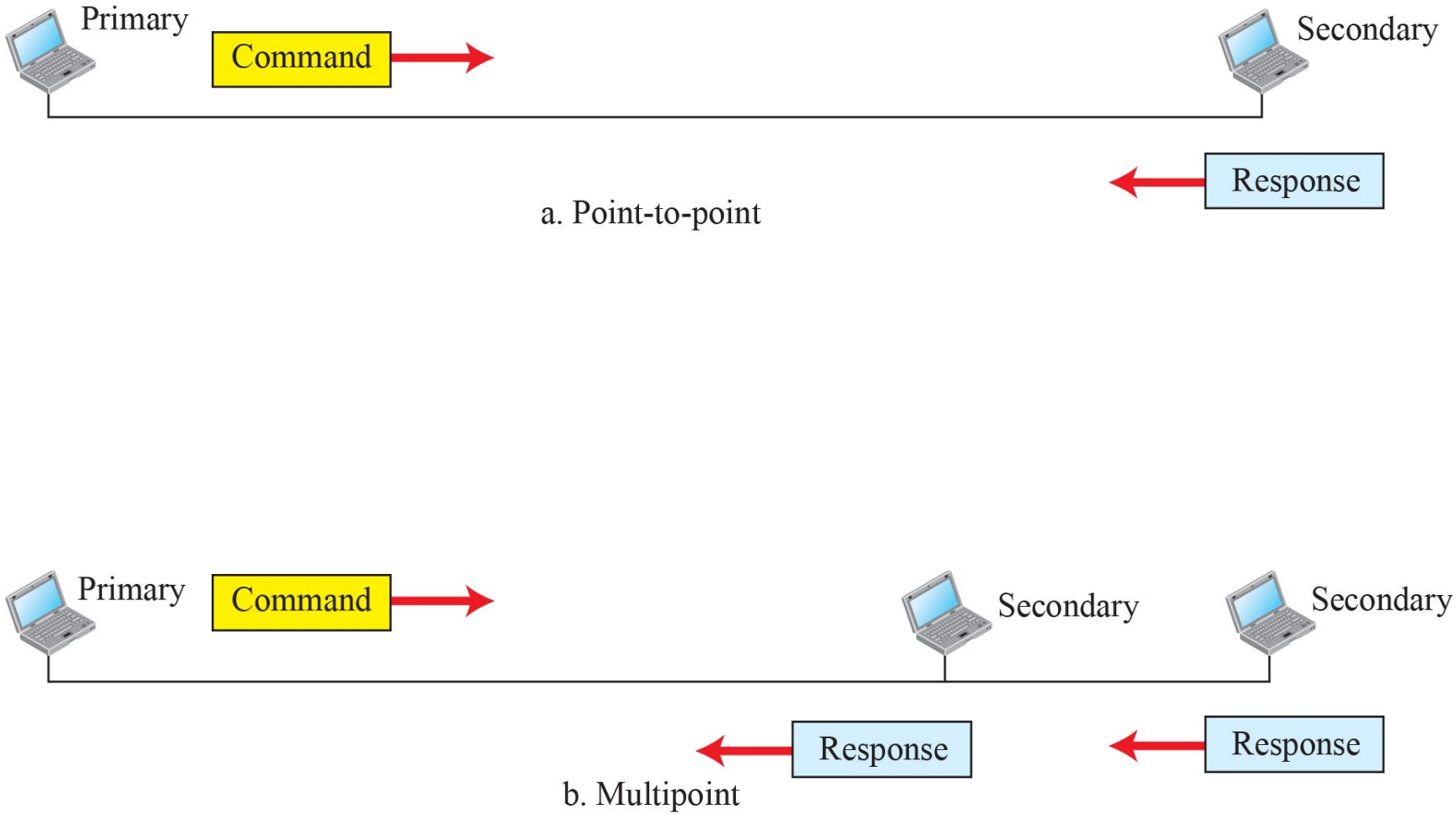


Figure 5.21: Asynchronous balanced mode

Figure 5.22: HDLC frames

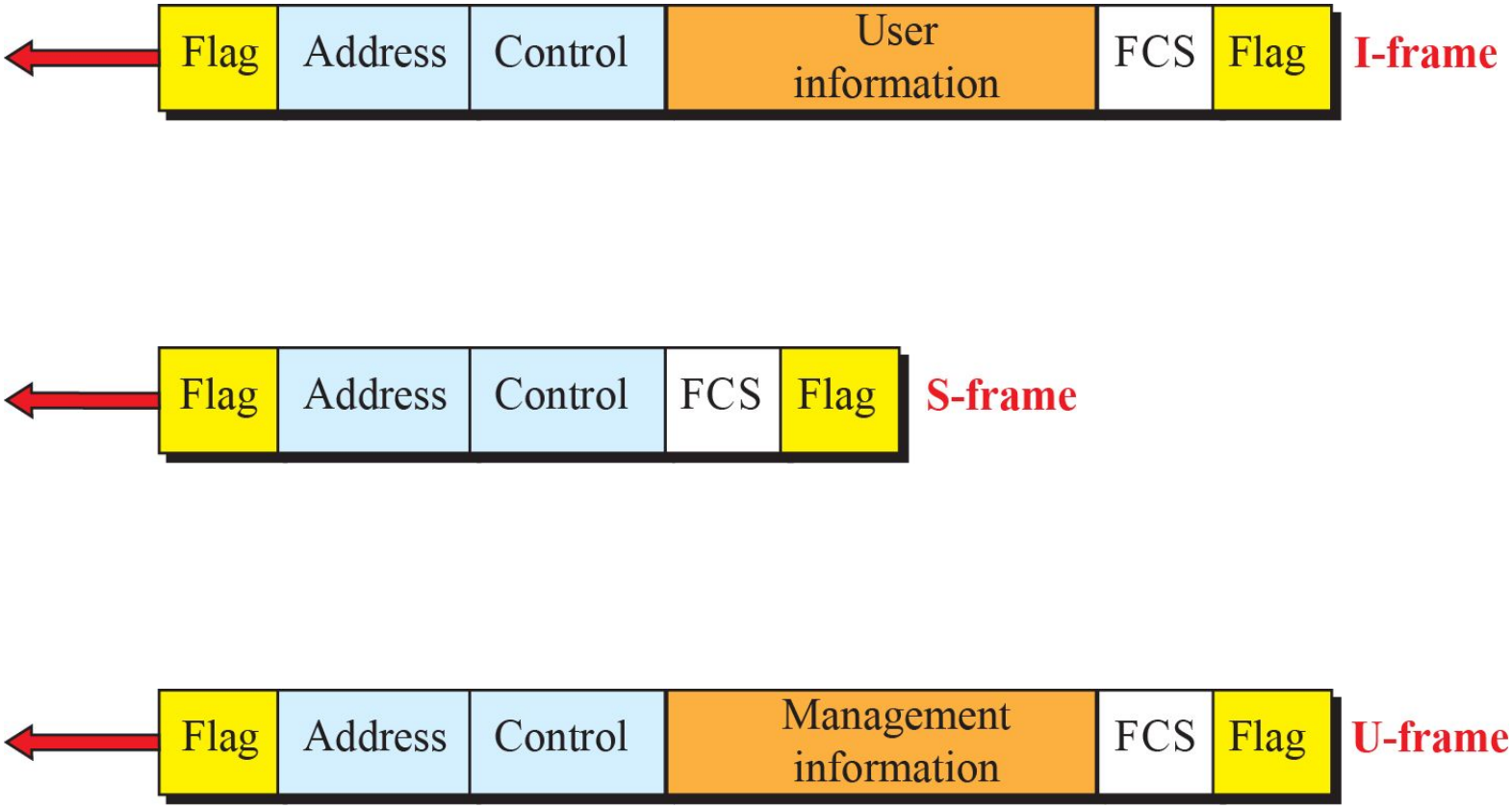


Figure 5.23: ***Control field format for the different frame types***

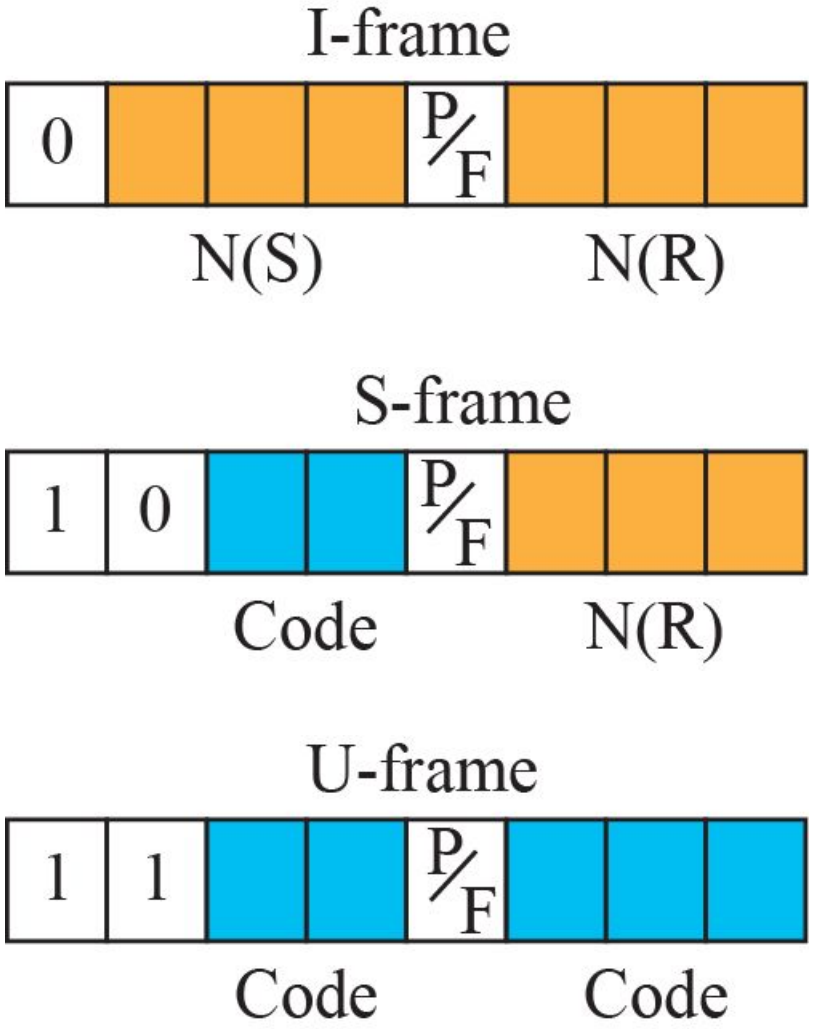


Figure 5.24: PPP frame format

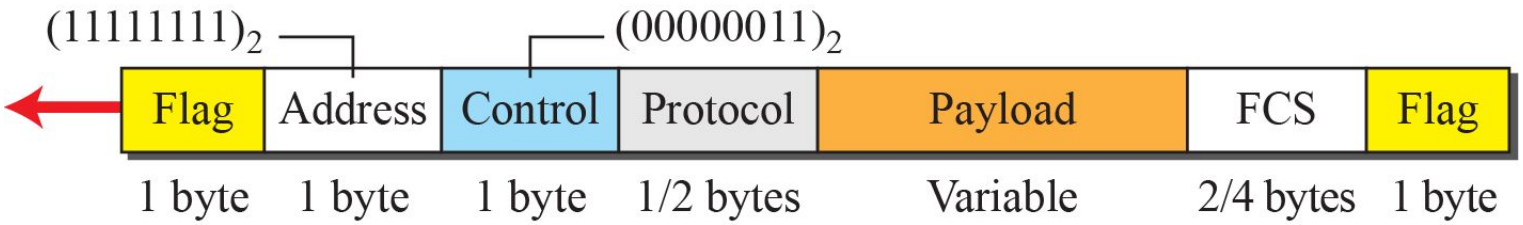


Figure 5.25: Transition phases

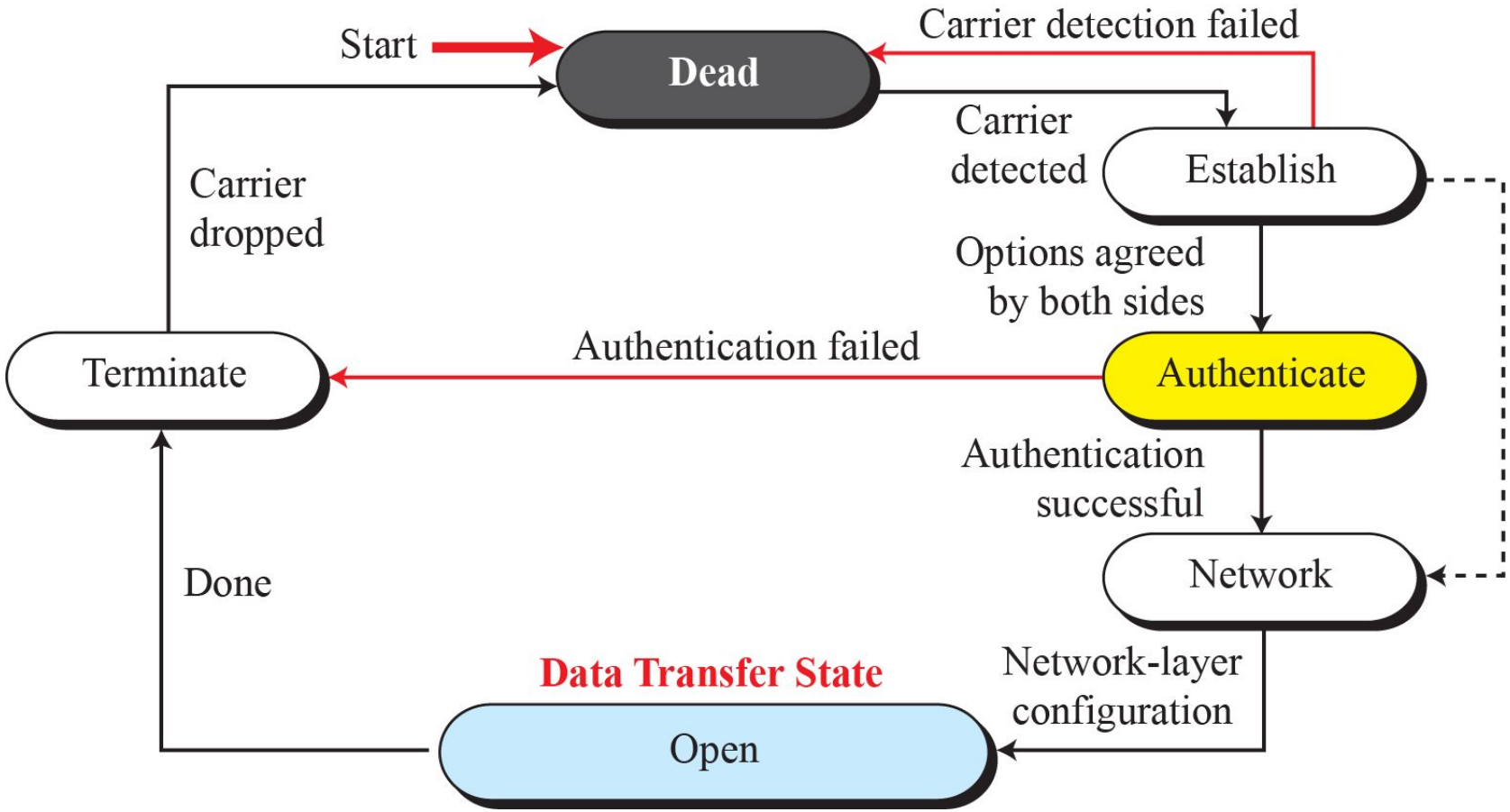
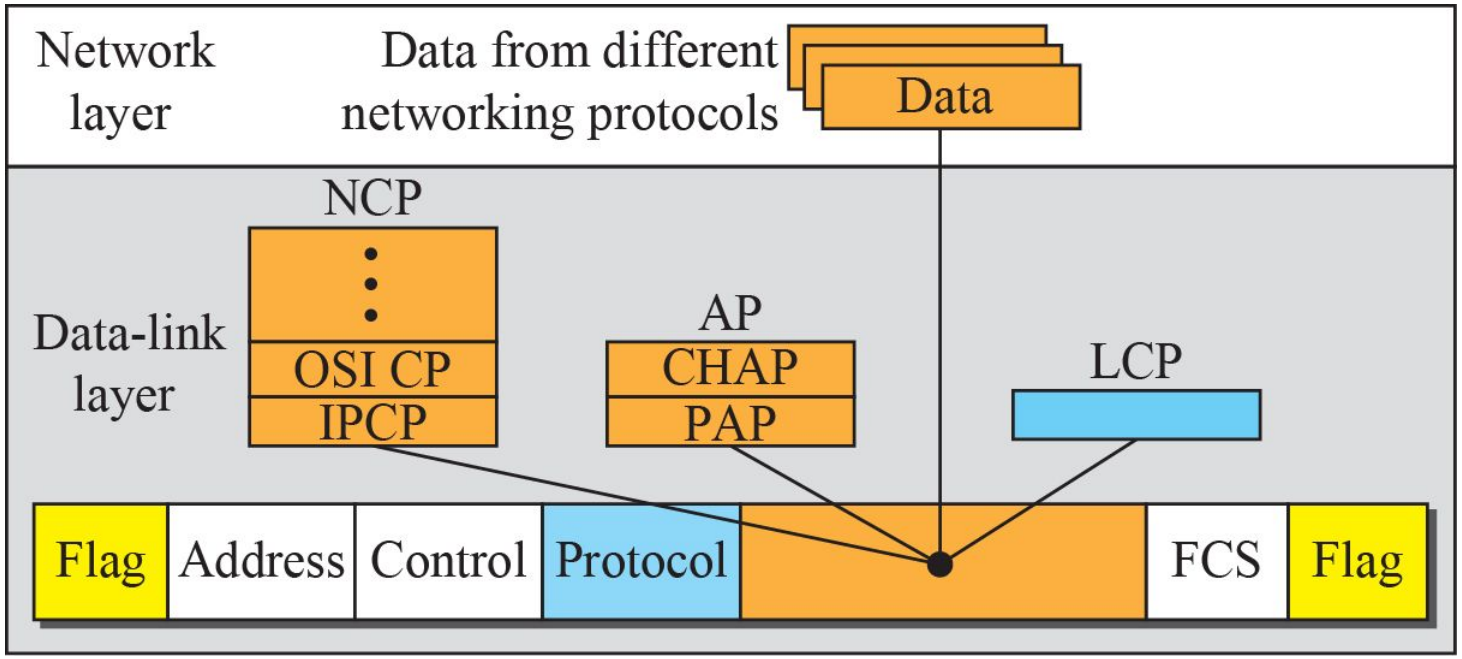


Figure 5.26: Multiplexing in PPP



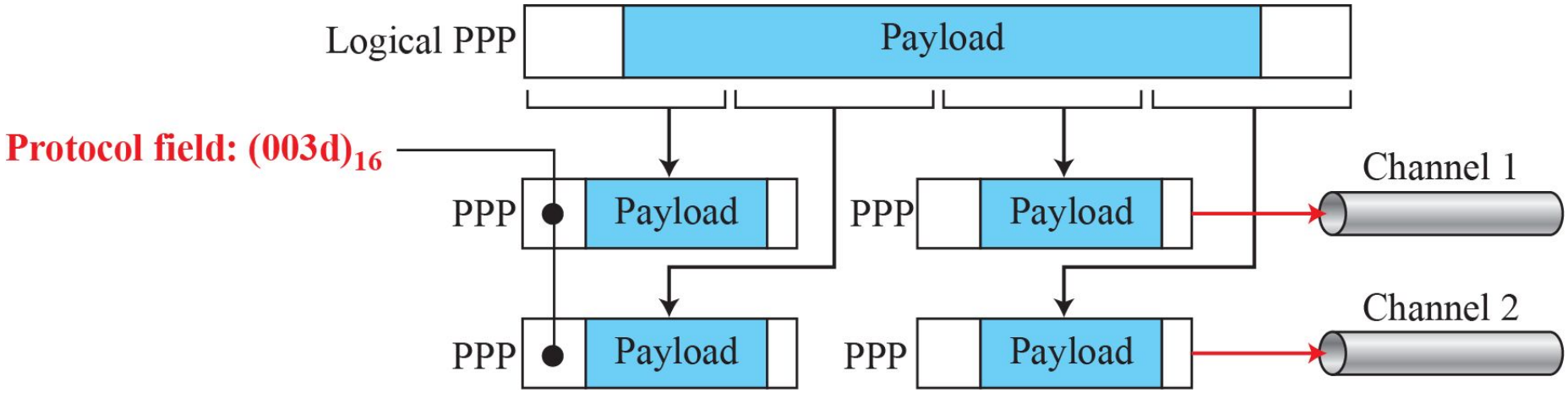
Legend

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 ....

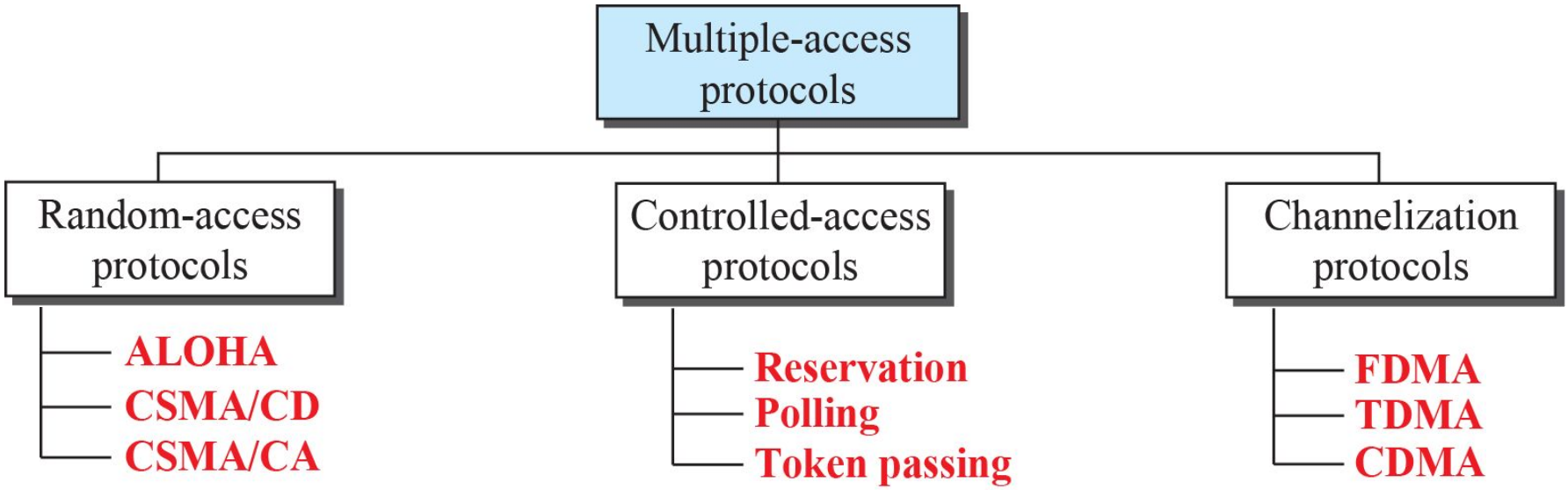
Figure 5.27: Multilink PPP



5-3 MULTIPLE ACCESS PROTOCOLS

We said that the data-link layer is divided into two sublayers: data link control (DLC) and media access control (MAC). We discussed DLC in the previous section; we talk about MAC in this section.

Figure 5.28: Taxonomy of multiple-access protocols



5.3.1 Random Access

In random-access or contention methods, no station is superior to another station and none is assigned the 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). In other words, each station can transmit when it desires on the condition that it follows the predefined procedure, including the testing of the state of the medium.

5.3.1 (continued)

- ALOHA
  - Pure ALOHA
  - Slotted ALOHA
- CSMA
  - Vulnerable Time
  - Persistence Methods
- CSMA/CD
  - Minimum Frame Size
  - Procedure
  - Energy Level
  - Throughput
  - Traditional Ethernet
- CSMA/CA

Figure 5.29: Frames in a pure ALOHA network

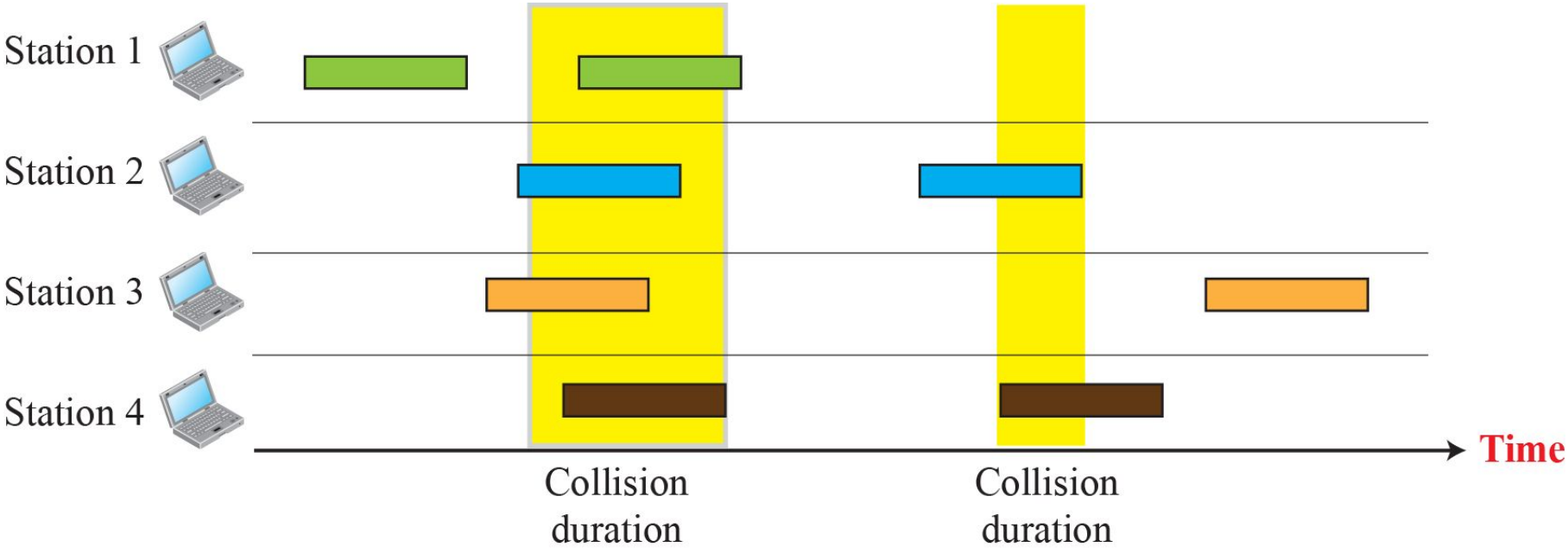
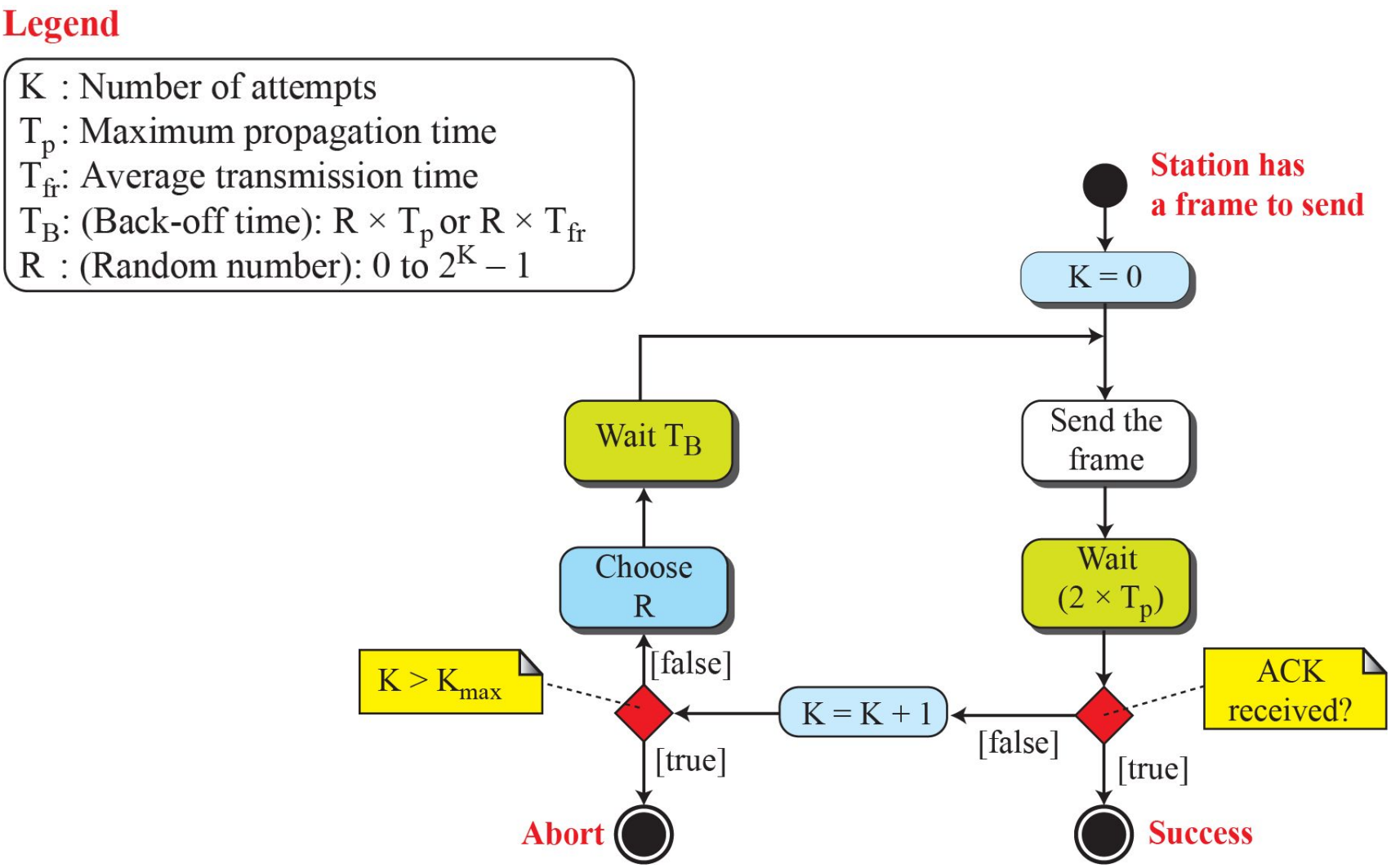


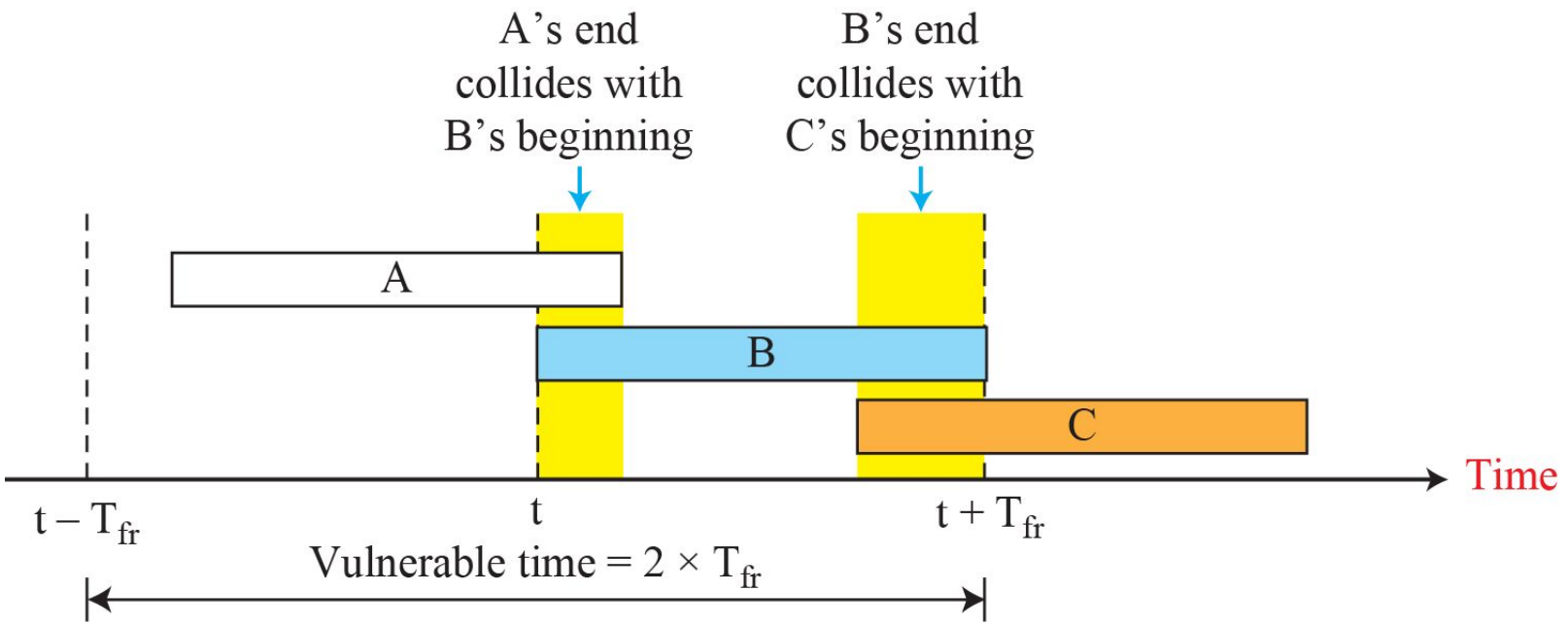
Figure 5.30: Procedure for pure ALOHA protocol



Example 5.11

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 5.31: Vulnerable time for pure ALOHA protocol



Example 5.12

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 5.13

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 5.13 (continued)

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 × 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 × 0.152 = 38. Only 38 frames out of 250 will probably survive

Figure 5.32: Frames in a slotted ALOHA network

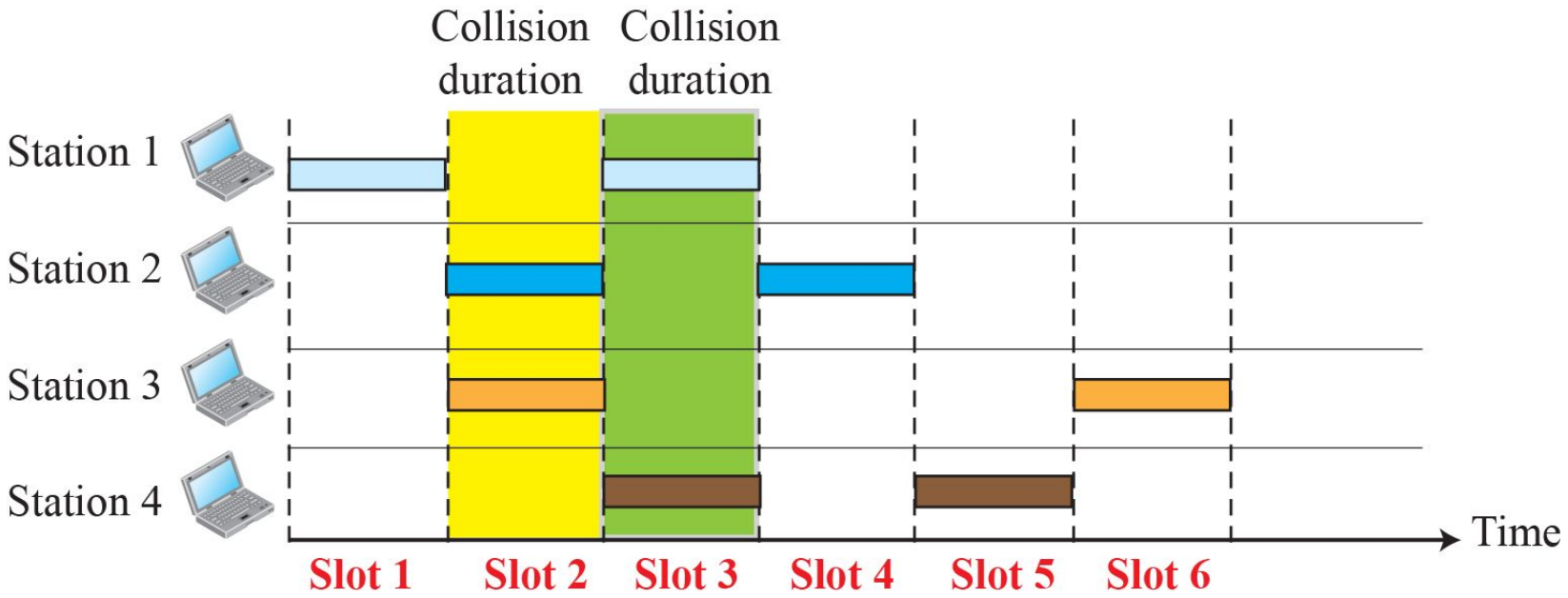
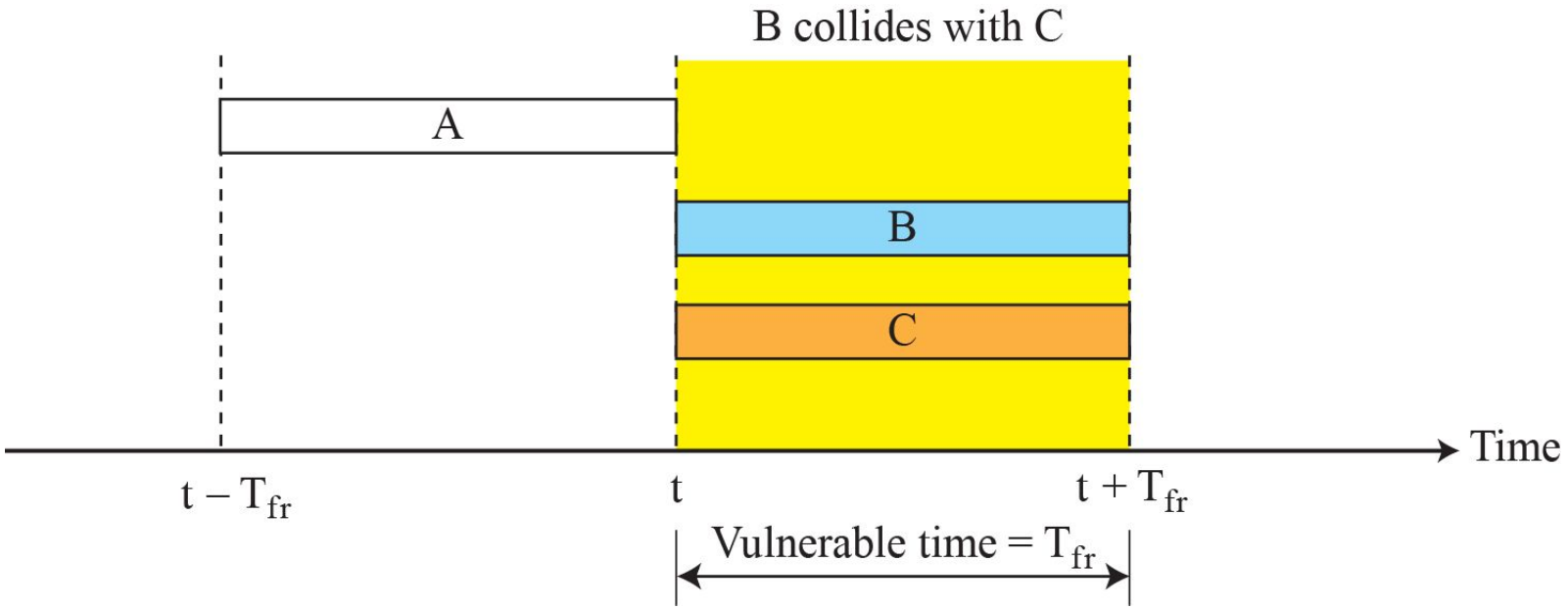


Figure 5.33: Vulnerable time for slotted ALOHA protocol



Example 5.14

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 5.14 (continued)

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.

Figure 5.34: Space/time model of a collision in CSMA (Part I: model)

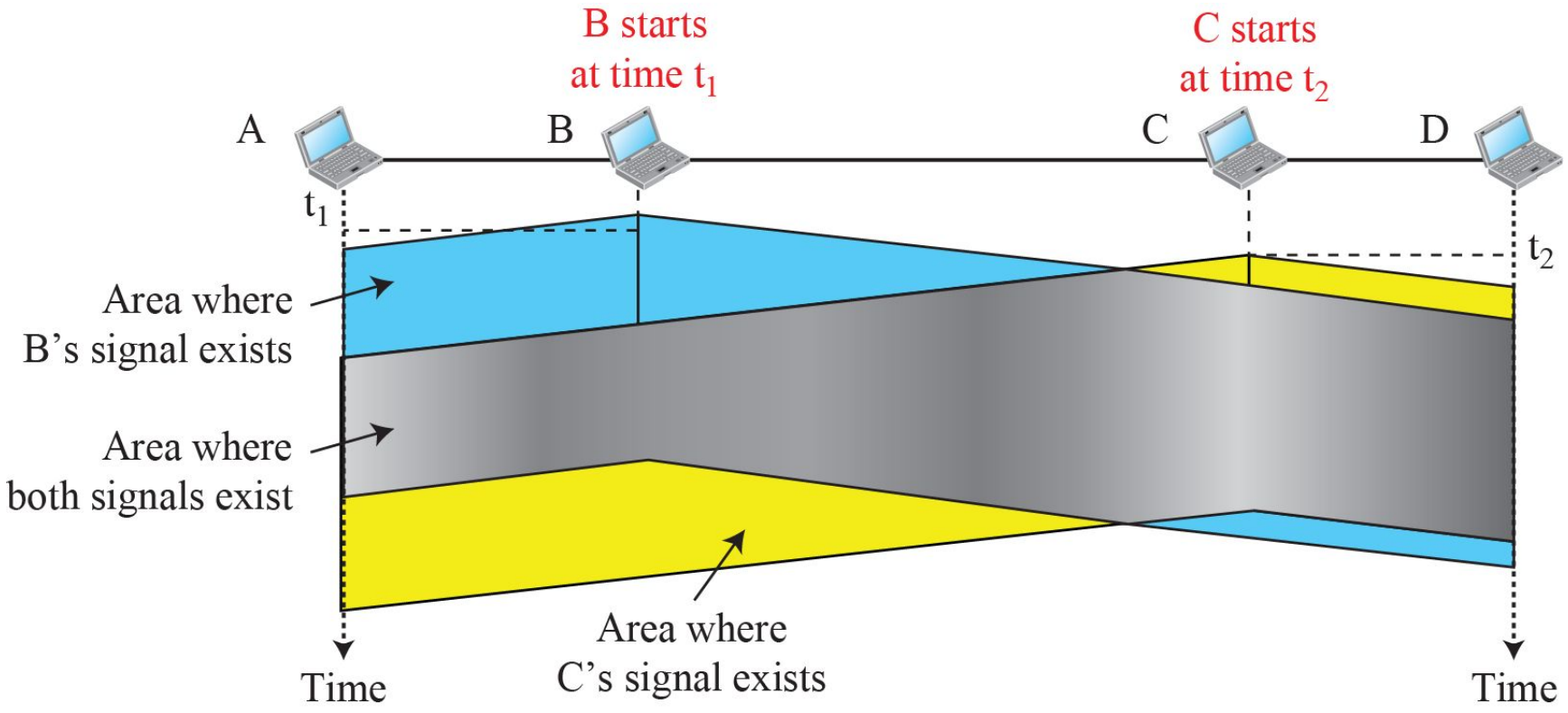


Figure 5.34: Space/time model of a collision in CSMA (Part II: timing)

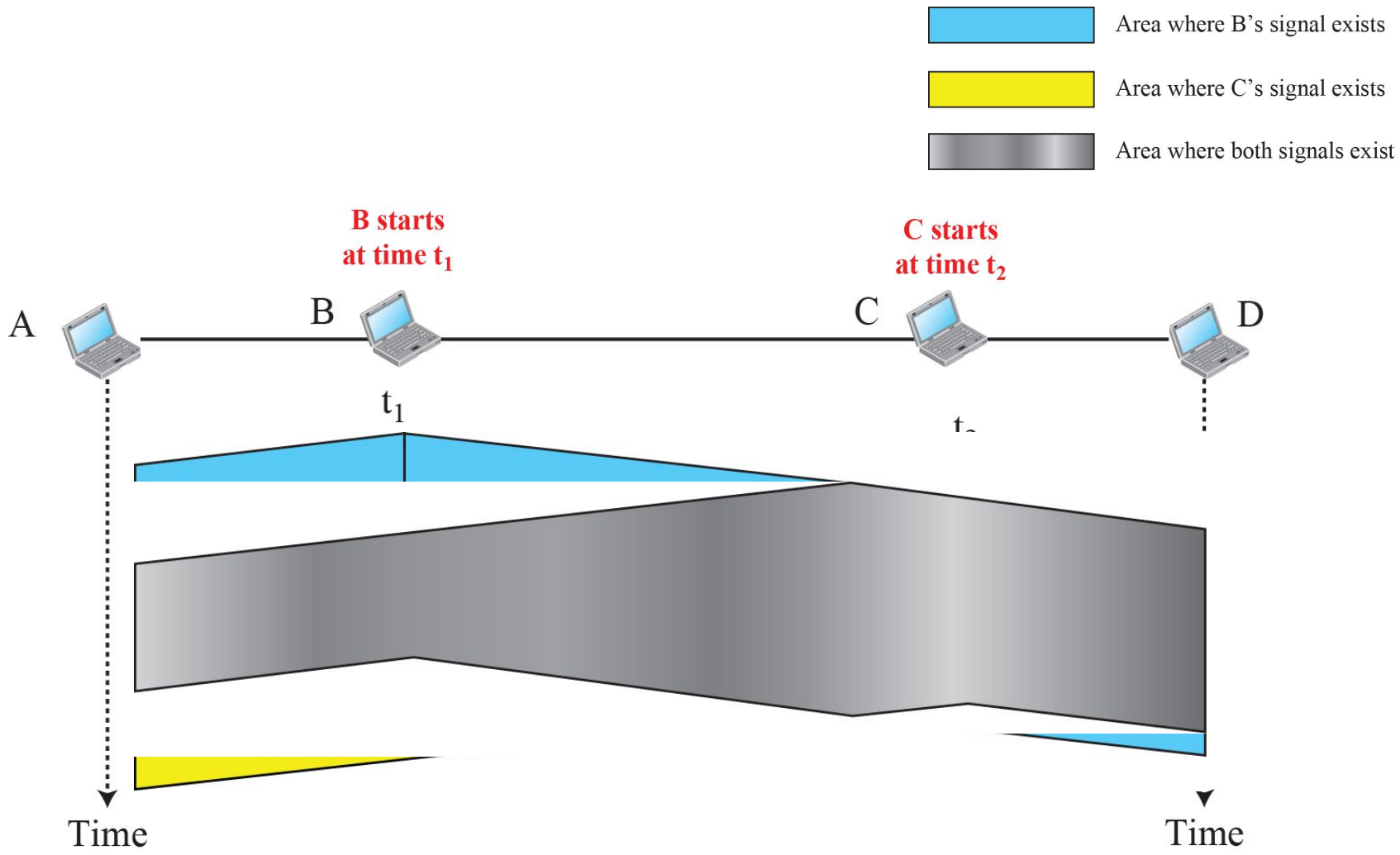


Figure 5.35: Vulnerable time in CSMA

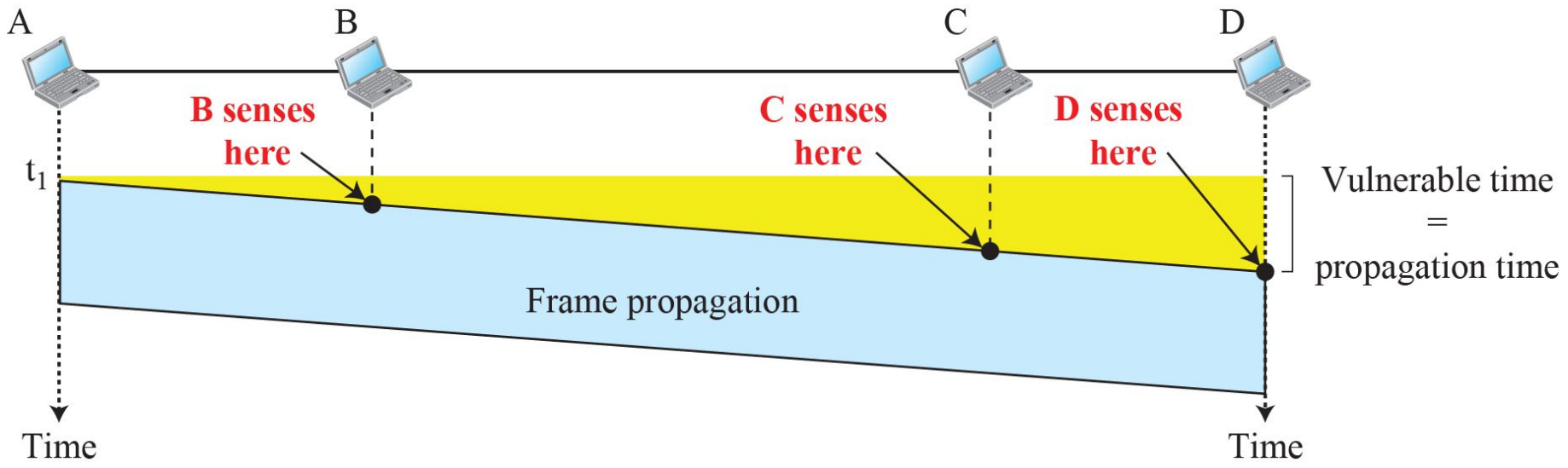
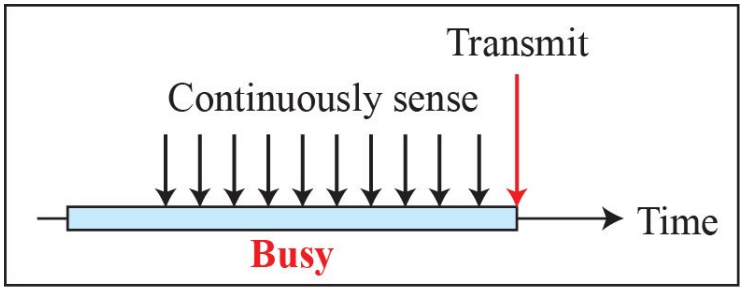
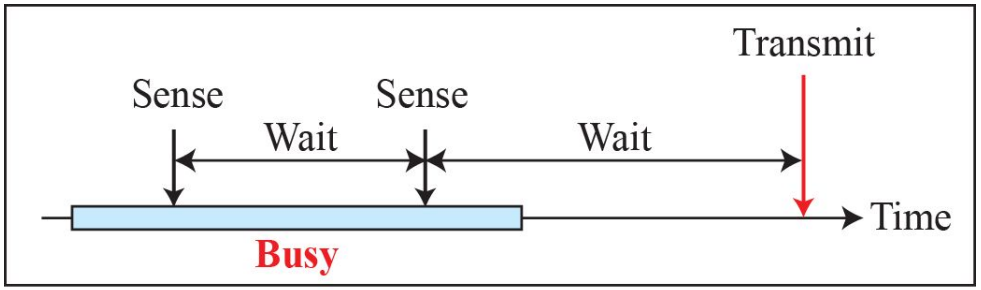


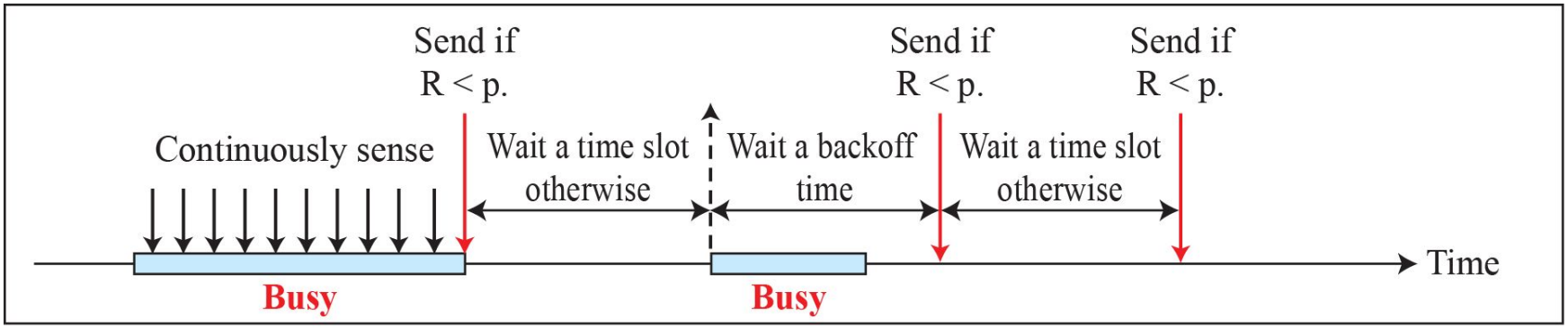
Figure 5.36: Behavior of three persistence methods



a. 1-persistent

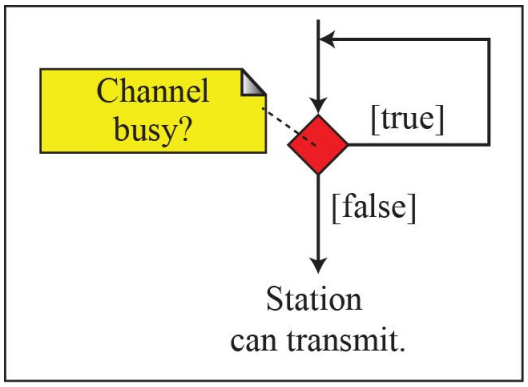


b. Nonpersistent

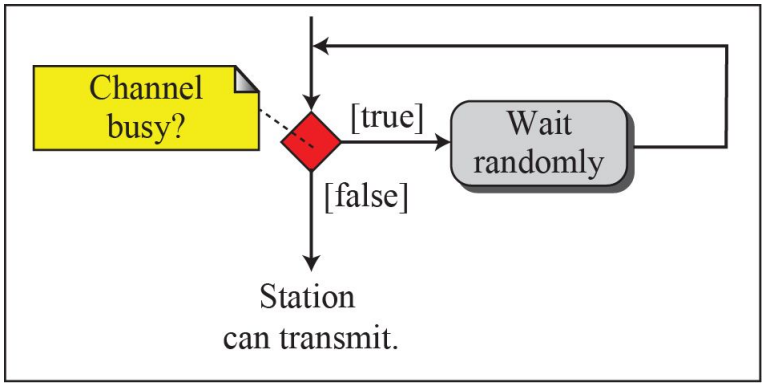


c. *p*-persistent

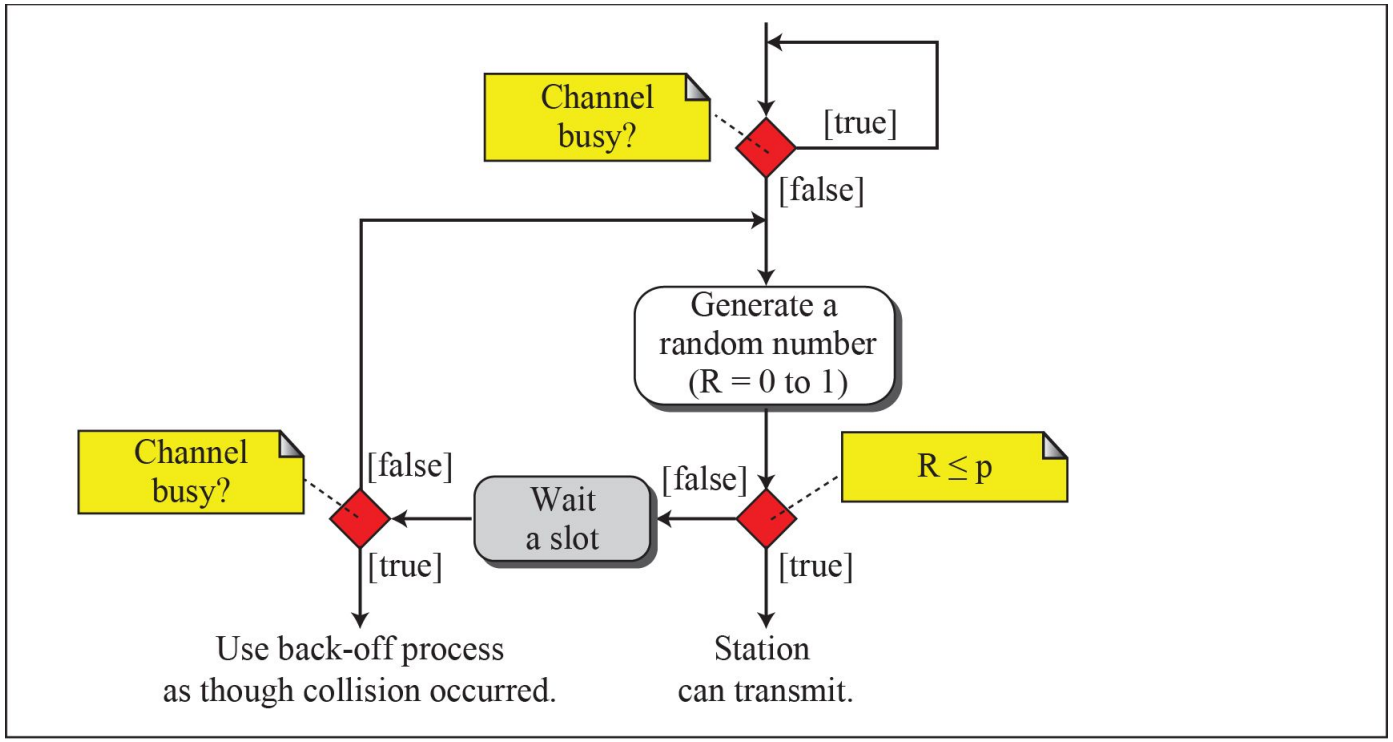
Figure 5.37: Flow diagram for three persistence methods



a. 1-persistent



b. Nonpersistent



c. *p*-persistent

Figure 5.38: Collision of the first bits in CSMA/CD

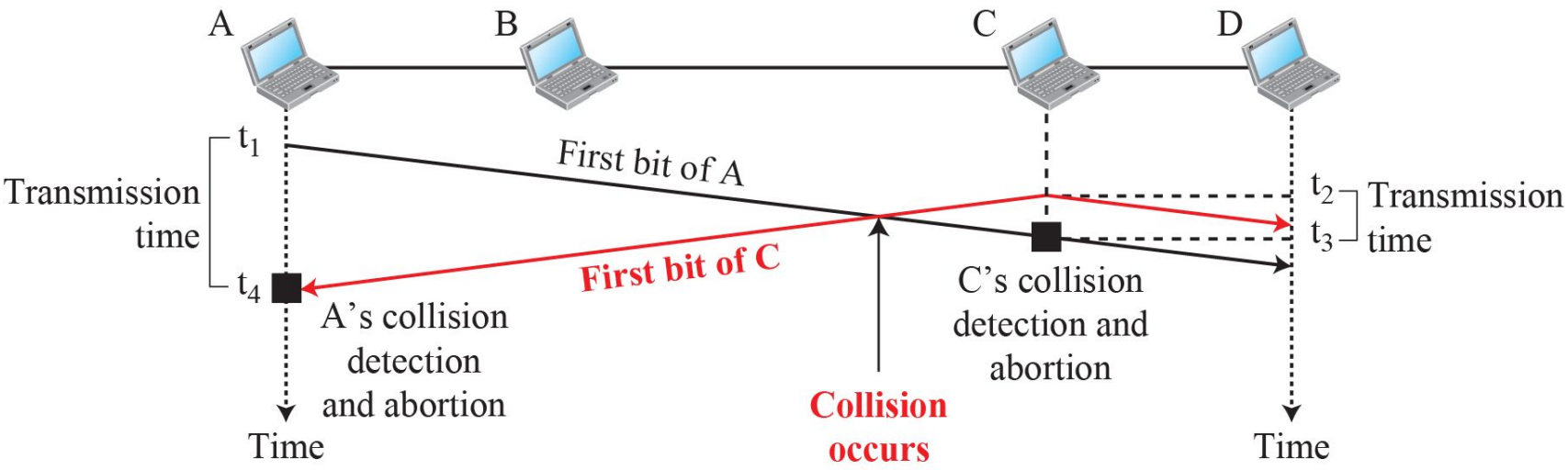
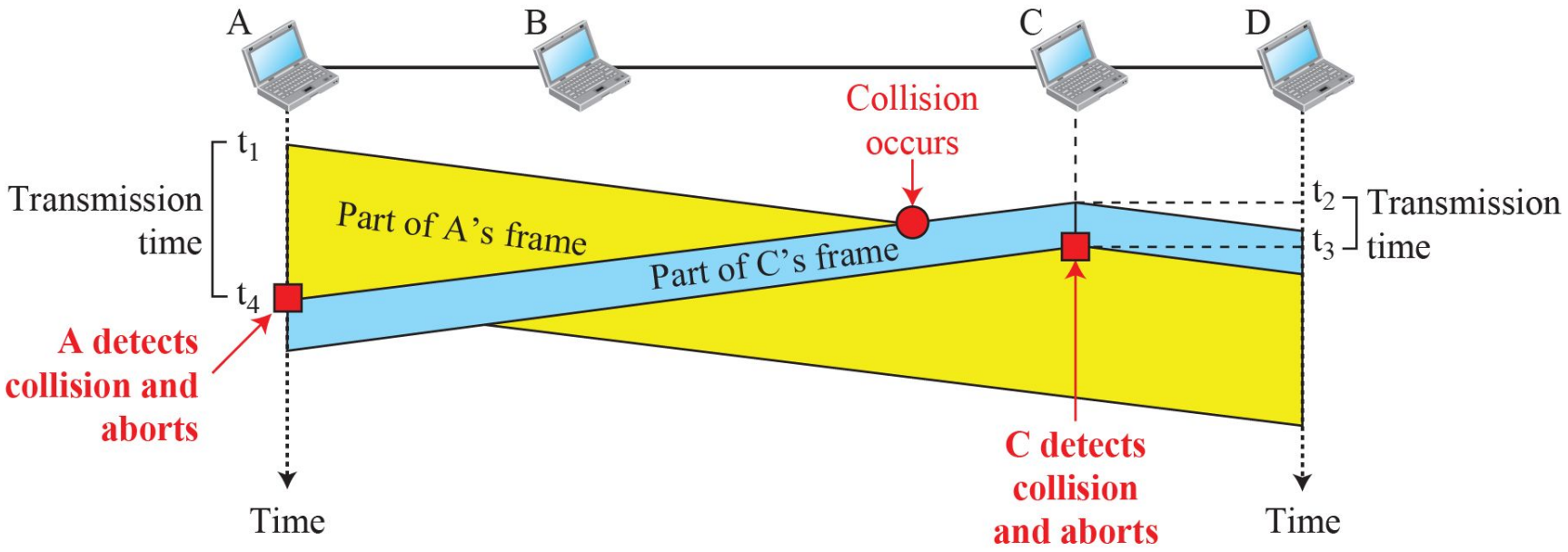


Figure 5.39: Collision and abortion in CSMA/CD



Example 5.15

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 5.40: Flow diagram for the CSMA/CD

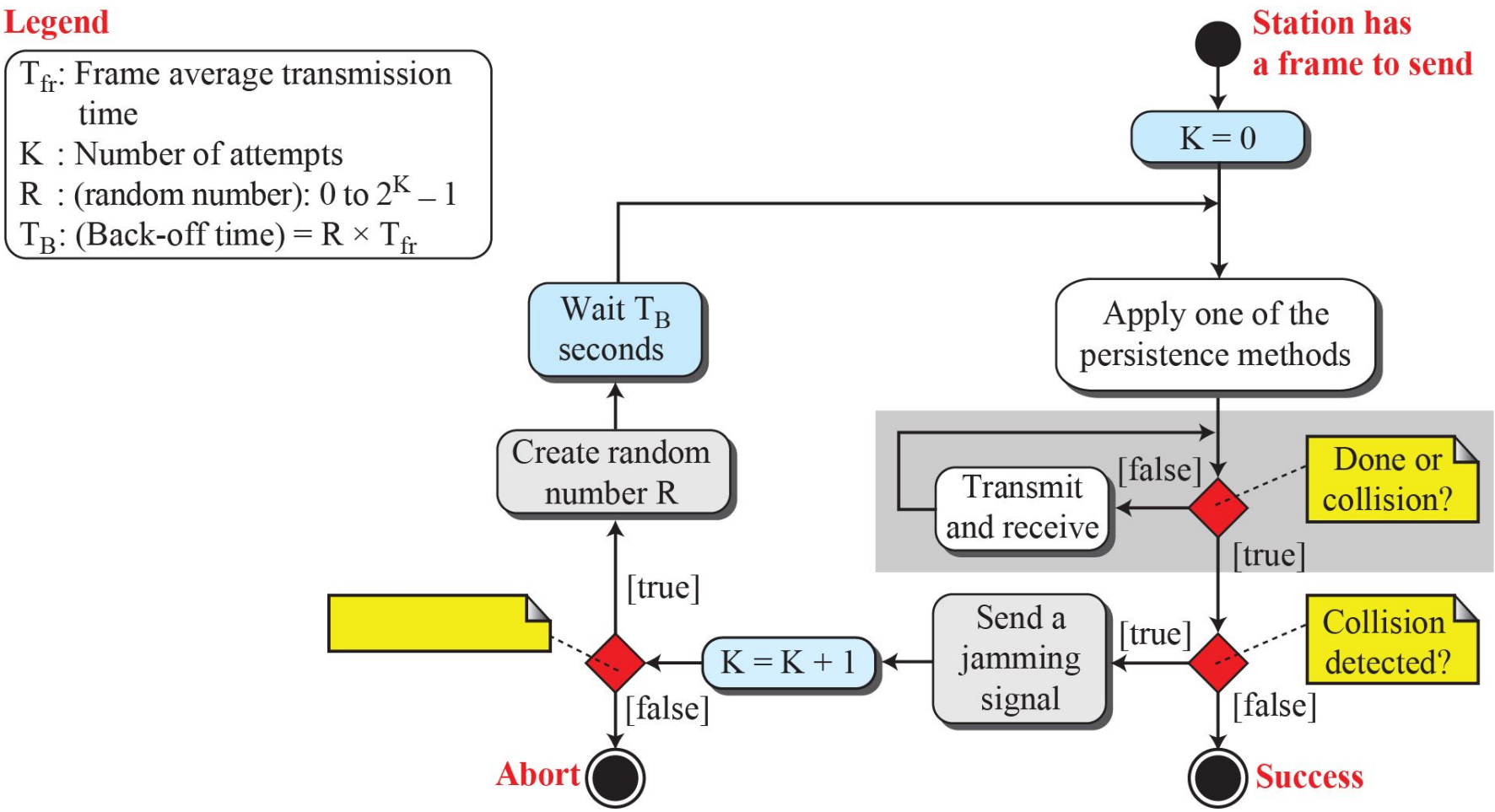
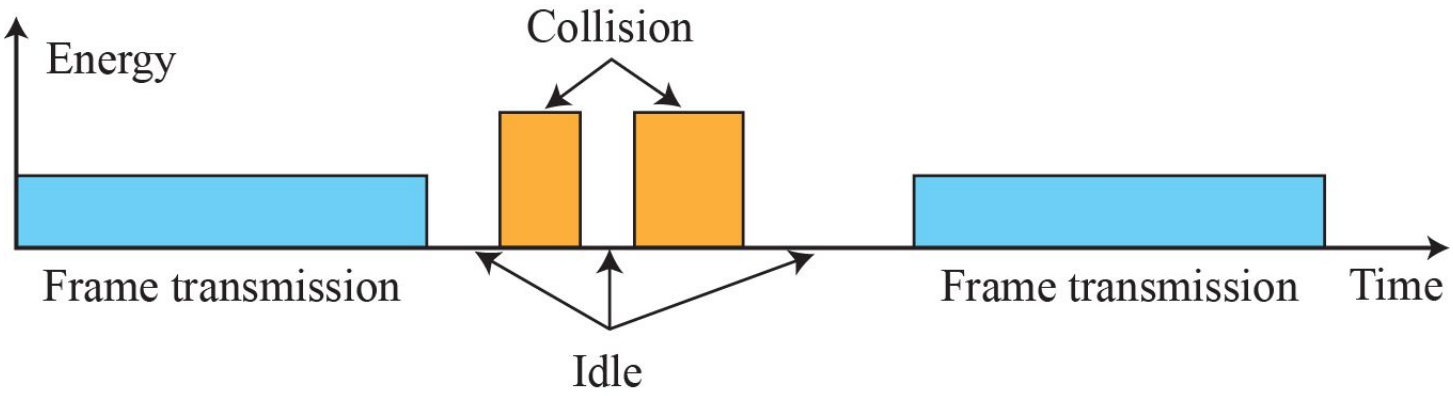


Figure 5.41: Energy level during transmission, idleness, or collision



5.3.2 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.

5.3.2 (continued)

- *Reservation*
- *Polling*
  - *Select*
  - *Poll*
- *Token Passing*
  - *Logical Ring*

Figure 5.42: Reservation access method

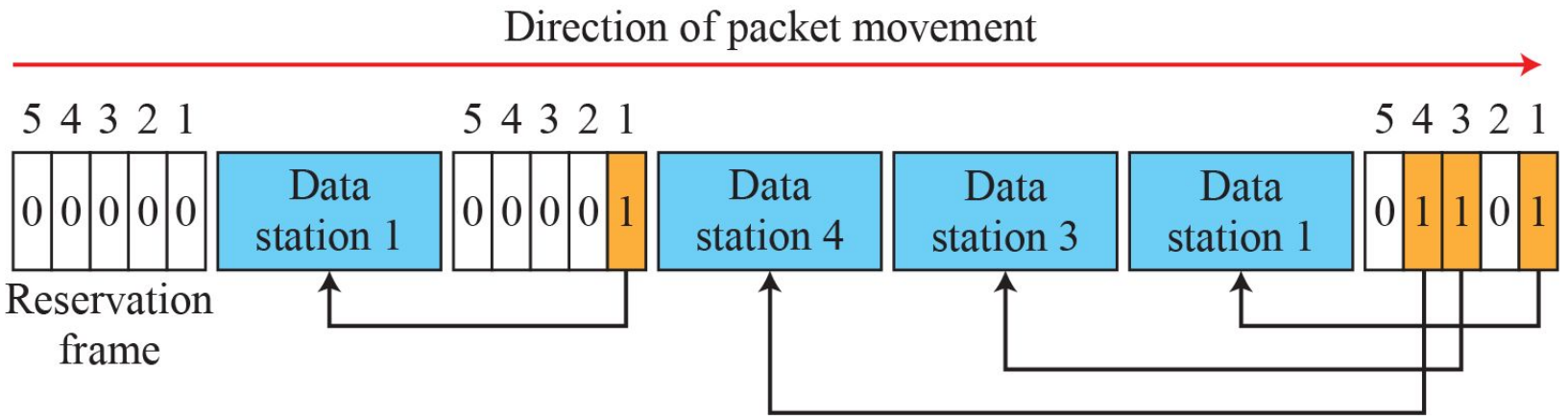


Figure 5.43: ***Select and poll functions in polling-access method***

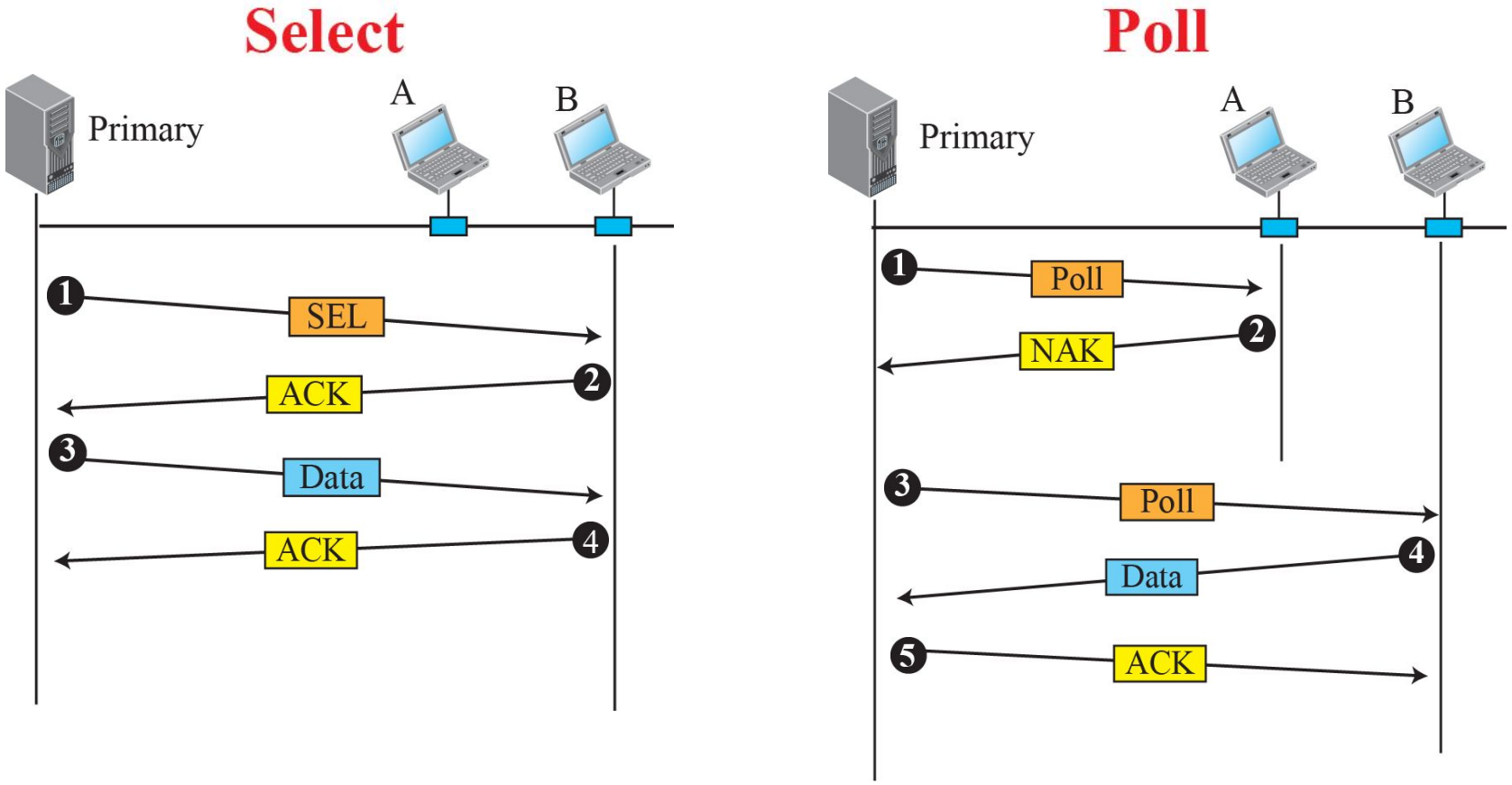
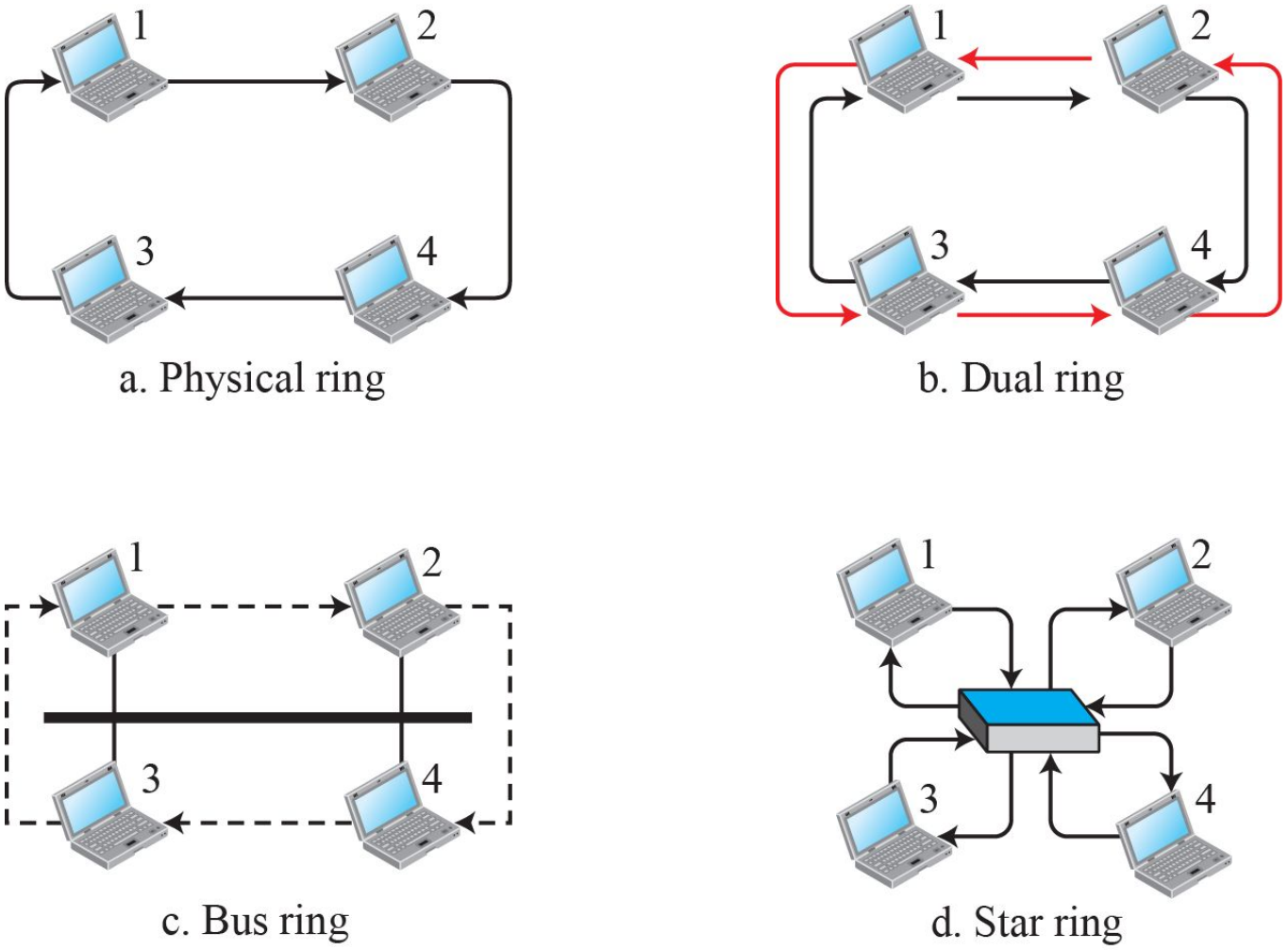


Figure 5.44: *Logical ring and physical topology in token-passing access method*



5.3.3 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 these methods are normally used in wireless networks, we postpone their discussion until the next chapter.

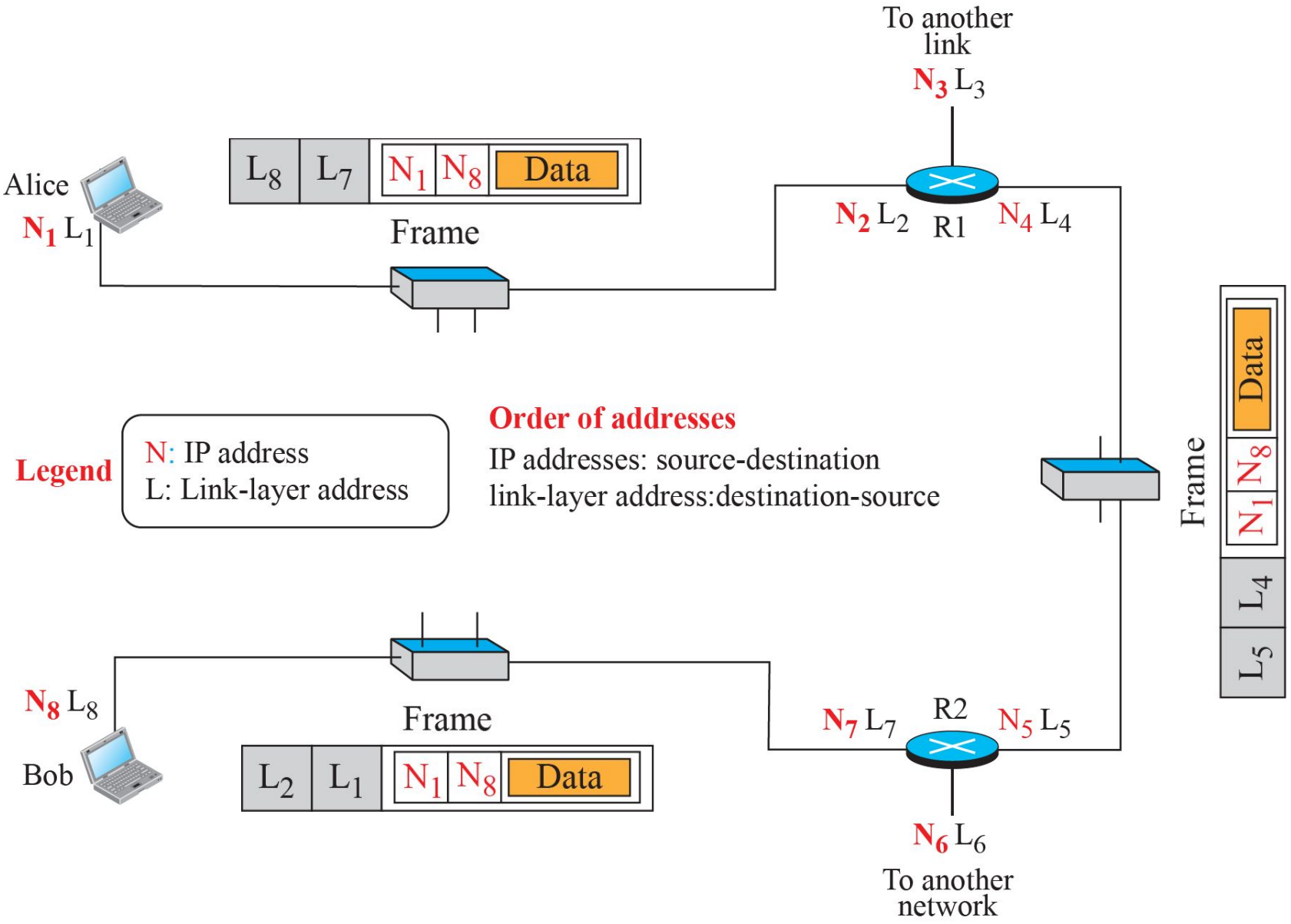
5-4 LINK-LAYER ADDRESSING

In Chapter 4, we discussed IP addresses as the identifiers at the network layer that define the exact points in the Internet where the source and destination hosts are connected. However, in a connectionless internetwork such as the Internet we cannot make a datagram reach its destination using only IP addresses.

5-4 Continued

- *Address Resolution Protocol (ARP)*
  - *Packet Format*
- *An Example*
  - *Activities at the Alice Site*
  - *Activities at Routers*
  - *Activities at Bob's Site*

Figure 5.45: IP addresses and link-layer addresses in a small internet



Example 5.16

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

Figure 5.46: Position of ARP in TCP/IP protocol suite

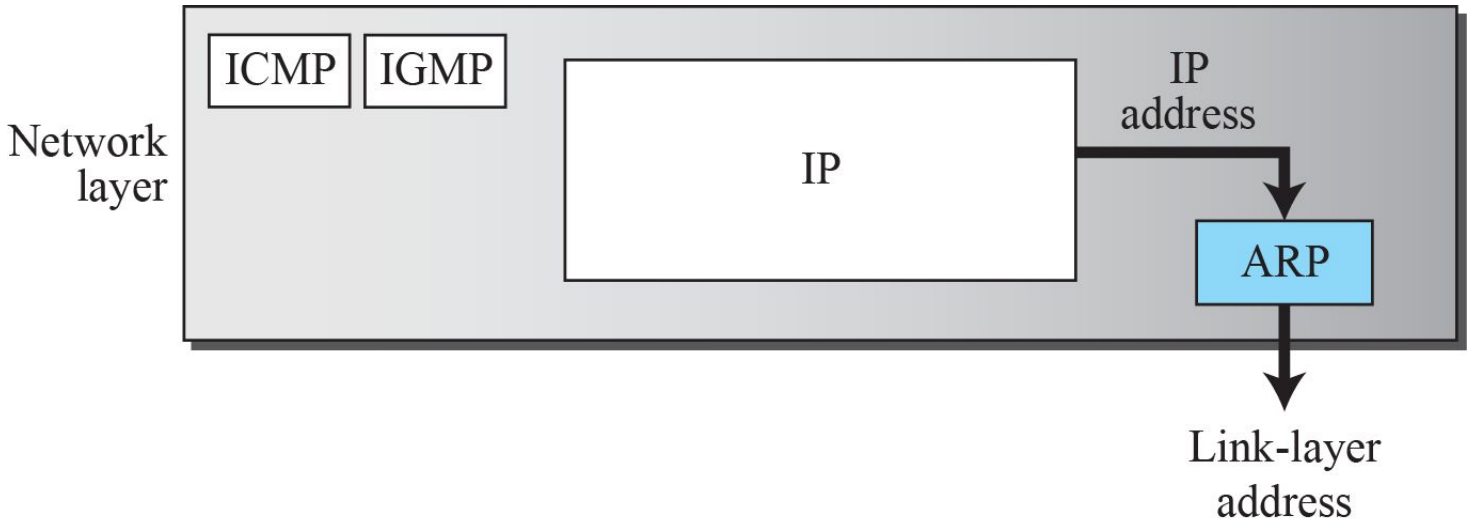
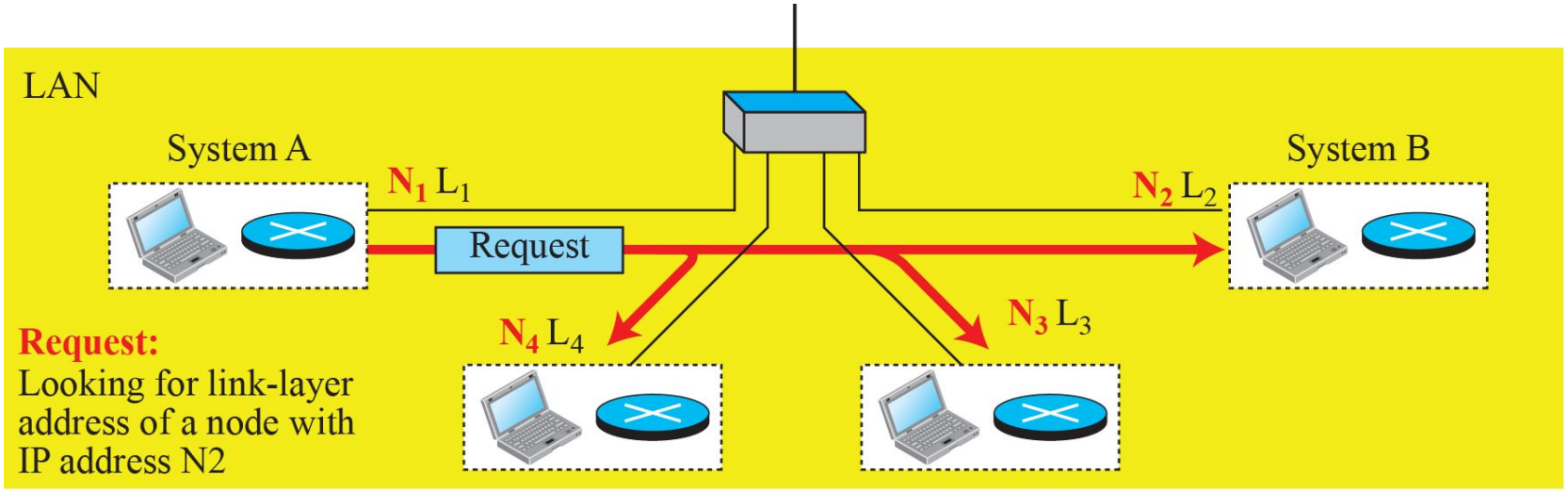
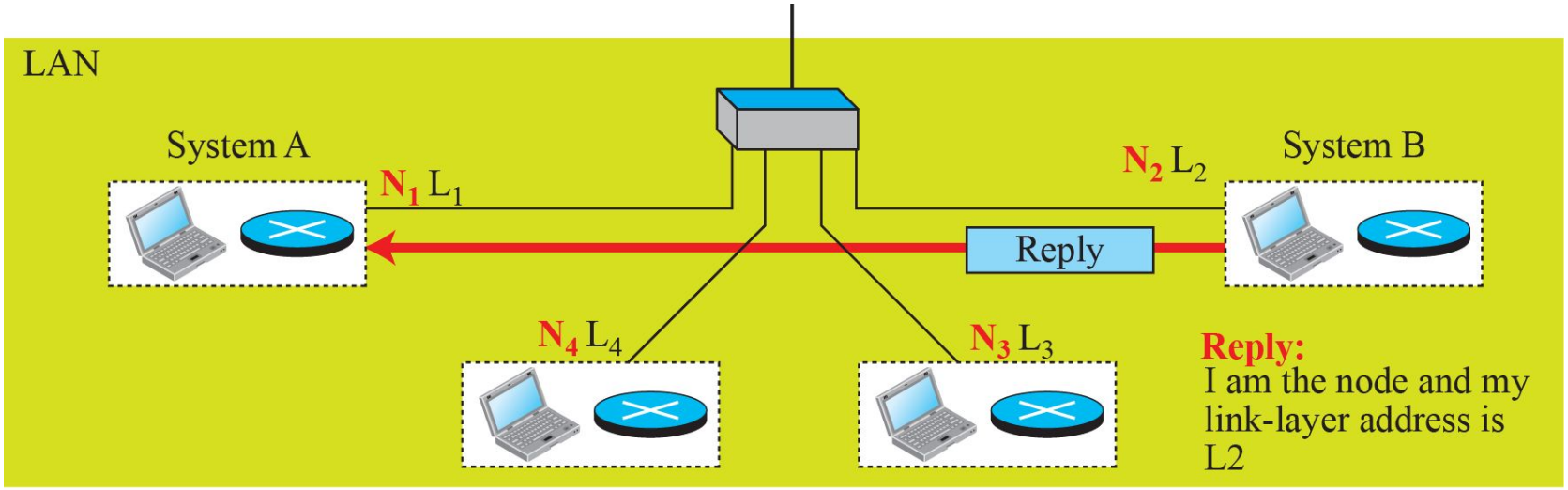


Figure 5.47: ARP operation

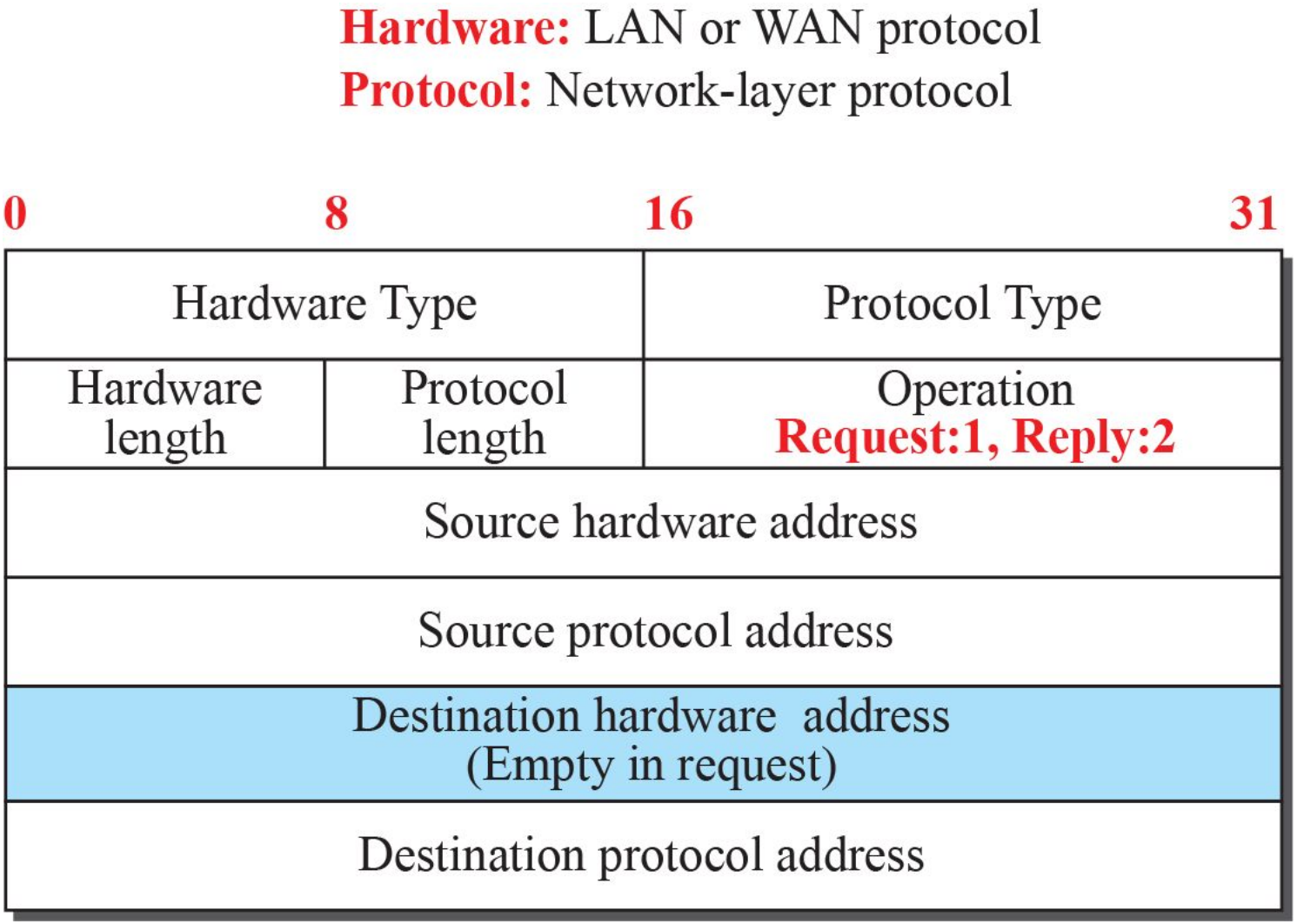


a. ARP request is broadcast



b. ARP reply is unicast

Figure 5.48: ARP packet



Example 5.17

A host with IP address N1 and MAC address L1 has a packet to send to another host with IP address N2 and physical address L2 (which is unknown to the first host). The two hosts are on the same network. Show the ARP request and reply packets encapsulated in Ethernet frames (see Figure 5.55).

Solution

Figure 5.49 shows the ARP request and reply packets. Note that the ARP data field in this case is 28 bytes, and that the individual addresses do not fit in the 4-byte boundary. That is why we do not show the regular 4-byte boundaries for these addresses. Also note that the IP addresses are shown in hexadecimal.

Figure 5.49: Example 5.17

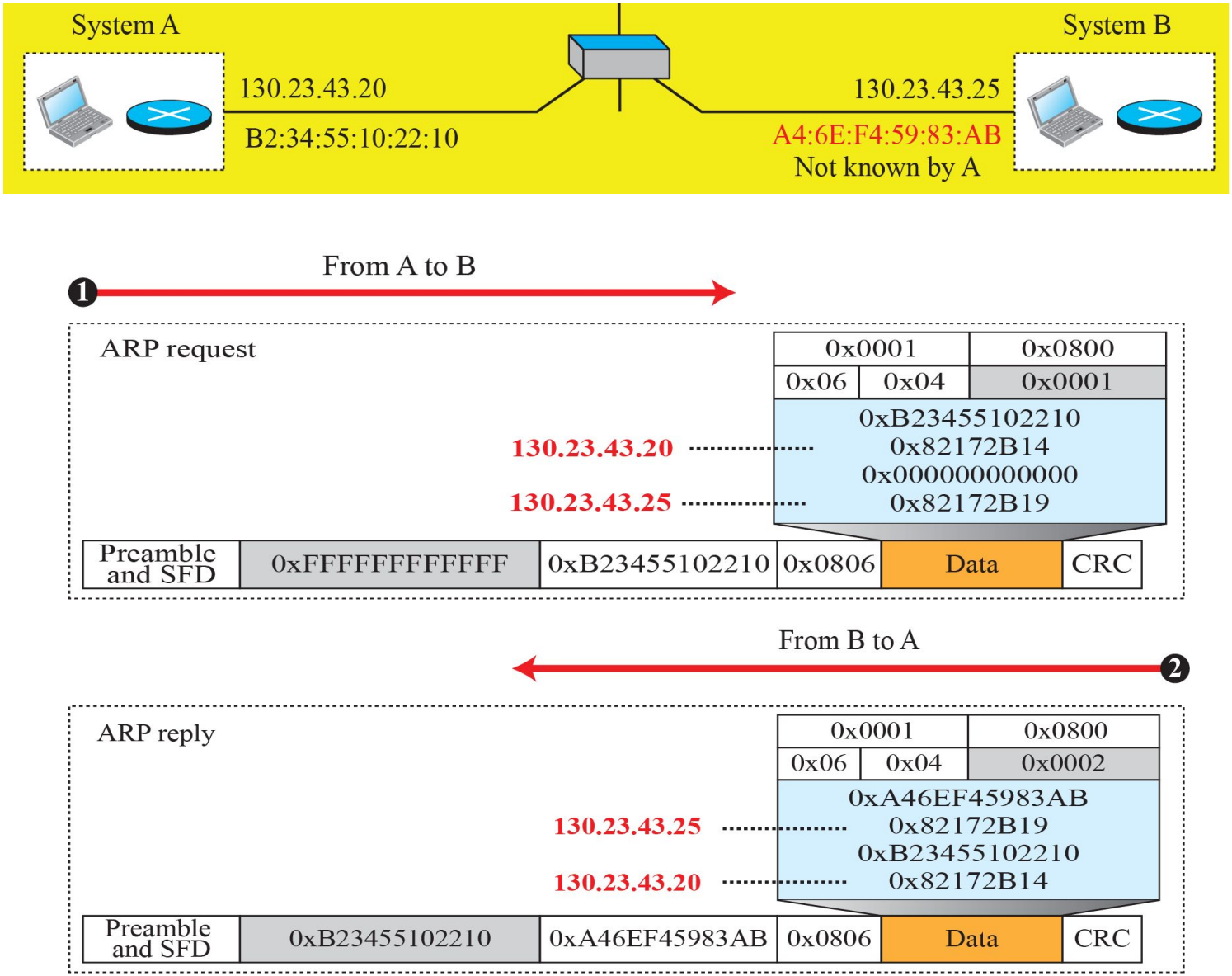


Figure 5.50: The internet for our example

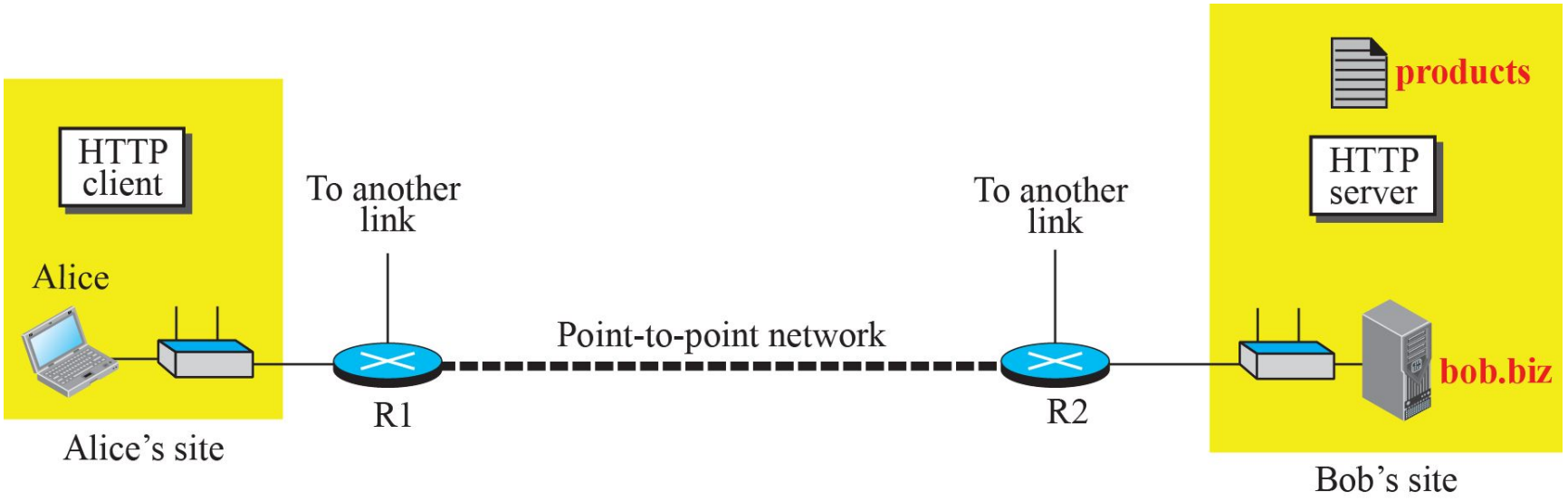
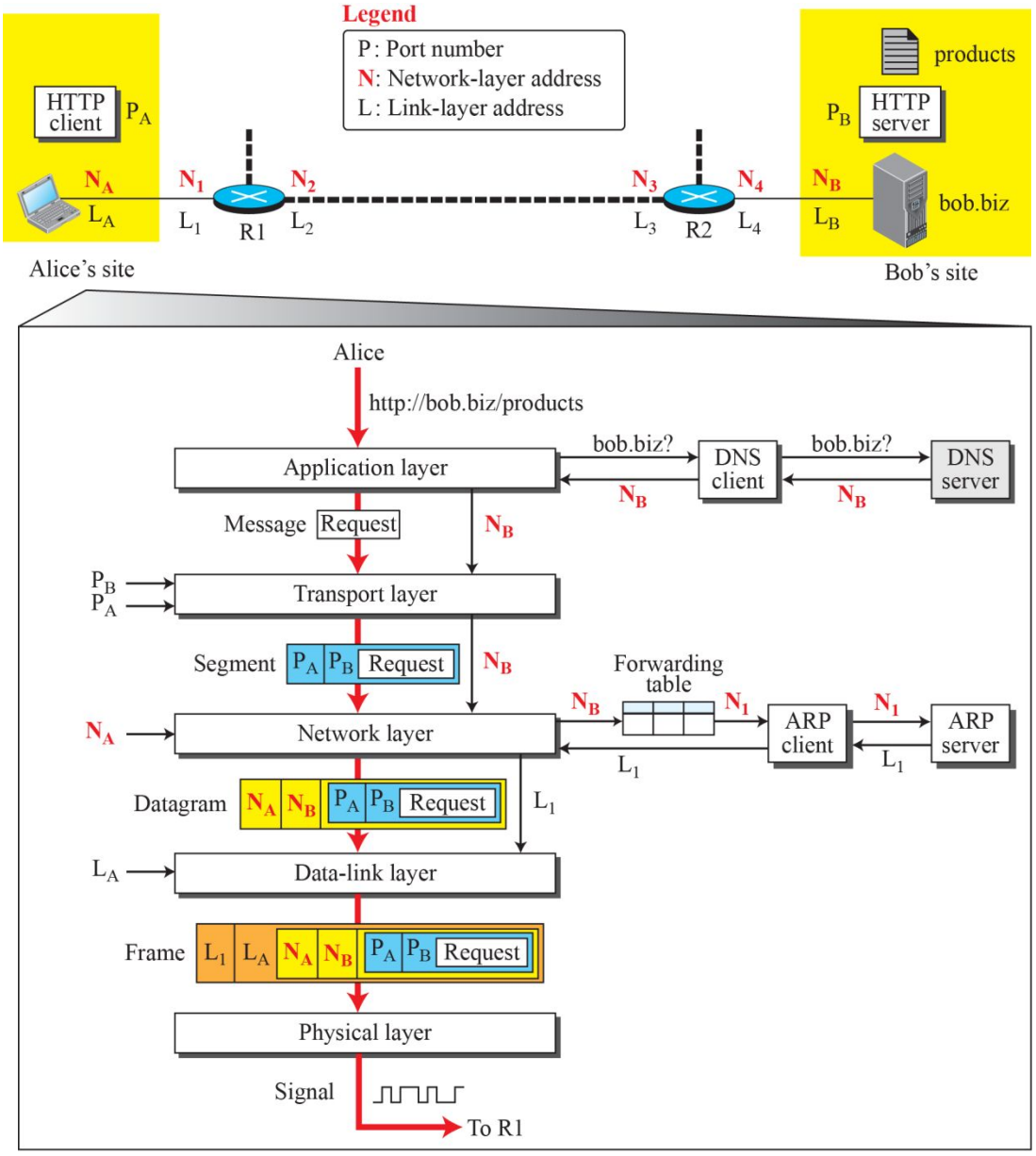
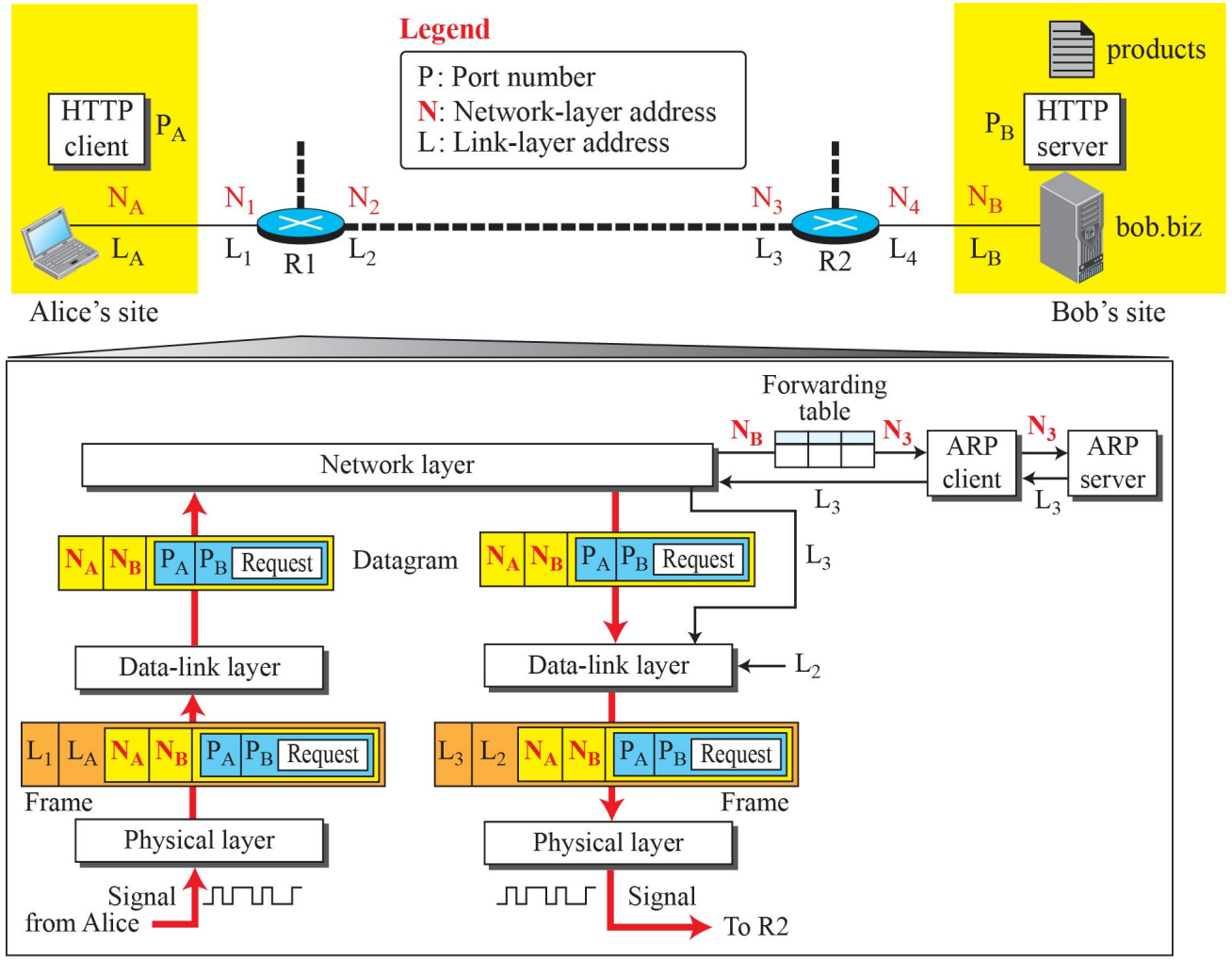


Figure 5.51: Flow of packets at Alice's computer



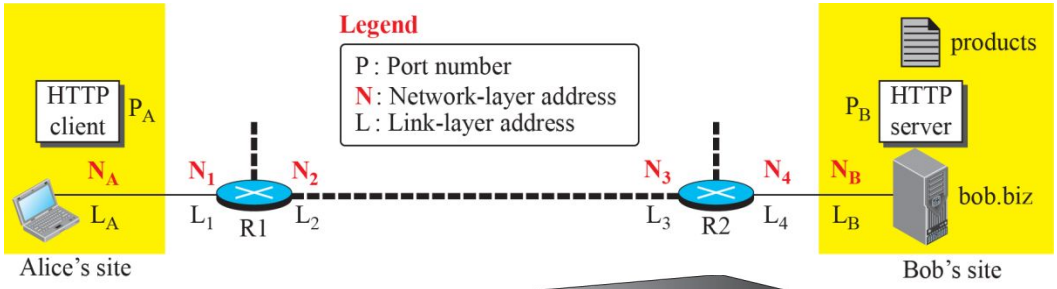
Flow of packets at Alice's computer

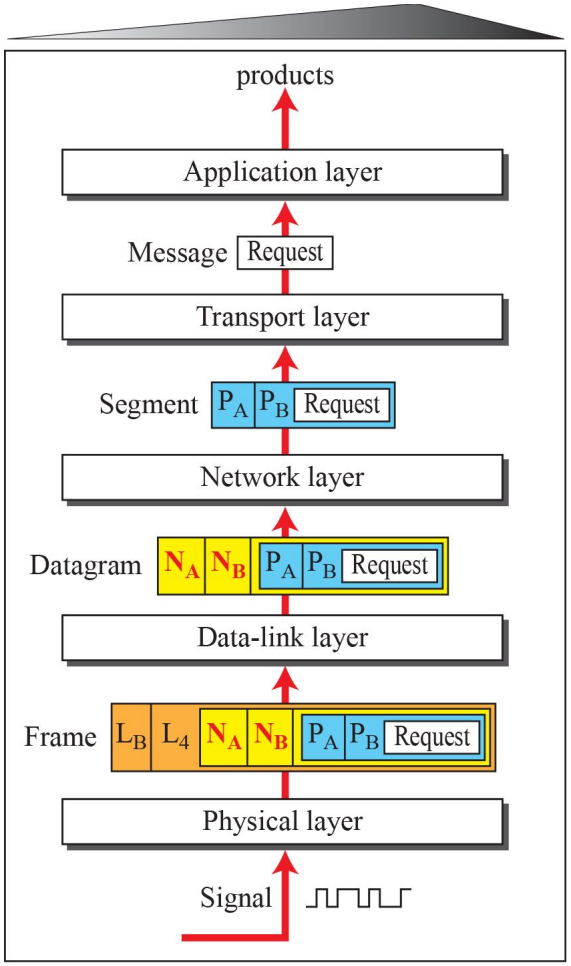
Figure 5.52: Flow of activities at router R1



Flow of packets at Router R1

Figure 5.53: Activities at Bob's site





Flow of packets at Bob's computer

5-5 WIRED LANS: ETHERNET PROTOCOL

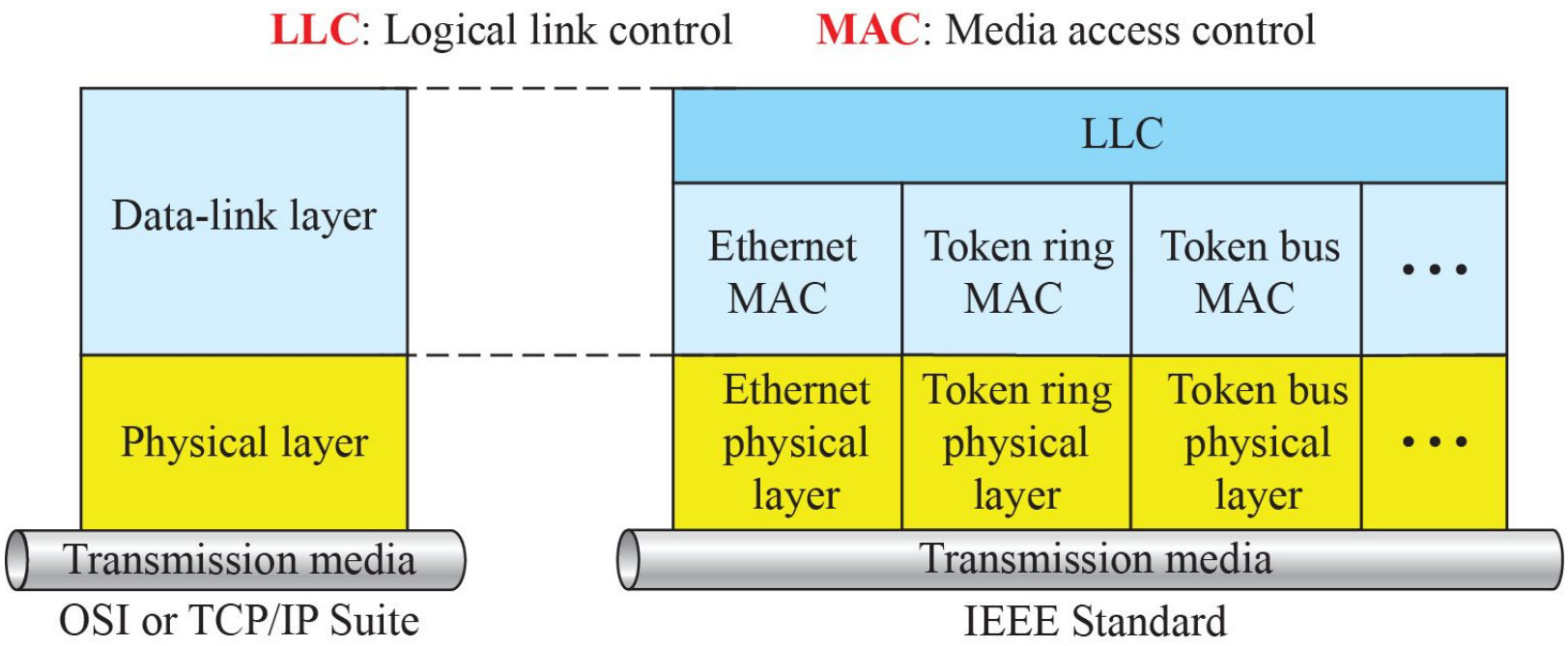
TCP/IP accepts any protocol at the data-link and physical layers. These two layers are actually the territory of the local and wide area networks. This means that when we discuss these two layers, we are talking about networks that are using them. We can have wired or wireless networks. We discuss wired networks in this chapter and wireless networks in the next chapter.

5.5.1 IEEE Project 802

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.

- *Logical Link Control (LLC)*
- *Media Access Control (MAC)*

Figure 5.54: IEEE standard for LANs



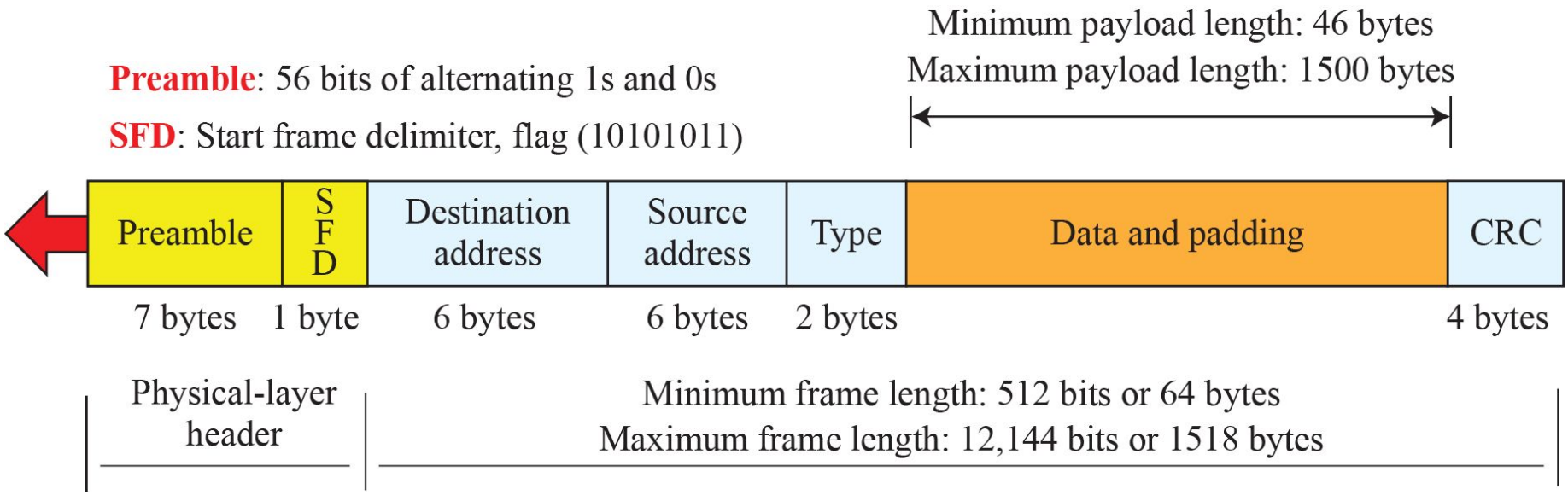
5.5.2 Standard Ethernet

We refer to the original Ethernet technology with he data rate of 10 Mbps as the Standard Ethernet. Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution. We discuss this standard version to pave the way for understanding the other three technologies.

5.5.2 (continued)

- *Frame Format*
- *Connectionless and Unreliable Service*
- *Frame Length*
- *Addressing*
  - *Transmission of Address Bits*
  - *Unicast, Multicast, and Broadcast Addresses*
  - *Distinguish between Unicast, Multicast, and Broadcast Transmission*
- *Access Method*
- *Efficiency of Standard Ethernet*
- *Implementation*

Figure 5.55: Ethernet frame



Example 5.18

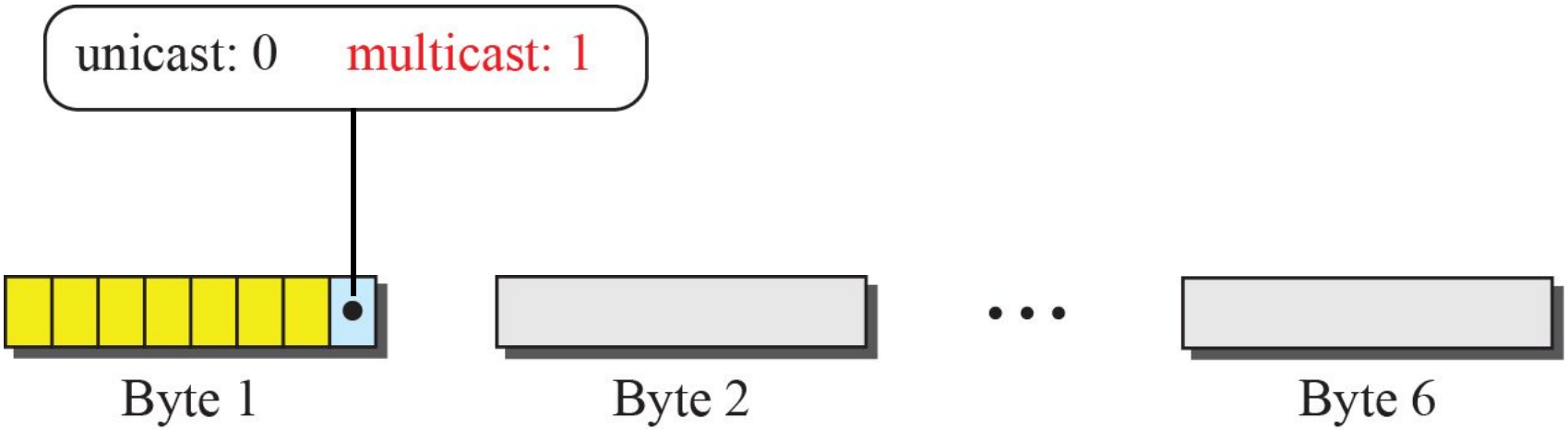
Show how the address 47:20:1B:2E:08:EE is sent out online.

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:

Hexadecimal	47	20	1B	2E	08	EE
Binarys	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Figure 5.56: Unicast and multicast addresses



Example 5.19

Define the type of the following destination addresses:

. 4A:30:10:21:10:1A

. 47:20:1B:2E:08:EE

. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are Fs, the address is broadcast. Therefore, we have the following:

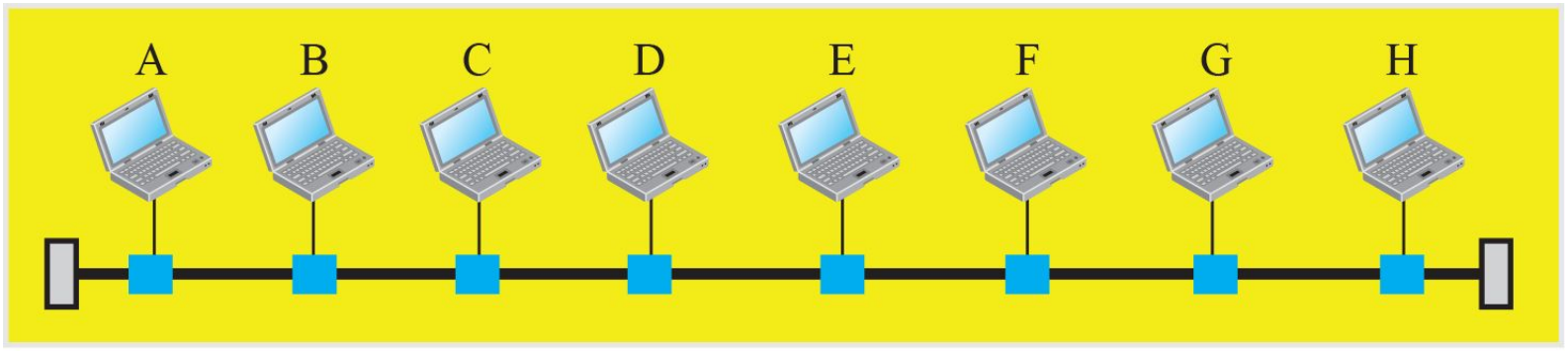
Example 5.19 (continued)

a. This is a unicast address because A in binary is 1010 (even).

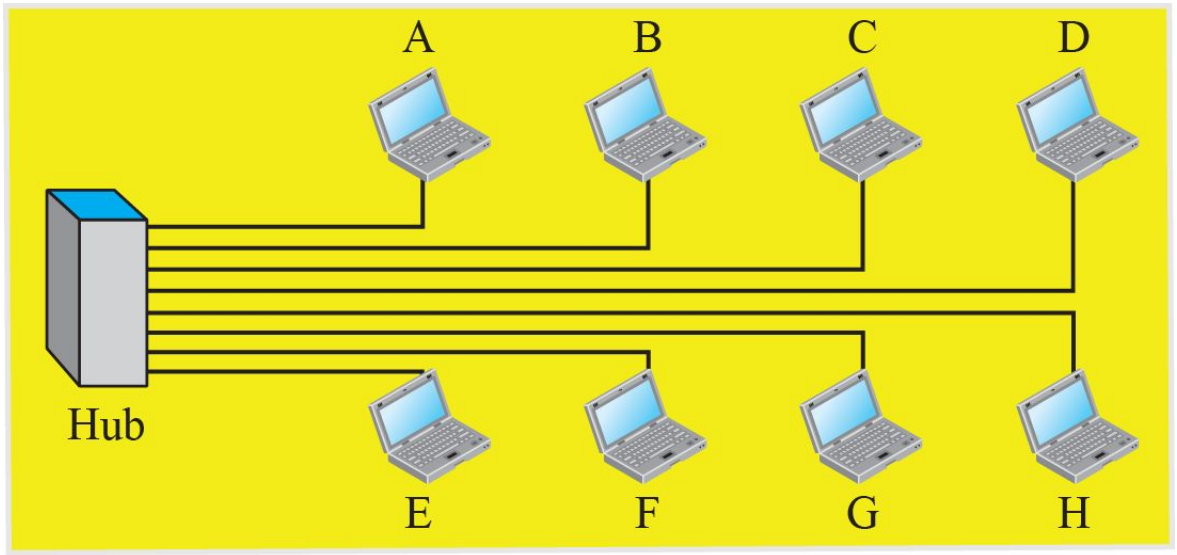
b. This is a multicast address because 7 in binary is 0111 (odd).

c. This is a broadcast address because all digits are Fs in hexadecimal.

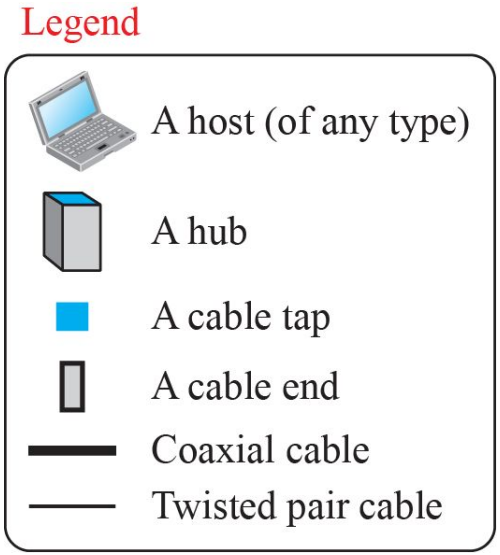
Figure 5.57: Implementation of standard Ethernet



a. A LAN with a bus topology using a coaxial cable



b. A LAN with a star topology using a hub



Example 5.20

In the Standard Ethernet with the transmission rate of 10 Mbps, we assume that the length of the medium is 2500 m and the size of the frame is 512 bits. The propagation speed of a signal in a cable is normally 2×10^8 m/s.

Propagation delay $= 2500/(2 \times 10^8) = 12.5$ µs	Transmission delay $= 512/(10^7) = 51.2$ µs
$a = 12.5/51.2 = 0.24$	Efficiency = 39%

The example shows that a = 0.24, which means only 0.24 of a frame occupies the whole medium in this case. The efficiency is 39 percent, which is considered moderate; it means that only 61 percent of the time the medium is occupied but not used by a station.

Table 5.6: Summary of Standard Ethernet implementations

Implementation	*Medium*	*Medium Length*	*Encoding*
10Base5	Thick coax	500 m	Manchester
10Base2	Thin coax	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000	Manchester

5.5.3 Fast Ethernet

Fast Ethernet was designed to operate at 100 Mbps. The designers of the Fast Ethernet needed to make it compatible with the Standard Ethernet. The MAC sublayer was left unchanged, which meant the frame format and the maximum and minimum size could also remain unchanged.

- *Access Method*
- *Autonegotiation*
- *Implementation*

Table 5.7: Summary of Fast Ethernet implementations

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	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

5.5.4 Gigabit Ethernet

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet were to upgrade the data rate to 1 Gbps, but keep the address length, the frame format, and the maximum and minimum frame length the same.

- *MAC Sublayer*
- *Implementation*

Table 5.8: 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

5.5.5 10-Gigabit Ethernet

In recent years, there has been another look into the Ethernet for use in metropolitan areas. The idea is to extend the technology, the data rate, and the coverage distance so that the Ethernet can be used as LAN and MAN (metropolitan area network). The IEEE committee created 10-Gigabit Ethernet and called it Standard 802.3ae.

- ***Implementation***

Table 5.9: Summary of 10-Gigabit Ethernet implementations

Implementation	*Medium*	*Medium Length*	*Number of wires*	*Encoding*
10GBase-SR	Fiber 850 nm	300 m	2	64B66B
10GBase-LR	Fiber 1310 nm	10 Km	2	64B66B
10GBase-EW	Fiber 1350 nm	40 Km	2	SONET
10GBase-X4	Fiber 1310 nm	300 m to 10 Km	2	8B10B

5.5.6 Virtual LANs

A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic. What happens if we need a virtual connection between two stations belonging to two different physical LANs? We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring.

5.5.6 (continued)

Membership

- Interface Numbers
- MAC Addresses
- IP Addresses
- Multicast IP Addresses
- Combination

Configuration

- Manual Configuration
- Automatic Configuration
- Semiautomatic Configuration

5.5.6 (continued)

- **Communication between Switches**
  - Table Maintenance
  - Frame Tagging
  - Time-Division Multiplexing (TDM)
- **IEEE Standard**
- **Advantages**
  - Cost and Time Reduction
  - Creating Virtual Work Groups
  - Security

Figure 5.58: A switch connecting three LANs

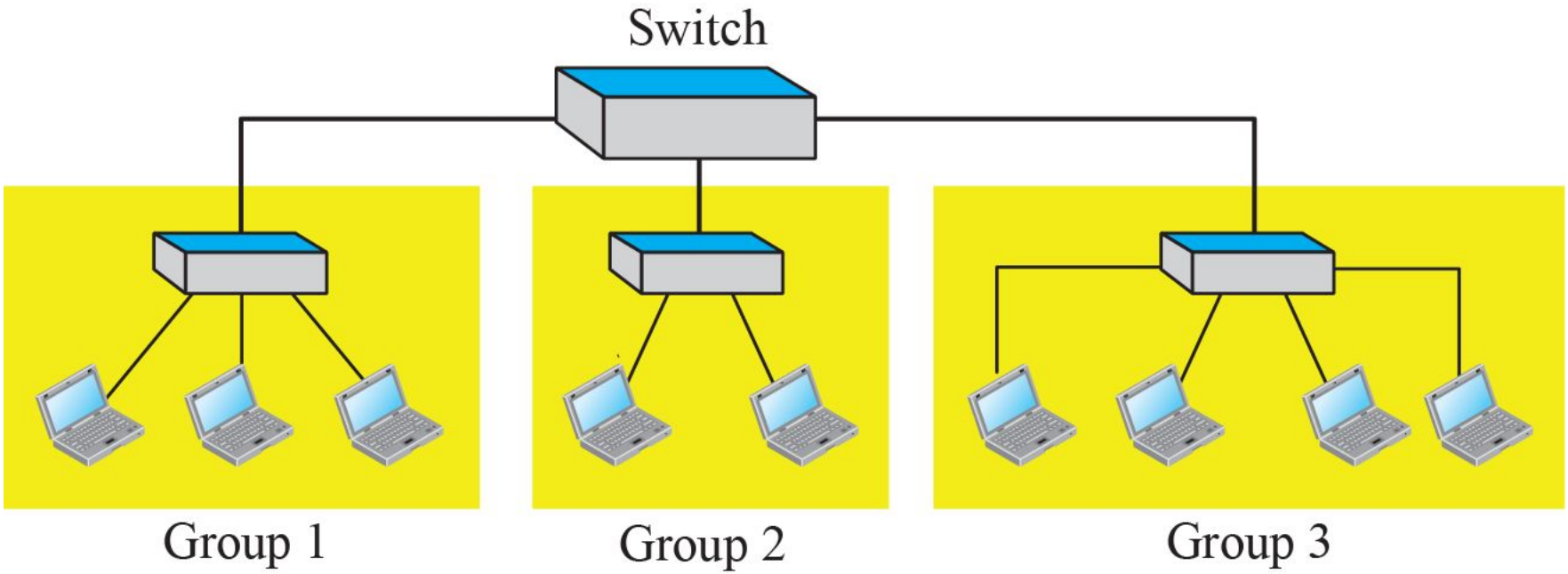


Figure 5.59: A switch using VLAN software

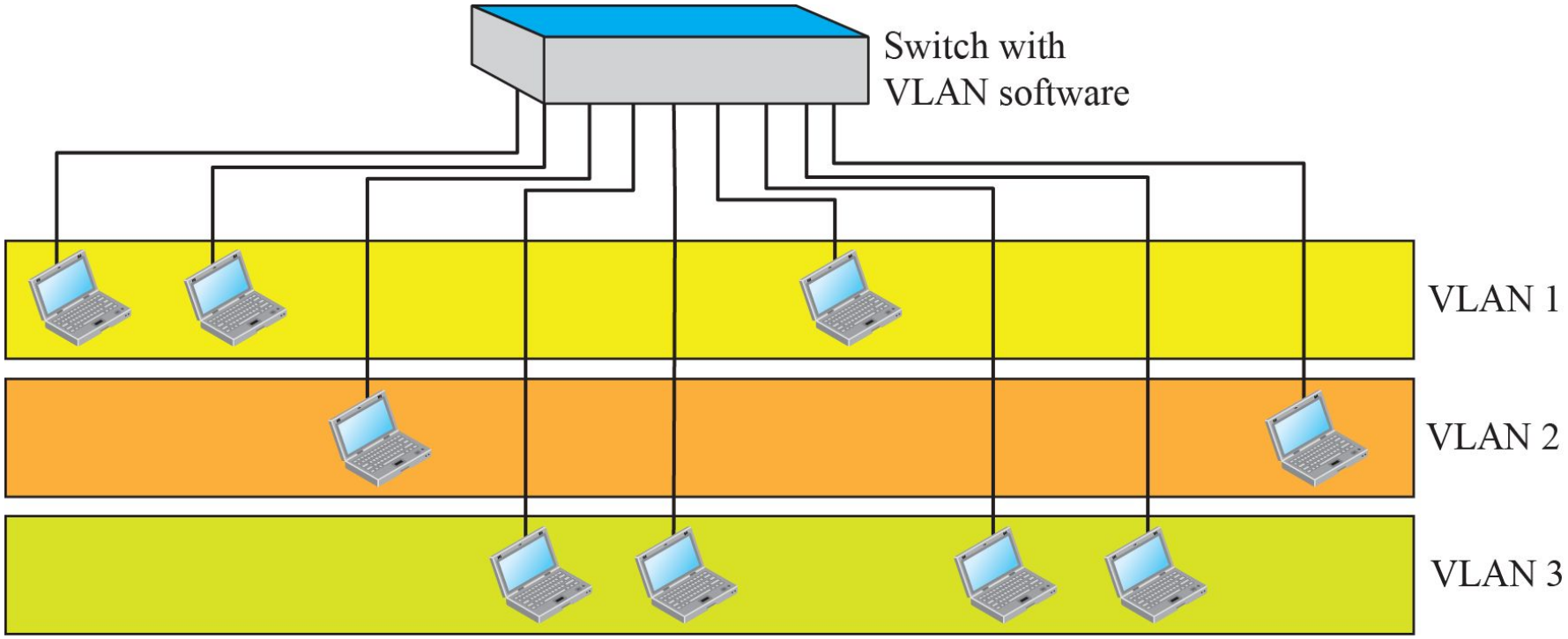
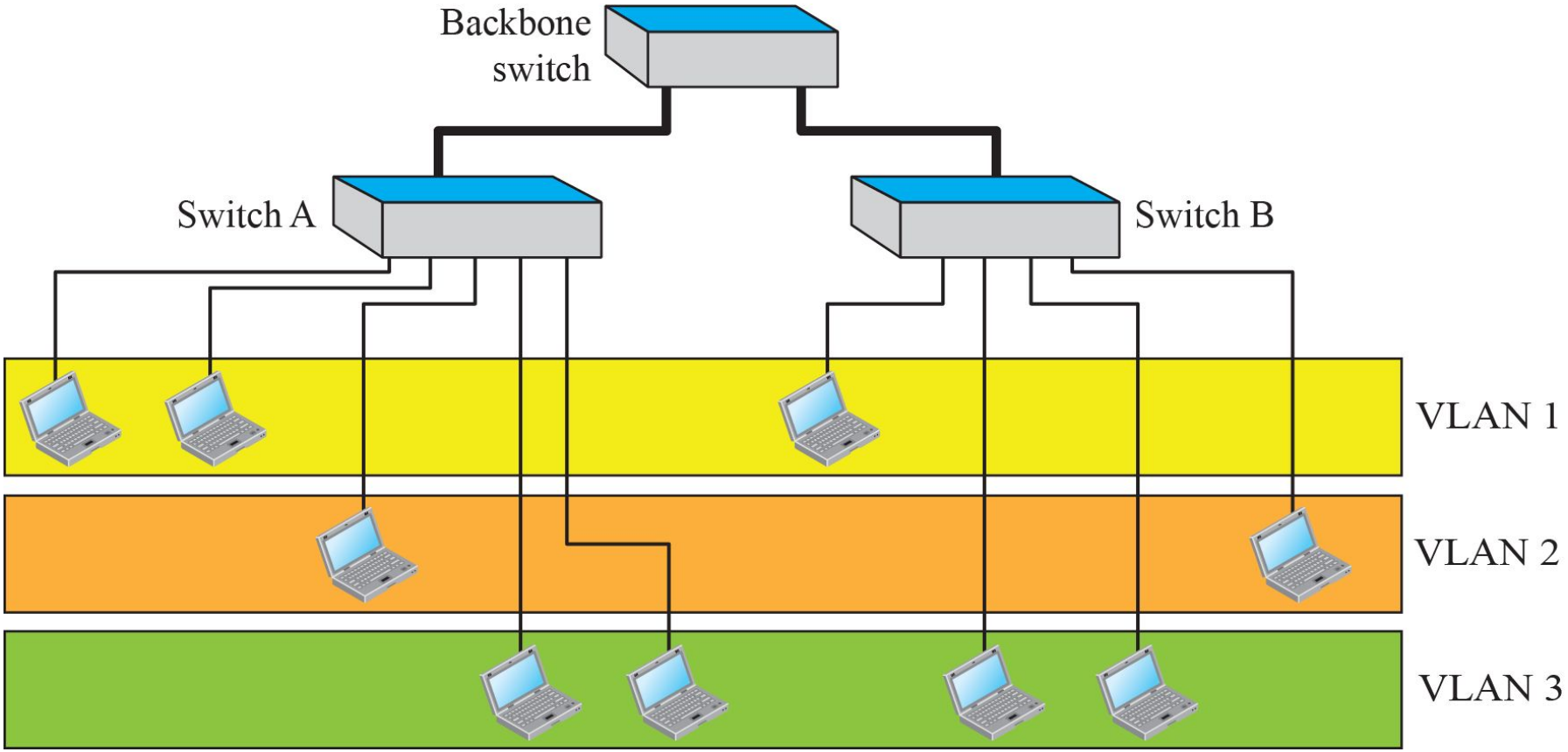


Figure 5.60: Two switches in a backbone using VLAN software



5-6 OTHER WIRED NETWORKS

As we discussed in Chapter 1, the networks that we encounter in the Internet are either LANs or WANs. However, sometimes the terminology is under dispute. For example, some access networks such as dial-up connection or cable connection are called WANs by some people and MANs by others.

5.6.1 Point-to-Point Networks

Some point-to-point networks, such as dial-up, DSL, and cable are used to provide internet access from Internet user premises. Since these networks use a dedicated connection between the two devices, they do not use media access control (MAC). The only protocol that is needed is PPP, as we discussed before.

5.6.1 (continued)

- *Dial-up*
- *Digital Subscriber Line (DSL)*
  - *Using Existing Local Loops*
- *Cable*
  - *Traditional Cable Networks*
  - *Hybrid Fiber-Coaxial (HFC) Network*
  - *Cable TV for Data Transfer*
  - *Sharing*
  - *CM and CMTS*

Figure 5.61: Dial-up network to provide Internet access

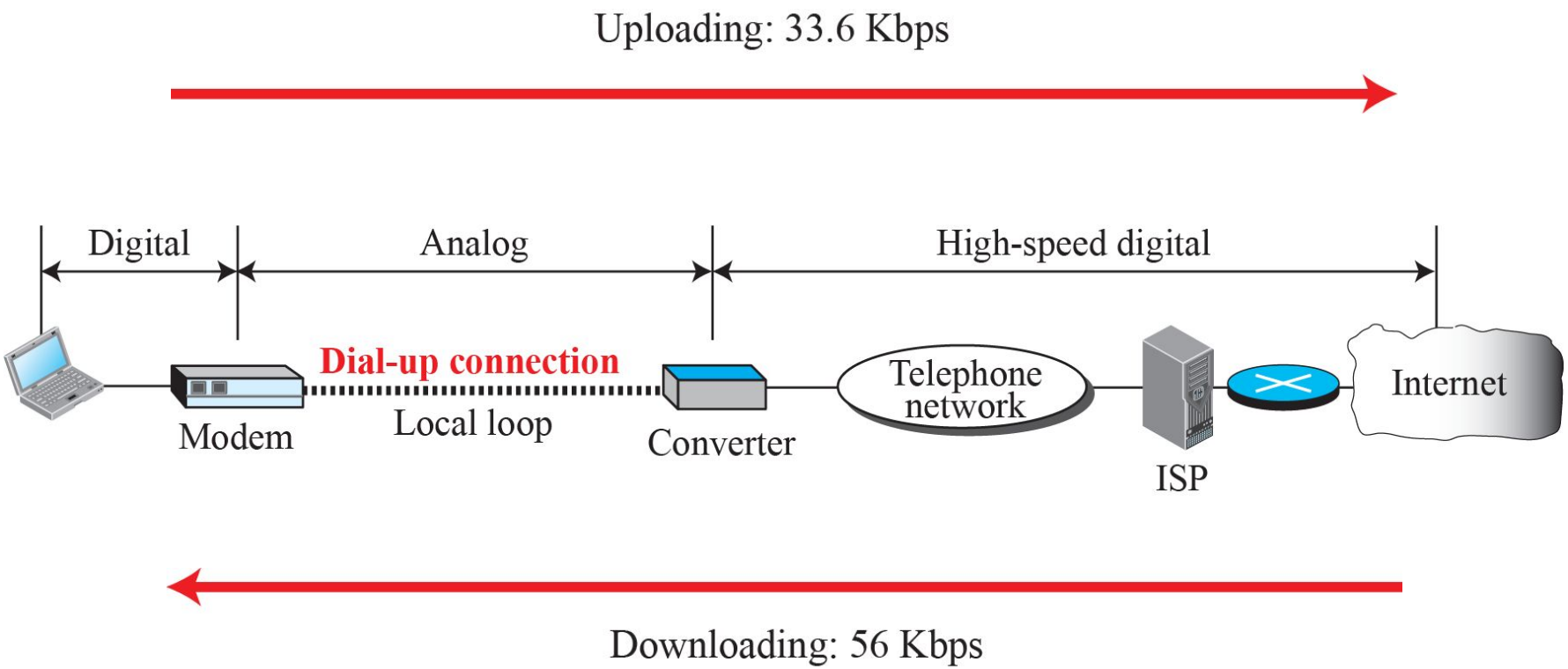


Figure 5.62: ASDL point-to-point network

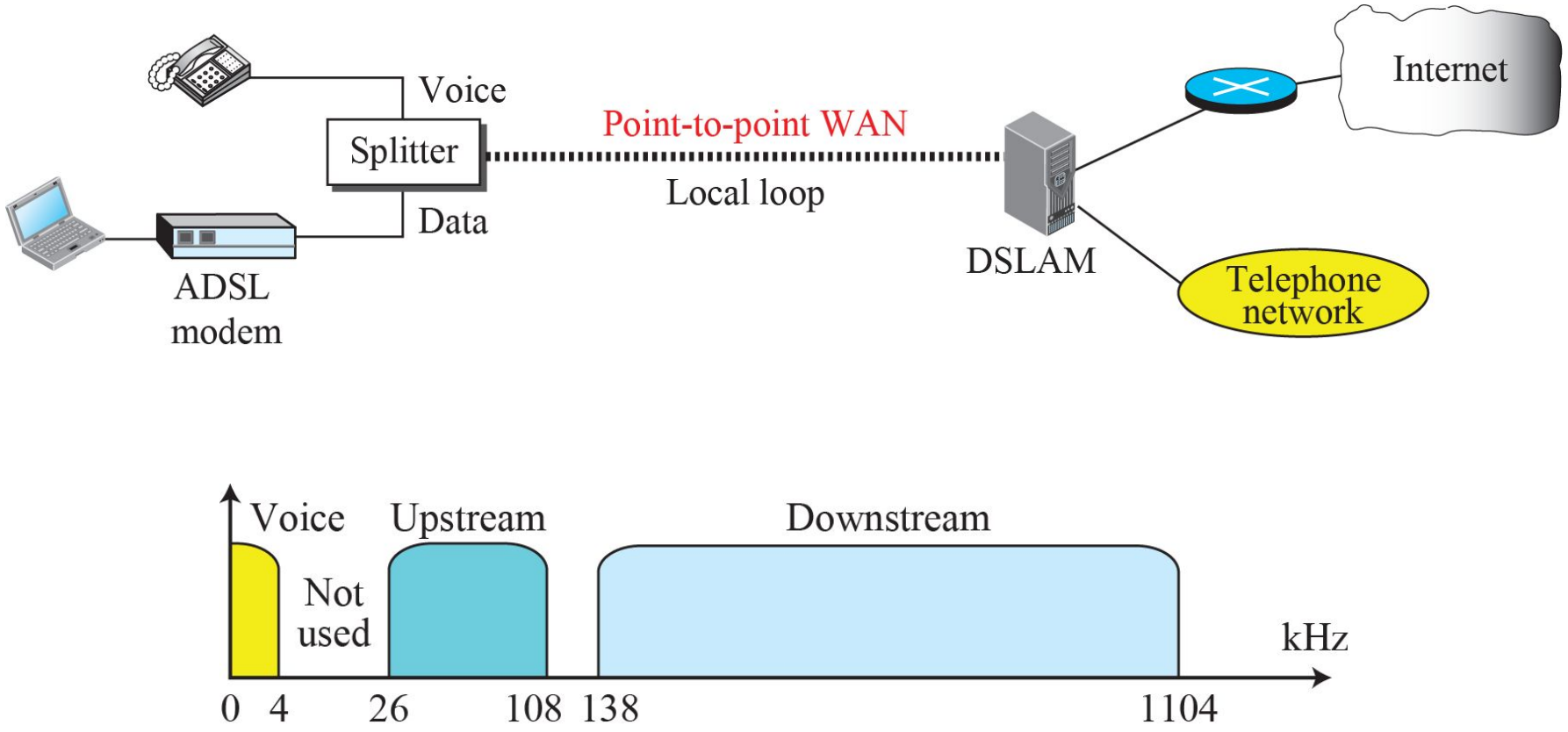


Figure 5.63: Traditional cable TV network

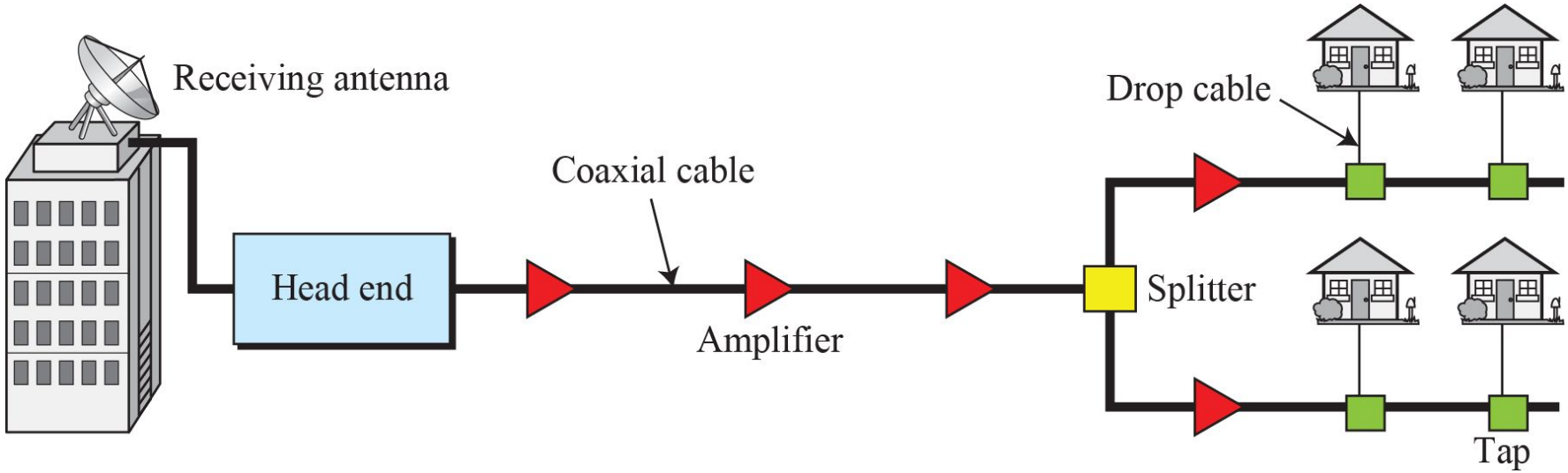


Figure 5.64: Hybrid Fiber-Coaxial (HFC) Network

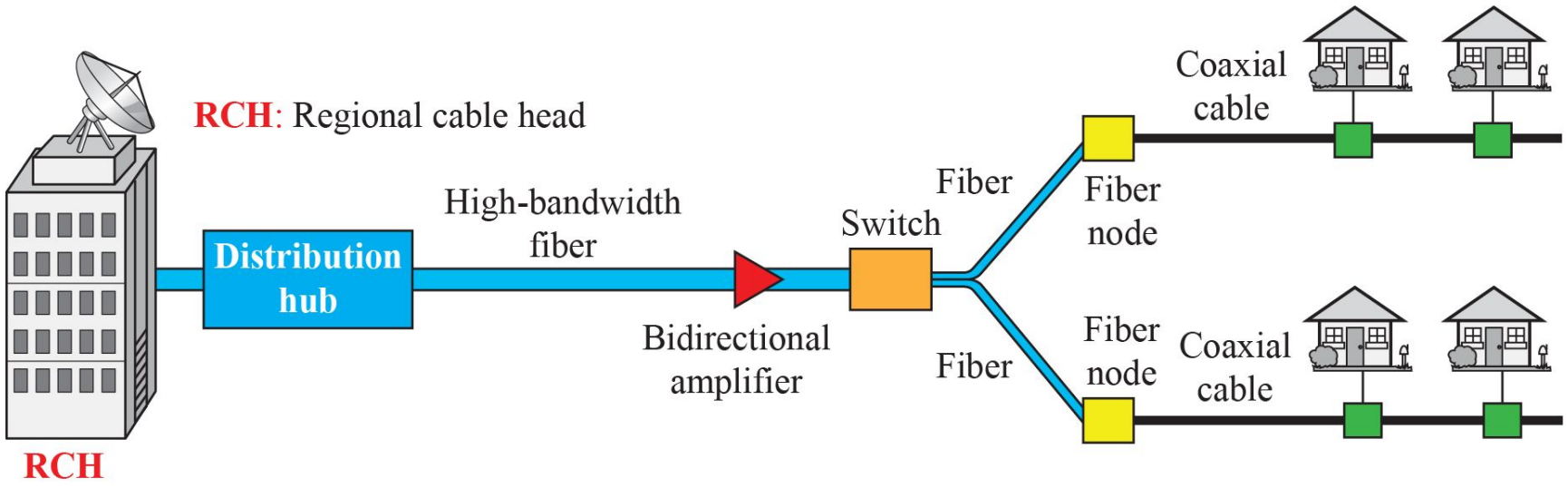


Figure 5.65: Division of coaxial cable band by CATV

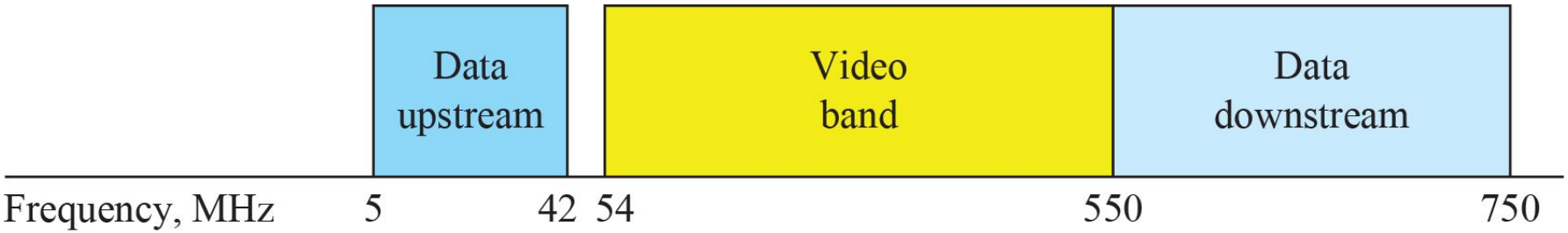
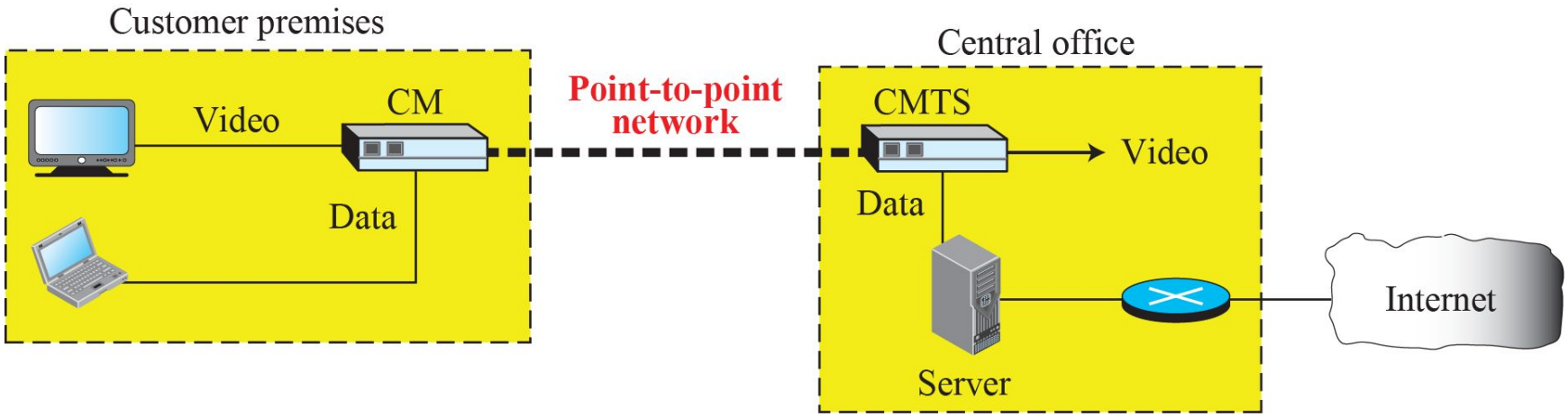


Figure 5.66: Cable modem transmission system (CMTS)



5.6.2 SONET

In this section, we introduce a high-speed network, SONET, that is used as a transport network to carry loads from other networks. We first discuss SONET as a protocol, and we then show how SONET networks can be constructed from the standards defined in the protocol.

5.6.2 (continued)

- *Architecture*
  - *Signals*
  - *SONET Devices*
- *Connections*
  - *Sections*
  - *Lines*
  - *Paths*
- *SONET Layers*
  - *Path Layer*
  - *Line Layer*
  - *Section Layer*
  - *Photonic Layer*

5.6.2 (continued)

- **SONET Frames**
  - Frame, Byte, and Bit Transmission
  - STS-1 Frame Format
- **STS Multiplexing**
  - Add/Drop Multiplexer
- **SONET Networks**
  - Linear Network
  - Ring Networks
  - Mesh Networks
- **Virtual Tributaries**

Table 5.10: SONET rates

STS	*OC*	*Rate (Mbps)*	*STS*	*OC*	*Rate (Mbps)*
STS-1	OC-1	51.840	STS-24	OC-24	1244.160
STS-3	OC-3	155.520	STS-36	OC-36	1866.230
STS-9	OC-9	466.560	STS-48	OC-48	2488.320
STS-12	OC-12	622.080	STS-96	OC-96	4976.640
STS-18	OC-18	933.120	STS-192	OC-192	9953.280

Figure 5.67: A simple network using SONET equipment

ADM: Add/drop multiplexer
STS MUX: Synchronous transport signal multiplexer
STS DEMUX: Synchronous transport signal demultiplexer
R: Regenerator
T: Terminal

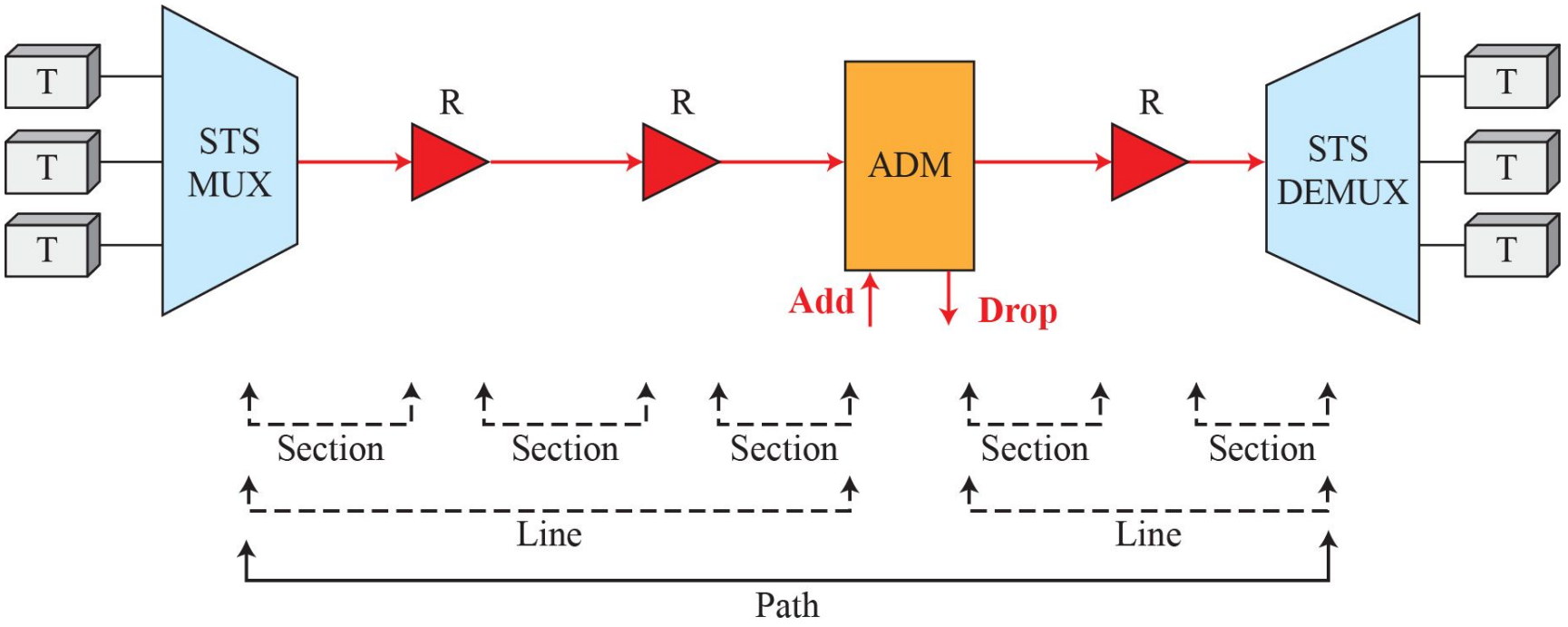


Figure 5.68: ***SONET layers compared with OSI or the Internet layers***

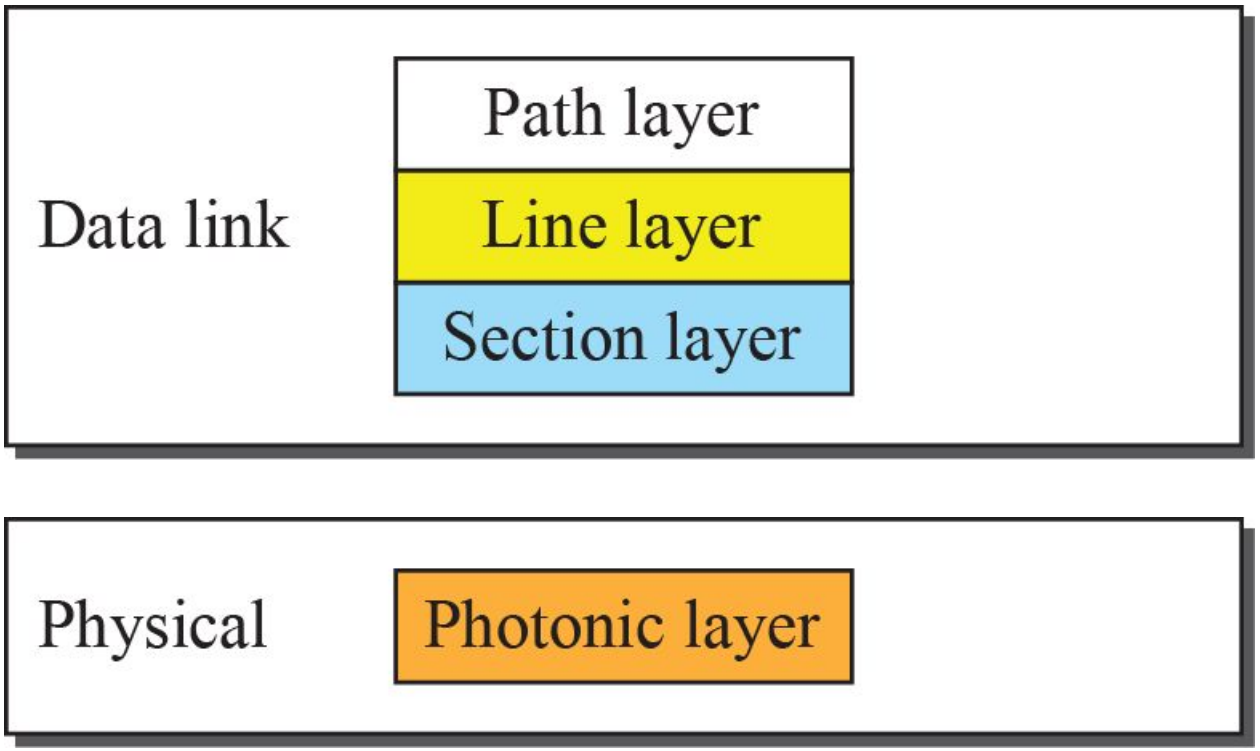


Figure 5.69: An STS-1 and an STS-n frame

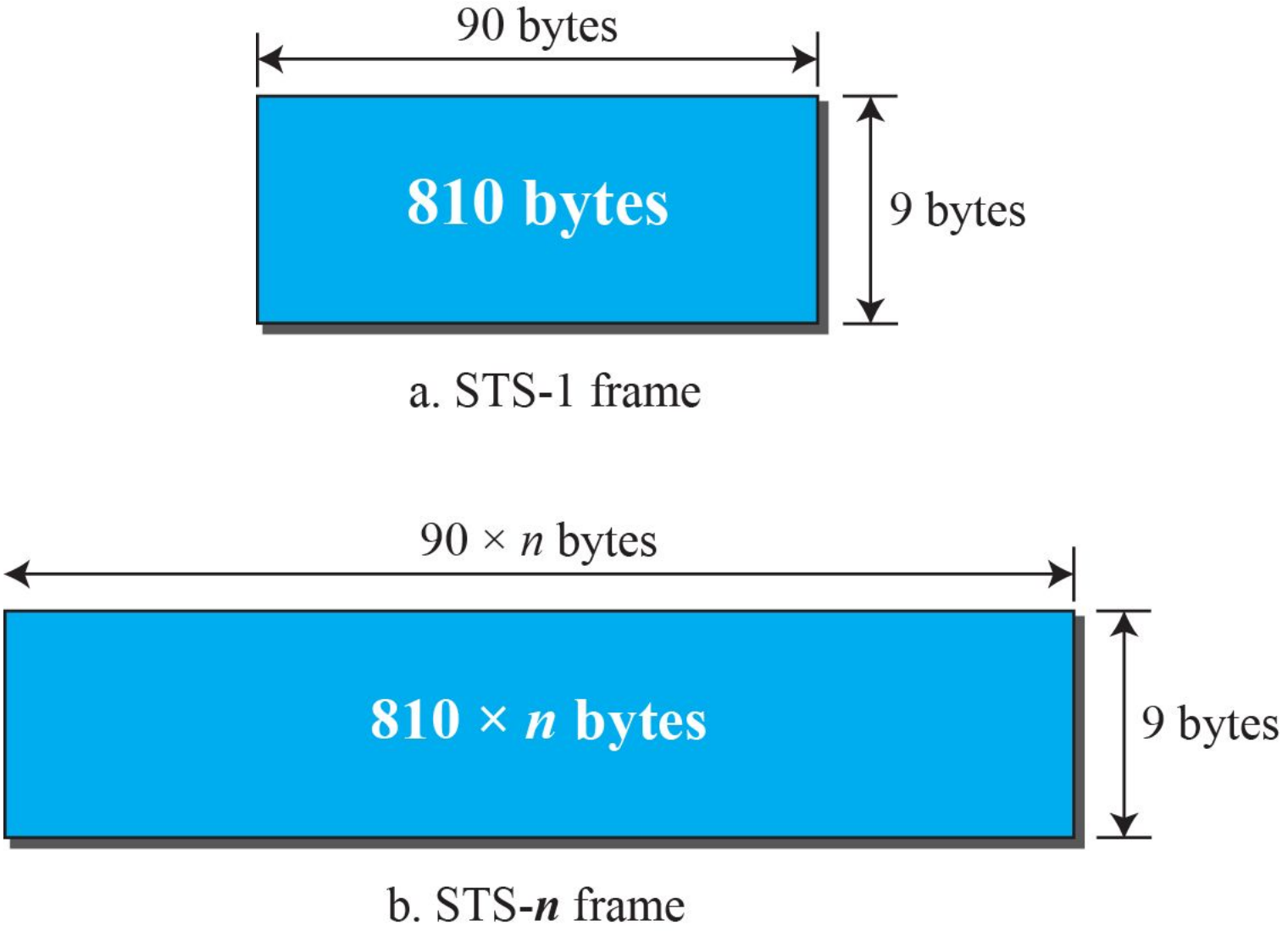


Figure 5.70: STS-1 frames in transition

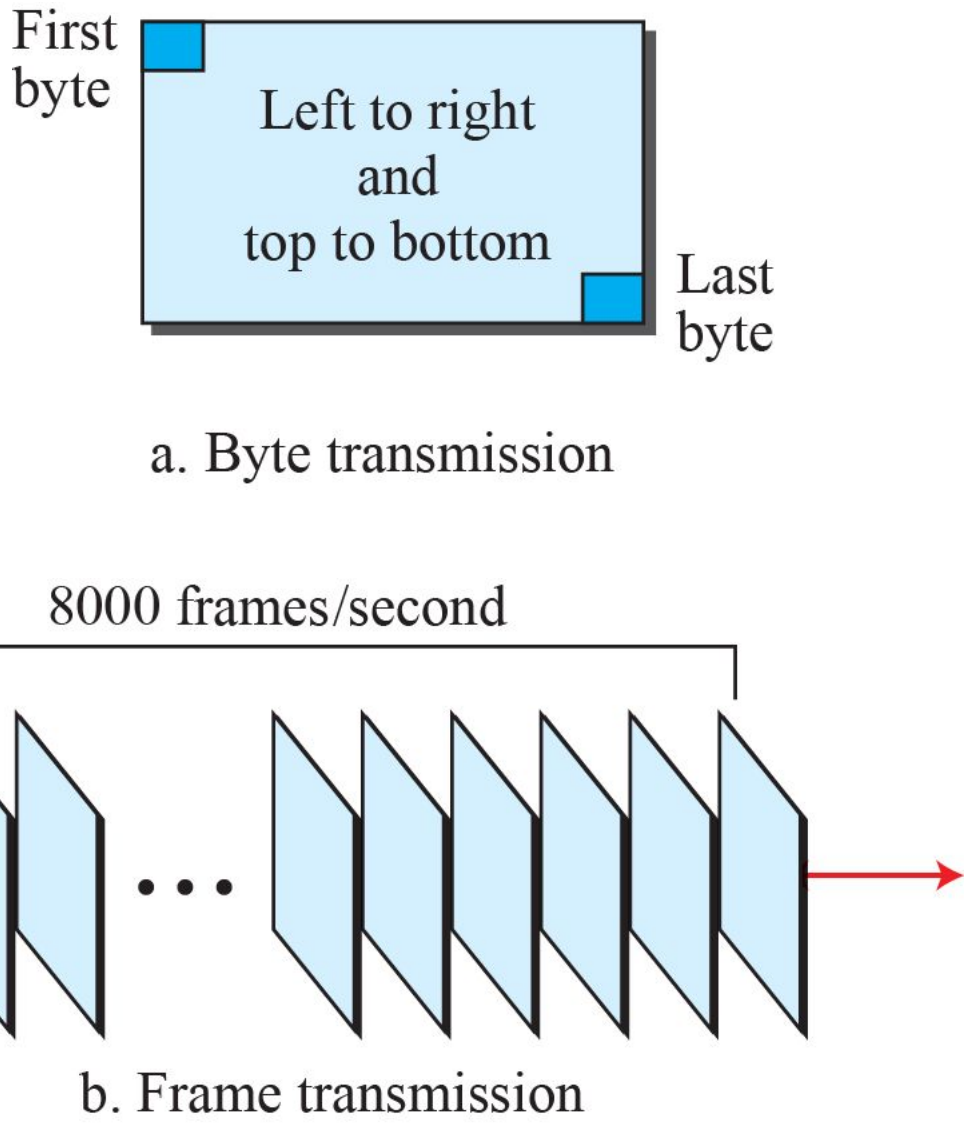


Figure 5.71: ***STS-1 frame overheads***

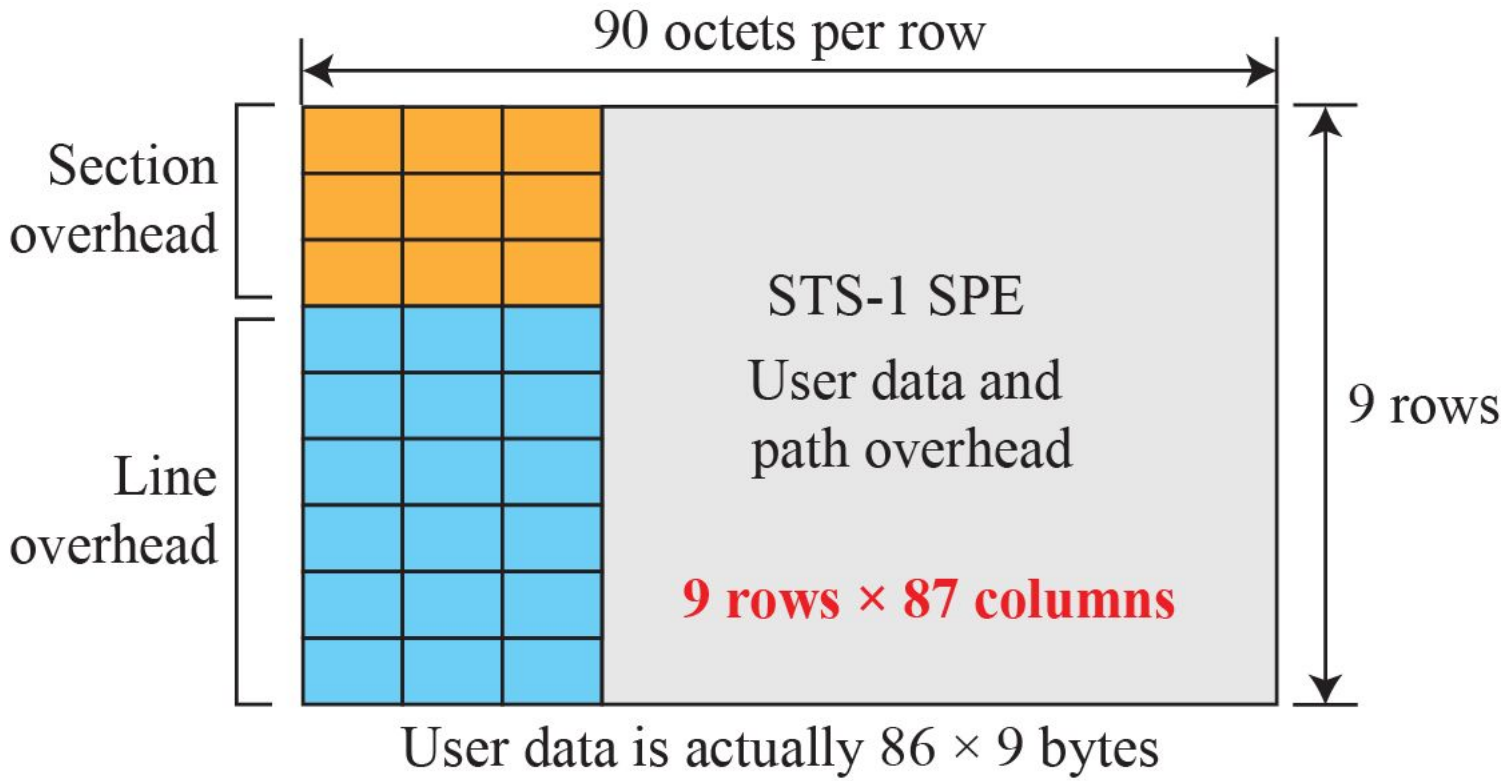


Figure 5.72: A linear SONET network

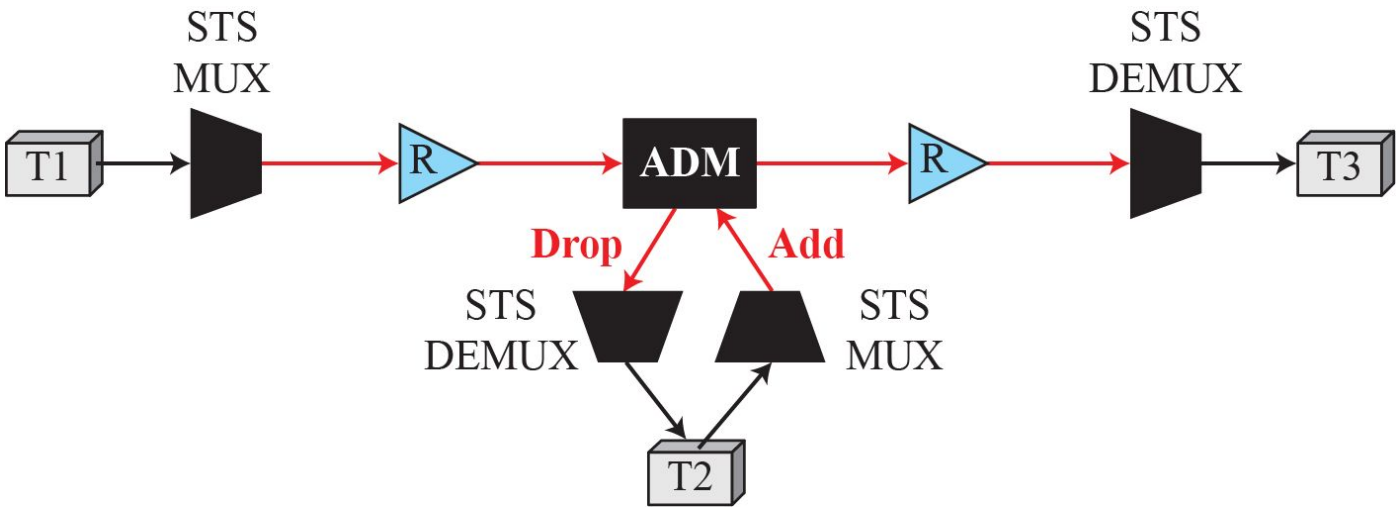


Figure 5.73: A unidirectional path switching ring

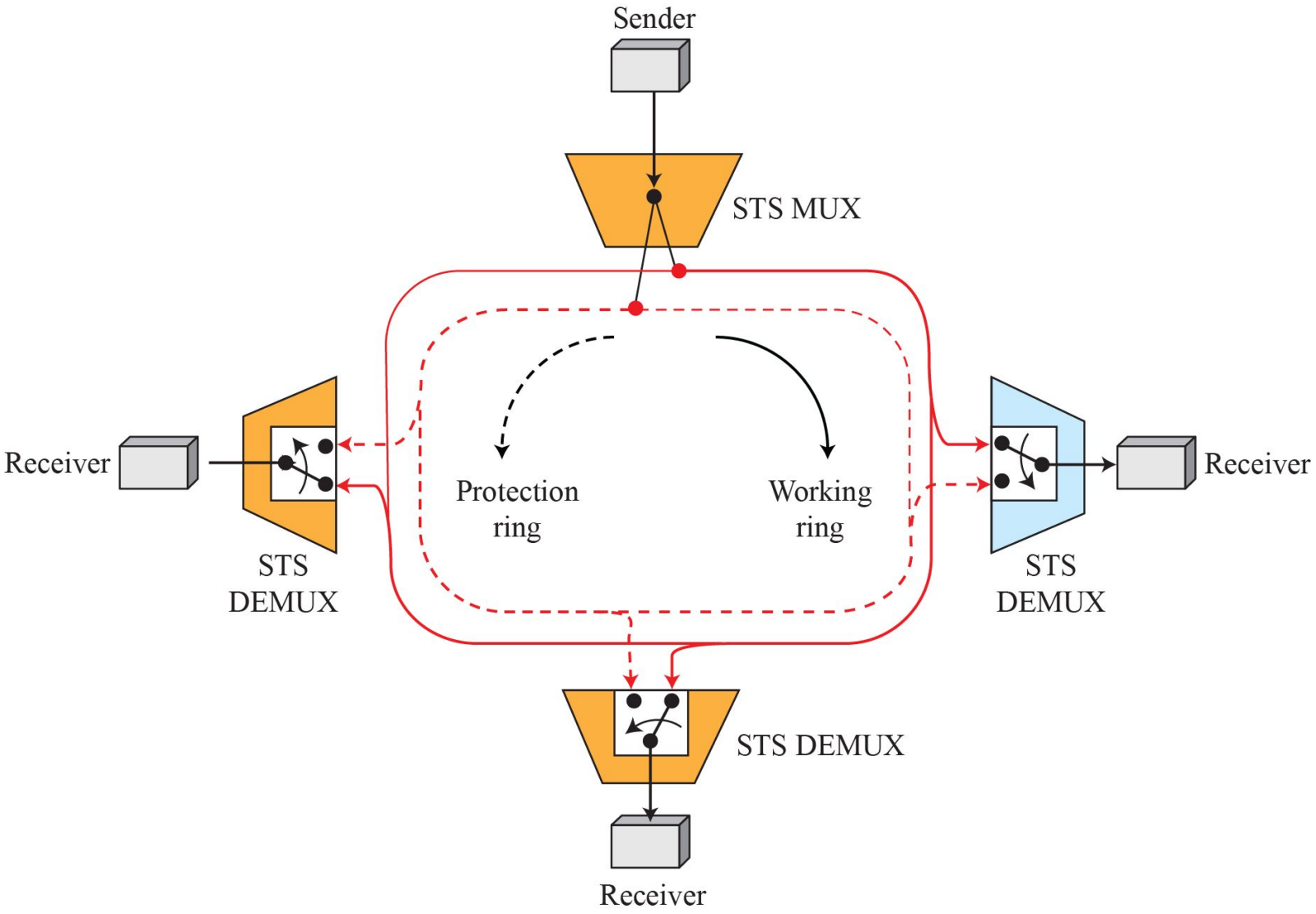
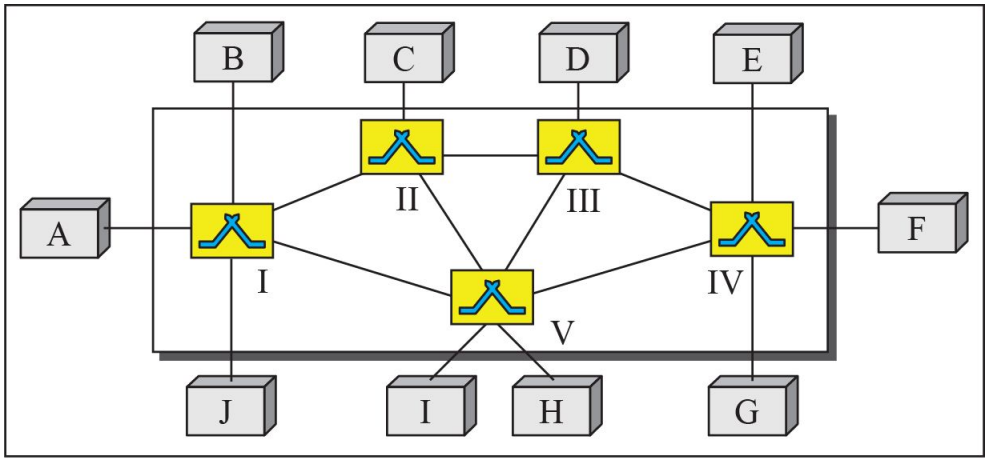
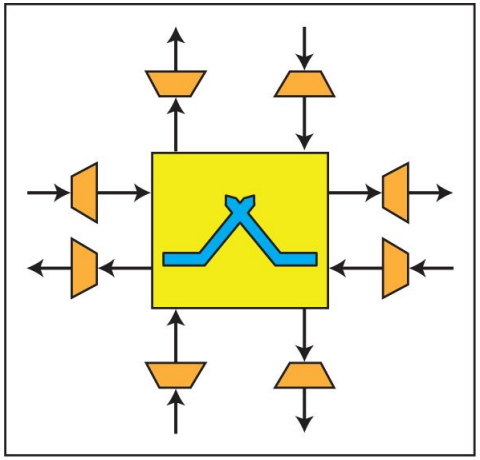


Figure 5.74: A mesh SONET network

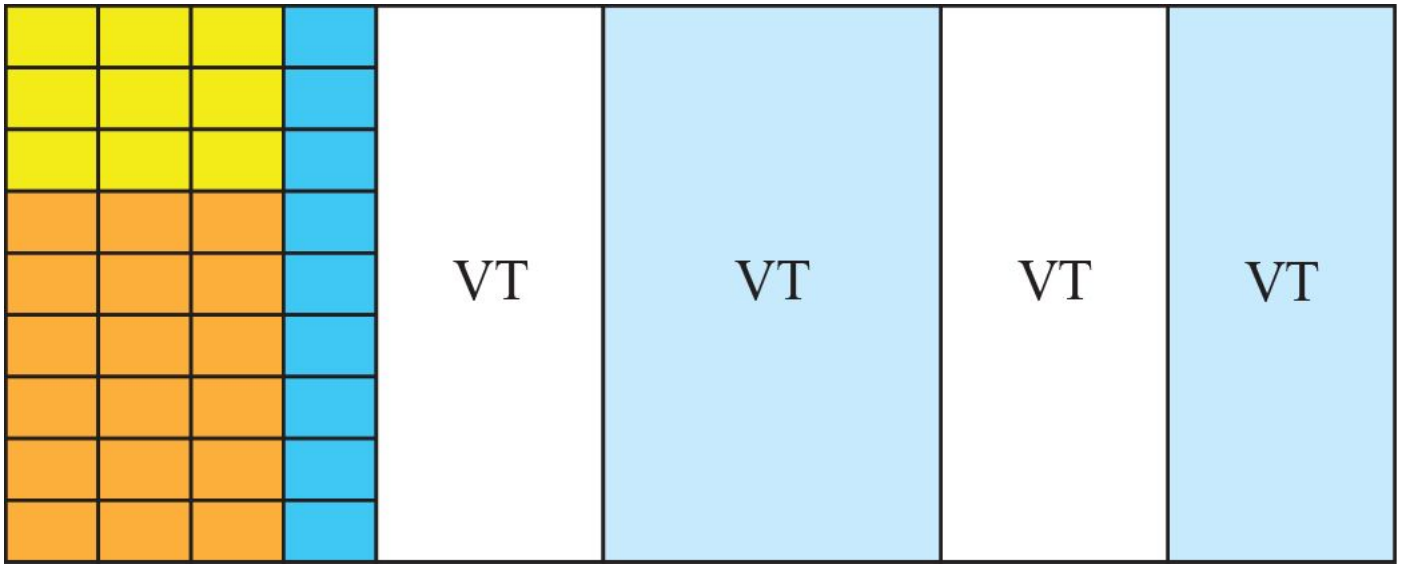


a. SONET mesh network



b. Cross-connect switch

Figure 5.75: Virtual tributaries



5.6.3 Switched Network: ATM

Asynchronous Transfer Mode (ATM) is a switched wide area network based on the cell relay protocol designed by the ATM forum and adopted by the ITU-T.

- ***Architecture***
  - ***Virtual Connection***
  - ***Connection Establishment and Release***
  - ***Switching***
  - ***ATM Layers***
  - ***Congestion Control and Quality of Service***

Figure 5.76: ATM multiplexing

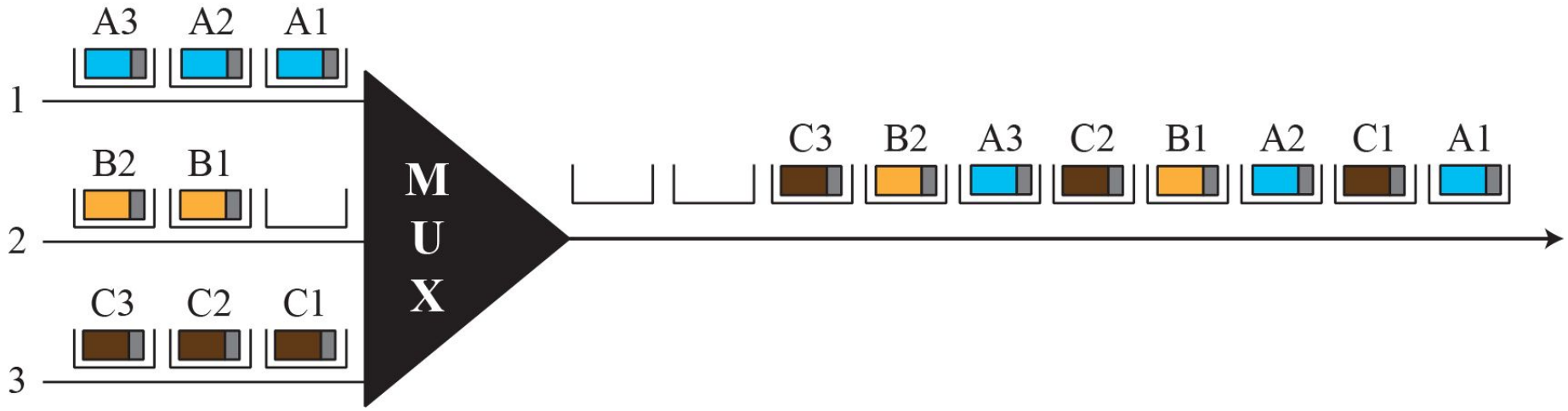


Figure 5.77: Architecture of an ATM network

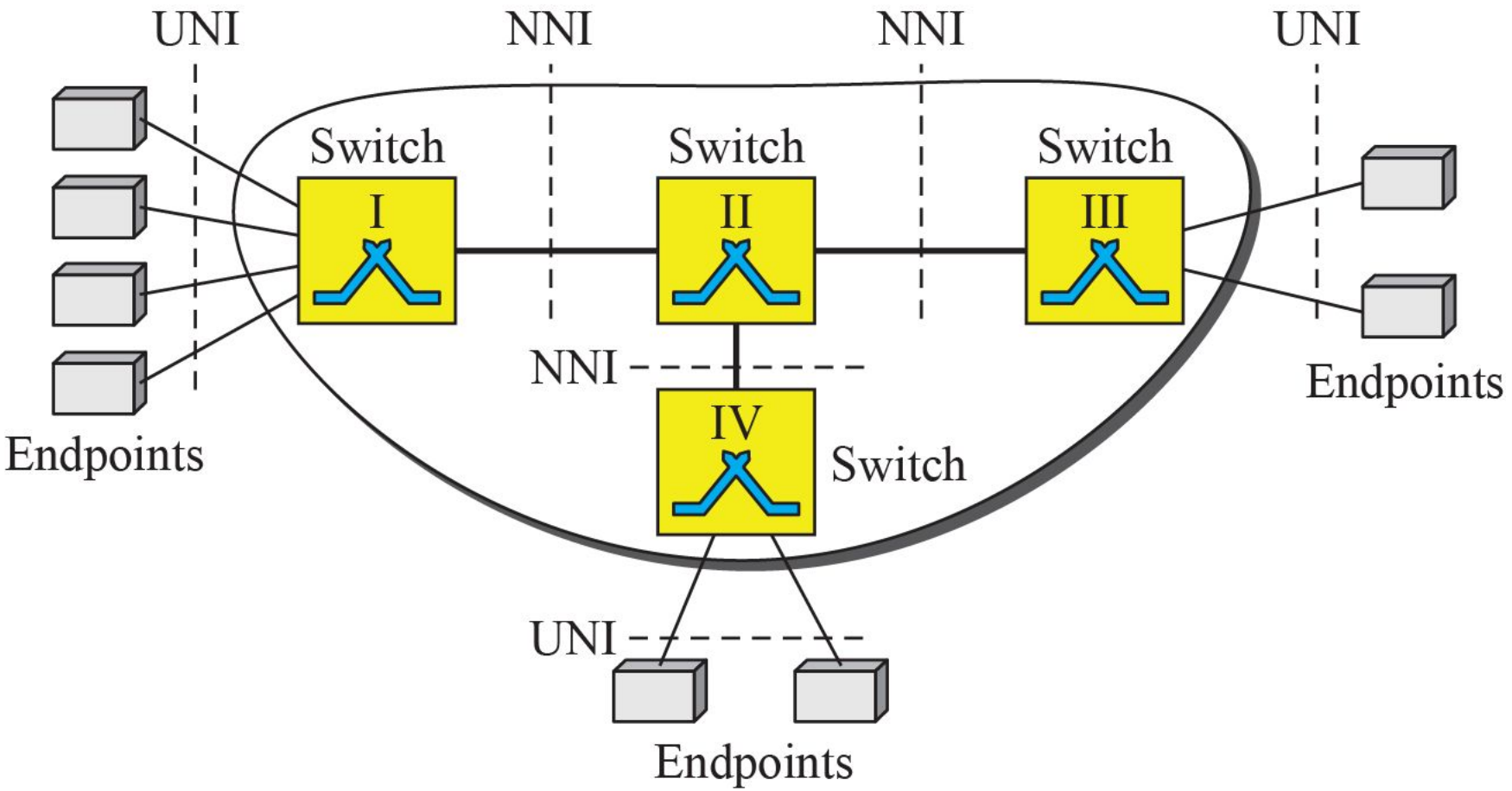
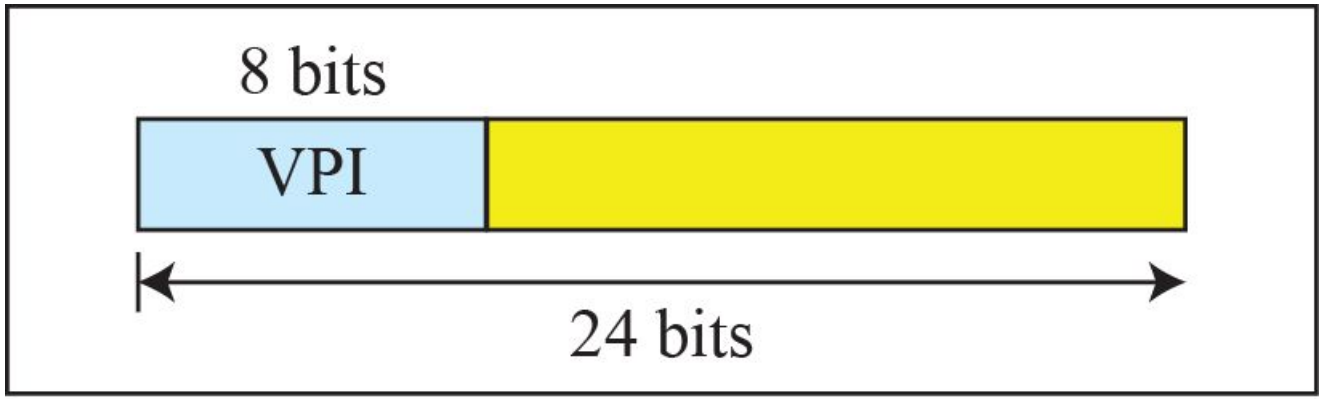
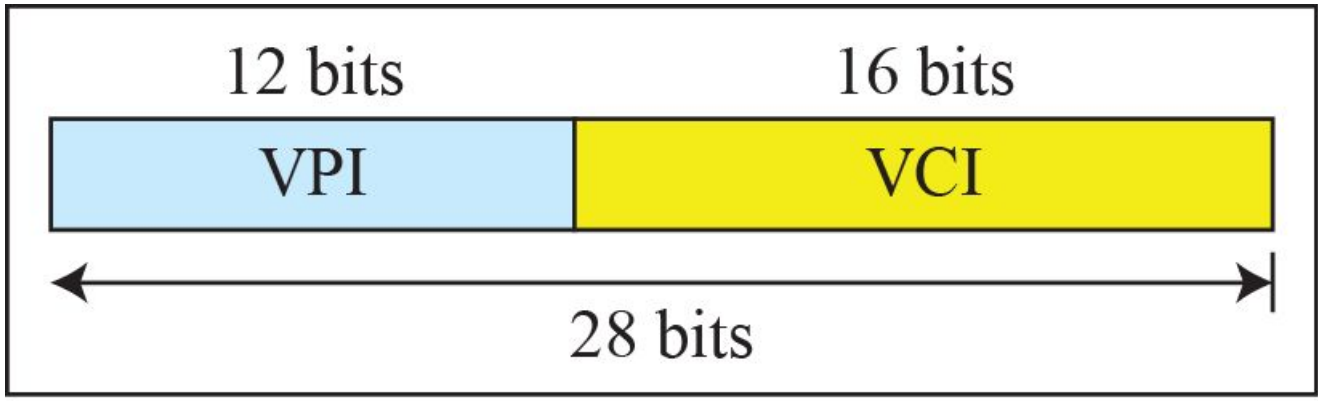


Figure 5.78: TP, VPs, and VCs

Figure 5.79: Virtual connection identifiers in UNIs and NNIs



a. VPI and VCI in a UNI



b. VPI and VCI in an NNI

Figure 5.80: An ATM cell

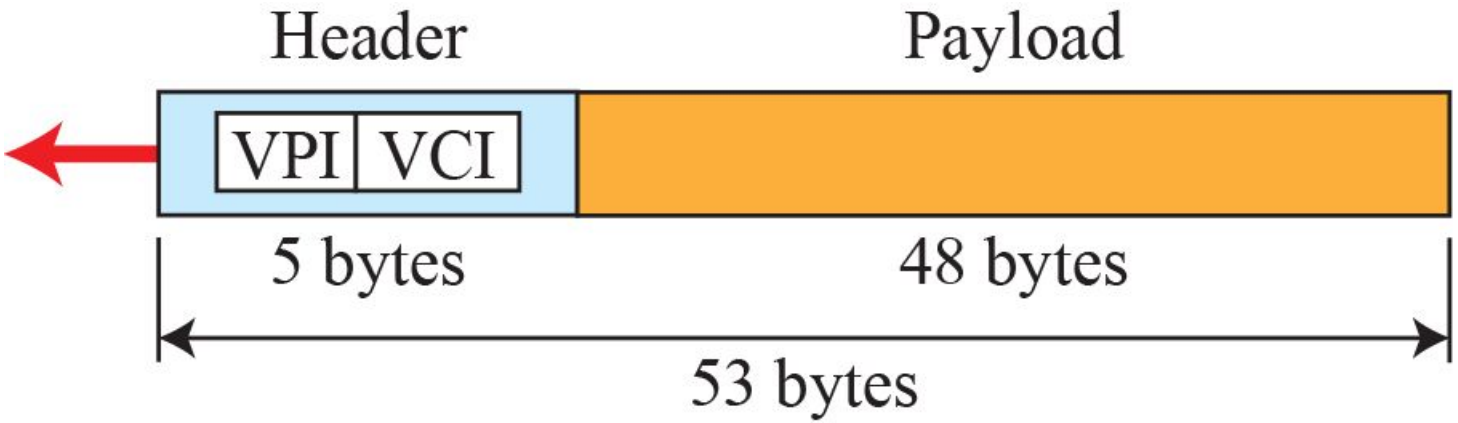


Figure 5.81: Routing with a switch

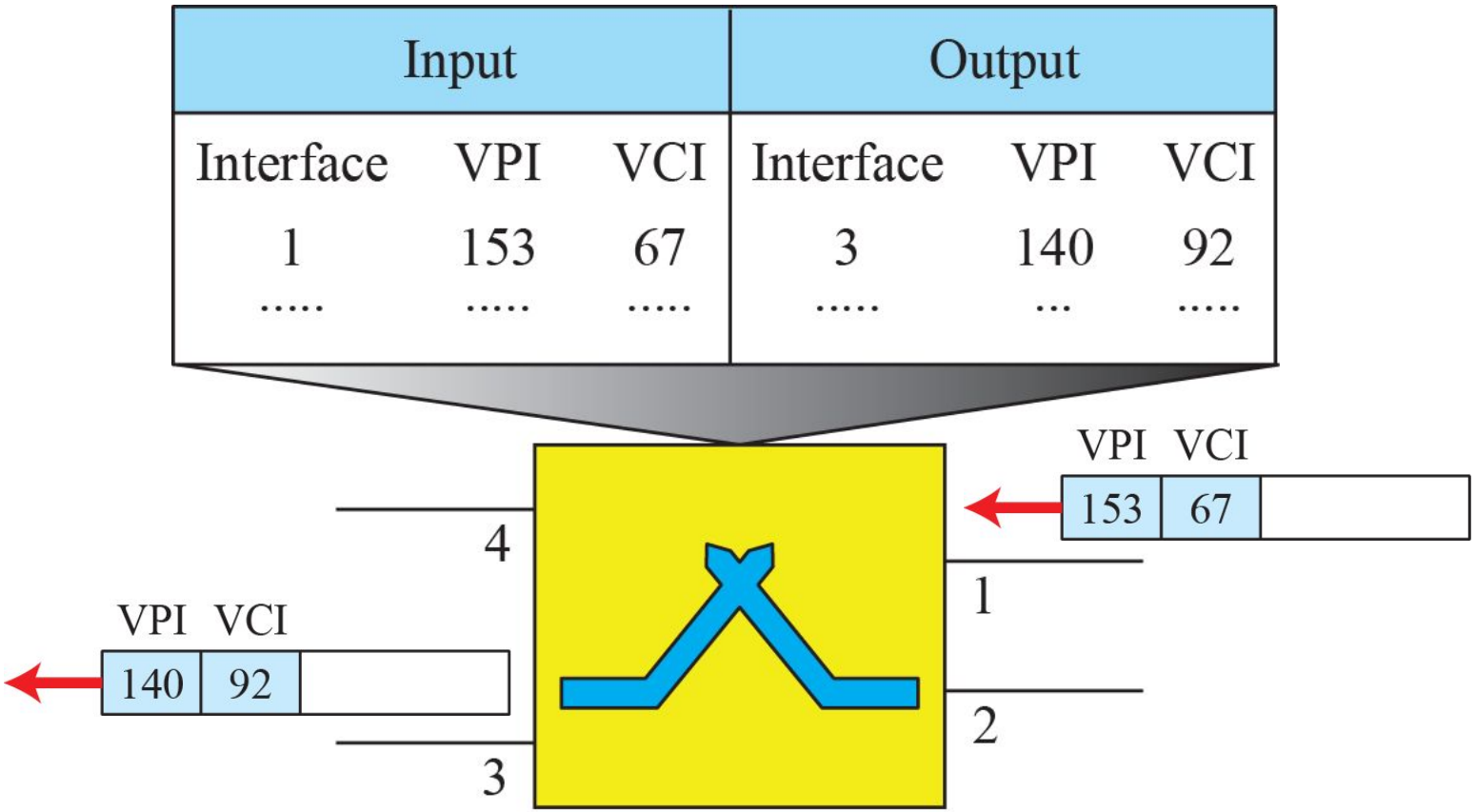


Figure 5.82: ATM layers

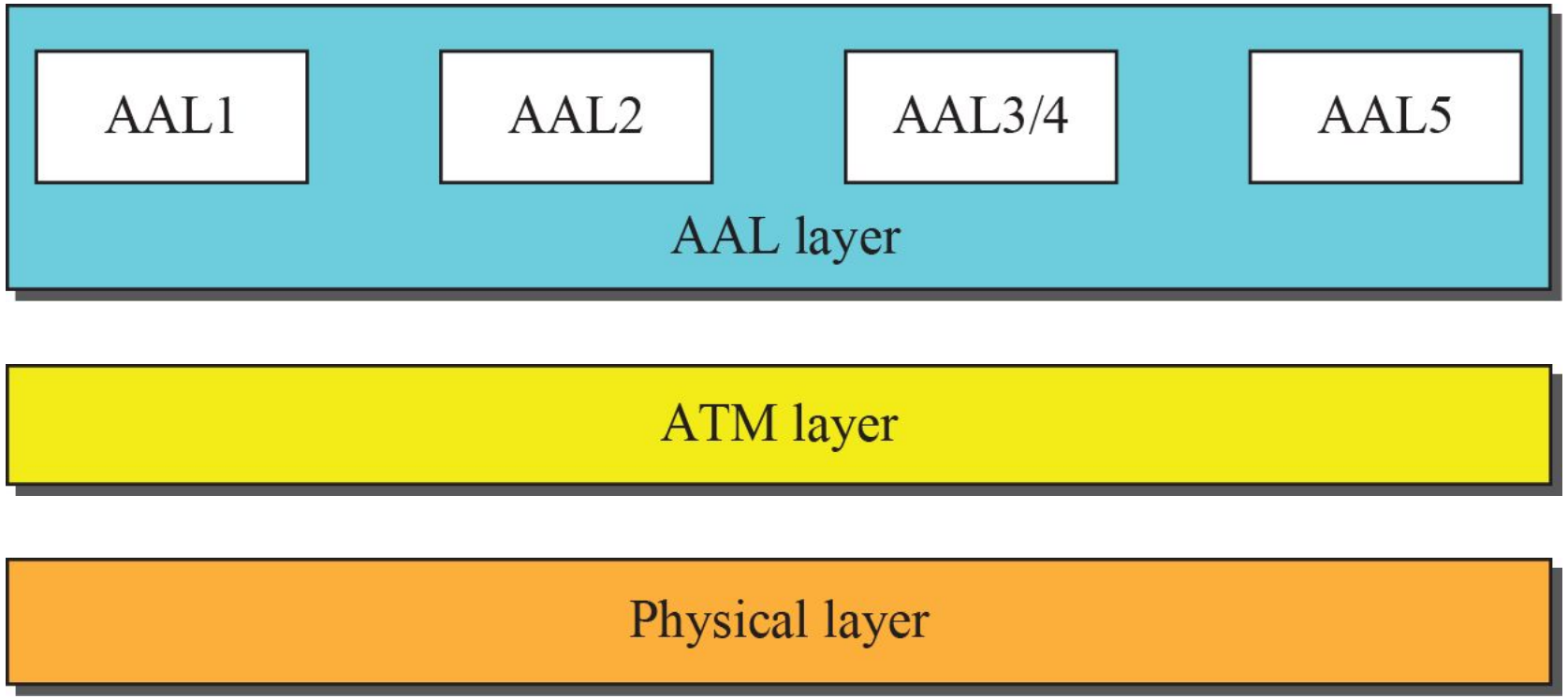
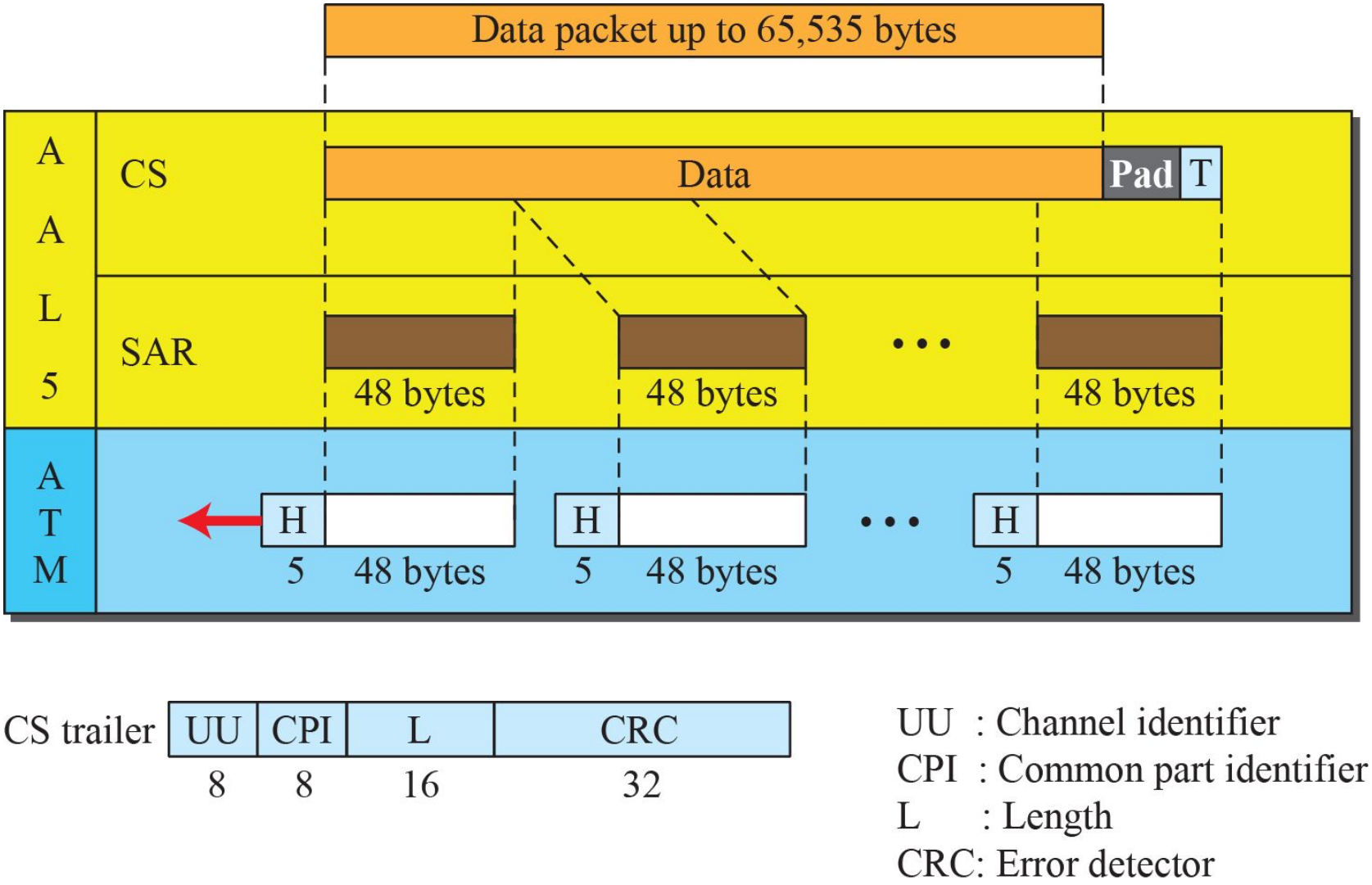


Figure 5.83: AAL5



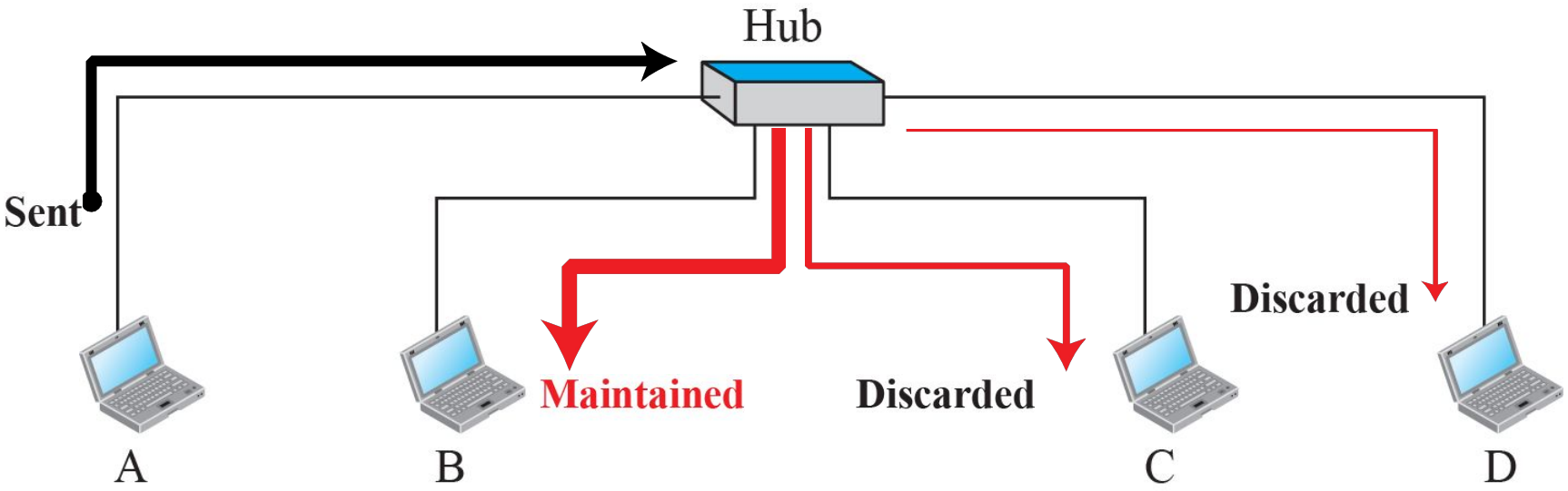
5-7 CONNECTING DEVICES

Hosts and networks do not normally operate in isolation. We use connecting devices to connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model. We discuss three kinds of connecting devices: repeaters link-layer switches, and routers.

5.7.1 Repeater or Hubs

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates and retimes the original bit pattern.

Figure 5.84: Repeater or hub



5.7.2 Link-Layer Switches

A link-layer switch operates in both the physical and the data-link layers. As a physical layer device, it regenerates the signal it receives. As a link-layer device, the link-layer switch can check the MAC addresses (source and destination) contained in the frame.

- *Filtering*
- *Transparent Switches*
  - *Forwarding*
  - *Learning*

Figure 5.85: Link-Layer Switch

Switching table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4

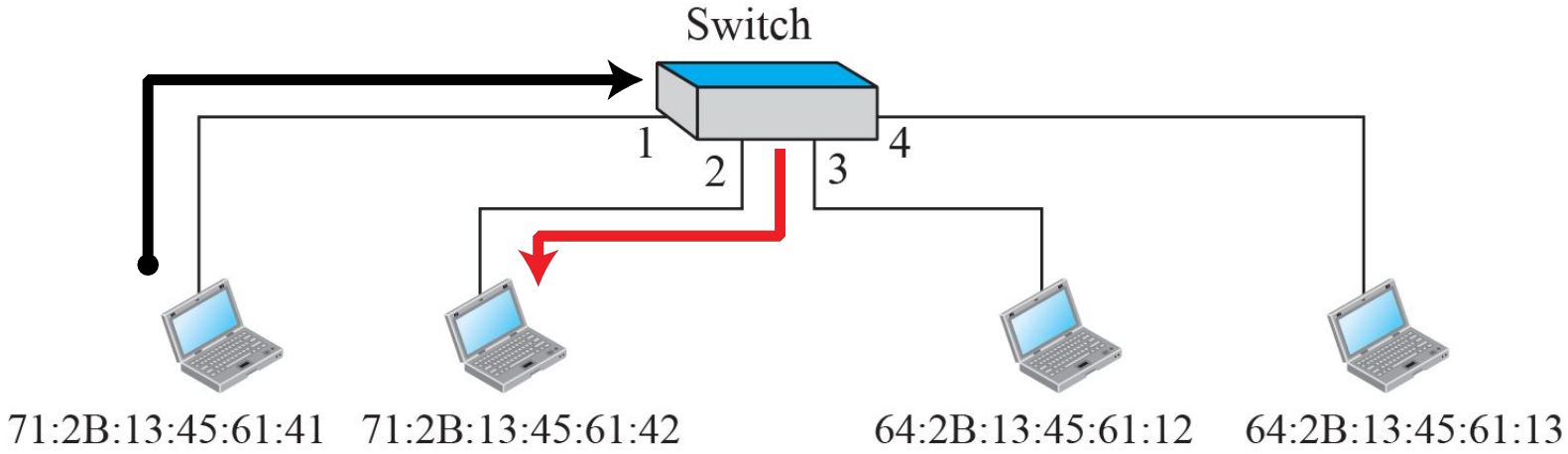


Figure 5.86: Learning switch

Address	Port

a. Original

Address	Port
71:2B:13:45:61:41	1

b. After A sends a frame to D

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4

c. After D sends a frame to B

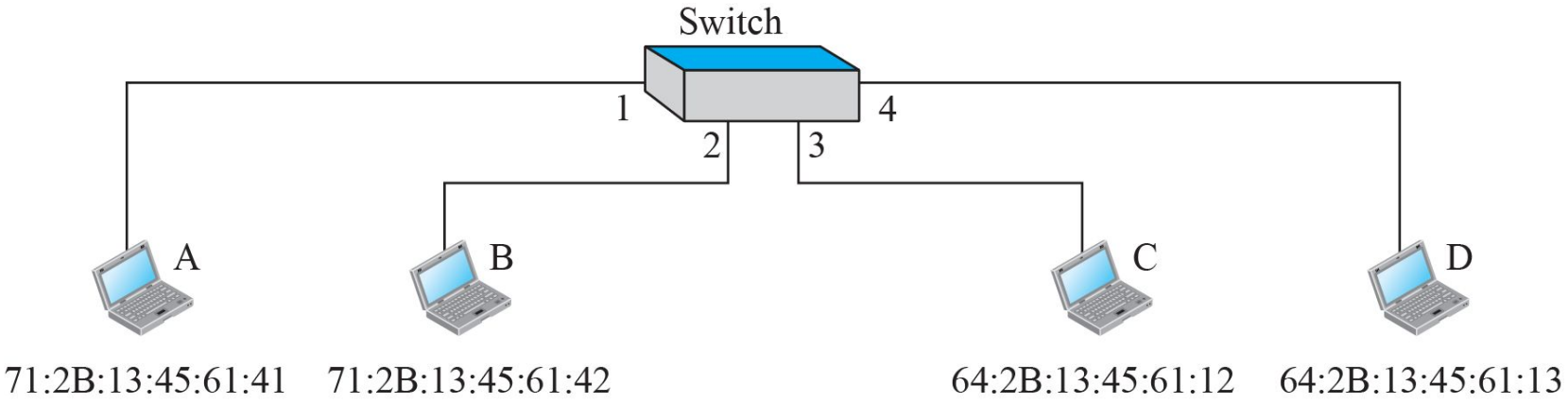
Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2

d. After B sends a frame to A

Address	Port
71:2B:13:45:61:41	1
64:2B:13:45:61:13	4
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3

e. After C sends a frame to D

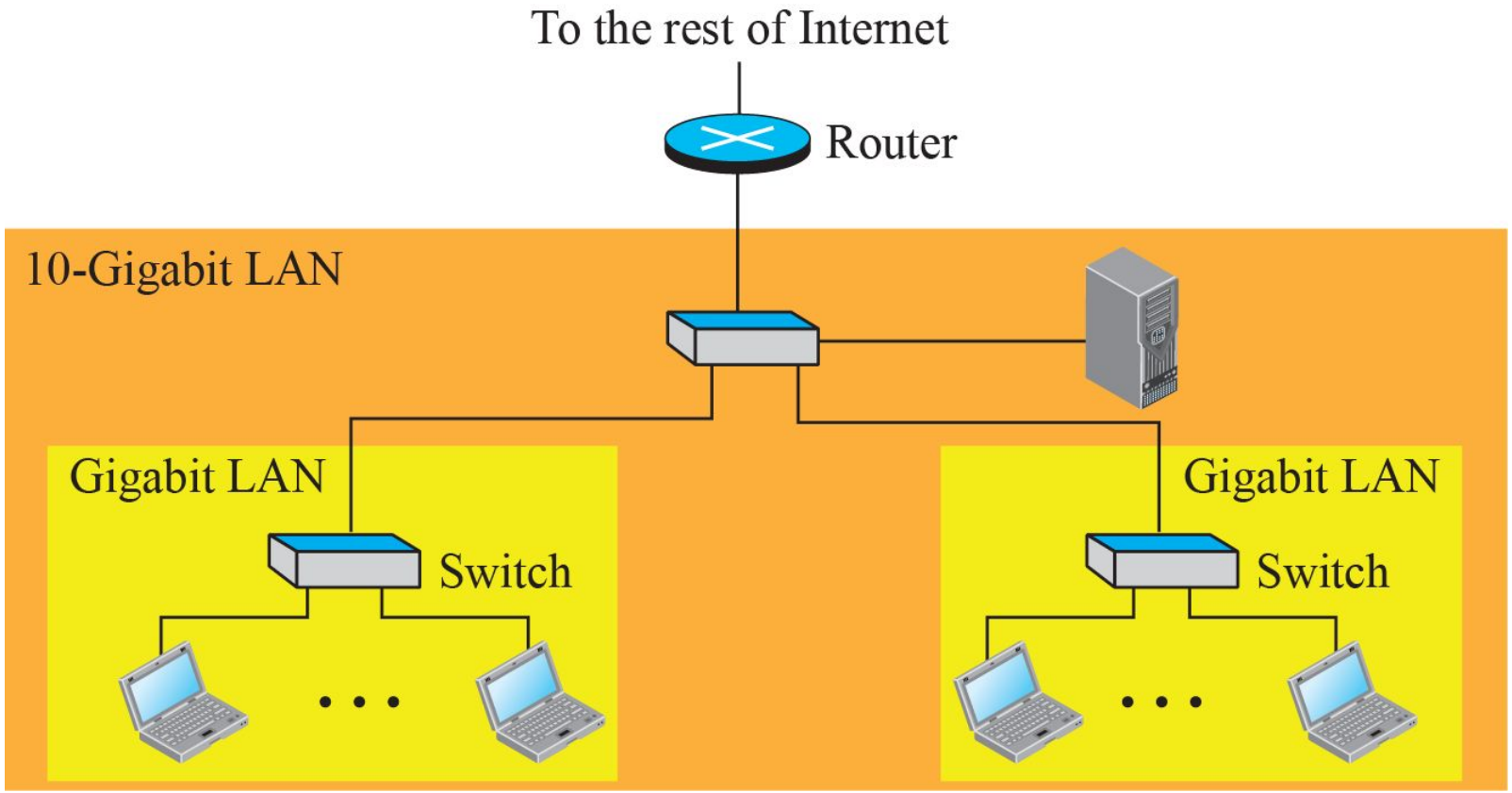
Gradual building of Table



5.7.3 Routers

We discussed routers in Chapter 4. In this chapter, we mention routers to compare them with a two-layer switch and a hub. A router is a three-layer device; it operates in the physical, data-link, and network layers.

Figure 5.87: ***Routing example***



Chapter 5: Summary

- *We can consider the data-link layer as two sublayers. The upper sublayer is responsible for data link control, and the lower sublayer is responsible for resolving access to the shared media. Data link control (DLC) deals with the design and procedures for communication between two adjacent nodes: node-to-node communication. This sublayer is responsible for framing and error control. Error control deals with data corruption during transmission. We discussed two link-layer protocols in this chapter: HDLC and PPP.*

- *Many formal protocols have been devised to handle access to a shared link. We categorize them into three groups: random access protocols, controlled access protocols, and channelization protocols.*

Chapter 5: Summary (continued)

- *At the data-link layer, we use link-layer addressing. The system normally finds the link-layer address of the next node using the Address Resolution Protocol.*

- *Ethernet is the most widely used local area network protocol. The data-link layer of Ethernet consists of the LLC sublayer and the MAC sublayer. The MAC sublayer is responsible for the operation of the CSMA/CD access method and framing. A virtual local area network (VLAN) is configured by software, not by physical wiring. Membership in a VLAN can be based on port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of these features.*

Chapter 5: Summary (continued)

- *We discussed two access networks: DSL and Cable. We also discussed two wide area networks: SONET and ATM.*

- *We also discussed connecting devices in this chapter. A repeater is a connecting device that operates in the physical layer of the Internet model. A switch is a connecting device that operates in the physical and data-link layers of the Internet model. A transparent switch can forward and filter frames and automatically build its forwarding table. A router is a connecting device that operates in the first three layers of the TCP/IP suite.*