Chapter 3
Principles of Computer Communications

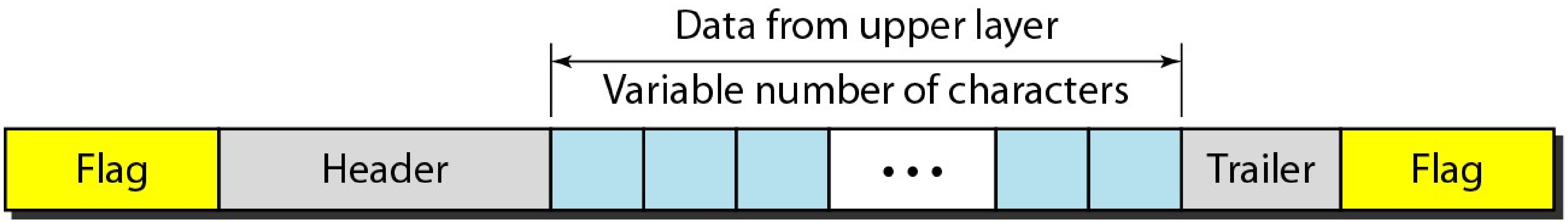
Data Link Layer

Data Link Layer

- The data link layer combines the following 3 functions to achieve the delivery of data from one node to another.
  - Framing
  - Error control
  - Flow control

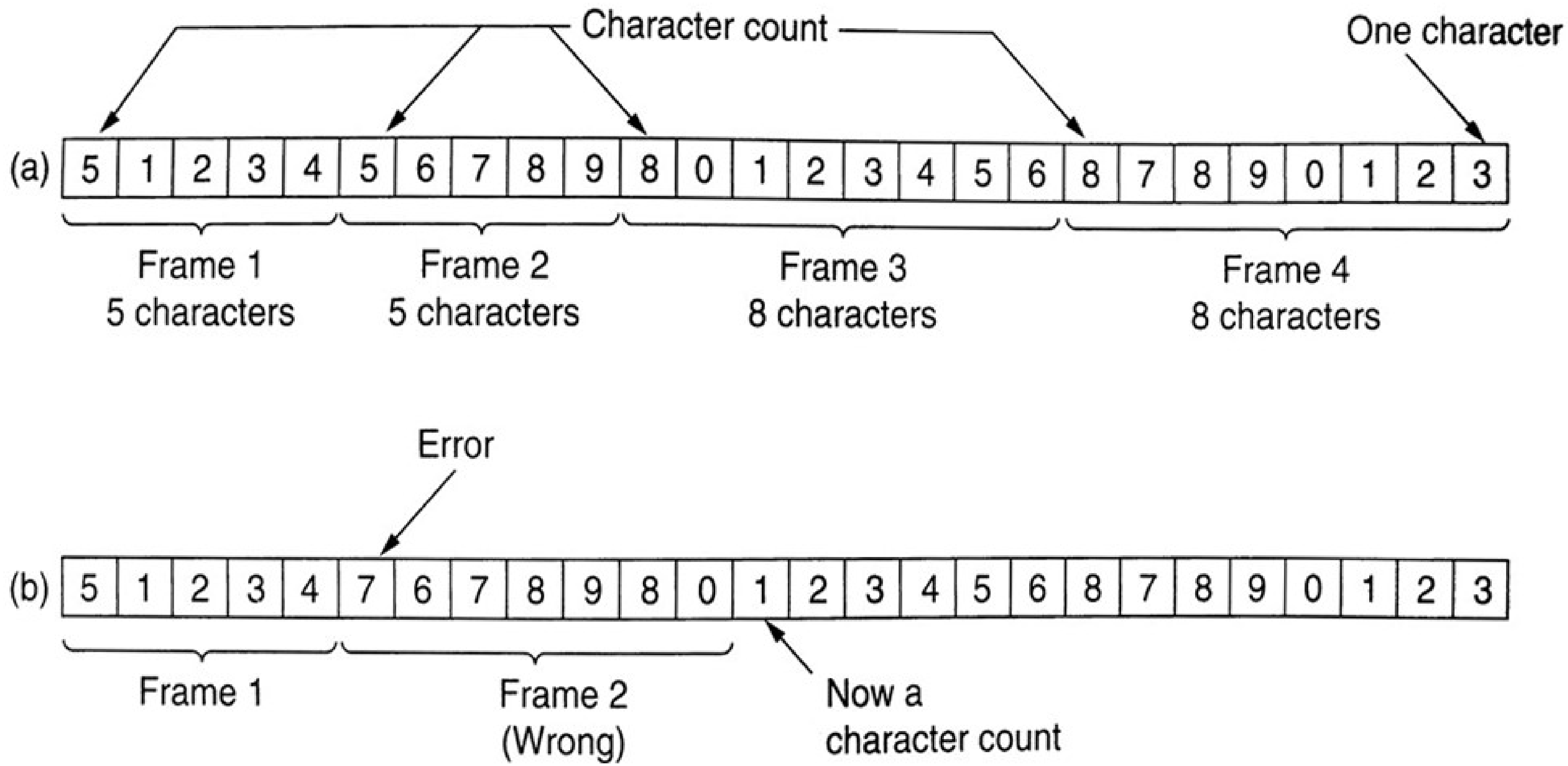
Framing

- The data link layer needs to pack bits into frames, so that each frame is distinguishable from another.
- The 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.
- To break the bit stream up into frames, some common methods are used.



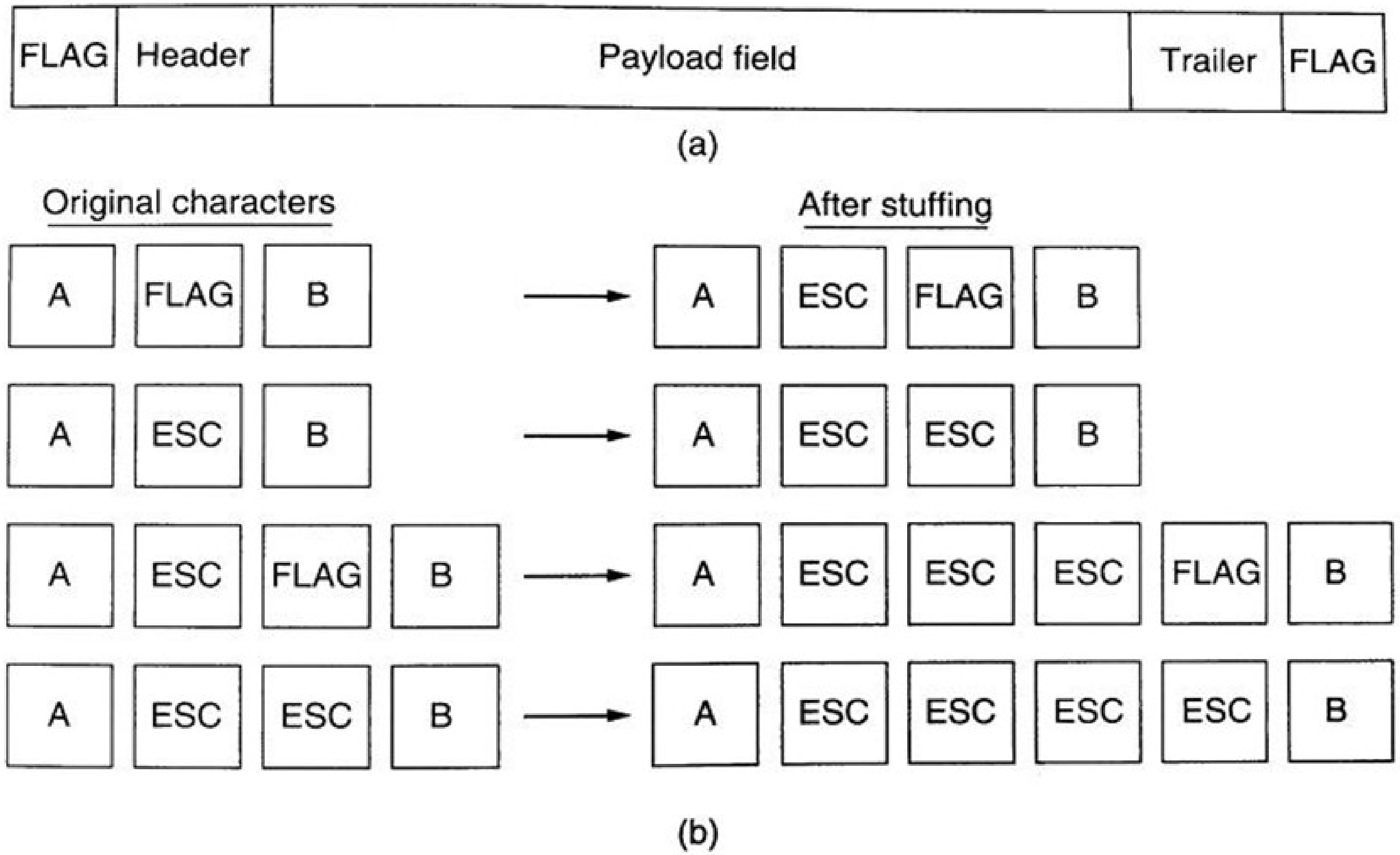
Framing: Character count

- Use a field in the header to specify the number of the characters in the frame.



Framing: Flag bytes with byte stuffing

- Each frame starts and ends with special bytes.
- If the flag byte's bit pattern occurs in that data, a special escape byte (ESC) will be inserted just before the bit pattern.



Framing: Starting and ending flags with bit stuffing

- Each frame begins and ends with a special bit pattern, 01111110.
- If the sender encounters five consecutive 1s in the data, a 0 bit will be inserted just after 1s.

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

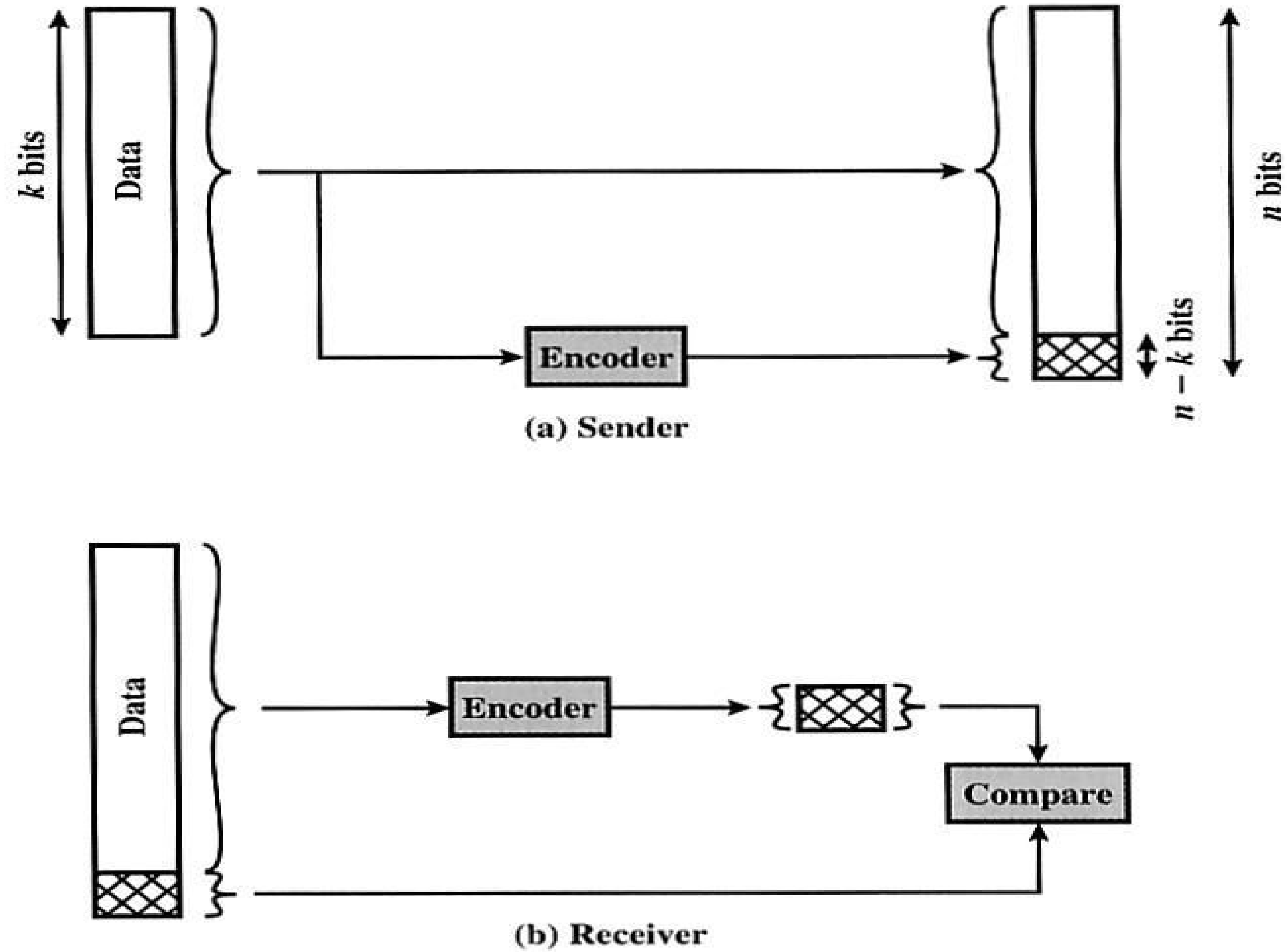
Stuffed bits

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(a) The original data. (b) The data as they appear on the line.
(c) The data as they are stored in the receiver's memory after destuffing.

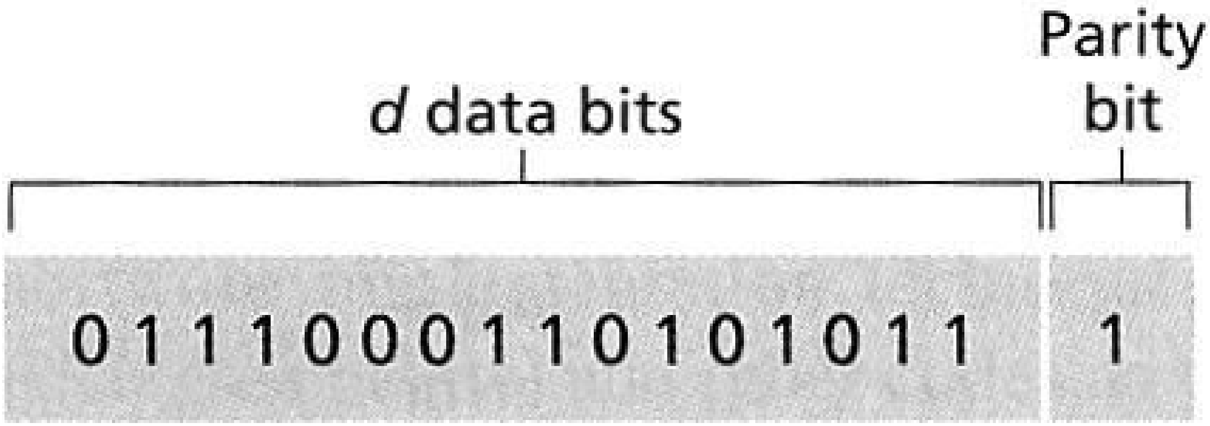
Error Control

Overview of error detection



Parity Check

- Append a parity bit to the end of a block of data (e.g., there are *d* bits in a block).
- Even parity scheme: the sender includes one additional bit and chooses its value such that the total number of 1s in the $d+1$ bits (the original information plus a parity bit) is even.
- Odd parity scheme: the parity bit value is chosen such that there is an odd number of 1s.

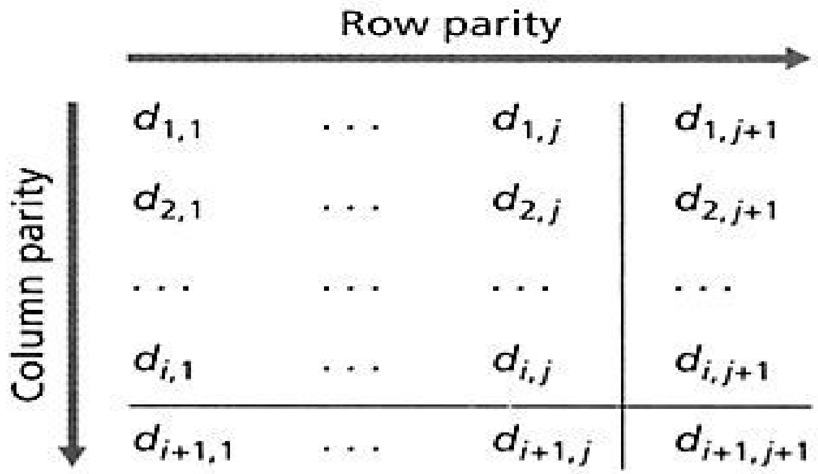


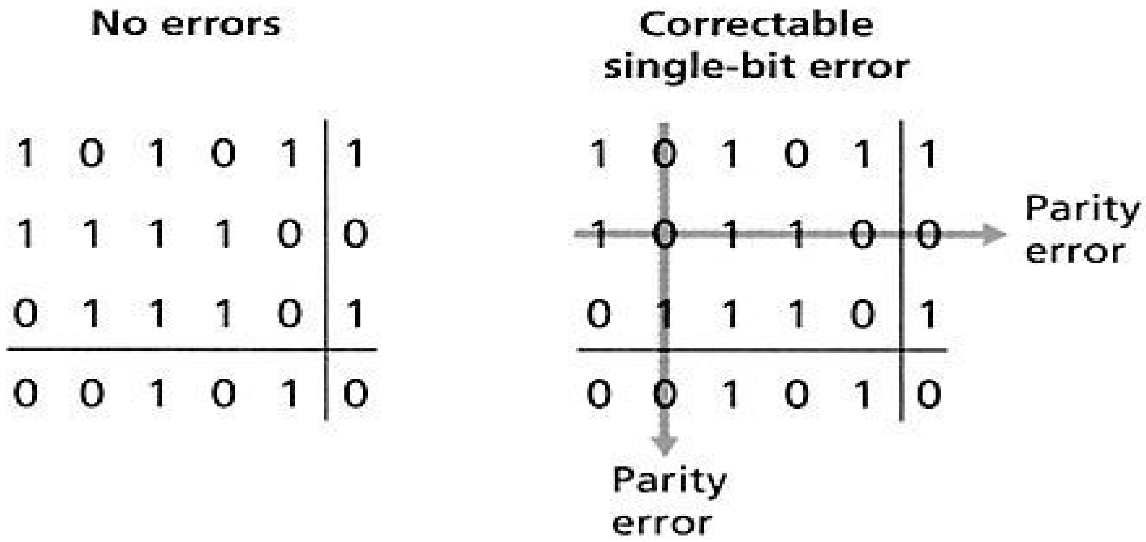
One-bit even parity

Two-dimensional Parity Check

- Two-dimensional parity is a generalization of single-bit parity.
- In this scheme, the data is formed as a rectangular matrix *j* bits wide and *i* bits high.
- A parity value is computed for each row and column. It has following properties:
  - A single bit error can be detected.
  - If there is a single error, we can use the column and row indices to identify the bit that was corrupted and correct that error.

Two-dimensional Parity Check





Two-dimensional even parity

Cyclic Redundancy Check (CRC)

- CRC treats bit streams as representations of polynomials with coefficients of 0 and 1 only.
  - e.g., 101 can be represented a polynomial as: $1x^2 + 0x^1 + 1x^0 = x^2 + 1$.
- Modulo-2 arithmetic is used for computing CRC.
  - There are no carriers for addition or borrows for subtraction.
- When the polynomial code method is employed, the sender and receiver must agree upon a **generator polynomial**, $G(x)$ in advance.

Cyclic Redundancy Check (CRC)

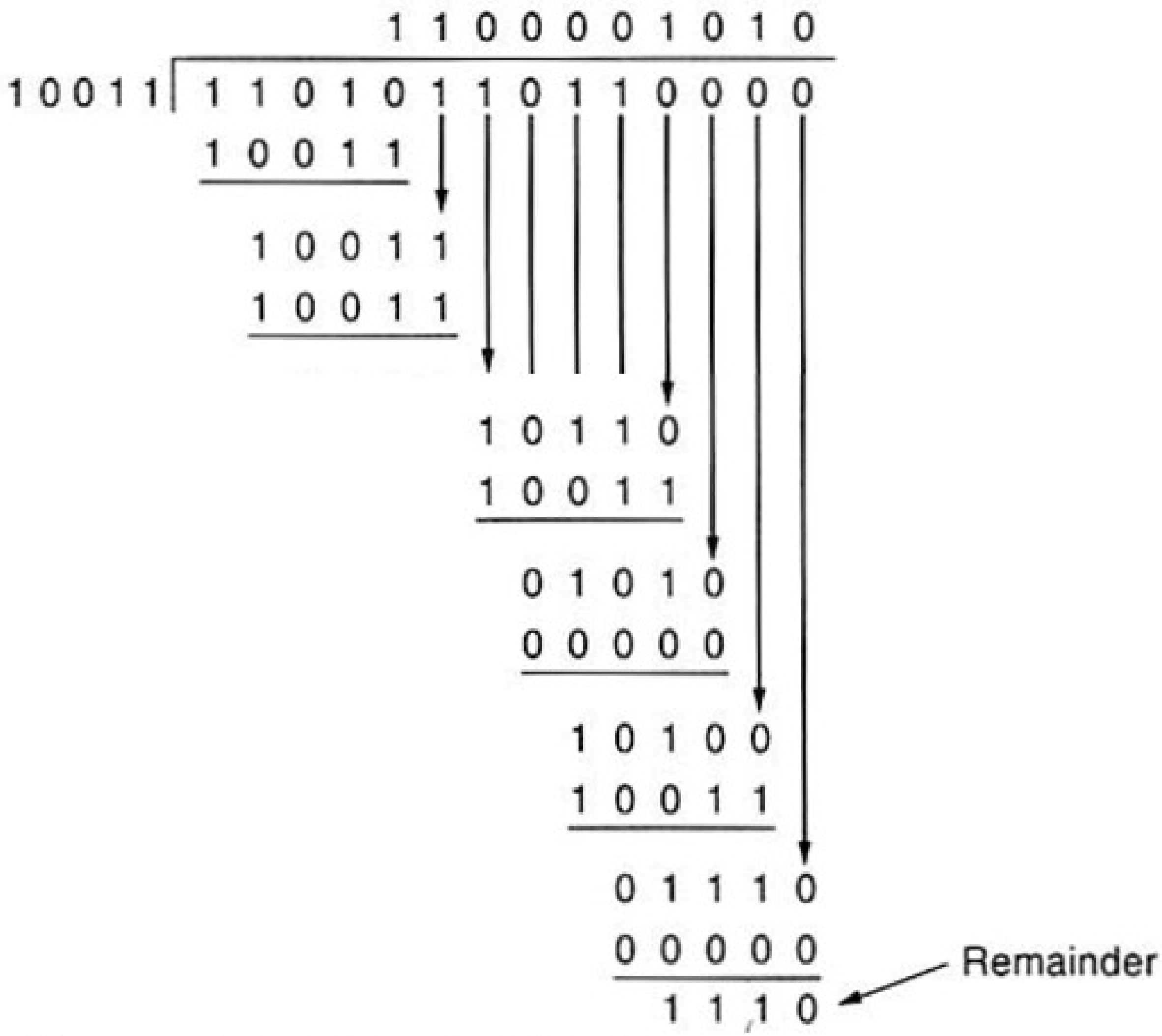
- To compute the checksum for some frame with m bits, corresponding to the polynomial $M(x)$, we have following steps:
  - Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame so it now contains $m + r$ bits and corresponds to the polynomial $x^r M(x)$.
  - Divide $G(x)$ into $x^r M(x)$ using modulo-2 division.
  - Subtract the remainder from $x^r M(x)$ using modulo-2 subtraction.
    - Append the remainder to the end of $M(x)$ to form the transmitted data frame.
- To detect the error, the receiver divides the checksummed frame by $G(x)$. If there is a remainder, there has been a transmission error.

Cyclic Redundancy Check (CRC)

Frame : 1 1 0 1 0 1 1 0 1 1

Generator: 1 0 0 1 1

Message after 4 zero bits are appended: 1 1 0 1 0 1 1 0 1 1 0 0 0 0



Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 1 0

Error Correction

- The use of error-correcting codes is often referred to as **forward error correction** (FEC).
- Basic concepts
  - Each block of data is mapped into an *n*-bit block, which consists of *m* data bits and *r* redundant. This *n*-bit block is referred to as an *n*-bit **codeword**.
  - **Hamming distance** is defined as the number of bit positions in which two code-words differ. For example (Hamming distance = 3):

$$
\begin{array}{cccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
\mathbf{\mathit{1}} & \mathbf{\mathit{1}} & 0 & 0 & 0 & 0 & 0 & \mathbf{\mathit{1}}
\end{array}
$$

Error Correction

- When transmission, each *m*-bits sequence is mapped into *n*-bit codeword. For example, "01" is mapped to "00111" in the codeword table.

Data block	Codeword
00	00000
01	00111
10	11001
11	11110

- When the receiver receives an invalid codeword (detects an error), then the valid codeword that is closest to it (minimum hamming distance) is selected.

Hamming Code

- Hamming codes are designed to correct single bit errors.
- Hamming code consists of two kinds of bits: check-bit and data-bit.
- The check-bits are in the positions which are power of 2 (i.e., 1, 2, 4, 8, 16, etc.); the rest positions (3, 5, 6, 7, 9, etc.) are filled up with the data bits.
- Each check bit forces the parity of some collection of bits, including itself, to be even (or odd).
- Hamming codes computation (demonstrated by example, 7 data bits: 100 1000):

Determine the number of check bits

- Calculate for the total number of check bits required to be added with the given message bits.
- The number of check bits can be obtained by:

$$2^c \geq d + c + 1$$

c is the number of check bits;
d is the number of data bits.

Hamming Code

- Hamming codes computation (demonstrated by example)
- 7 data bits: 100 1000

Check bits

Position	**1**	**2**	3	**4**	5	6	7	**8**	9	10	11
Value	0	0	1	1	0	0	1	0	0	0	0

Hamming Code

- Hamming codes computation

Pos. k	Value of Pos. k	Rewrite Pos. k as sum of power 2
3	1	2 + 1
5	0	4 + 1
6	0	4 + 2
7	1	4 + 2 + 1
9	0	8 + 1
10	0	8 + 2
11	0	8 + 2 + 1

Hamming Code

- When a codeword arrives, the receiver initializes a counter to zero.
- It then examines each check bit, k ($k = 1, 2, 4, 8 \ldots$), to see if it has the correct parity.
- If not, the receiver adds k to the counter.
  - If the counter is zero after all the check bits have been examined, the codeword is accepted as valid.
  - If the counter is nonzero, it contains the number of the incorrect bit.

Flow Control

- To control the transmission rate between a sender and a receiver, two approaches are used.
  - Feedback-based flow control: the receiver sends back its status to the sender.
  - Rate-based flow control: a built-in mechanism is used to limit the rate at which senders may transmit data.
- Stop-and-Wait Protocol
  - The sender sends one frame and then waits for an acknowledgement before proceeding.
  - This kind of protocols is called **Automatic Repeat reQuest (ARQ)**.

Flow Control

- Sliding Window Protocols
  - One-Bit Sliding Window Protocol
    - A sliding window protocol with a maximum window size of 1 (stop- and-wait protocol).
    - What is the disadvantage for the One-Bit Sliding Window?
  - Go-back-N Protocol
    - A sliding window protocol with a maximum windows size of *w* (where *w* is larger than 1).
    - It is a need for a large window on the sending side occurs whenever the product of bandwidth & round-trip-delay is large.
      - ✓ If the bandwidth is high, the sender will exhaust its window quickly.
      - ✓ If the delay is high, the sender will exhaust its window quickly.
    - Two approaches are used to deal with errors during transmission: go-back-n and selective repeat.

Flow Control

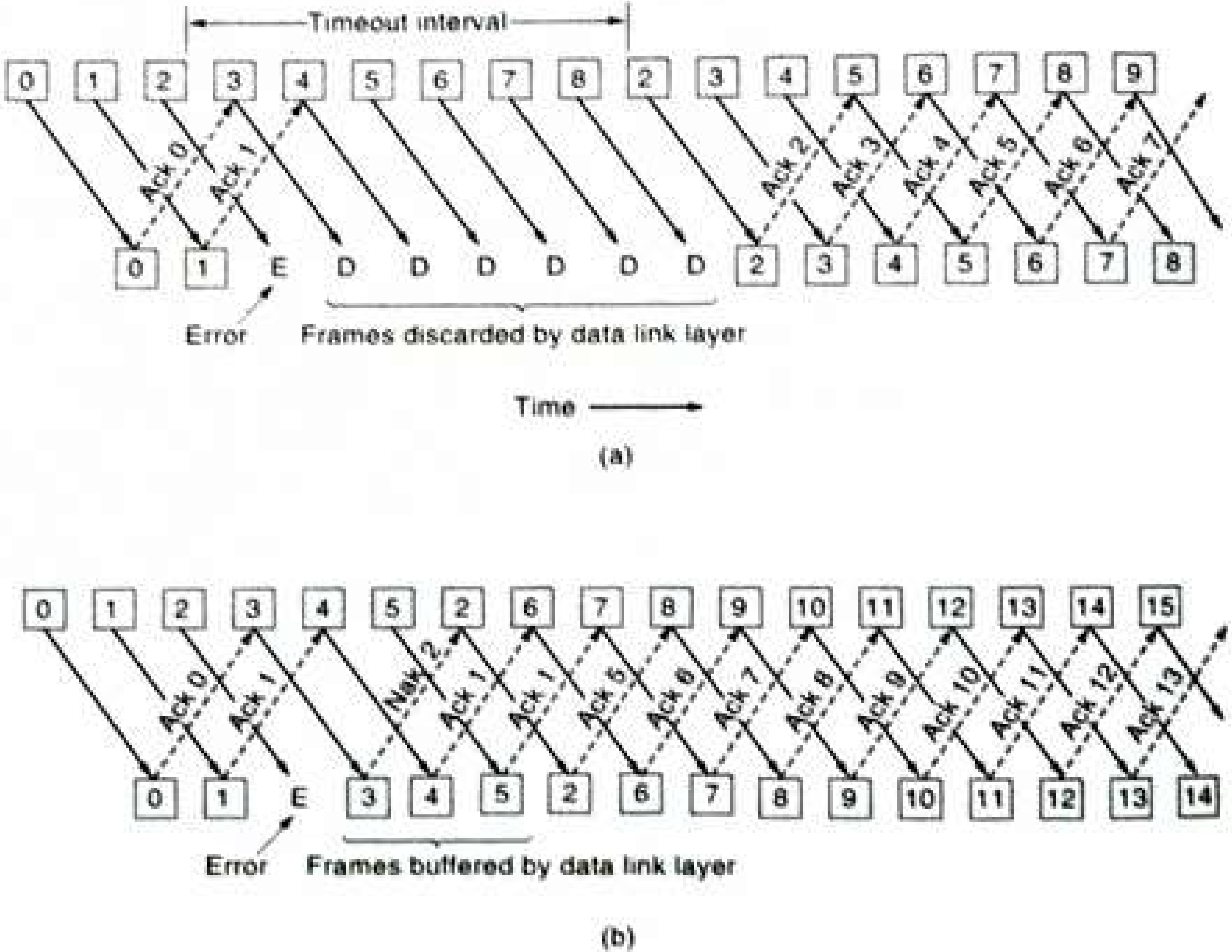
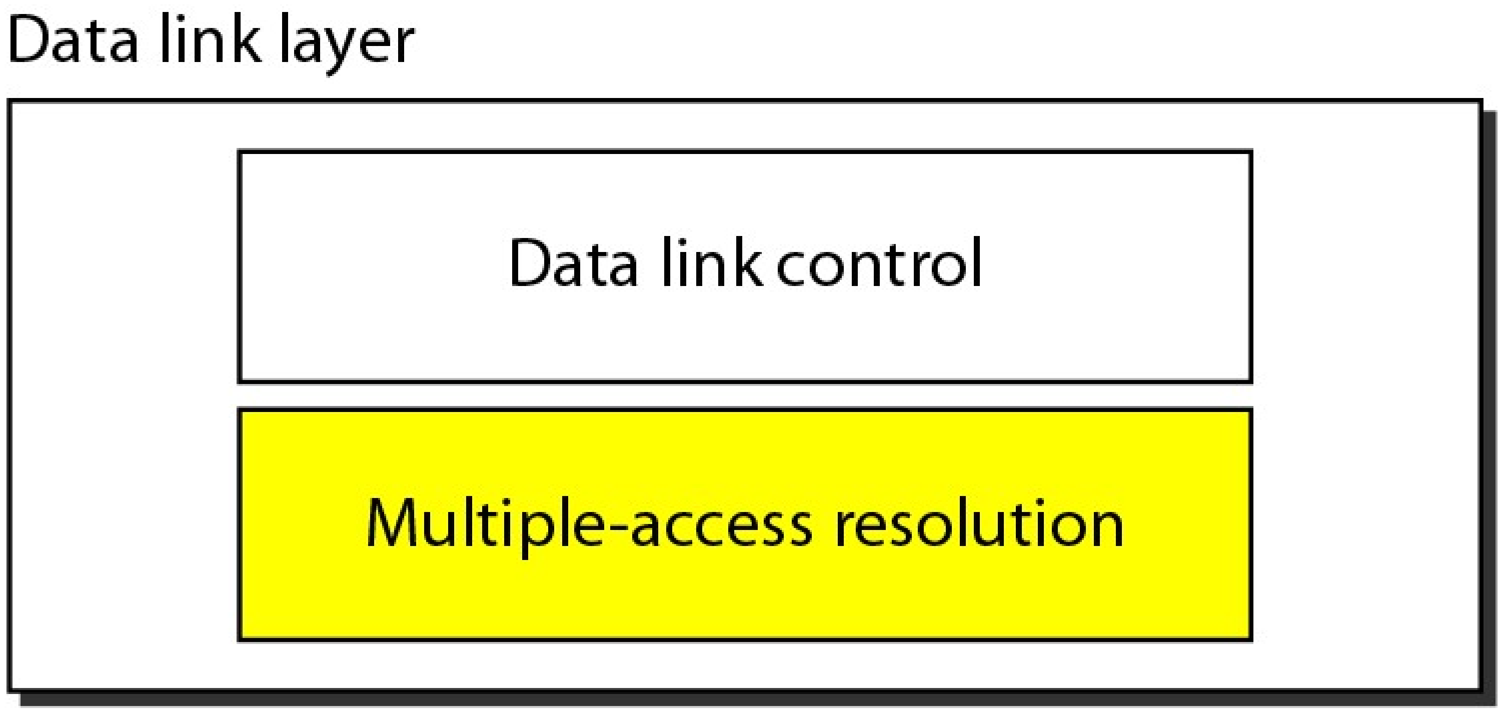
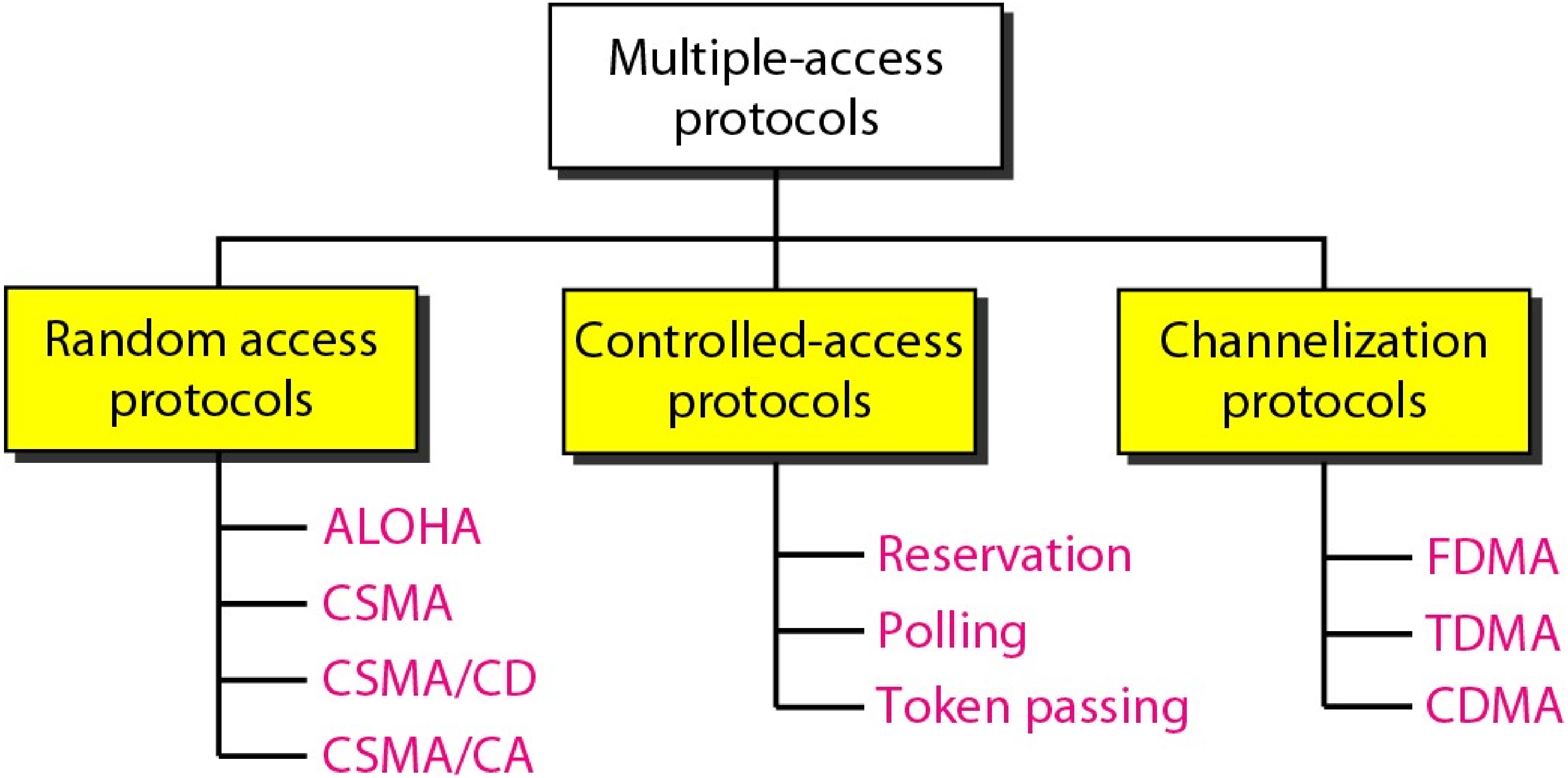


Figure 3-16. Pipelining and error recovery. Effect of an error when (a) receiver's window size is 1 and (b) receiver's window size is large.

Data link layer divided into two functionality-oriented sublayers



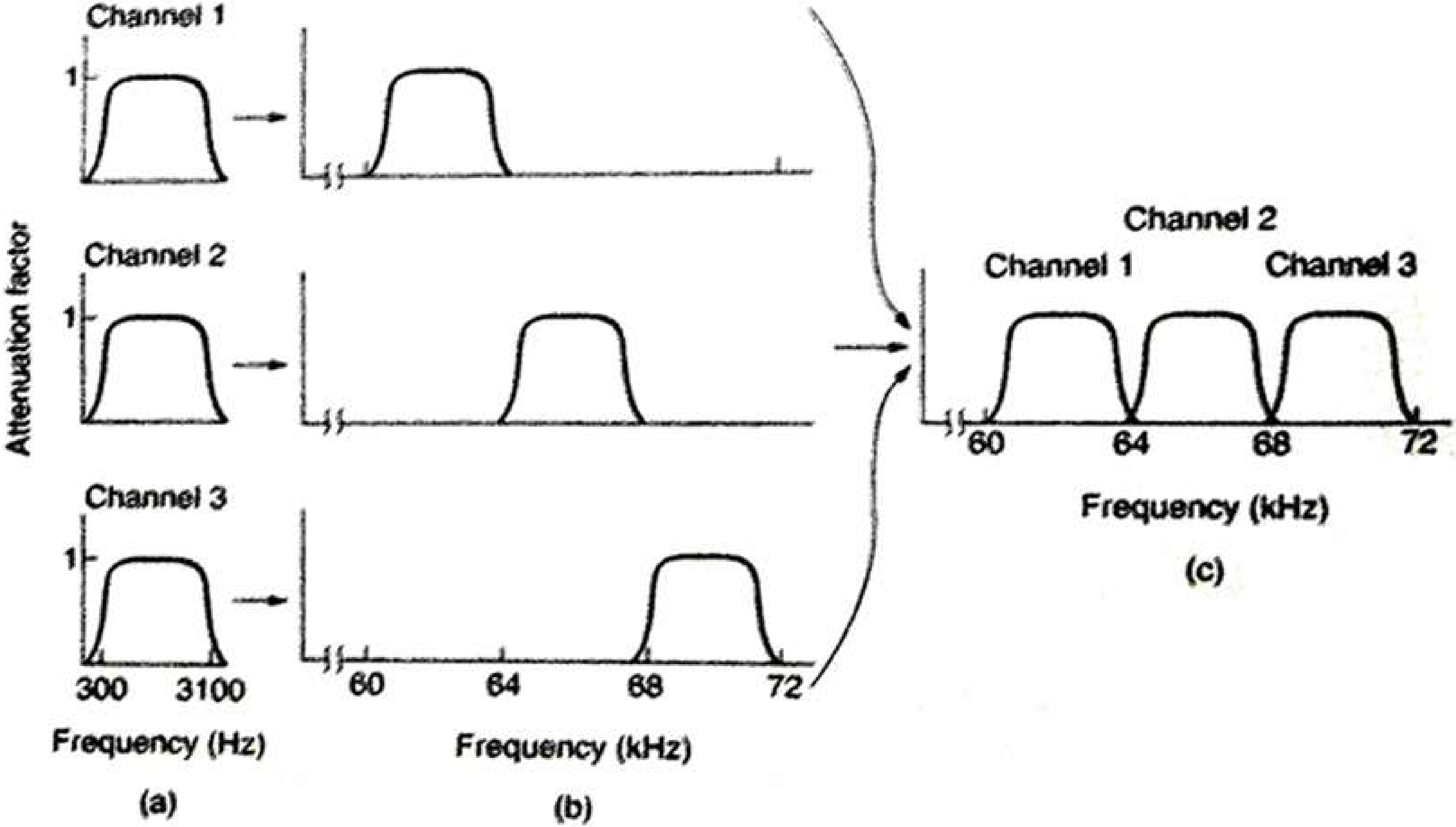
Taxonomy of Common Multiple-access Protocols



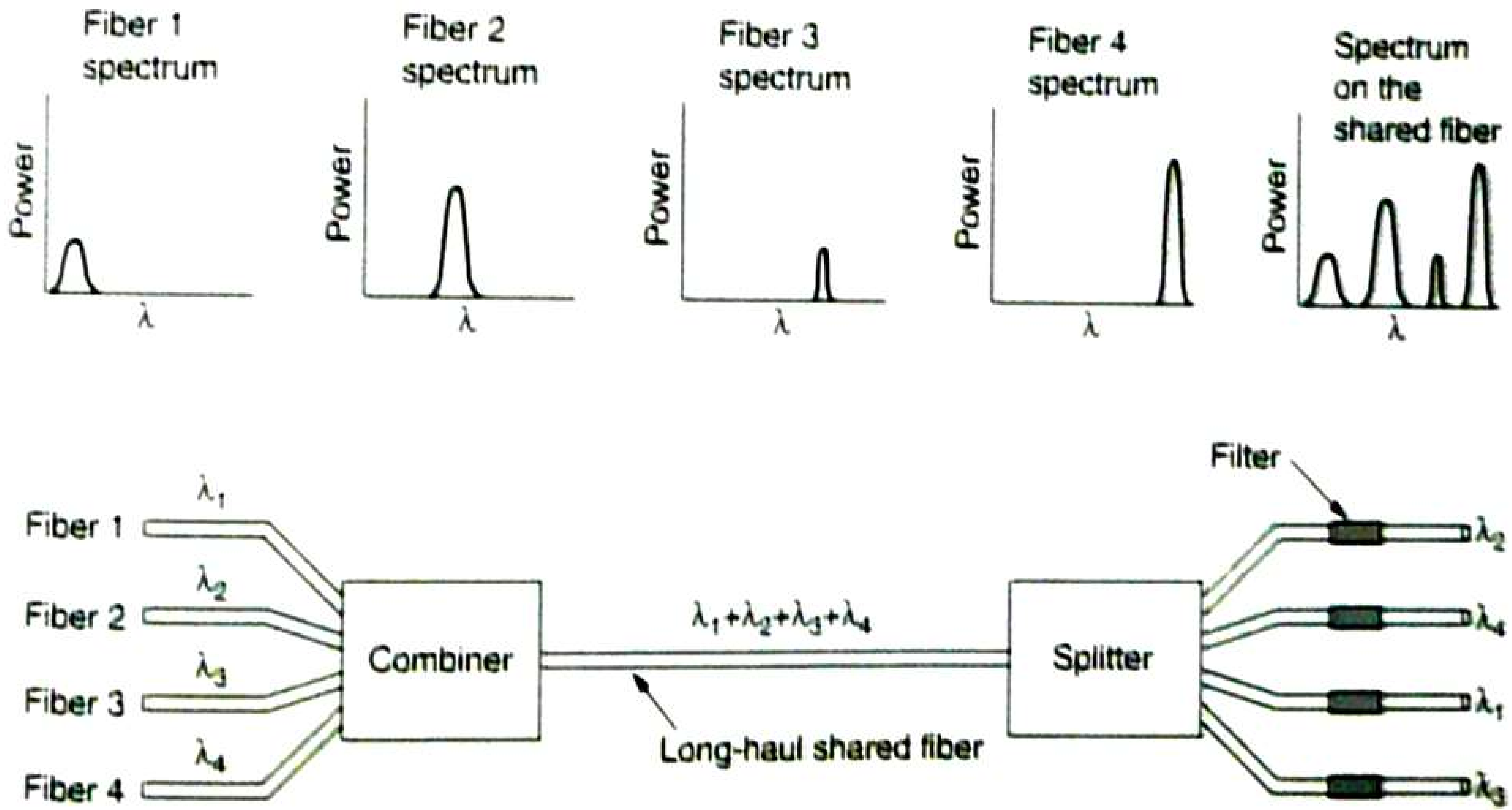
Channelization

- Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.
- Different methods are developed to share a single communication channel.
- Here we discuss three channelization protocols.
  - Frequency-Division Multiple Access (FDMA)
  - Time-Division Multiple Access (TDMA)
  - Code-Division Multiple Access (CDMA)

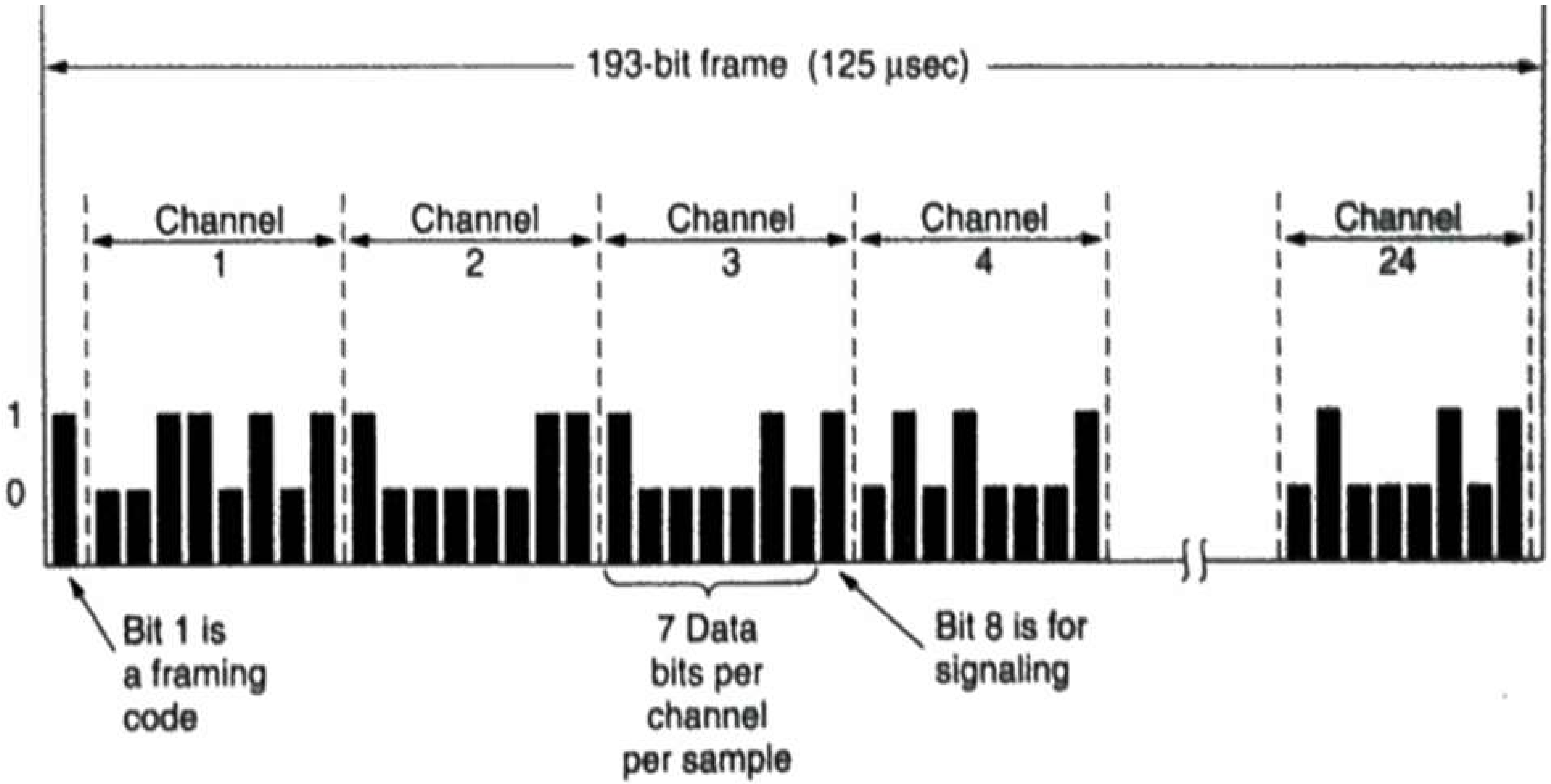
Frequency Division Multiplexing



Wavelength Division Multiplexing (for optical fiber)



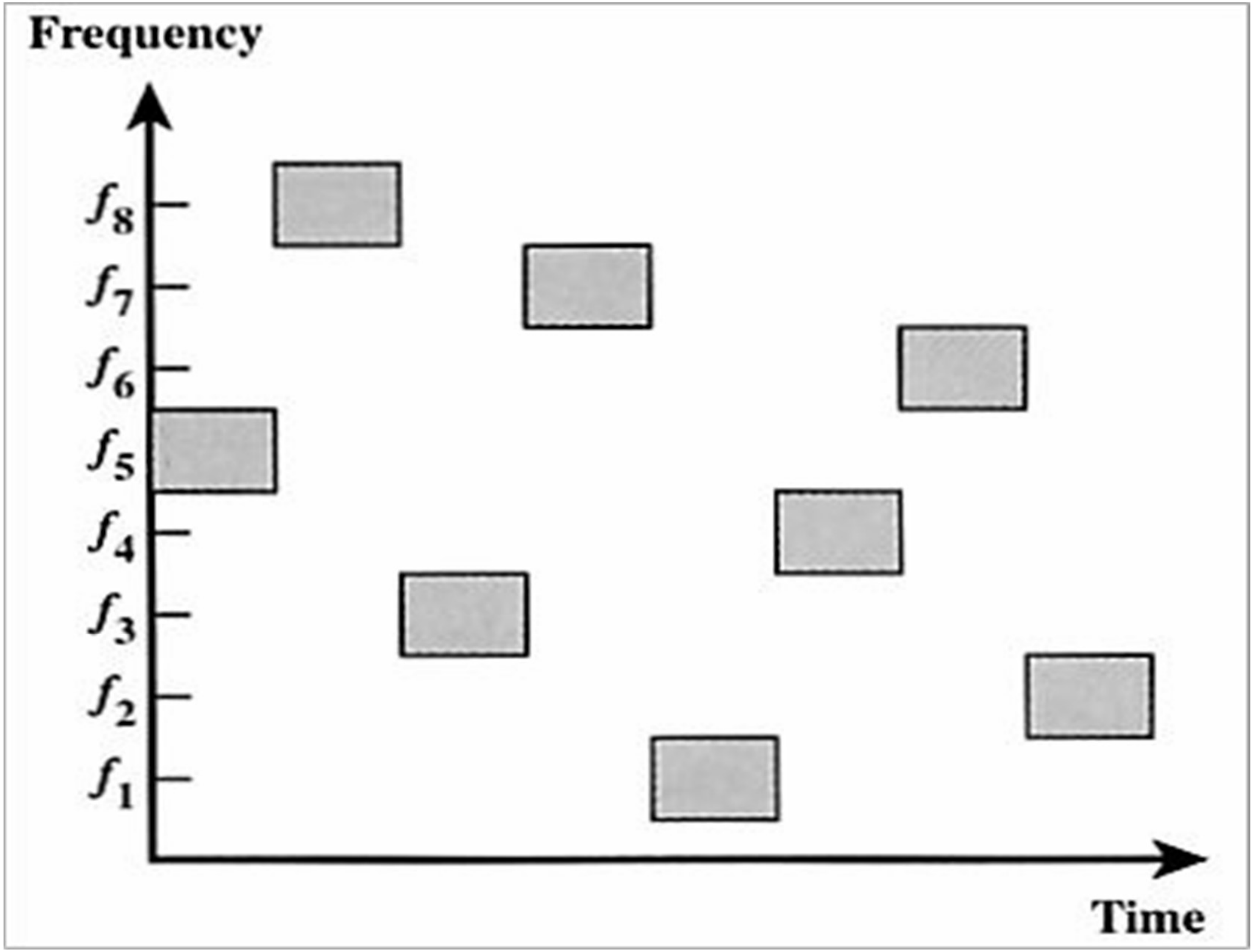
Time Division Multiplexing



Frequency-hopping spread spectrum

- The signal is broadcast over a seemingly random series of radio frequencies, hoping from frequency to frequency at fixed intervals.
- A receiver picks up the message by hopping between frequencies in synchronization with the transmitter.
- Steps
  - A number of channels are allocated for data transmission.
  - The transmitter operates in one channel at a time for a fixed interval. During that interval, some number of bits are transmitted.
  - The sequence of channels the transmitter used is dedicated by a spreading code.
  - The receiver uses the same code to receive the bits.

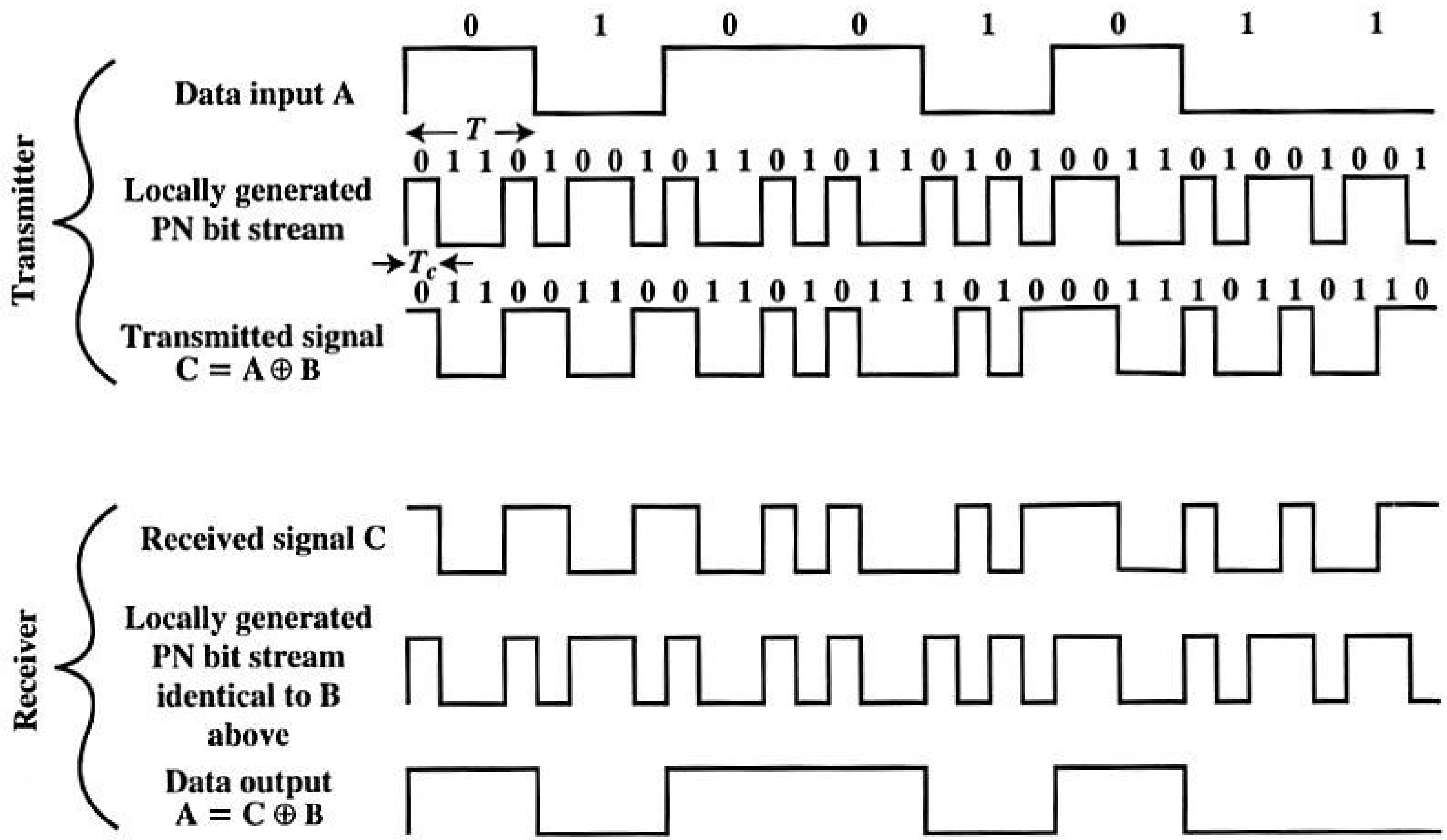
Frequency-hopping spread spectrum



Direct Sequence Spread Spectrum

- Using the spreading code, each bit in the original signal is represented by multiple bits in the transmitted signal.
- The effect of the spreading code is to spread the signal across a wider frequency band.
- The receiver uses the same spreading code to recover the original signal.
  - Transmitting: the transmitter combines the digital information stream with the spreading code bit-stream using an exclusive-OR, and produces the transmitted signal. Then the signal is sent to the receiver.
  - Receiving: the receiver combines the received information stream with the same spreading code bit-stream using an exclusive-OR, then recovers the original information stream.

Direct sequence spread spectrum

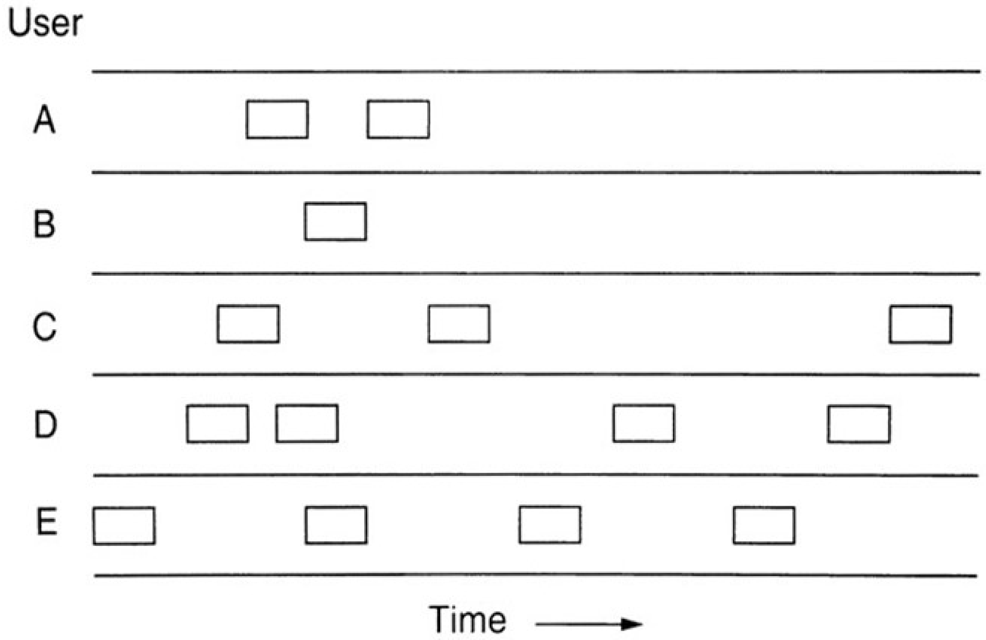


Random Access Protocols

- In random access or contention methods, no station is superior to another station and none is assigned the control over another.
- No station permits, or does not permit, another station to send.
- At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

Aloha

- Let users transmit whenever they have data to be sent.



In pure ALOHA, frames are transmitted at completely arbitrary times.

- Slotted Aloha
  - Time is divided into slots.
  - A special station will be setup to provide synchronization signal.
  - When a user has data to send, he/she waits until the beginning of the next slot.
  - If there is a collision, the user retransmits the data again until successful.

Carrier Sense Multiple Access

- Persistent CSMA
  - When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.
  - If the channel is busy, the station waits until it is idle.
  - When the station detects an idle channel, it transmits a frame.
  - If a collision occurs, the station waits a random amount of time and start all over again.
- Non-persistent CSMA
  - When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.
  - If the channel is busy, it will wait for the random time and again sense the channel whether idle or busy.
  - When the station detects an idle channel, it transmits a frame.

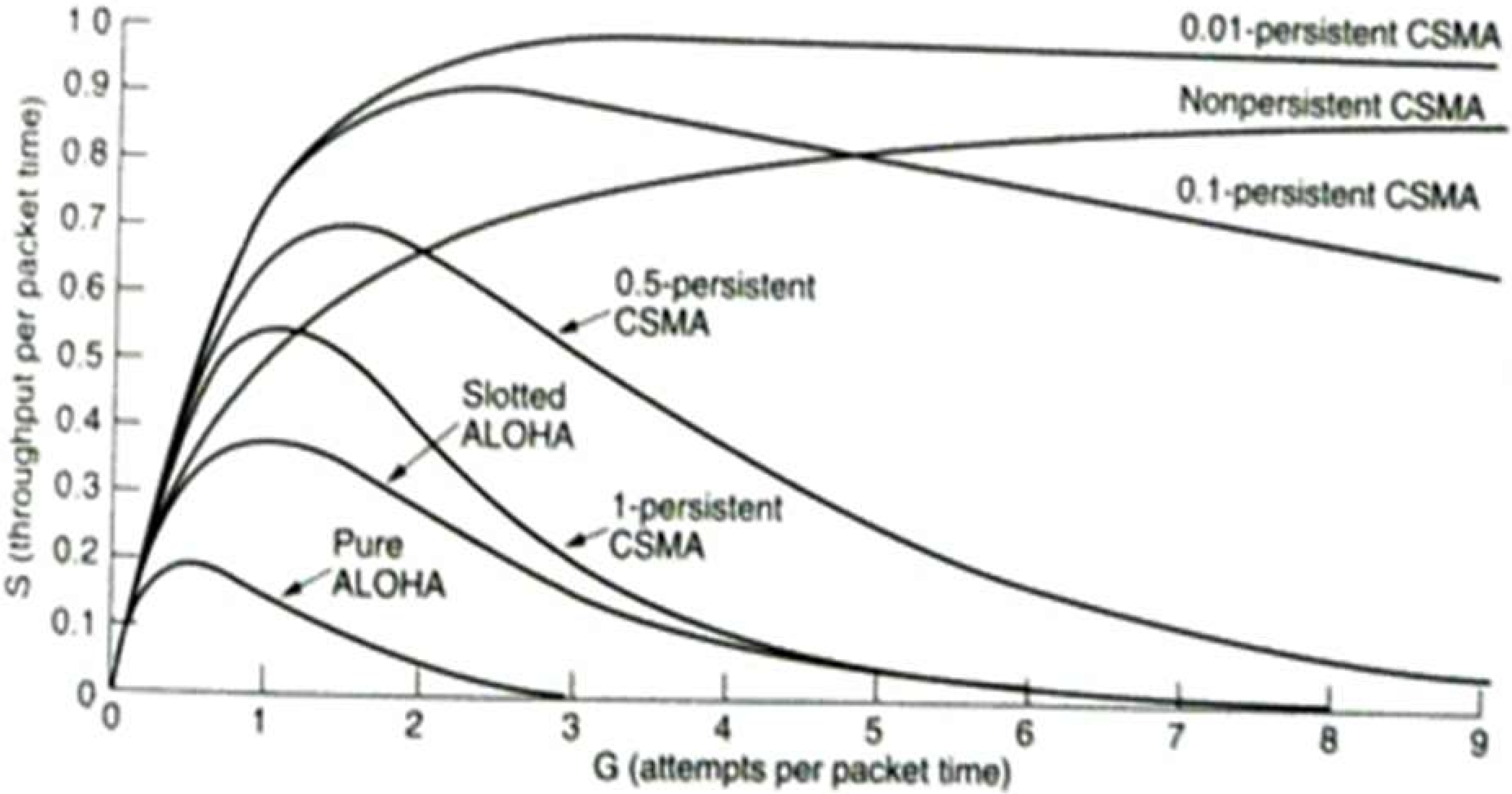
Carrier Sense Multiple Access

- Non-persistent CSMA
  - When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.
  - When the station detects an idle channel, it transmits a frame.
  - If the channel is busy, the station stops sensing the channel. It waits for random period of time and tries it again.
  - If a collision occurs, the station waits a random amount of time and start all over again.

CSMA with Collision Detection

- To abort the transmissions as soon as the stations detect a collision.
- The sender's hardware must listen to the cable while it is transmitting.
- If what it reads back is different from what it is putting on, the sender knows that a collision is occurring.
- After a station detects a collision, it aborts its transmission, waits a random period of time, and tries again.

Performance Comparison of Protocols

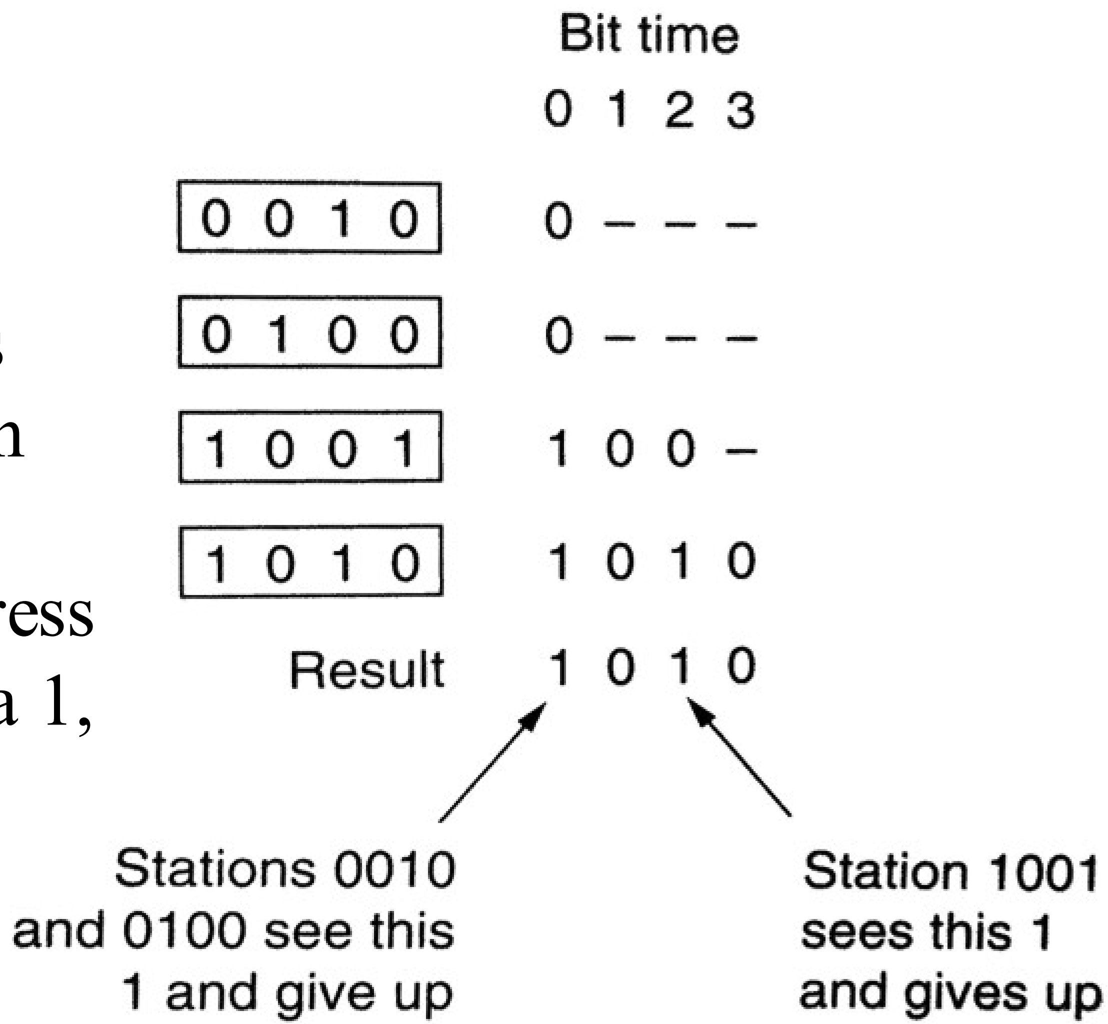


Controlled-Access Protocols: Collision-Free Protocol

- A Bit-Map Protocol:
  - Each contention period consists of exactly *N* slots.
  - If station *i* has a frame to send, it transmits a 1 bit during the i^{th} slot. No other station is allowed to transmit during this slot. (What are the disadvantages?)

Controlled-Access Protocols: Collision-Free Protocol

- Binary Countdown:
  - All addresses are the same length.
  - The bits in each address position are Boolean.
  - To avoid conflicts, a rule is applied: as soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up.



Controlled-Access Protocols: Collision-Free Protocol

- Polling Protocol
  - It requires one of the nodes to be designed as a master node.
  - The master node polls each of the nodes in a round-robin fashion.
  - Example: the master node first sends a message to node 1, saying that it can transmit up to some maximum number of frames. After node 1 transmits some frames, the master node tells node 2 it can transmit up to the maximum number of frames.
- Token-Passing Protocol
  - A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.
  - When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise it immediately forwards the token to the next node.