

Module 3

Data Link Layer

NETWORK AND COMMUNICATION



Theory_Class_12

Error Detection and Correction

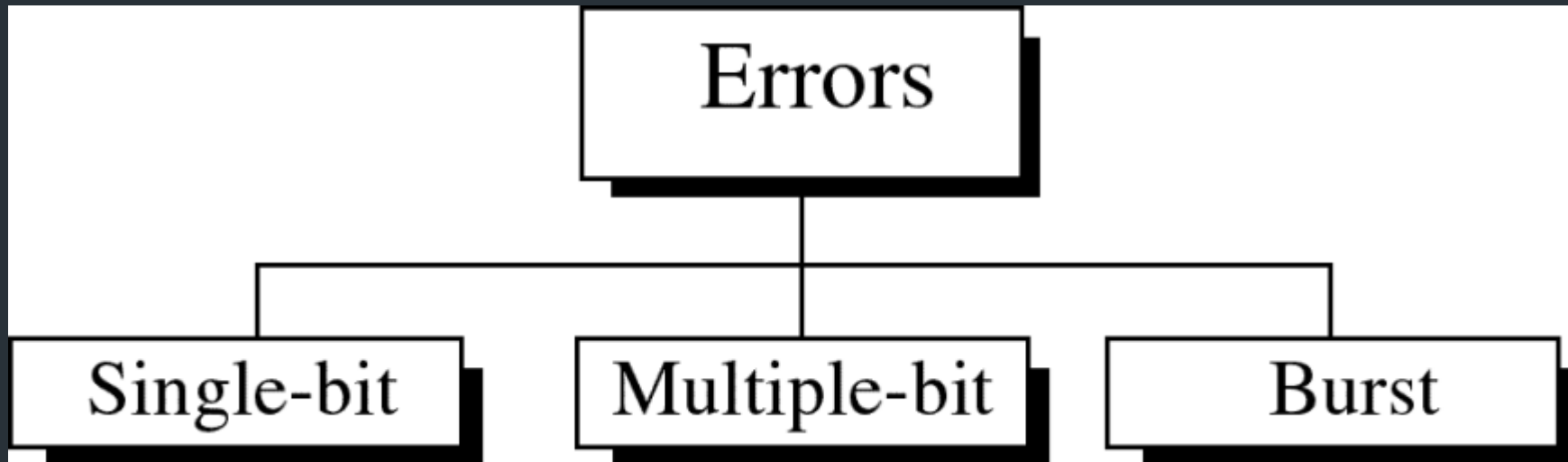
Overview

- **Types of Errors**
- **Detection**
- **Correction**

Basic concepts

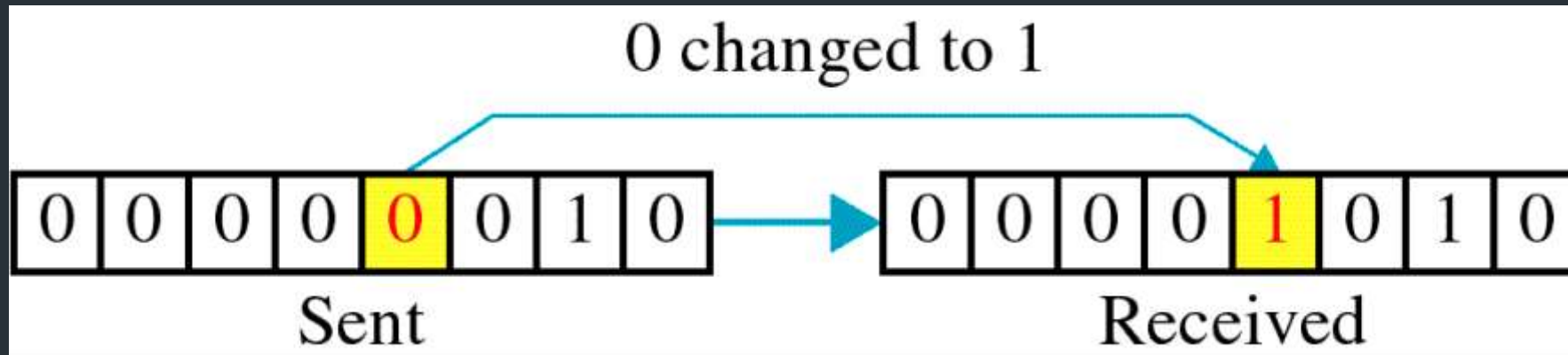
- Networks must be able to transfer data from one device to another with complete accuracy.
- Data can be corrupted during transmission.
- For reliable communication, errors must be detected and corrected.
- **Error detection and correction** are implemented either at the **data link layer** or the **transport layer** of the OSI model.

Types of Errors



Source: Data Communications and Networking – Behrouz A. Forouzan

Single-bit error



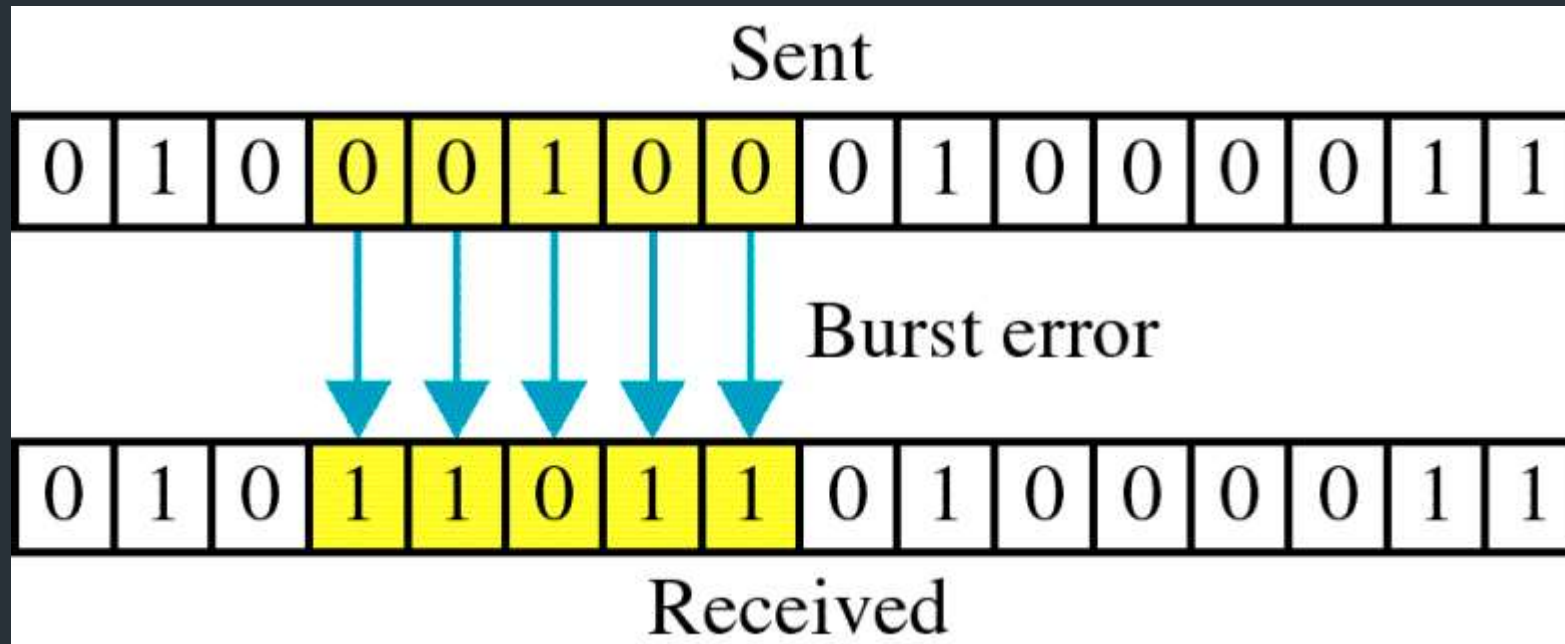
Source: Data Communications and Networking – Behrouz A. Forouzan

Single bit errors are the **least likely** type of errors in serial data transmission because the noise must have a very short duration which is very rare. However this kind of errors can happen in parallel transmission.

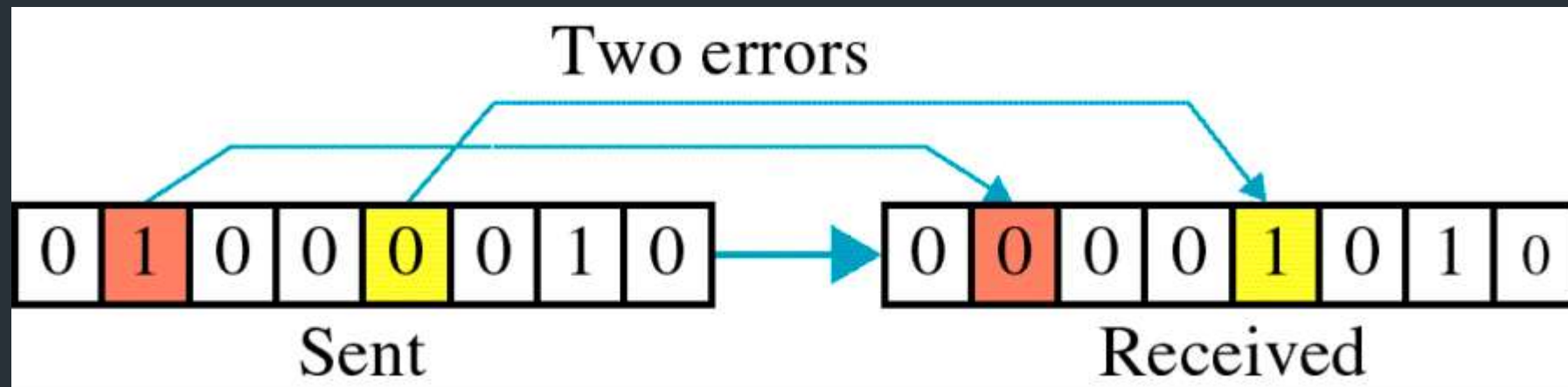
Example:

- If data is sent at 1Mbps then each bit lasts only $1/1,000,000$ sec. or $1\ \mu\text{s}$.
- For a single-bit error to occur, the noise must have a duration of only $1\ \mu\text{s}$, which is very rare.

Burst error



Source: Data Communications and Networking – Behrouz A. Forouzan



Source: Data Communications and Networking – Behrouz A. Forouzan

The term **burst error** means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst errors does not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

- **Burst error is most likely to happen in serial transmission** since the duration of noise is normally longer than the duration of a bit.
- The number of bits affected depends on the data rate and duration of noise.

Example:

- If data is sent at rate = 1Kbps then a noise of 1/100 sec can affect 10 bits. $(1/100 * 1000)$
- If same data is sent at rate = 1Mbps then a noise of 1/100 sec can affect 10,000 bits. $(1/100 * 10^6)$

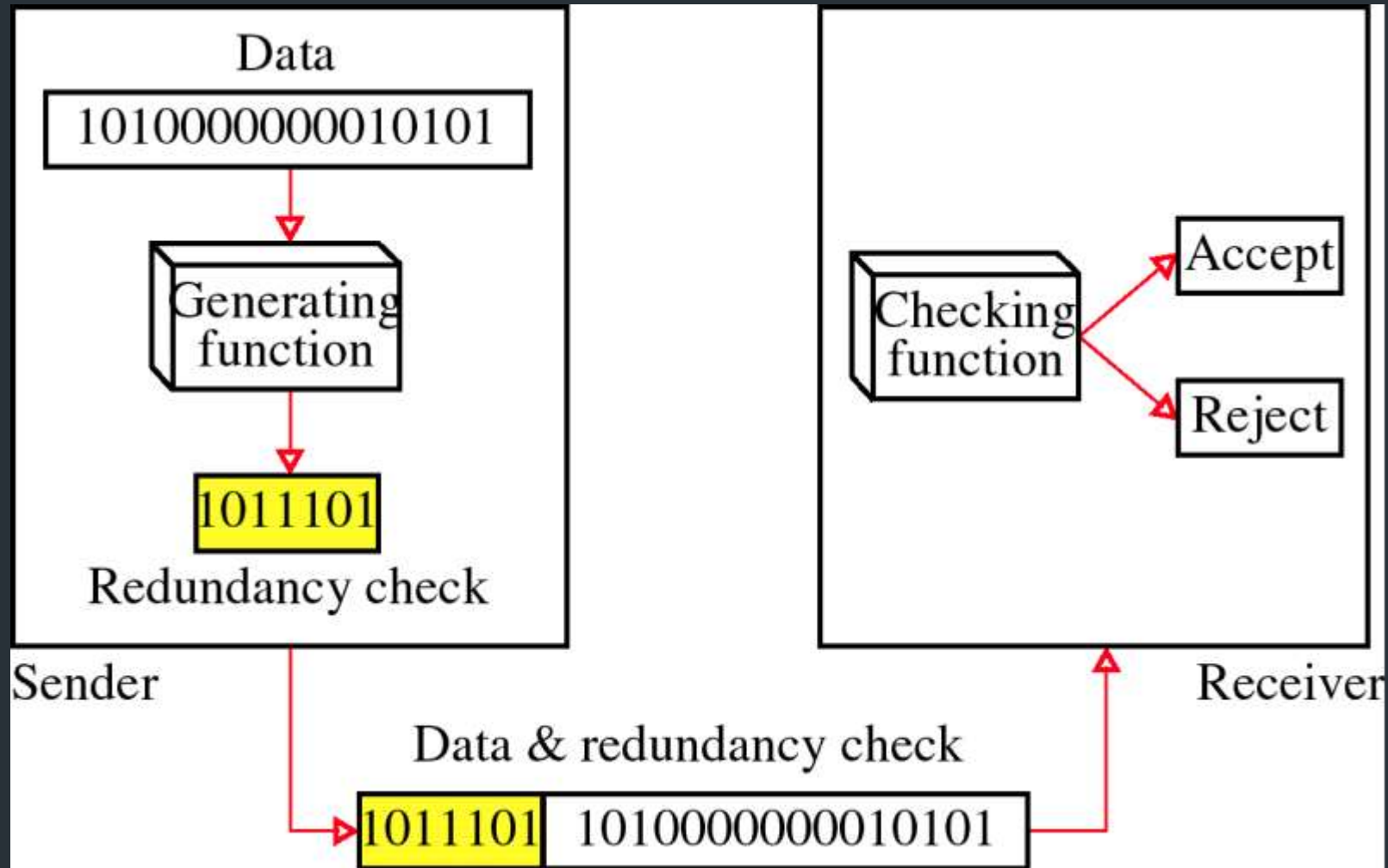
Error detection

Error detection means to decide whether the received data is correct or not without having a copy of the original message.

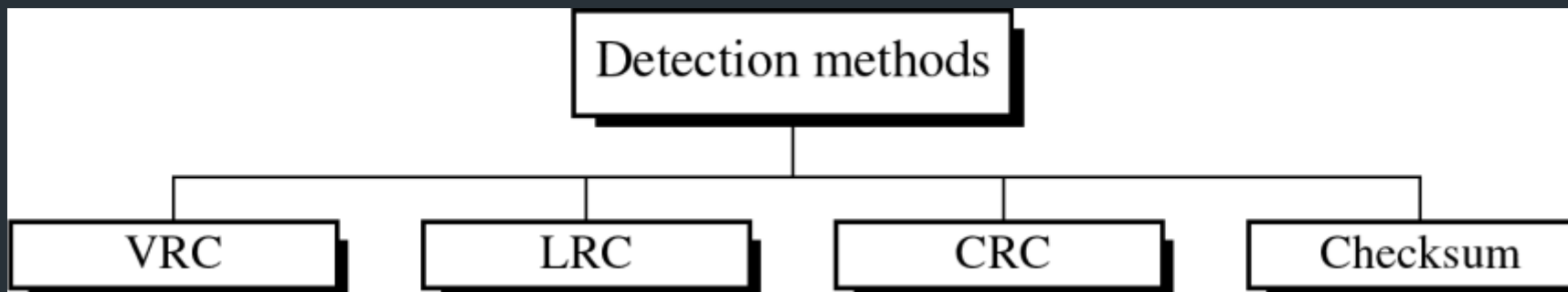
Error detection **uses the concept of redundancy, which means** adding extra bits for detecting errors at the destination.

Redundancy

13

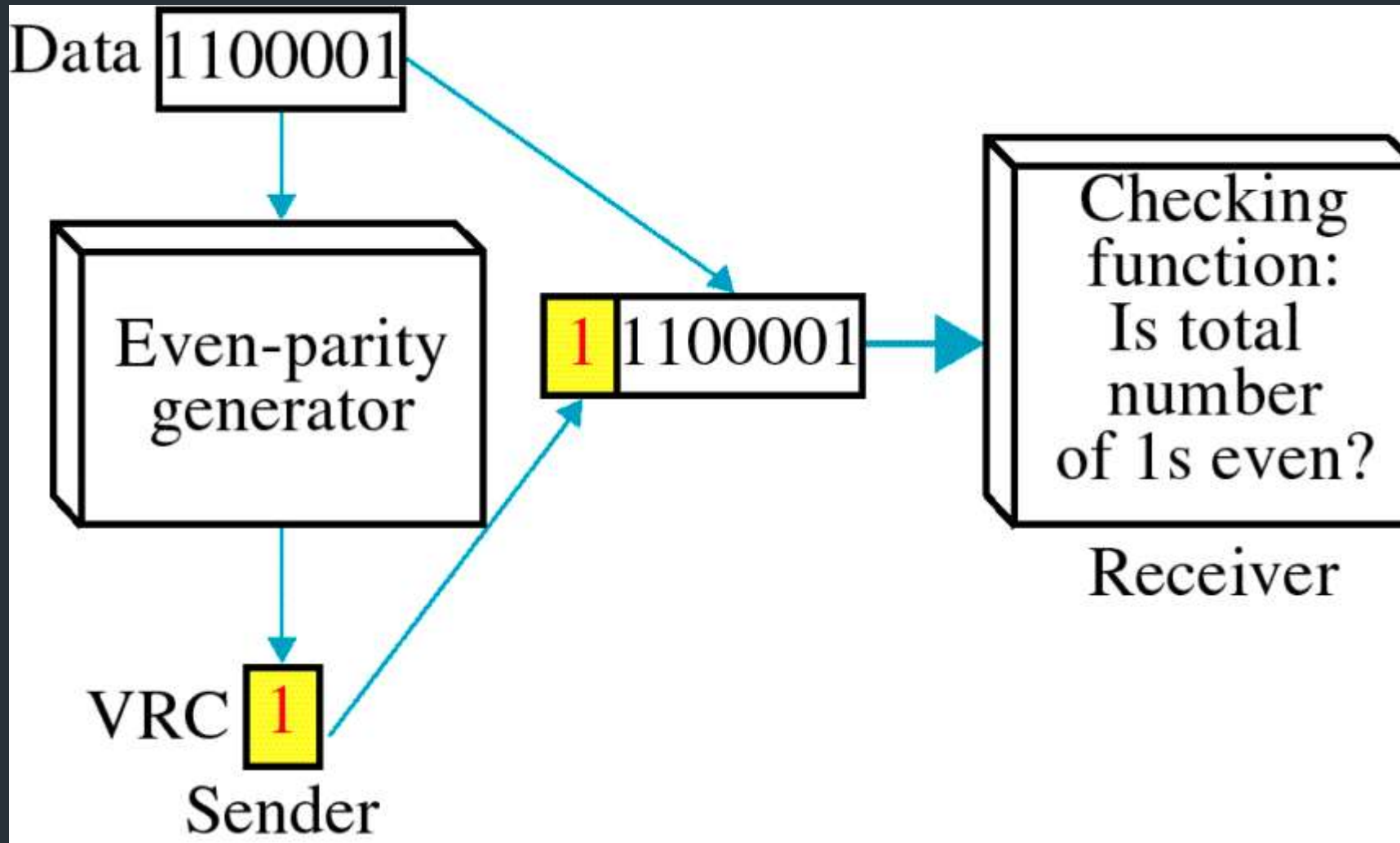


Four types of redundancy checks are used in data communications



Vertical Redundancy Check VRC

15

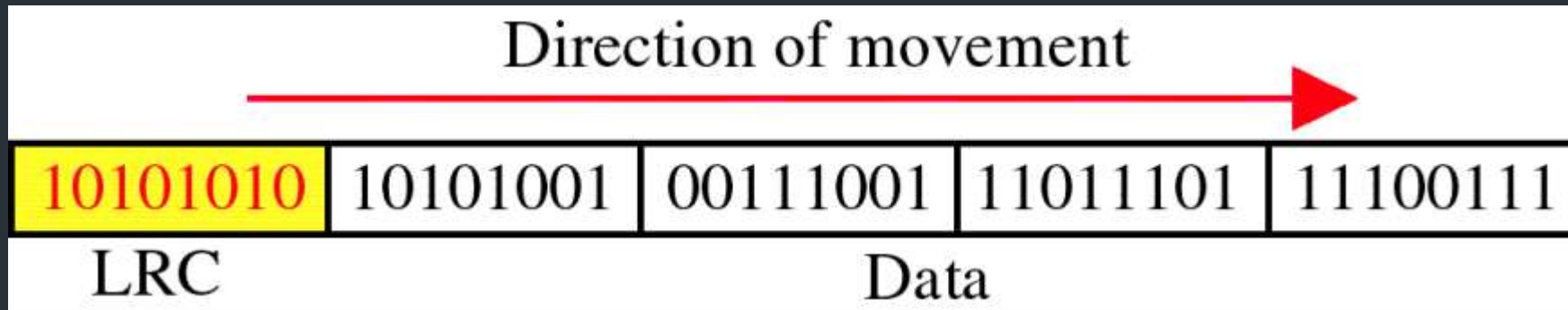


Performance

- It can detect single bit error
- It can detect burst errors only if the total number of errors is odd.

Longitudinal Redundancy Check LRC

17

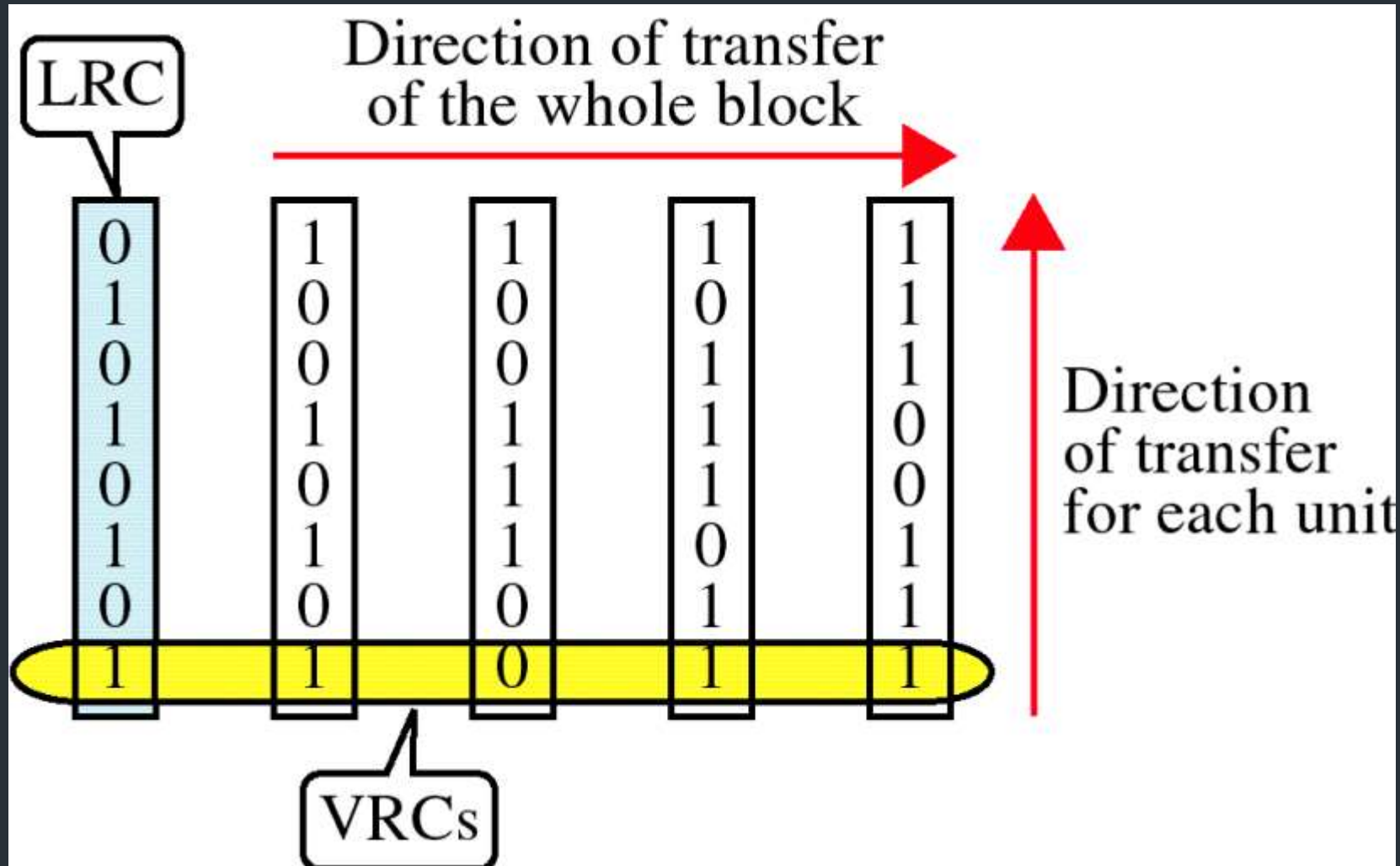


Source: Data Communications and Networking – Behrouz A. Forouzan

Performance

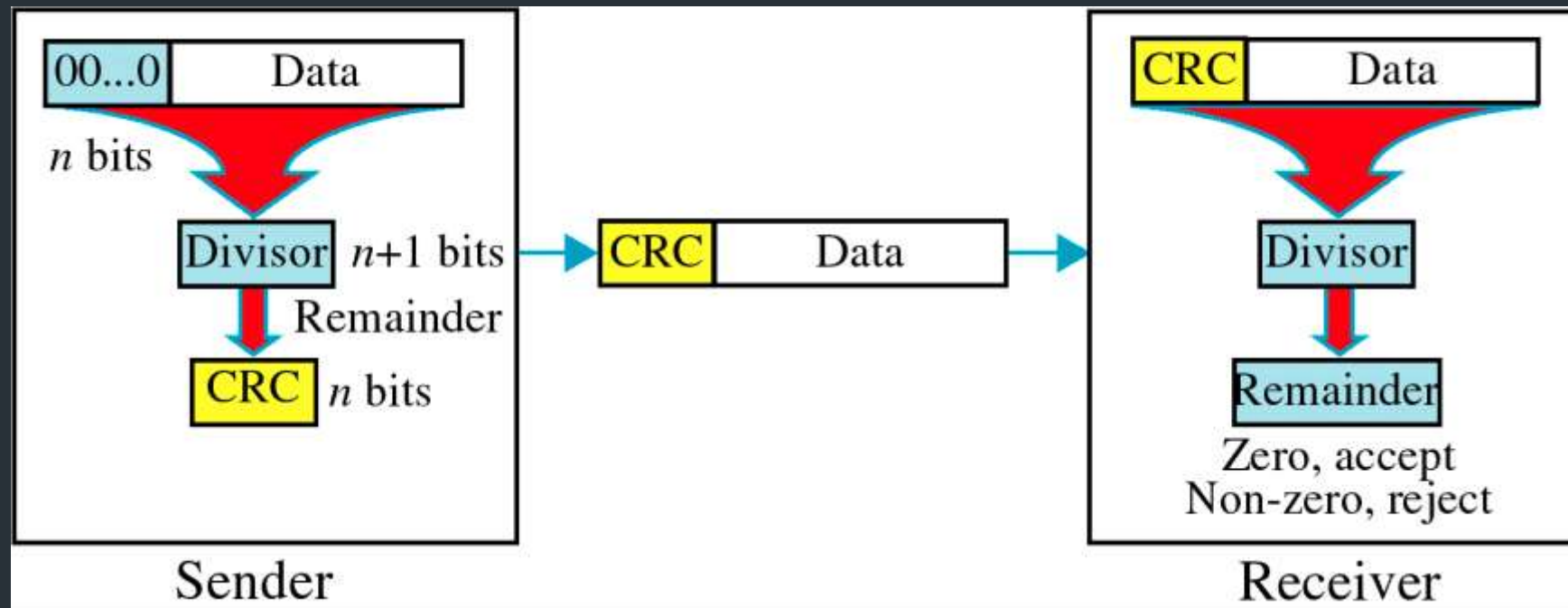
- LCR increases the likelihood of detecting burst errors.
- If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.

VRC and LRC



Cyclic Redundancy Check CRC

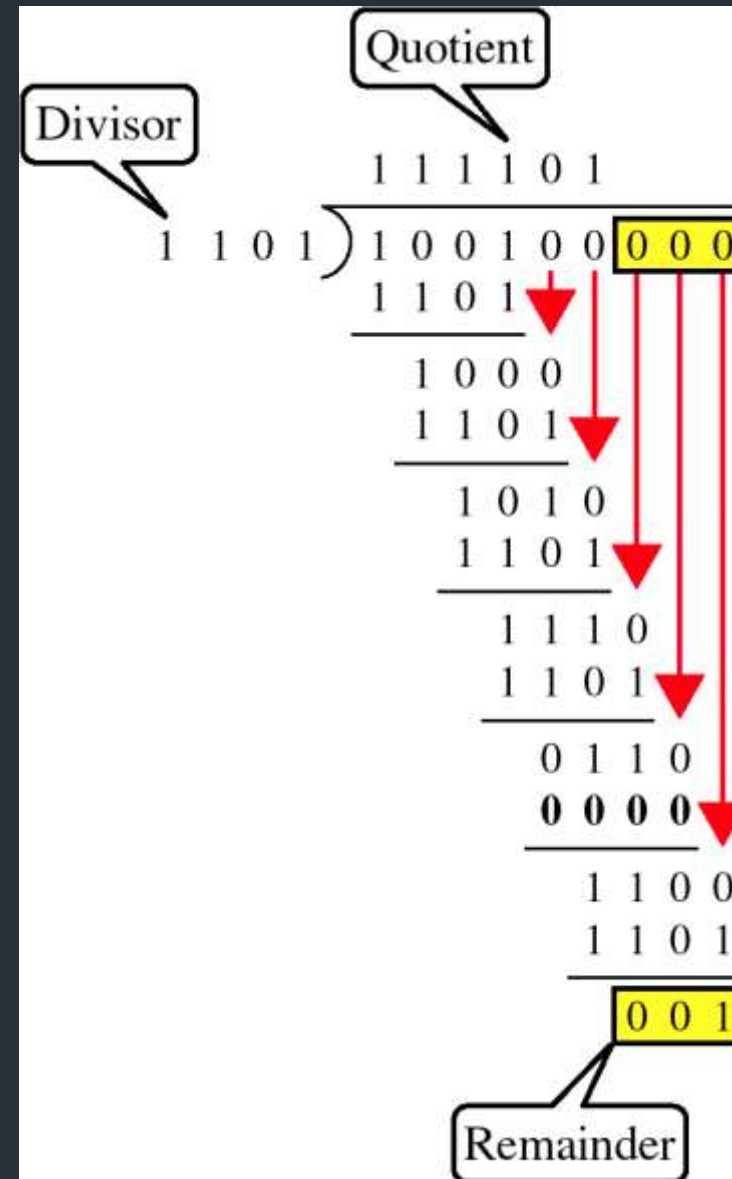
20



Cyclic Redundancy Check

- Given a k -bit frame or message, the transmitter generates an n -bit sequence, known as a *frame check sequence (FCS)*, so that the resulting frame, consisting of $(k+n)$ bits, is exactly divisible by some predetermined number.
- The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

Binary Division



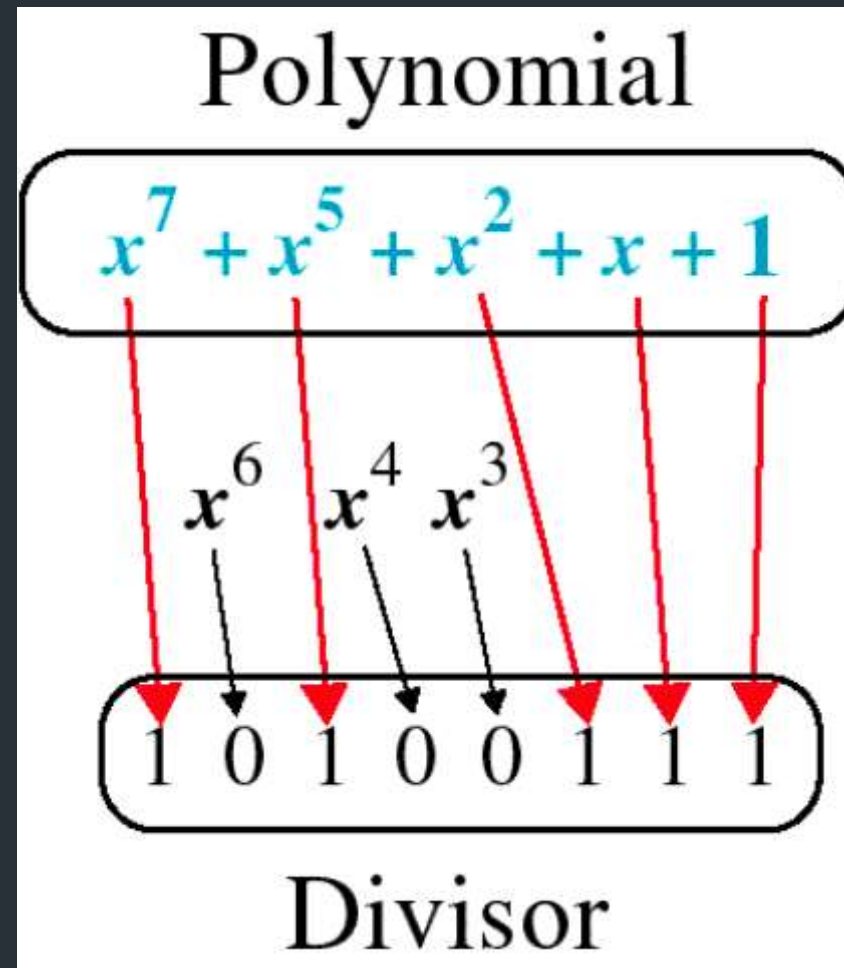
Polynomial

$$x^7 + x^5 + x^2 + x + 1$$

Source: Data Communications and Networking – Behrouz A. Forouzan

Polynomial and Divisor

24



Source: Data Communications and Networking – Behrouz A. Forouzan

Mr.A.Swaminathan VIT Chennai

Standard Polynomials

CRC-12

$$x^{12} + x^{11} + x^3 + x + 1$$

CRC-16

$$x^{16} + x^{15} + x^2 + 1$$

CRC-ITU

$$x^{16} + x^{12} + x^5 + 1$$

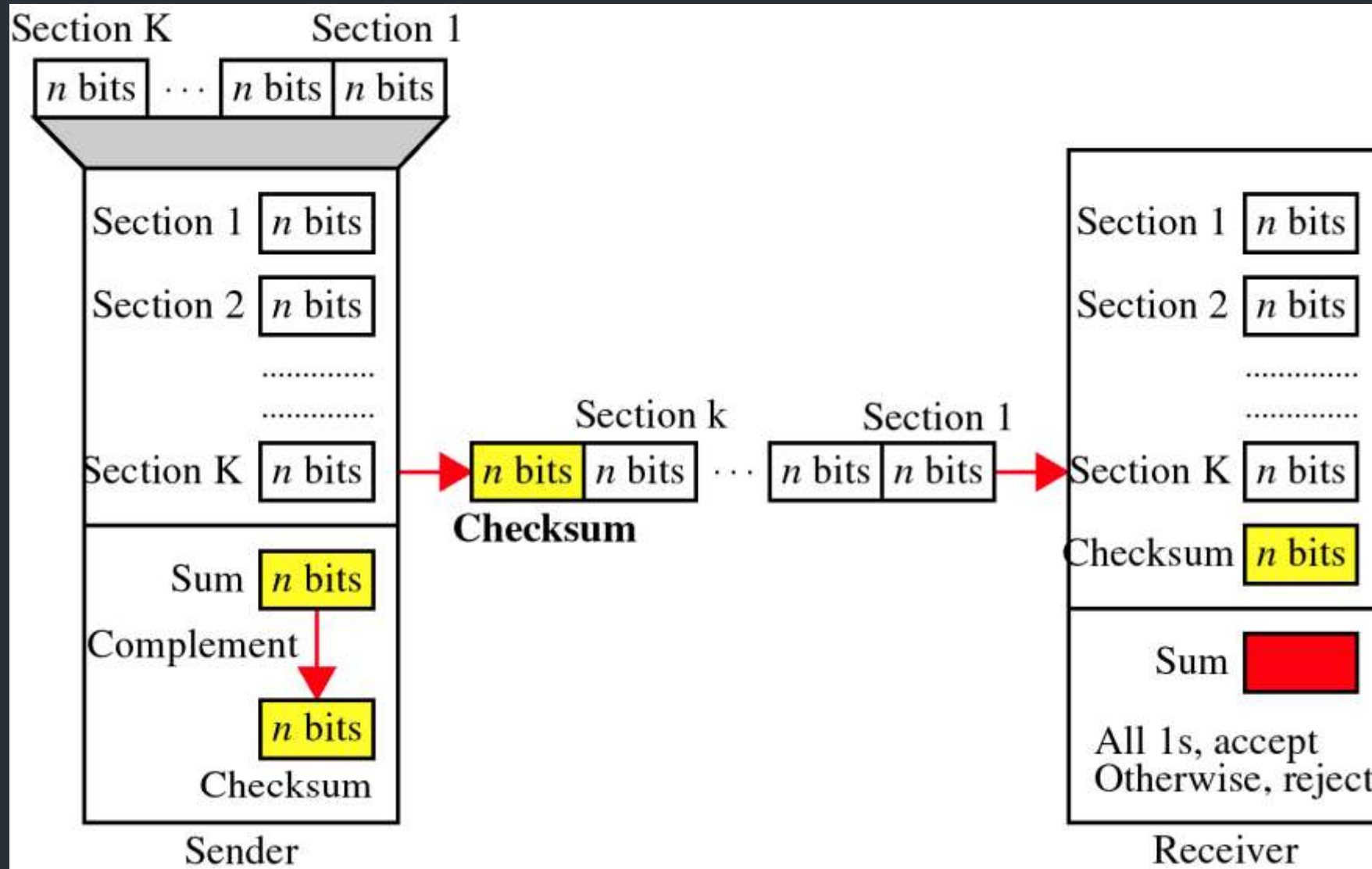
CRC-32

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Source: Data Communications and Networking – Behrouz A. Forouzan

Checksum

26



At the sender

- The unit is divided into k sections, each of n bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data

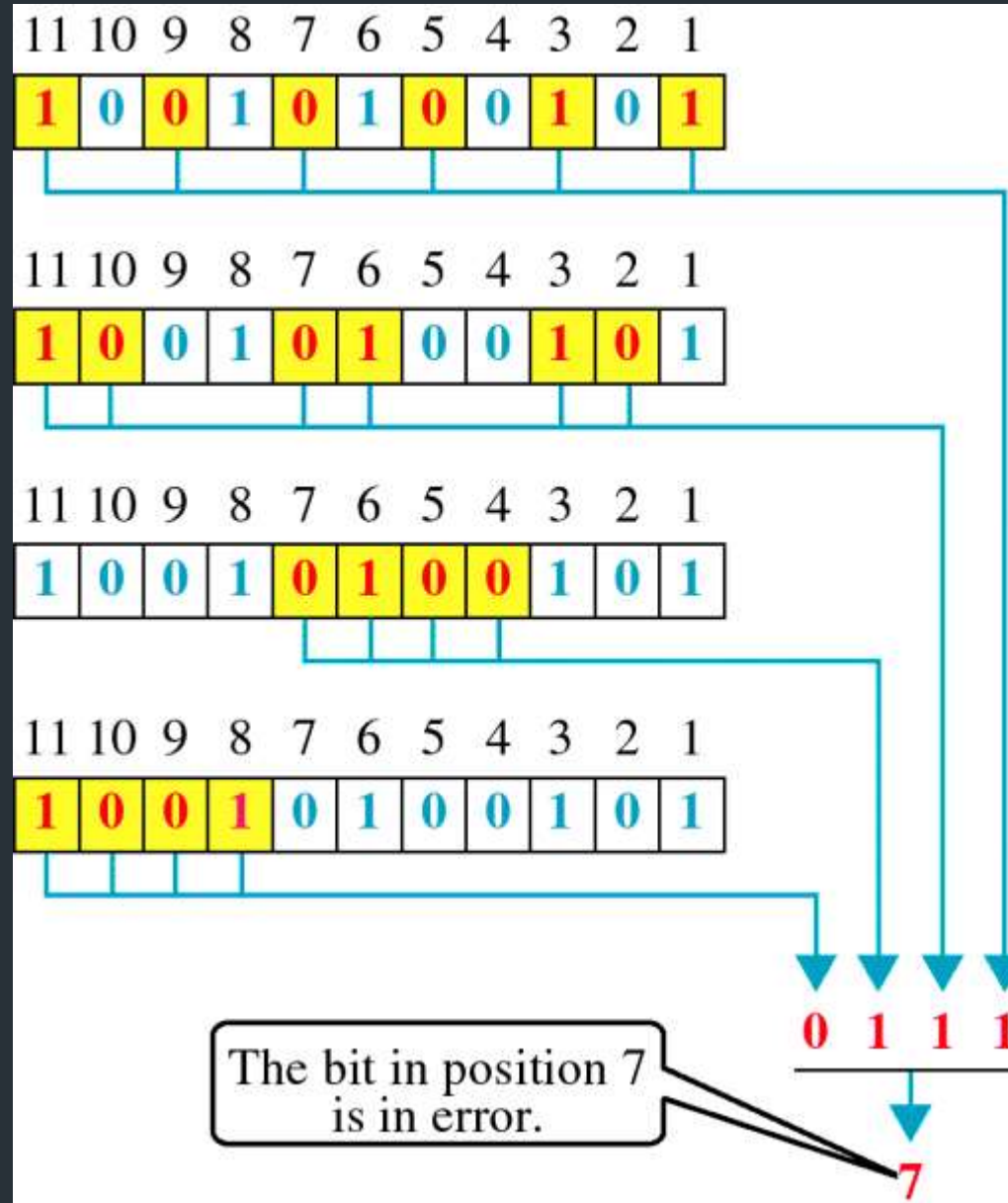
At the receiver

- The unit is divided into k sections, each of n bits.
- All sections are added together using one's complement to get the sum.
- The sum is complemented.
- If the result is zero, the data are accepted: otherwise, they are rejected.

Performance

- ➔ The checksum detects all errors involving an odd number of bits.
- ➔ It detects most errors involving an even number of bits.
- ➔ If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

Error Detection



Error Correction

It can be handled in two ways:

- 1) receiver can have the sender retransmit the entire data unit.
- 2) The receiver can use an error-correcting code, which automatically corrects certain errors.

Single-bit error correction

To correct an error, the receiver reverses the value of the altered bit. To do so, it must know which bit is in error.

Number of redundancy bits needed

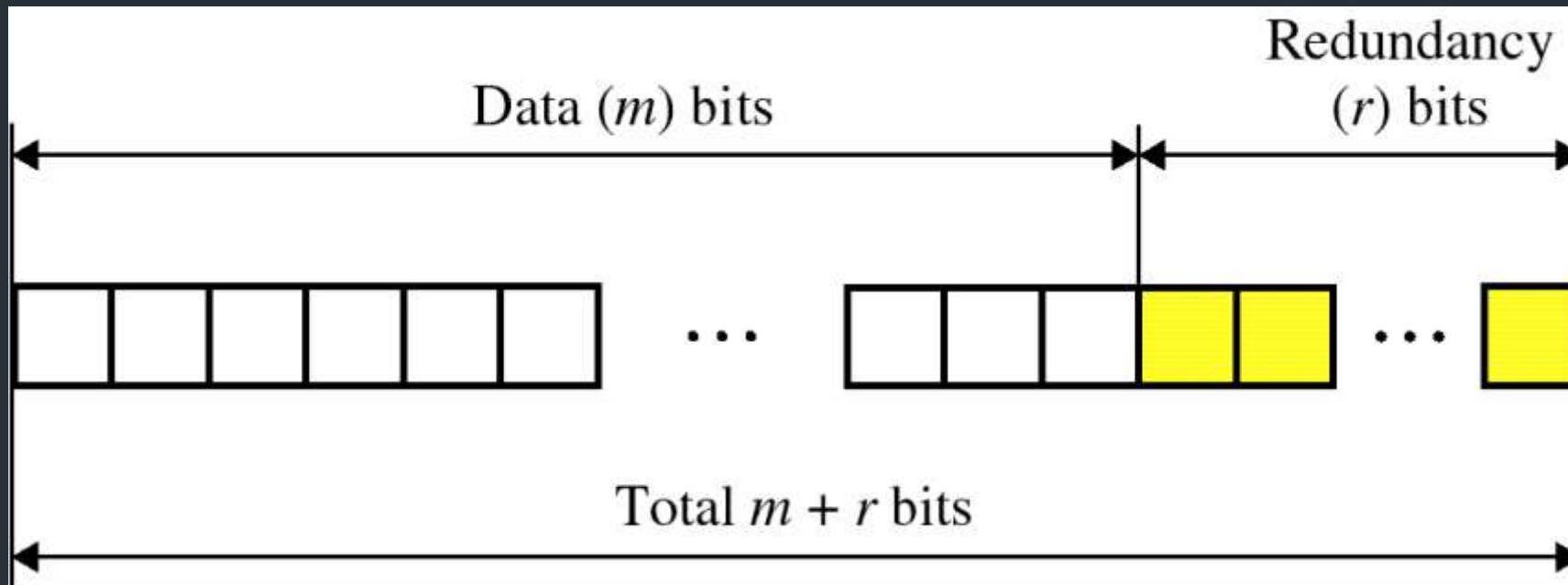
- Let data bits = m
- Redundancy bits = r

∴ Total message sent = $m+r$

The value of r must satisfy the following relation:

$$2^r \geq m+r+1$$

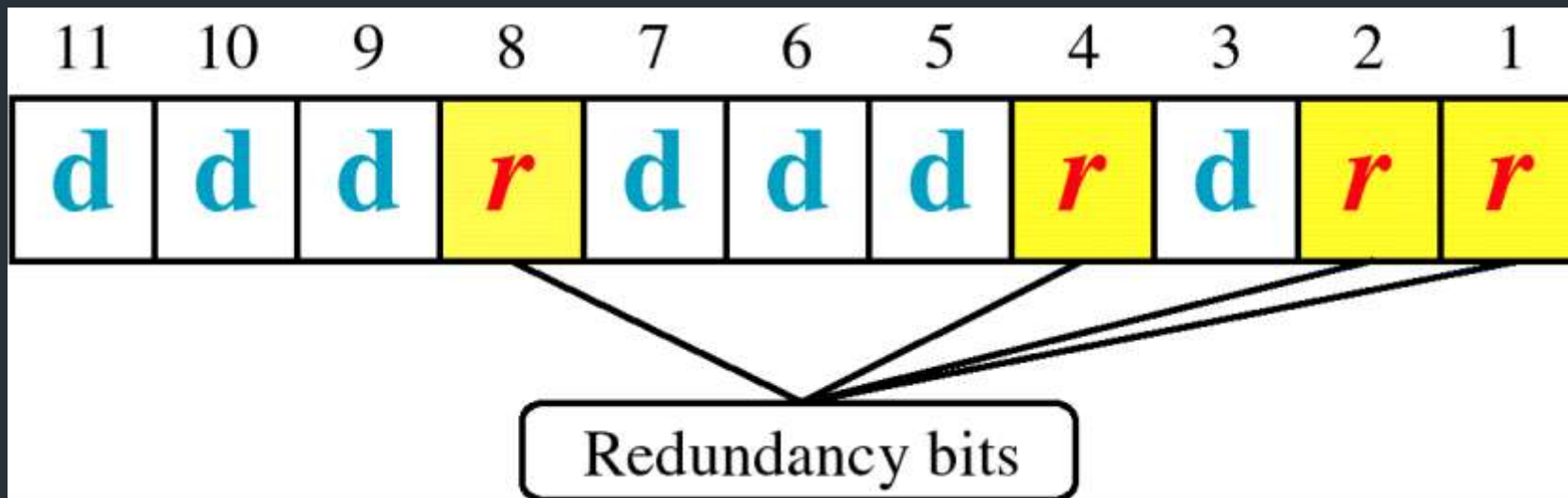
Error Correction



Source: Data Communications and Networking – Behrouz A. Forouzan

Hamming Code

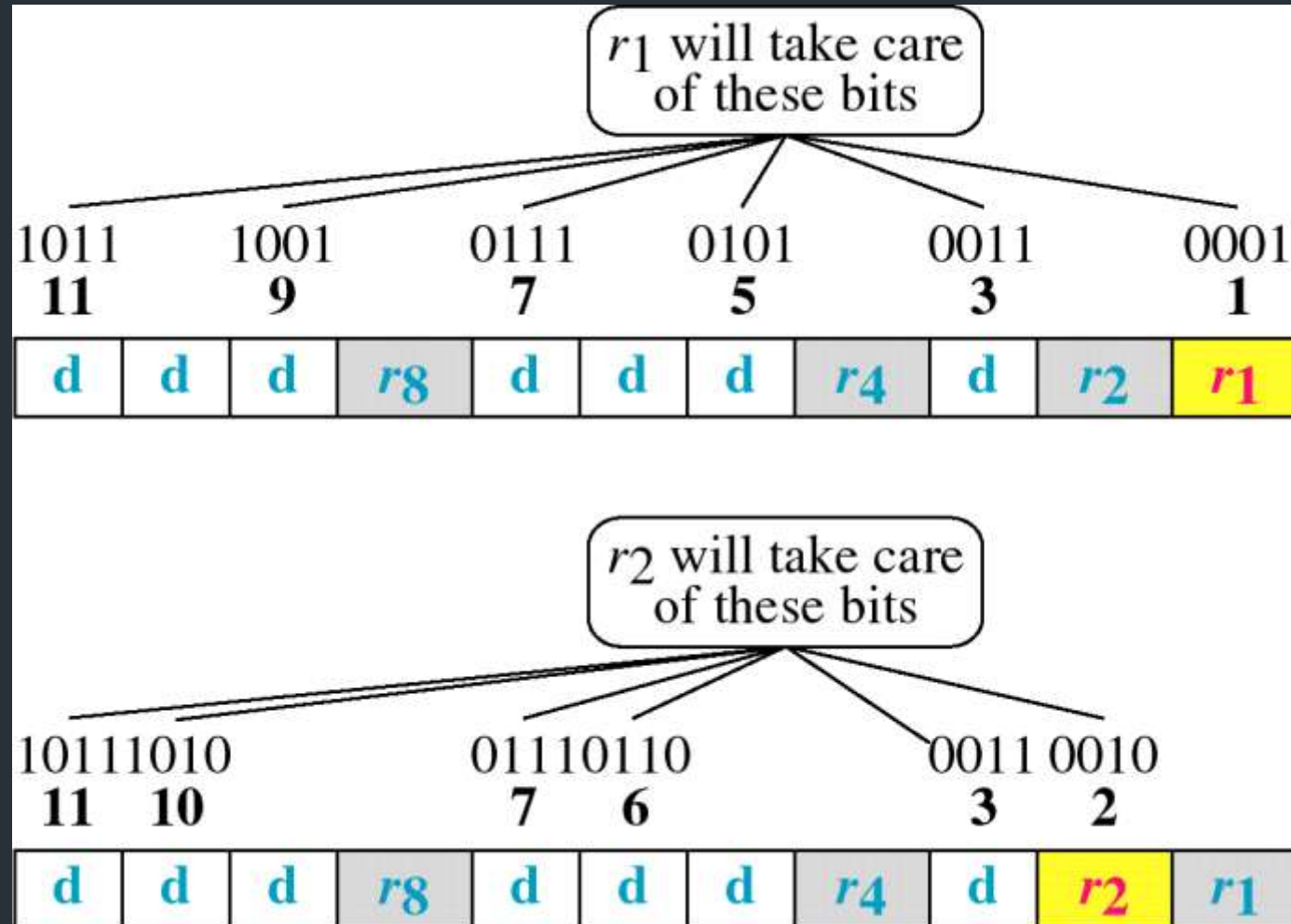
34



Source: Data Communications and Networking – Behrouz A. Forouzan

Hamming Code

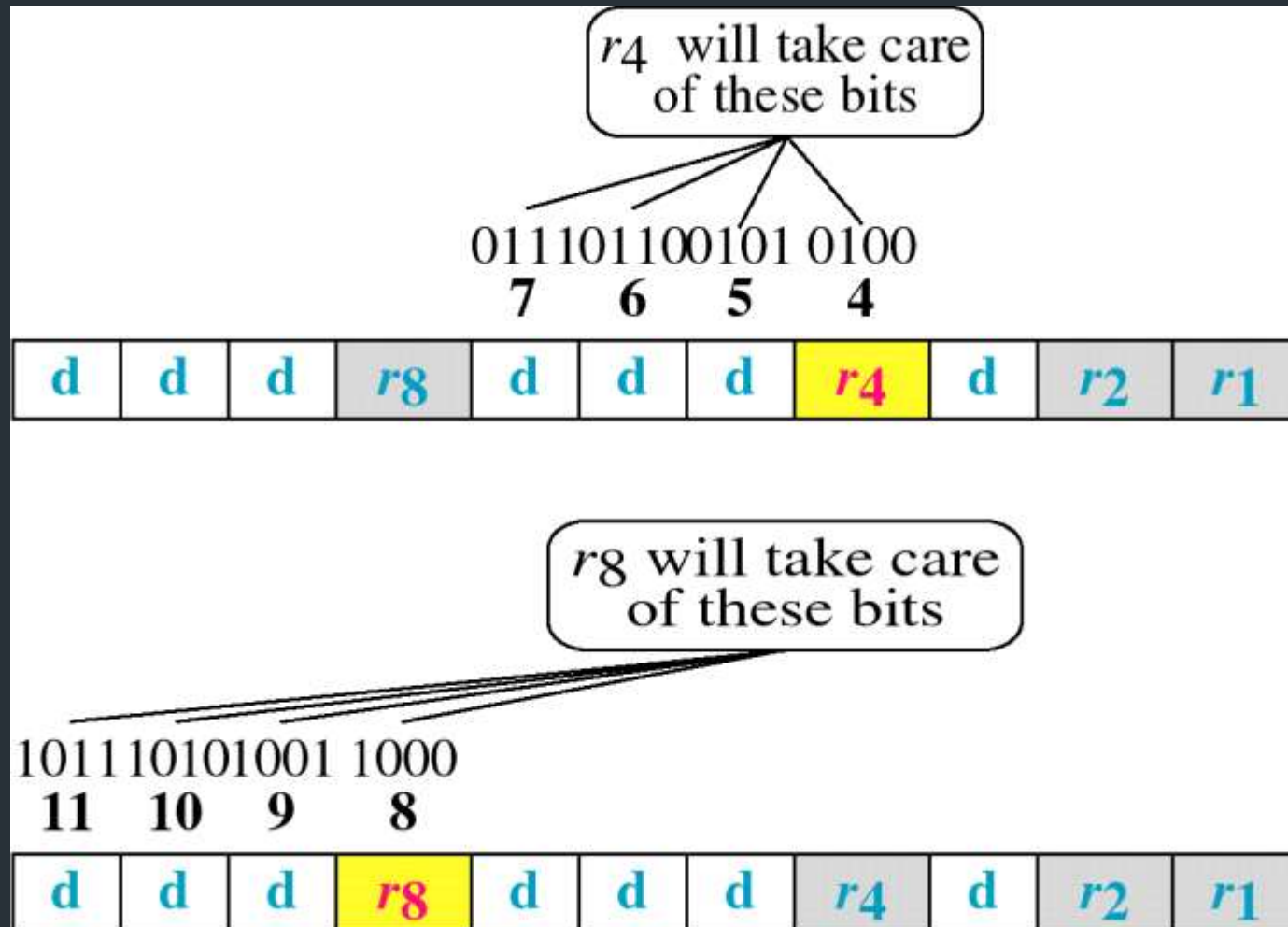
35



Source: Data Communications and Networking – Behrouz A. Forouzan

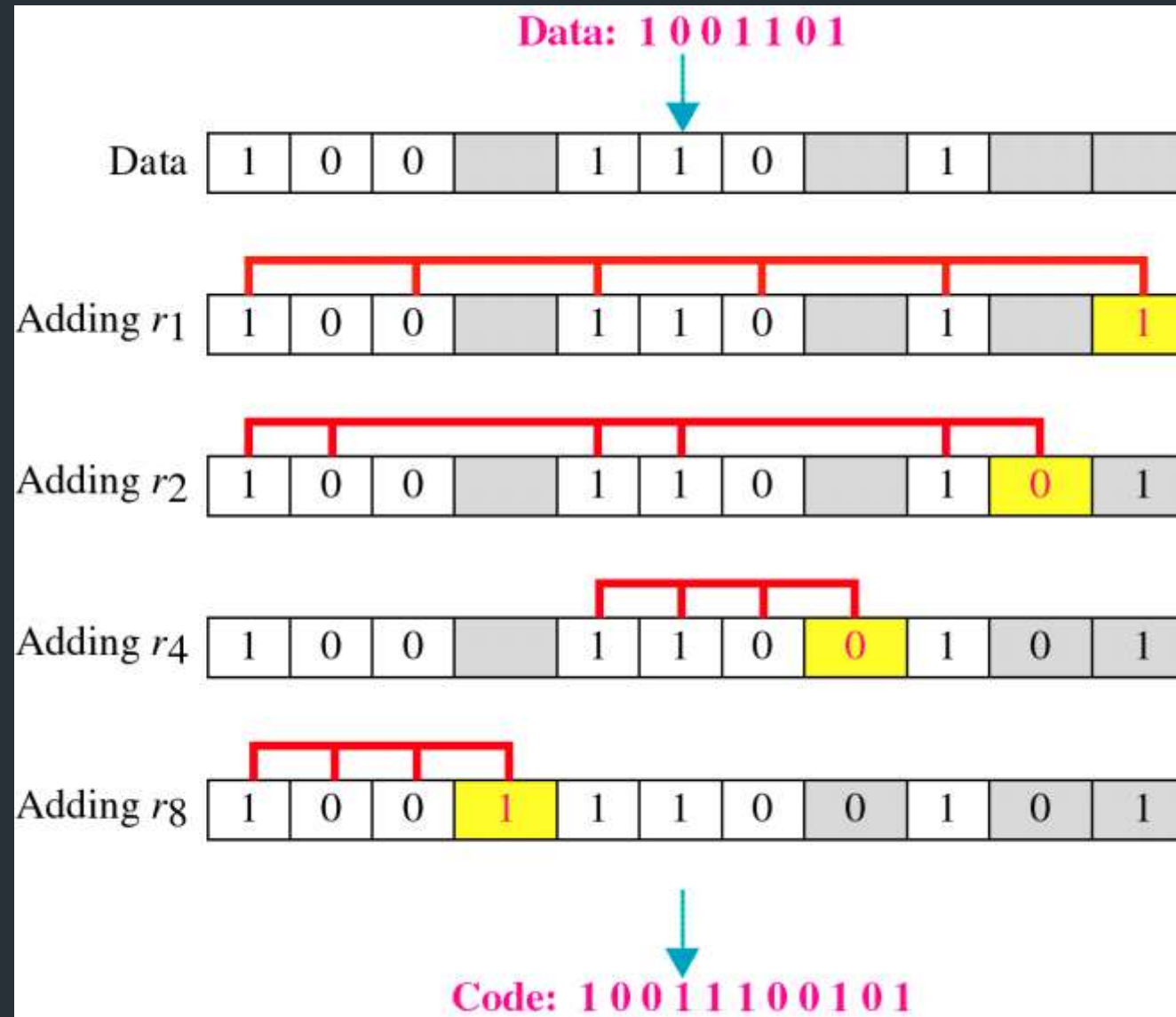
Hamming Code

36



Example of Hamming Code

37



References

- Forouzan Behrouz, A. "Data Communication and networking." (2008).
- Peterson, Larry L., and Bruce S. Davie. *Computer networks: a systems approach*. Elsevier, 2007.
- Stallings, William. *Data and computer communications*. Pearson Education India, 2007.
- Web Links as mentioned in source

Theory_Class_13

Flow control

- NETWORK AND COMMUNICATION
- Theory_Class_13

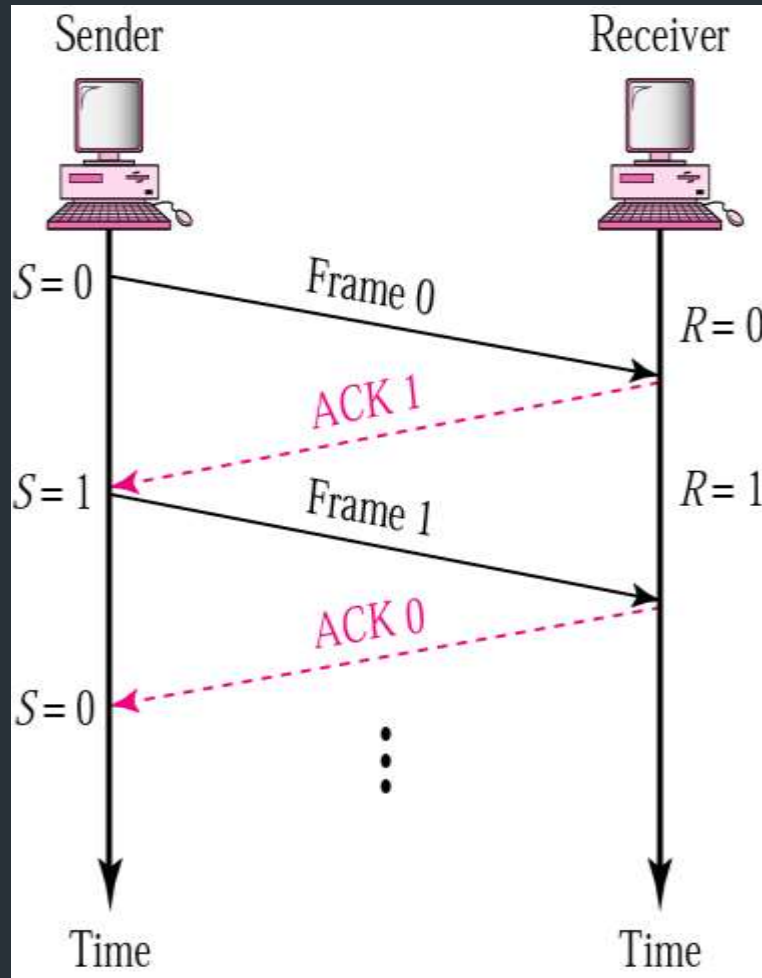
Overview

- Flow control
- Simplest
- Stop and wait
- Stop and wait ARQ
- Sliding window protocol
- Go back N with ARG
- Selective repeat ARQ

Flow Control

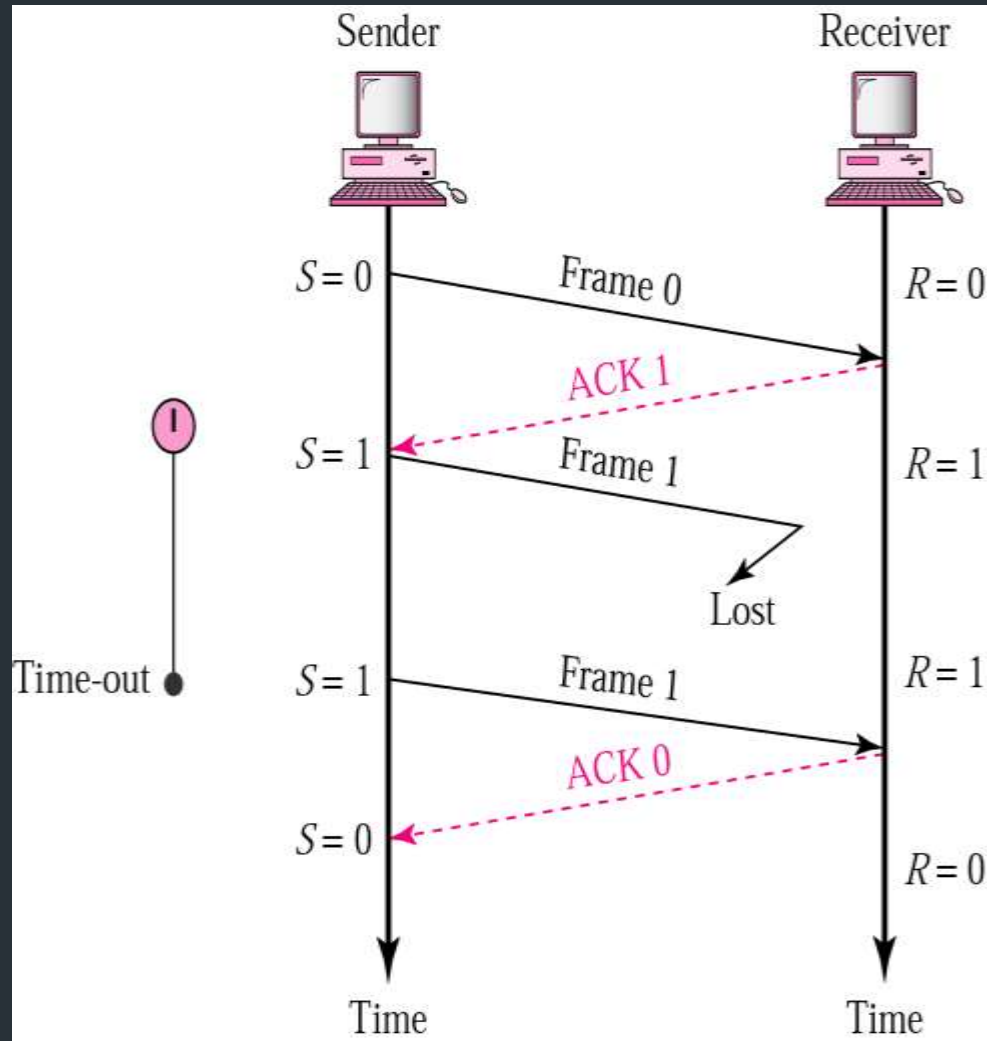
- It is one of the most important functions of data link layer.
- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- Receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- Receiver must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.
- When the rate of processing is often slower than the rate of transmission, receiver has a block of memory (buffer) for storing incoming data until they are processed.

Stop-and-Wait ARQ



- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control variable (R) that holds the number of the next frame expected (0 or 1).
- Receiver send only positive ACK if the frame is intact.
- ACK number always defines the number of the next expected frame

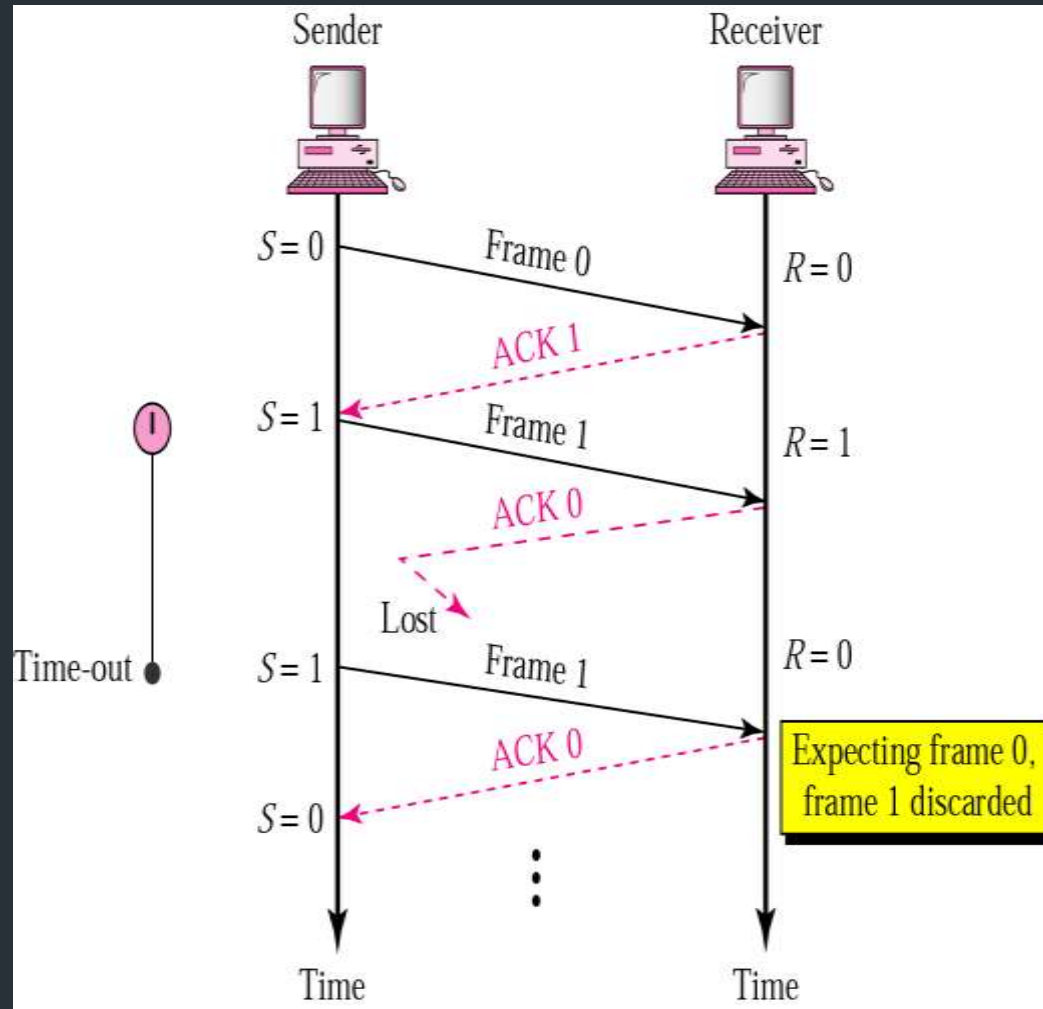
Stop-and-Wait ARQ, lost ACK frame



- Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it
- When a receiver receives a damaged frame, it discards it and keeps its value of R.
- After the timer at the sender expires, another copy of frame 1 is sent.

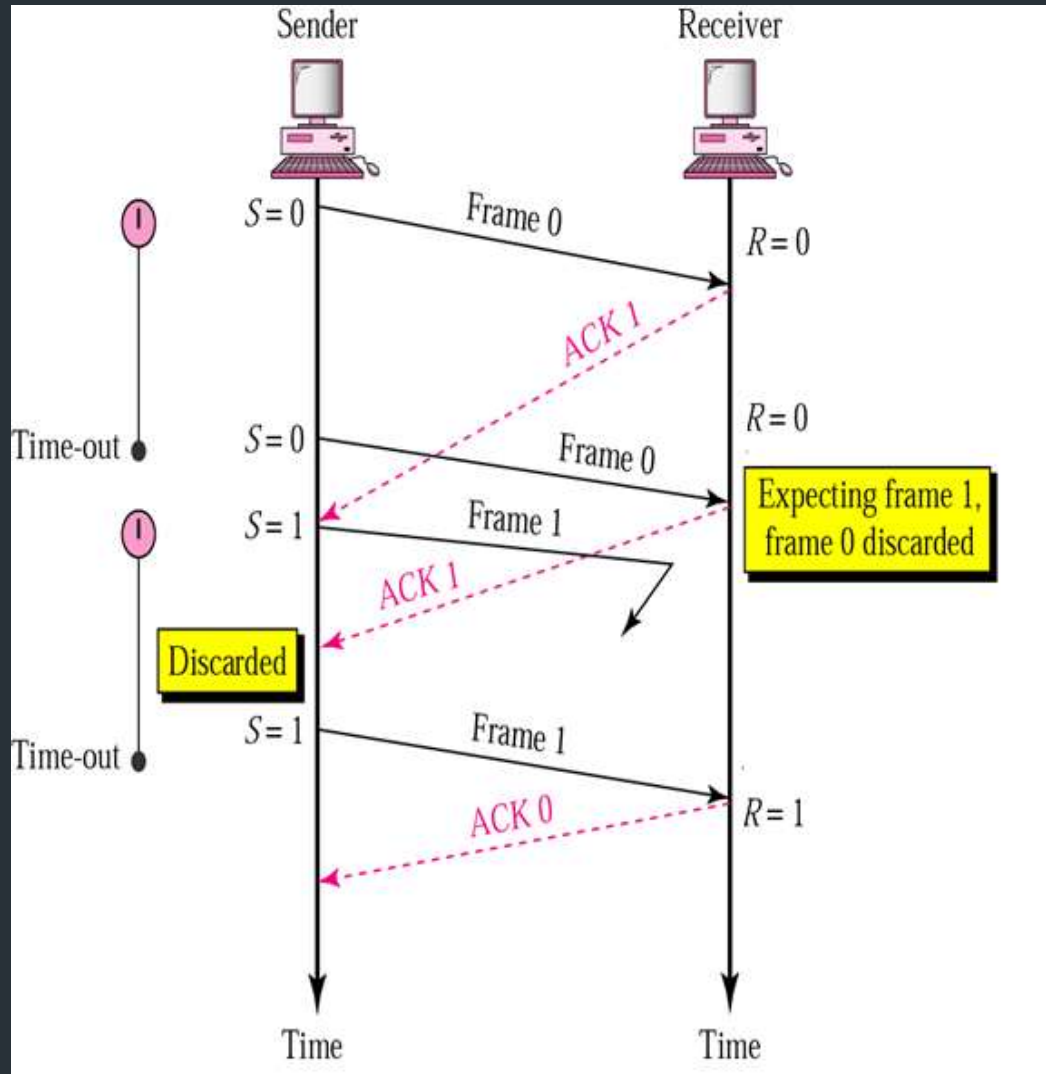
Stop-and-Wait, lost ACK frame

45



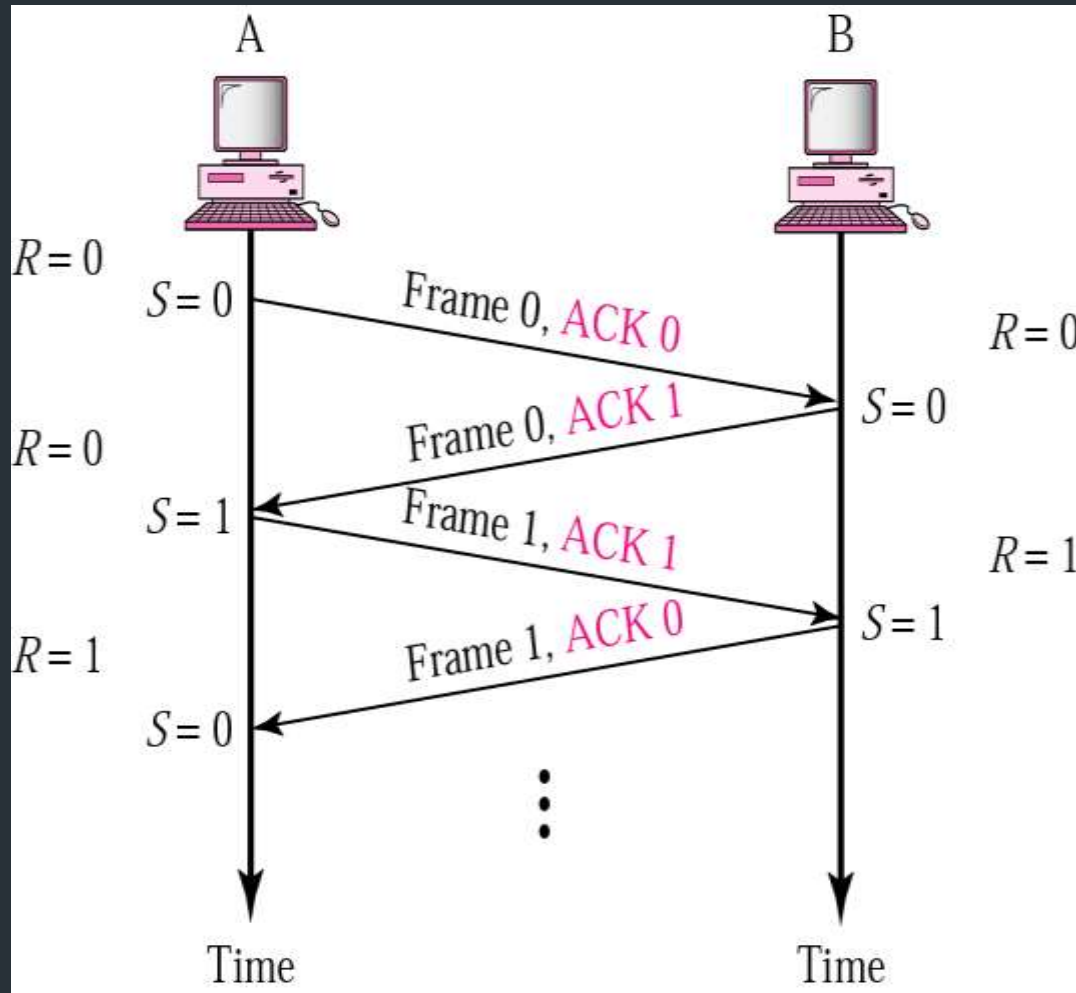
- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 ($R=0$). Therefore it discards the second copy of frame 1.

Stop-and-Wait, delayed ACK frame



- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However, since $R=0$ which means receiver already has frame 0. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

Piggybacking



- A method to combine a data frame with ACK.
- Station A and B both have data to send.
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing.
- Piggybacking saves bandwidth.

Disadvantage of Stop-and-Wait

- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.
- Two protocols use the above concept,
 - **Go-Back-N ARQ**
 - **Selective Repeat ARQ**

Go-Back-N ARQ

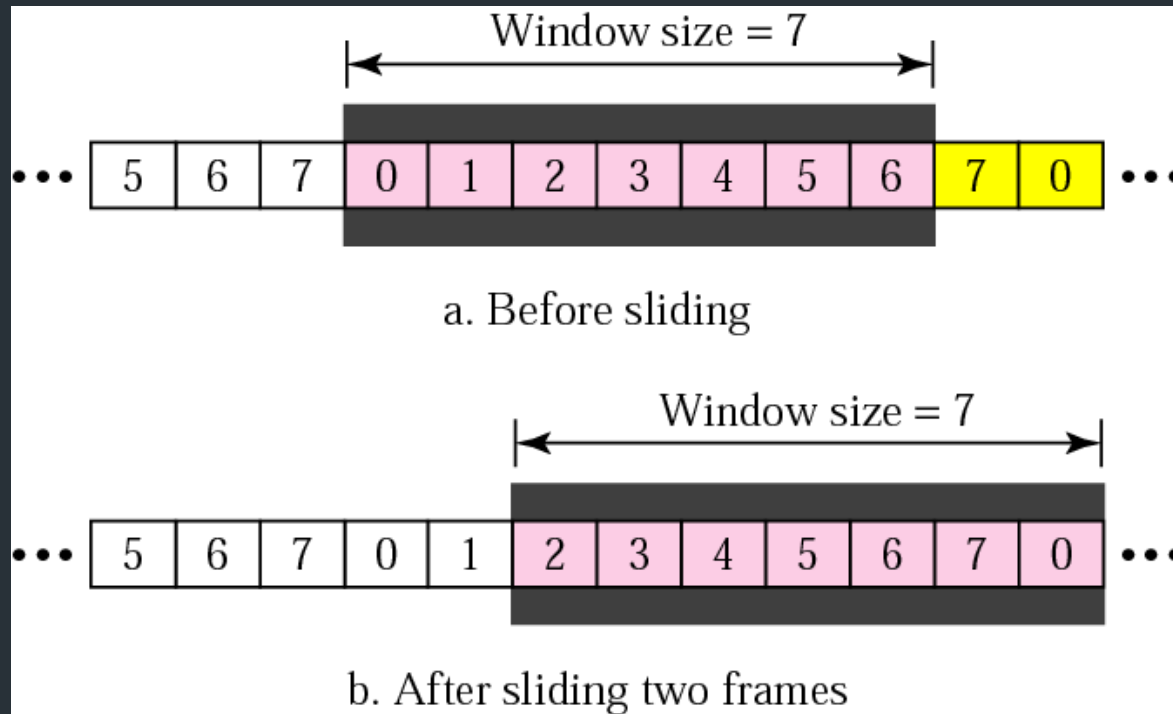
- Sender can send up to W frames before worrying about ACKs.
- Sender keeps the copy of these frames until the ACKs arrive.
- This procedure requires additional features to be added to Stop-and-Wait ARQ.

Sequence Numbers

- Frames from a sender are numbered sequentially.
- We need to set a limit since we need to include the sequence number of each frame in the header.
- If the header of the frame allows m bits, the sequence numbers range from 0 to $2^m - 1$. for $m = 3$, sequence numbers are: 1, 2, 3, 4, 5, 6, 7.
- We can repeat the sequence number.
- Sequence numbers are:
0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, ...

Sender Sliding Window

51

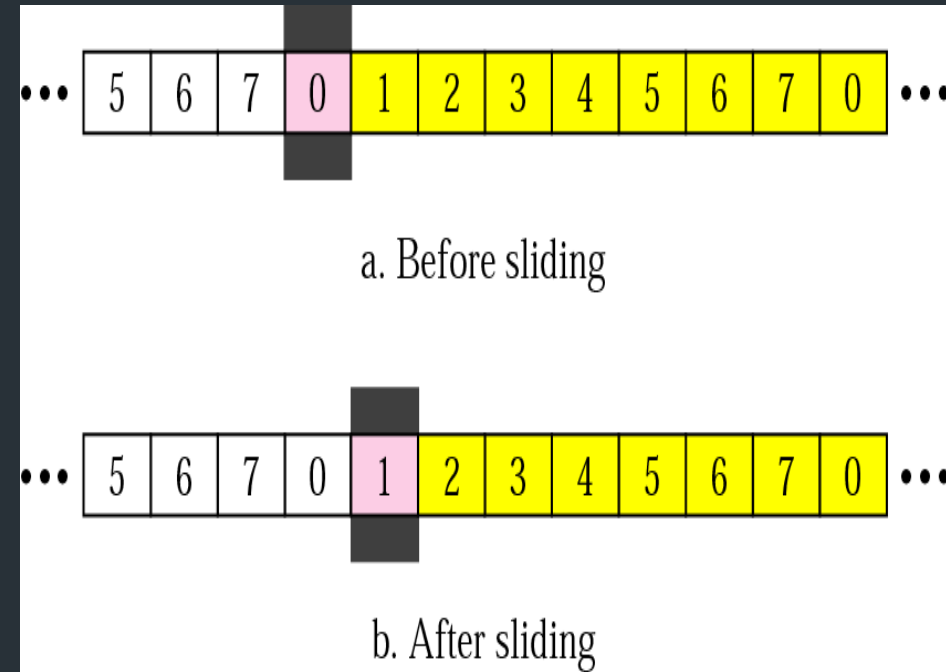


- At the sending site, to hold the outstanding frames until they are acknowledged, we use the concept of a window.
- The size of the window is at most $2^m - 1$ where m is the number of bits for the sequence number.
- Size of the window can be variable.
- The window slides to include new unsent frames when the correct ACKs are received

Source: Data Communications and Networking – Behrouz A. Forouzan

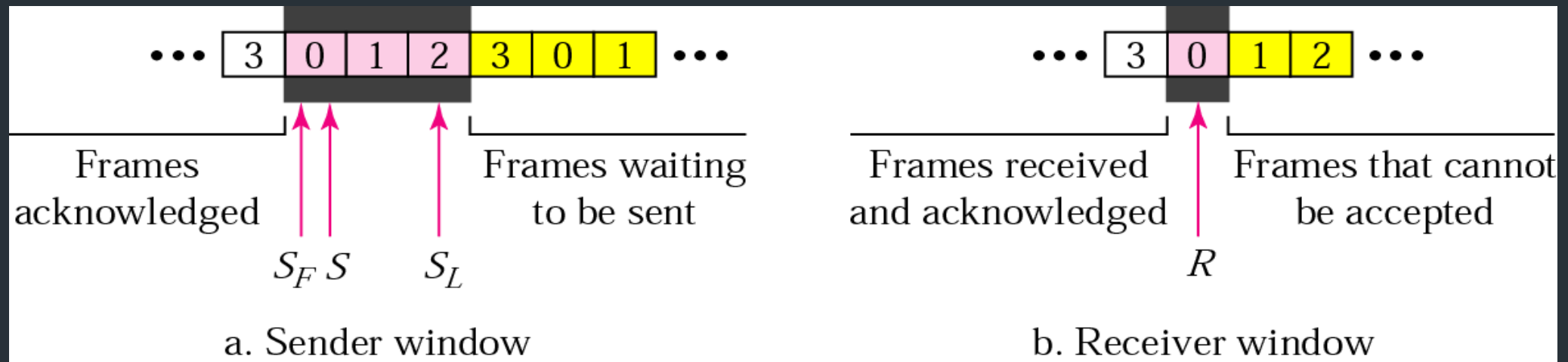
Receiver Sliding Window

- Size of the window at the receiving site is always 1 in this protocol.
- Receiver is always looking for a specific frame to arrive in a specific order.
- Any frame arriving out of order is discarded and needs to be resent.
- Receiver window slides as shown in fig. Receiver is waiting for frame 0 in part a.



Source: Data Communications and Networking
– Behrouz A. Forouzan

- Sender has 3 variables: S , S_F and S_L
- S holds the sequence number of recently sent frame
- S_F holds the sequence number of the first frame
- S_L holds the sequence number of the last frame
- Receiver only has the one variable, R , that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of R , the frame is accepted, otherwise rejected.



Source: Data Communications and Networking – Behrouz A. Forouzan

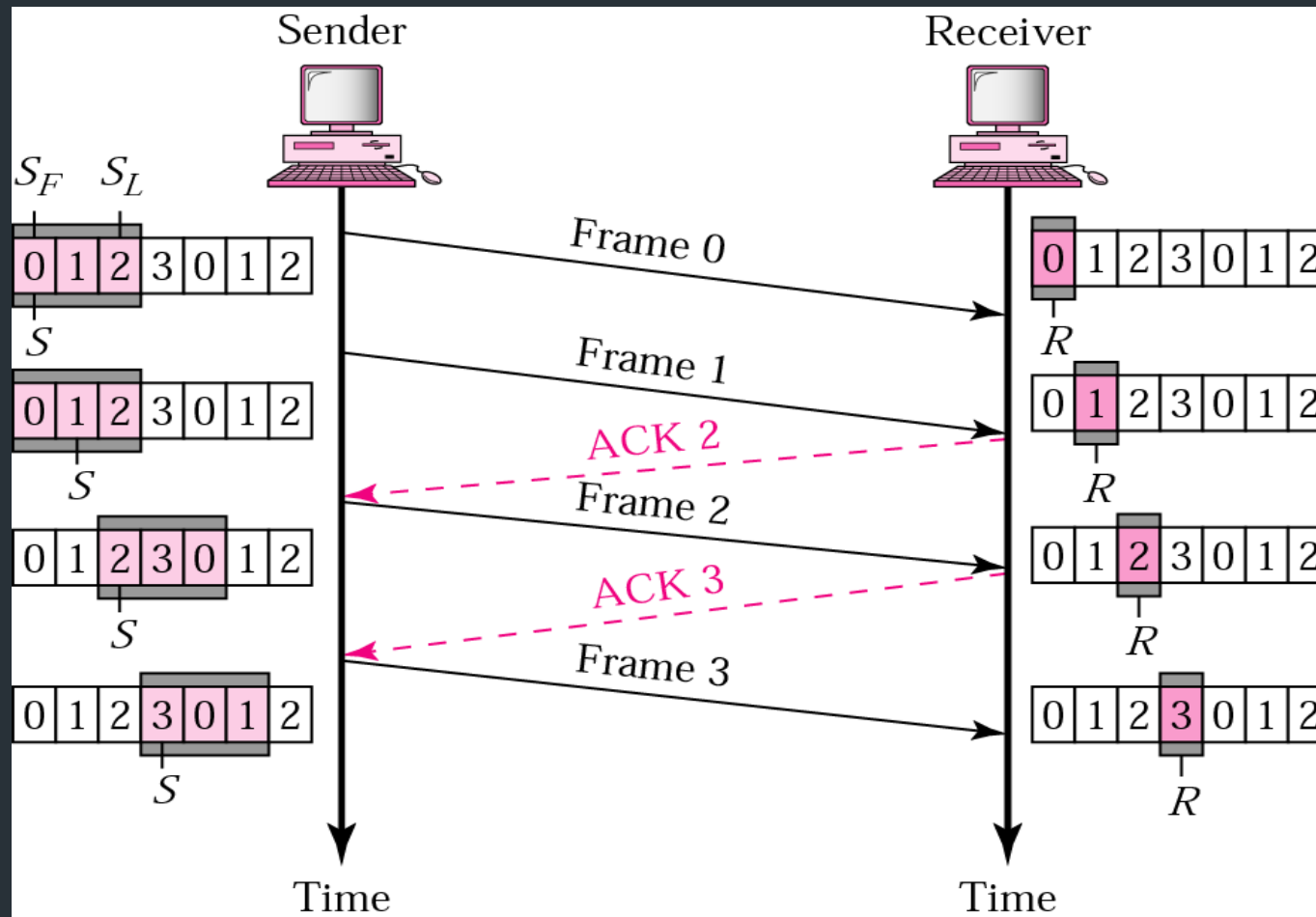
Acknowledgement

- ▶ Receiver sends positive ACK if a frame is arrived safe and in order.
- ▶ If the frames are damaged/out of order, receiver doesn't respond and discard all subsequent frames until it receives the one it is expecting.
- ▶ The silence of the receiver causes the timer of the unacknowledged frame to expire.
- ▶ Then the sender resends all frames, beginning with the one with the expired timer.
- ▶ For example, suppose the sender has sent frame 6, but the timer for frame 3 expires (i.e. frame 3 has not been acknowledged), then the sender goes back and sends frames 3, 4, 5, 6 again. Thus it is called Go-Back-N-ARQ
- ▶ The receiver does not have to acknowledge each frame received, it can send one cumulative ACK for several frames.

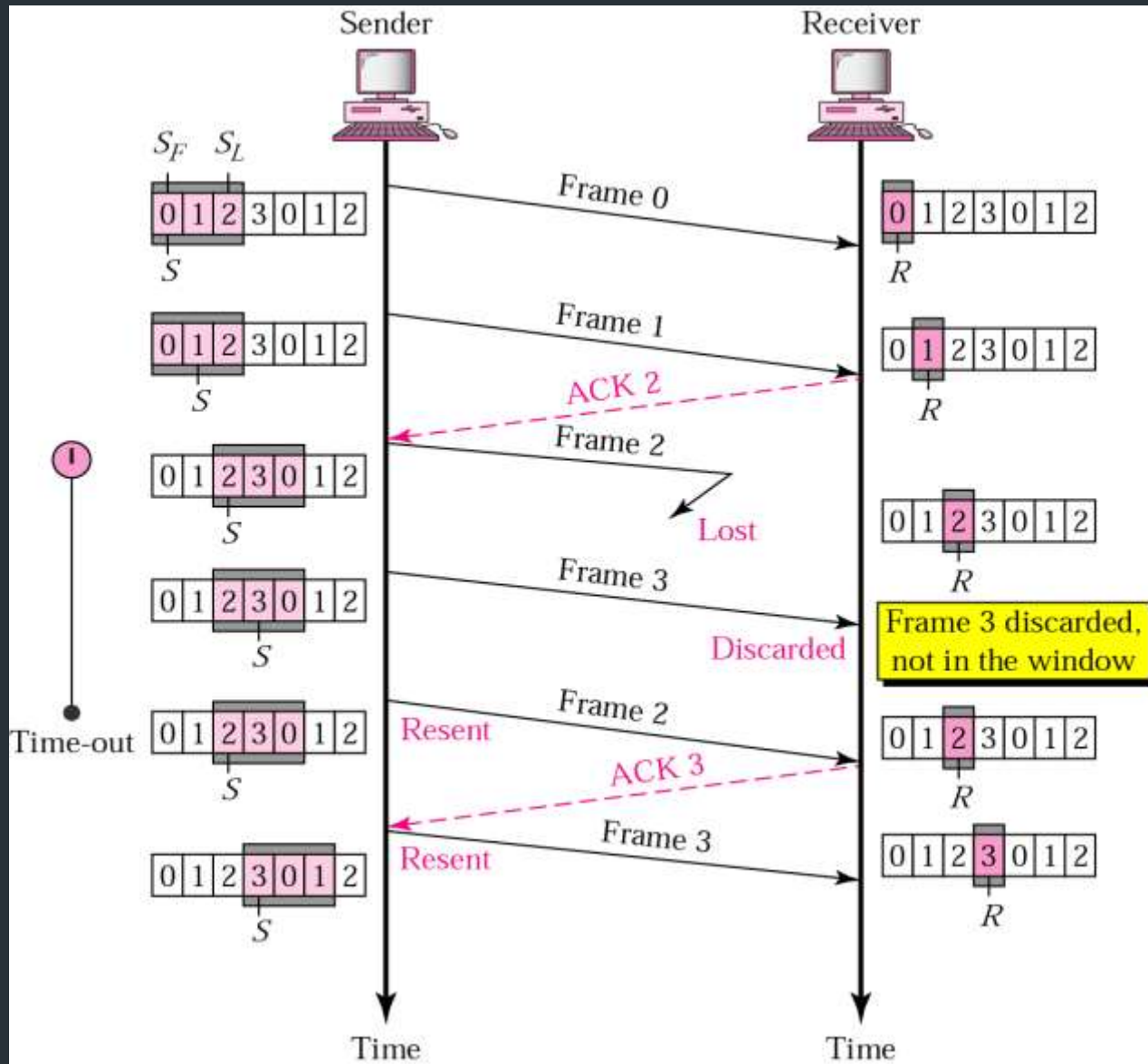
Go-Back-N ARQ, normal operation

56

- The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



Go-Back-N ARQ, lost frame



- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window).
- After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)

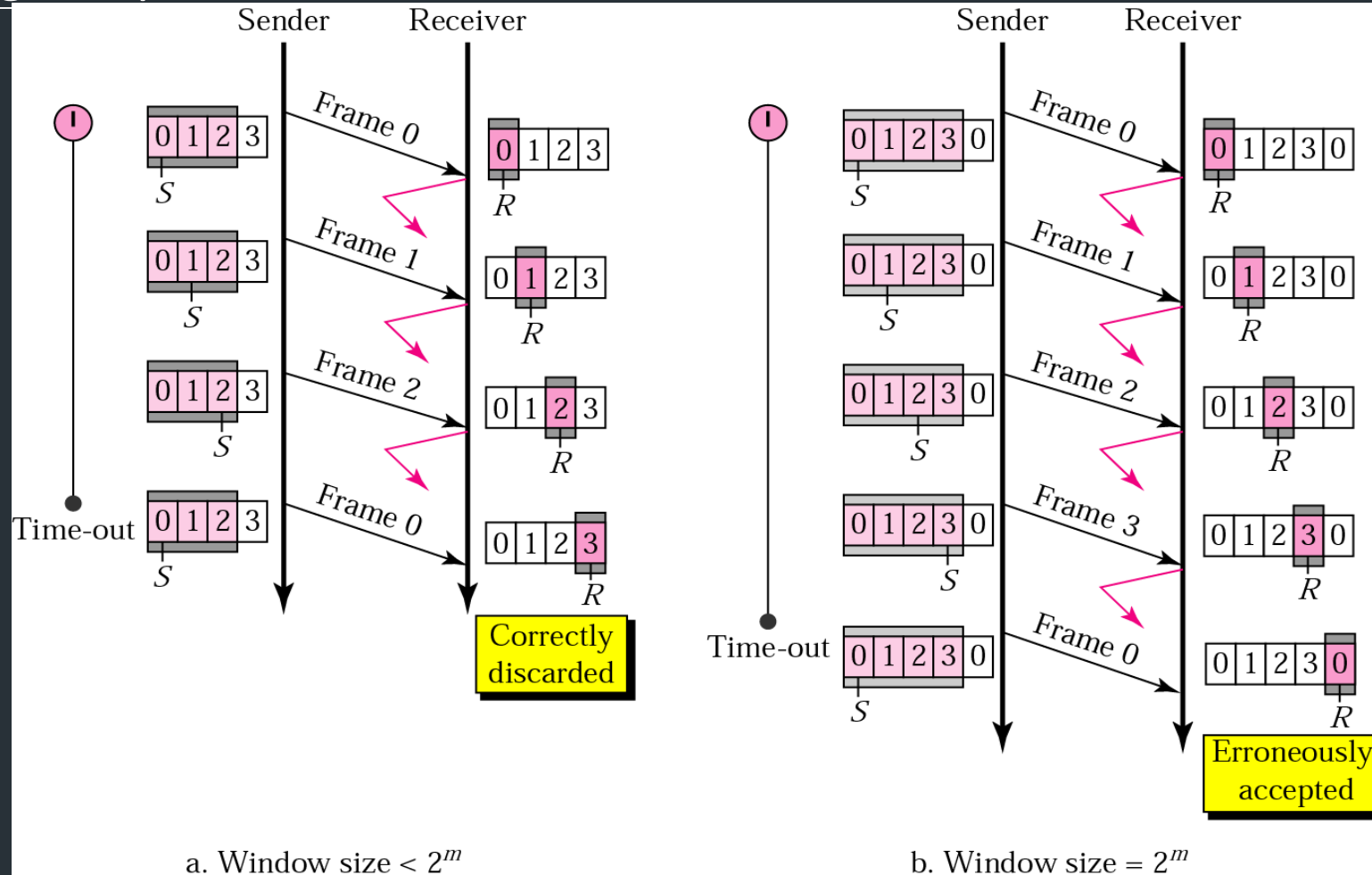
Go-Back-N ARQ, damaged/lost/delayed ACK

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
- If ACK1, ACK2, and ACK3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- Receiver never resends an ACK.
- A delayed ACK also triggers the resending of frames

Go-Back-N ARQ, sender window size

- Size of the sender window must be less than 2^m . Size of the receiver is always 1. If $m = 2$, window size = $2^m - 1 = 3$.
- Fig compares a window size of 3 and 4.

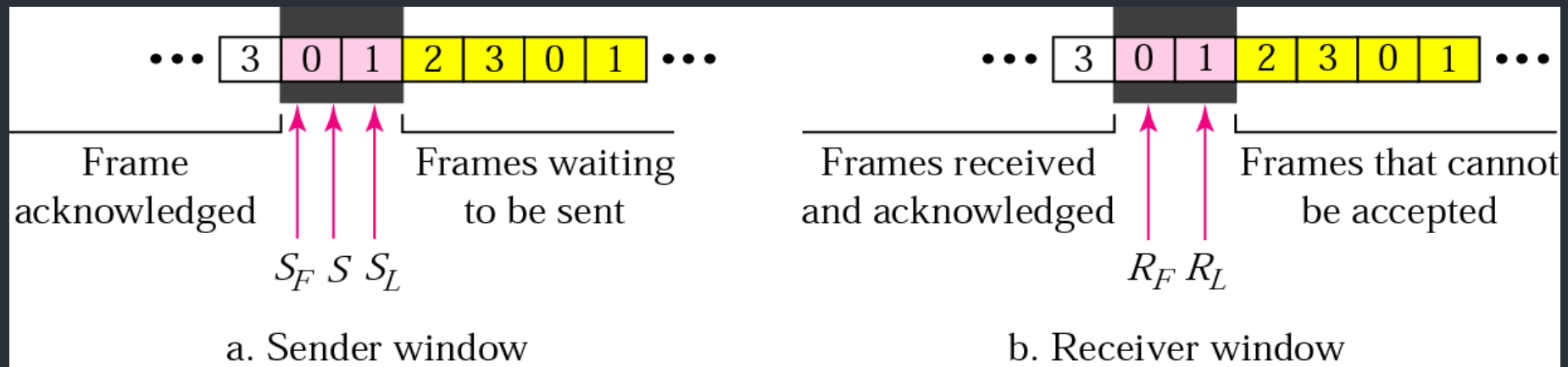
59



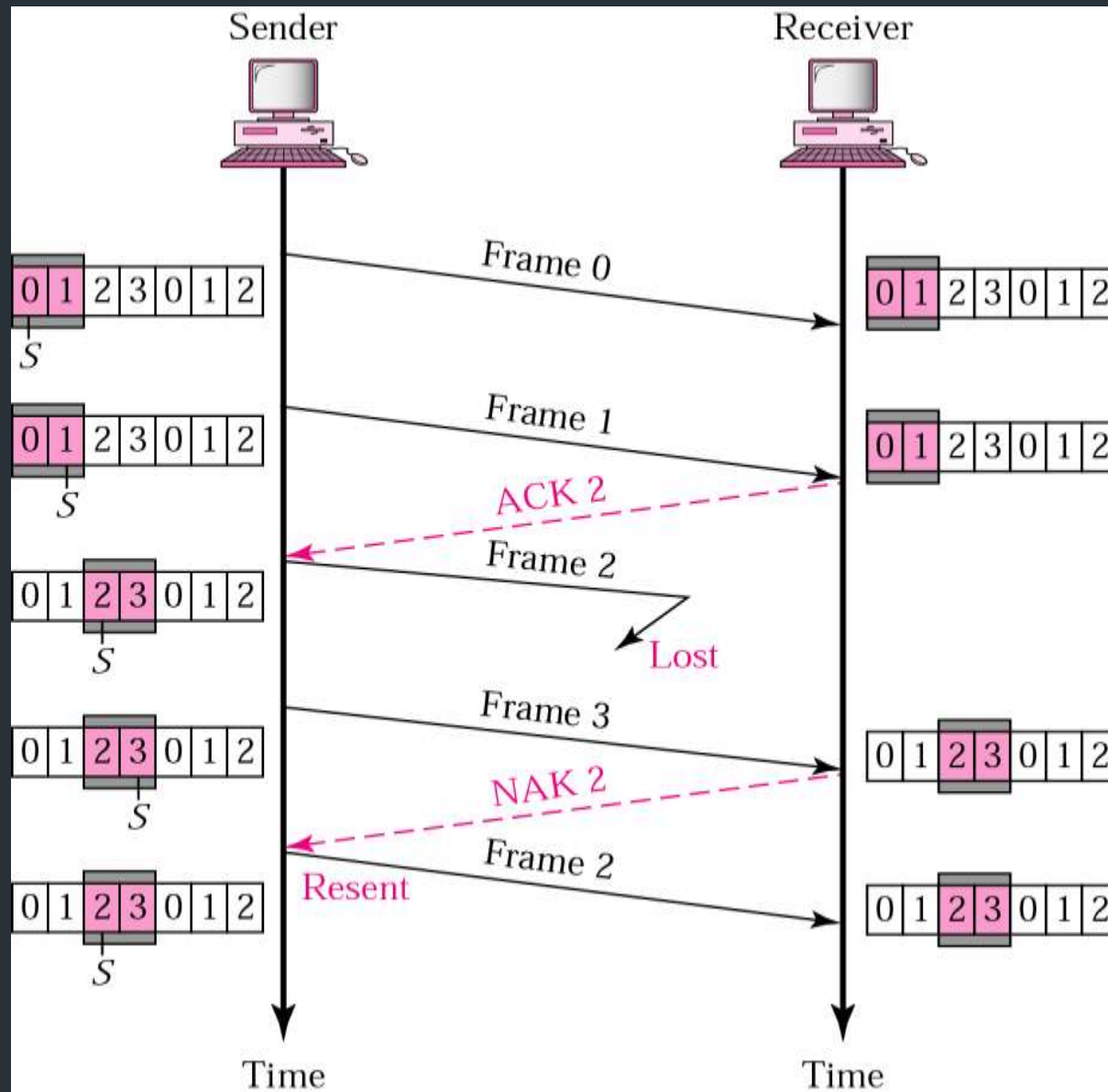
Selective Repeat ARQ, sender and receiver windows

60

- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.



Selective Repeat ARQ, lost frame



- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

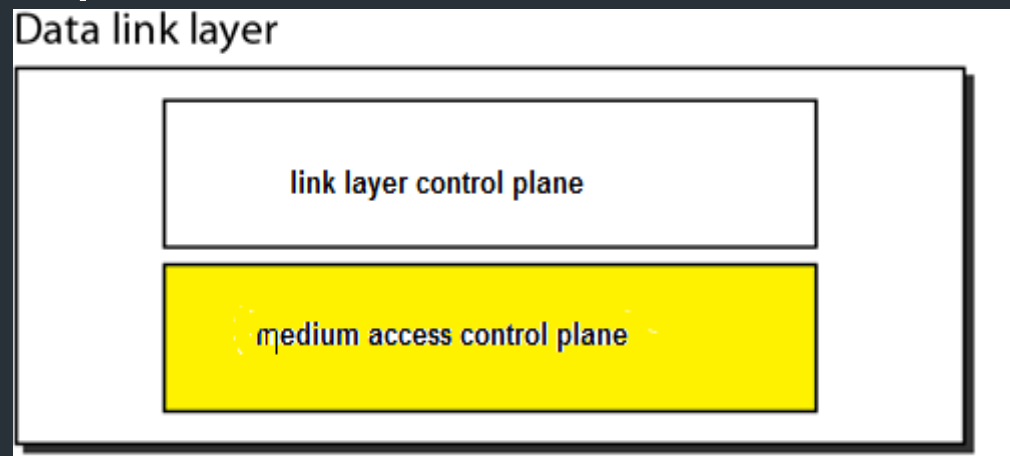
References

- Forouzan Behrouz, A. "Data Communication and networking." (2008).
- Peterson, Larry L., and Bruce S. Davie. *Computer networks: a systems approach*. Elsevier, 2007.
- Stallings, William. *Data and computer communications*. Pearson Education India, 2007.
- Web Links as mentioned in source

Theory_Class_14

Multiple Access

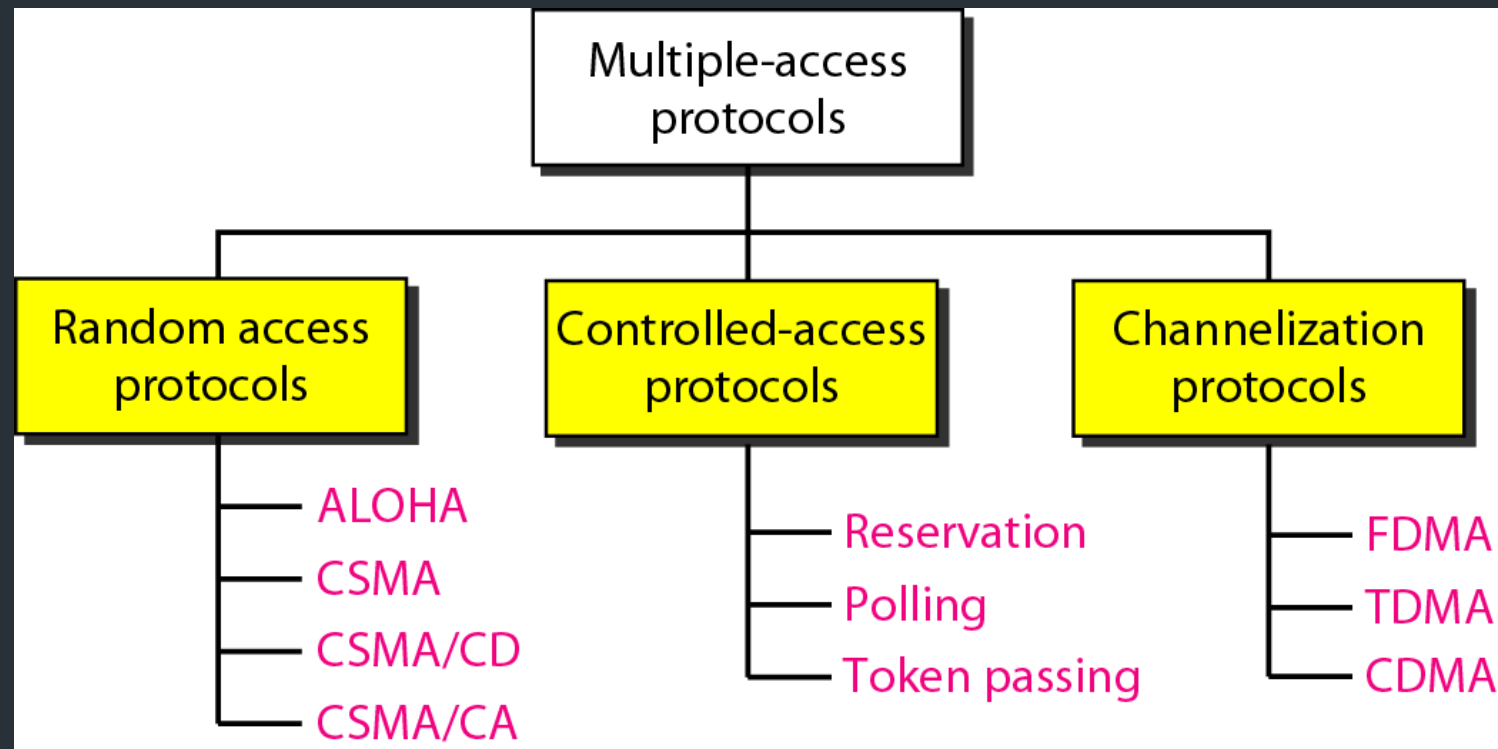
- In data link control protocols, it is **assumed** that there is **dedicated** link between the sender and receiver.
- Data link layer divided into **two** functionality-oriented sublayers
- Upper sublayer is responsible for data link (**flow and error**) control (Link Layer Control - LLC).
- Lower sublayer is responsible for resolving **access** to the shared media (Medium Access Control - MAC).
- Multiple access protocol **coordinates** to access the link (media)



Source: Data
Communications and
Networking – Behrouz
A. Forouzan

Multiple Access

Many protocols have been devised to handle shared link and are mainly categorized into **three** groups



Source: Data Communications and Networking – Behrouz A. Forouzan

RANDOM ACCESS

In **random access**

- no station is superior to another station
- none is assigned the control over another
- No station permits, or 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.

RANDOM ACCESS

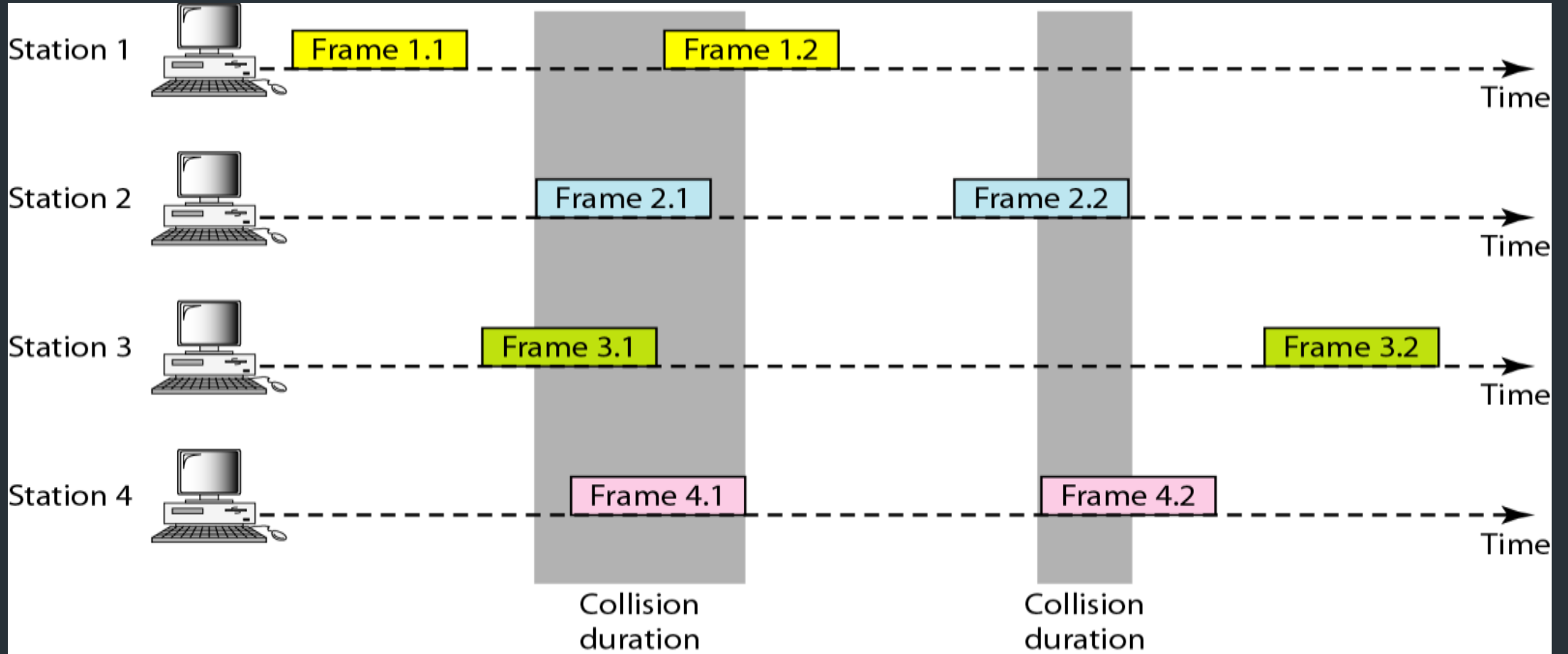
- Two features gives the method its name:
 - Transmission is random among stations.
 - Stations compete with one another to access the medium.
- **Collision:** an access **conflict** occurs when more than one station tries to send, as a result the frame will be either **destroyed or modified**.

Aloha

- Developed at the University of Hawaii (US) in early 1970 and designed for wireless LAN, but can be used on any shared medium.
- Original ALOHA protocol is called pure ALOHA
- A node sends the frame whenever it has a frame to send.
- Medium is shared between the stations, there is possibility of collision between frames from different stations.

Pure ALOHA

Frames in a pure ALOHA network



Source: Data Communications and Networking – Behrouz A. Forouzan

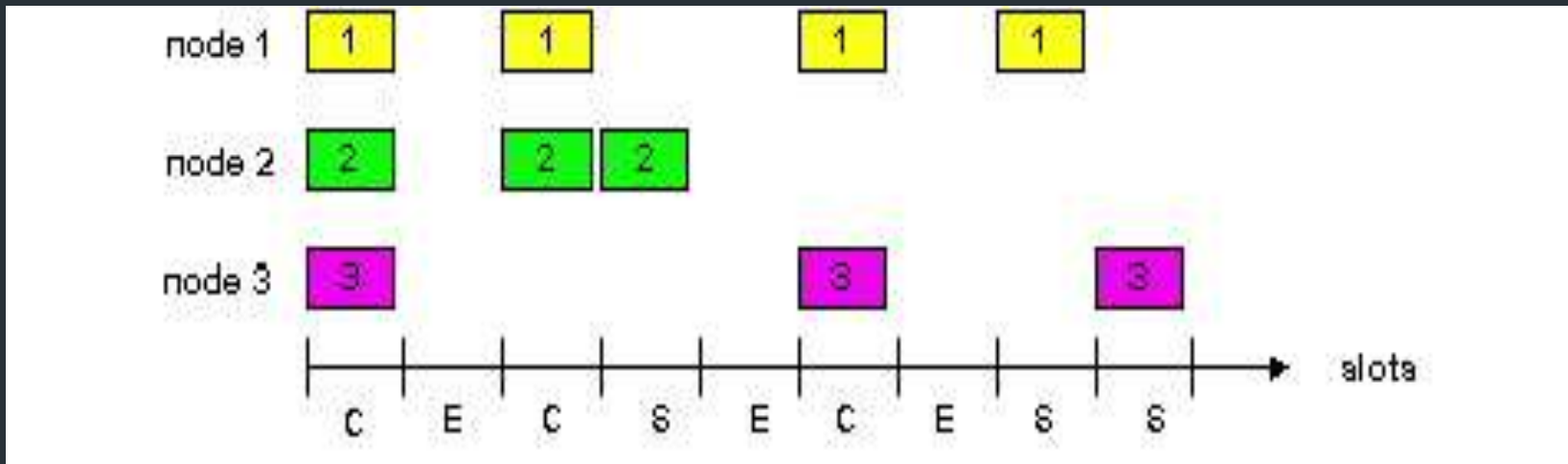
Mr.A.Swaminathan VIT Chennai

Aloha

- A collision involves two more stations. If all the stations try to send their frames after the time-out, the frames will collide again.
- To avoid collision stations will try again in random period, this time is the back-off time T_B .

Slotted Aloha

71



Source: Data Communications and Networking – Behrouz A. Forouzan

All frames are of same size.

Time is divided into **slots** of size L/R seconds time (equal size slots)

L: Bandwidth and R: Time to transmit 1 frame

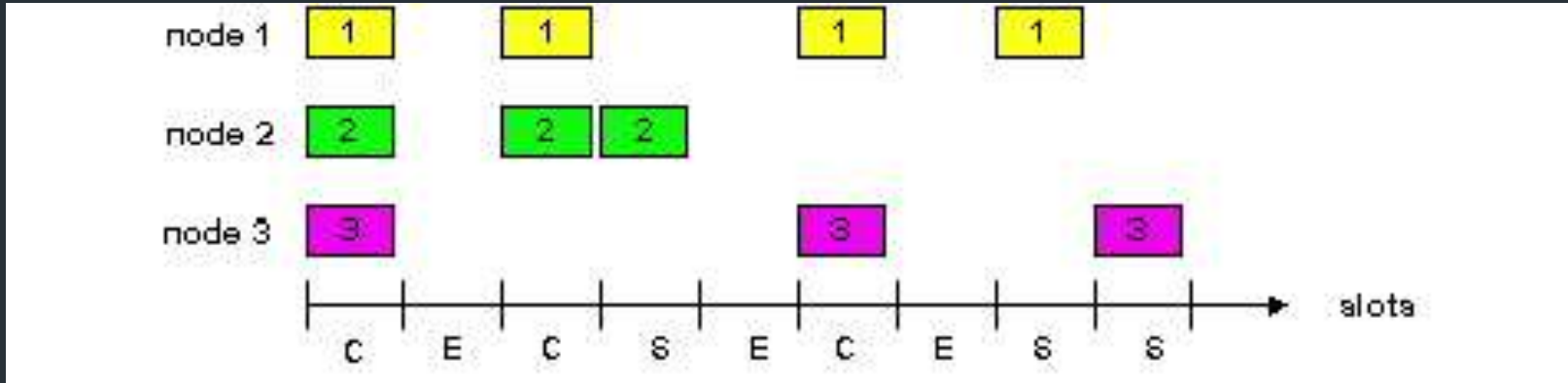
Start to transmit frames only at **beginning of slots**

Nodes are **synchronized** so that each node knows when the slots begin.

If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends.

Slotted ALOHA

72



Source: Data Communications and Networking – Behrouz A. Forouzan

when node obtains fresh frame, it transmits in next slot

If no collision is detected, node can send new frame in next slot

If collision, node retransmits frame in each subsequent slot with prob. p until success

The number of collisions is reduced. And hence, the performance become much better compared to Pure Aloha.

Carrier Sense Multiple Access (CSMA)

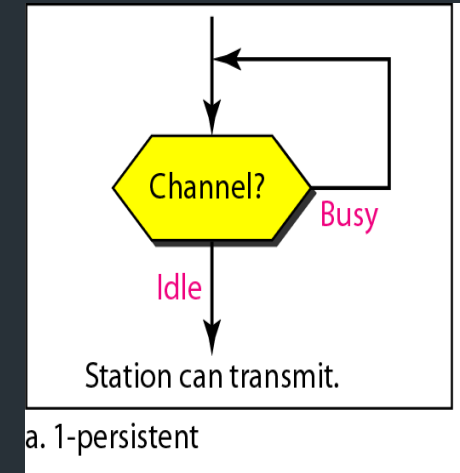
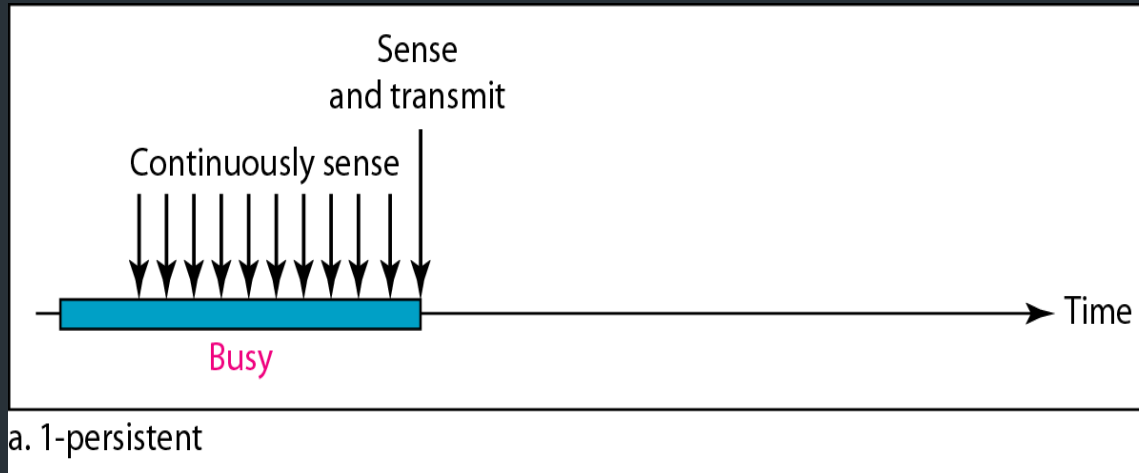
73

- To minimize the collision CSMA was developed, chance of collision was reduced
- Station senses the channel before accessing medium.
- The possibility of collision still exists because of propagation delay

CSMA – Persistence methods

74

- 1- persistence method:
- If the channel is idle it sends its frame immediately with probability 1
- When two or more stations find the line idle and send their frames immediately to create collisions



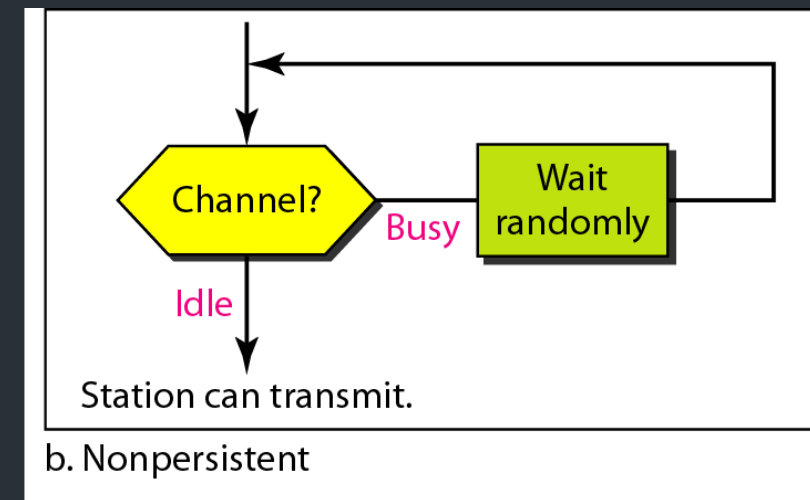
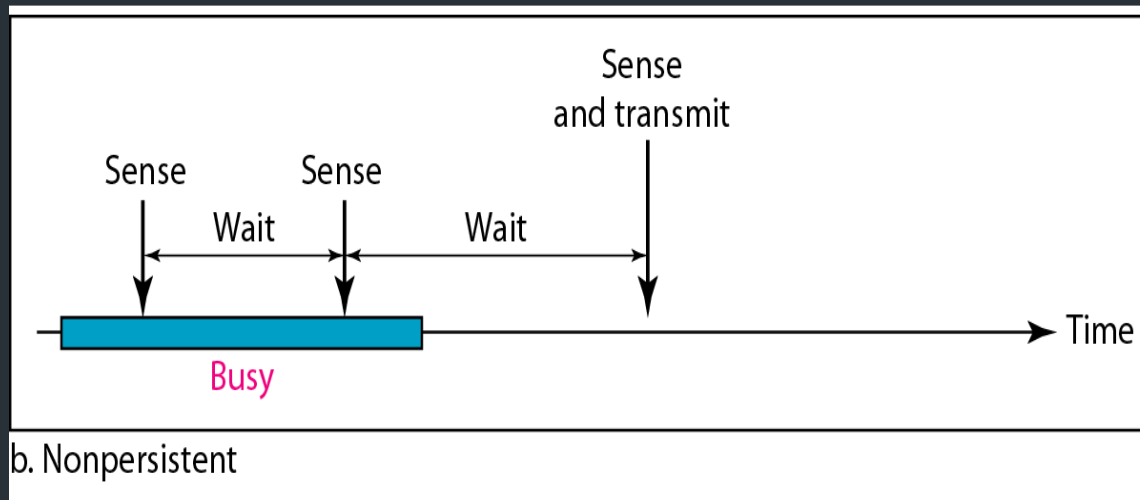
Source: Data Communications and Networking – Behrouz A. Forouzan

Mr.A.Swaminathan VIT Chennai

CSMA –Non Persistence methods

75

- If the line is idle it sends its frame immediately.
- If the line is busy it waits random amount of time and then senses the line again.
- Reduces the collision because it is unlikely that two or more stations will wait the same amount of time and retry

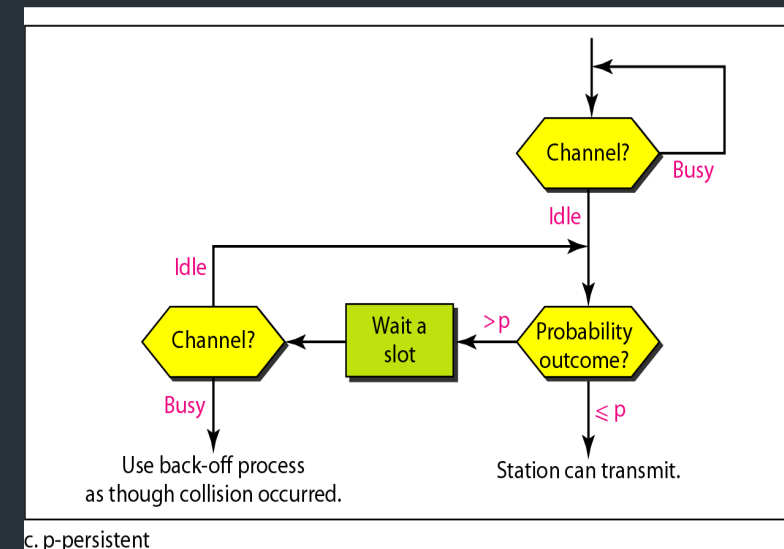
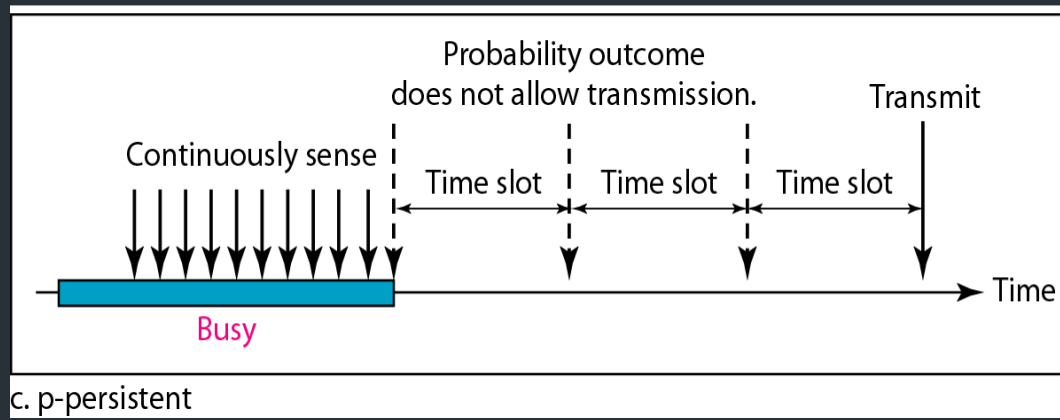


Source: Data Communications and Networking – Behrouz A. Forouzan

CSMA – P-Persistent Method

76

- It applies to slotted channels.
- It senses the channel, If it is idle, it transmits with a probability p .
- With a probability $q = 1 - p$, it waits for the next slot.
- If that slot is idle, it goes to step 1
- If the line is busy it act as though collision has occurred and uses the back off procedure.

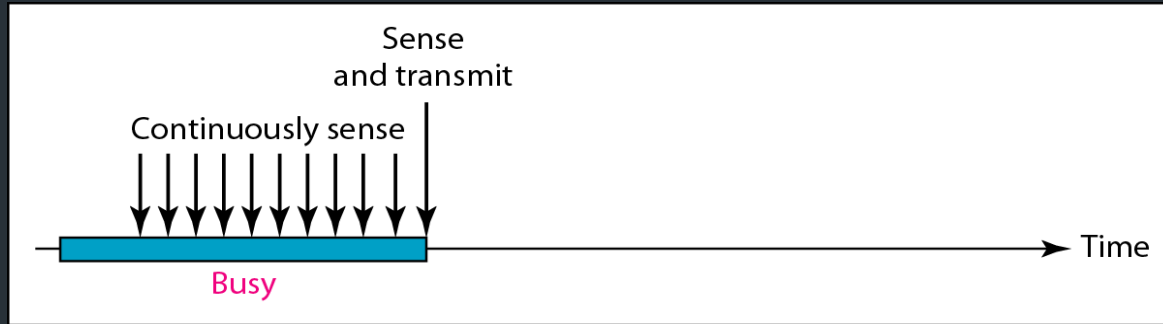


Source: Data Communications and Networking – Behrouz A. Forouzan

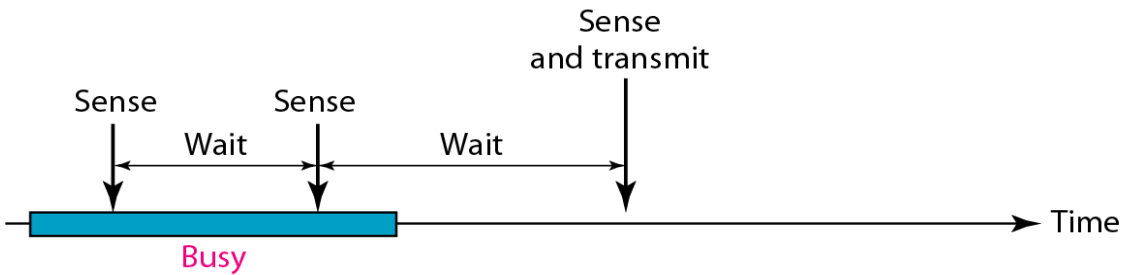
Mr.A.Swaminathan VIT Chennai

CSMA – Persistent Methods

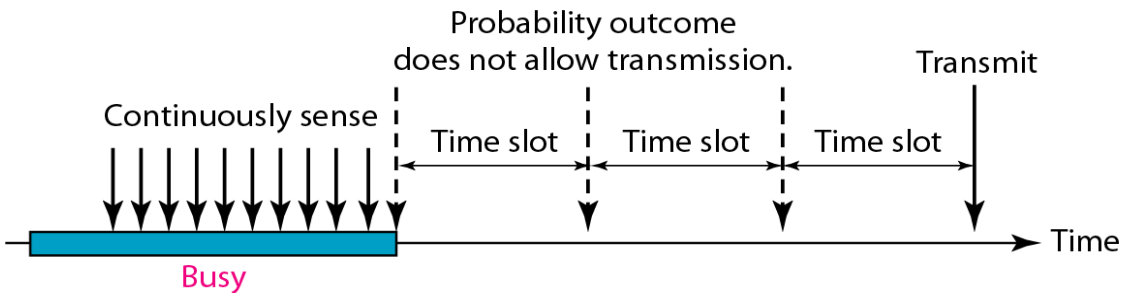
Behavior of three persistence methods



a. 1-persistent



b. Nonpersistent



c. p-persistent

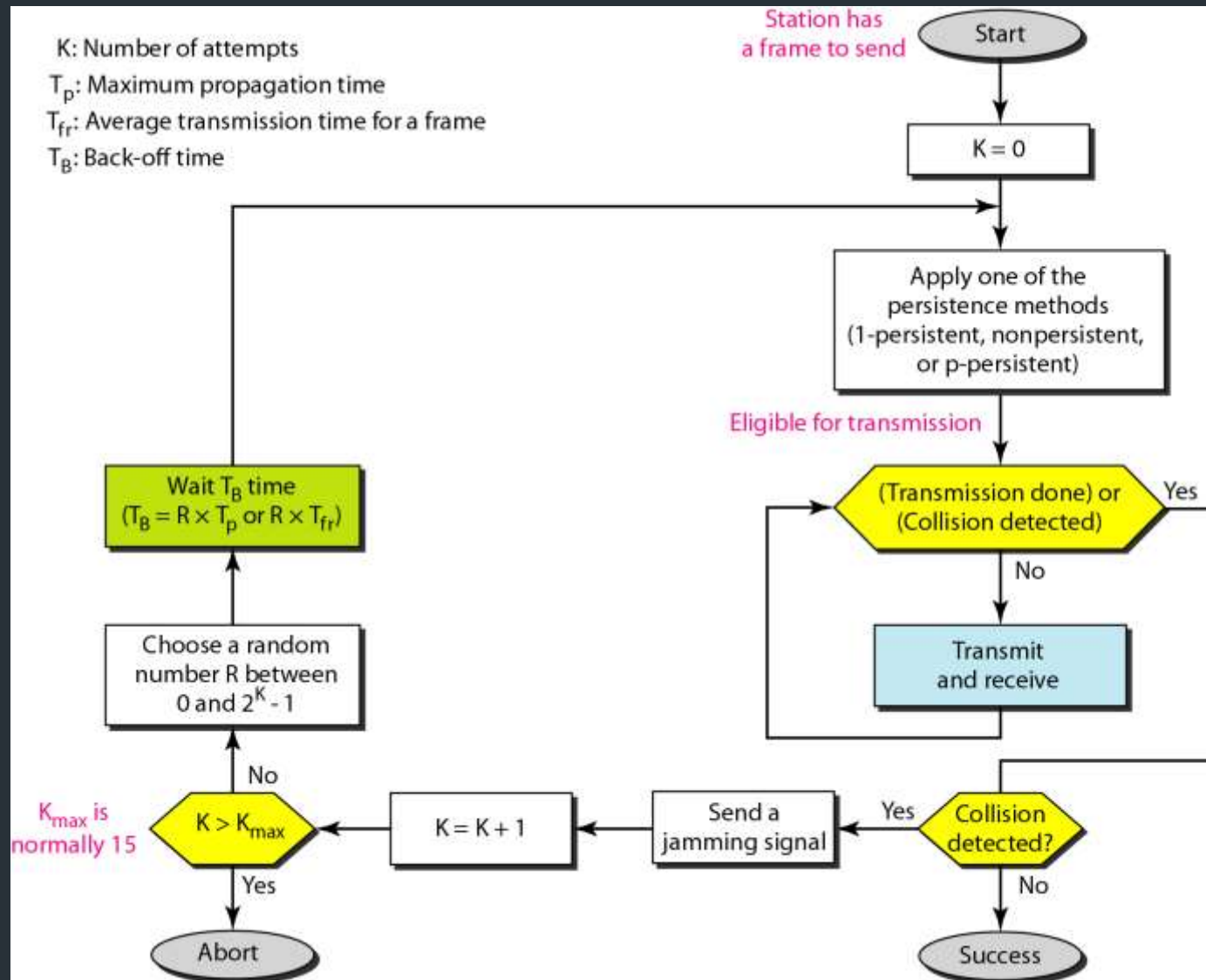
Source: Data Communications and Networking
– Behrouz A. Forouzan

CSMA/CD

- Abort their transmissions as soon as they detect a collision
- Waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.
- Frame transmission time must be two times the maximum propagation time: $T_{fr} = 2 \times T_p$
- Energy levels: zero, Normal Abnormal.

Flow diagram for the CSMA/CD

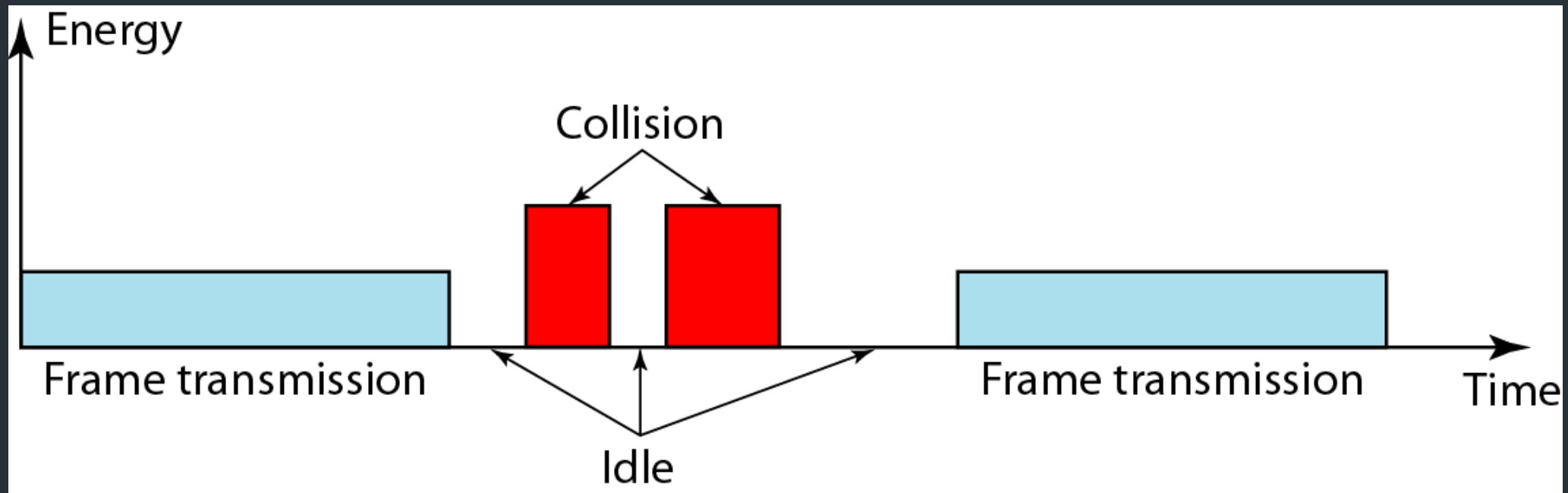
79



Source: Data Communications and Networking – Behrouz A. Forouzan

Energy level during transmission, idleness, or collision

80



Source: Data Communications and Networking – Behrouz A. Forouzan

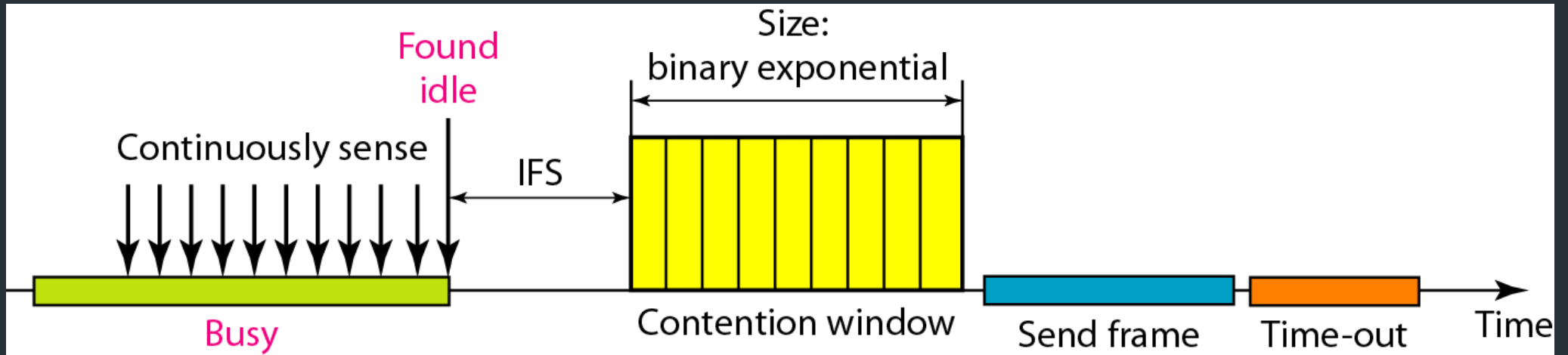
CSMA/CA

- When there is collision the station receives two signals: its own and the signal transmitted by a second station.
- In wired N/W received signal is the same as the sent signal (Losses are less).
- In wireless N/W much of the sent energy is lost in transmission (Transmission Losses).
- Avoid collision on wireless network because they cannot be detected.

CSMA/CA

- When channel is free waits for period of time called the interframe space or IFS.
- After IFS time the station still waits to a time equal to the contention time
- Contention window is an amount of time divided into slots.

Timing in CSMA/CA

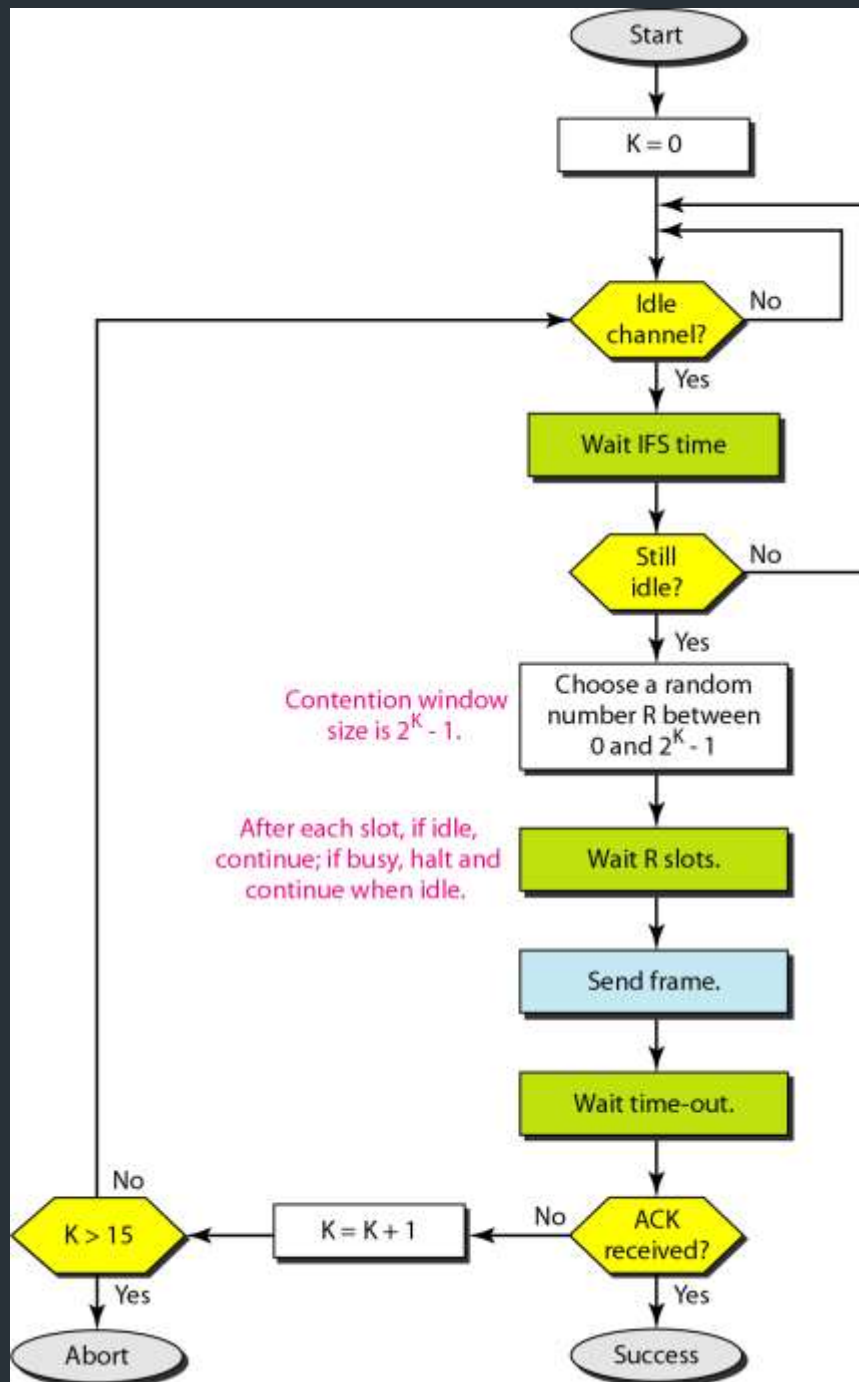


Source: Data Communications and Networking – Behrouz A. Forouzan

Flow diagram CSMA/CA

84

Source: Data Communications and Networking – Behrouz A. Forouzan



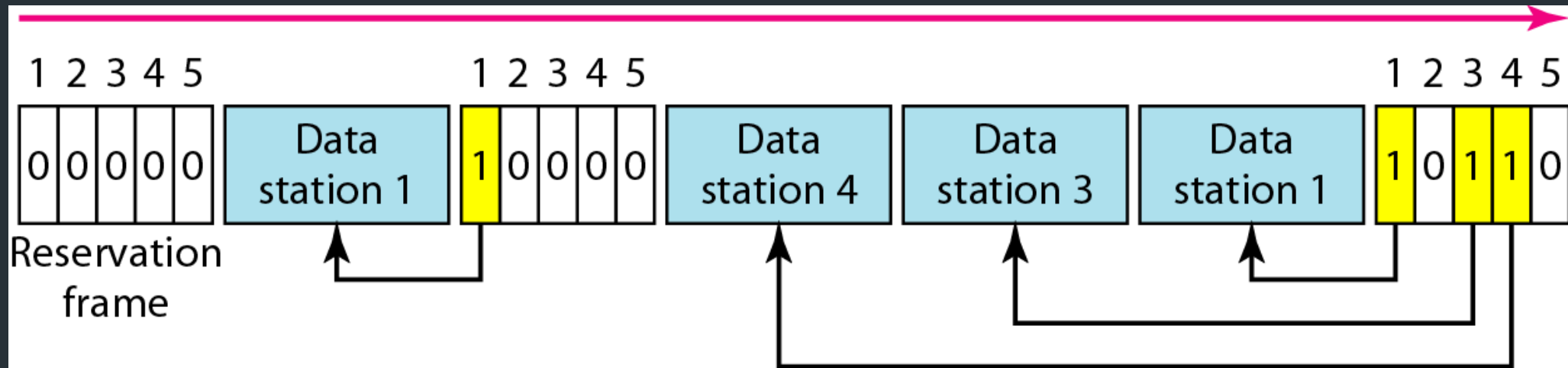
Controlled Access

- 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.
- Reservation
- Polling
- Token Passing

Reservation access method

- A station must make a reservation before sending data
- Time is divided into intervals
- A reservation frame proceeds each time interval
- Number of stations and number of time slots in the reservation frame are equal
- Each time slot belongs to a particular station

Reservation access method

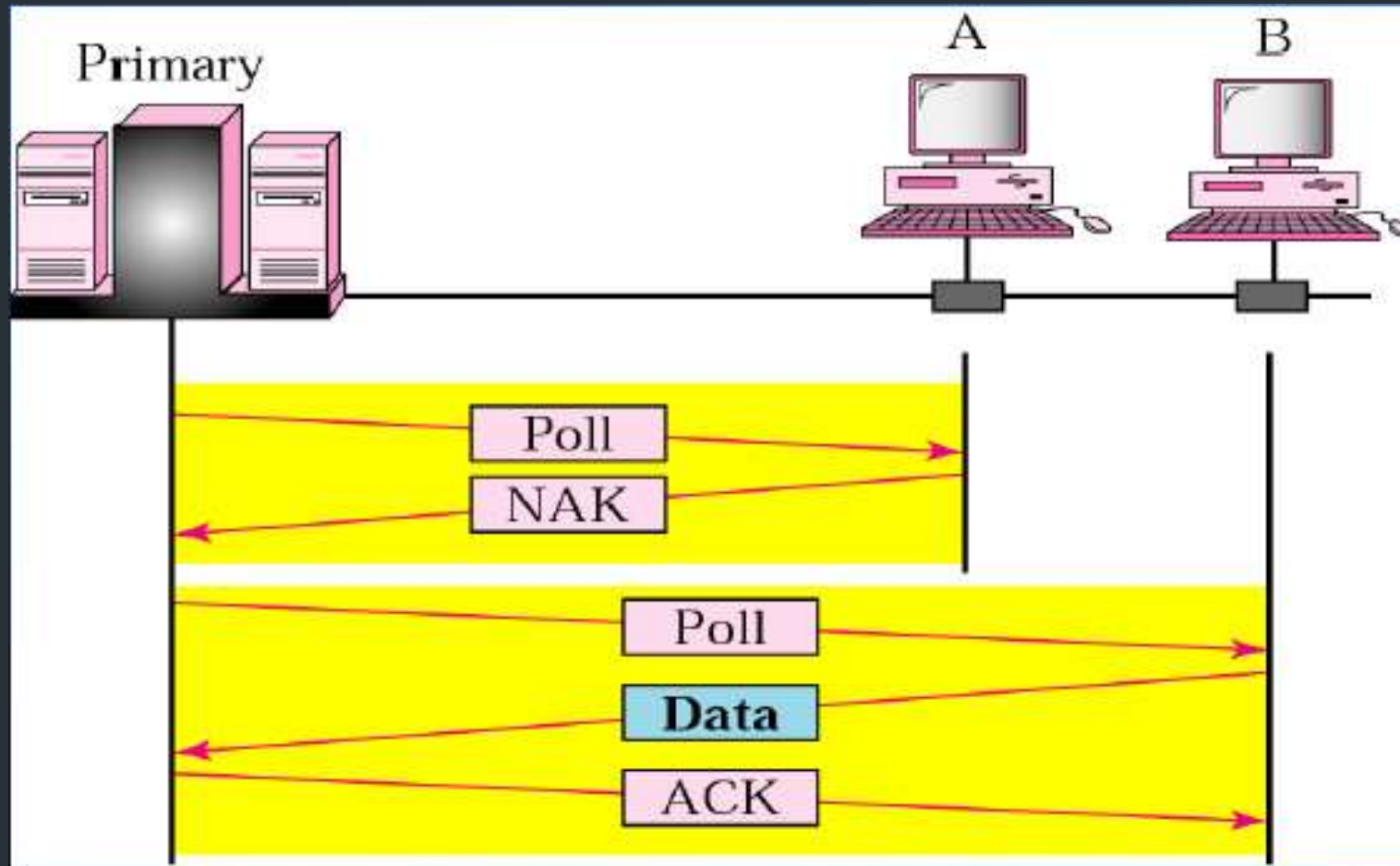


Source: Data Communications and Networking – Behrouz A. Forouzan

Polling

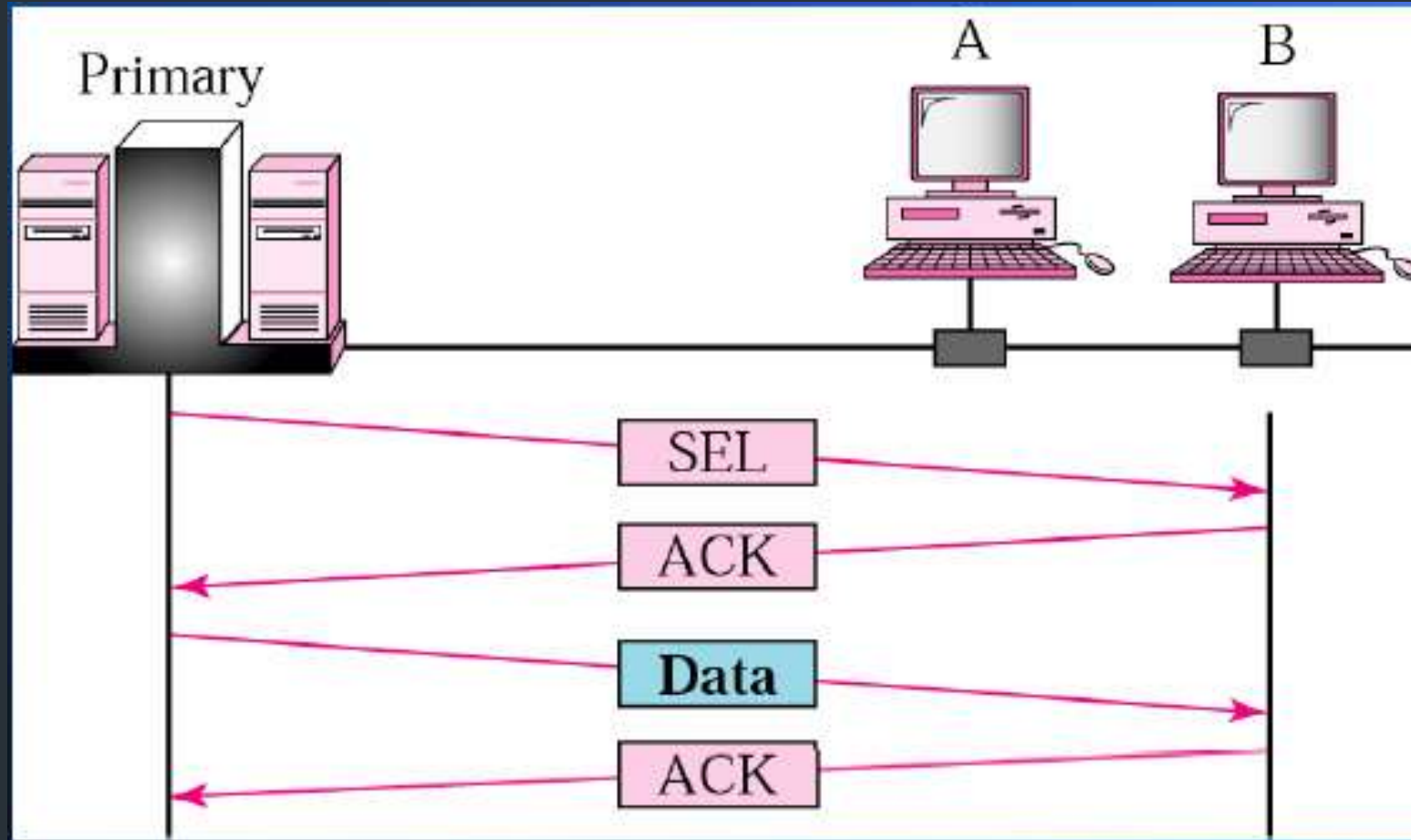
- Devices are categorized into:
 - Primary station (PS)
 - Secondary station (SS)
- All data exchange must go through the primary station
- Primary station controls the link and initiates the session
- Secondary station obey the instructions of PS.
- 1. PS polls stations
 - Asking SS if they have something to send
- 2. PS select a SS
 - Telling it to get ready to receive data

PS Polls Stations



Source: Data Communications and Networking – Behrouz A. Forouzan

PS select a SS



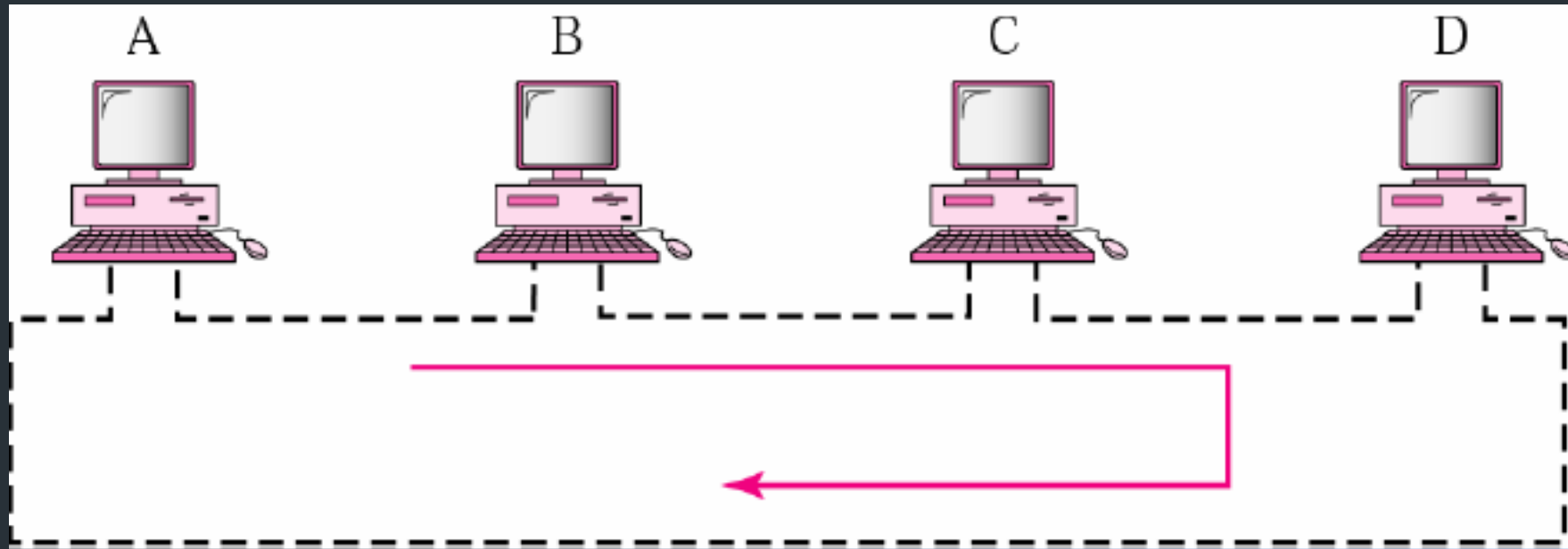
Source: Data Communications and Networking – Behrouz A. Forouzan

Token passing

- Stations in a network are organized in a logical ring, for each station, there is a predecessor and a successor
- For a station to access the channel, it must possess a token (special packet) that gives the station the right to access the channel and send its data
- Once the station has finished its task, the token will then be passed to the successor (next station)
- The station cannot send data until it receives the token again in the next round
- Token management is necessary
 - Every station is limited in the time of token possession
 - Token must be monitored to ensure no loss or destroyed
 - Assign priorities to the stations and to the types of data transmitted
 - To make low-priority stations release the token to high priority stations

Token Passing Procedure

92



Source: Data Communications and Networking – Behrouz A. Forouzan

Channelization

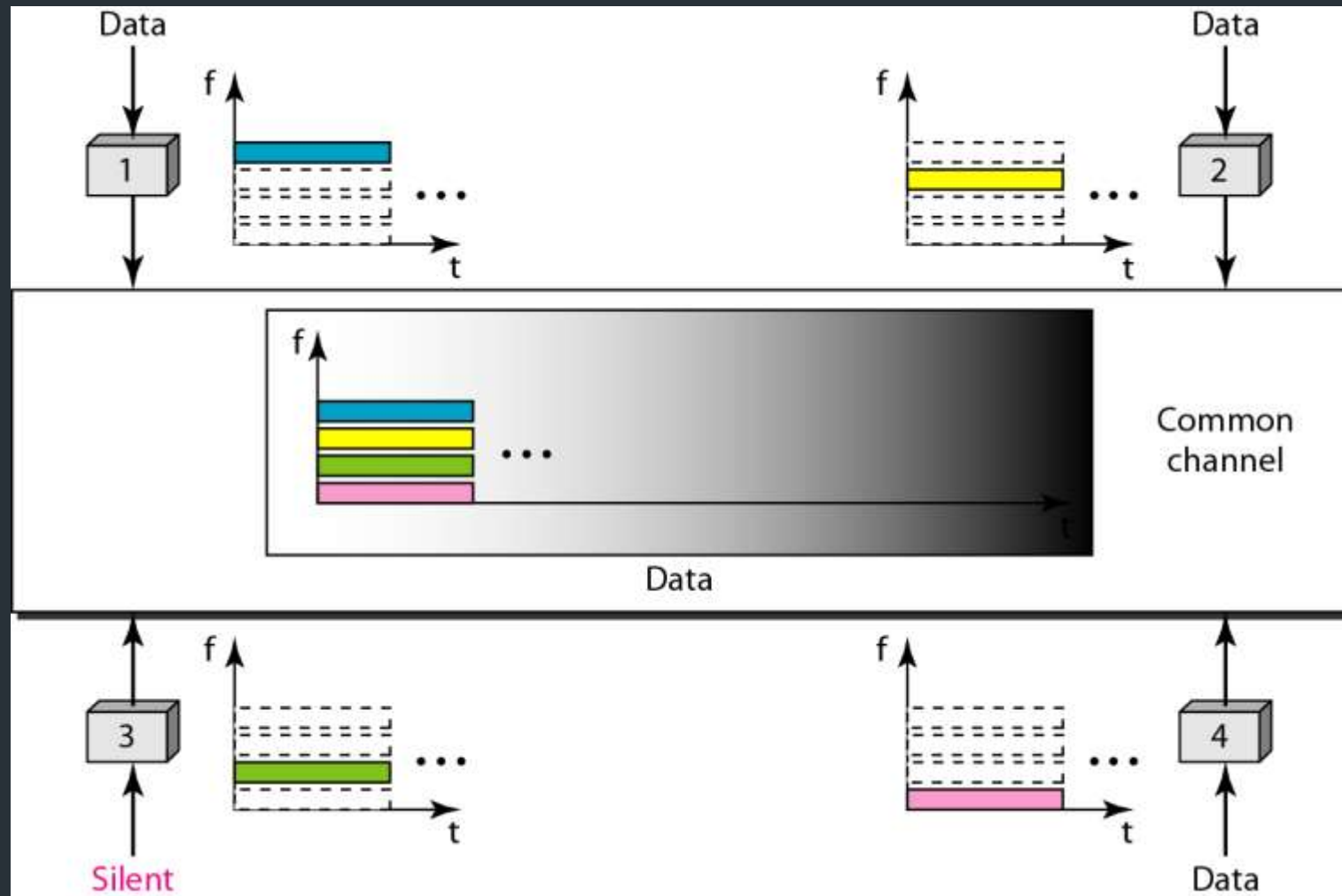
- **Channelization** is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations. In this section, we discuss three channelization protocols.
- Frequency-Division Multiple Access (FDMA)
- Time-Division Multiple Access (TDMA)
- Code-Division Multiple Access (CDMA)

Frequency –Division Multiple Access (FDMA)

- In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.

FDMA

95



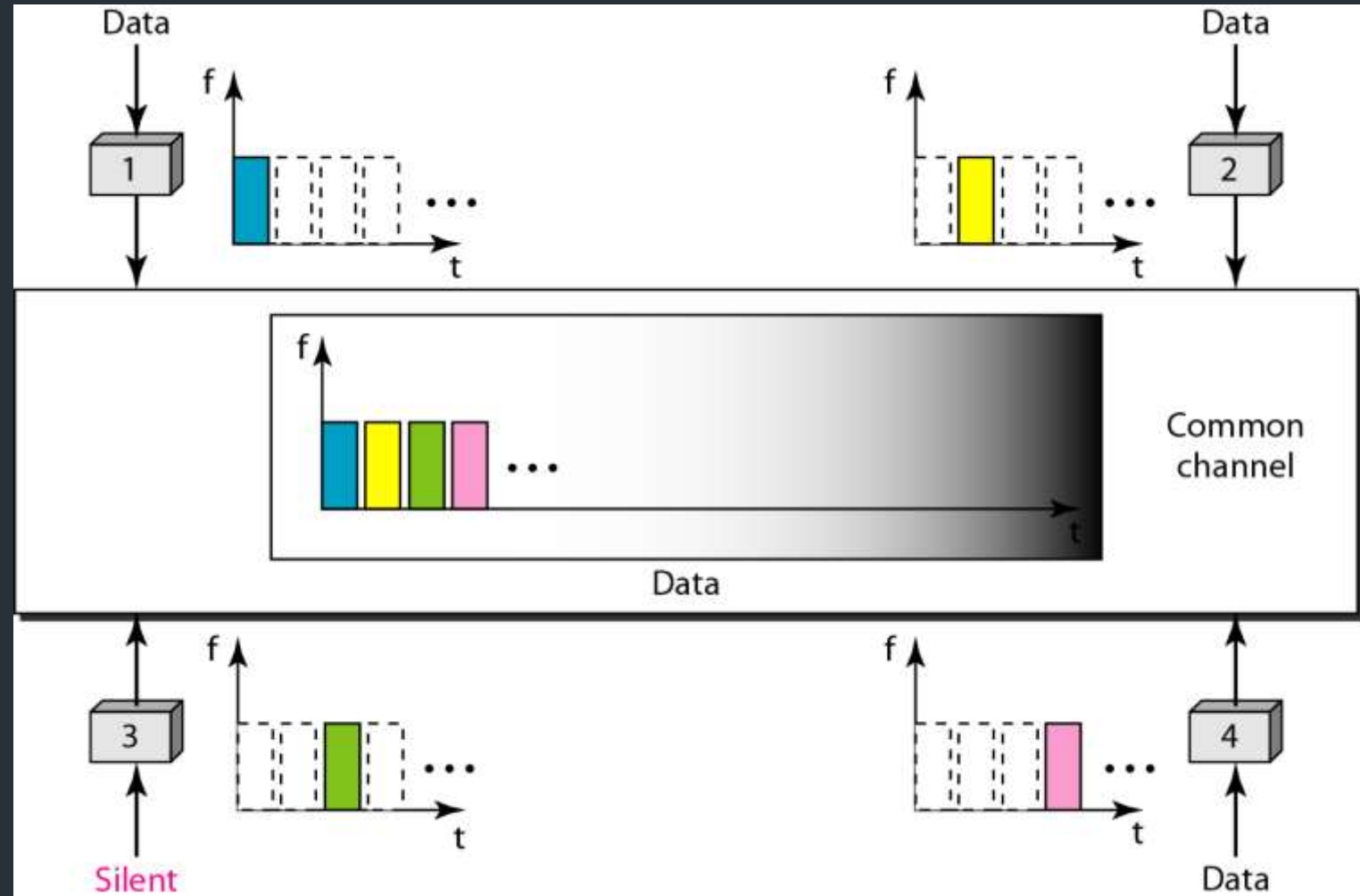
Source: Data Communications and Networking – Behrouz A. Forouzan

Mr.A.Swaminathan VIT Chennai

Time Division Multiple Access (TDMA)

96

- In TDMA, the bandwidth is just one channel that is timeshared between different stations.

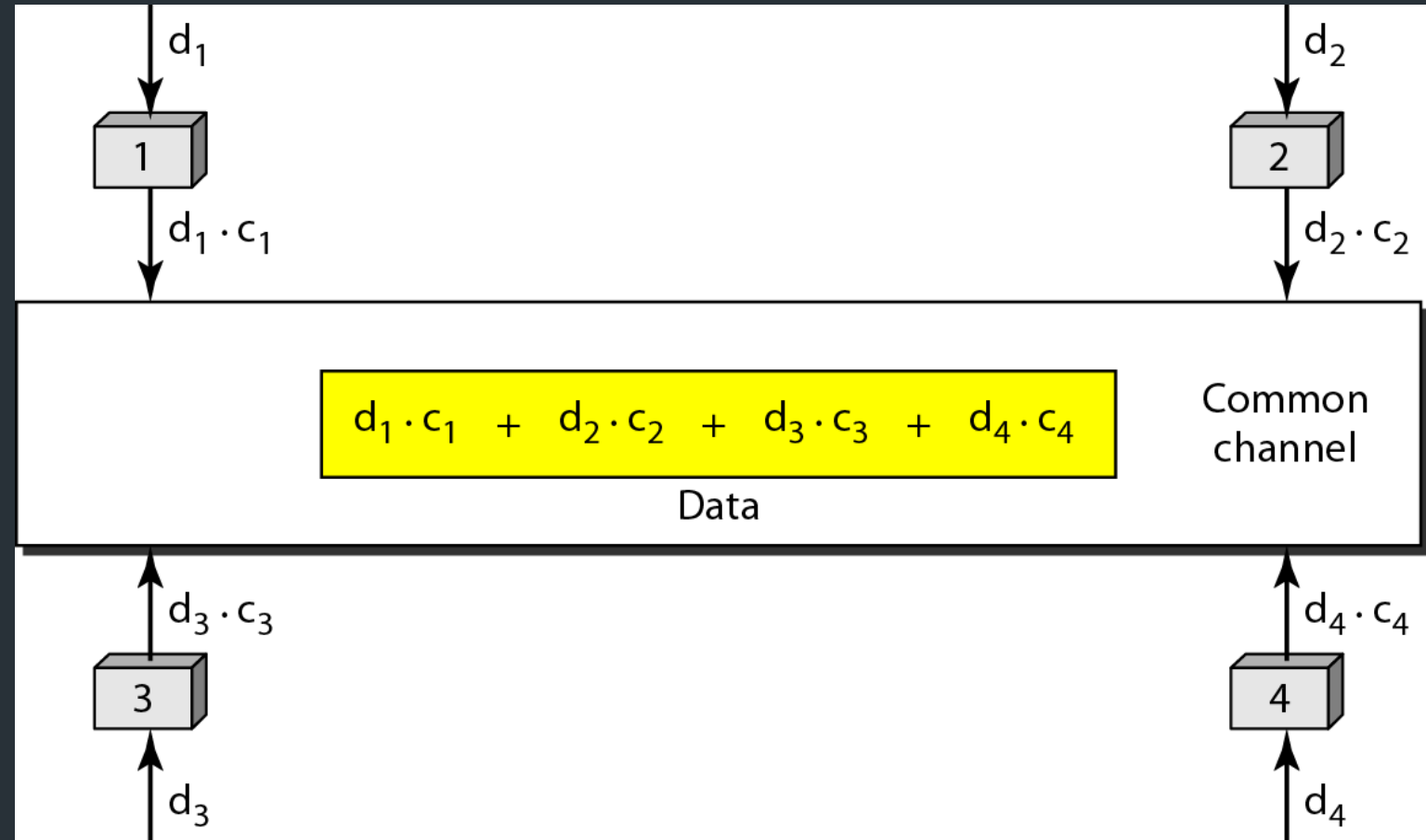


Source: Data Communications and Networking – Behrouz A. Forouzan

Code-Division Multiple Access (CDMA)

- In CDMA, one channel carries all transmissions simultaneously.

Simple idea of communication with code

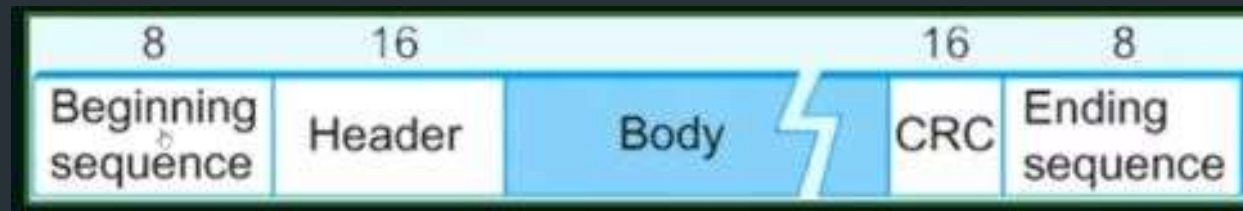


Source: Data Communications and Networking – Behrouz A. Forouzan

FRAME FORMATION IN DATALINK LAYER

98

- A frame is viewed as collection of bits
- Protocol HDLC – High Level Data Link Control



Source: Data Communications and Networking – Behrouz A. Forouzan

Allows frame to contain arbitrary number of bits and arbitrary character size.

The frames are separated by separating flag.

Each frame begins and ends with a special bit pattern, 01111110 called a flag byte.

When five consecutive 1's are encountered in the data, it automatically stuffs a '0' bit into outgoing bit stream.

Bit stuffing

- In this method, frames contain an arbitrary number of bits and allow character codes with an arbitrary number of bits per character. In this case, each frame starts and ends with a special bit pattern, 01111110.
- In the data a 0 bit is automatically stuffed into the outgoing bit stream whenever the sender's data link layer finds five consecutive 1s.

Bit Stuffing

- This bit stuffing is similar to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit.
- Bit Stuffing is completely transparent to network layer as byte stuffing.
- The figure1 below gives an example of bit stuffing.
- This method of framing finds its application in networks in which the change of data into code on the physical medium contains some repeated or duplicate data.
- For example, some LANs encodes bit of data by using 2 physical bits.

Bit Stuffing

101

(a) 0110111111111111111111110010

(b) 011011111011111011111010010

(c) 01101111111111111111111111110010

Stuffed bits

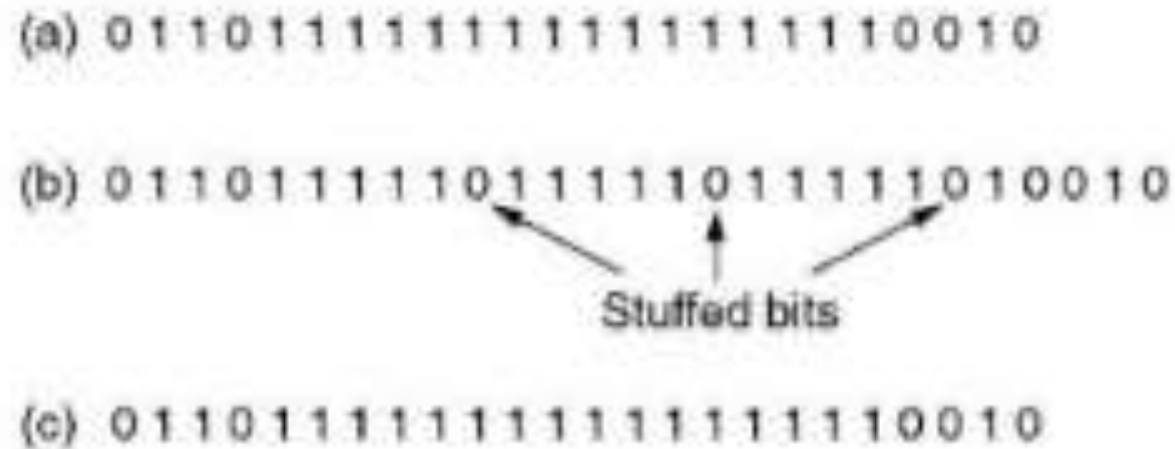


Fig1: Bit stuffing

Source: Data Communications and Networking – Behrouz A. Forouzan

Byte Stuffing

- In this method, start and end of frame are recognized with the help of flag bytes. Each frames starts with and ends with a flag byte.
- Two consecutive flag bytes indicate the end of one frame and start of the next one. The flag bytes used in the figure 2 used is named as “ESC” flag byte.
- A frame delimited by flag bytes. This framing method is only applicable in 8-bit character codes which are a major disadvantage of this method as not all character codes use 8-bit characters e.g. Unicode.
- Four example of byte sequences before and after stuffing:

Byte Stuffing

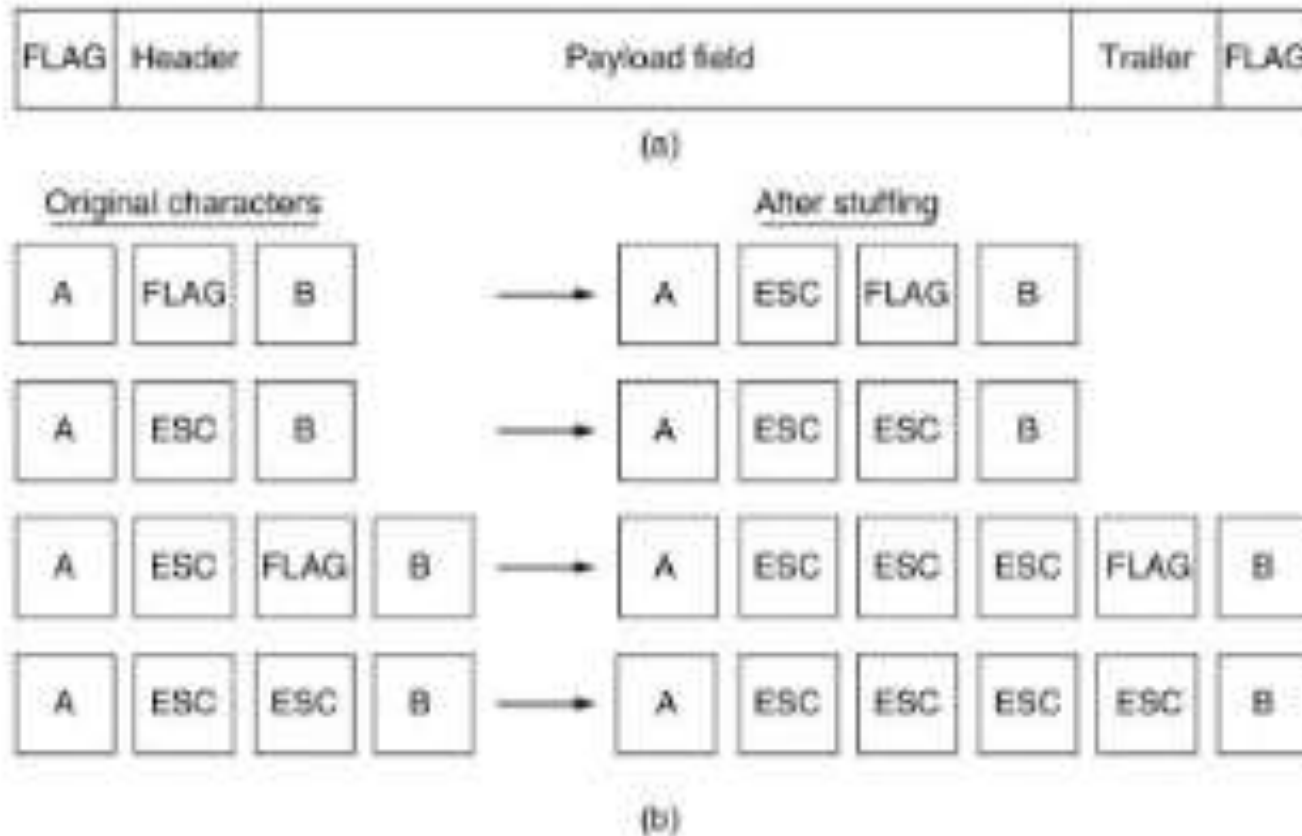


Fig2: Framing with Byte stuffing

Character or Byte Stuffing

- When a binary data contains a data which resembles flag byte pattern then there occurs a problem.
- This situation will usually interfere with framing.
- The solution for this is Character or Byte stuffing where sender's data link layer insert a special escape byte (ESC) just before each "original data that resembles flag byte".
- At the receiver end the data link layer removes ESC byte before the data are given to the network layer.

Theory_Class_14

Bluetooth

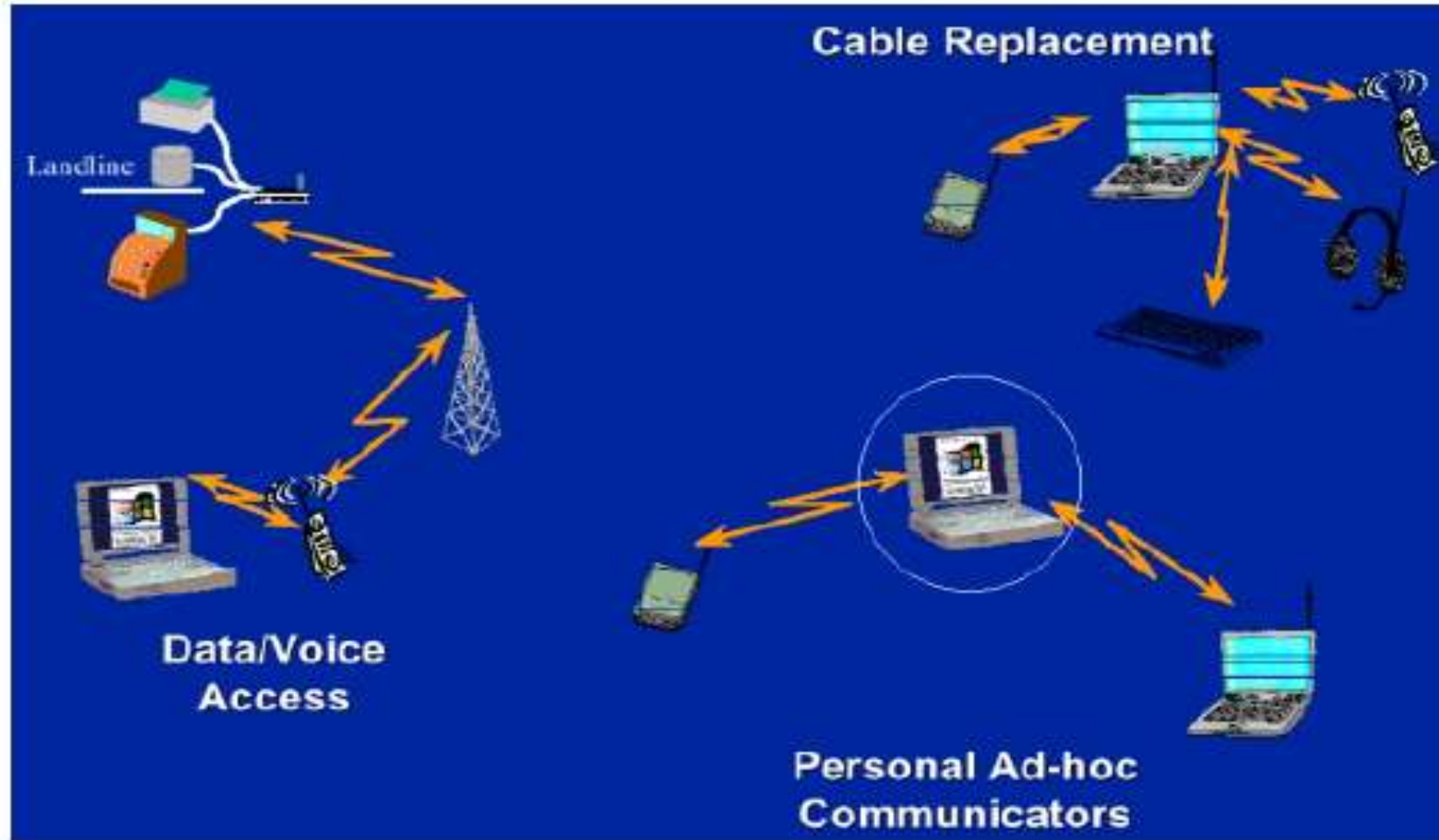
106



- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio + baseband
 - ✓ at low power & low price
- Why not use Wireless LANs?
 - power
 - cost

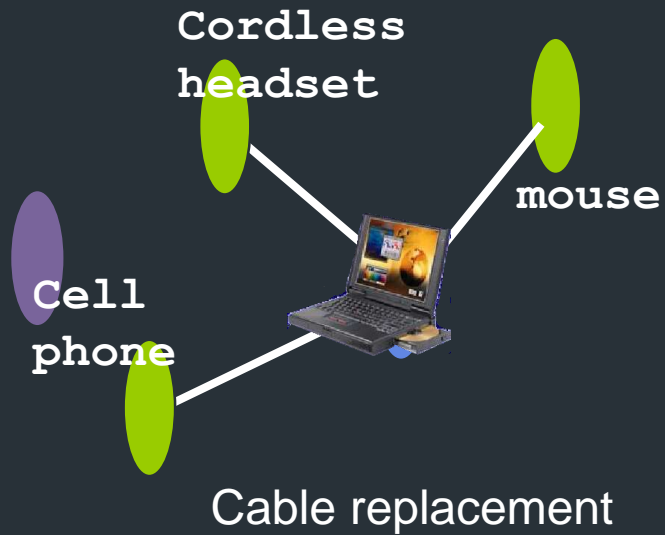
Bluetooth Concept

107



Applications of Bluetooth

108



Bluetooth

- **The ultimate goal is to make small products (PC/Laptops) have only one wire attached to power cord.**
- **In case of PDA, the power cord is also eliminated.**
- **A simple application of Bluetooth is updating the phone directory of the PC from a mobile telephone.**
- **A typical Bluetooth has a range of 10 m.**

Usage Models (1)

110

- Internet Bridge

- ◆ Mobile browsing in the sofa, on the go, in the office, in the car



Usage Models (2)

- Instant Postcard
 - ◆ Send instant postcards and videoclips



Usage Models (3)

112

- Ultimate Headset
 - ◆ Keep your hands free



Usage Models (4)

- Briefcase Trick

- ◆ Laptop in briefcase

E-mail alert through phone,
browse E-mails in phone

- ◆ Phone off

Answer mail on laptop and
send mail from phone or
laptop at arrival



Usage Models (5)

114

- Synchronizer

- ◆ Background synchronization

PDAs

Cellular phones

Notebooks



Usage Models (6)

115

- Wireless Workspace
 - ◆ Wirelessly connected computer peripherals



Usage Models (7)

116

- Conference Table
 - ◆ Share and exchange data in the meeting room



Radio Features

117

- **Connected radios can be master or slave**
- **Radios are symmetric**
 - Same radio can be master or slave
- **Piconet: Master can connect to 7 simultaneous or 200+ park slaves per Piconet.**
- **Data rate: 1M Hz**
 - Symbol rate: 1M bps
 - Data rate: 721k bps excluding header

Radio Features

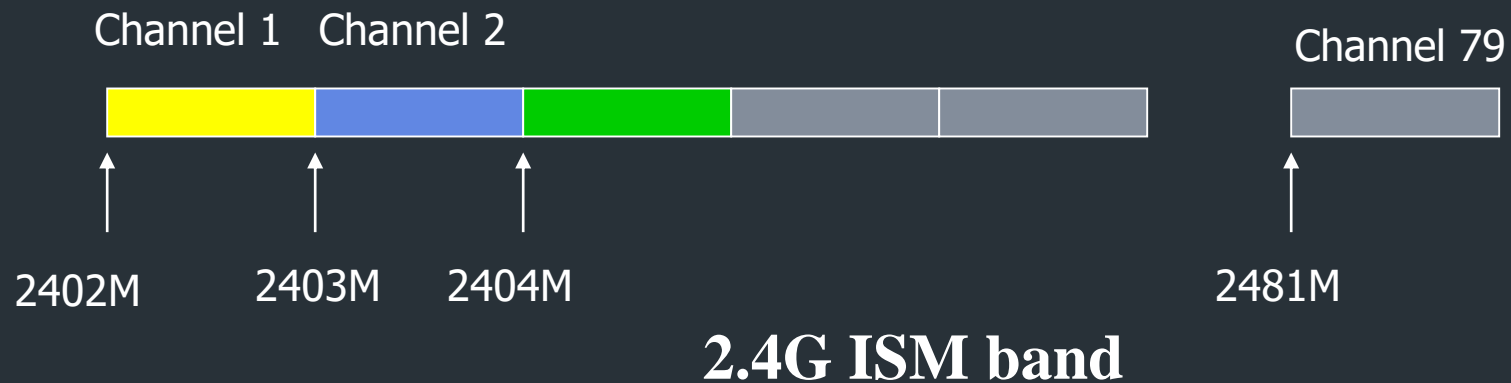
118

- **2.4Ghz ISM unlicensed band.**
- **Spread spectrum frequency hopping radio**
 - **Avoid interference**
 - **79 channels hops every packet.**
 - **Nominally hops at 1600 times a second**

Bandwidth Management

119

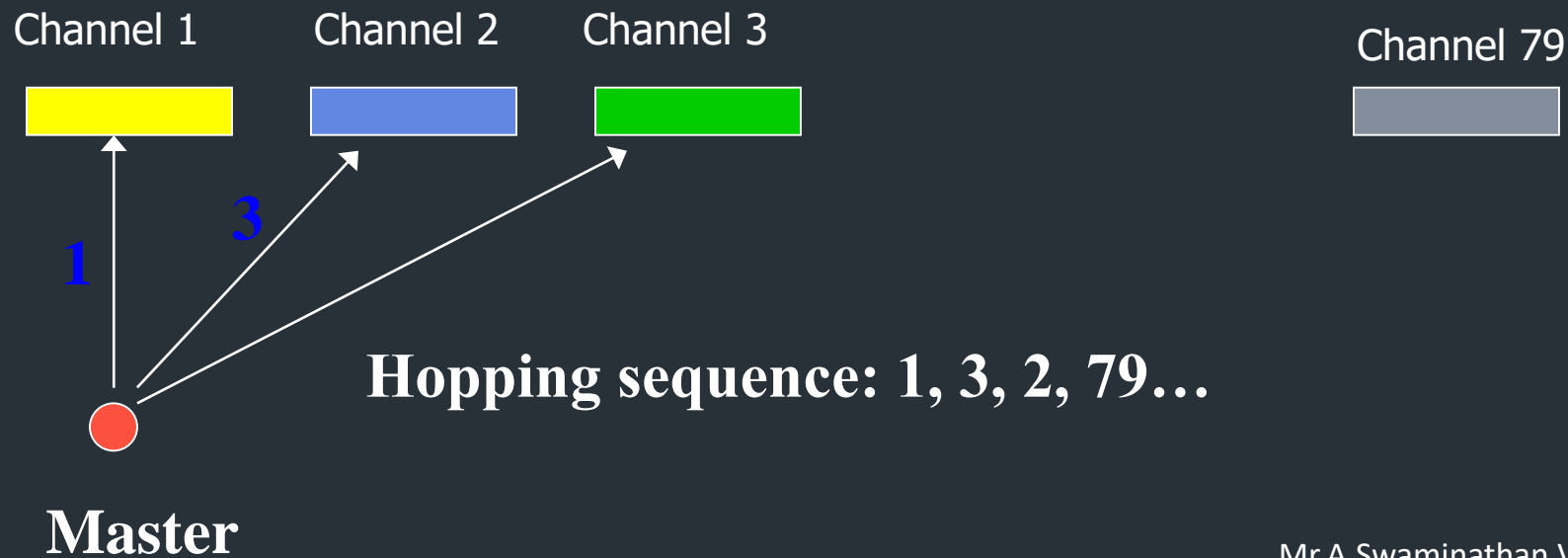
- **2.4G ISM band**
 - 2402-2480 M Hz
 - In total, 79 channels are scheduled
 - Each channel occupies 1M Hz
 - Bandwidth: 1M bps



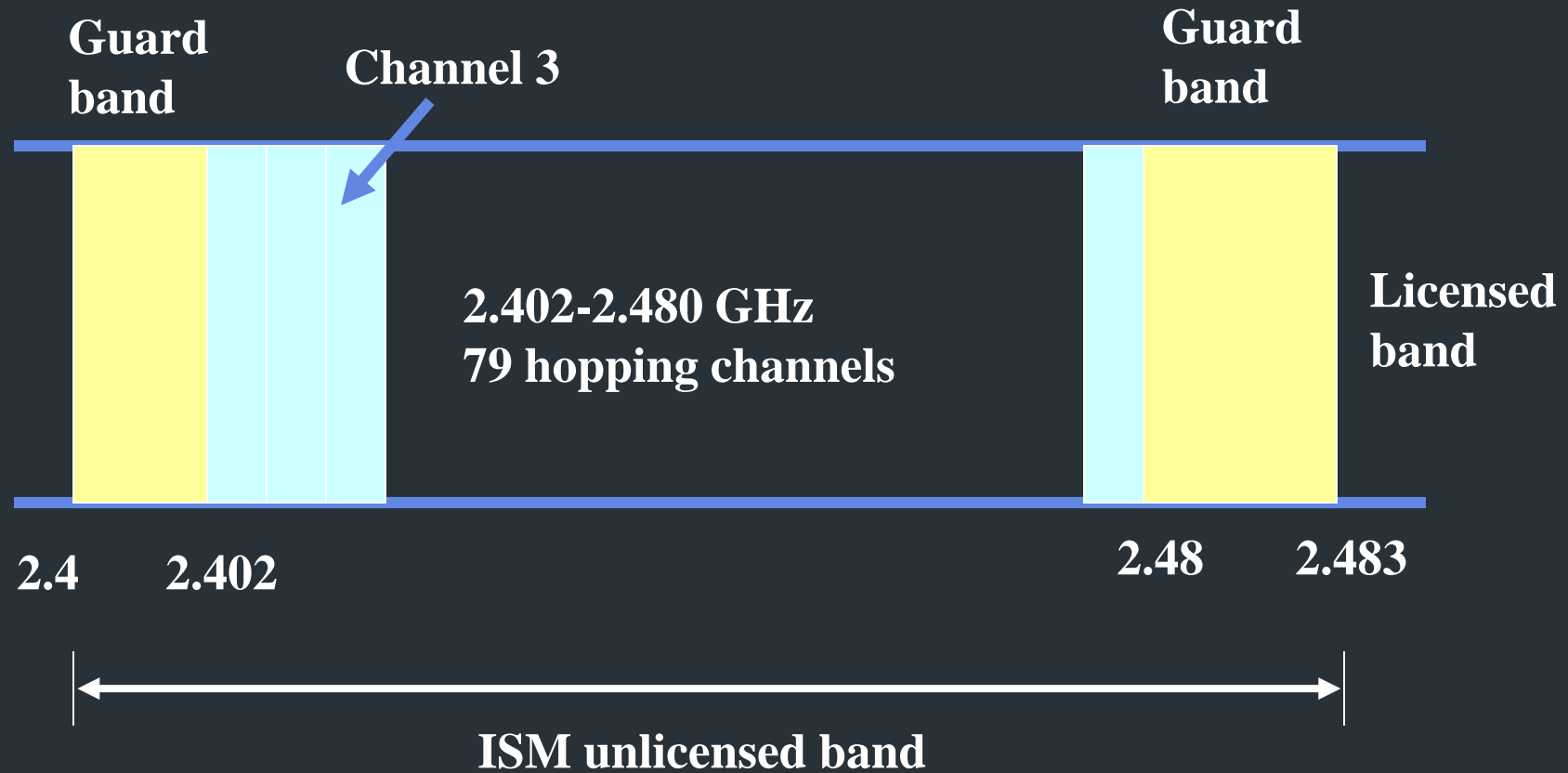
Frequency Hopping

120

- Master hops 1600/s → 0.625ms/hop
- The master hops to another channel according to its hopping sequence

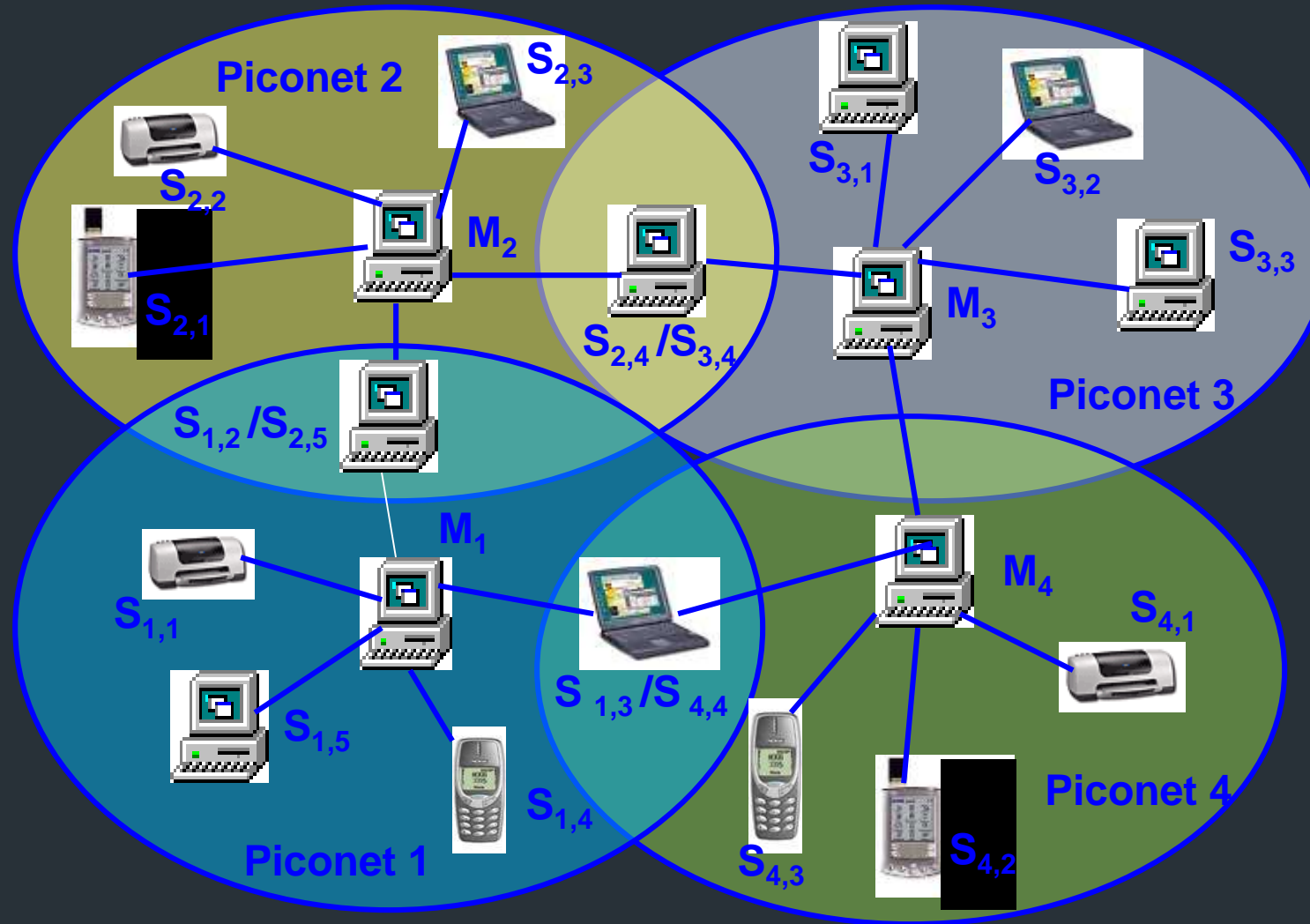


Frequency Bands



Architecture of Bluetooth System and Scatternet

122



Bluetooth Technological Characteristics

123

Frequency band	2.4 GHz (unlicensed ISM band)
Technology	Spread spectrum
Transmission method	Hybrid direct sequence and frequency hopping
Transmission power	1 milli-watt (0 dBm)
Range	10 meters (40 feet)
Number of devices	8 per piconet, 10 piconets per coverage area
Data speed	Asymmetric link: 721+57.6 kbps
	Symmetric link: 432.6 kbps
Maximum voice channels	3 per piconet
Maximum data channels	7 per piconet
Security	Link layer w/s fast frequency hopping (1600 /sec)
Power consumption	30 μ A sleep, 60 μ A hold, 300 μ A standby, 800 μ A max transmit
Module size	3 square cm (0.5 square inches)
Price	Expected to fall to \$5 in the next few years
C/I co-channel	11 dB (0.1% BER)
C/I 1 MHz	-8 dB (0.1% BER)
C/I 2 MHz	-40 dB (0.1% BER)
Channel switching time	220 μ s

Architecture

- **Bluetooth radio typically hops faster and uses shorter packets as compared to other systems operating in the same frequency band.**
- **Use of FEC (Forward Error Correction) limits the impact of random noise.**
- **As the interference increases, the performance decreases.**

Architecture (cont'd)

125

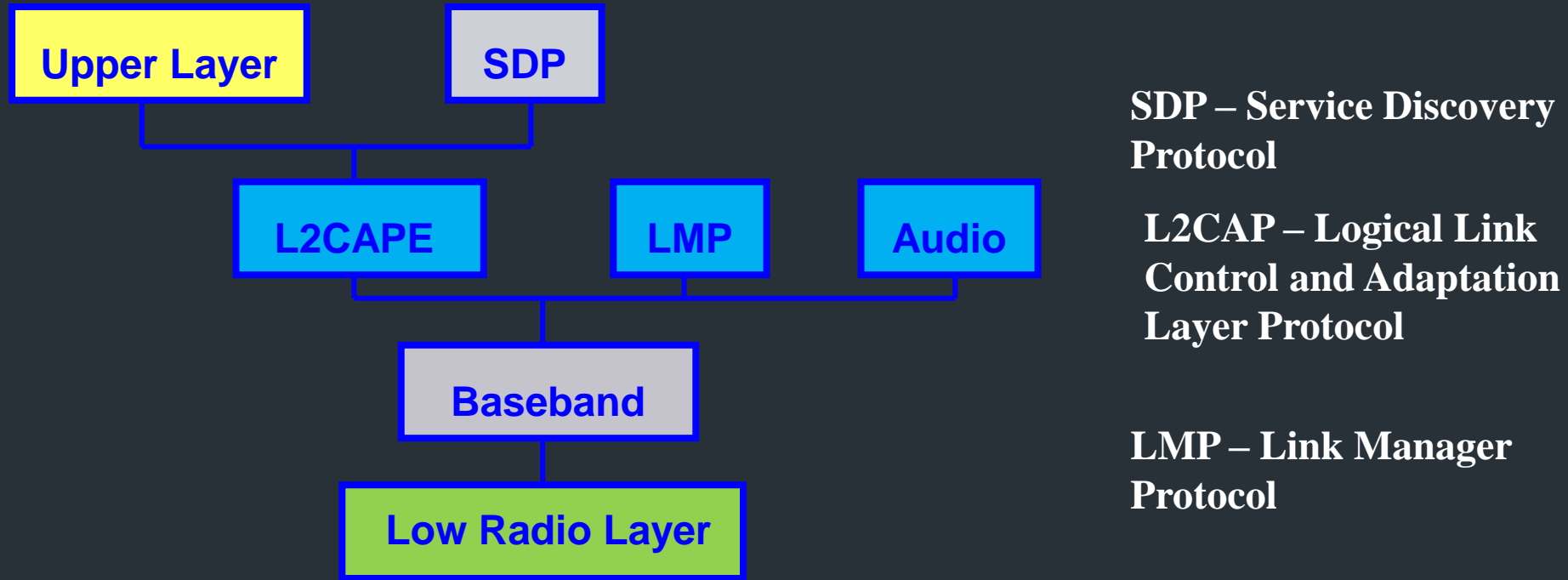
- **Bluetooth devices can interact with other Bluetooth devices.**
- **One of the devices acts as a master and others as slaves.**
- **This network is called “Piconet”.**
- **A single channel is shared among all devices in Piconet.**
- **There can be up to seven active slaves in the Piconet.**
- **Each of the active slaves has an assigned 3 bit Active Member address.**
- **A lot of other slaves can remain synchronized to the Master through remaining inactive slaves, referred to as parked nodes.**
- **A parked device remains synchronized to the master clock and can become active and start communicating in the Piconet anytime.**

Architecture (cont'd)

- If Piconets are close to each other, they have overlapping areas
- The scenario where the nodes of two or more Piconets mingle is called Scatternet
- Before any connections in the Piconet are created all devices are in STDBY mode
- In this mode an unconnected unit periodically “listens” for message every 1.28 seconds

Bluetooth Core Protocol

127



- **SDP:** Provides a mean for applications to discover which services are provided by or available through a Bluetooth device
- **L2CAP:** Supports higher level protocol multiplexing, packet segmentation and reassembly and conveying of QoS information
- **LMP:** Used by Link managers for link set up and control
- **Baseband:** Enables the physical RF link between Bluetooth units forming a Piconet

Bluetooth(IEEE 802.15.1)

- It is named after the King of Denmark.
- It is a short range RF communication.
- Low cost, low power, radio based wireless link eliminates the need for short cable.
- Bluetooth radio technology built into both the cellular telephone and the laptop would replace the cable used today to connect a laptop to cellular phone.
- Printers, desktops can all be wireless.
- It also provides a universal bridge to existing data networks (Fig 14.11).

Theory_Class_15

Presentation Outline

- Wireless Technology overview
- The IEEE 802.11 WLAN Standards
- Secure Wireless LANs
- Migrating to Wireless LANs (Cutting the cord)

Wireless?

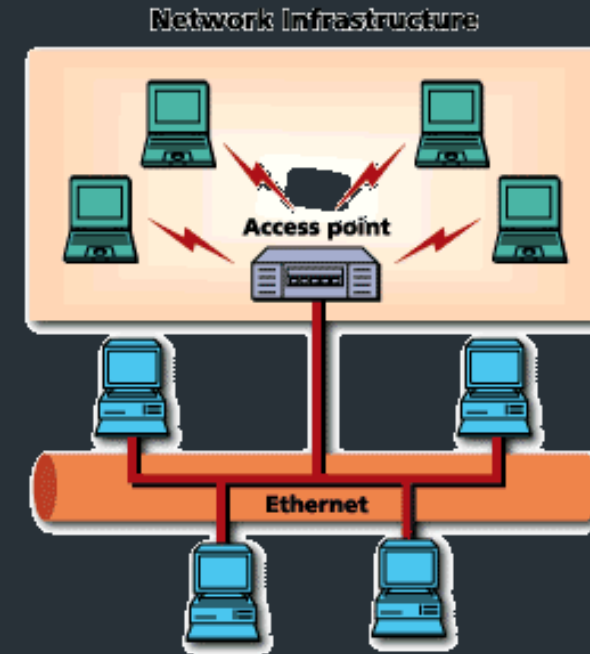
- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.
- The last link with the users is wireless, to give a network connection to all users in a building or campus.
- The backbone network usually uses cables

Common Topologies

132

The wireless LAN connects to a wired LAN

- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



Common Topologies

133

Complete Wireless Networks

- The physical size of the network is determined by the maximum reliable propagation range of the radio signals.
- Referred to as **ad hoc** networks
- Are self-organizing networks without any centralized control
- Suited for temporary situations such as meetings and conferences.



How do wireless LANs work?

Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications.

How are WLANs Different?

- They use specialized **physical and data link** protocols
- They integrate into existing networks through **access points** which provide a bridging function
- They let you stay connected as you **roam** from one coverage area to another
- They have unique **security** considerations
- They have specific **interoperability** requirements
- They require **different hardware**
- They offer **performance** that differs from wired LANs.

Physical and Data Link Layers

Physical Layer:

- The wireless **NIC** takes **frames** of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a **radio carrier signal**.

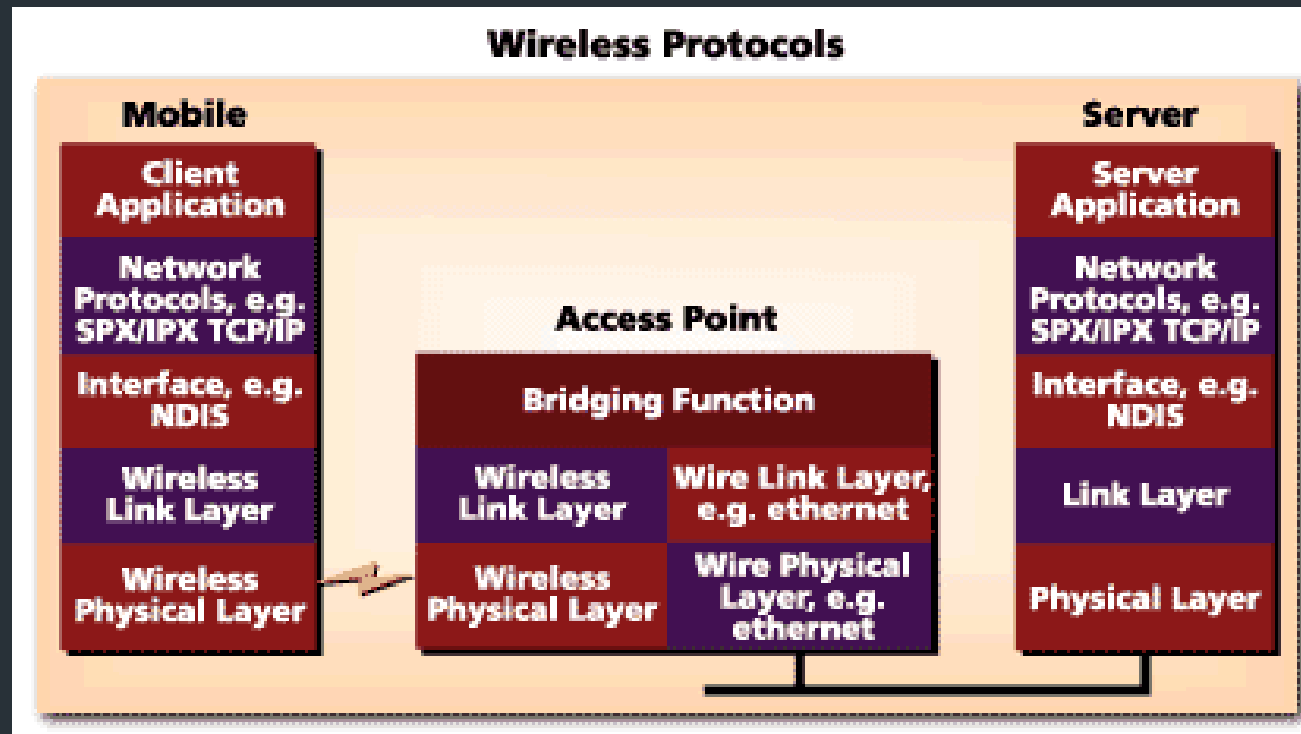
Data Link Layer:

- Uses **Carriers-Sense-Multiple-Access with Collision Avoidance** (CSMA/CA).

Integration With Existing Networks

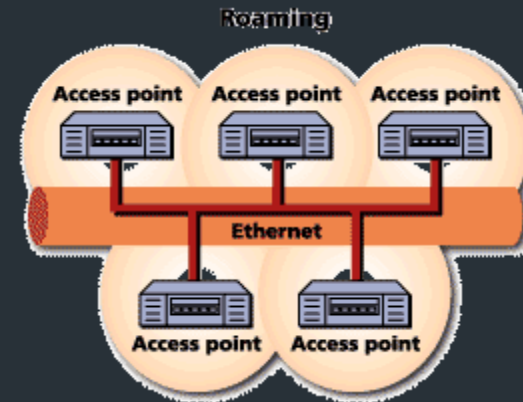
- Wireless Access Points (APs) - a small device that bridges wireless traffic to your network.
- Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.

Integration With Existing Networks



Roaming

- Users maintain a continuous connection as they roam from one physical area to another
- Mobile nodes automatically register with the new access point.
- Methods: DHCP, Mobile IP
- IEEE 802.11 standard does not address roaming, you may need to purchase equipment from one vendor if your users need to roam from one access point to another.



Security

- In theory, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used
- The IEEE 802.11 standard specifies optional security called "**Wired Equivalent Privacy**" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

Interoperability

- Before the IEEE 802.11 interoperability was based on cooperation between vendors.
- IEEE 802.11 only standardizes the physical and medium access control layers.
- Vendors must still work with each other to ensure their IEEE 802.11 implementations interoperate
- Wireless Ethernet Compatibility Alliance (WECA) introduces the Wi-Fi Certification to ensure cross-vendor interoperability of 802.11b solutions

Hardware

- PC Card, either with integral antenna or with external antenna/RF module.
- ISA Card with external antenna connected by cable.
- Handheld terminals
- Access points

Hardware

143



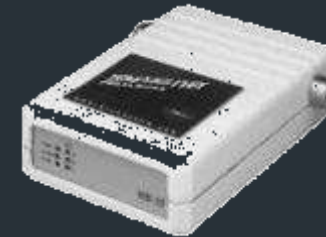
CISCO Aironet 350 series



Wireless Handheld Terminal



Semi Parabolic Antenna



BreezeCOM AP

Performance

- **802.11a** offers speeds with a theoretically maximum rate of 54Mbps in the 5 GHz band
- **802.11b** offers speeds with a theoretically maximum rate of 11Mbps at in the 2.4 GHz spectrum band
- **802.11g** is a new standard for data rates of up to a theoretical maximum of 54 Mbps at 2.4 GHz.

What is 802.11?

- A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE)
- Defines standard for WLANs using the following four technologies
 - Frequency Hopping Spread Spectrum (FHSS)
 - Direct Sequence Spread Spectrum (DSSS)
 - Infrared (IR)
 - Orthogonal Frequency Division Multiplexing (OFDM)
- Versions: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

802.11 - Transmission

- Most wireless LAN products operate in unlicensed radio bands
 - 2.4 GHz is most popular
 - Available in most parts of the world
 - No need for user licensing
- Most wireless LANs use spread-spectrum radio
 - Resistant to interference, secure
 - Two popular methods
 - Frequency Hopping (FH)
 - Direct Sequence (DS)

Frequency Hopping Vs. Direct Sequence

- FH systems use a radio carrier that “hops” from frequency to frequency in a pattern known to both transmitter and receiver
 - Easy to implement
 - Resistance to noise
 - Limited throughput (2-3 Mbps @ 2.4 GHz)
- DS systems use a carrier that remains fixed to a specific frequency band. The data signal is spread onto a much larger range of frequencies (at a much lower power level) using a specific encoding scheme.
 - Much higher throughput than FH (11 Mbps)
 - Better range
 - Less resistant to noise (made up for by redundancy – it transmits at least 10 fully redundant copies of the original signal at the same time)

802.11a

- Employs Orthogonal Frequency Division Multiplexing (OFDM)
 - Offers higher bandwidth than that of 802.11b, DSSS (Direct Sequence Spread Spectrum)
 - 802.11a MAC (Media Access Control) is same as 802.11b
- Operates in the 5 GHz range

802.11a Advantages

- Ultra-high spectrum efficiency
 - 5 GHz band is 300 MHz (vs. 83.5 MHz @ 2.4 GHz)
 - More data can travel over a smaller amount of bandwidth
- High speed
 - Up to 54 Mbps
- Less interference
 - Fewer products using the frequency
 - 2.4 GHz band shared by cordless phones, microwave ovens, Bluetooth, and WLANs

802.11a Disadvantages

- Standards and Interoperability
 - Standard not accepted worldwide
 - No interoperability certification available for 802.11a products
 - Not compatible or interoperable with 802.11b
- Legal issues
 - License-free spectrum in 5 GHz band not available worldwide
- Market
 - Beyond LAN-LAN bridging, there is limited interest for 5 GHz adoption

802.11a Disadvantages

- Cost
 - 2.4 GHz will still has >40% cost advantage
- Range
 - At equivalent power, 5 GHz range will be ~50% of 2.4 GHz
- Power consumption
 - Higher data rates and increased signal require more power
 - OFDM is less power-efficient than DSSS

802.11a Applications

- Building-to-building connections
- Video, audio conferencing/streaming video, and audio
- Large file transfers, such as engineering CAD drawings
- Faster Web access and browsing
- High worker density or high throughput scenarios
 - Numerous PCs running graphics-intensive applications

802.11a Vs. 802.11b

153

802.11a vs. 802.11b	802.11a	802.11b
Raw data rates	Up to 54 Mbps (54, 48, 36, 24, 18, 12 and 6 Mbps)	Up to 11 Mbps (11, 5.5, 2, and 1 Mbps)
Range	50 Meters	100 Meters
Bandwidth	UNII and ISM (5 GHz range)	ISM (2.4000— 2.4835 GHz range)
Modulation	OFDM technology	DSSS technology

802.11g

- 802.11g is a high-speed extension to 802.11b
 - Compatible with 802.11b
 - High speed up to 54 Mbps
 - 2.4 GHz (vs. 802.11a, 5 GHz)
 - Using OFDM for backward compatibility
 - Adaptive Rate Shifting

802.11g Advantages

- Provides higher speeds and higher capacity requirements for applications
 - Wireless Public Access
- Compatible with existing 802.11b standard
- Leverages Worldwide spectrum availability in 2.4 GHz
- Likely to be less costly than 5 GHz alternatives
- Provides easy migration for current users of 802.11b WLANs
 - Delivers backward support for existing 802.11b products
- Provides path to even higher speeds in the future

802.11e Introduces Quality of Service

- Also known as P802.11 TGe
- Purpose:
 - To enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service (QoS)
- Cannot be supported in current chip design
- Requires new radio chips
 - Can do basic QoS in MAC layer

802.11f – Inter Access Point Protocol

- Also known as P802.11 TGf
- Purpose:
 - To develop a set of requirements for Inter-Access Point Protocol (IAPP), including operational and management aspects

802.11b Security Features

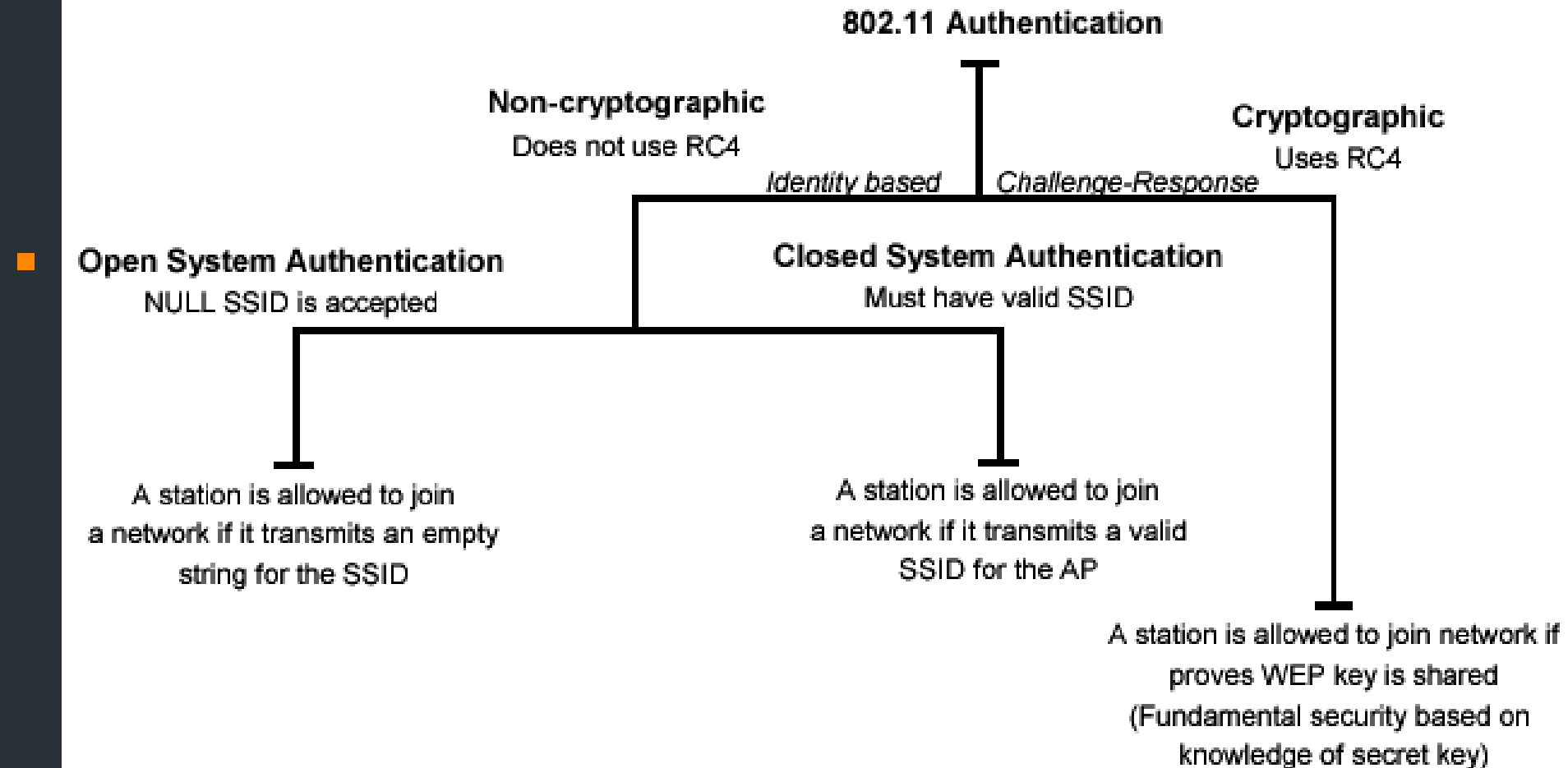
- Wired Equivalent Privacy (**WEP**) – A protocol to protect link-level data during wireless transmission between clients and access points.
- Services:
 - **Authentication**: provides access control to the network by denying access to client stations that fail to authenticate properly.
 - **Confidentiality**: intends to prevent information compromise from casual eavesdropping
 - **Integrity**: prevents messages from being modified while in transit between the wireless client and the access point.

Authentication

Means:

- Based on cryptography
- Non-cryptographic
- Both are identity-based verification mechanisms (devices request access based on the SSID – Service Set Identifier of the wireless network).

Authentication



Privacy

- Cryptographic techniques
- WEP Uses RC4 symmetric key, stream cipher algorithm to generate a pseudo random data sequence. The stream is XORed with the data to be transmitted
- Key sizes: 40bits to 128bits
- Unfortunately, recent attacks have shown that the WEP approach for privacy is vulnerable to certain attack regardless of key size

Data Integrity

- Data integrity is ensured by a simple encrypted version of CRC (Cyclic Redundant Check)
- Also vulnerable to some attacks

Security Problems

- Security features in Wireless products are frequently not enabled.
- Use of static WEP keys (keys are in use for a very long time). WEP does not provide key management.
- Cryptographic keys are short.
- No user authentication occurs – only devices are authenticated. A stolen device can access the network.
- Identity based systems are vulnerable.
- Packet integrity is poor.

Other WLAN Security Mechanisms

- 3Com Dynamic Security Link
- CISCO LEAP - Lightweight Extensible Authentication Protocol
- IEEE 802.1x – Port-Based Network Access Control
- RADIUS Authentication Support
- EAP-MD5
- EAP-TLS
- EAP-TTLS
- PEAP - Protected EAP
- TKIP - Temporal Key Integrity Protocol
- IEEE 802.11i

WLAN Migration – Cutting The Cord

- Essential Questions
- Choosing the Right Technology
- Data Rates
- Access Point Placement and Power
- Antenna Selection and Placement
- Connecting to the Wired LAN
- The Site Survey

Essential Questions

- Why is the organization considering wireless? Allows to clearly define requirements of the WLAN -> development plan
- How many users require mobility?
- What are the applications that will run over the WLAN? Helps to determine bandwidth requirements, a criteria to choose between available technologies. Wireless is a **shared** medium, not switched!!!

Choose the right technology

- Usually IEEE 802.11b or 802.11a
- 802.11b offers interoperability (WECA Wi-Fi Certification Program)
- 802.11a offers higher data rates (up to 54 mbps) -> higher throughput per user. Limited interoperability.

Data rates

- Data rates affect range
- 802.11b 1 to 11 Mbps in 4 increments
- 802.11a 6 to 54 Mbps in 7 increments
- The minimum data rate must be determined at design time
- Selecting only the highest data rate will require a greater number of APs to cover a specific area
- Compromise between data rates and overall system cost

Access Point Placement and Power

- Typically – mounted at ceiling height.
- Between 15 and 25 feet (4.5m to 8m)
- The greater the height, the greater the difficulty to get power to the unit. Solution: consider devices that can be powered using CAT5 Ethernet cable (CISCO Aironet 1200 Series).
- Access points have internal or external antennas

Antenna Selection and Placement

- Permanently attached.
- Remote antennas connected using an antenna cable.
- Coax cable used for RF has a high signal loss, should not be mounted more than a 1 or 2 meters away from the device.
- Placement: consider building construction, ceiling height, obstacles, and aesthetics. Different materials (cement, steel) have different radio propagation characteristics.

Connecting to the Wired LAN

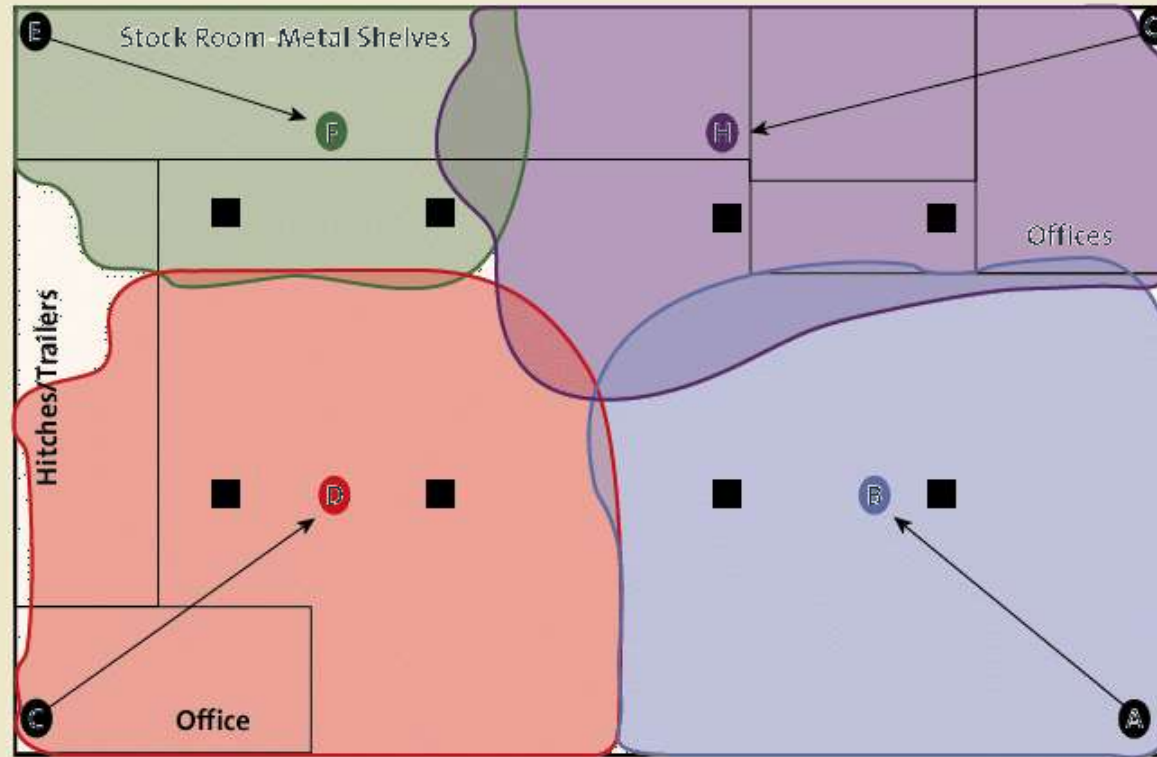
- Consider user mobility
- If users move between subnets, there are challenges to consider.
- OSes like Windows XP and 2000, Linux support DHCP to obtain the new IP address for the subnet. Certain applications such as VPN will fail.
- Solution: access points in a roaming area are on the same segment.

The Site Survey

- Helps define the coverage areas, data rates, the precise placement of access point.
- Gather information: diagramming the coverage area and measuring the signal strength, SNR (signal to noise ratio), RF interference levels

Site Survey

"OUTSIDE IN" SURVEY METHOD—EXAMPLE



Vendor Information

- **CISCO Systems Wireless**
<http://www.cisco.com/warp/public/44/jump/wireless.shtml>
- **3Com Wireless**
http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=13&selcat=Wireless+Products
- **Breeze Wireless Communications**
<http://www.breezecom.com>
- **Lucent Technologies**
<http://www.wavelan.com>
- **Symbol Technologies** <http://www.symbol.com>

References

- CISCO Packet Magazine, 2nd Quarter 2002
http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac168/about_cisco_packet_issue_home.html
- 3Com University – Wireless LANs A Technology Overview
www.3com.com/3comu
- National Institute of Standards and Technology Wireless Network Security <http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>