GENERAL SIR JOHN KOTELAWALA DEFENCE UNIVERSITY

Communication Networks

ET 3102

https://classroom.google.com/u/1/c/NjUwODgwNjkwNTY3

Classroom > Communication Networks - ET 3102

- Photonic and Laser Engine...
- Next Generation Cellular N...
- Communication Technology
- Communication Theory
- Communication Systems
- Deep Learning
- Machine Learning
- 35th Intake : EE & ET
- Individual Design Project (...
- Random Signals and Proce...

Archived classes

Settings

Stream | Classwork | People | Grades

Class code

nhqhb2c

Announce something to your class

Upcoming

No work due soon

View all

This is where you can talk to your class

Use the stream to share announcements, post assignments, and respond to student questions

Stream settings

10:49 AM

Outline

Overview on ISO/OSI reference model for open systems, packet and distributed systems and Topologies.

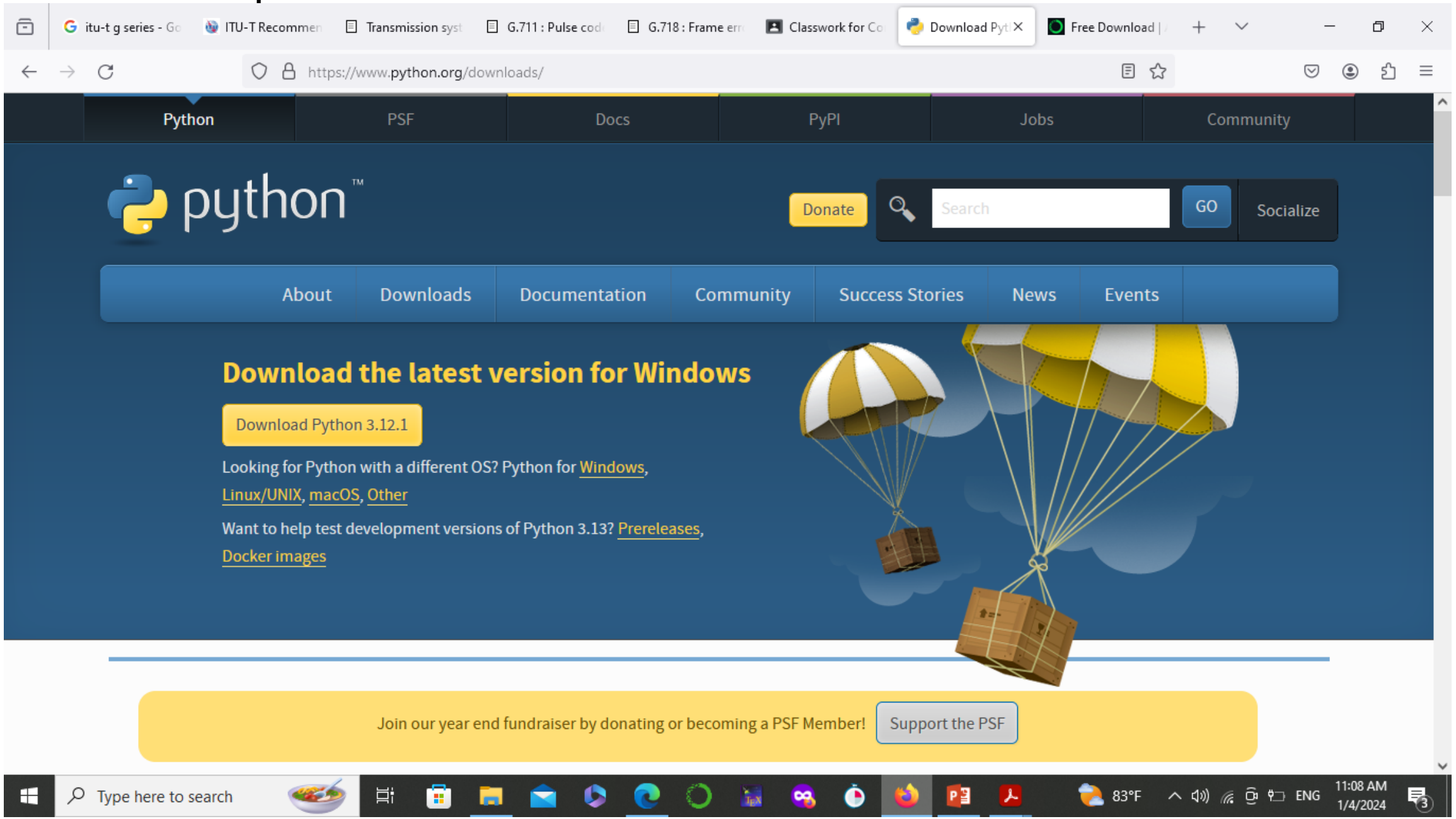
Physical and Data Link Layers.

Network (IP) and Transport Layers (TCP/UDP).

Session Layer, Presentation and Application Layer.

Local Area Network and Wide Area Networks.

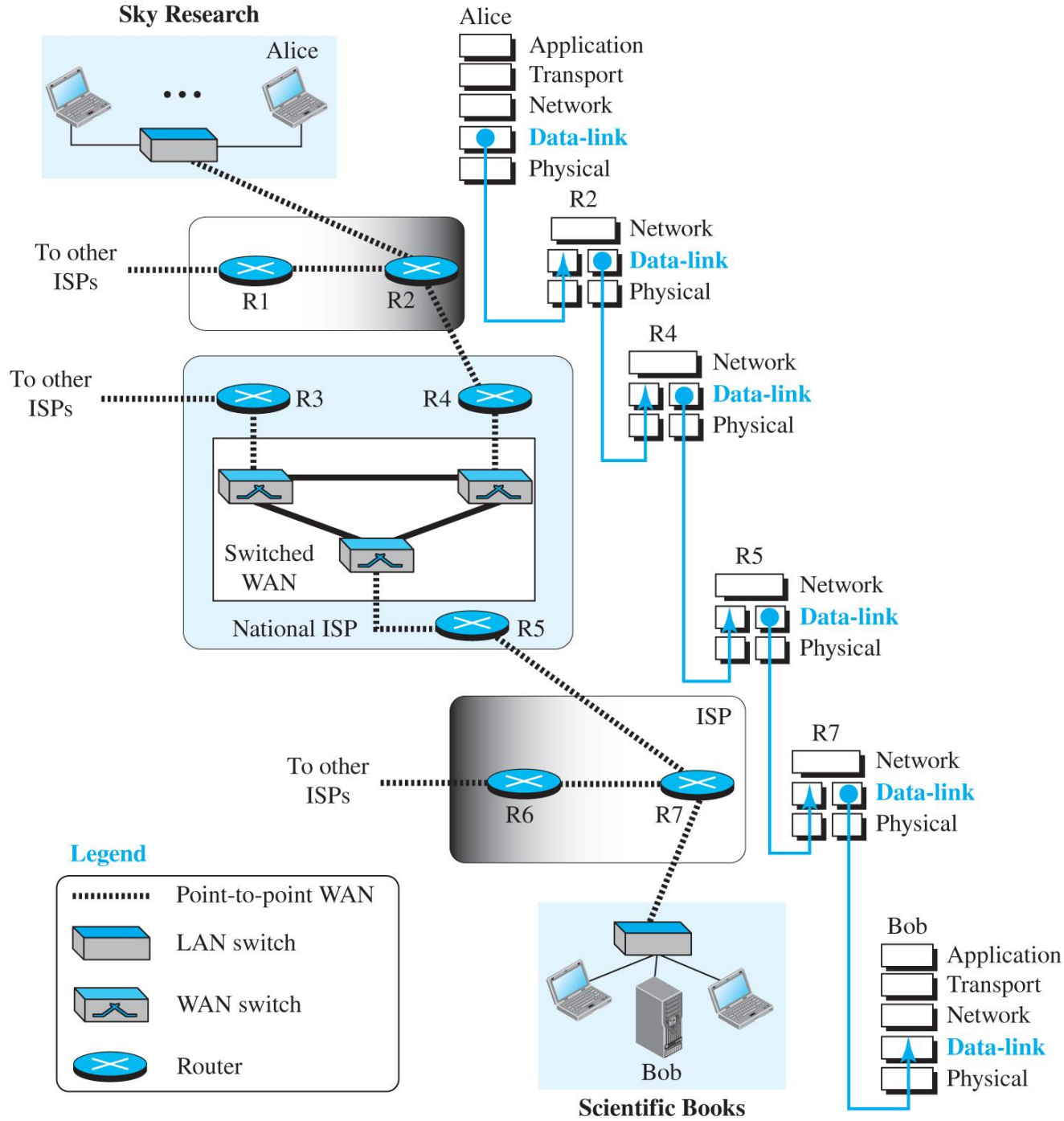
Software Requirements



Physical and Data Link Layers

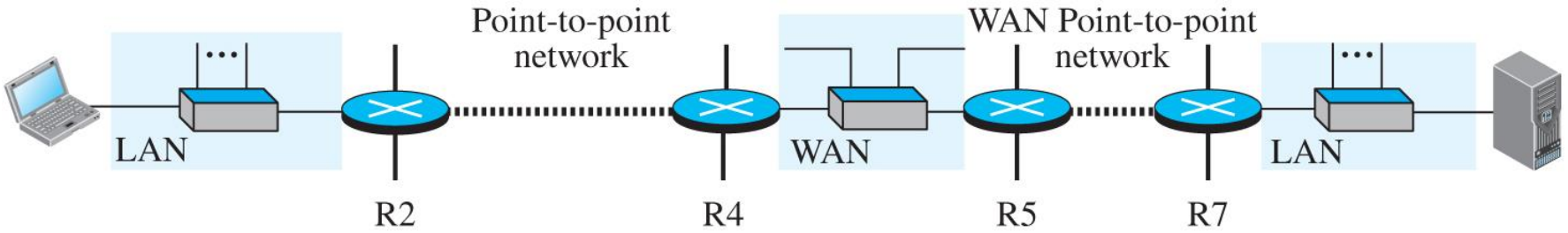
Introduction

- 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 shows the same scenario, we are now interested in communication at the data-link layer.



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 is a simple representation of links and nodes when the path of the data unit is only six nodes.



a. A small part of the Internet

b. Nodes and links

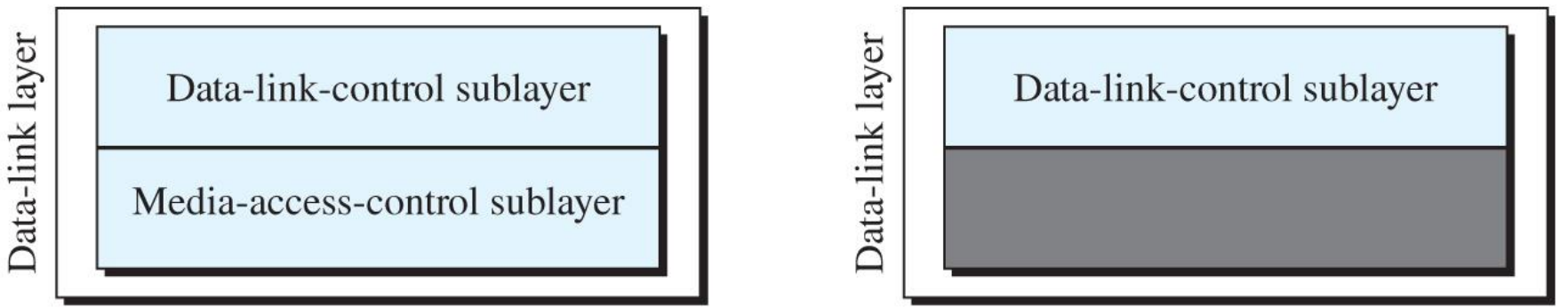
Two Types of Links

- 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.

.

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, LAN protocols actually use the same strategy.



a. Data-link layer of a broadcast link

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

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 control, and
  - error control.

.

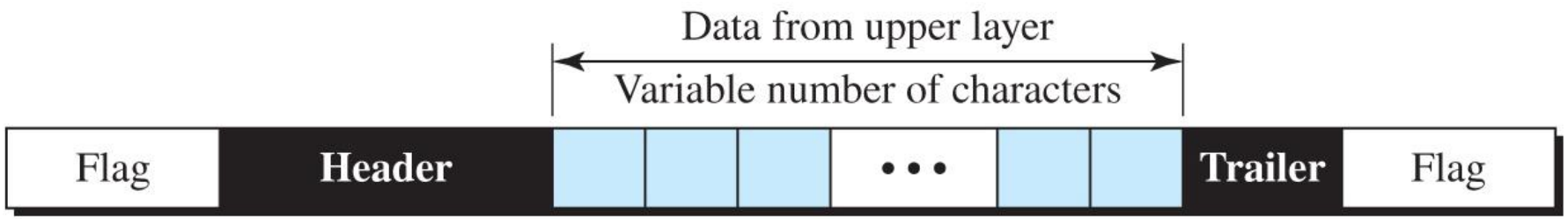
Framing

Framing

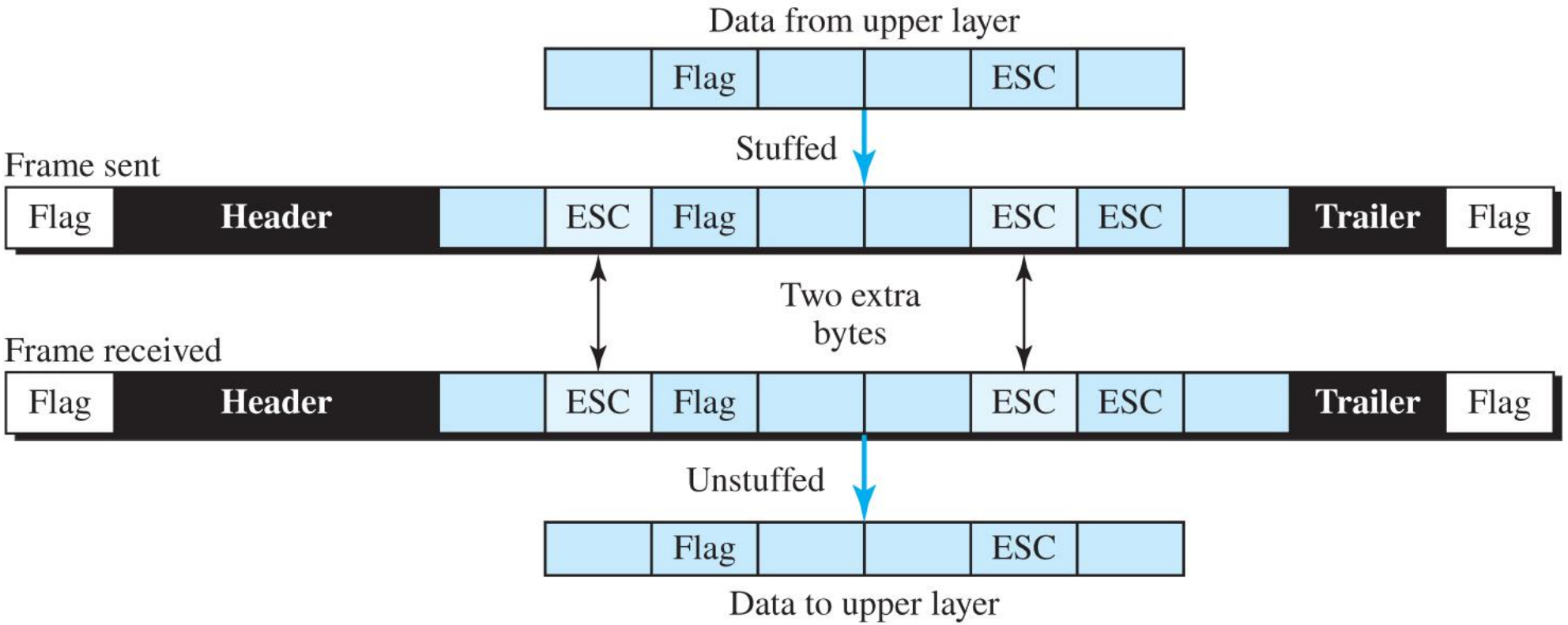
- The data-link layer needs to pack bits into frames, so that each frame is distinguishable from another.
- Our postal system practices a type of framing.
- The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.
- Frames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

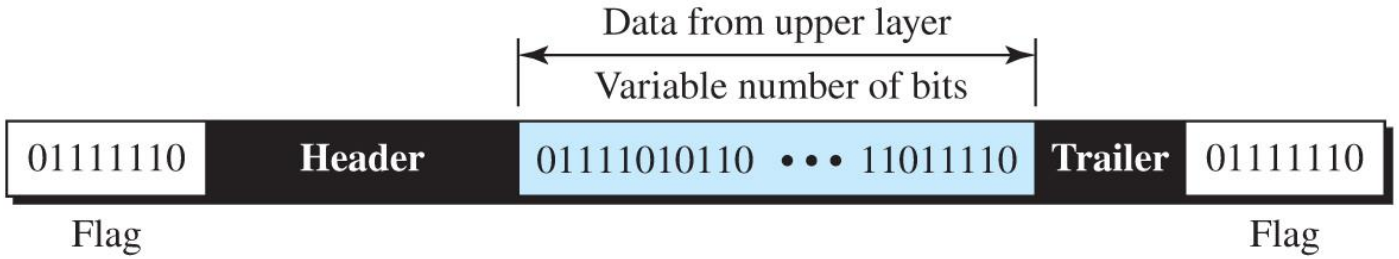


Byte stuffing and unstuffing

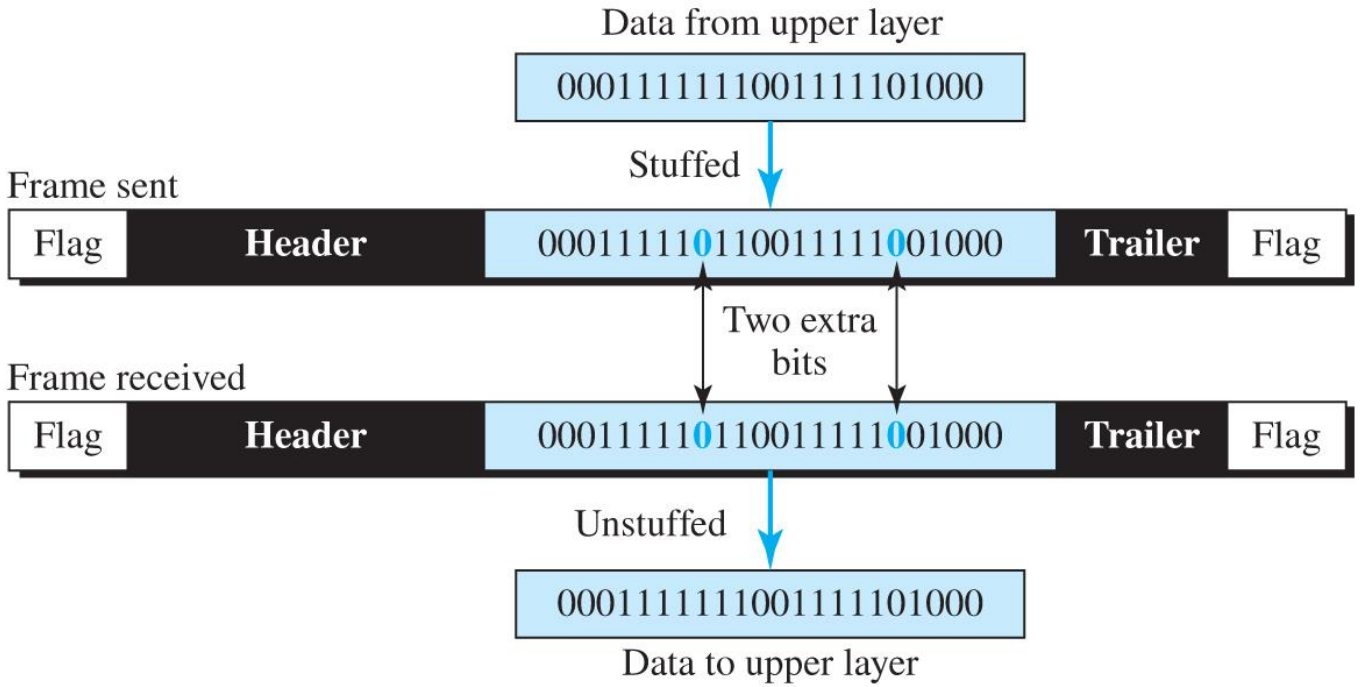


Bit-Oriented Framing

- 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



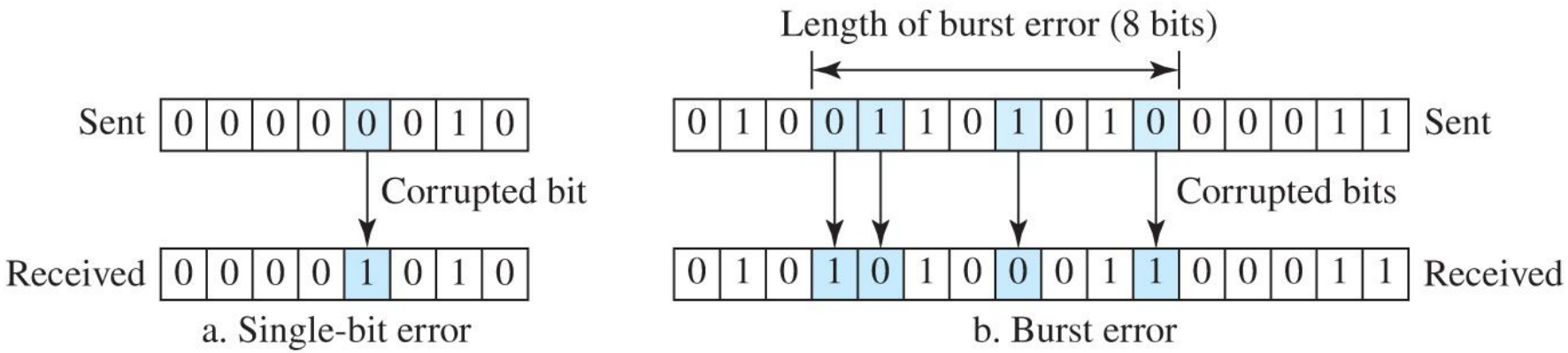
Error Control

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.

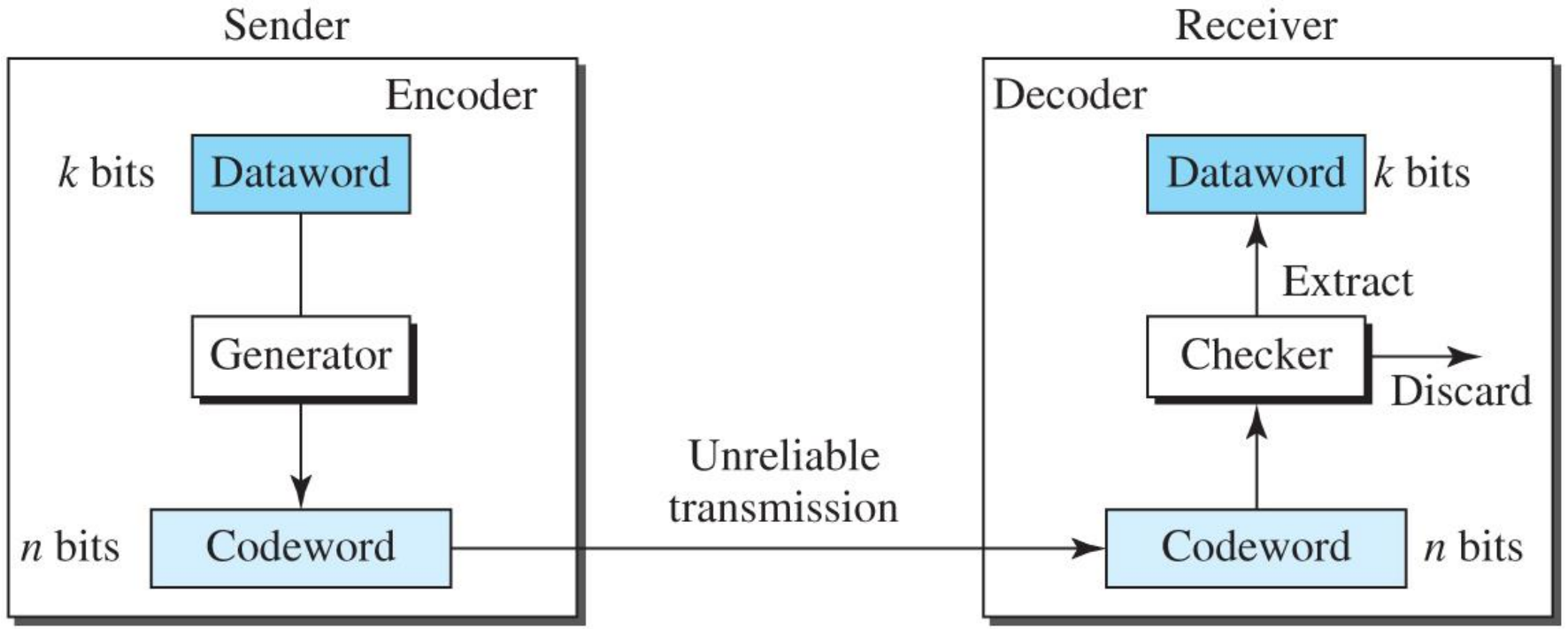
Types of Error

- 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 shows the effect of a single-bit and a burst error on a data unit.



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 ?.



Error Control – Example 1

- Let us assume that k = 2 and n = 3.
- Table below shows the list of datawords and codewords.
- Later slides will guide on how to derive a codeword from a dataword.

• Table: A code for error detection in Example

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

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

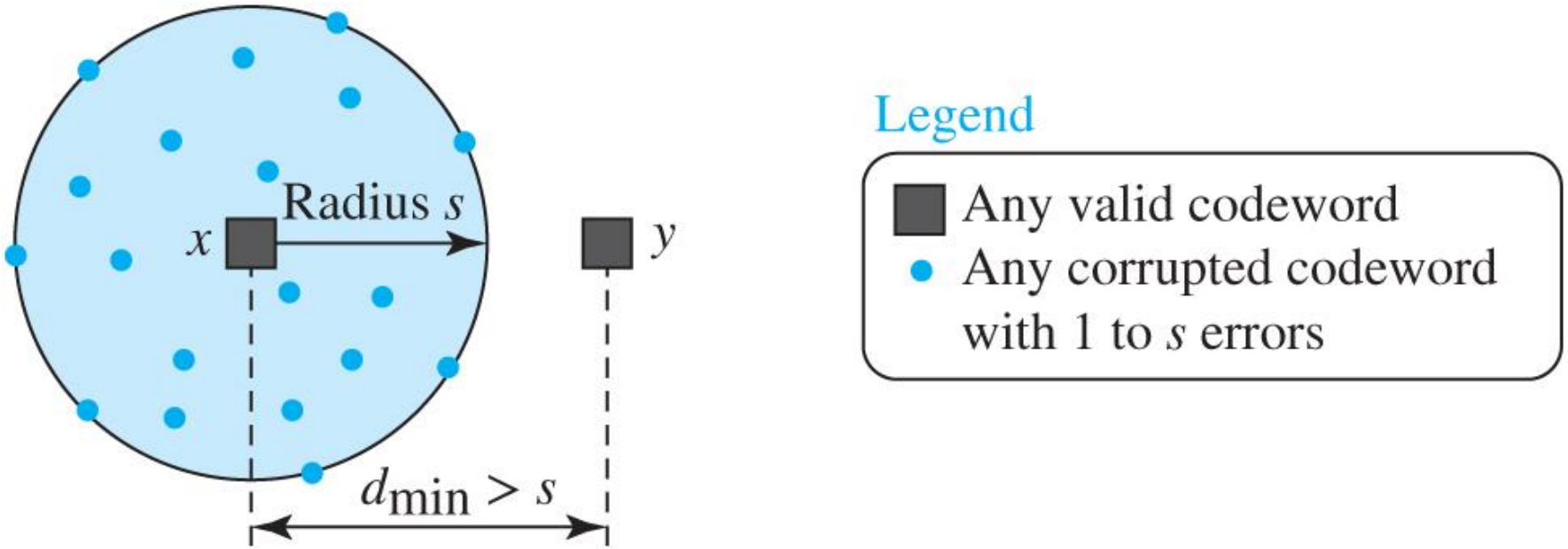
Hamming Distance - Example

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: Geometric concept explaining d_{min} in error detection



Hamming Distance - Example

- The minimum Hamming distance for our first code scheme (Table) 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.

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

- A code scheme has a Hamming distance dmin = 4.
- This code guarantees the detection of up to three errors (d = s + 1 or s = 3).

Linear Block Codes

- Almost all block codes[1] 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

Linear Block Codes - Example

- The code in Table 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.

.

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

Linear Block Codes

- Perhaps the most familiar error-detecting code is the parity-check code.

2

- 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.

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

- In our first code (Table above), the numbers of 1s in the nonzero codewords are 2, 2, and 2. So the minimum Hamming distance is dmin = 2.

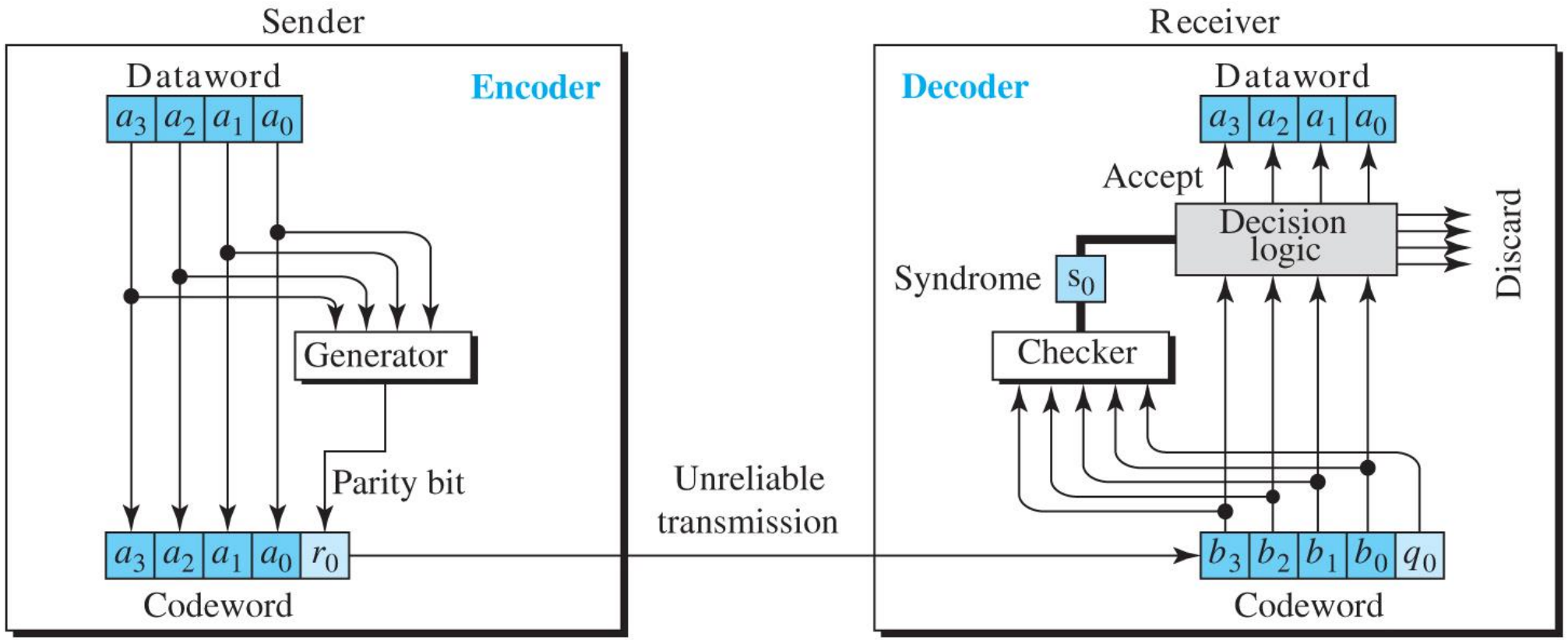
.

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**

Simple parity-check code

Figure: Encoder and decoder for simple parity-check code



Simple parity-check code – Example

- 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:
  - No error occurs; the received codeword is 10111.
  - The syndrome is 0. The dataword 1011 is created.
  - One single-bit error changes a1. The received codeword is 10011.
  - The syndrome is 1. No dataword is created.

Simple parity-check code – Example

- One single-bit error changes r_0. The received codeword is 10110.
- 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.
- An error changes r_0 and a second error changes a_3. The received codeword is 00110.
- 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.
- Three bits—a_3, a_2, and a_1—are changed by errors. The received codeword is 01011.
- 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 the subject: Communication Networks.
- Here, 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

- CRC supports Arbitrary length message
- Excellent error detection
- Fast Hardware implementation, CPU can do CRC computation fast
- Transmitter generates n-bit sequence called

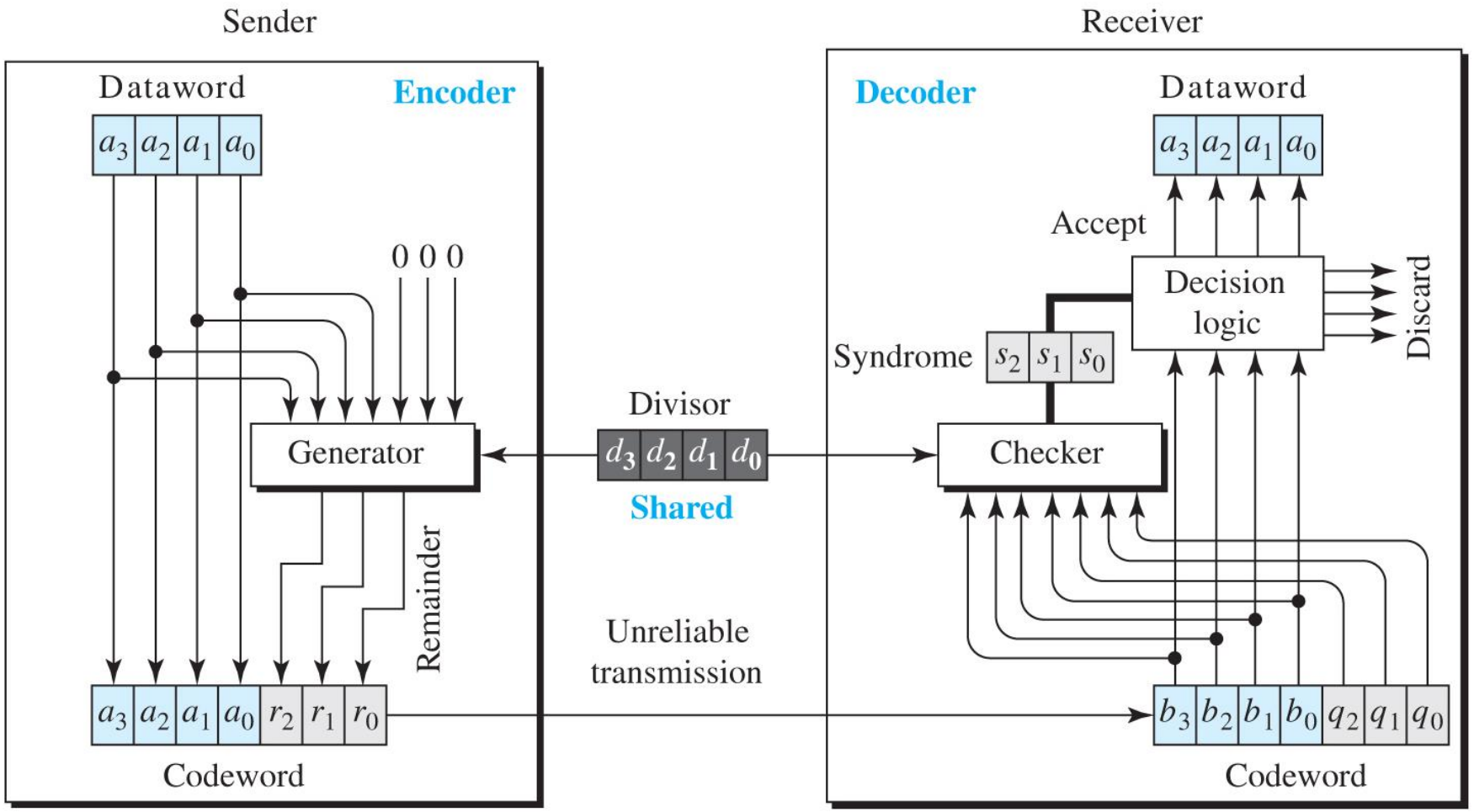
  FCS (frame check sequence)
- The k+n bit is divisible by some predetermined number.
- The receiver divides the total by the predetermined

  number. If no remainder, then the block is fine.

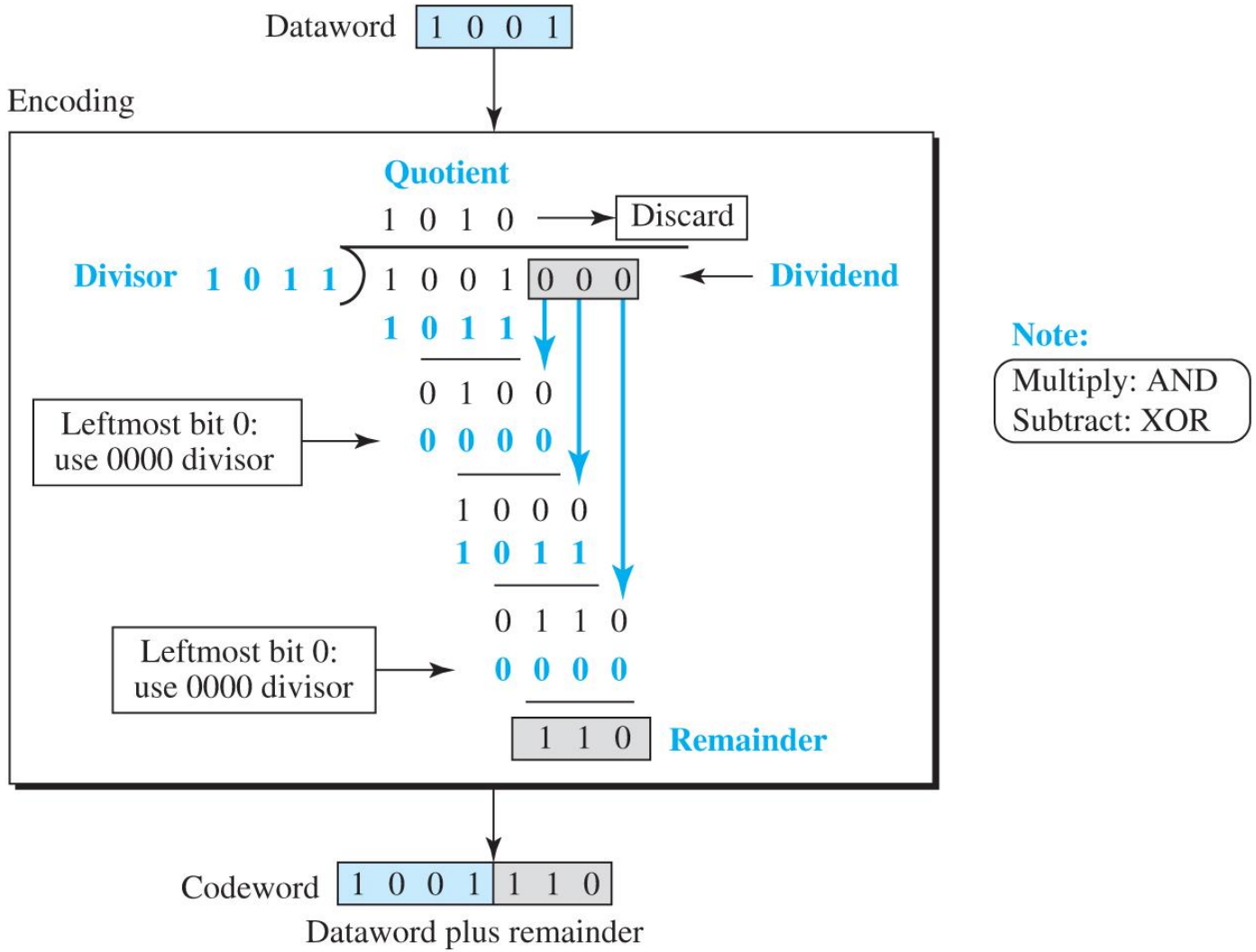
Datawords	*Codewords*	*Datawords*	*Codewords*
0000	**0000000**	1000	**1000101**
0001	**0001011**	1001	**1001110**
0010	**0010110**	1010	**1010011**
0011	**0011101**	1011	**1011000**
0100	**0100111**	1100	**1100010**
0101	**0101100**	1101	**1101001**
0110	**0110001**	1110	**1110100**
0111	**0111010**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

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

CRC encoder and decoder



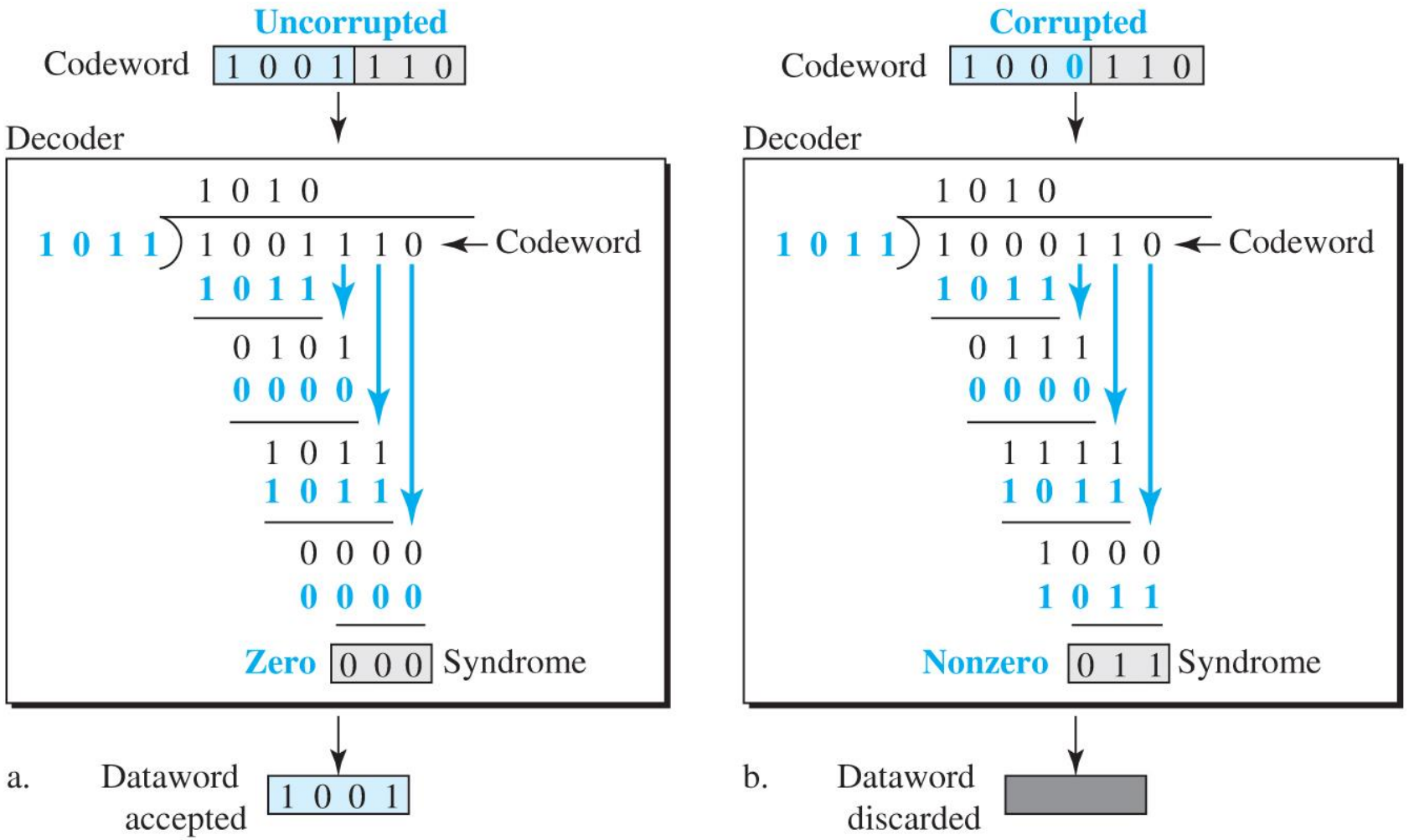
Division in CRC encoder



Note:

Multiply: AND
Subtract: XOR

Division in the CRC decoder for two cases



Standard polynomials

Name	Binary	Application
CRC-8	100000111	ATM header
CRC-10	11000110101	ATM AAL
CRC-16	1000100000100001	HDLC
CRC-32	10000010011000001000111011011011 1	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.

DLC Protocols

DLC Protocols

- 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.

Figure: Normal response mode

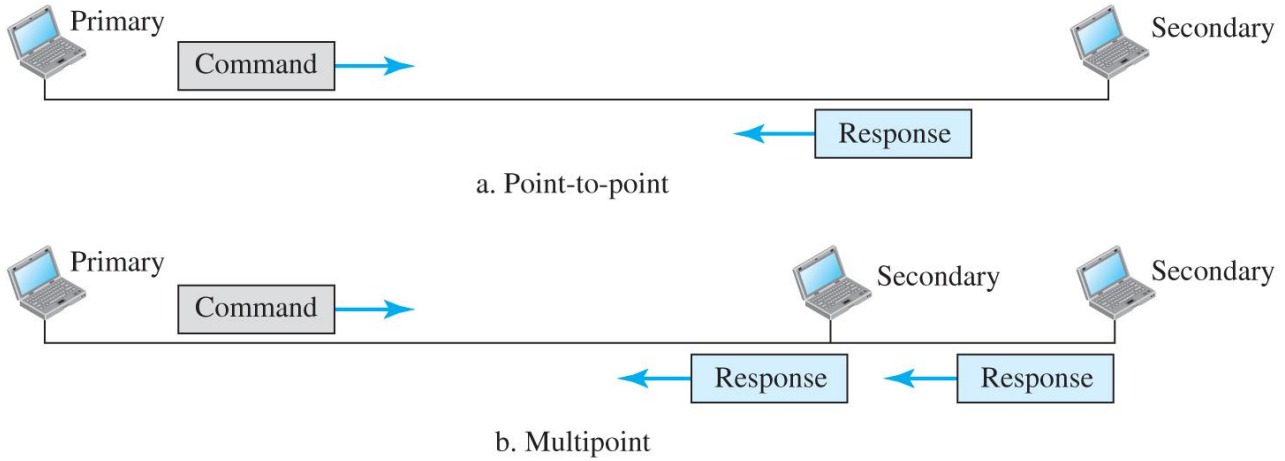
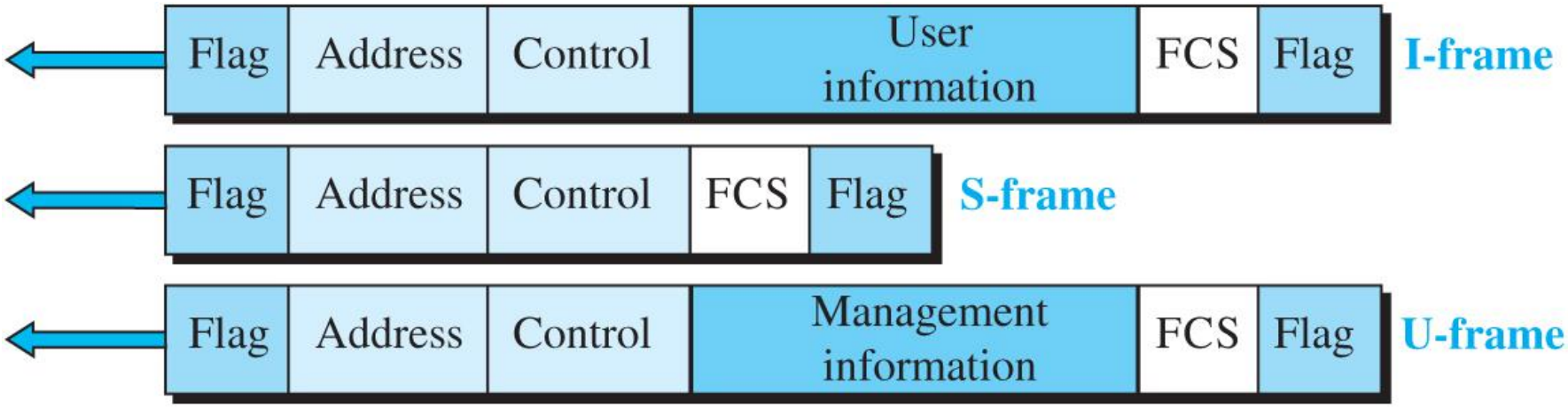
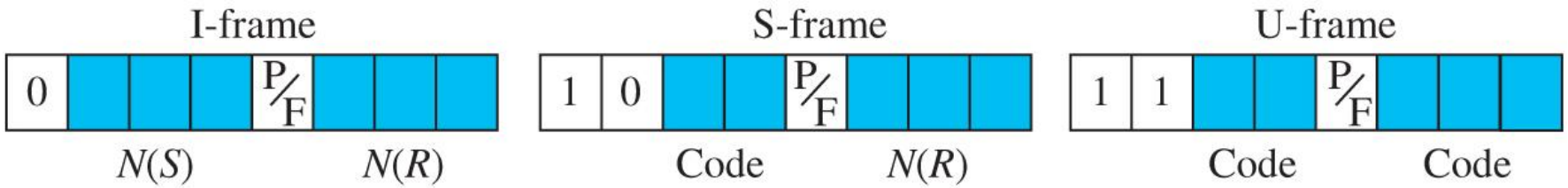


Figure: Asynchronous balanced mode

HDLC frames



Control field format for the different frame types



Point-to-Point Protocol (PPP)

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

Figure: PPP frame format

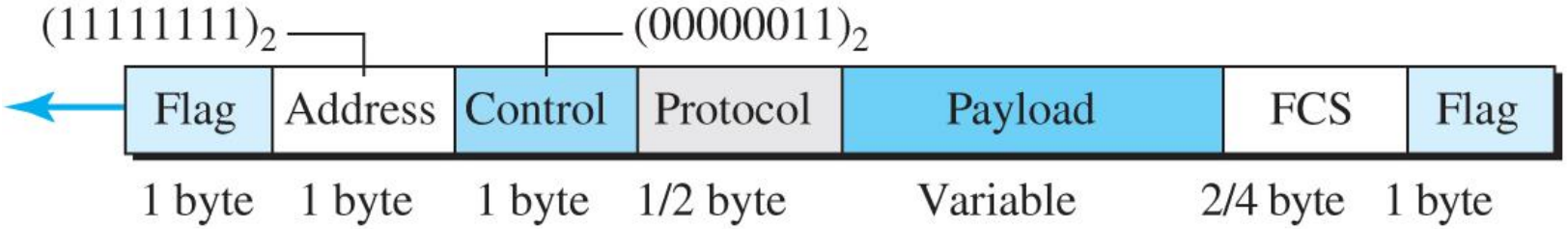
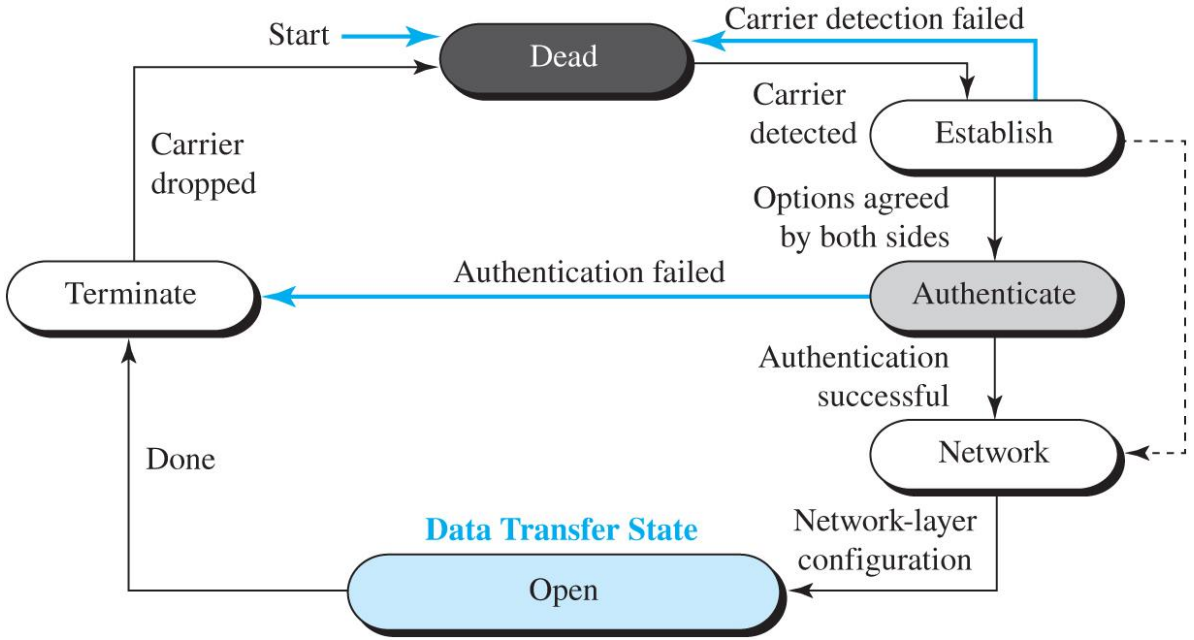


Figure: Transition phases



Point-to-Point Protocol (PPP) - Multiplexing

r.

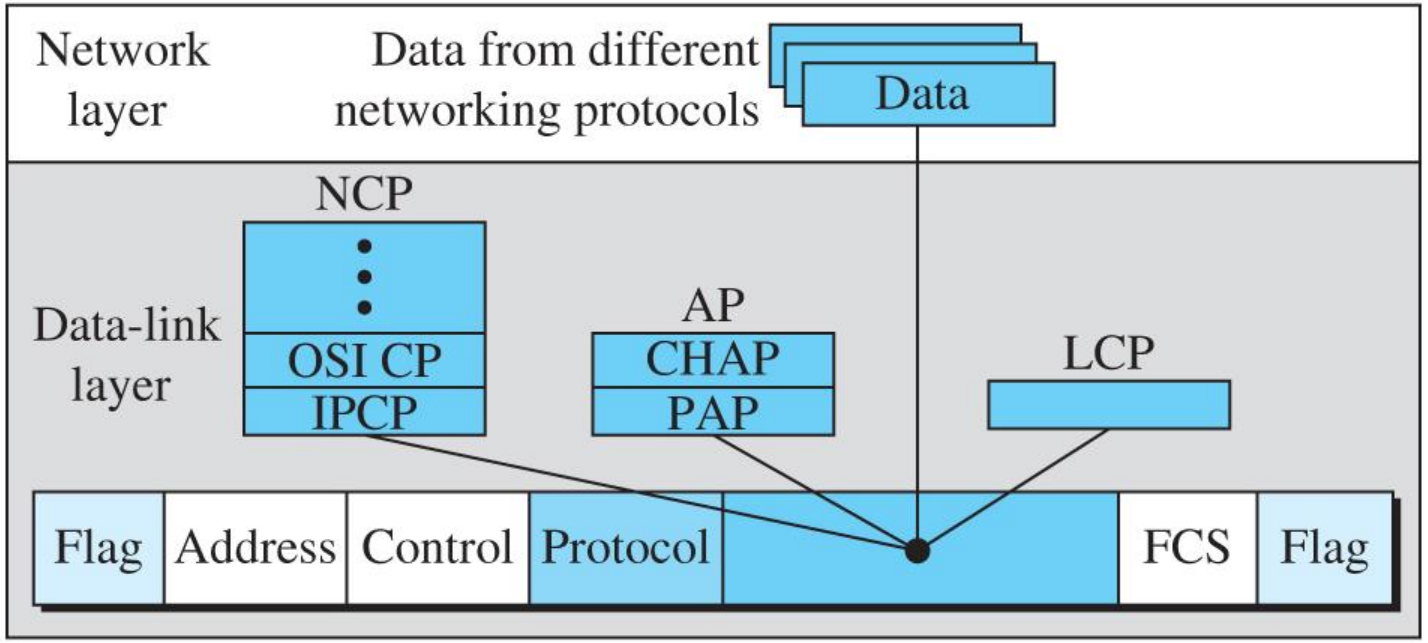
Figure: Multiplexing in PPP

Legend

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

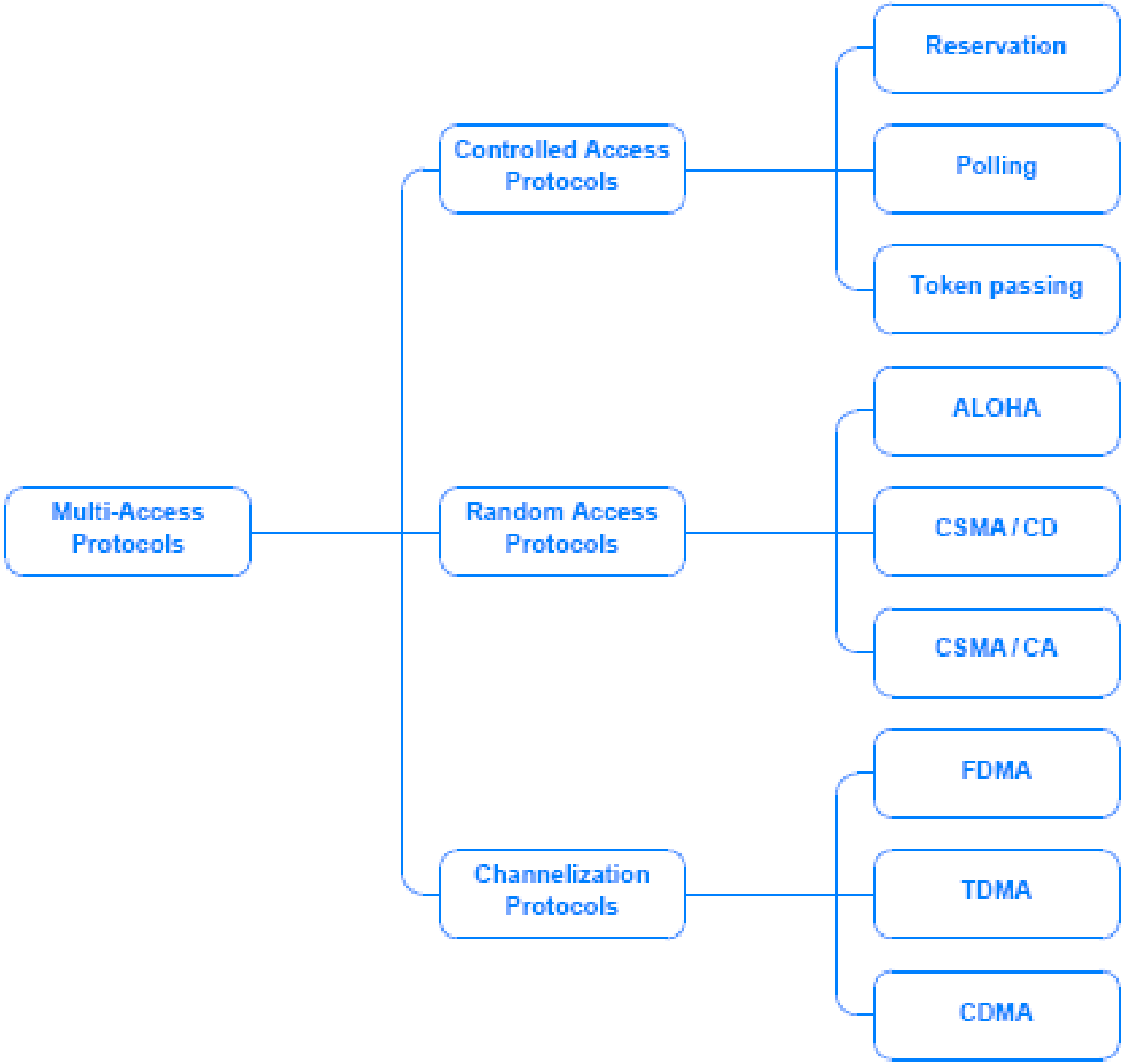
Protocol values:

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



Media Access Protocols

Media Access Protocols



Static and Dynamic Channel Allocation

Static Channel Allocation

- 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.
- Other method are:
  - FDMA
  - TDMA
  - Code Division Multi-Access

Controlled Access Protocols

Controlled Access Protocols

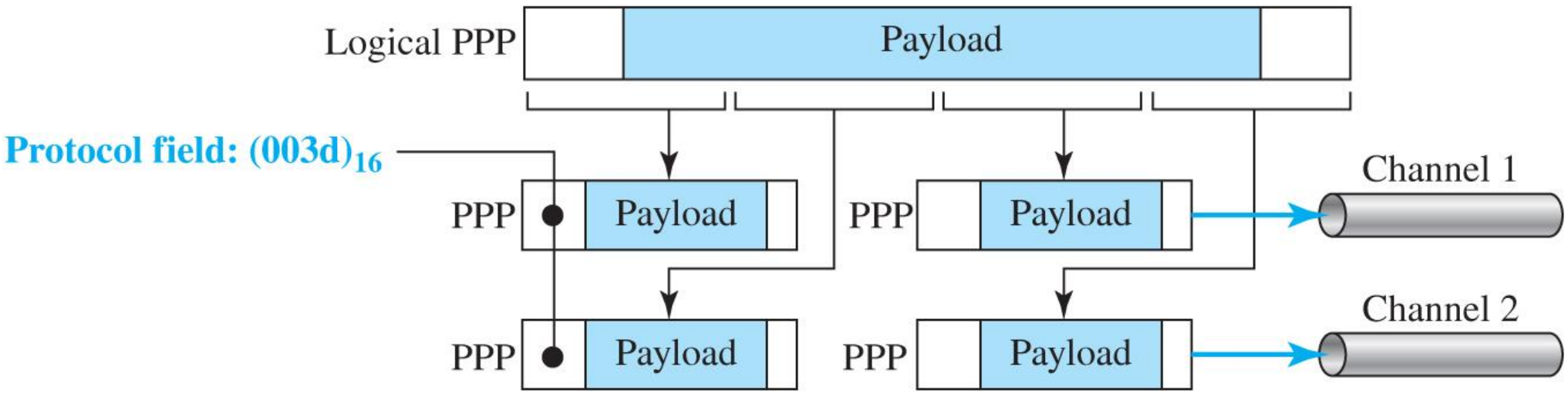
- Polling: A centralized controller cycles through all stations on the network and gives each an opportunity to transmit a packet, either uses round robin order or priority order
- Reservation Collision Free: Often used with satellite transmission, employs a two-step process. Each transmission is planned 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 Countdown:
  - 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

- 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

.

Multilink PPP



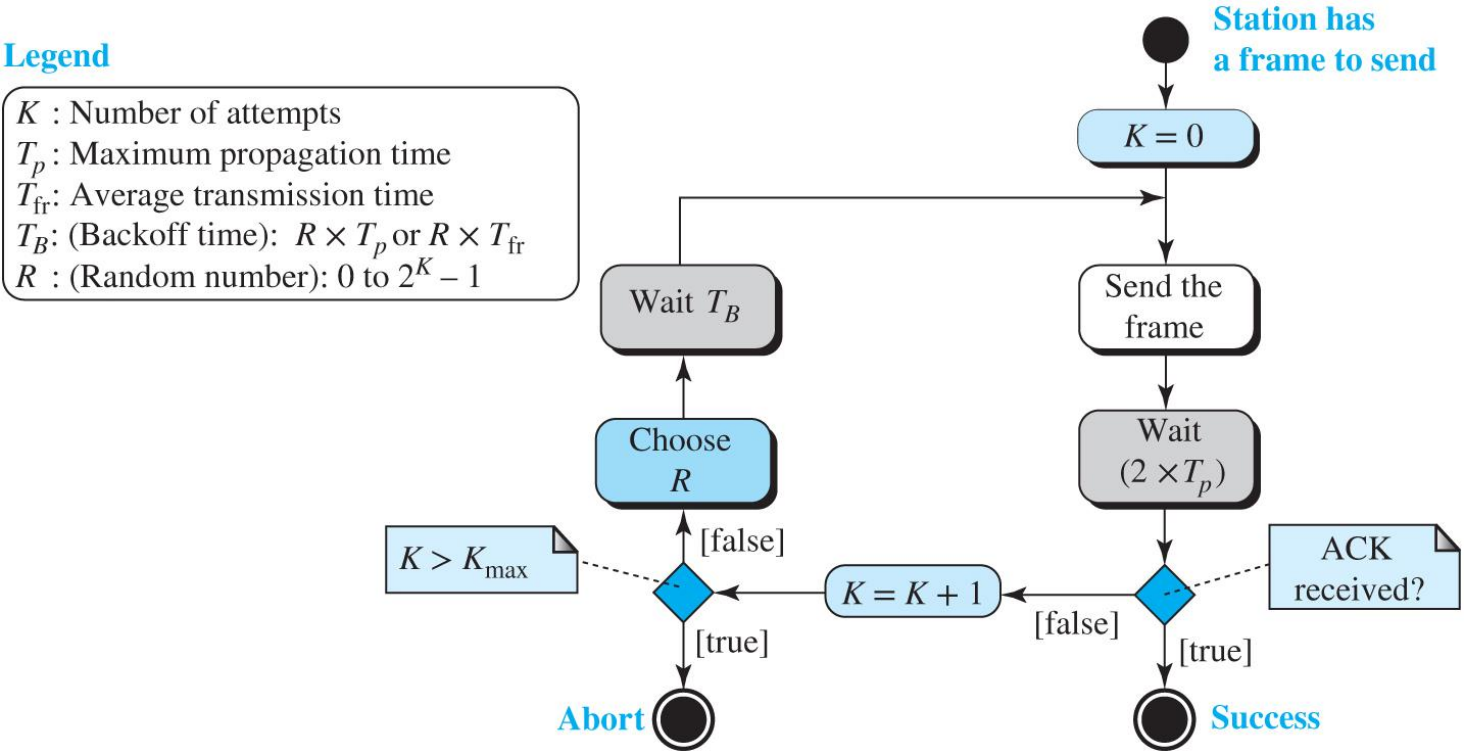
Random Access Methods

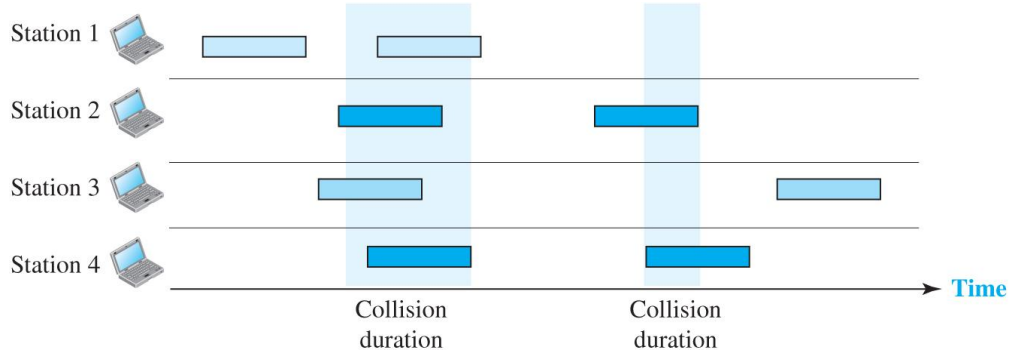
Random Access Methods

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

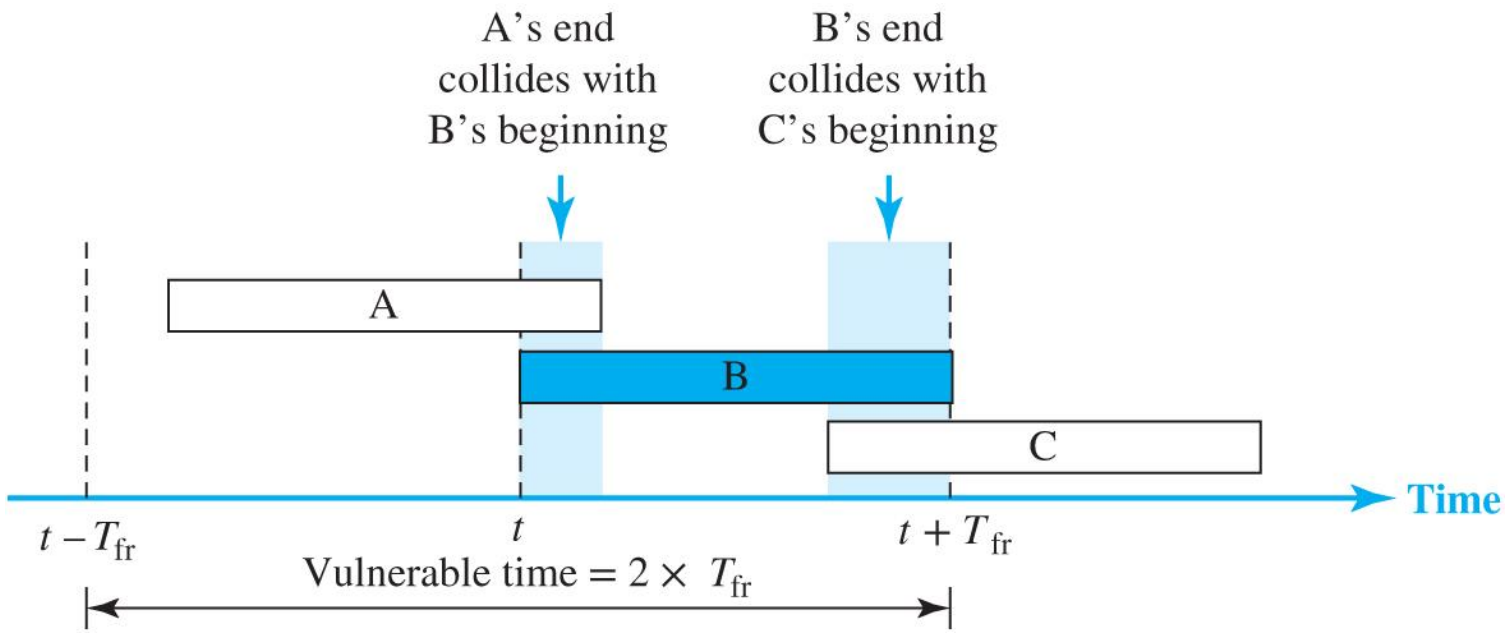




ALOHA – Example 1

- The stations on a wireless ALOHA network are a maximum of 600 km apart.
- If we assume that signals propagate at 3 × 108 m/s, we find Tp = (600 × 103)/(3 × 108) = 2 ms.
- For K = 2, the range of R is {0, 1, 2, 3}.
- This means that TB can be 0, 2, 4, or 6 ms, based on the outcome of the random variable R.

Figure: Vulnerable time for pure ALOHA protocol



ALOHA – Example 2

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

ALOHA – Example 3

- 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 × 0.135 = 135 frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, or 1/2 frames per millisecond, then G = 1/2. In this case S = G × 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 × 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

Slotted ALOHA

Figure: Frames in a slotted ALOHA network

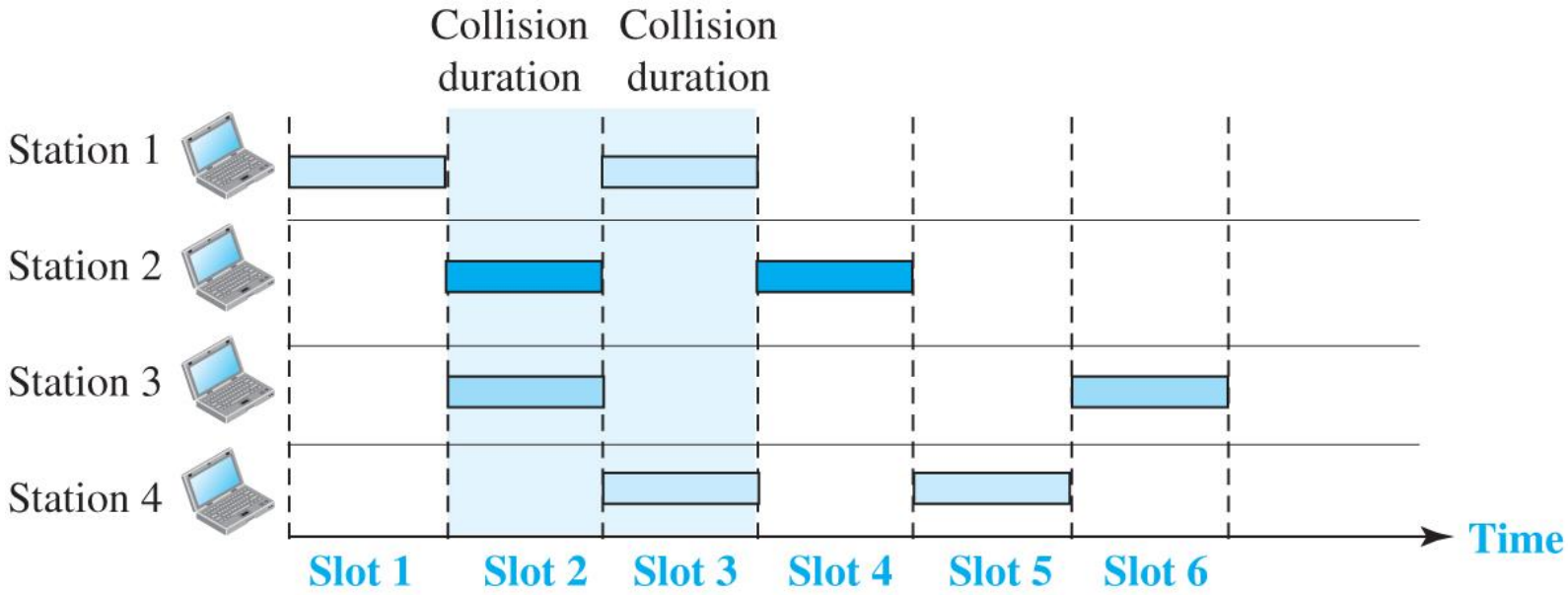
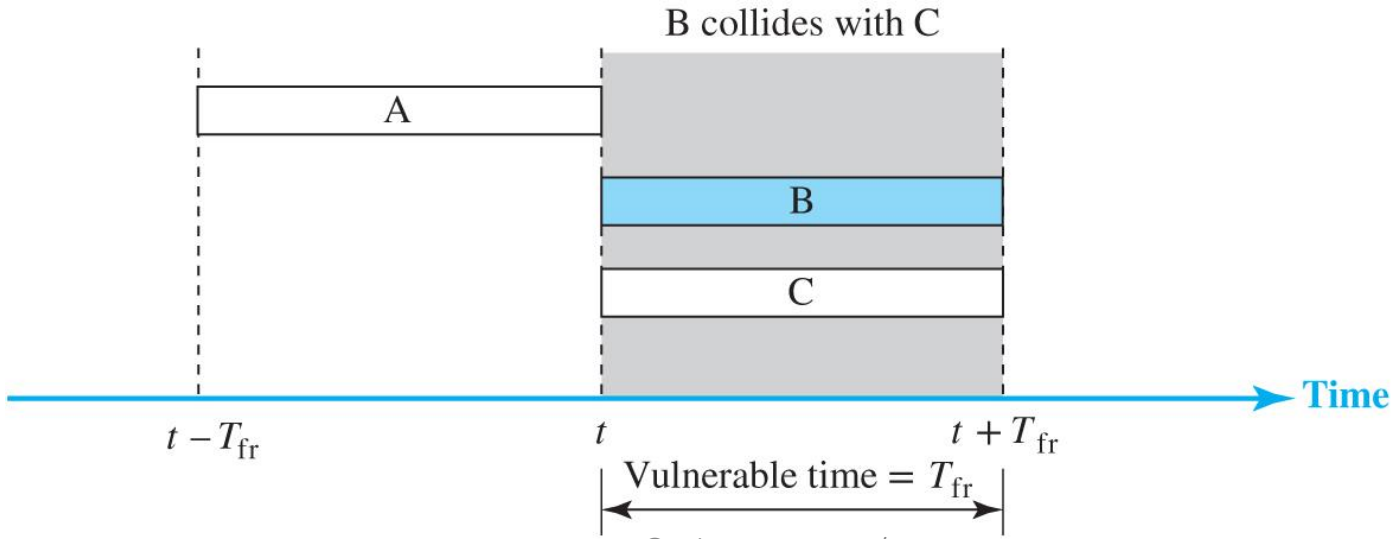


Figure: Vulnerable time for slotted ALOHA protocol



Slotted ALOHA – Example 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.

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.”
- Method
  - Listen for a transmission
  - If the line is clear then transmit
- Implementations:
  - Persistent, Non Persistent and p-persistent
  - CSMA with collision detection

CSMA – 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

CSMA – 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

CSMA – P Persistent

- Slotted channels.
- Listen, if free send at the beginning of the next slot

.

CSMA with Collision Detection

- 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.

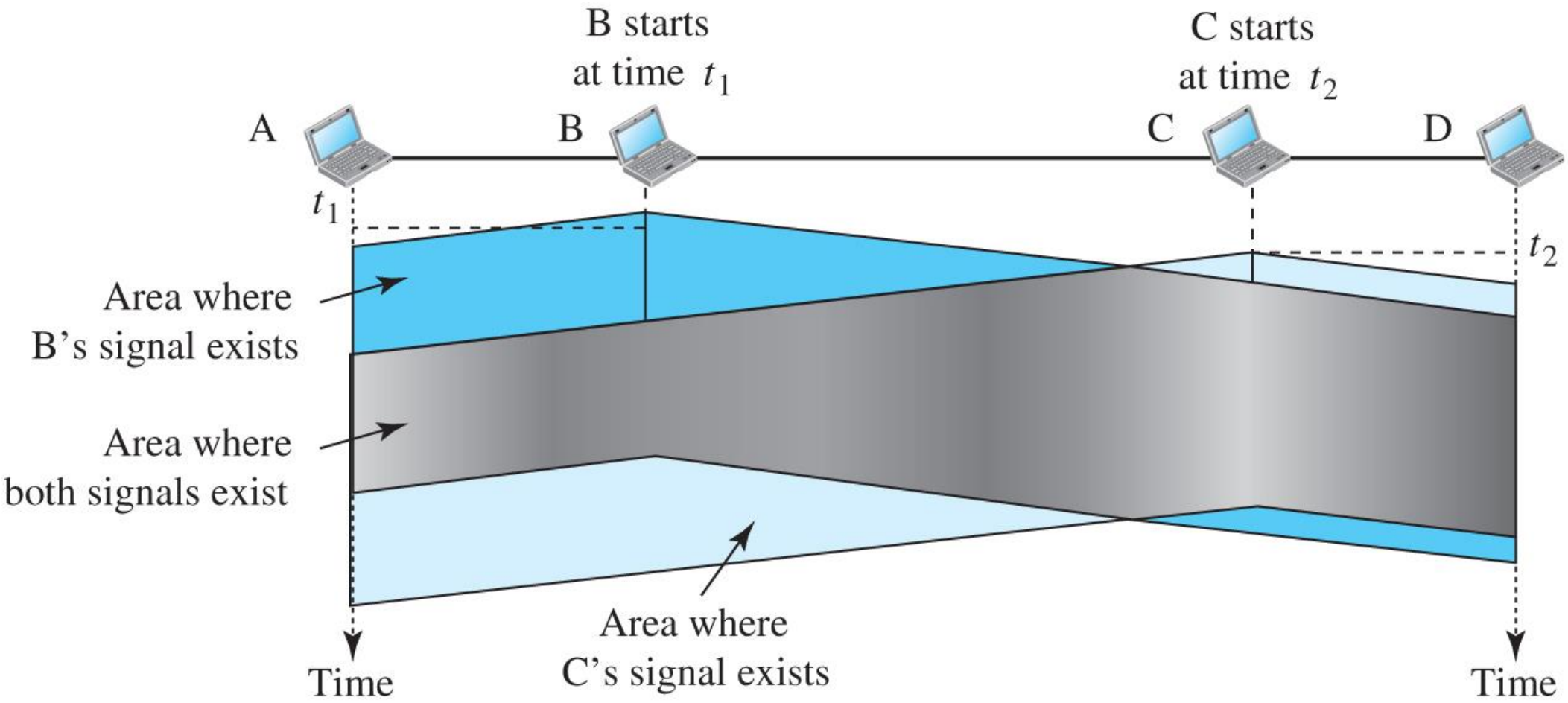
Binary Exponential Back off

- 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

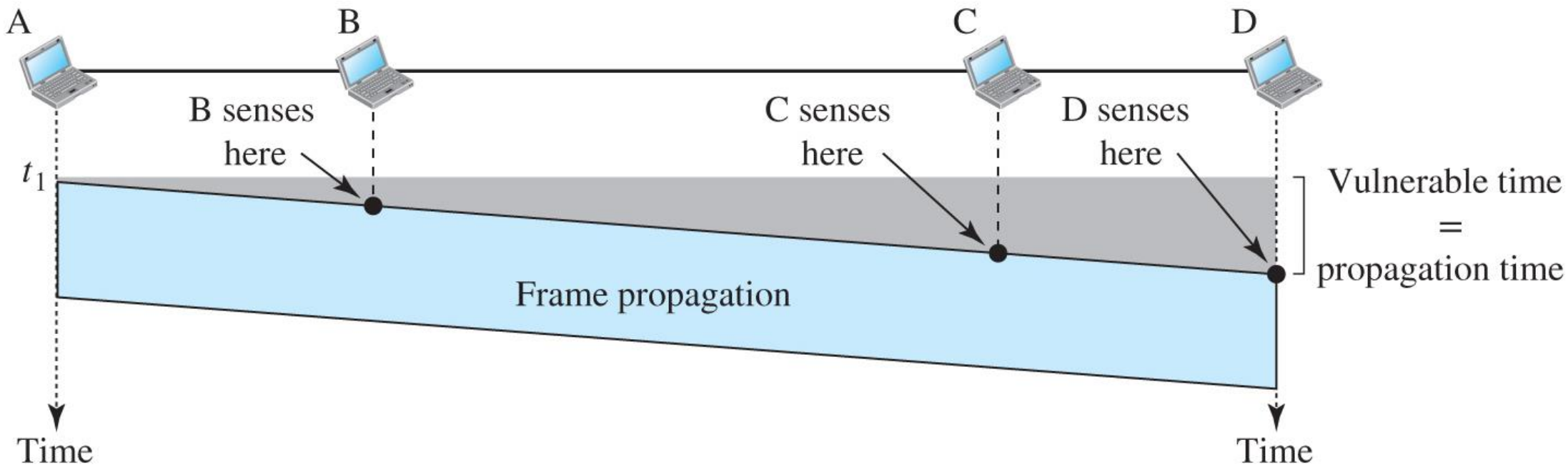
CSMA CA

- 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.

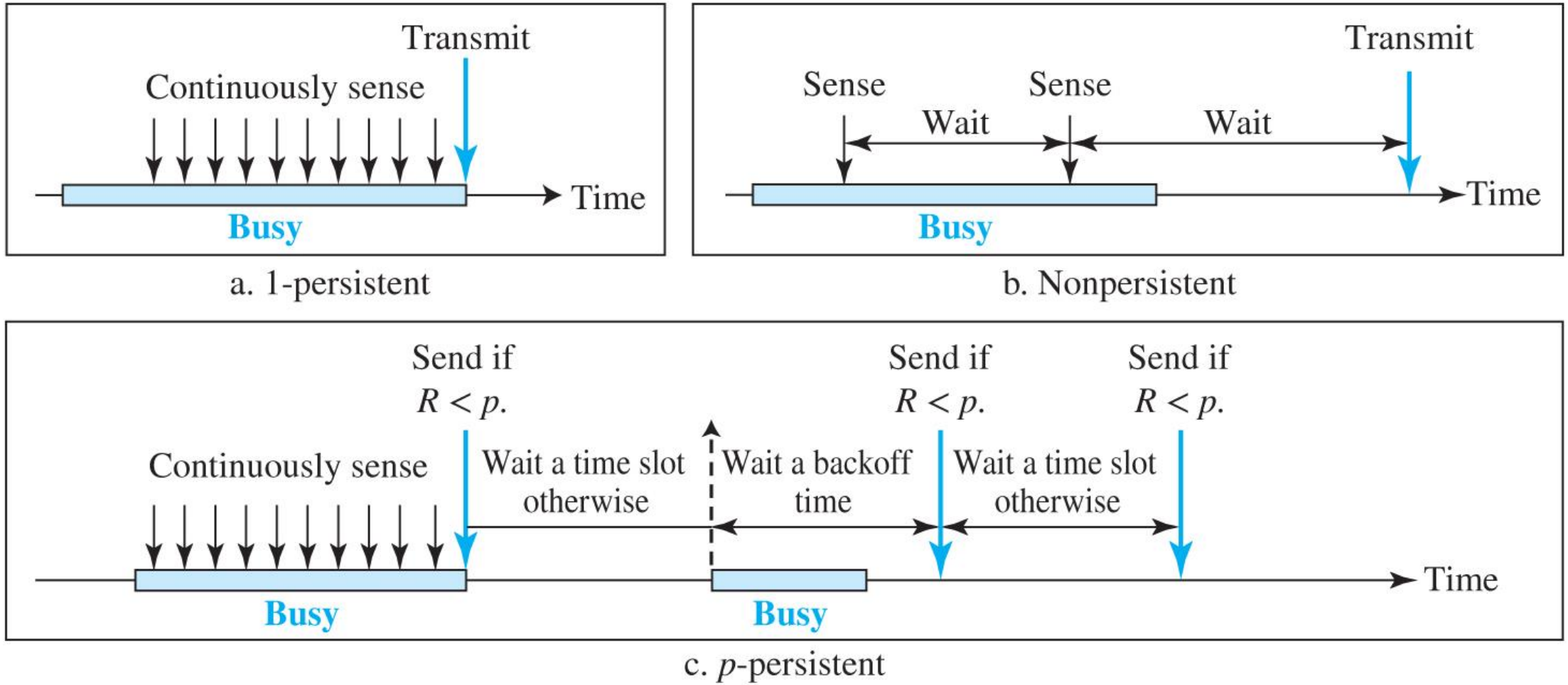
Space and time model of a collision in CSMA



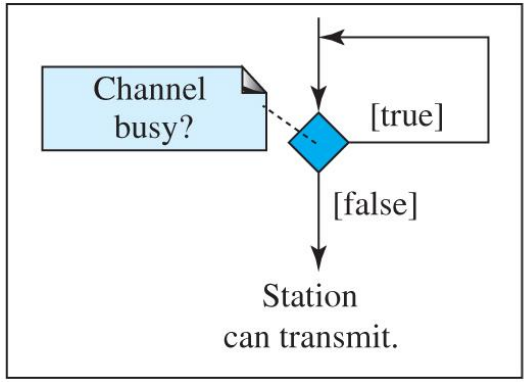
Vulnerable time in CSMA



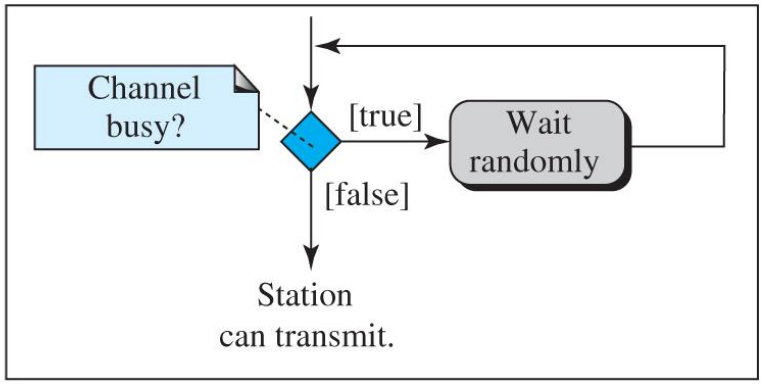
Behavior of three persistence methods



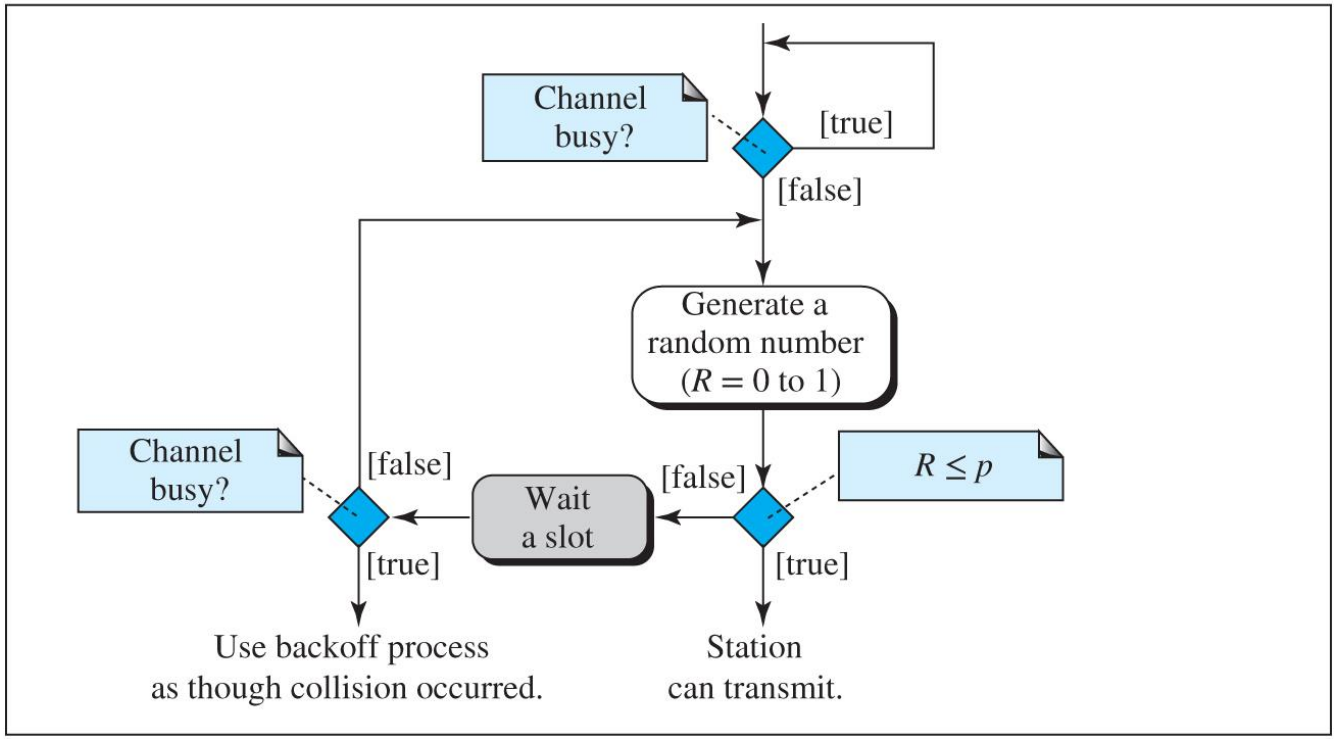
Flow diagram for three persistence methods



a. 1-persistent



b. Nonpersistent

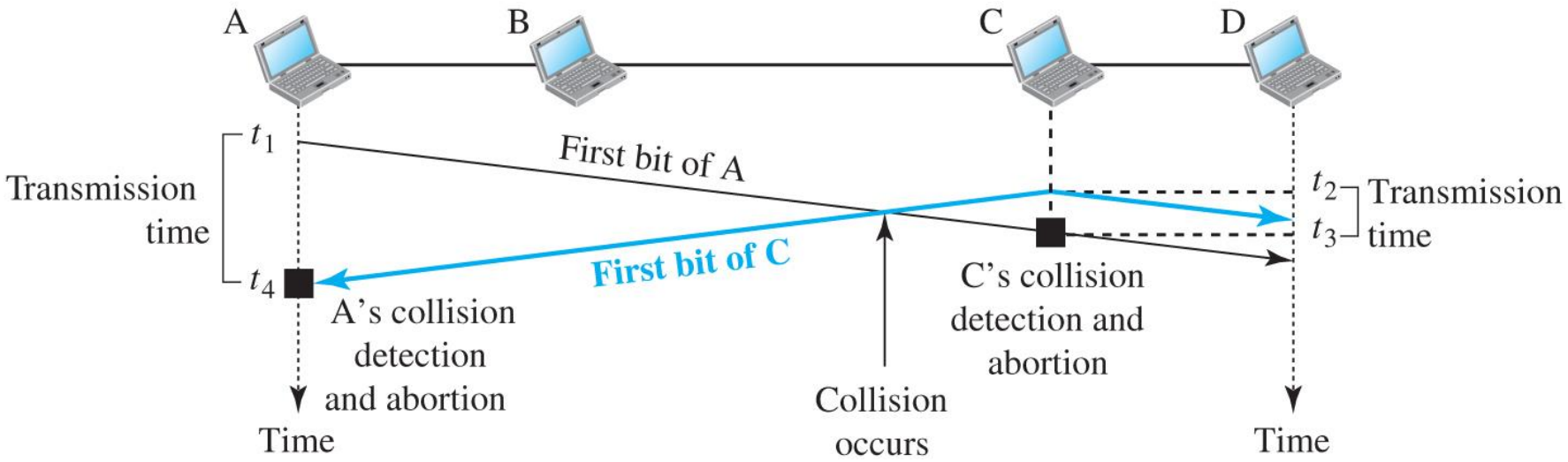


c. *p*-persistent

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

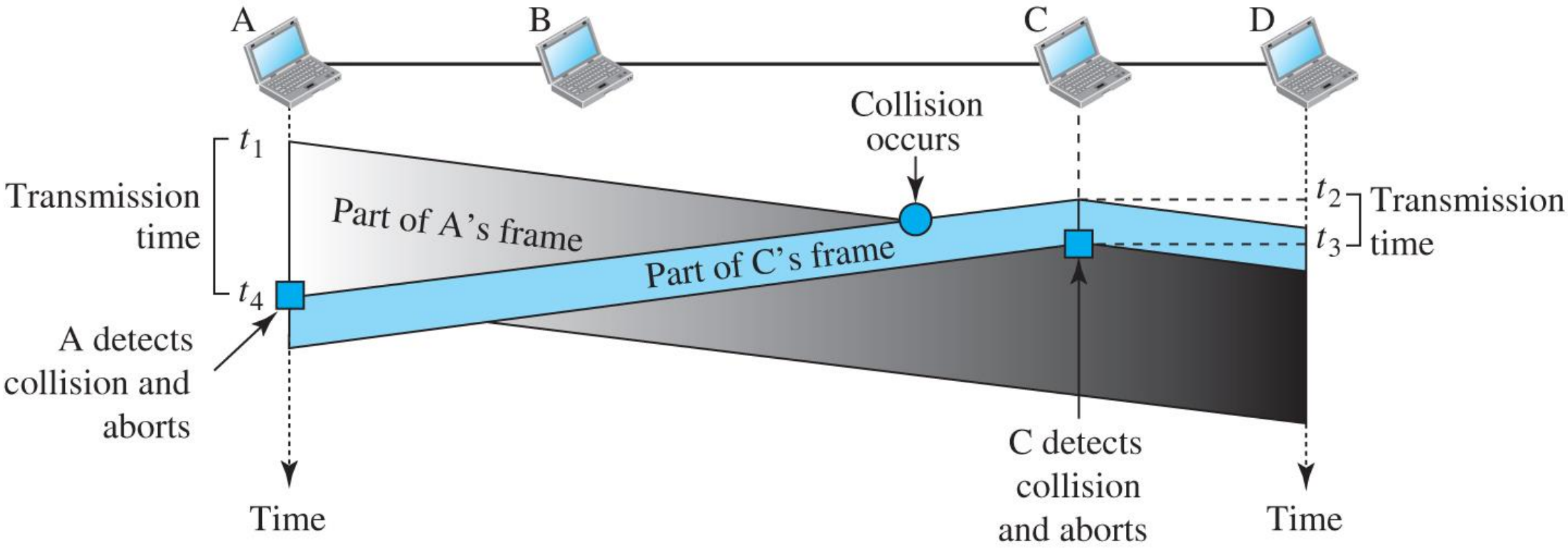
- The CSMA method does not specify the procedure following a collision.
- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.
- If so, the station is finished. If, however, there is a collision, the frame is sent again.

Collision of the first bits in CSMA/CD



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

Collision and abortion in CSMA/CD



CSMA/CD - Example

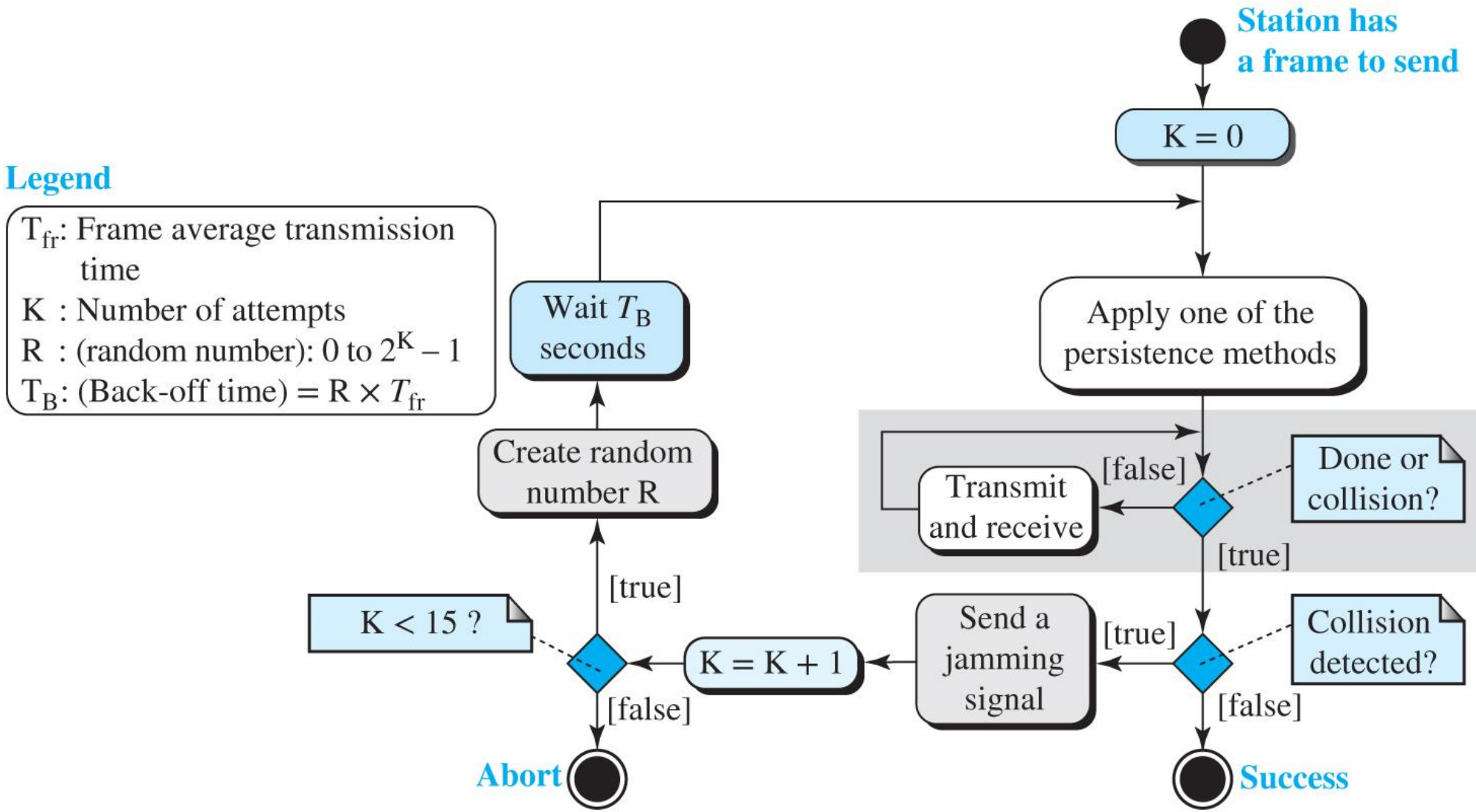
A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time (including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.6 µs, what is the minimum size of the frame?

Solution

The minimum frame transmission time is Tfr = 2 × Tp = 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.

CSMA/CD

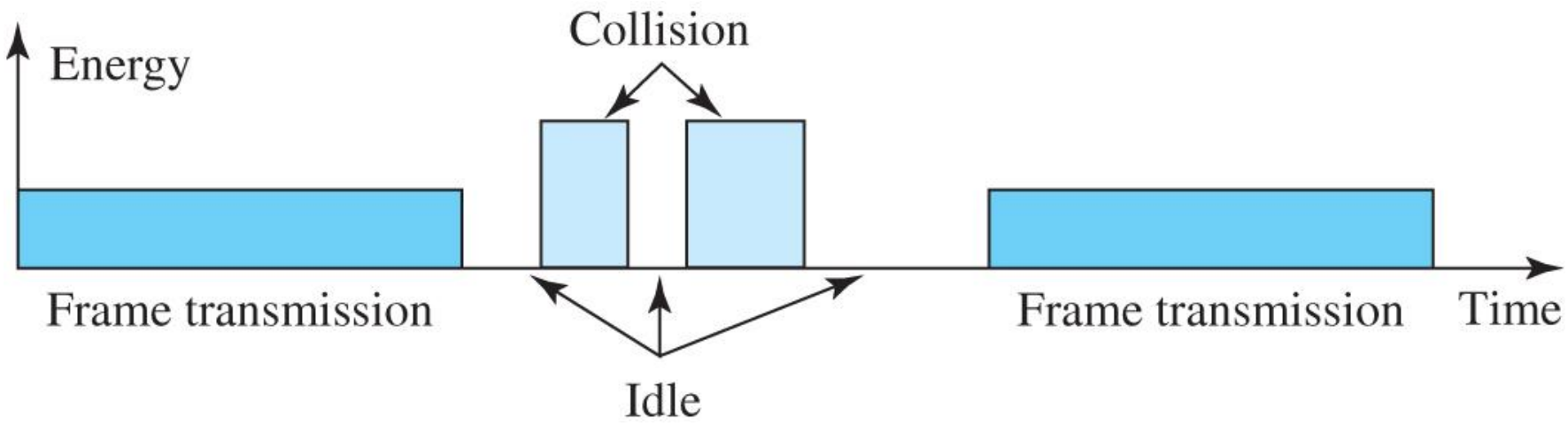
Figure: Flow diagram for the CSMA/CD



CSMA/CD

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

Figure: Energy level during transmission, idleness, or collision



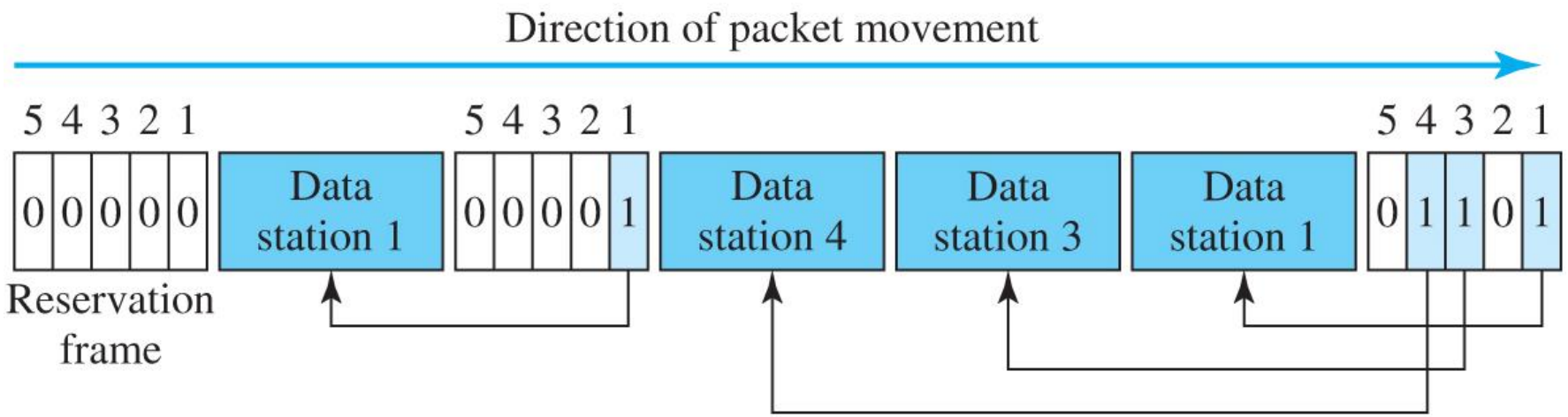
Controlled Access

- 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.

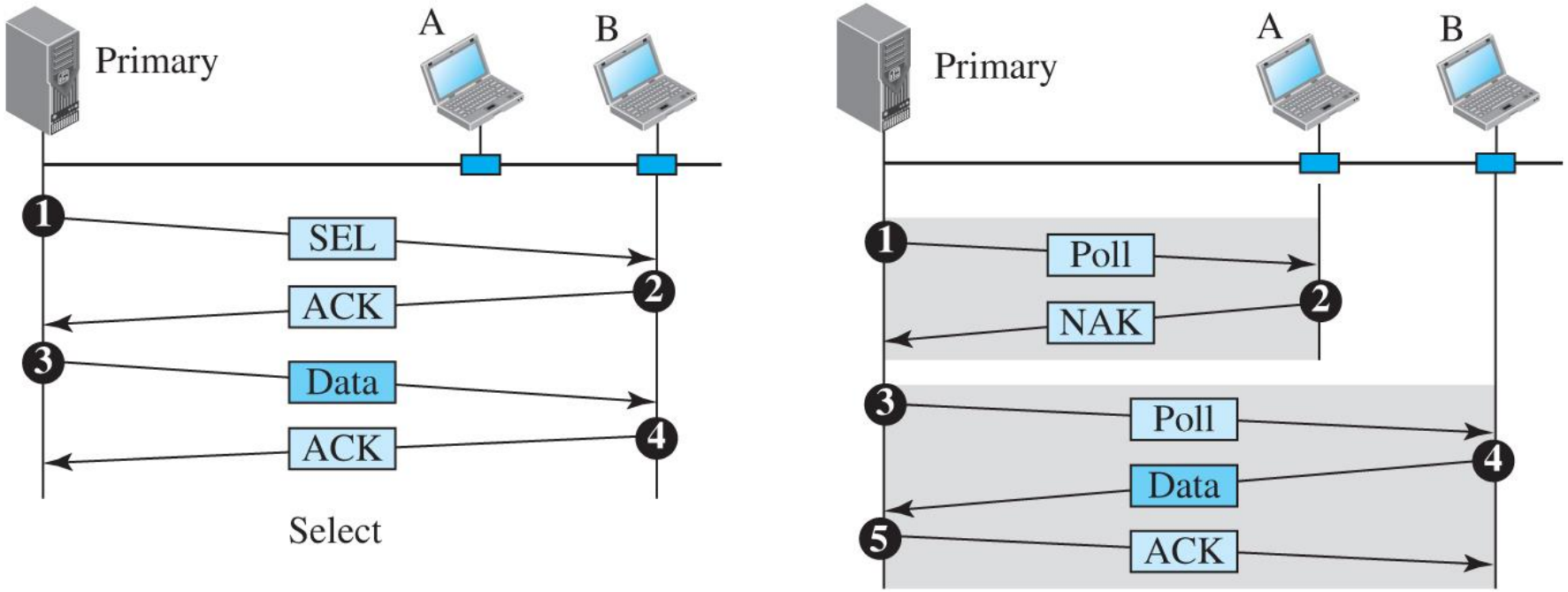
Figure: Reservation access method



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.

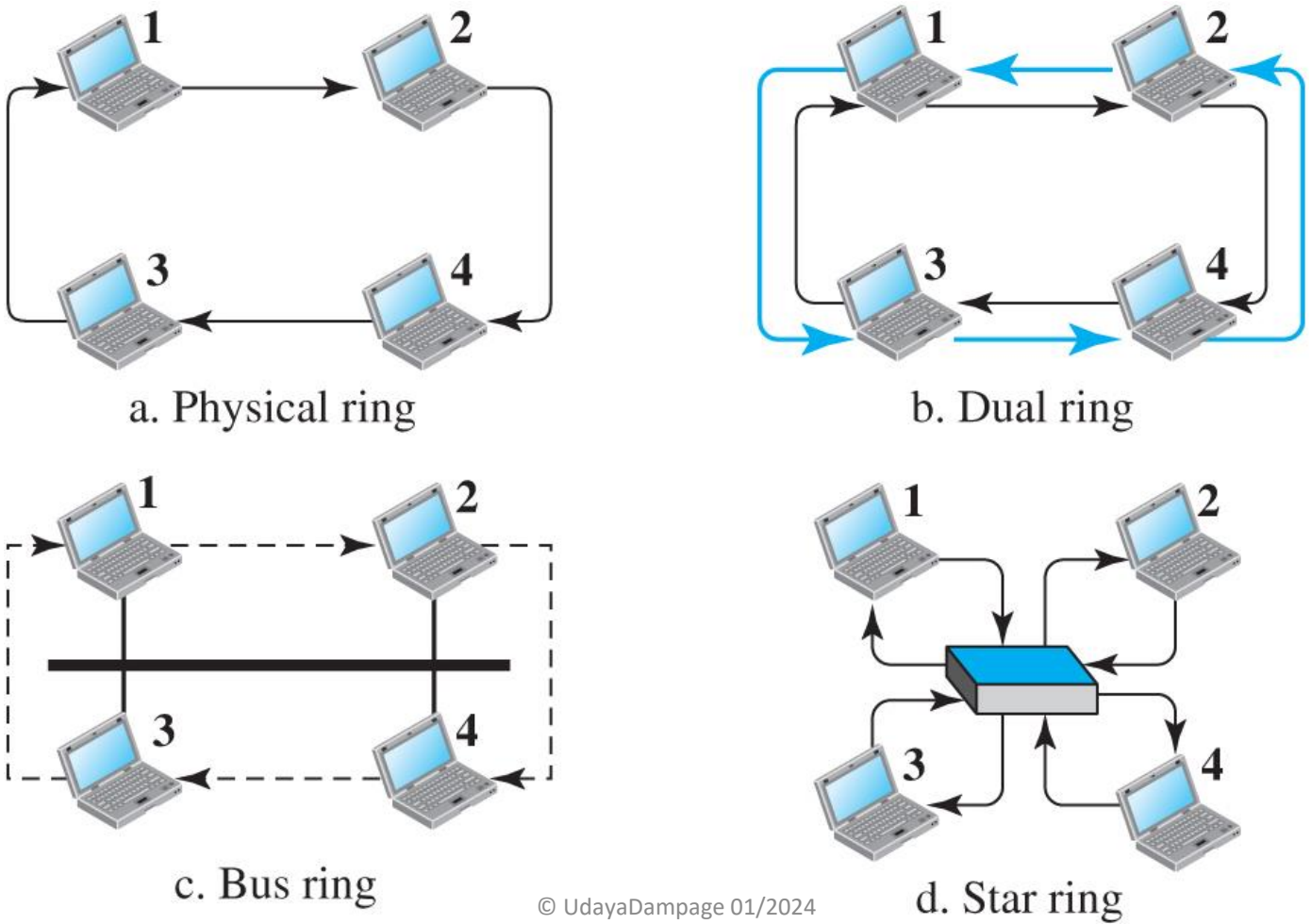
Figure: Select and poll functions in polling-access method



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



Channelization

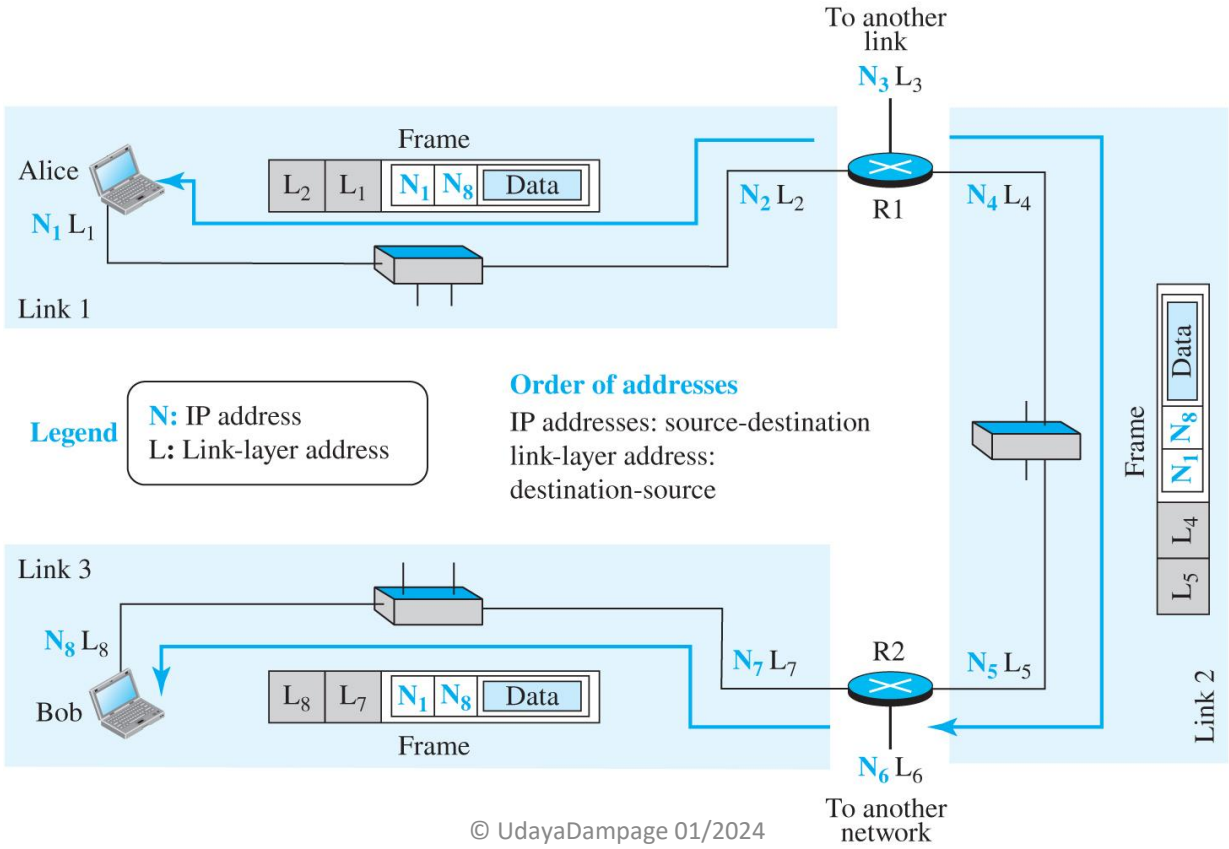
- Channelization (or channel partition, as it is sometimes called) is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, among different stations.
- Since this method is normally used in wireless LAN.

Link Layer Addressing

Link Layer Addressing

- We already discussed 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: IP addresses and link-layer addresses in a small internet



Type of Addresses

- Some link-layer protocols define three types of addresses:
  - Unicast - Each host or interface is assigned a unicast address.
  - Multicast – This means one-to-many communication.
  - Broadcast - A broadcast address means one-to-all address.

.

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**

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

- **FF:FF:FF:FF:FF:FF**

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 already discussed.

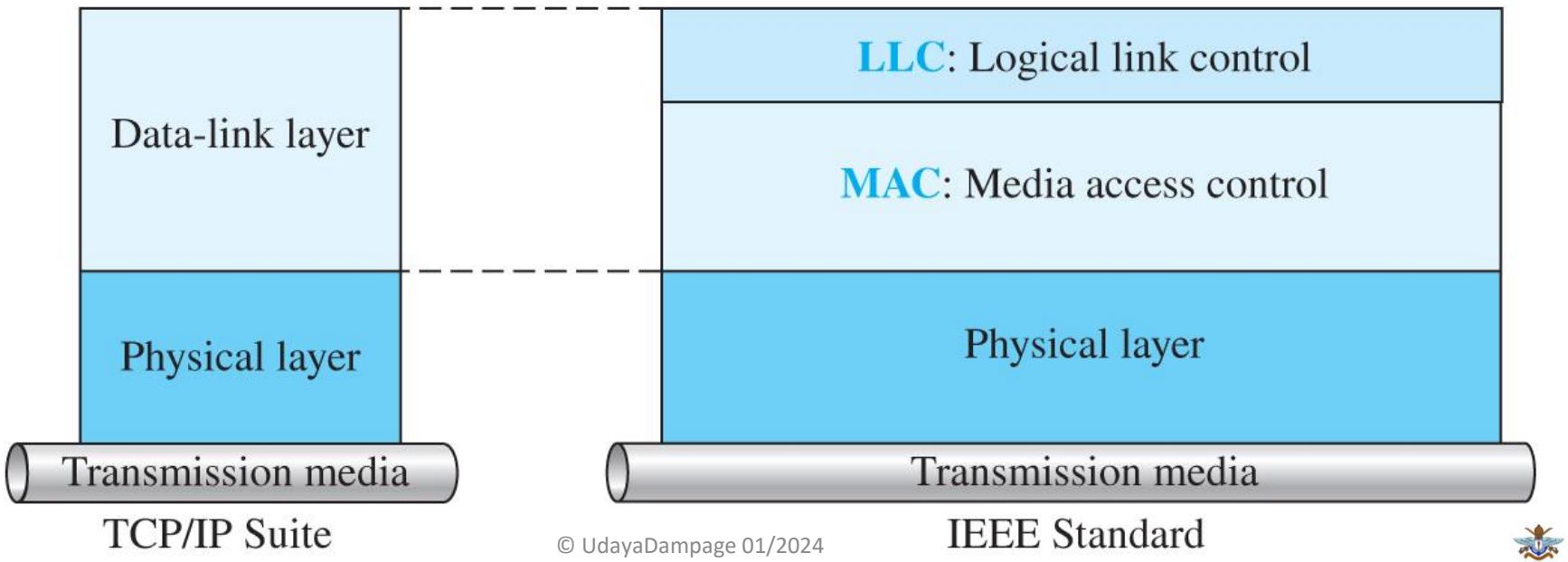
Ethernet

Ethernet

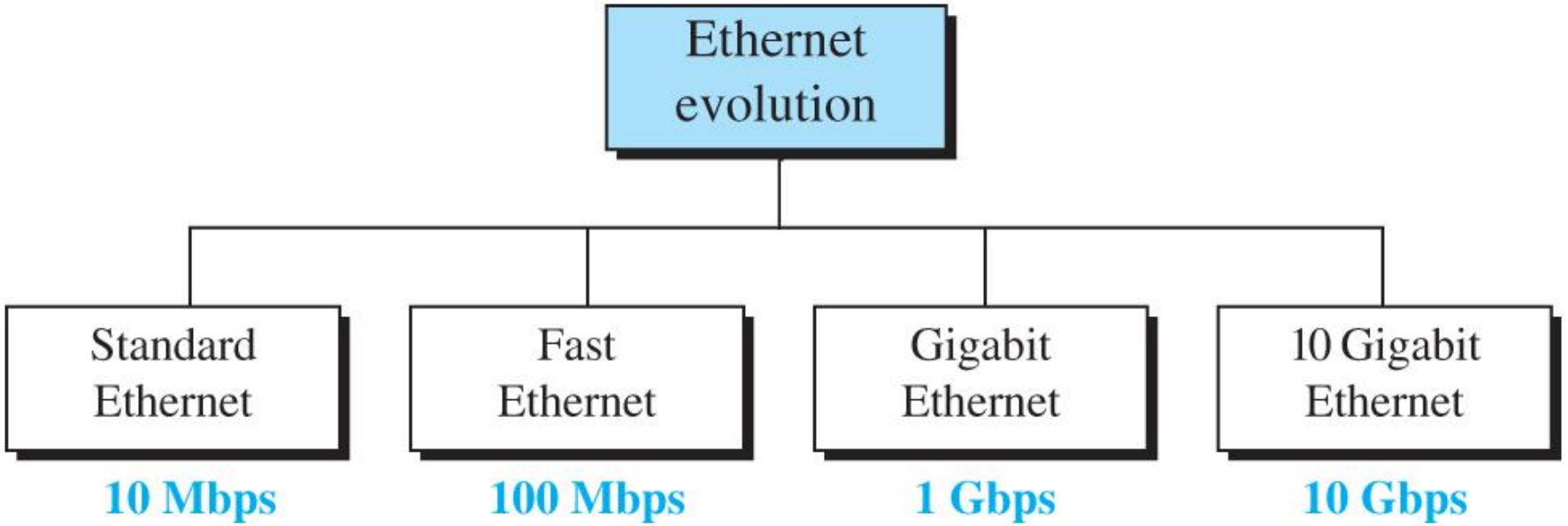
- We already learned that a local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus.
- In the 1980s and 1990s several different types of wired LANs were used. The IEEE has subdivided the data-link layer into two sub-layers: logical link control (LLC) and media access control (MAC).

.

Figure: IEEE standard for LANs

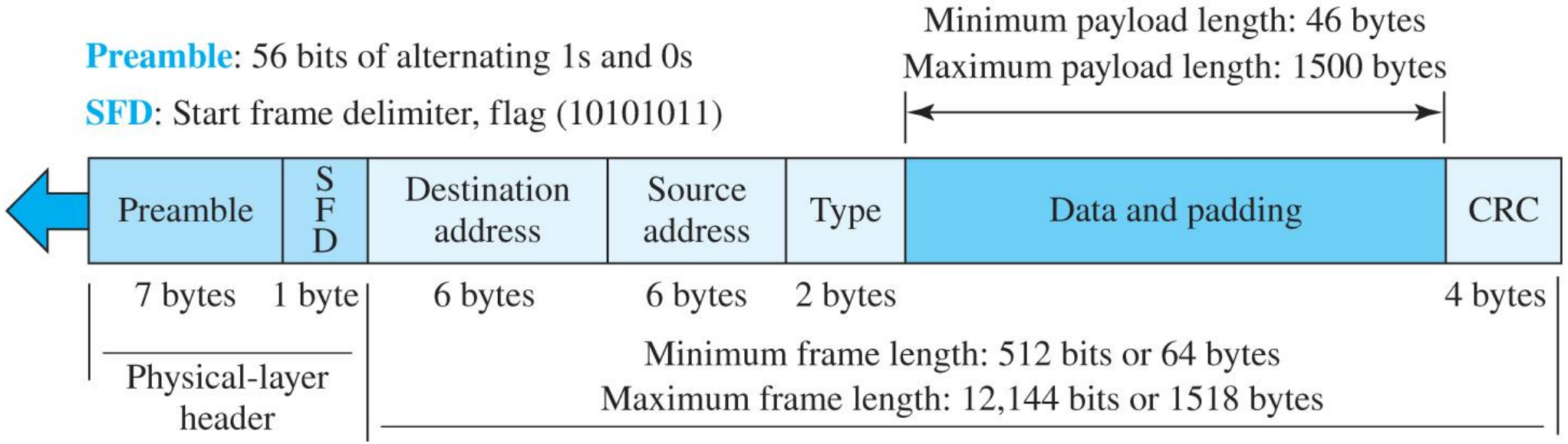


Ethernet evolution through four generations



- We refer to the original Ethernet technology with the 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.
- Ethernet provide a connectionless service, which means that the frames are sent independent of each other.

Ethernet frame format



- Ethernet has imposed restriction on maximum and minimum length to provide correct operation of CSMA/CD.
- An Ethernet frame has minimum length of 64 bytes.
- The maximum length limit is 1518 bytes (without preamble and SFD). This means that maximum payload is 1500 bytes.

Addressing

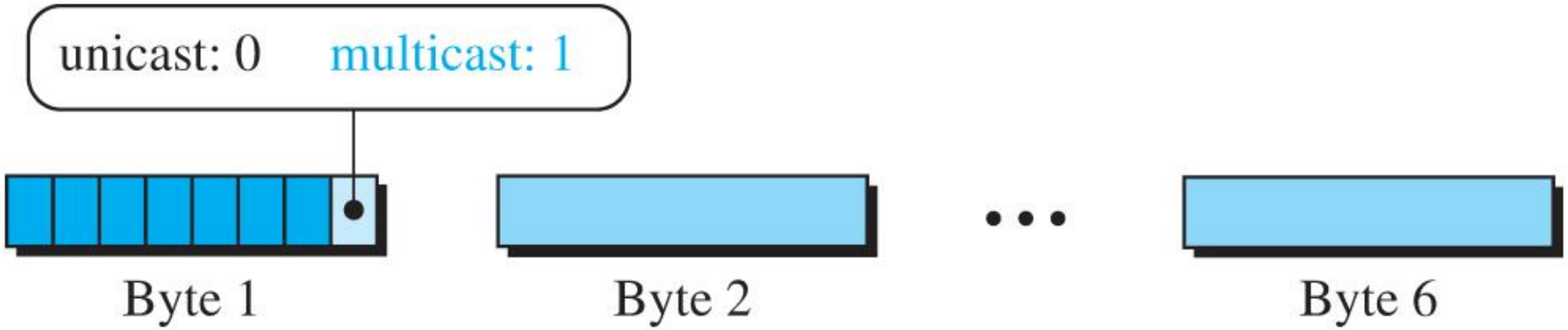
- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC).
- The NIC fits inside the station and provides the station with a link-layer address.
- The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.
- For example, the following shows an Ethernet MAC address.

  • 4A:30:10:21:10:1A

- The way addresses are sent online is different from they way they are written in hexadecimal notation:
- Transmission is left to right, byte by byte; however, for each byte, the least significant bit that defines the address type is sent first.
- The example shows how how the address 47:20:1B:2E:08:EE is sent out online.
- 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**
Binary	01000111	00100000	00011011	00101110	00001000	11101110
Transmitted ←	11100010	00000100	11011000	01110100	00010000	01110111

Unicast and multicast addresses



Define the type of the following destination addresses:

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

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

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

Solution

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

Summary of Standard Ethernet implementations

Implementation	*Medium*	*Medium Length(m)*	*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

Fast Ethernet

- In the 1990s, Ethernet made a big jump by increasing the transmission rate to 100 Mbps, and the new generation was called the Fast Ethernet.
- The designers of the Fast Ethernet needed to make it compatible with the Standard Ethernet.
- The MAC sublayer was left unchanged. But the features of the Standard Ethernet that depend on the transmission rate, had to be changed.

Access Method

- We remember that the proper operation of the CSMA/CD depends on the transmission rate, the minimum size of the frame, and the maximum network length.
- If we want to keep the minimum size of the frame, the maximum length of the network should be changed.
- In other words, if the minimum frame size is still 512 bits, and it is transmitted 10 times faster, the collision needs to be detected 10 times sooner, which means the maximum length of the network should be 10 times shorter (the propagation speed does not change).
- A new feature added to Fast Ethernet is auto-negotiation. It allows two station to negotiate the mode or data rate of transmission.

Physical Layer

- To be able to handle a 100 Mbps data rate, several changes need to be made at the physical layer.
- Fast Ethernet implementation at the physical layer can be categorized as either two-wire or four-wire.
- The two-wire implementation can be either shielded twisted pair (STP), which is called 100Base-TX, or fiber-optic cable, which is called 100Base-FX.
- The four-wire implementation is designed only for unshielded twisted pair (UTP), which is called 100Base-T4.
- Table is a summary of the Fast Ethernet implementations

Implementation	*Medium*	*Medium Length*	*Wires*	*Encoding*
100Base-TX	STP	100 m	2	4B/5B + MLT-3
100Base-FX	Fiber	185 m	2	4B/5B + NRZ-I
100Base-T4	UTP	100 m	4	Two 8B/6T

Gigabit Ethernet (1000 Mbps)

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps).
- The IEEE committee calls it 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
  - A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched.
  - However, to achieve a data rate of 1 Gbps, this was no longer possible.
  - Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex.
  - Almost all implementations of Gigabit Ethernet follow the full-duplex approach, so we mostly ignore the half-duplex mode

Gigabit Ethernet

- In the full duplex mode, there is a central switch connected to all computers. There is no collision in this mode.
- In half duplex mode, a switch can be replaced by a hub.
- The physical layer in Gigabit Ethernet is more complex that the other version. We have different implementations.

Implementation	*Medium*	*Medium Length(m)*	*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	2	4D-PAM5

- 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

Gigabit Ethernet

- 10 Gigabit Ethernet operates only in full-duplex mode, which means there is no need for contention; CSMA/CD is not used in 10 Gigabit Ethernet.
- Four implementations are the most common: 10GBase-SR, 10GBase-LR, 10GBase-EW, and 10GBase-X4. Table shows a summary of the 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

References

1. Nevio Benvenuto and Michele Zorzi, (2011). Principles of Communications Networks and Systems, John Wiley.

2. Thomas Robertazzi, (2011). Basics of Computer Networking (Springer Briefs in Electrical and Computer Engineering), Springer

3. Behrouz A. Forouzan (2022). Data Communications and Networking, With TCP/IP protocol suite, Sixth Edition, McGrew Hill.