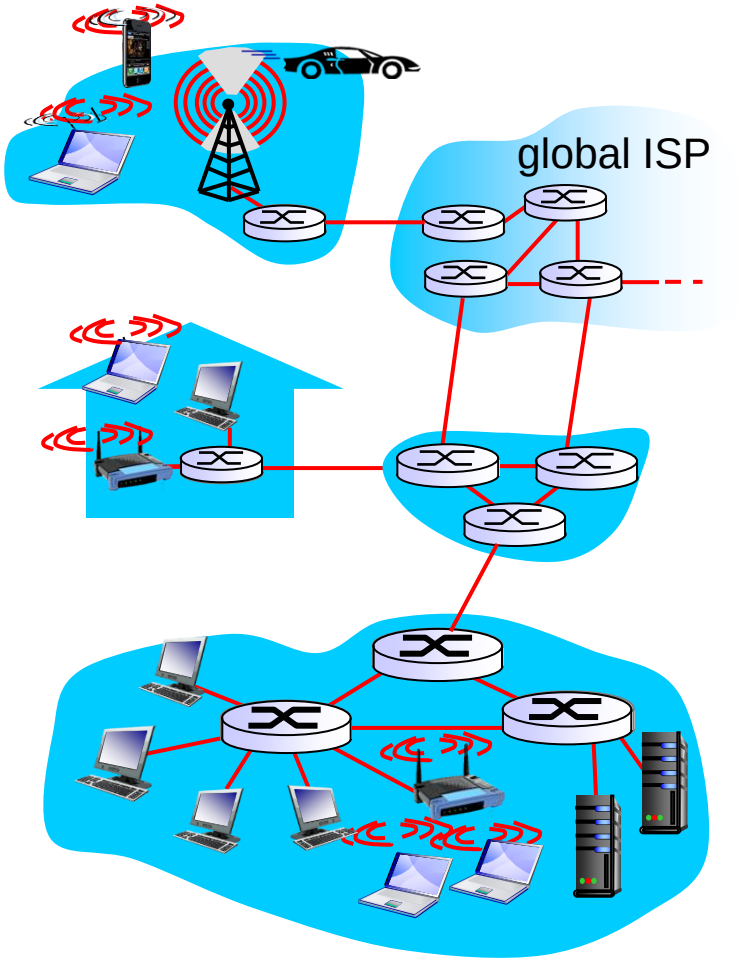
Computer Networks

Data Link Layer

Introduction

- Host and routers are as nodes.
- Communication channels that connect adjacent nodes along communication path, its called links.
  - ✓ Wired links
  - ✓ Wireless links
  - ✓ LANs
- In this layer, Packet is form of frame from encapsulate datagram.
- This layer has responsibility of transferring datagram from one node to physically adjacent node over a link.



Link Layer Services

- **Framing**
  - ✓ Encapsulate datagram into frame.
  - ✓ Adding header and trailer.
- **Link Access**
  - ✓ “MAC” addresses used in frame headers to identify source and destination. It is different from IP address.
- **Reliable delivery**
  - ✓ If this layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error.
  - ✓ A link-layer reliable delivery service can be achieved with acknowledgments and retransmissions.
- **Flow Control**
  - ✓ Pacing between adjacent sending and receiving nodes.

Link Layer Services – Cont…

- Error Detection & Correction
  - ✓ Errors caused by signal attenuation and noise.
  - ✓ Receiver detects presence of errors.
  - ✓ Sender send signal for retransmission or drops frame.
  - ✓ Receiver identifies *and corrects* bit error(s) without resorting to retransmission.

Error Detection & Correction Technique

- Techniques for error detection
  - ✓ Parity Check
  - ✓ Checksum Method
  - ✓ Cyclic Redundancy Check

Parity Check

- One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.
- For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even.
- If the number of 1s is odd, to make it even a bit with value 1 is added.

Parity Check – Cont…

- Receiver counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted.
- If the count of 1s is odd and odd parity is used, the frame is still not corrupted.
- If a single bit flips in transit, the receiver can detect it by counting the number of 1s.
- But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

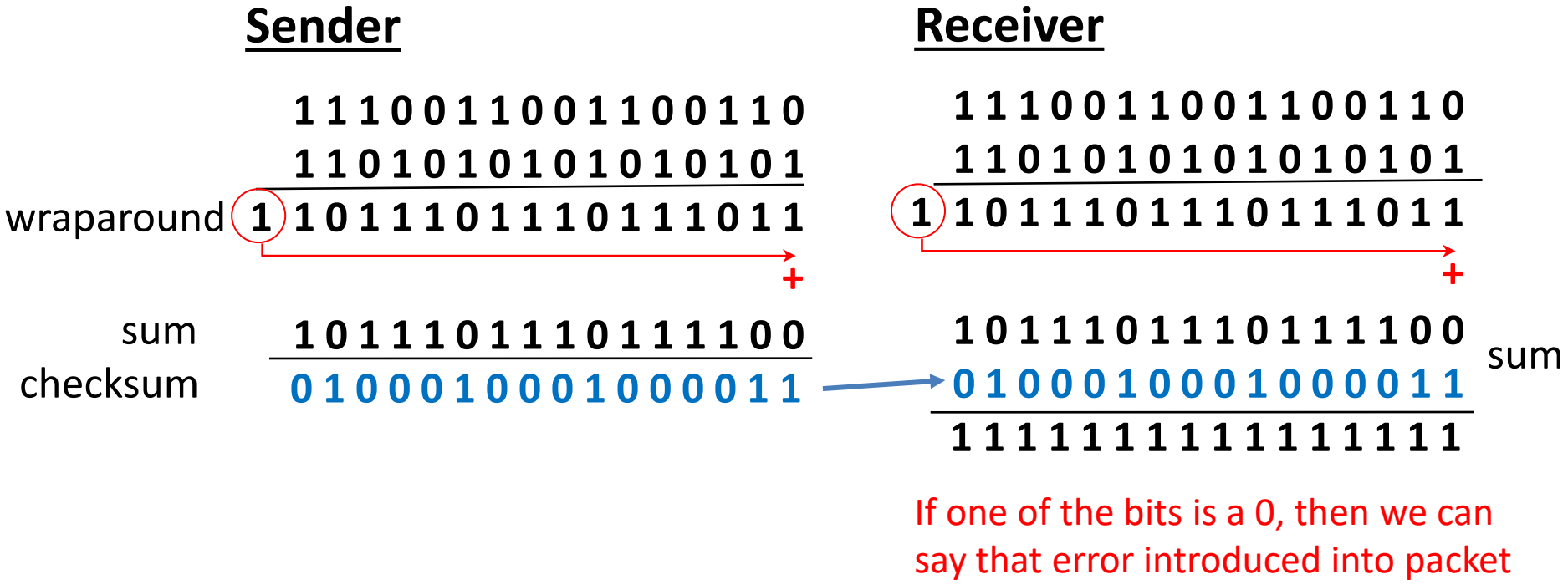
10010011 → 00010011

Checksum

- Data is divided into k segments each of m bits.
- Sender Side: Segments are added using 1's complement arithmetic to get the sum.
- Sum is complemented to get the checksum.
- Checksum segment is sent along with the data segments.
- Receiver Side: All received segments are added using 1's complement arithmetic to get complemented sum.
- If the result is zero, the received data is accepted; otherwise discarded.

Checksum - Example

- Add two 16-bit integers word



***Note**:* when adding numbers, a carryout from the most significant bit needs to be added to the result

Cyclic Redundancy Check

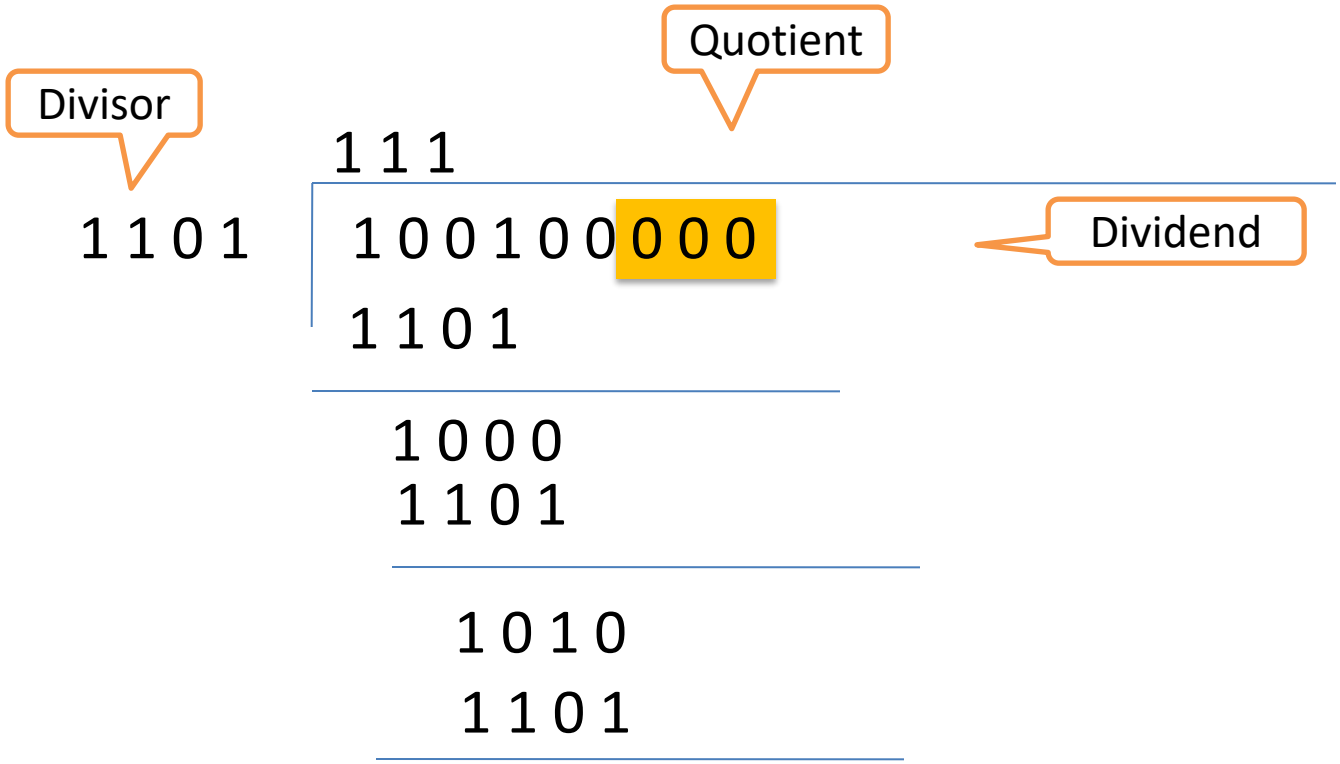
- CRC is the most powerful and easy to implement technique.
- CRC is based on binary division.
- In CRC, a sequence of redundant bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number.
- If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.
- The binary number, which is (r+1) bit in length, can also be considered as the coefficients of a polynomial, called Generator Polynomial.

CRC Generation at Sender Side

- 1. Find the length of divisor ‘L’
- 2. Append ‘L-1’ bits to the original message.
- 3. Perform binary division operation.
- 4. Remainder of the division = CRC

- Note: The CRC must be of L-1 bits

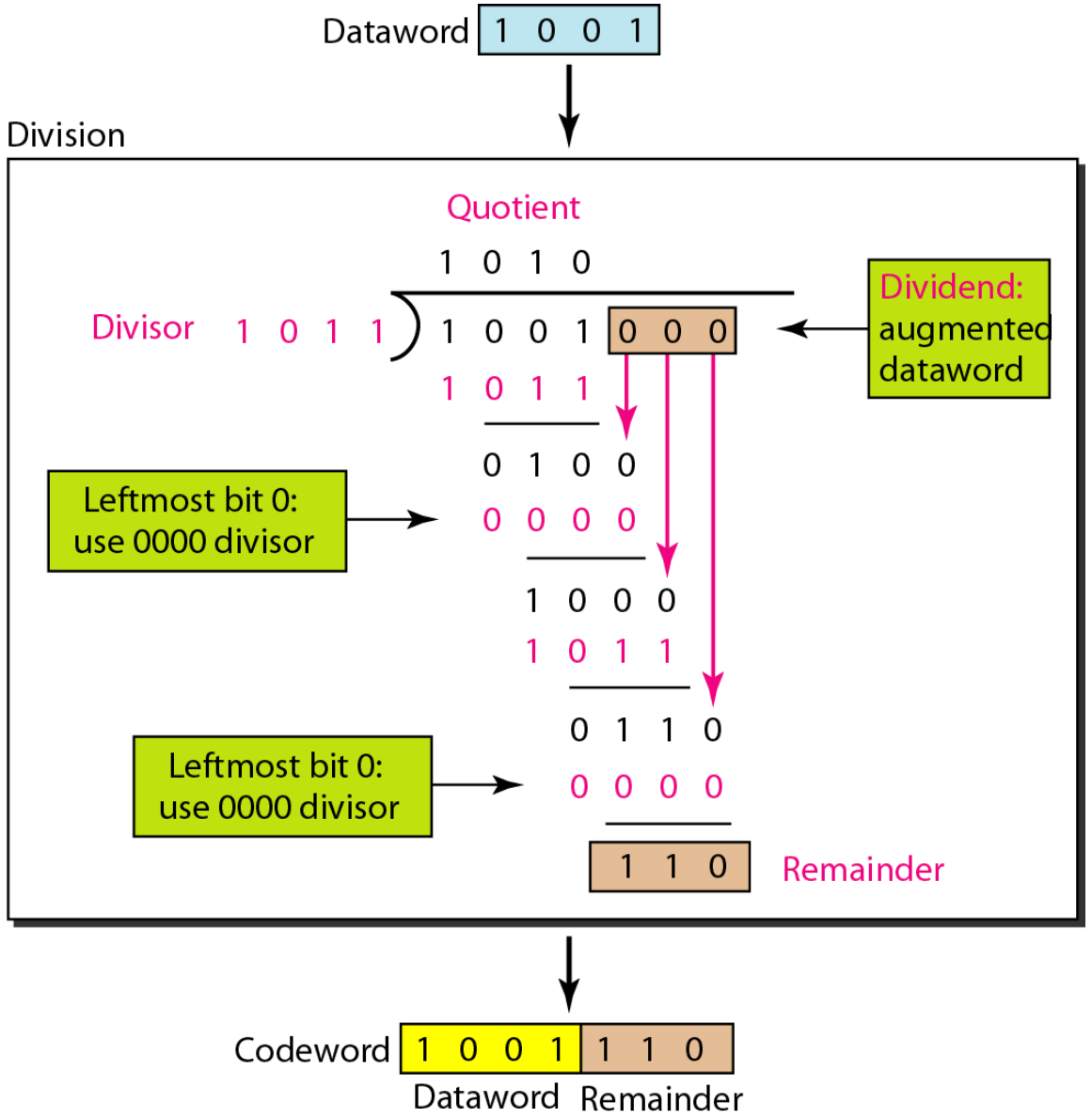
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0



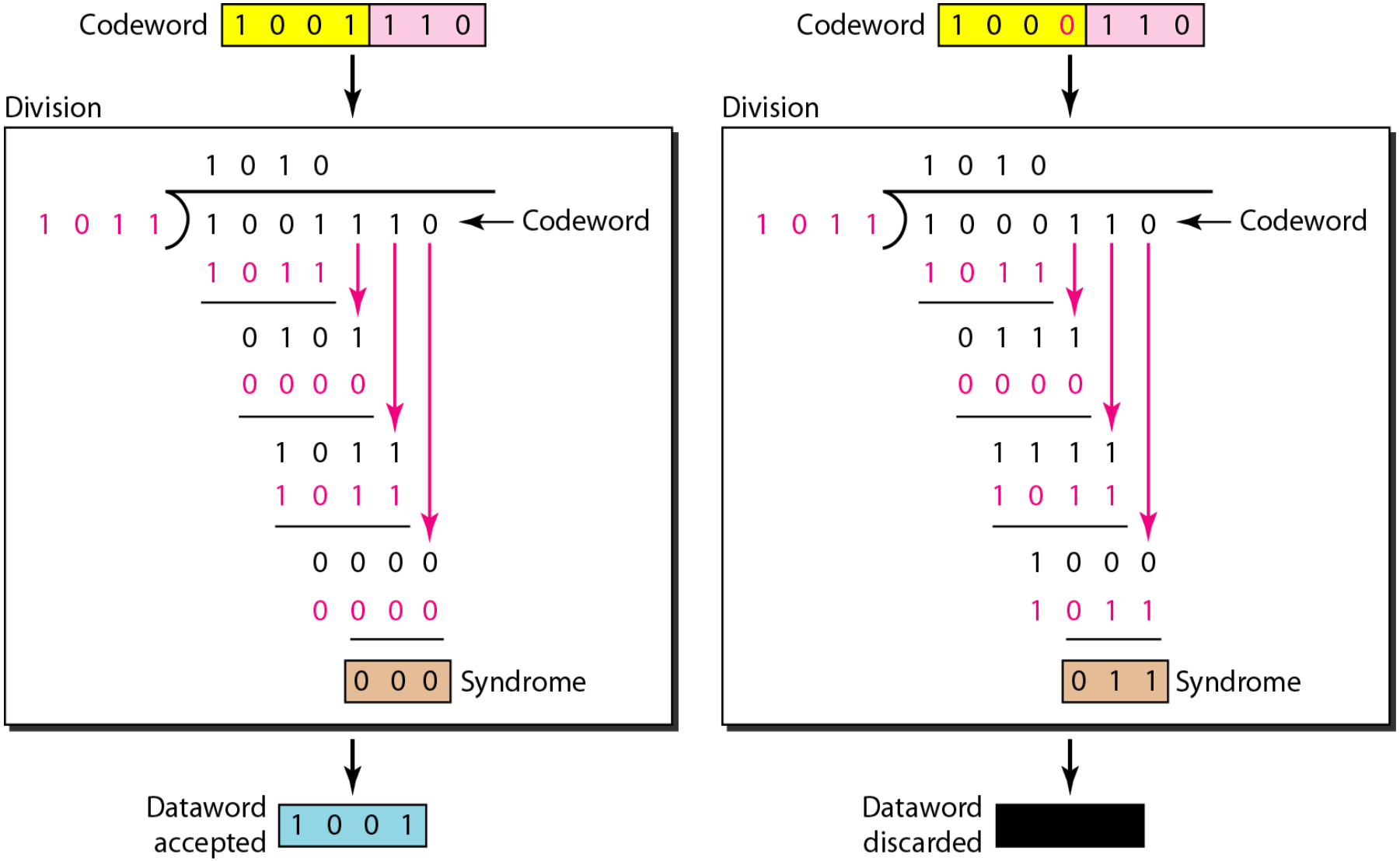
Original Message: 1001

Divisor: 1011

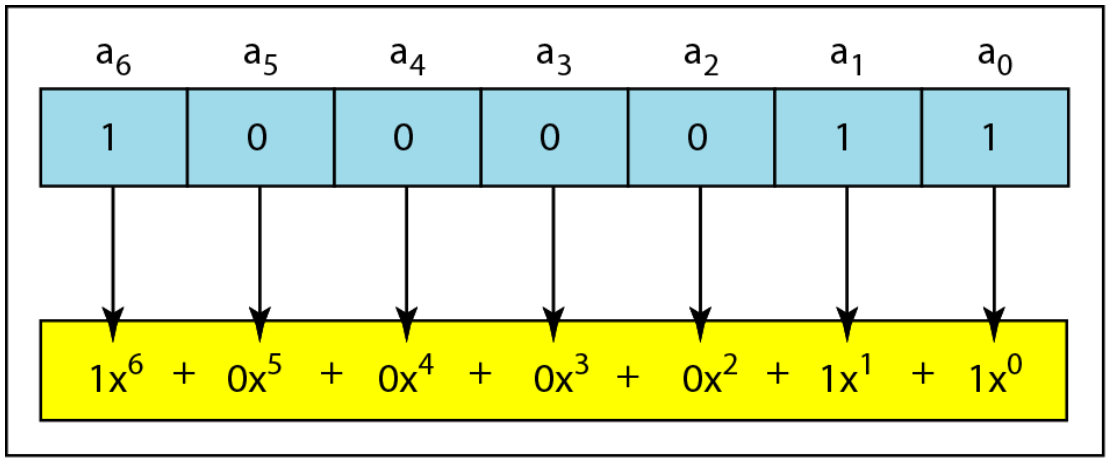
Division in CRC encoder



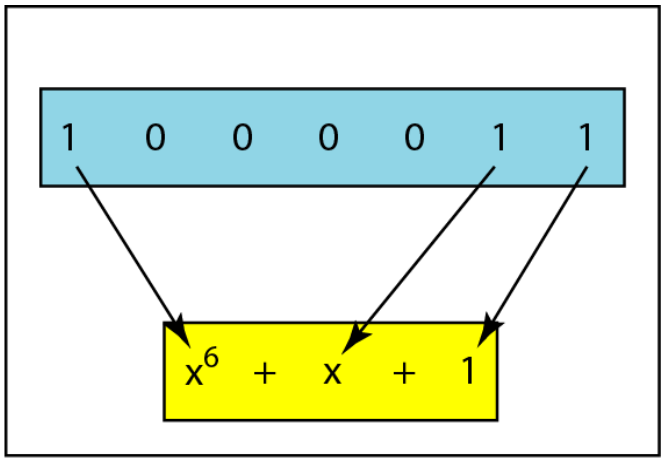
Division in the CRC decoder for two cases



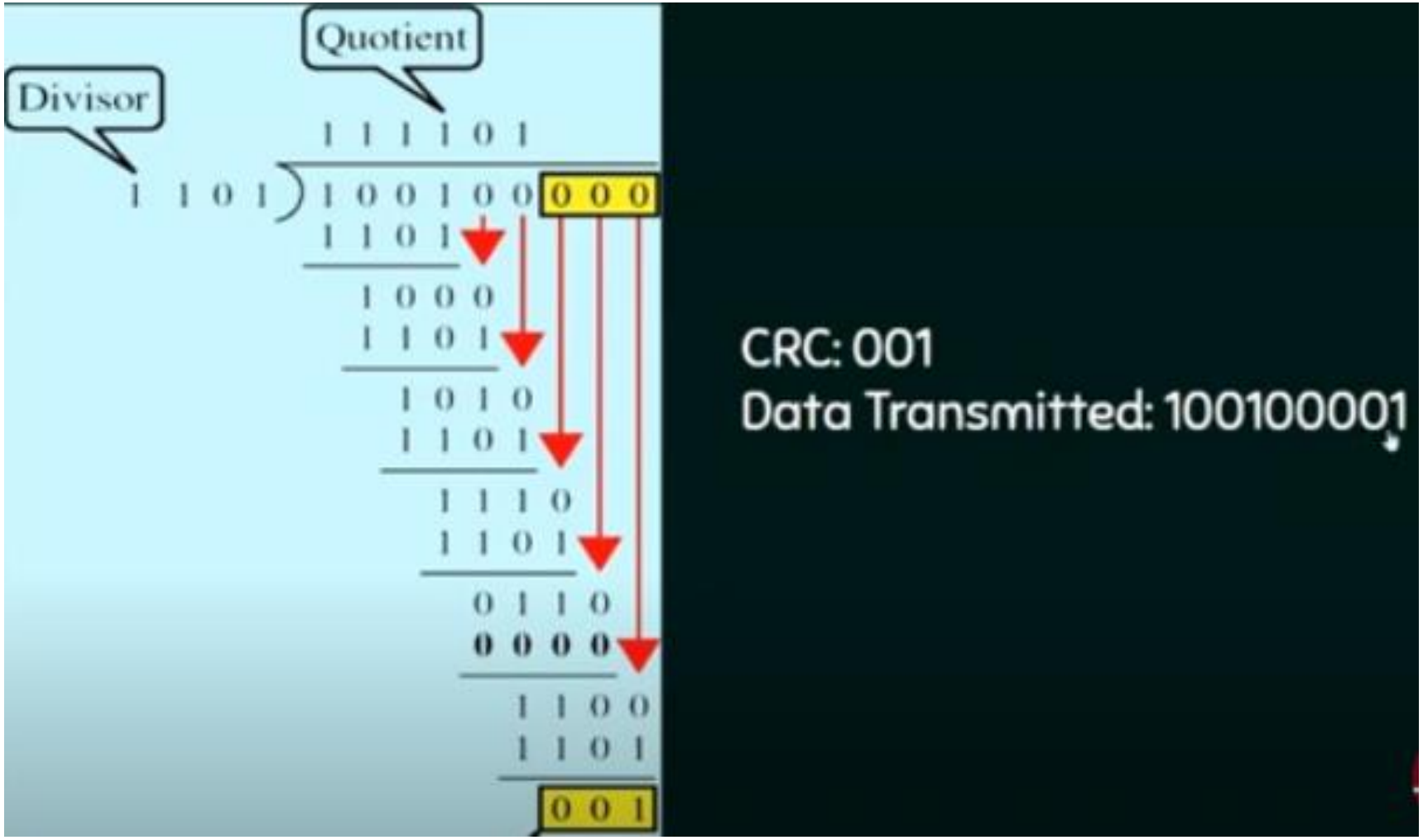
A polynomial to represent a binary word



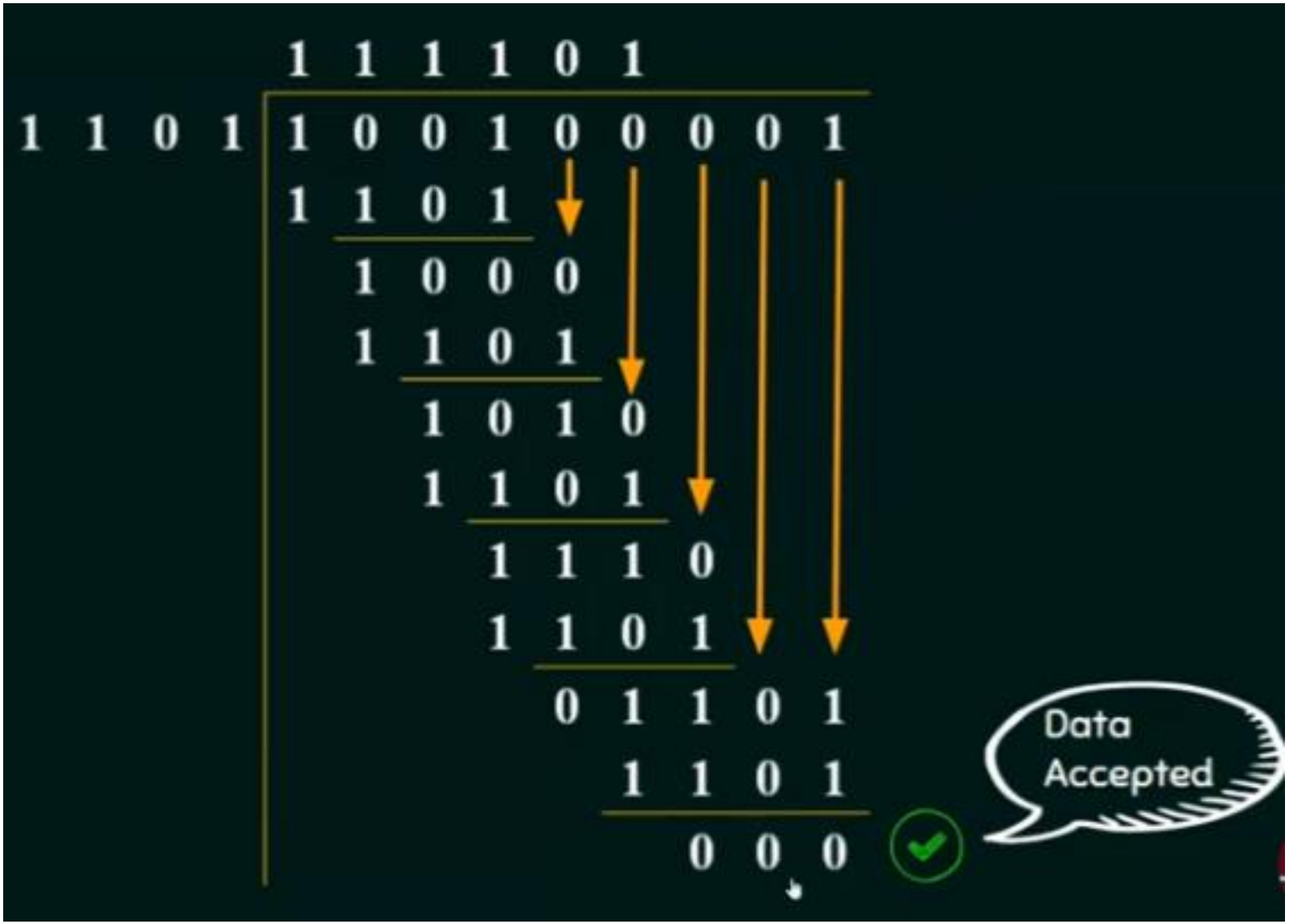
a. Binary pattern and polynomial



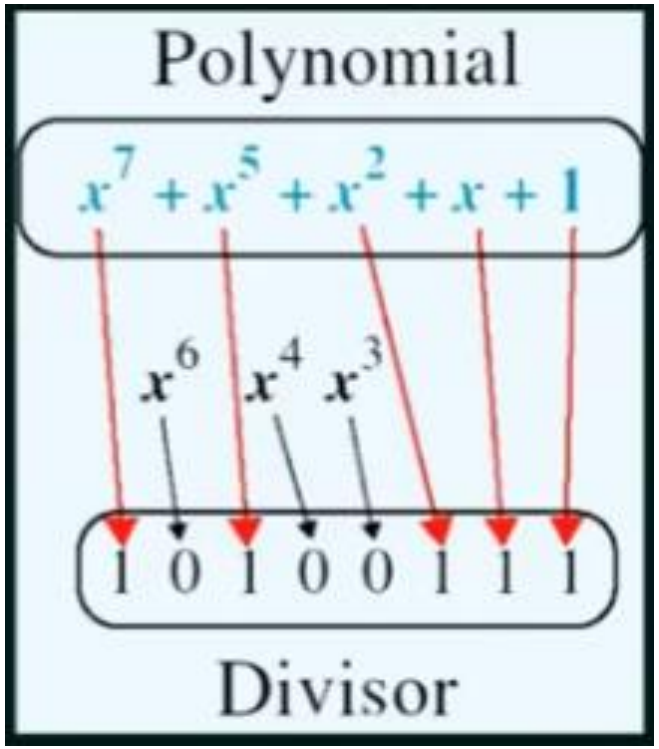
b. Short form


Quotient
Divisor
1 1 1 1 0 1
1 1 0 1) 1 0 0 1 0 0 0 0 0
1 1 0 1
1 0 0 0
1 1 0 1
1 0 1 0
1 1 0 1
1 1 1 0
1 1 0 1
0 1 1 0
0 0 0 0
1 1 0 0
1 1 0 1
0 0 1
CRC: 001
Data Transmitted: 100100001

CRC at Receiver Side



- Find the CRC for 1110010101 with the divisor x3 + x2 + 1?



CRC – Example:1

original message

1 0 1 0 0 0 0

@ means X-OR

Generator polynomial

x^3+1

$1.x^3+0.x^2+0.x^1+1.x^0$

CRC generator

1 0 0 1 4-bit

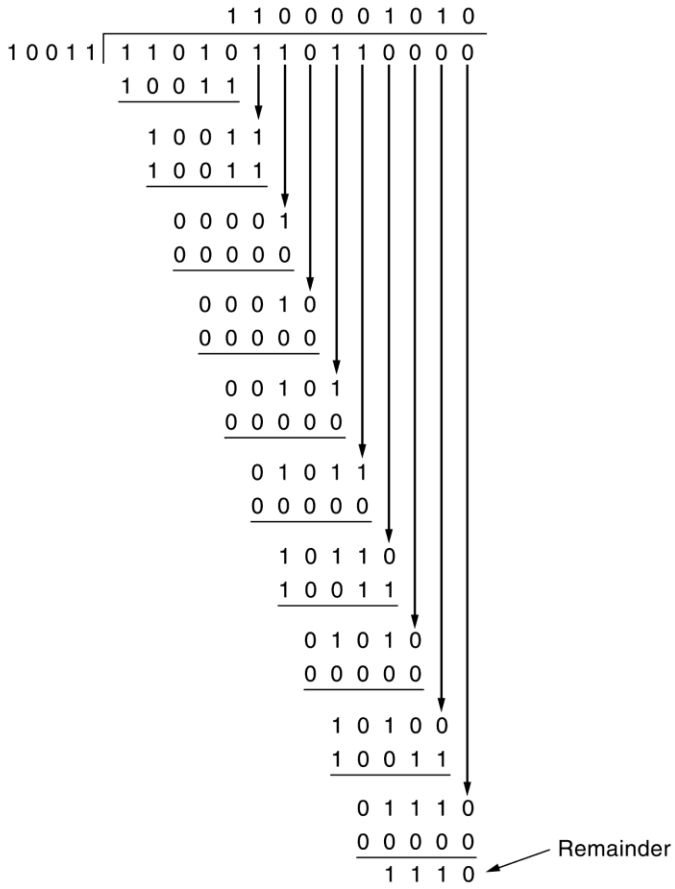
If CRC generator is of n bit then append (n-1) zeros in the end of original message

CRC – Example:2

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

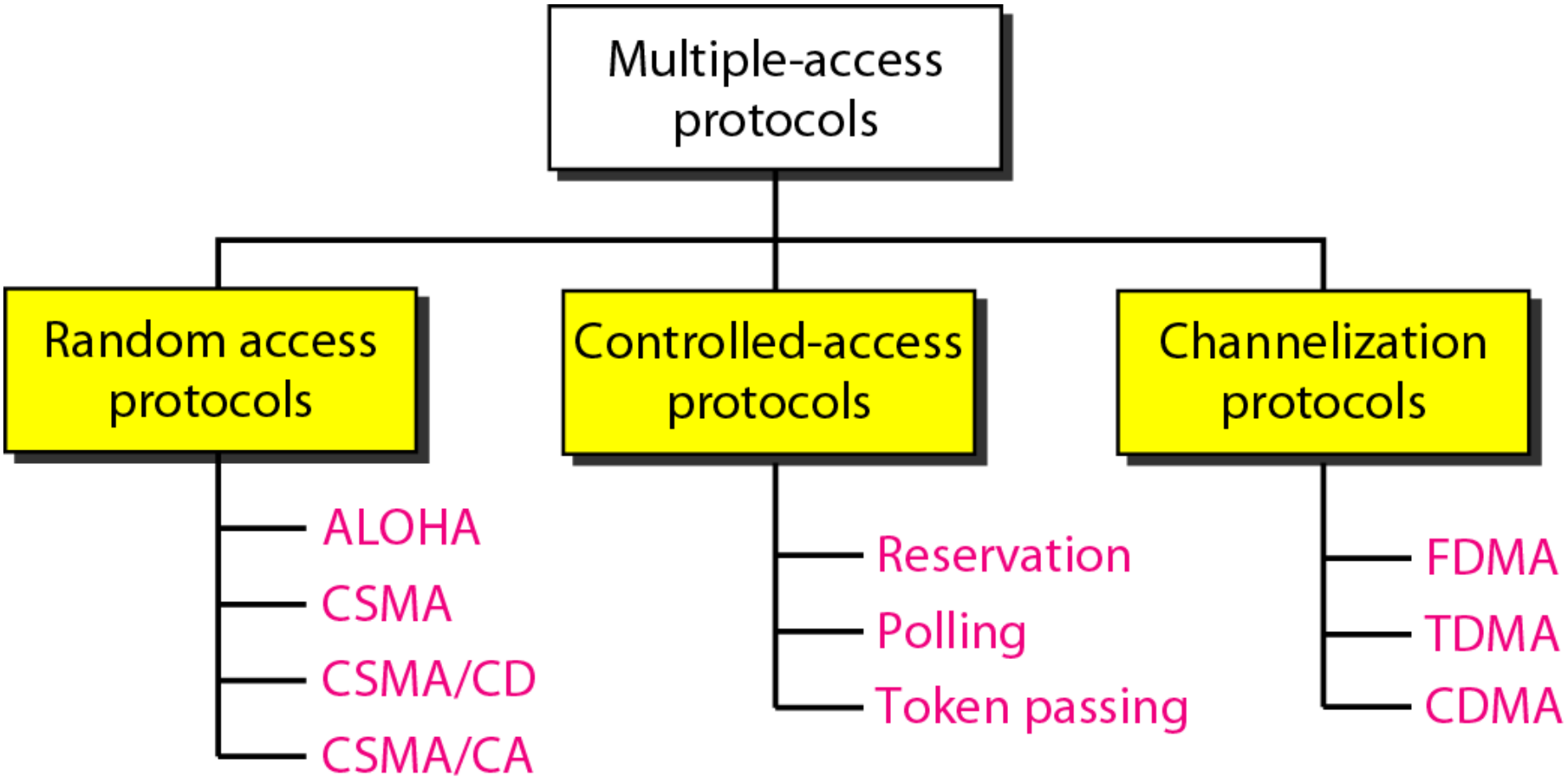


Transmitted frame: 1 1 0 1 0 1 1 0 1 1 1 1 0

Multiple Access Links

- There are two types of network links:
- A point-to-point link consists of a single sender at one end of the link and a single receiver at the other end of the link.
- A broadcast link, can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel.
- The term broadcast is used here because when any one node transmits a frame, the channel broadcasts the frame and each of the other nodes receives a copy.

Taxonomy of multiple-access protocols



Multiple Access Protocols

Categories of Multiple Access Protocol:

1. Channel Partitioning Protocols
   - ✓ Divide channel into smaller “pieces” (time slots, frequency, code)
   - ✓ Allocate piece to node for exclusive use
   - ✓ Examples of channel partitioning protocols
     - TDMA: Time Division Multiple Access
     - FDMA: Frequency Division Multiple Access
     - CDMA: Code Division Multiple Access

Multiple Access Protocols – Cont…

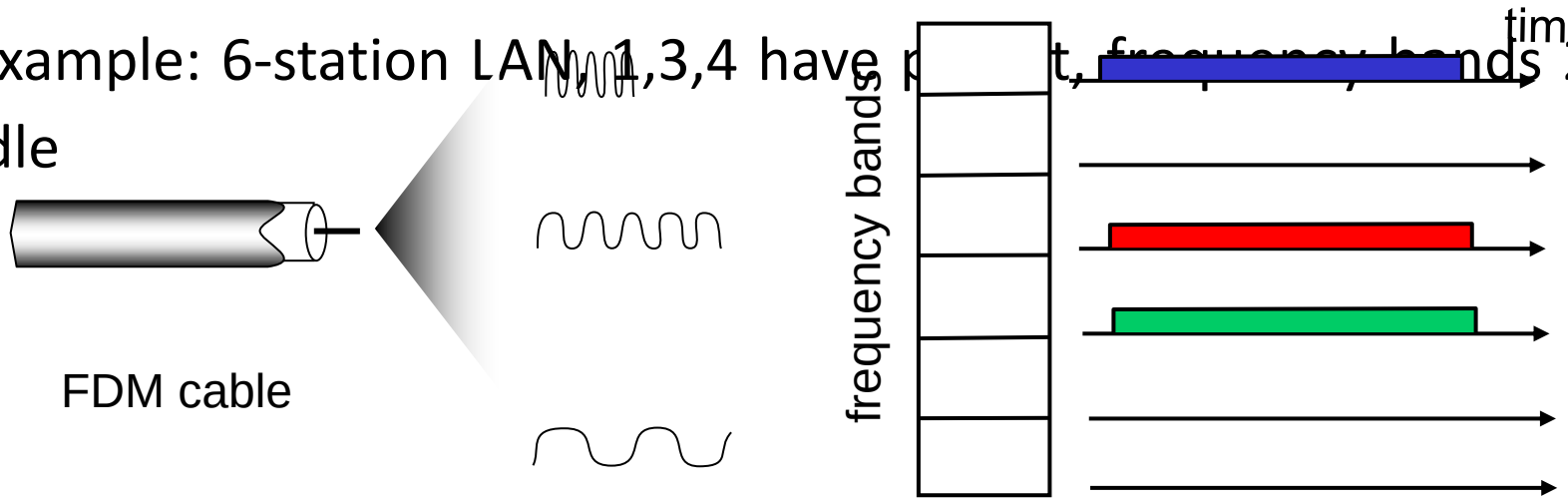
2. Random Access Protocols
   - ✓ Channel is not divided and allow collisions.
   - ✓ “Recover” from collisions
   - ✓ Examples of random access MAC (Medium Access Control) protocols
     - Pure ALOHA
     - Slotted ALOHA
     - CSMA, CSMA/CD, CSMA/CA

Multiple Access Protocols – Cont…

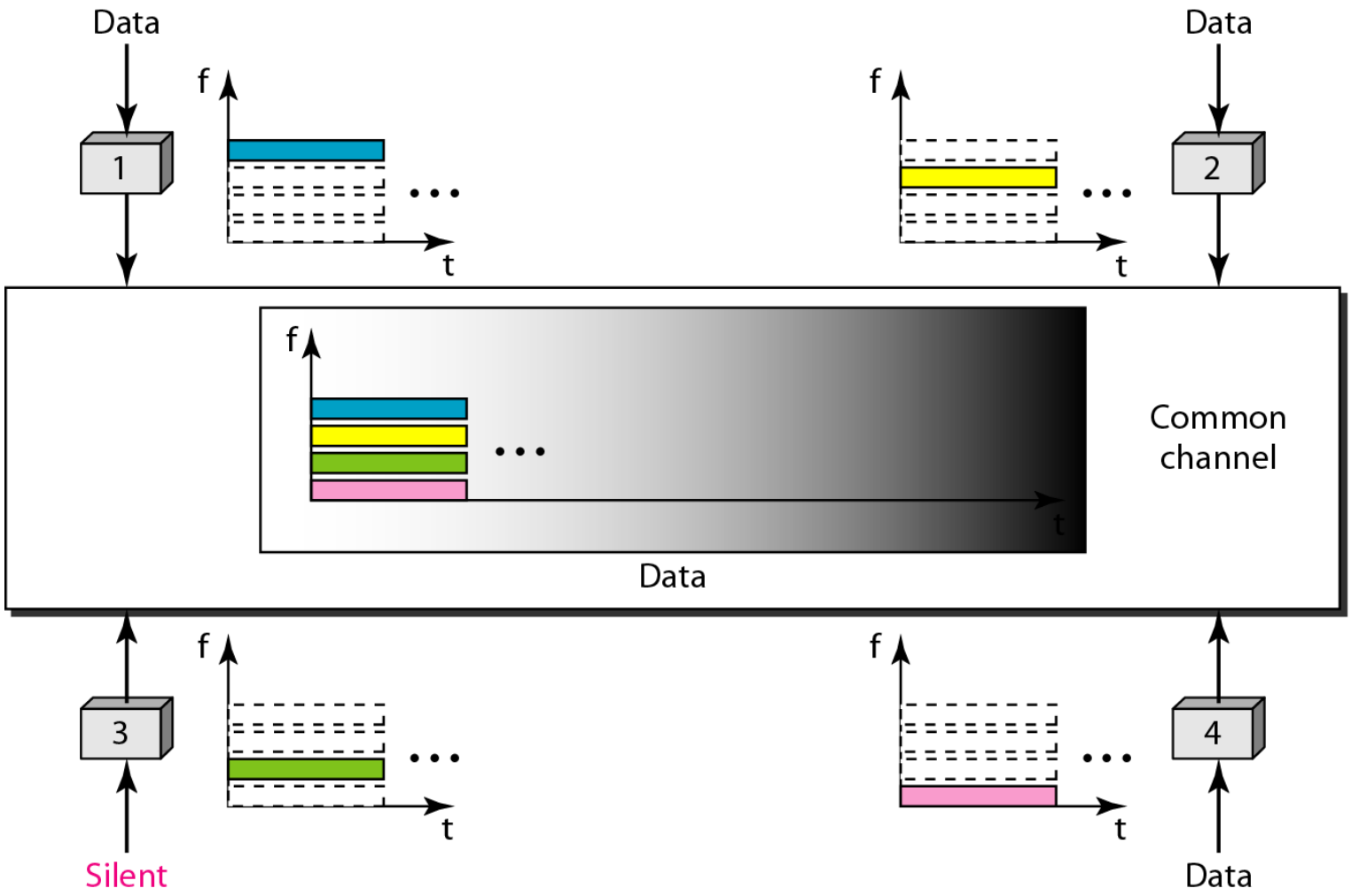
3. Taking-turns protocols
   - ✓ Nodes take turns but nodes with more to send can take longer turns.
   - ✓ Examples of taking-turns protocols
     - Polling
     - Token passing

FDMA: Frequency Division Multiple Access

- Channel spectrum divided into frequency bands.
- Each station assigned fixed frequency band.
- Unused transmission time in frequency bands go idle.
- Different Frequency Band for Different User
- Its 1st Generation
- Example: 6-station LAN, 1,3,4 have p[illegible]t, frequency bands 2,5,6 idle

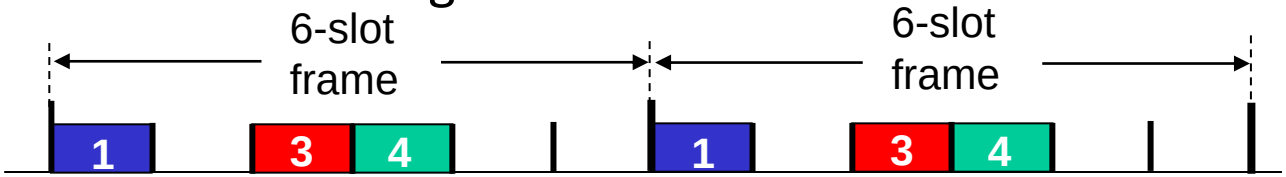


Frequency-division multiple access (FDMA)



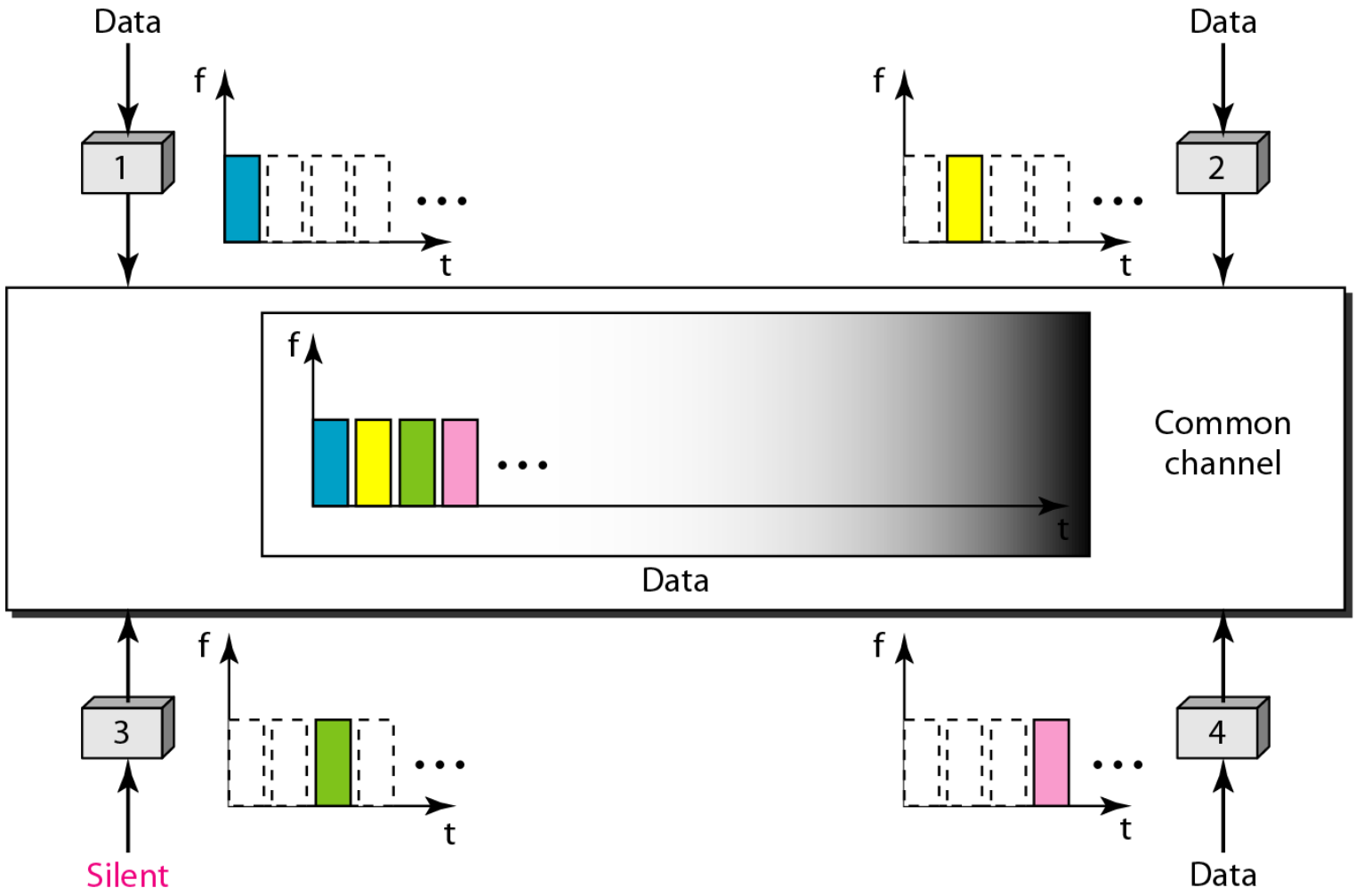
TDMA: Time Division Multiple Access

- Suppose the channel supports N nodes and that the transmission rate of the channel is R bps.
- TDM divides time into time frames and further divides each time frame into N time slots.
- Each time slot is then assigned to one of the N nodes.



- Example: 6-station LAN, 1,3,4 have packet, slots 2,5,6 idle
- Major drawbacks: First, A node is limited to an average rate of R/N bps even when it is the only node with packets to send.
- Second drawback is that a node must always wait for its turn in the transmission sequence again, even when it is the only node with a frame to send.
- 2nd Generation: TDMA
- Problem of Delay
- GSM, GPRS

Time-division multiple access (TDMA)



CDMA: Code Division Multiple Access

- CDMA assigns a different code to each node, While TDM and FDM assign time slots and frequencies respectively.
- Each node then uses its unique code to encode the data bits it sends.
- If the codes are chosen carefully, CDMA networks have the wonderful property that different nodes can transmit simultaneously.
- Their respective receivers correctly receive a sender's encoded data bits in spite of interfering transmissions by other nodes.
- Example: Used in military and widespread civilian use, particularly in cellular telephony.
- Because CDMA's use is so tightly tied to wireless channels.

ALOHA

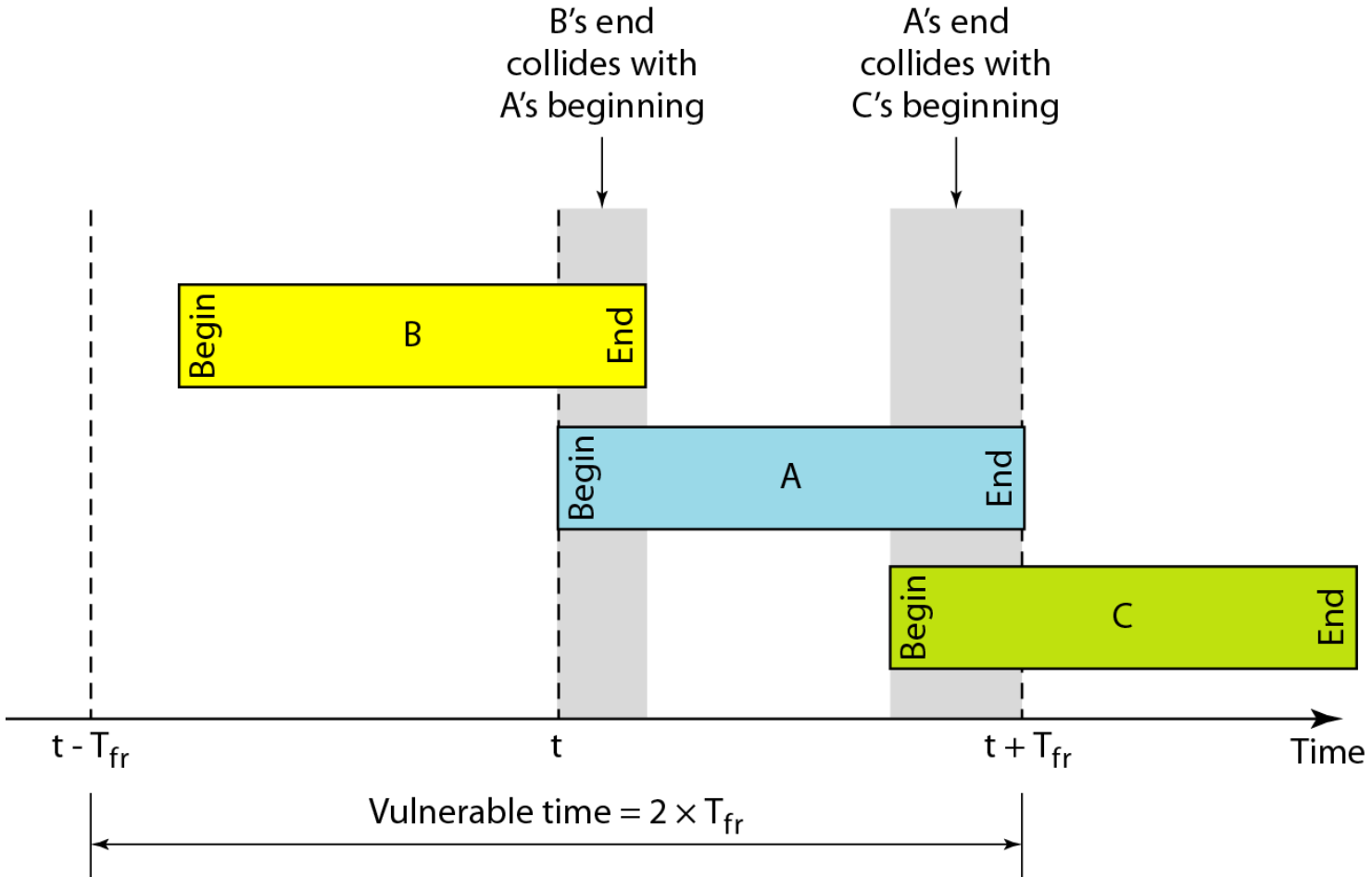
- Aloha is a random access protocol
- Is was actually designed for WLAN but it is also applicable for shared medium.
- In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

Pure Aloha Protocol

- It allows users to transmit whenever they have data to be sent.
- Senders wait to see if a collision occurred (after whole message has been sent).
- If collision occurs, each station involved waits a random amount of time then tries again.
- Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention systems.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
- If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

- Pure ALOHA allows stations to transmit whenever they have data to be sent.
- When a station sends data it waits for an acknowledgement.
- If the acknowledgement does not come within the allotted time then the station waits for a random amount of time called back-off time and re-sends the data.
- Since different stations wait for different amount of time, the probability of further collision decreases.

- Whenever two frames try to occupy the channel at the same time there will be a collision and both will be garbled.
- If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

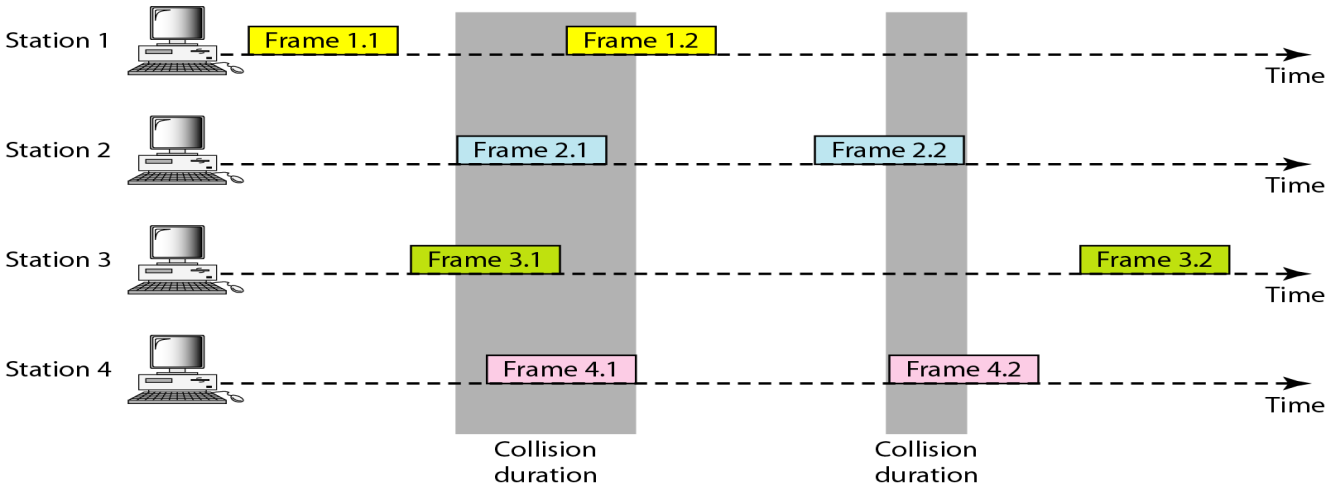


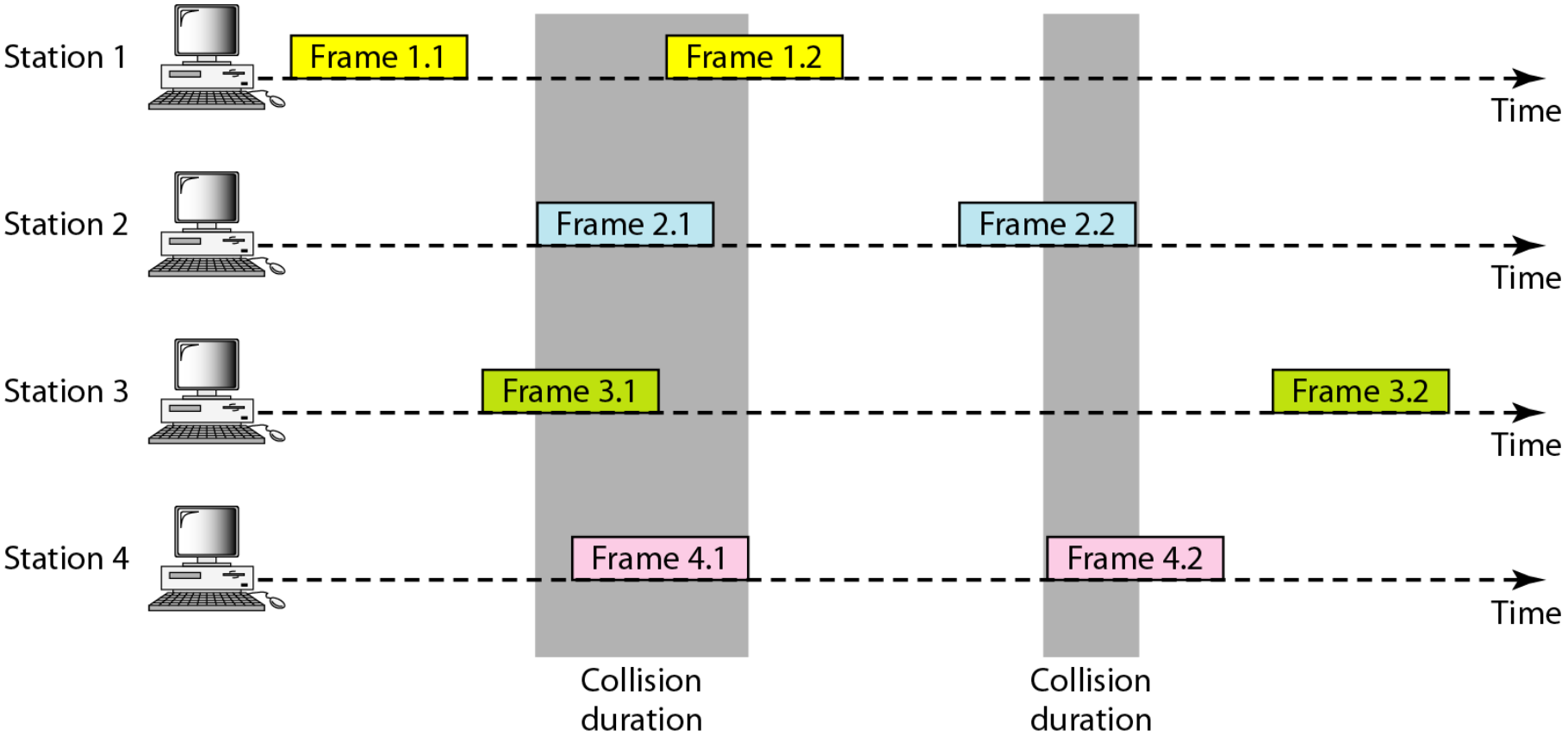
Pure ALOHA – Cont…

- Frames are transmitted at completely arbitrary times.
- The throughput of the Pure ALOHA is maximized when the frames are of uniform length.
- The formula to calculate the throughput of the Pure ALOHA is

$$S=G*e^{-2G}$$

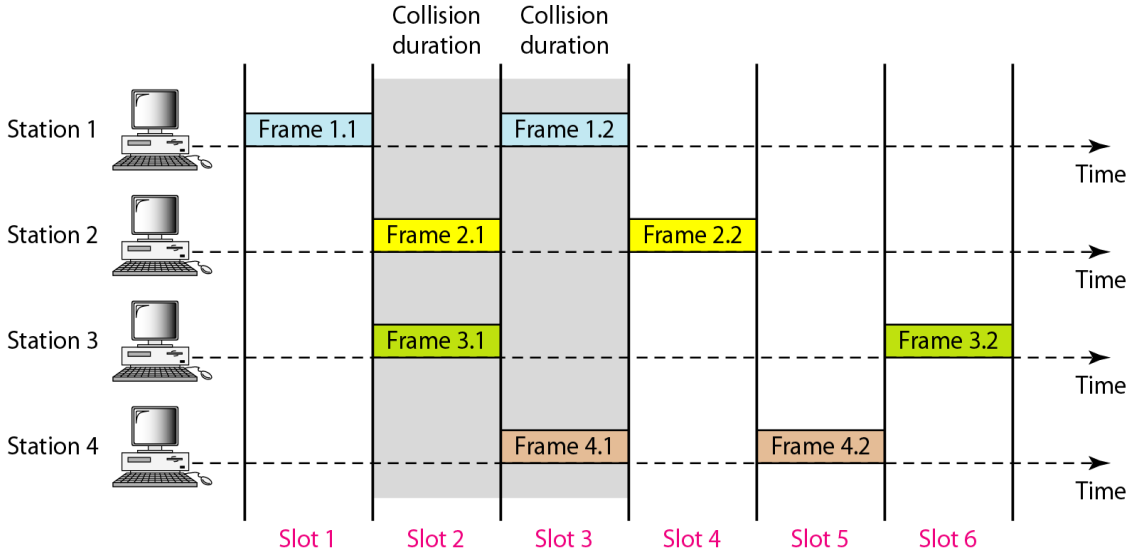
- The throughput is maximum when G=1/2 which is 18% of the total transmitted data frames.




Station 1
Frame 1.1
Frame 1.2
Time
Station 2
Frame 2.1
Frame 2.2
Time
Station 3
Frame 3.1
Frame 3.2
Time
Station 4
Frame 4.1
Frame 4.2
Time
Collision duration
Collision duration

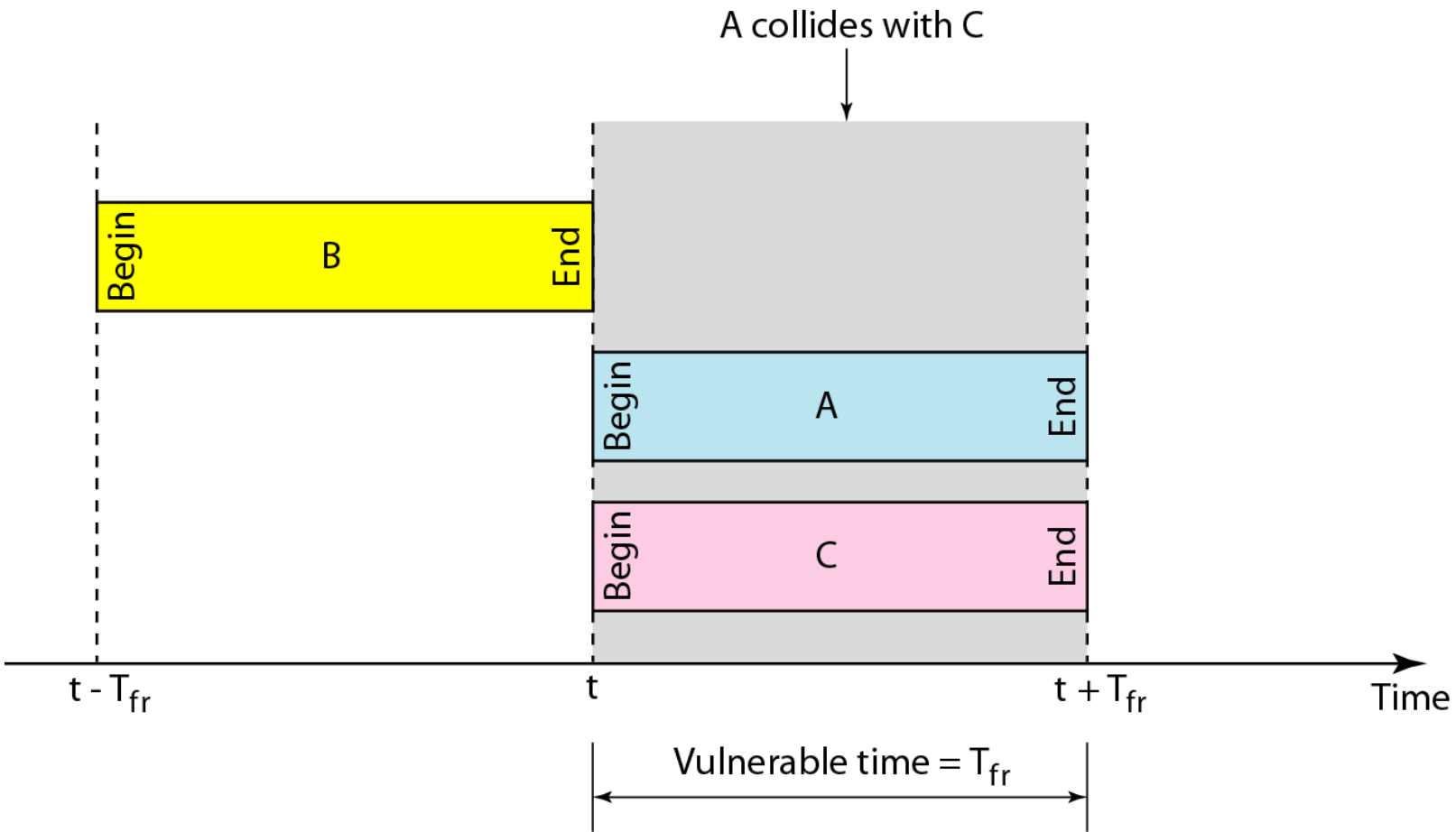
Slotted Aloha

- It was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- The time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.

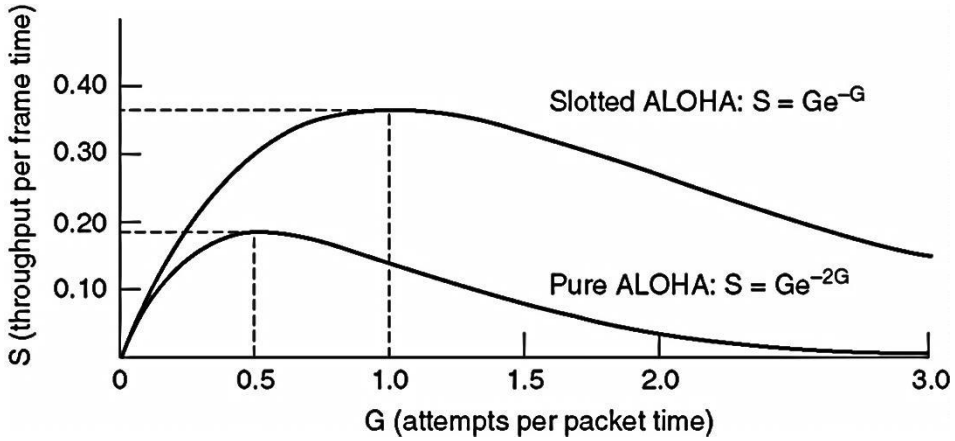


Slotted ALOHA

- If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.



Slotted Aloha – Cont…



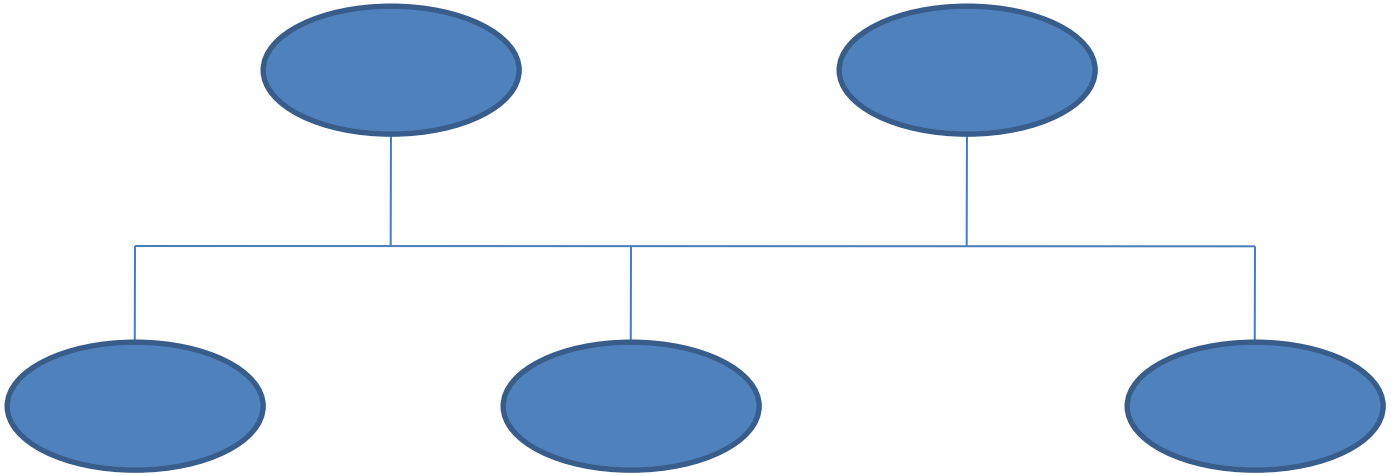
- If any station is not able to place the frame onto the channel at the beginning of the slot then the station has to wait until the beginning of the next time slot.
- The formula to calculate the throughput of the Slotted ALOHA is

  $S=G*e^{-G}$

- The throughput is maximum when G=1 which is 37% of the total transmitted data frames.
- 37% of the time slot is empty, 37% successes and 26% collision.

CSMA

- To minimize the chance of collision and therefore, increase the performance, the CSMA method was developed.
- Principle of CSMA **“Sense before transmit”** or **“Listen before talk”**



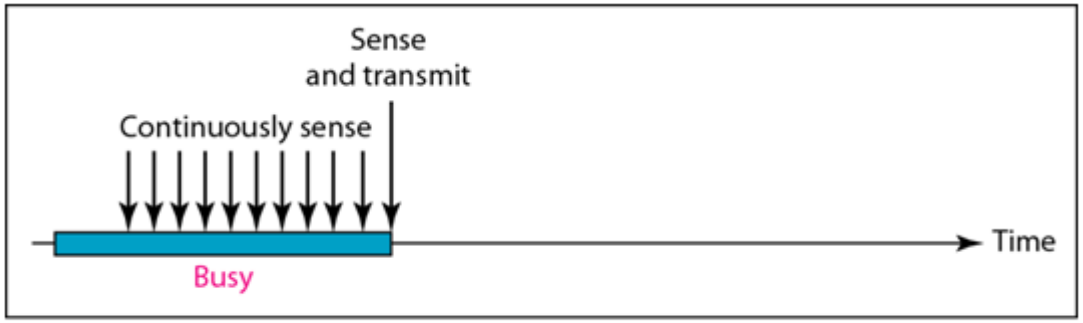
- Carrier busy: Transmission is taking Place
- Carrier idle: No Transmission currently taking Place

Types of CSMA

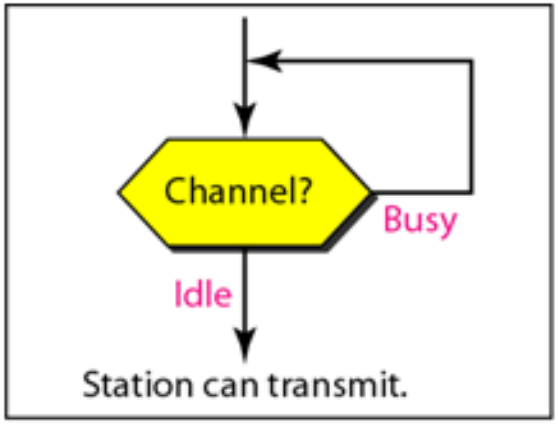
- 1-Persistent CSMA
- Non-Persistent CSMA
- P-Persistent CSMA

1 – Persistent CSMA

- Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
- *If the channel is idle*, the station transmits a frame.
- *If channel is busy*, then it senses the transmission medium **continuously** until it becomes idle.
- Since the station transmits the frame with the probability of 1 when the carrier or channel is idle, this scheme of CSMA is called as **1-Persistent CSMA**.



a. 1-persistent

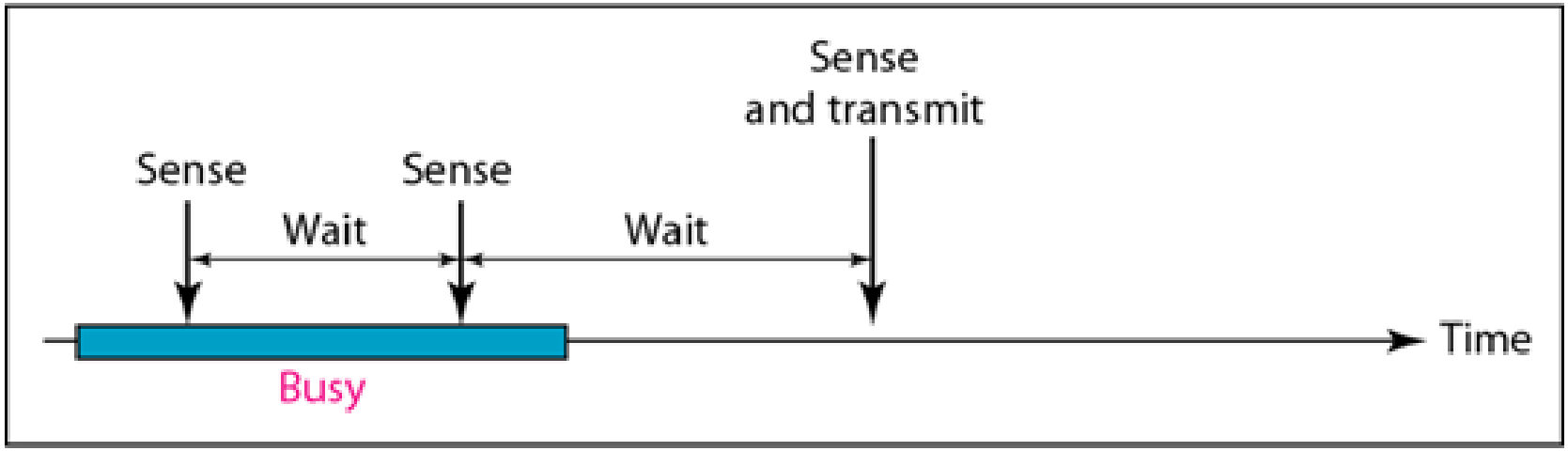


a. 1-persistent

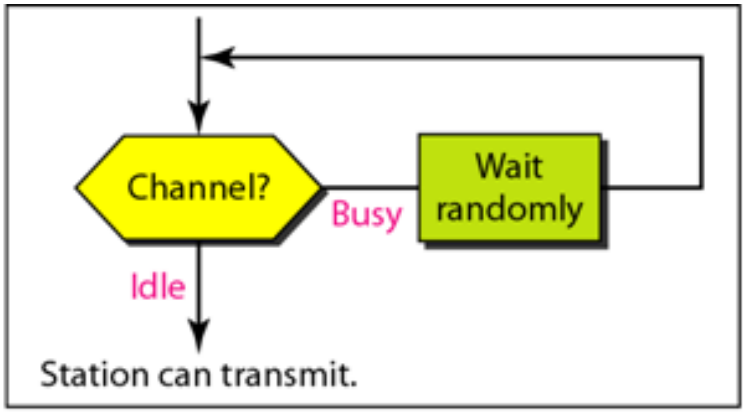
Non-Persistent CSMA

- Before sending, a station senses the channel.
- If no one else is sending, the station begins doing so itself.
- In the non-persistent method,
  - ✓ a station that has a frame to send senses the line.
  - ✓ If the line is idle, it sends immediately.
  - ✓ If the line is not idle, it waits a **random amount of time** and then senses the line again.
- The non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.
- However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

Non-Persistent CSMA



b. Nonpersistent

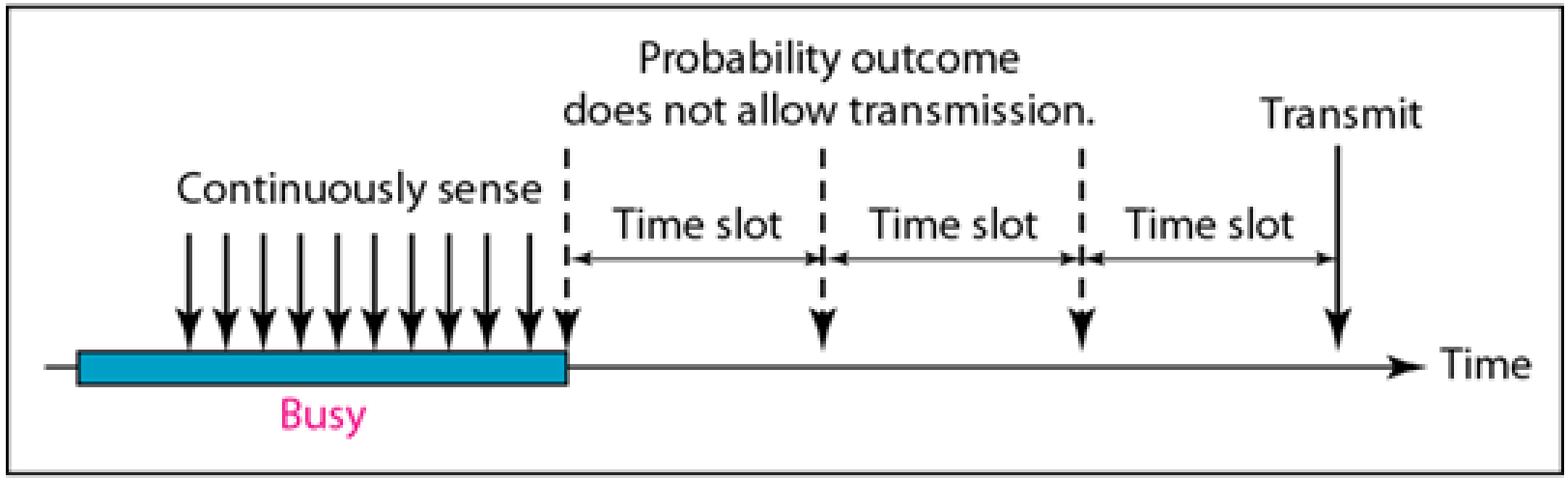


b. Nonpersistent

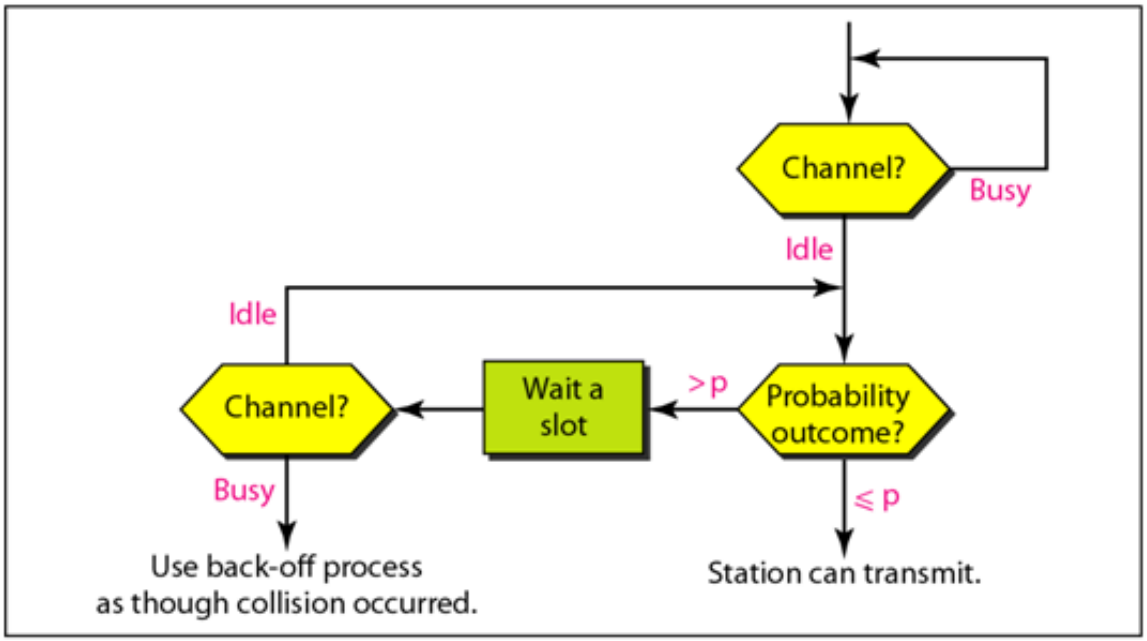
P-Persistent

- The **p-persistent method** is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.
- The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency.
- **In this method, after the station finds the line idle it follows these steps:**
  1. With probability *p, the station sends its frame.*
  2. With probability *q = 1 - p, the station waits for the beginning of the next time slot* and checks the line again.
     a. If the line is idle, it goes to step 1.
     b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

P-Persistent



c. p-persistent

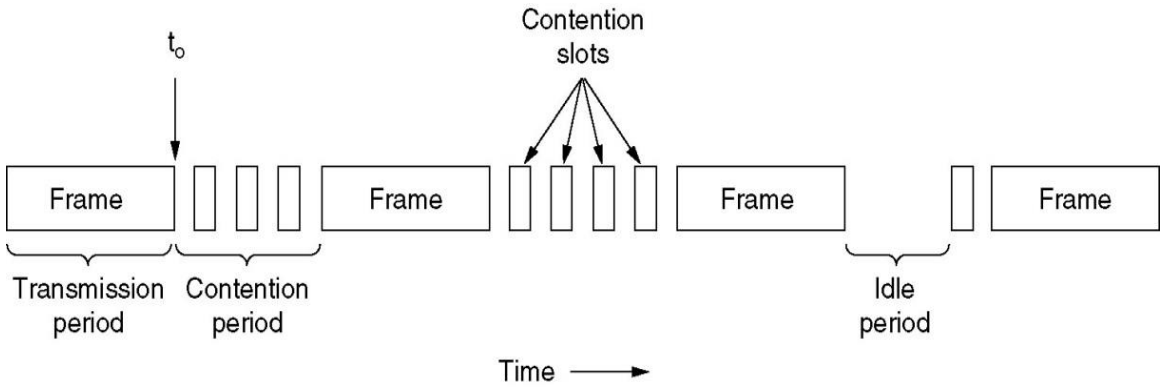


c. p-persistent

CSMA/CD

- If two stations sense the channel to be idle and g=begin transmitting simultaneously, they will both detect the collision almost immediately.
- Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collision is detected.
- Quickly terminating damaged frames saves time and bandwidth.
- This protocol, known as CSMA/CD is widely used on LAN in MAC sublayer.

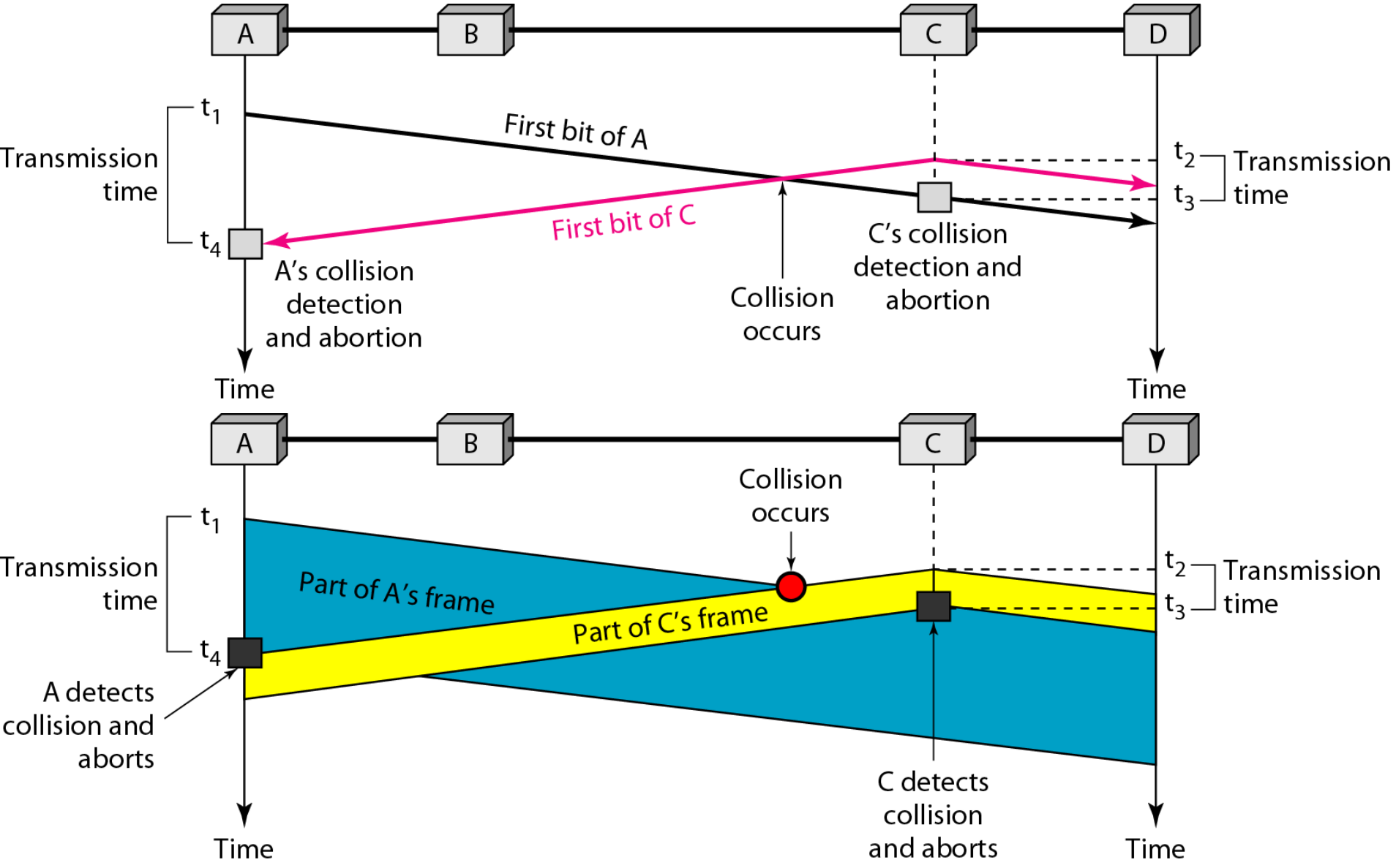
CSMA/CD – Cont…



- At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so.
- After a station detects a collision, it aborts transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.
- Therefore, CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

CSMA/CD (CSMA with Collision Detection)

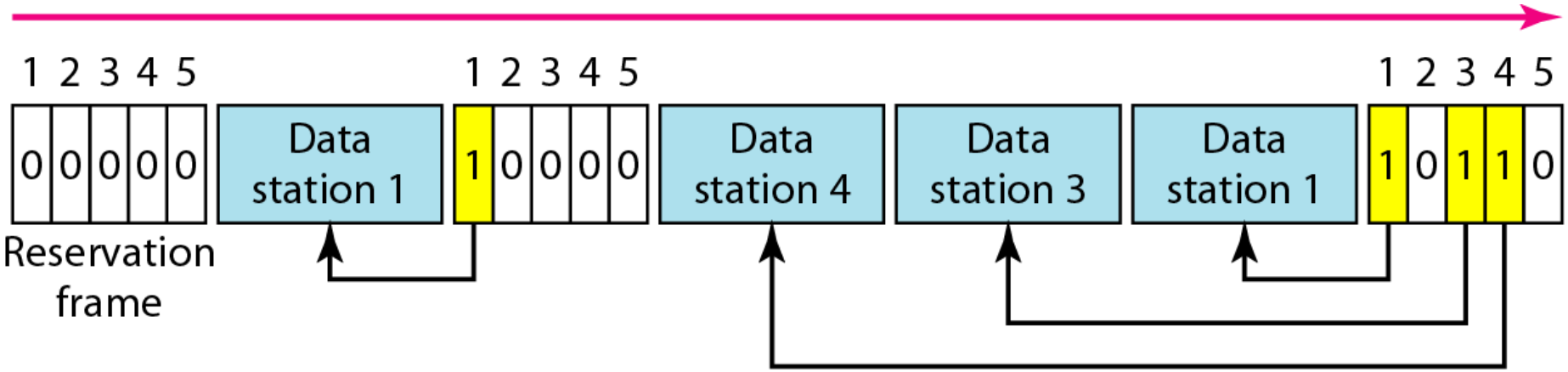
- If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
- Rather than finish transmitting, they should abruptly stop transmitting as soon as the collision is detected.
- Quickly terminating damaged frames saves time and bandwidth.
- This protocol, known as CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sub layer.


A
B
C
D
t_1
Transmission time
t_4
First bit of A
First bit of C
A's collision detection and abortion
Collision occurs
C's collision detection and abortion
t_2
t_3
Transmission time
Time
Time
A
B
C
D
Collision occurs
t_1
Transmission time
t_4
Part of A's frame
Part of C's frame
t_2
t_3
Transmission time
A detects collision and aborts
C detects collision and aborts
Time
Time

Reservation

- A Station need to make a reservation before sending data.
- In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame.
- Each mini slot belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own mini slot.
- The Stations that have made reservations can send their data frames after the reservation frame.

Reservation

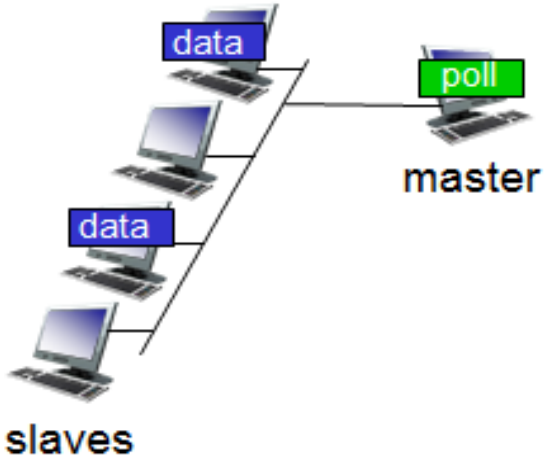


Polling

- It requires one of the nodes to be designated as a master node.
- The master node polls each of the nodes in a round-robin fashion.
- The master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames.
- After node 1 transmits some frames, the master node tells node 2 it (node 2) can transmit up to the maximum number of frames.
- The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.

Polling – Cont…

- The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

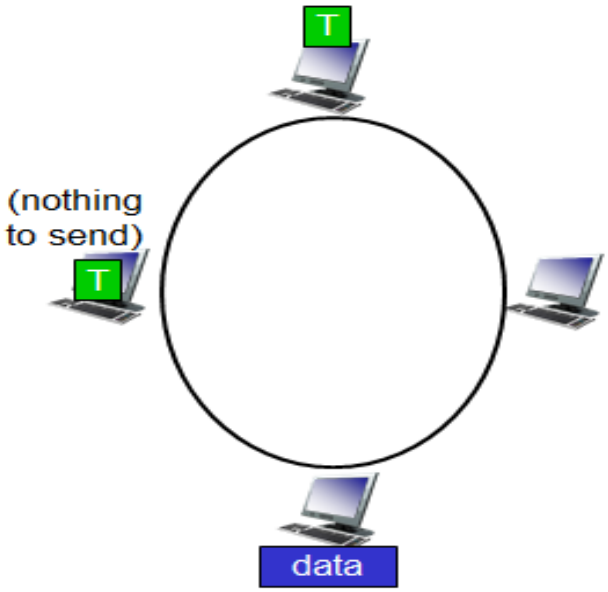


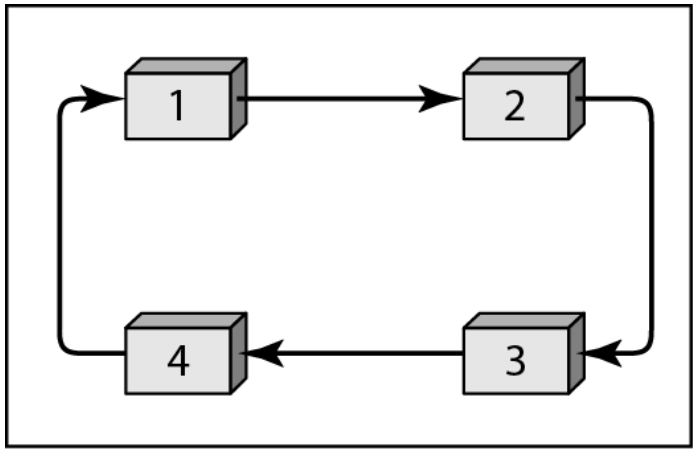
- The polling protocol eliminates the collisions and empty slots that plague random access protocols.

- A station is authorized to send data when it receives a special frame called a token.
- Here there is no master node.

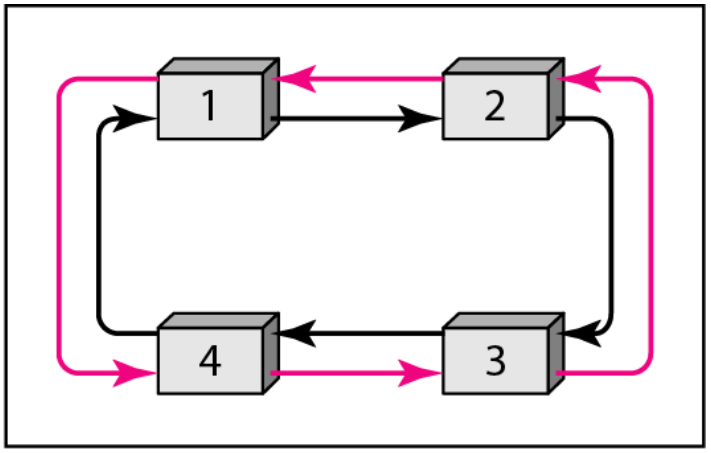
Token Passing

- There is no master node.
- A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.
- For example, node 1 might always send the token to node 2, node 2 might always send the token to node 3, and node N might always send the token to node 1.
- 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.
- If failure of one node can crash the entire channel. Or if a node accidentally neglects to release the token.

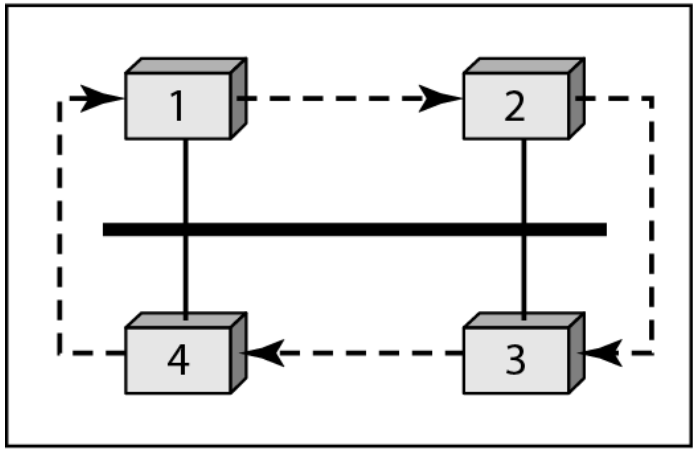




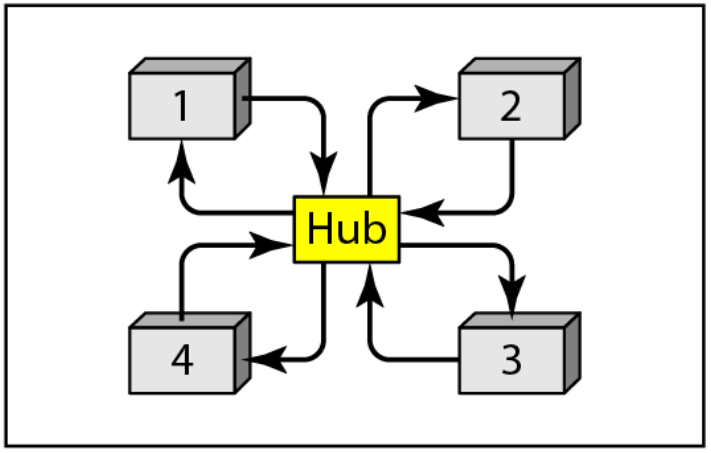
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

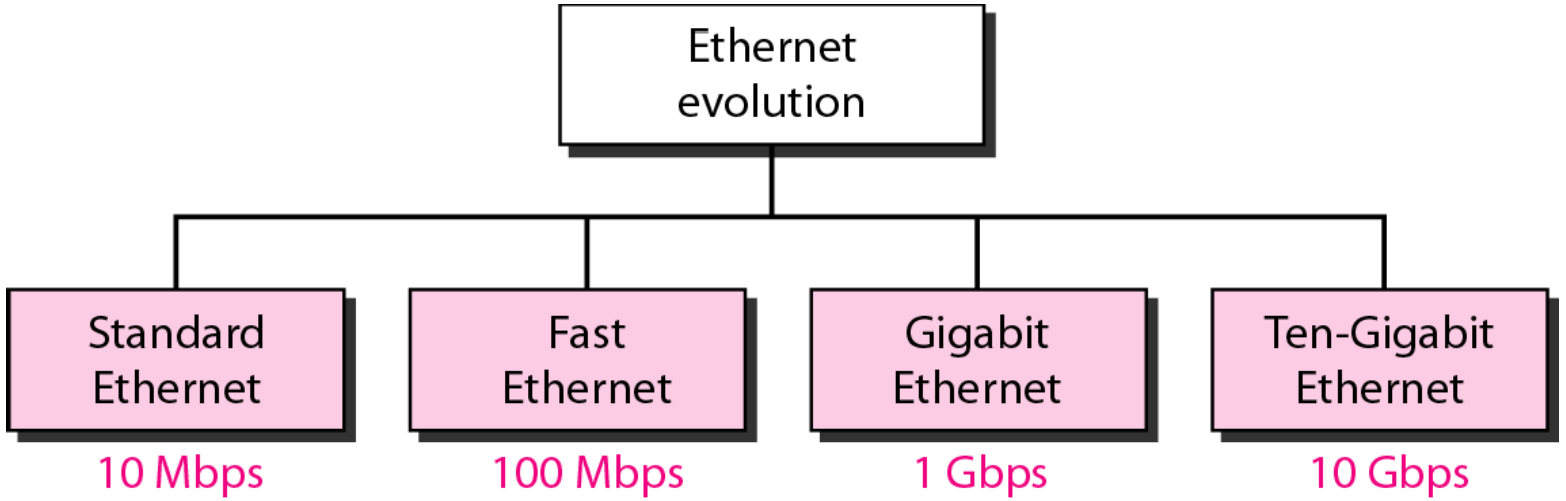
Ethernet

- Ethernet is one of the widely used local area network (LAN) technology.

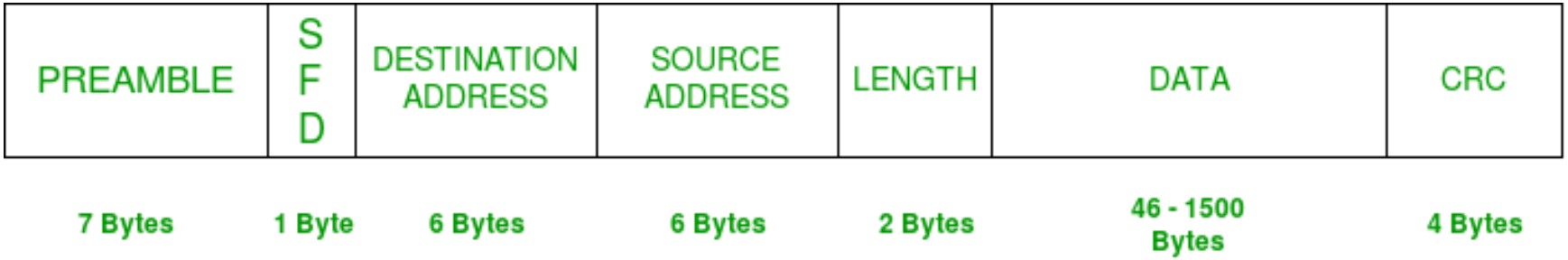
1. Switched Ethernet
   - ✓ It gives dedicated 10 Mbps bandwidth on each of its ports.
   - ✓ On each of the ports one can connect either a thick/thin segment or a computer.
2. Fast Ethernet
   - ✓ The 802.u or the fast Ethernet was approved by the IEEE 802 Committee.
   - ✓ It uses the same frame format, same CSMA/CD protocol and same interface as the 802.3, but uses a data transfer rate of 100 Mbps instead of 10 Mbps.
   - ✓ Fast Ethernet is based entirely on 10-Base-T.

Ethernet – Cont…

3. Gigabit Ethernet
   - ✓ Gigabit Ethernet is carried primarily on optical fiber (with very short distances possible on copper media).
   - ✓ Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone.
   - ✓ An alternative technology that competes with Gigabit Ethernet is ATM.
   - ✓ A newer standard, 10-Gigabit Ethernet is also becoming available.



Ethernet (IEEE 802.3) Frame Format



IEEE 802.3 ETHERNET Frame Format

Bit Stuffing

- In a bit-oriented protocol, the data to send is a series of bits.
- In order to distinguish frames, most protocols use a bit pattern of 8-bit length (01111110) as flag at the beginning and end of each frame.
- Here also cause the problem of appearance of flag in the data part to deal with this an extra bit added.
- This method is called bit stuffing.
- If a 0 and five successive 1 bits are encountered, an extra 0 is added.
- The receiver node removes the extra-added zero.

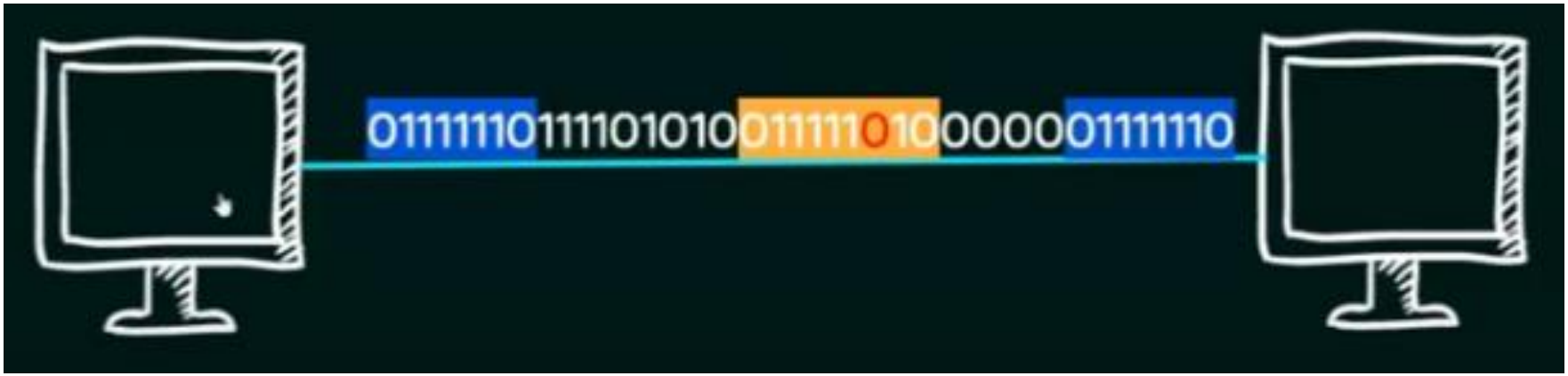
Bit Stuffing - Example

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

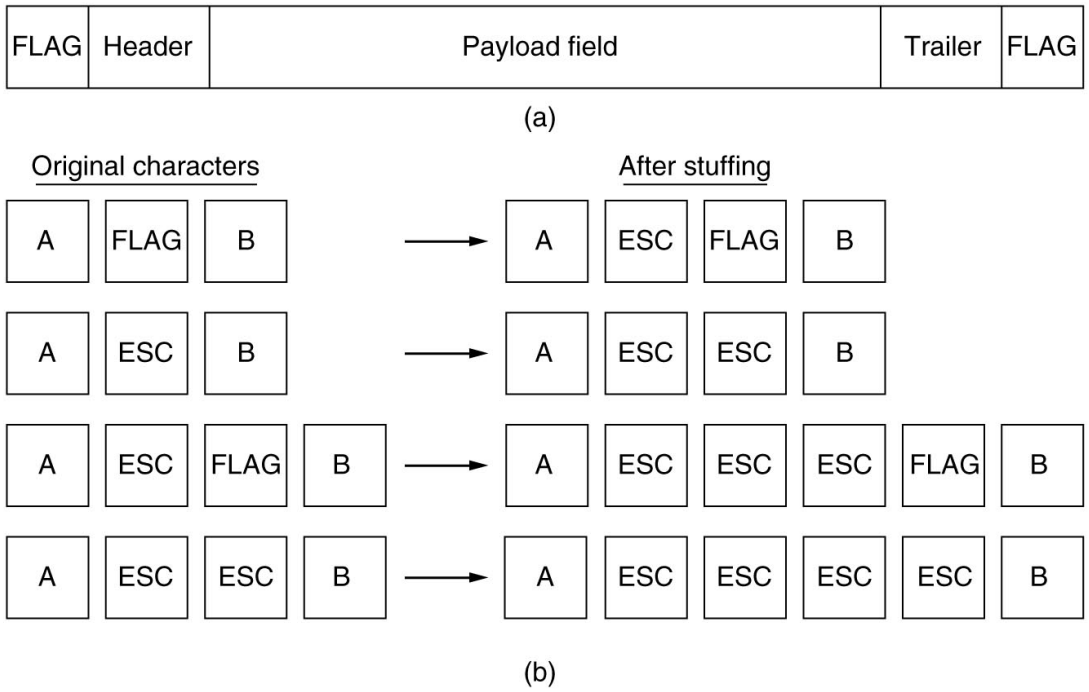


Byte Stuffing

- Problem of resynchronization by having each frame start and end with special bytes.
- A flag byte is used to separate the frame as both the starting and ending delimiter.
- This technique is called *byte stuffing* or *character stuffing*.
- In this way, if the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame.
- Two consecutive flag bytes indicate the end of one frame and start of the next one.

Byte Stuffing - Example

- To solve this problem, is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data.
- The data link layer on the receiving end removes the escape byte before the data are given to the network layer.



Thank You