



Computer Network

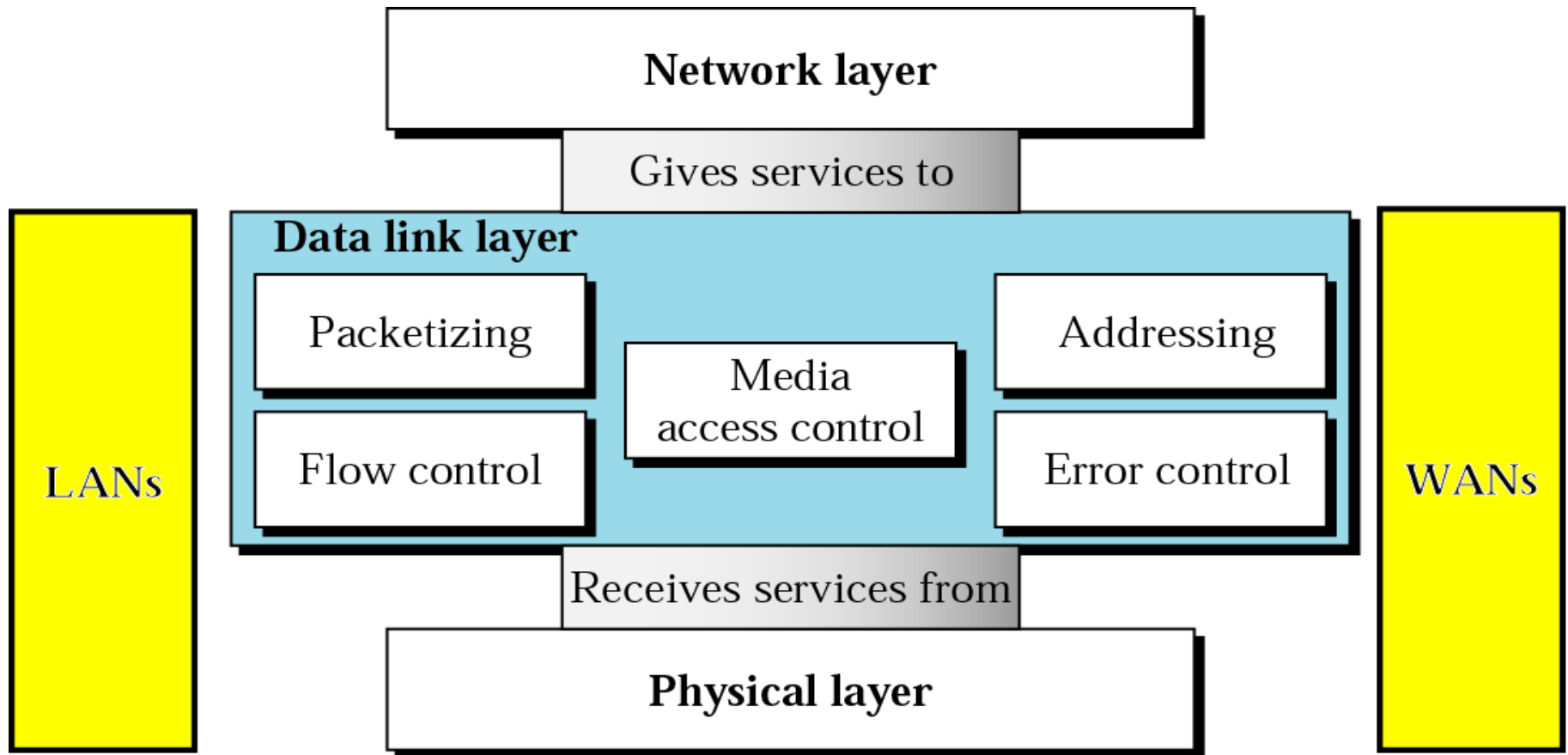
Chapter 4: Data Link Layer



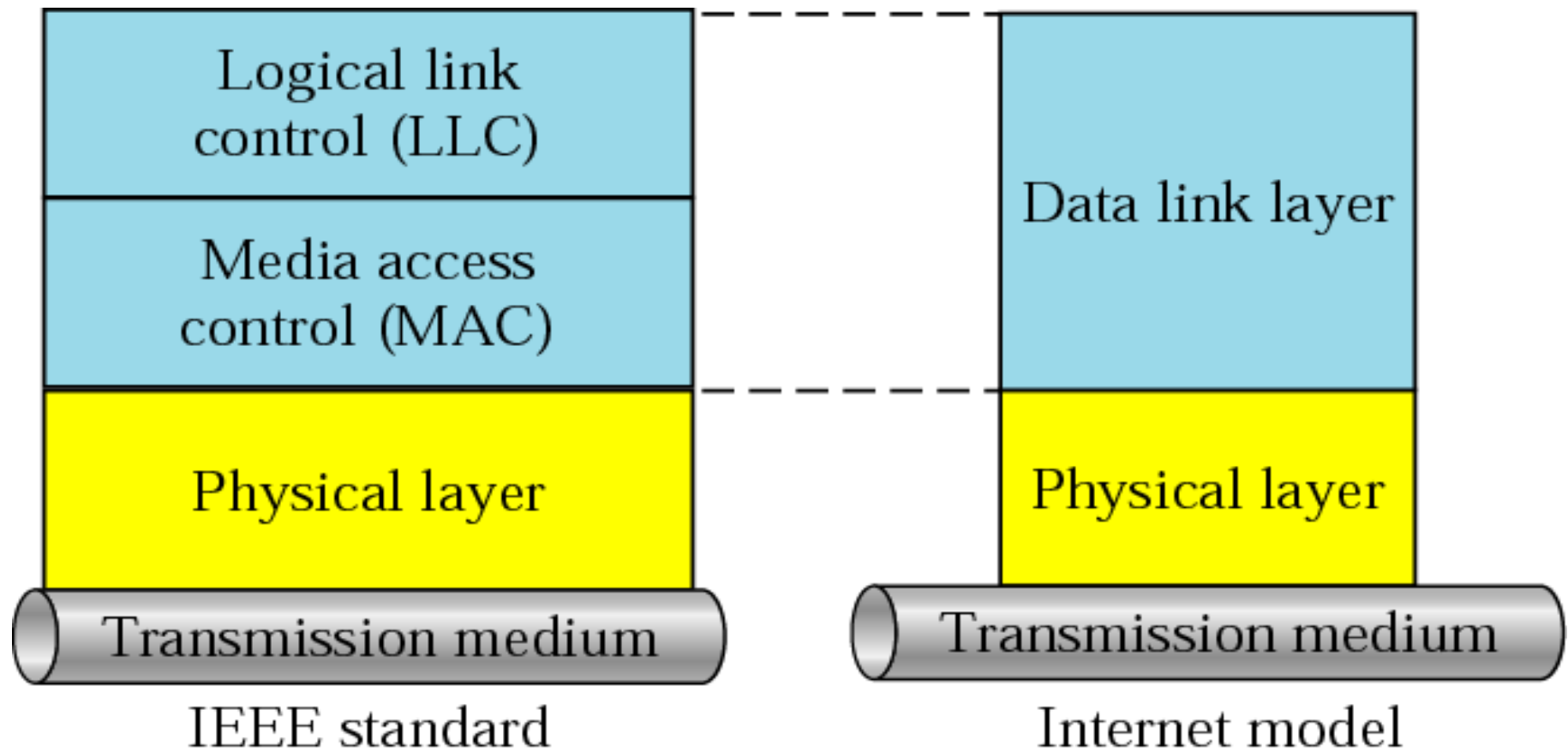
Data Link Layer

- Data link layer is layer 2 in OSI Model
- In the TCP/IP reference model, it is part of the link layer
- Examples
 - Ethernet, Point-to-Point Protocol (PPP), HDLC, ATM,
 - Frame Relay
- concerned with local delivery of frames between devices on the same LAN/WAN

Data Link Layer: Position



LLC and MAC SubLayer Overview





DataLink Layer: LLC

- Logic Link Control
- Define by IEEE 802.2 Standard
- Multiplexes protocols running at Layer 3 (IP, IPX, IPV4, IPV6)
- LLC provides flow control, acknowledgment, and error Notification for L3 Protocols.
- The LLC sublayer acts as an interface between the media access control (MAC) sublayer and the network layer



Media Access Control

- Provides addressing and channel access control mechanisms
- Functions performed in the MAC sublayer
 - End Devices Addressing Mechanism
 - Using physical address
- Channel access control mechanism
 - CSMA/CD, CSMA/CA
- multiple access protocol is not required in a switched full-duplex network

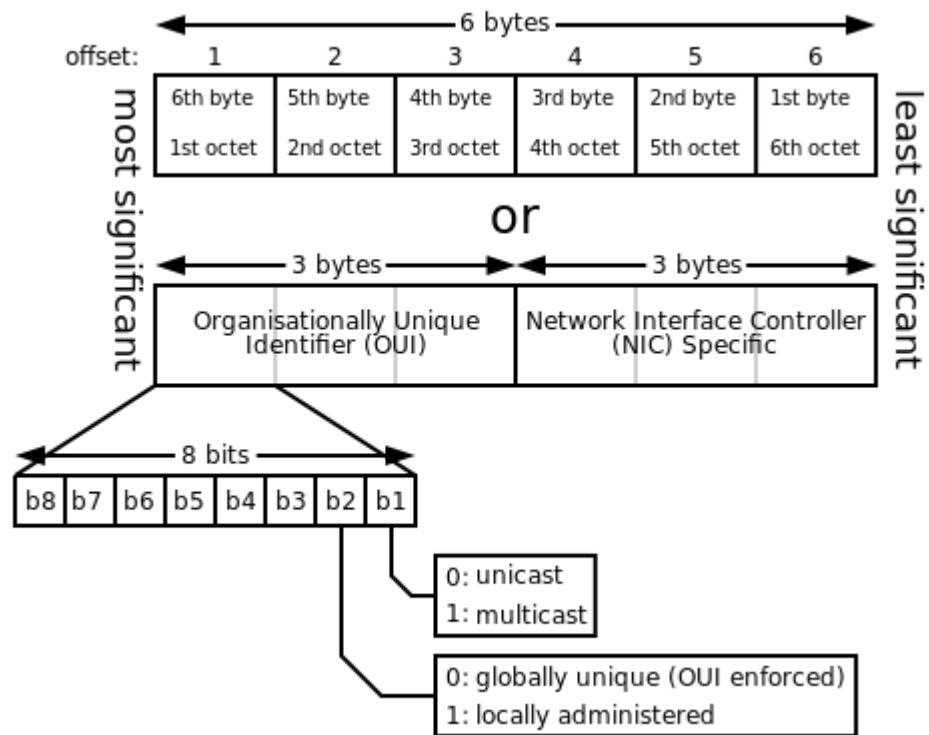


Physical(MAC) addressing Overview

- Unique identifier assigned to network interfaces controllers(NIC)
- Also called Physical Address OR Hardware Address
- 48-bit address
- Represented in Hexadecimal number
- Example
 - 01:23:45:67:89:ab
 - Upper 3 bytes represents the OUI (Organization Unique Identifier) also called Manufacturer ID

MAC cont'd..

- Lower 3 bytes represent the Device ID



Framing ?? Types of Framing

- **Frame**
 - Frame is a data on the Layer 2 of the OSI model
 - Small data Units
 - Created By Data Link Layer
 - The Process Of Creating Frames By The Data Link Layer Is Known As **Framing**.
- **Examples of Frames**
 - Ethernet Frames
 - PPP Frames (Byte oriented Framing)
 - HDLC Frame (bit oriented Framing)



Types of Framing

- Framing
 - Fixed size Framing
 - Variable size Framing
- Fixed size Framing
 - Have Fixed Length
 - No need to define boundaries for Frames
 - Examples
 - ATM Frames (54 byte cells)

Types of Framing Cont'd..

- Variable Size Framing
 - Not Fixed Size
 - Need a way to define the end of the frame and the beginning of the next frame
 - Different Types of Variable Size Framing
 - 1.Character Oriented Framing / Byte oriented Framing
 - 2.Bit Oriented Framing
 - 3.Character Stuffing Framing
 - 4.Bit Stuffing Framing
 - 5.Character Counting
 - 6.Clock Based Framing
 - 7.Physical layer Code Voilations

Character Oriented Framing

- Also called **Byte Oriented Framing**
- Data to be carried are 8-bit characters from a coding
- To separate one frame from the next, an **8-bit (I-byte) flag** is added at the beginning and the end of a frame
- Differentiates one byte from another.
- older style of framing
- used in the terminal/mainframe environment
- Examples of byte-oriented framing include IBM's BISYNC(Binary
- synchronous Communication) protocol



Bit Oriented Framing

- Allows the sender to transmit a long string of bits at one time.
- IBM's SDLC (Synchronous Data Link Control) and HDLC (High-level Data Link Control) are examples of bit-oriented protocols.
- Most LANs use bit-oriented framing.
- There is usually a maximum frame size. For example, Ethernet has a
- maximum frame size of 1,526 bytes.



Character stuffing Framing

- Each frame starts with the ASCII character sequence DLE STX
 - **DLE**: Data Link Escape
 - **STX**: Start of TeXt
- Ends with the sequence DLE ETX
 - **DLE**: Data Link Escape
 - **STE**: End of TeXt

Bit Stuffing Framing

- At the start and end of each frame is a flag byte consisting of the special bit pattern **01111110**
- whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called **bit stuffing**
- When the receiver sees five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically **destuffs** the 0 bit.
- The boundary between two frames can be determined by locating the flag pattern



Character Counting

- This method uses a field in the header to specify the **number of characters** in the frame
- Destination sees the character count, it knows **how many characters follow**, destination sees the character count, it knows how many characters follow
- **Disadvantages**
 - Garbled by a transmission error
 - Destination will lose synchronization and will be unable to locate the start of the next frame. So, this method is rarely used



Physical layer coding violations Framing

- 1 bit is a high-low pair and a 0 bit is a low-high pair is used to Indicate the start and end of frame



Clock Based Framing

- repetitive pulses are used to maintain a constant bit rate
- Examples
 - SONET



Flow Control and Error Control At Data Link Layer

- Flow Control
 - Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.
- Error Control
 - Error control in the data link layer is based on automatic repeat request, which is the retransmission of data
 - Error control includes both error detection and error correction
 - Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted



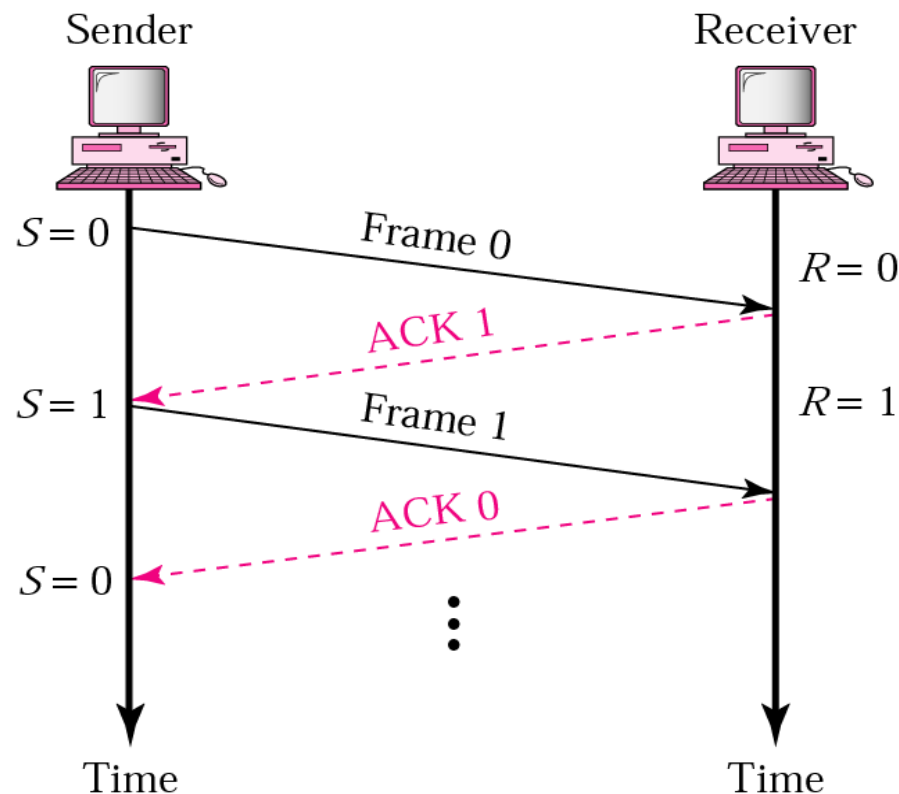
Error and Flow Control Mechanism

- Stop and Wait
- Go-back-N
- Selective Repeat Request

Stop and Wait:

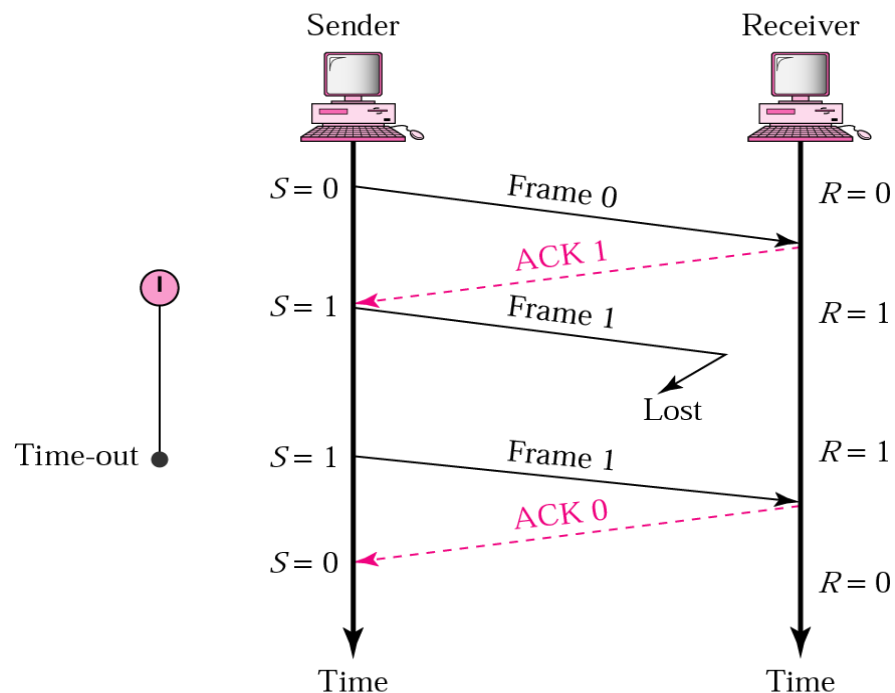
- If data frames arrive at the receiver site faster than they can be processed,
 - the frames must be stored until their use
 - Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources.
 - This may result in either the discarding of frames or denial of service.
 - To prevent the receiver from becoming over-whelmed with frames, we somehow need to tell the sender to slow down.
(Stop to transmit and wait for Receiver acknowledgement signals)

Stop and Wait: Normal Operation



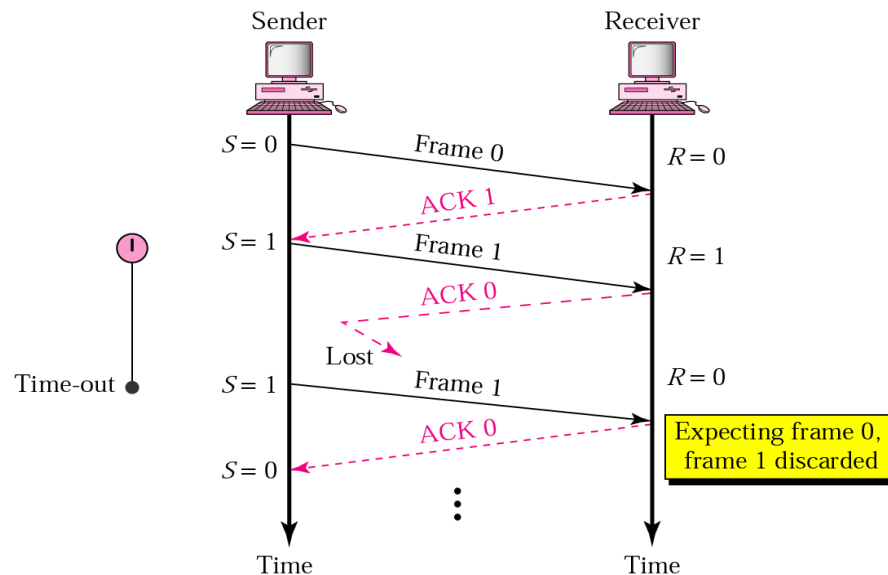
- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control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



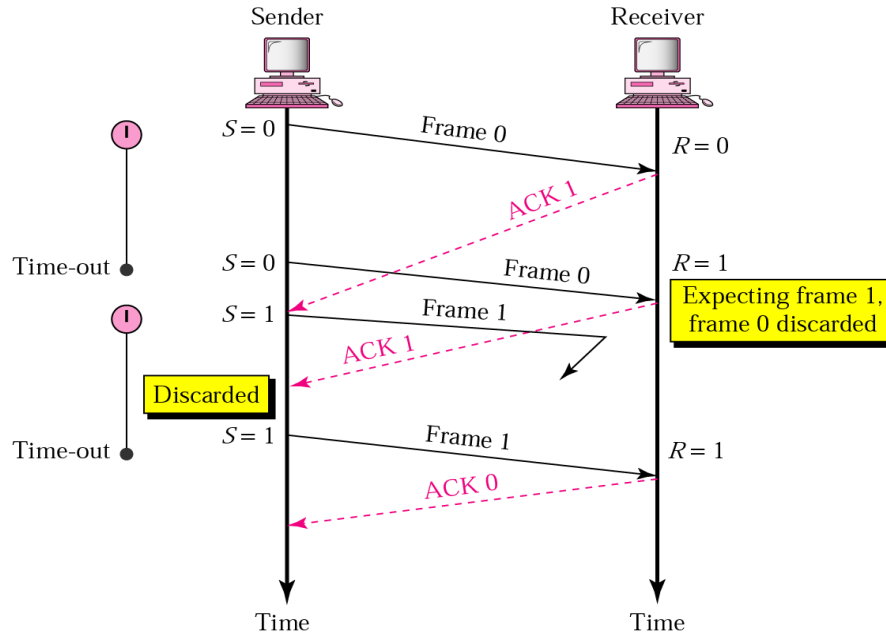
- When a receiver receives a damaged frame, it discards it and keeps its value of R .
- After the timer at the sender expires, another copy of frame 1 is sent.

Stop and wait Lost ACK



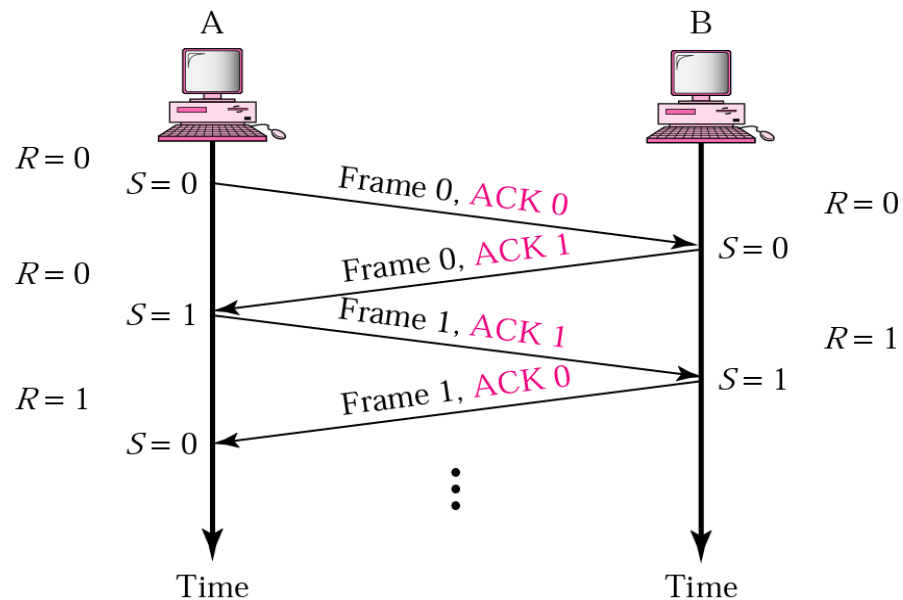
- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 ($R=0$). Therefore it discards the second copy of frame 1.

Stop-and-Wait ARQ, delayed ACK



- 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, $R = 1$ means receiver expects to see frame 1. 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



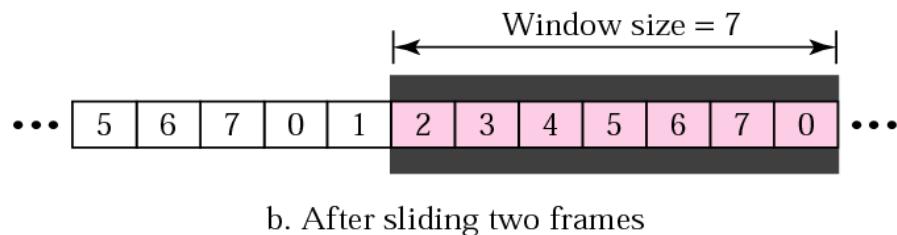
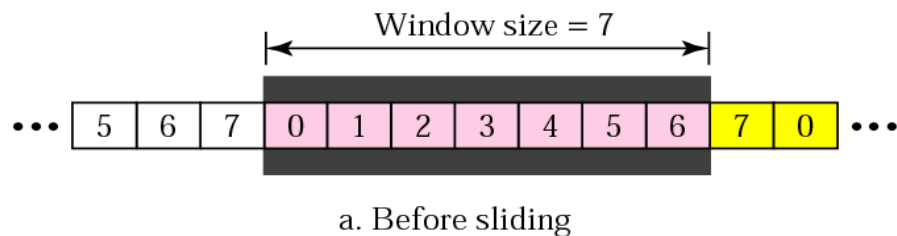
Go-Back-N ARQ

- We can send up to W frames before worrying about ACKs.
 - i.e Sending W Frames before Receiving ACKs Signals
- We keep a copy of these frames until the ACKs arrive.
- This procedure requires additional features to be added to Stop-and-Wait ARQ.
- Use Sequence Numbering Techniques to track the Frames
- It can send one cumulative acknowledgment for several frames

Sequence Number

- 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 for sequence number, the sequence numbers range from 0 to $2^m - 1$.
for $m = 3$, sequence numbers are: 0, 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, ...

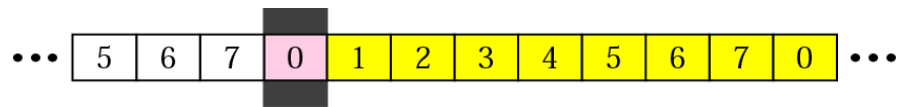
Go-Back-N ARQ: Sender sliding window



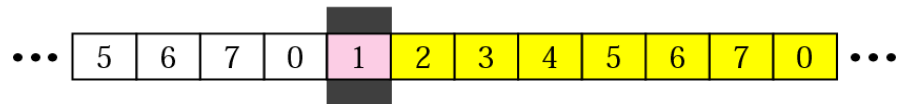
- Sliding window Define the range of Sequences Number
- Here Sender Sliding window define the window size=7
- Total Number of Frames that can be sent without receiving ACKs is 7

Receiver sliding window

- Size of the window at the receiving site is always 1 in this protocol.

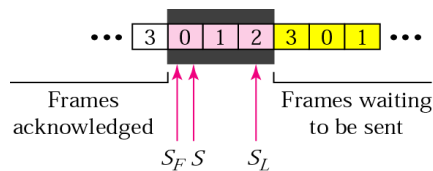


a. Before sliding

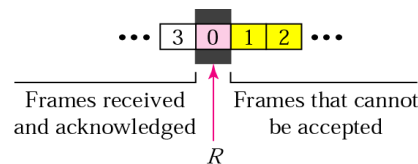


b. After sliding

Control Variables



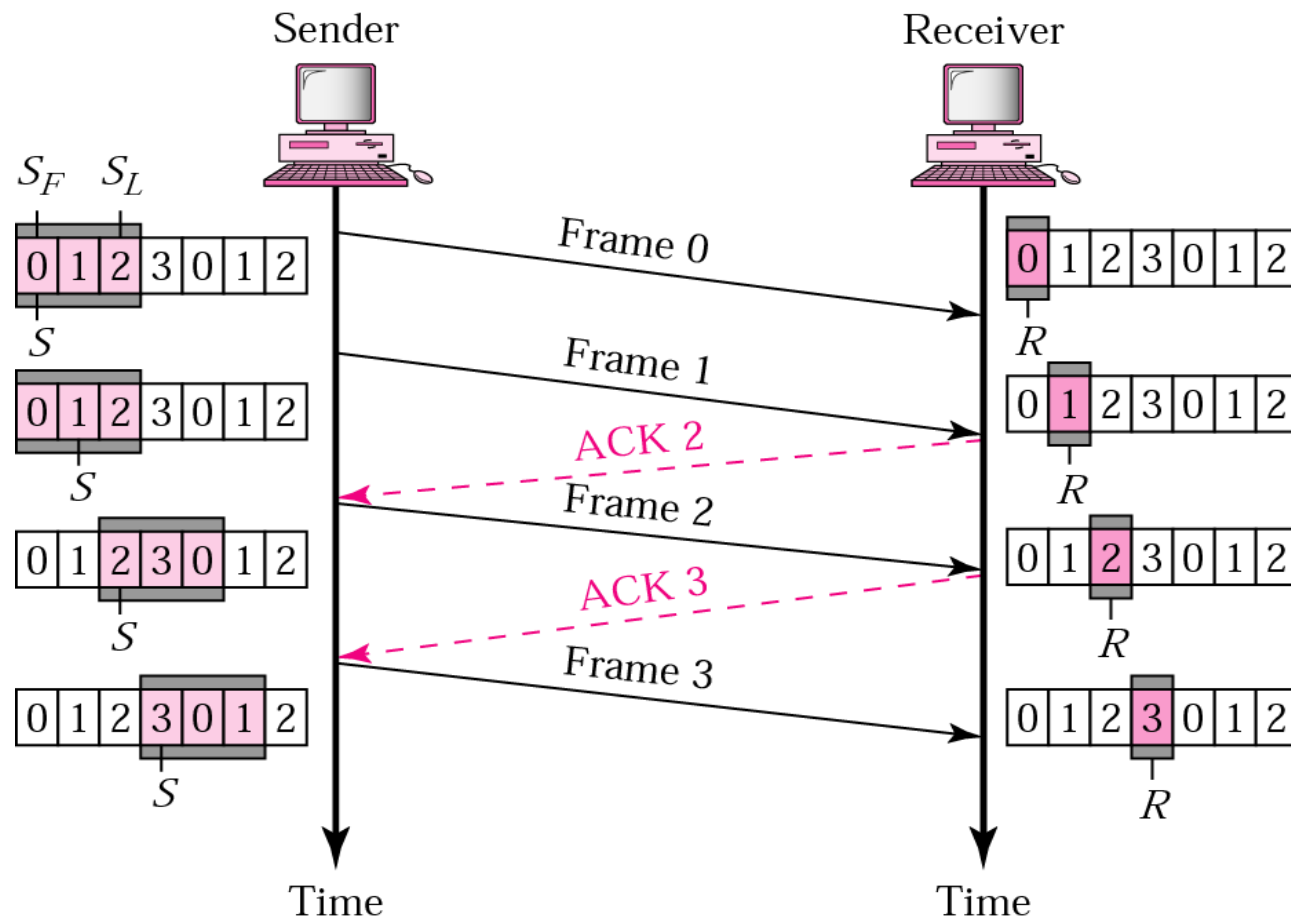
a. Sender window



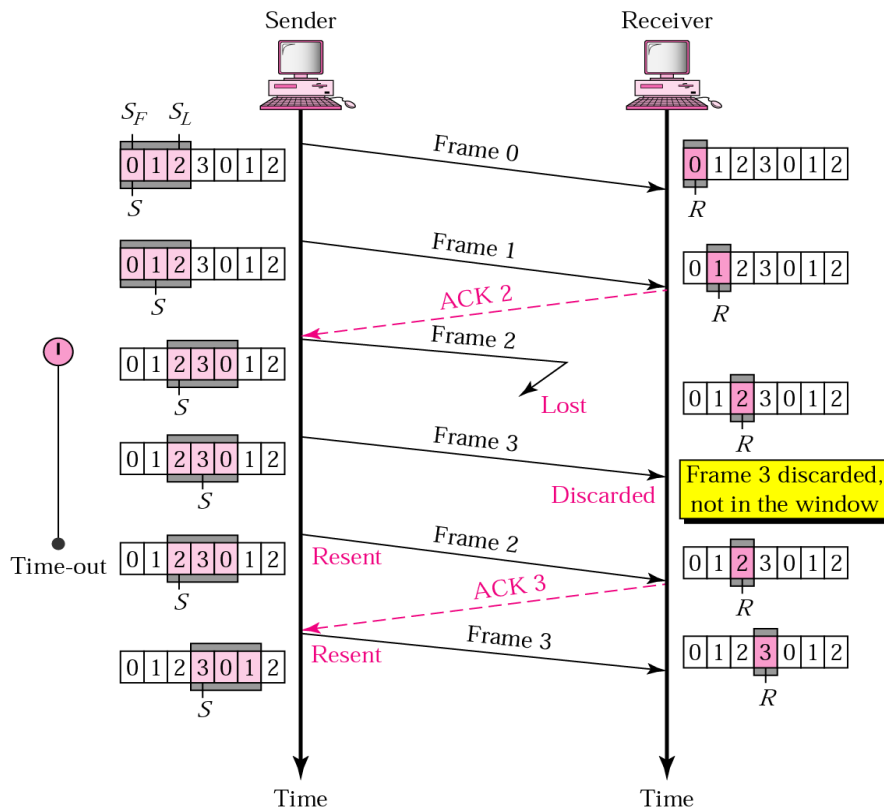
b. Receiver window

- 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.

Go-Back-N ARQ, normal operation



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

Note:

In Go-Back-N ARQ, the size of the sender window must be less than 2^m ; the size of the receiver window is **always 1**.

Go-Back-N ARQ Versus Stop-and- Wait ARQ ??

- Stop-and-WaitARQ Protocol is actually a Go-Back-N ARQ
 - When $m=1$ for 2^m-1
- Sender window Size differentiate Go-Back-N ARQ and Stop-and- Wait ARQ

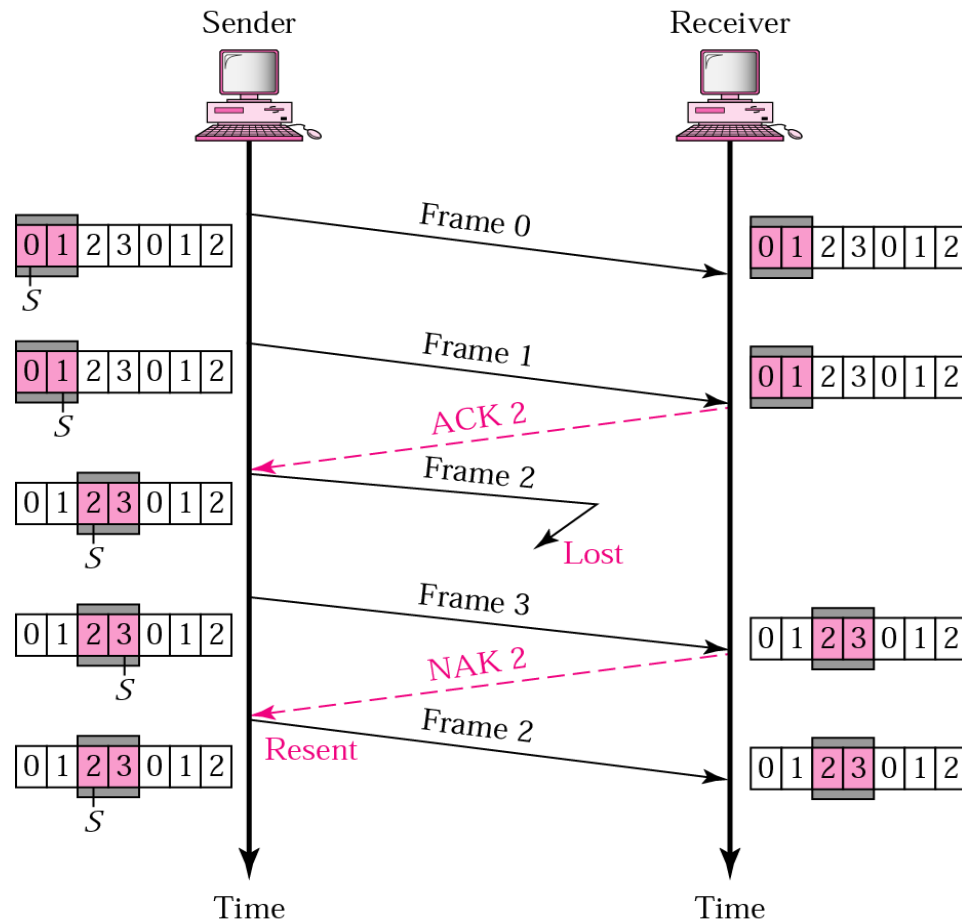
Selective Repeat Request

- This mechanism is called Selective Repeat ARQ.
- It is more efficient for **noisy links**
- The Selective Repeat Protocol also uses two windows: a **send window** and a **receive window**
- Size of The Same window and Receive window are Same
 - $s=2^{(m-1)}$, for $m=4$, $s=8$
- It is 15 in the **Go-Back-N Protocol**
- The Selective Repeat Protocol allows as many frames as the size of the receive window to **arrive out of order** and be kept until there is a set of in-order frames to be delivered to the network layer.

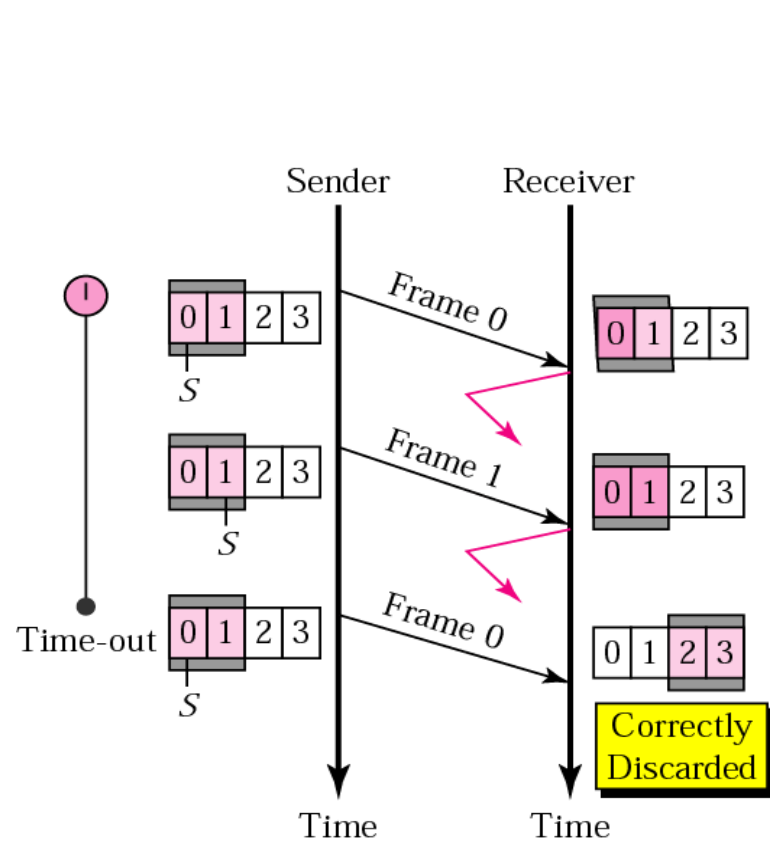
Window Size of Selective Repeat Request

- The size of the sender and receiver windows must be at most one-half of 2^m
- For an example, we choose $m = 2$,
 - The size of the window is $2^m / 2$, or 2
- Next Slide compares a window size of 2 with a window size of 3.

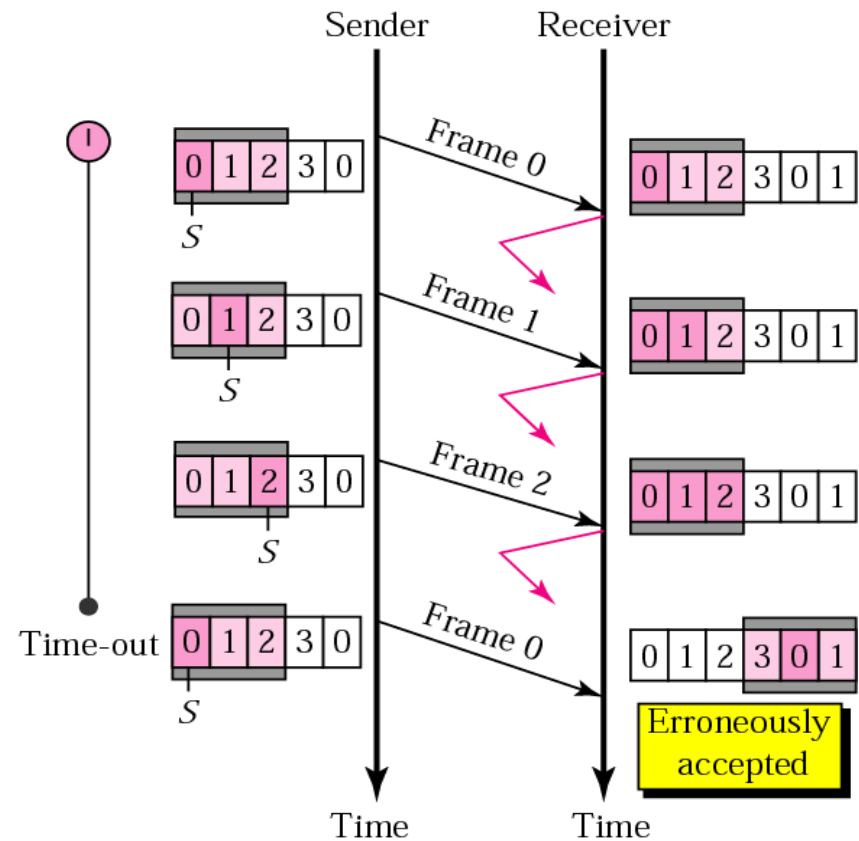
Selective Repeat Request: Lost Frame



Selective Repeat Request for different Window size



a. Window size = 2^{m-1}



b. Window size > 2^{m-1}

Selective Repeat Request cont'd..

- For an example, we choose $m = 2$, which means the size of the window is $2^m / 2$, or 2.
- Slide No.39 compares a window size of 2 with a window size of 3.
- If the size of the window is 2 and all acknowledgments are lost, the timer for frame 0 expires and frame 0 is resent. However, the window of the receiver is now expecting frame 2, not frame 0, so this duplicate frame is correctly discarded

Selective Repeat Request cont'd..

- When the size of the window is 3 and all acknowledgments are lost, the sender sends a duplicate of frame 0. However, this time, the window of the receiver expects to receive frame 0 (0 is part of the window), so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is clearly an error



Note: In Selective Repeat ARQ, the size of the sender and receiver window must be at most one-half of 2^m .



Error Control Mechanism

- Error Detection
 - Parity Check
 - CRC (Cyclic Redundancy Check)
 - CheckSum
- Error Correction
 - Hamming Code

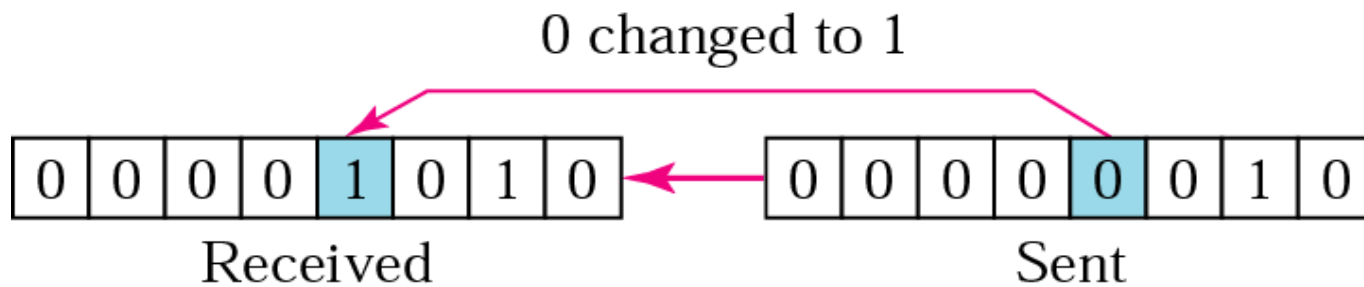


Error:

- Whenever bits flow from one point to another
 - subject to unpredictable changes because of interference
 - Changes in bits results in Error
- Types of Error
 - Single Bit Error
 - Burst Error

Single Bit Error

- Occours when Single bit Changes
 - from 1 to 0 or from 0 to 1.

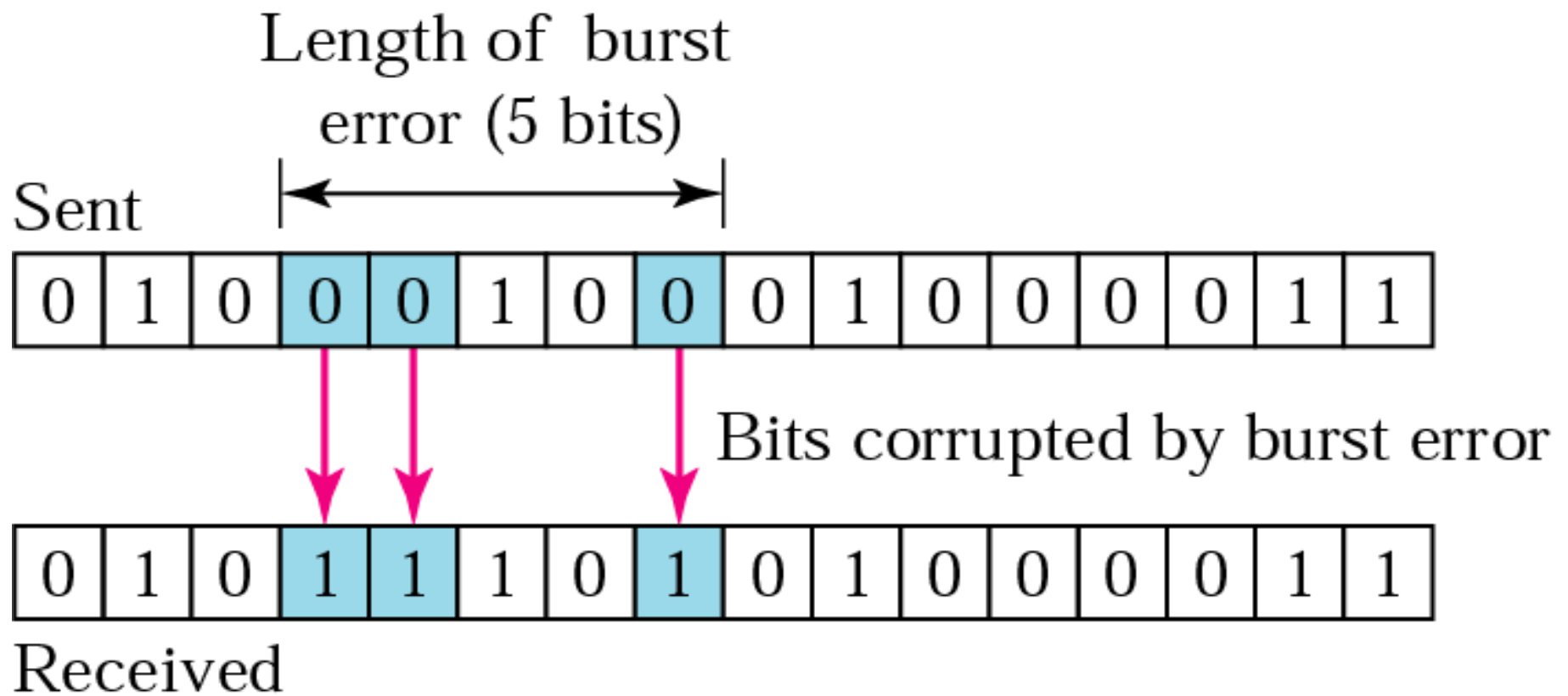




Burst Error

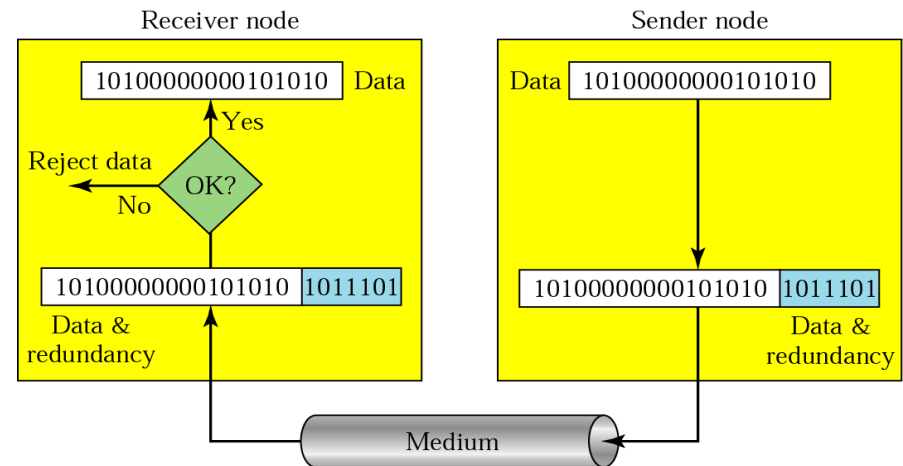
- 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.
- Burst error is more likely to occur than a single-bit error

Burst Error

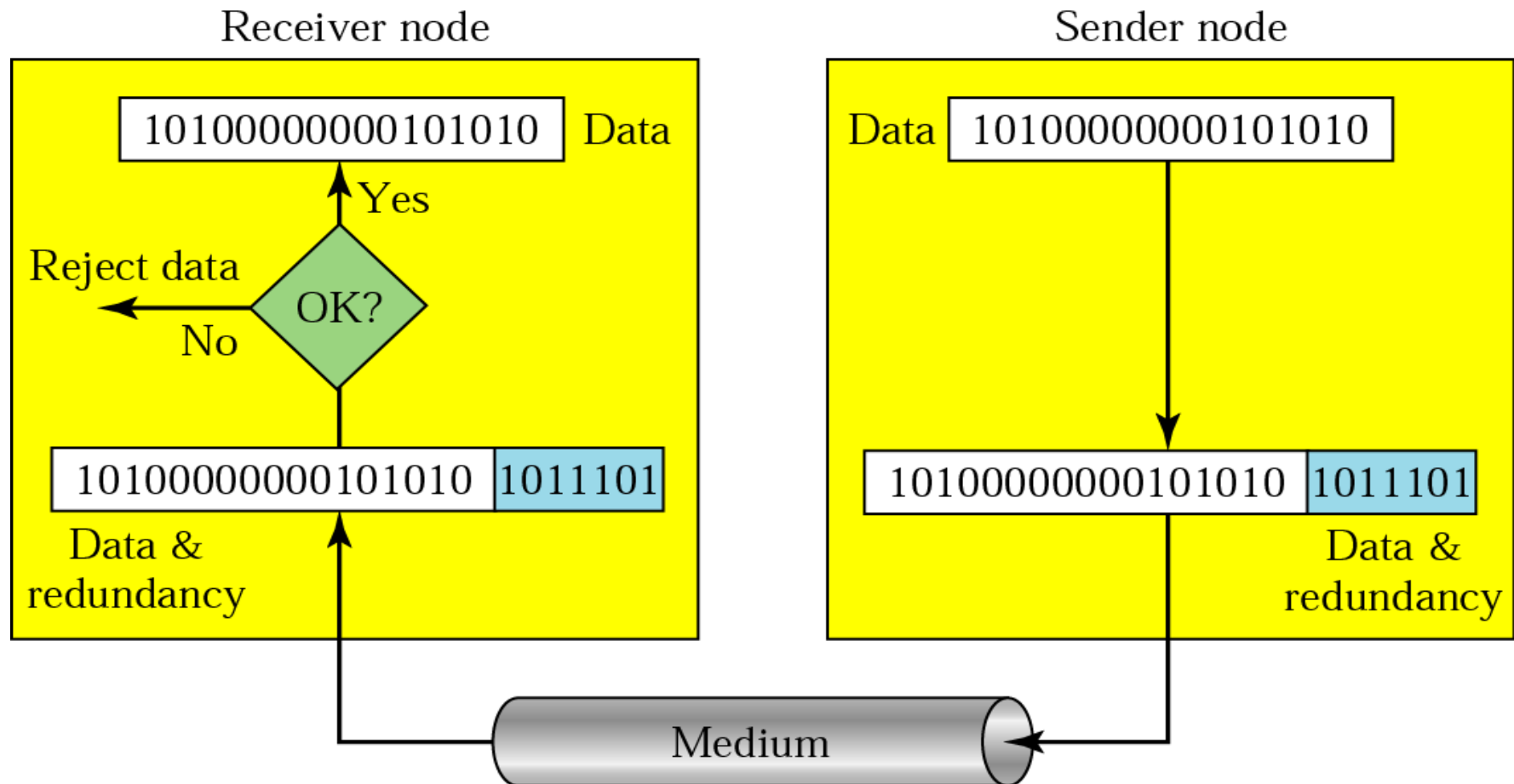


Error Detection Method

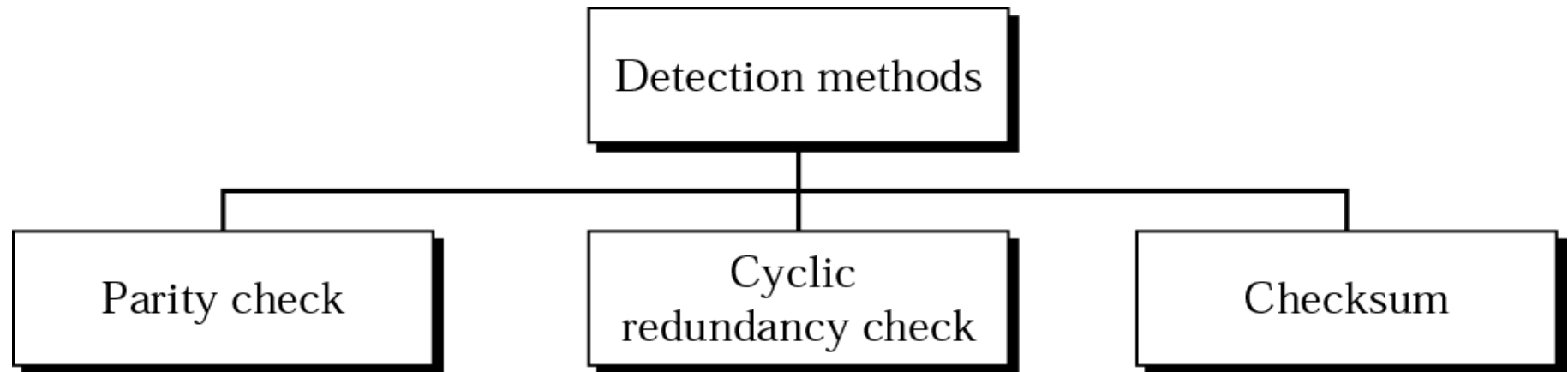
- Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.
- Redundancy bits are generated by making some relation with data bits
 - Examples
 - CRC
 - Parity Check
 - CheckSum



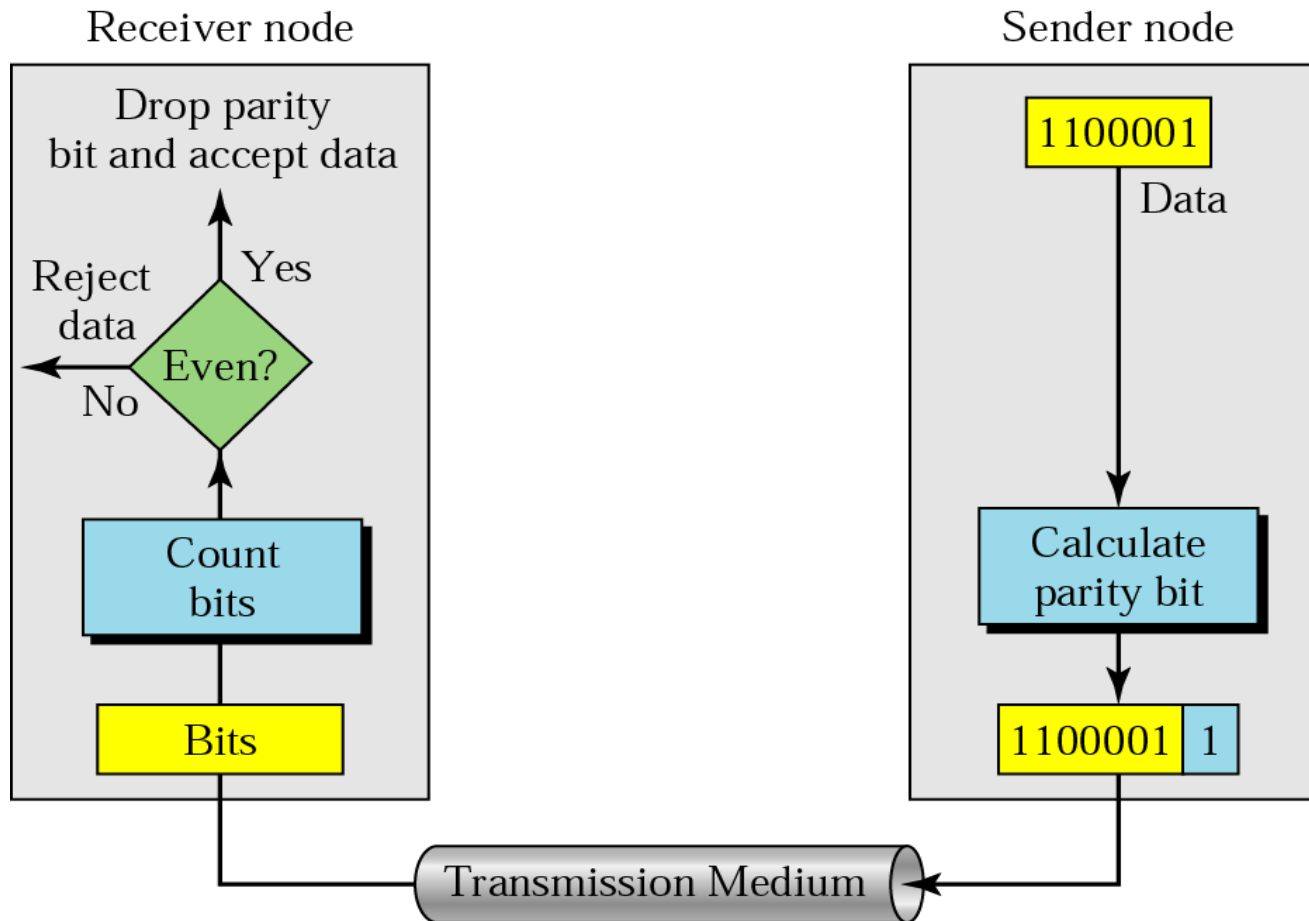
Redundancy Cont'd..



Detection Method by Redundancy



Parity Check: Even Parity





Parity Check: Odd Parity ??

- **Note:** In parity check, a **parity bit is added** to every data unit so that the total number of 1s is even (or odd for odd-parity).
- **ODD Parity:** **Classwork**



Note:

Simple parity check can detect all single-bit errors. It can detect burst errors only if the total number of errors in each data unit is odd.

Example 2

Now suppose the word world in Example 1 is received by the receiver without being corrupted in transmission.

11101110 11011110 11100100 11011000 11001001

The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.

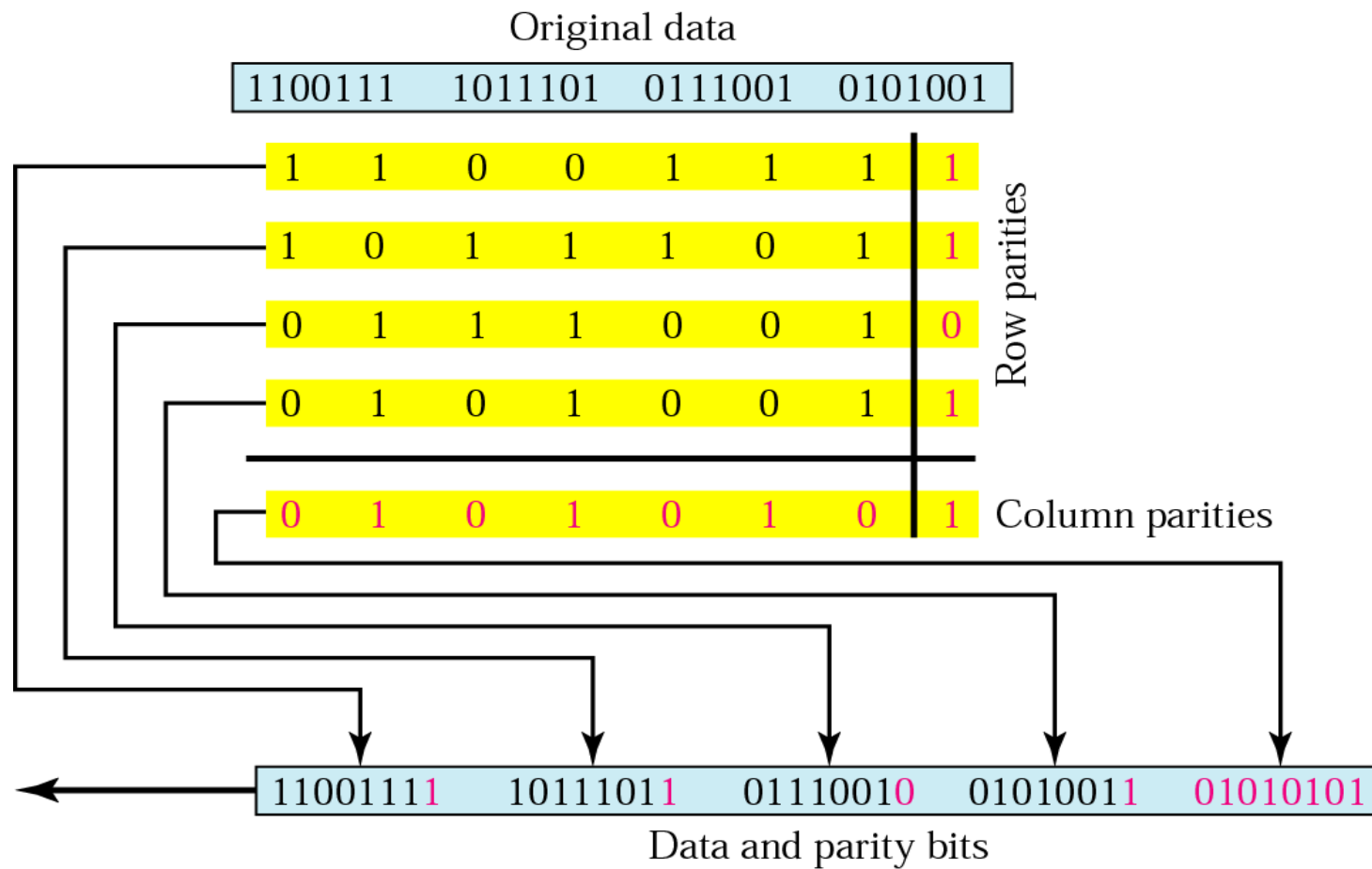
Example 3

Now suppose the word world in Example 1 is corrupted during transmission.

11111110 11011110 11101100 11011000 11001001

The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4, 4). The receiver knows that the data are corrupted, discards them, and asks for retransmission.

Two Dimensional Parity Check





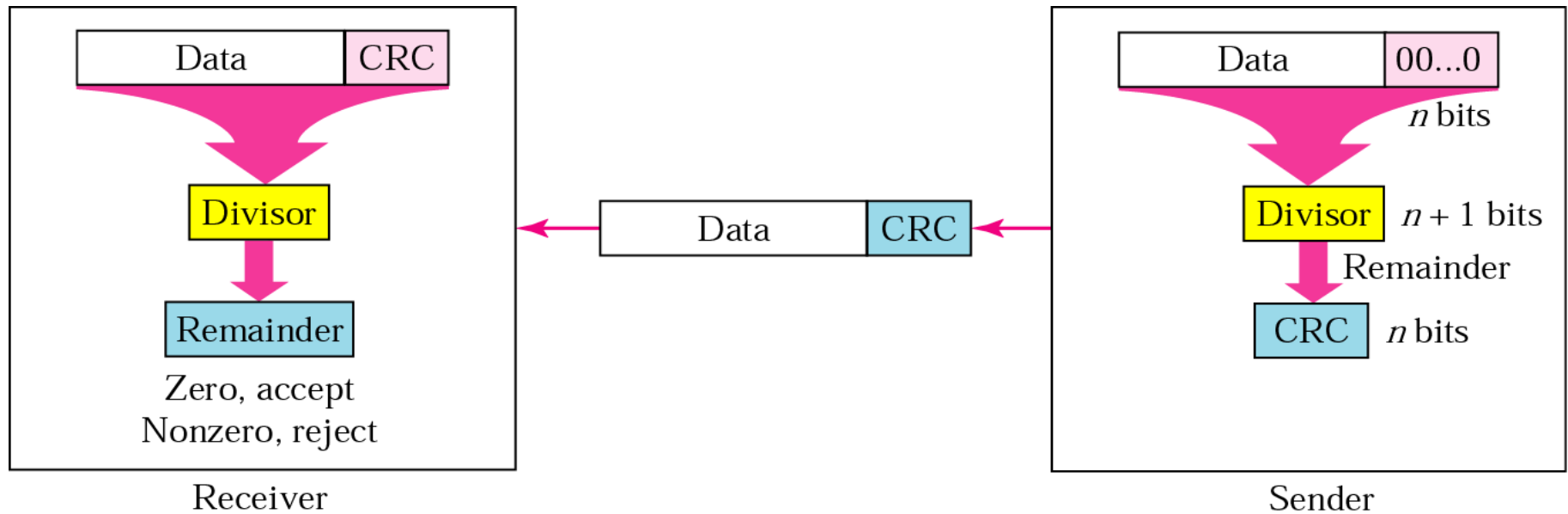
Two Dimensional parity Check

Two Dimensional Parity Check can detect Burst Errors

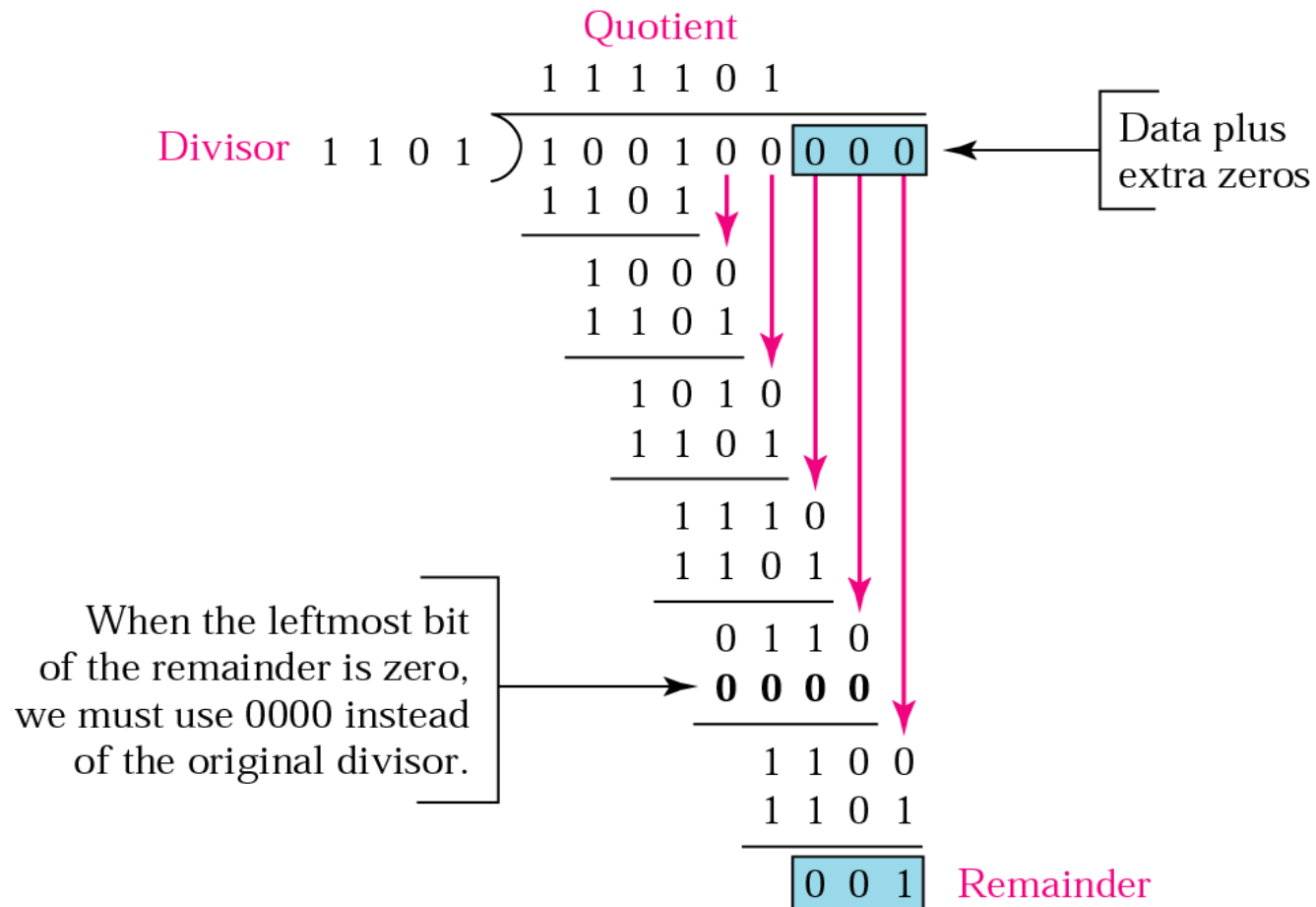
CRC: Cyclic redundancy Check

- 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.

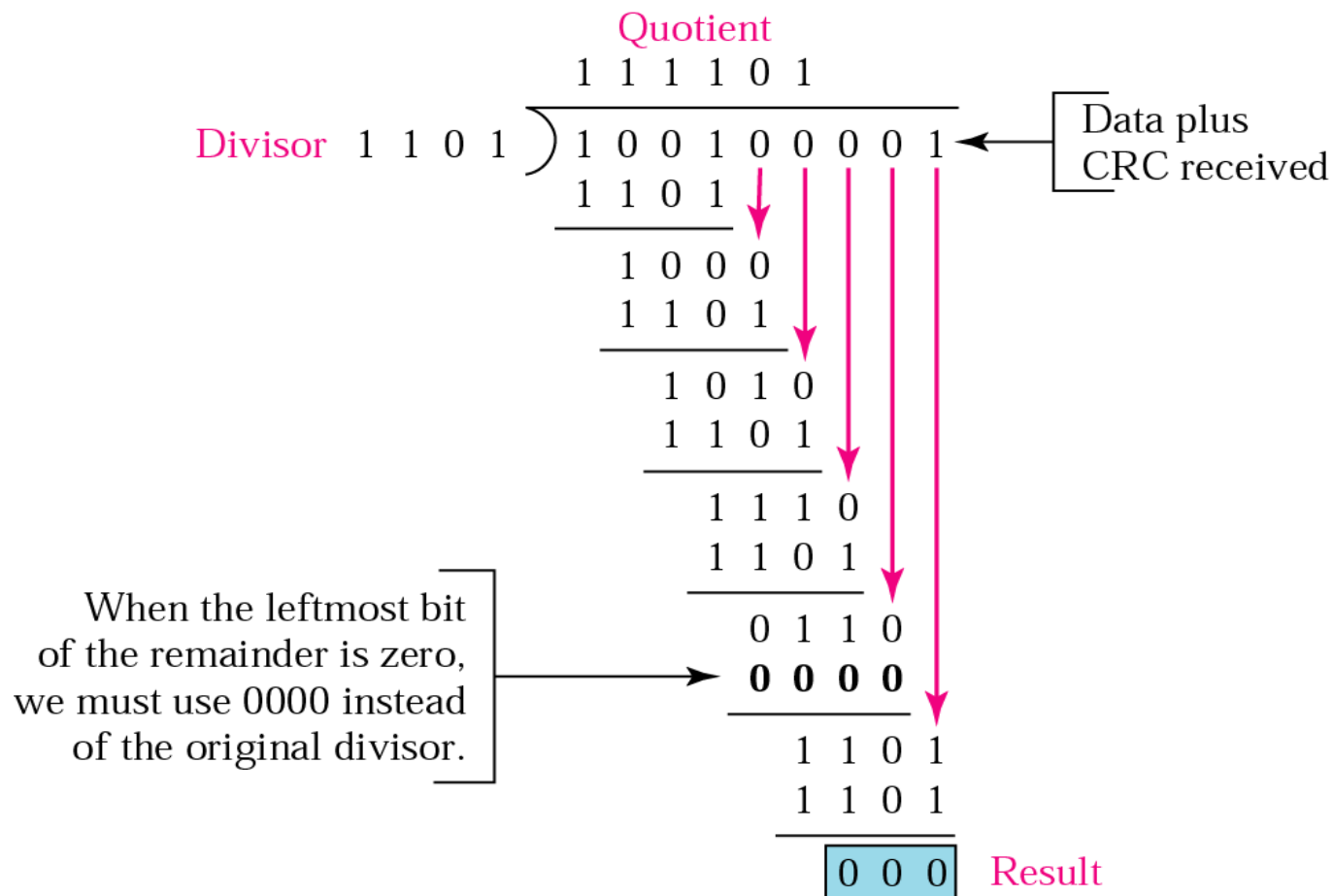
CRC: Cyclic Redundancy Check



CRC Encoding



CRC Decoding





Error Detection: CRC

NOTE:

- 000 Remainder Indicates of No errors in Data during Transmission

Polynomial For CRC

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

Polynomial Representing Standard Divisor

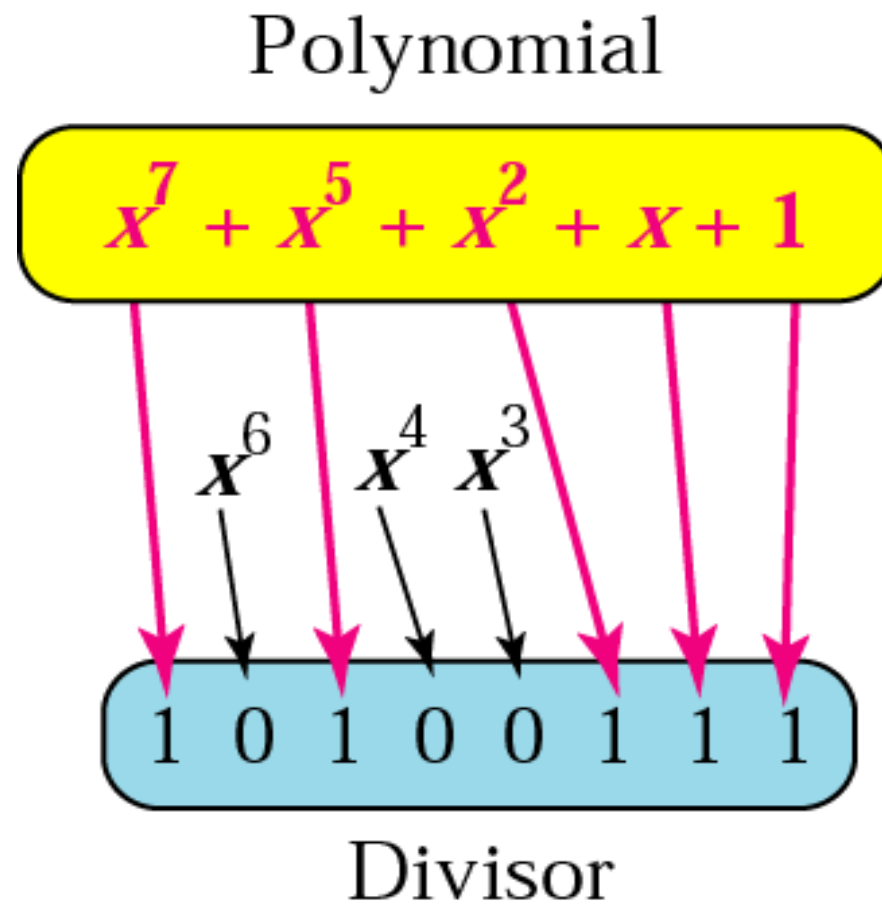
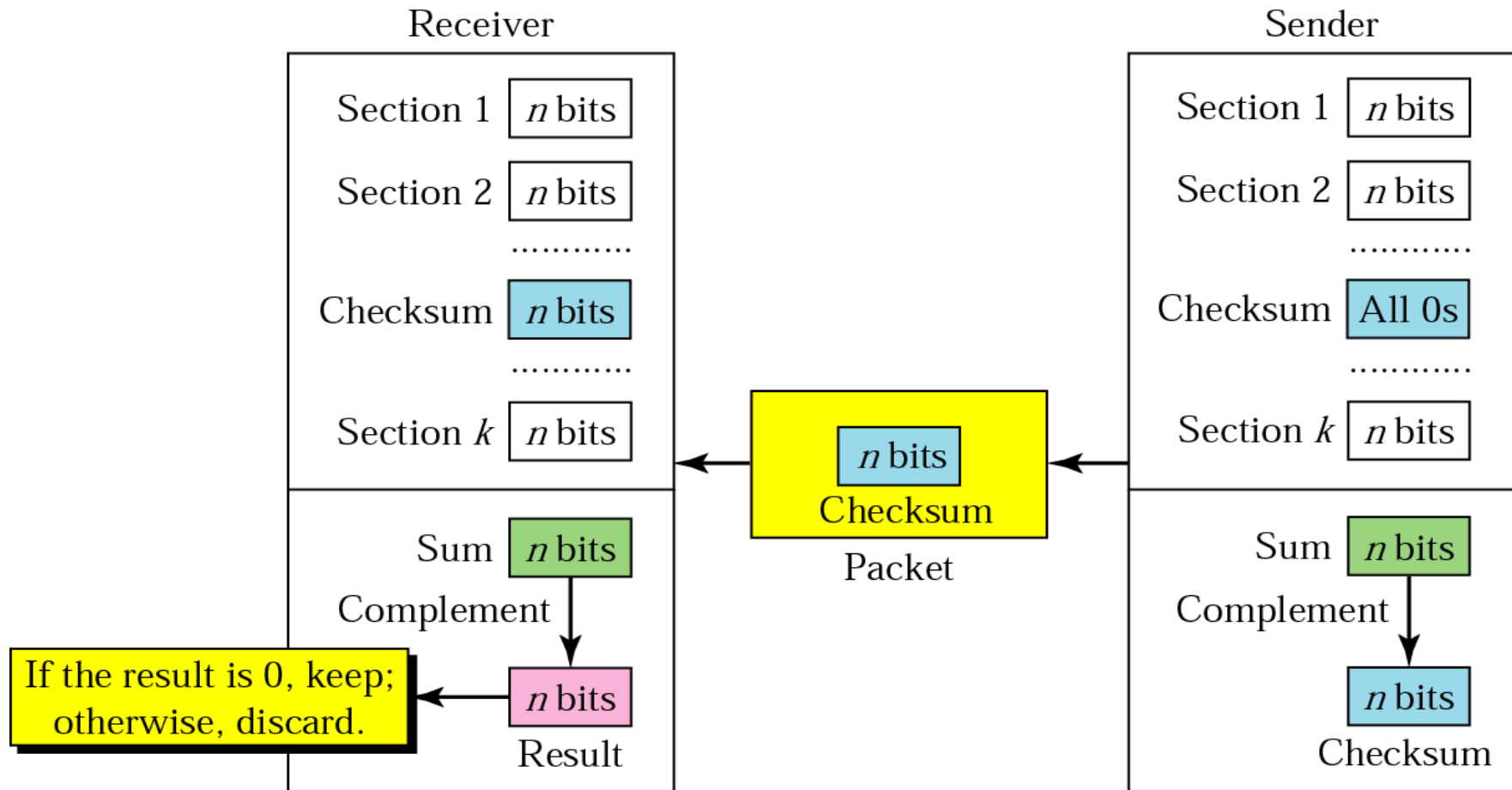


Table 10.1 Standard polynomials

Name	Polynomial	Application
CRC-8	$x^8 + x^2 + x + 1$	ATM header
CRC-10	$x^{10} + x^9 + x^5 + x^4 + x^2 + 1$	ATM AAL
ITU-16	$x^{16} + x^{12} + x^5 + 1$	HDLC
ITU-32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8$ $+ x^7 + x^5 + x^4 + x^2 + x + 1$	LANs

Checksum



Checksum Example: Sender Side

- Suppose the block of 16 bits is to be sent using a checksum of 8 bits.
[10101001 00111001]
- Two 8 Bit Numbers are added.
 $10101001 + 00111001 = 11100010$
- One's Complement of 11100010 = 00011101
- The Pattern Sent is
10101001 00111001 00011101

Checksum Example: Receiver Side

- The Received data along with checksum is added

10101001

00111001

00011101

11111111

- Compute One's Complement of 11111111 = 00000000
- No Error in Transmission.



Error Correction

- Error Correction By Retransmission
 - ✓ Stop AND Wait ARQ
 - ✓ Go-Back-N ARQ
 - ✓ Selective Repeat ARQ
- ARQ => Automatic Repeat Request
- Error Correction By Forward Error Control
 - ✓ Hamming Code




Error Correction Code: Hamming Code

- Error Correcting Codes
- designed with $d_{\min} = 3$
- d_{\min} =Minimum Hamming Distance
- The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words



Hamming Code cont'd..

- Find the minimum Hamming distance of the coding scheme $d(00000, 01011)$



Number of data bits m	Number of redundancy bits r	Total bits m + r
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

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

Positions of redundancy bits in Hamming code

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

Redundancy bits calculation

r_1 will take care of these bits.

11		9		7		5		3		1
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

r_2 will take care of these bits.

11	10			7	6			3	2	
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

r_4 will take care of these bits.

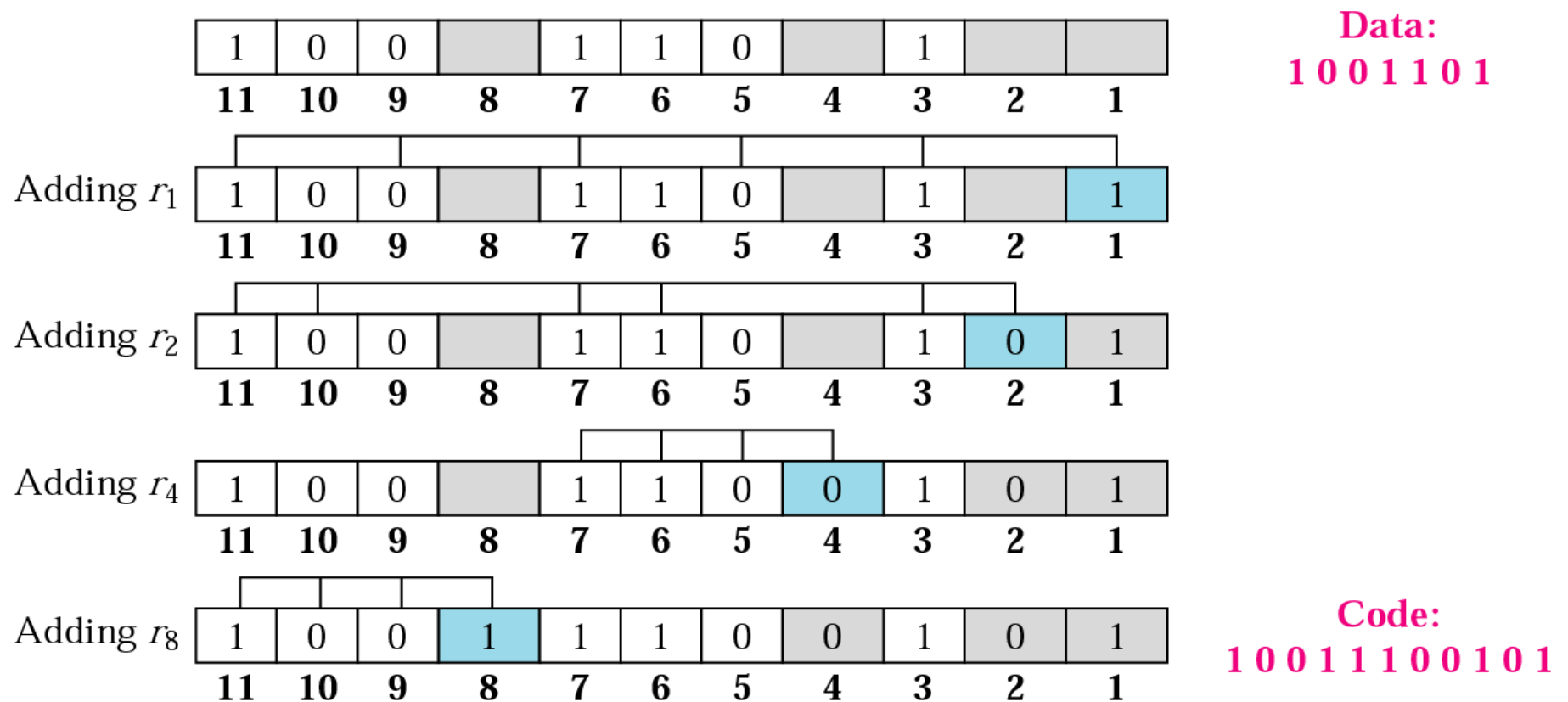
				7	6	5	4			
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

r_8 will take care of these bits.

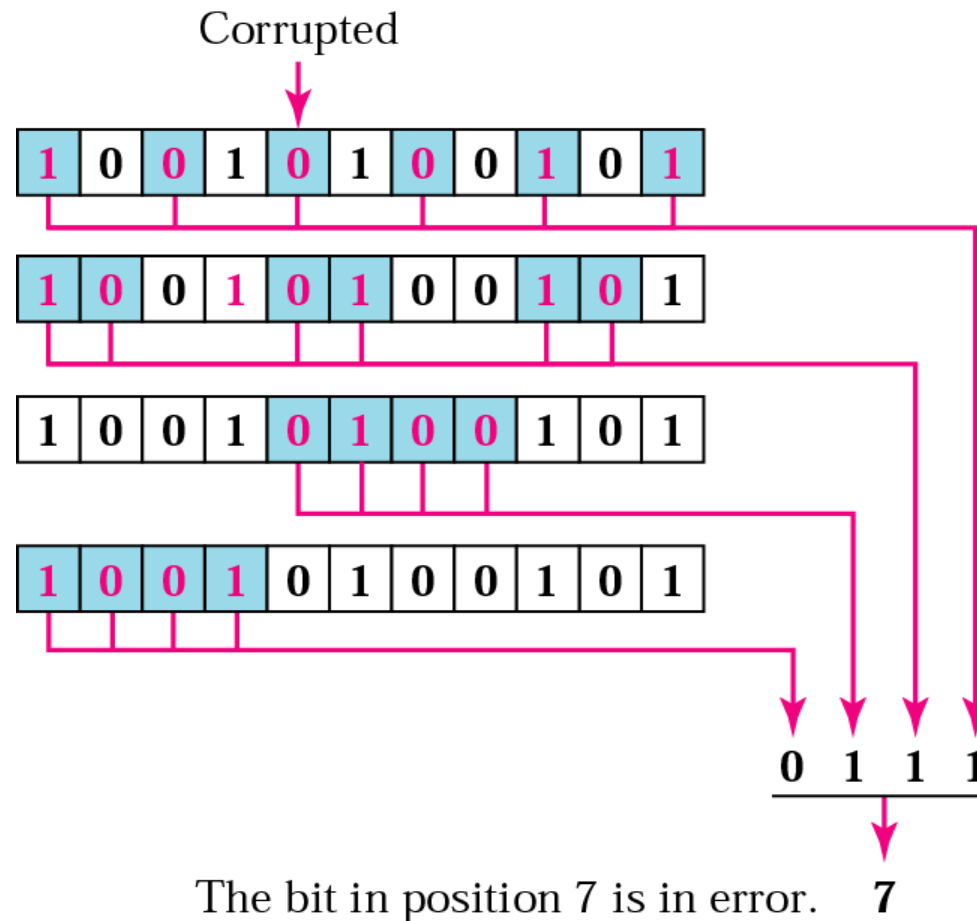
11	10	9	8							
d	d	d	r_8	d	d	d	r_4	d	r_2	r_1

Calculate even parity for r_1, r_2, r_4 and r_8 using their respective bit position

Example of redundancy bit calculation



Error detection using Hamming code



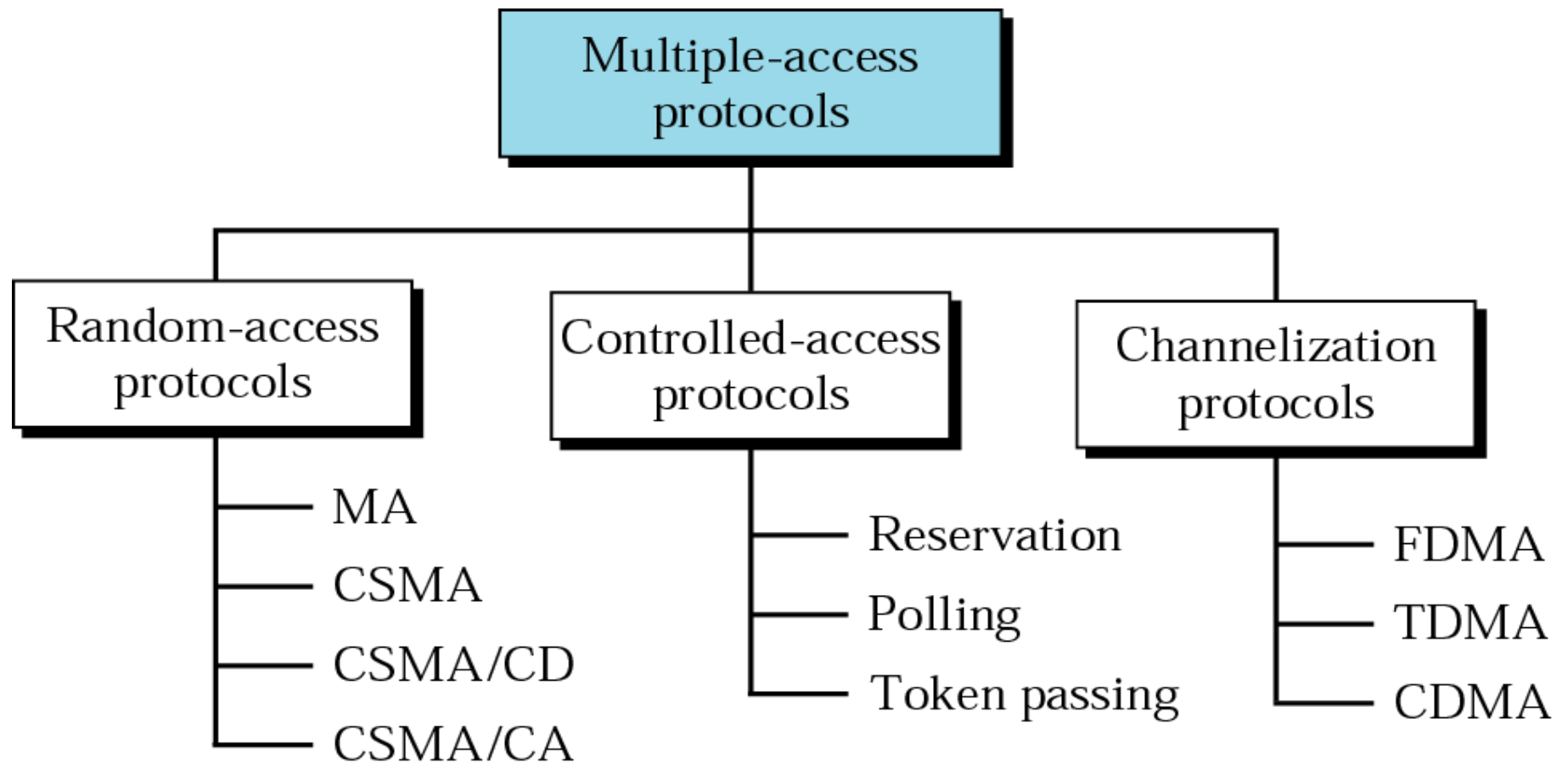
calculate the even parity for r1, r2, r4 and r8 using respective bit position



Channel Access Mechanism

- Allows **several terminals** connected to the same multi-point transmission medium to transmit over it and to share its capacity
- Examples of shared physical media are **wireless networks, bus networks, ring networks and half-duplex point-to-point links**

Channel Access Types



Random Access Method

Random Access: Many terminals communicate to a single base station

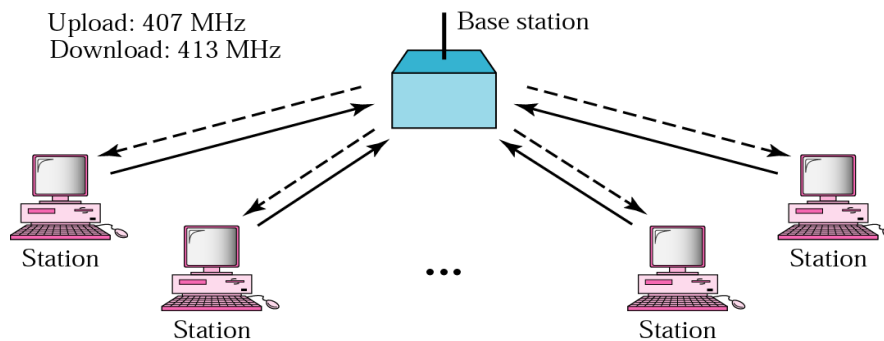
Random Access works better for

- many users, where ..
- each user only occasionally sends a message
- **Types**
 - ALOHA SYSTEM
 - MA
 - CSMA
 - CSMA/CD
 - CSMA/CA

Random Access Method: ALOHA SYSTEM

- Any terminal is allowed to transmit without considering whether channel is idle or busy
- If packet is received correctly, the base station transmits an acknowledgement.
- If no acknowledgement is received by the mobile,
 - 1) it assumes the packet to be lost
 - 2) it retransmits the packet after waiting a *random* time

ALOHA System

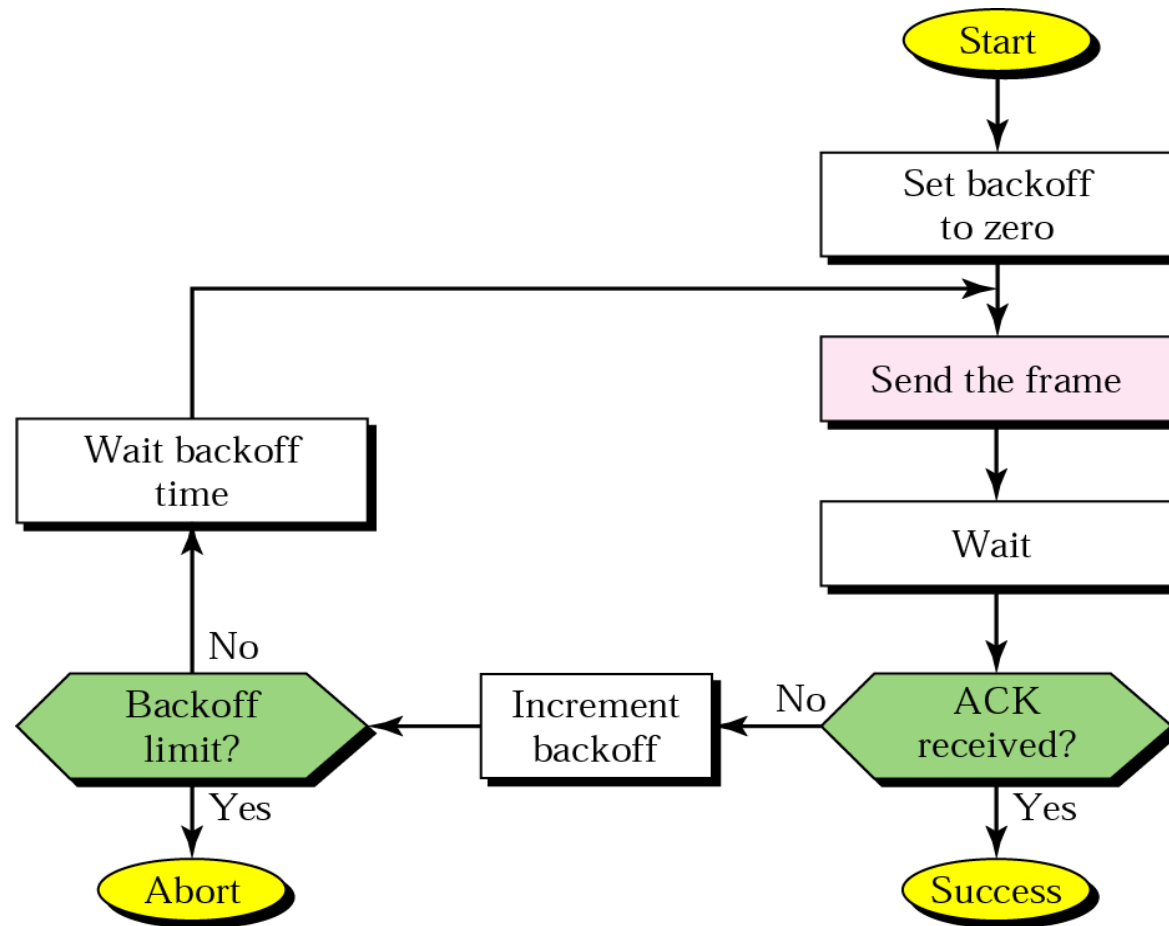


- Any terminal is allowed to transmit without considering whether channel is idle or busy
- If packet is received correctly, the base station transmits an acknowledgement.
- If no acknowledgement is received by the mobile,
 - 1) it assumes the packet to be lost
 - 2) it retransmits the packet after waiting a *random* time, usually with probability P_r in every slot.

ALOHA SYSTEM: Types

- Unslotted ALOHA (PURE ALOHA)
 - Transmission may start anytime
 - If you have data to send, send the data. If message collides with other transmission try resending later.
- Slotted ALOHA
 - packets are transmitted in time slots
 - Introduced discrete timeslots and increased the maximum throughput.

Procedure for ALOHA protocol

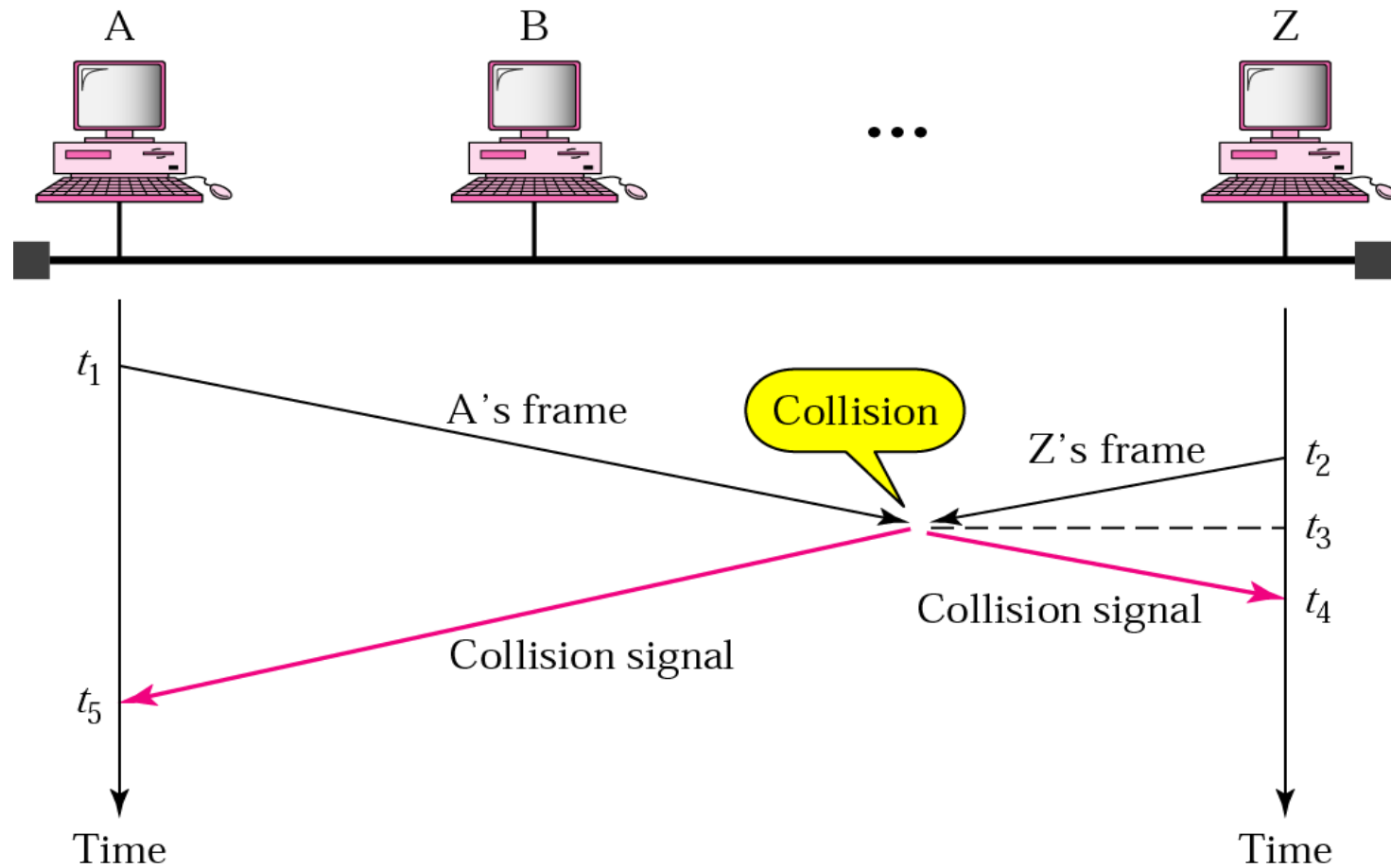




CSMA

- Based on the principle "sense before transmit" or "listen before talk."
- Node **verifies the absence of other traffic** before transmitting on a shared transmission medium
- Multiple access means that multiple stations send and receive on the medium
- Each station first **listen to the medium before Sending**

Collision in CSMA





Vulnerable Time

- The vulnerable time for CSMA is the propagation time T_p that a signal to propagate from one end of the medium to the other.



Persistent Methods in CSMA

- What should a station do if the channel is idle?
- Three methods have been devised to answer these questions:
 - 1 persistent
 - Non Persistent
 - P-Persistent



CSMA- I Persistent

- When Station Find Channel Idle
 - Sends Frame Immediately with probability 1
 - Has the highest Chance of Collision
 - Because two or more station find the line idle



CSMA Nonpersistent

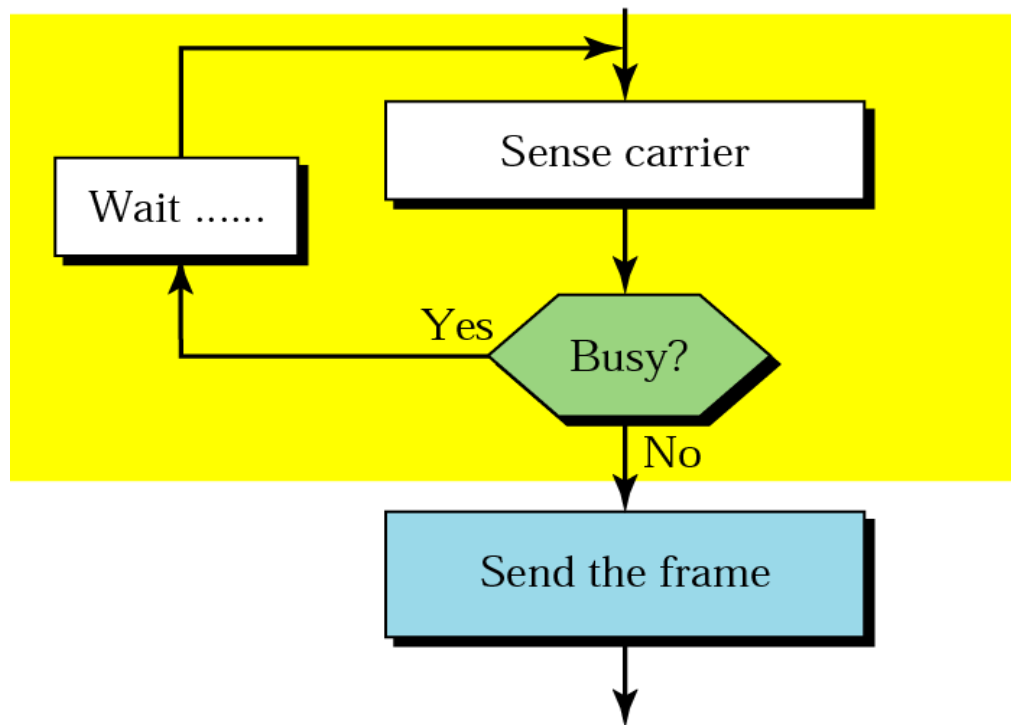
- senses the line.
- If the line is idle, it sends immediately
- If the line is not idle
 - Waits, random amount of time and then senses the line again
- The nonpersistent approach reduces the chance of collision
- Reduces the efficiency of the network
 - Because medium remains idle when there may be stations with frames to send

CSMA P-Persistent

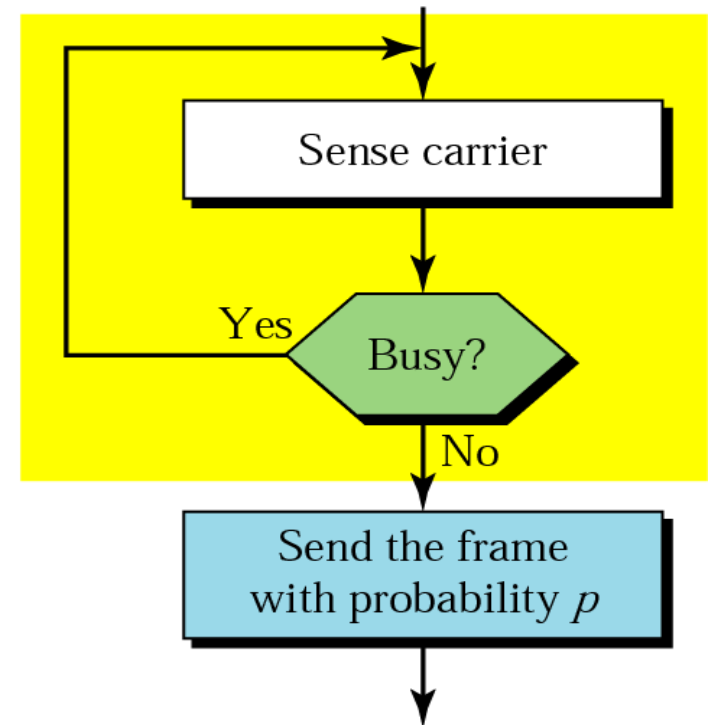
- P-Persistent Use the time slot with time slot equal or greater than maximum propagation time
- In this Method if the station find the channel is idle, it follows these steps
 - With probability P , the station sends it frame
 - With probability $q = 1 - p$, the station waits for the beginning of the next time slot
 - and checks the line again
 - With probability $q = 1 - p$, the station waits for the beginning of the next time slot and checks the line again
 - If the line is busy, it acts as though a collision has occurred and uses the back-off procedure

Non Persistent and P-Persistent

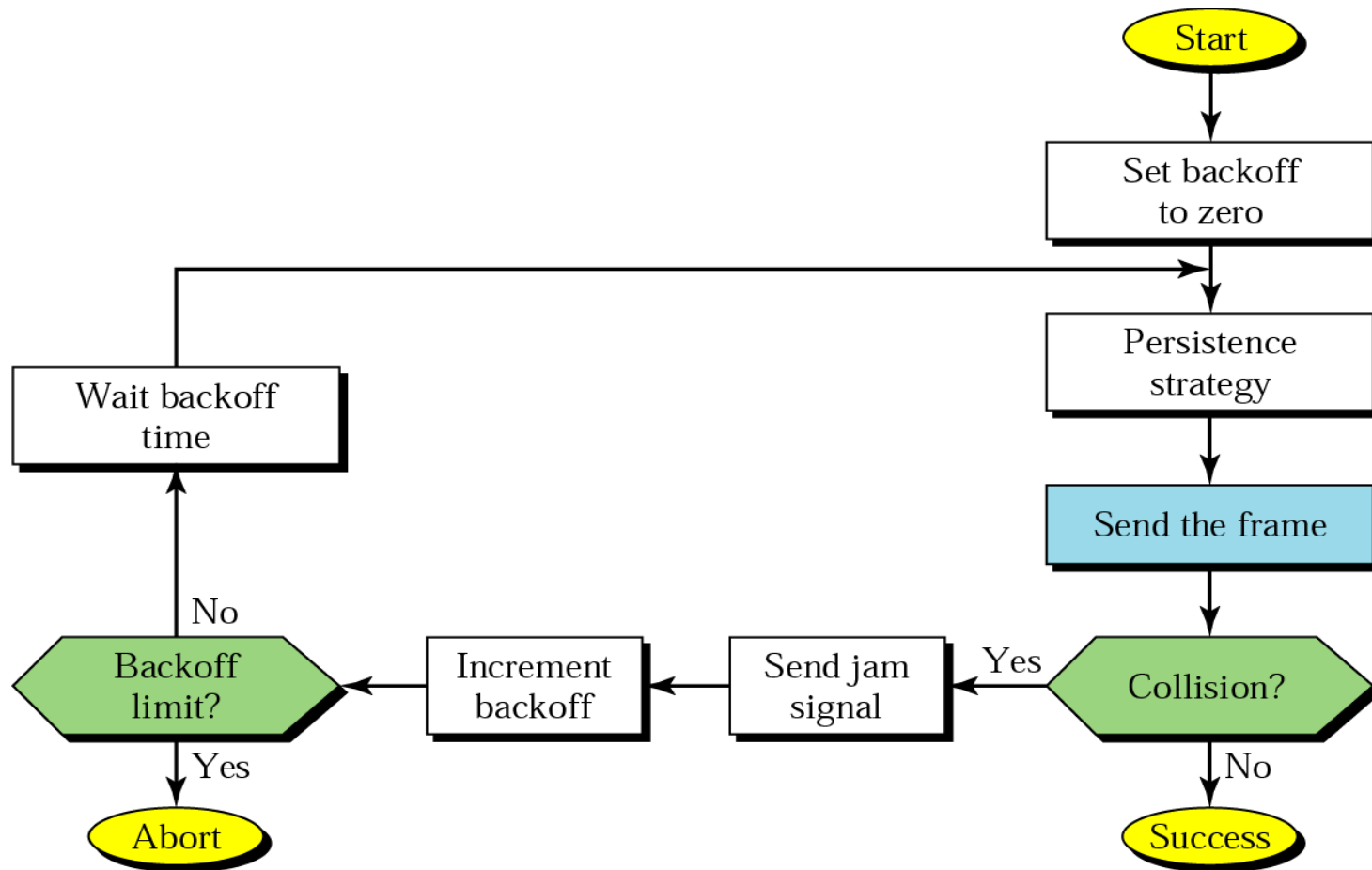
Nonpersistent strategy



Persistent strategy



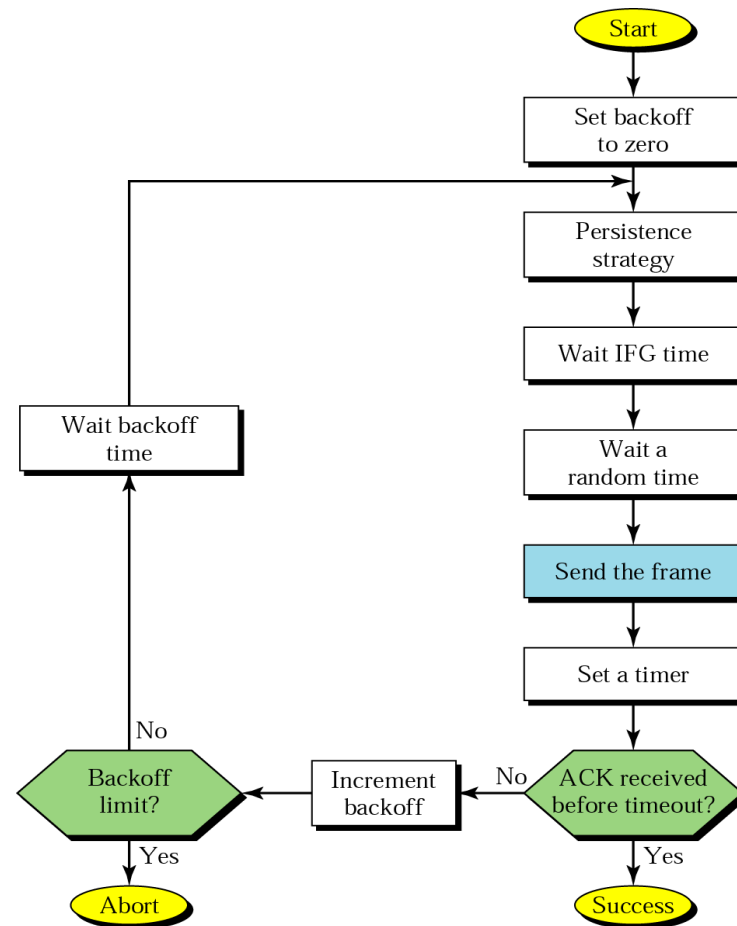
CSMA/CD procedure



CSMA/CD

- A network using CSMA/CD has a bandwidth of 10 Mbps. If the maximum propagation time including the delays in the devices and ignoring the time needed to send a jamming signal, as we see later) is 25.611S, what is the minimum size of the frame?
-
- Formula
 - $\text{Framesize} * 2tp$

CSMA/CA

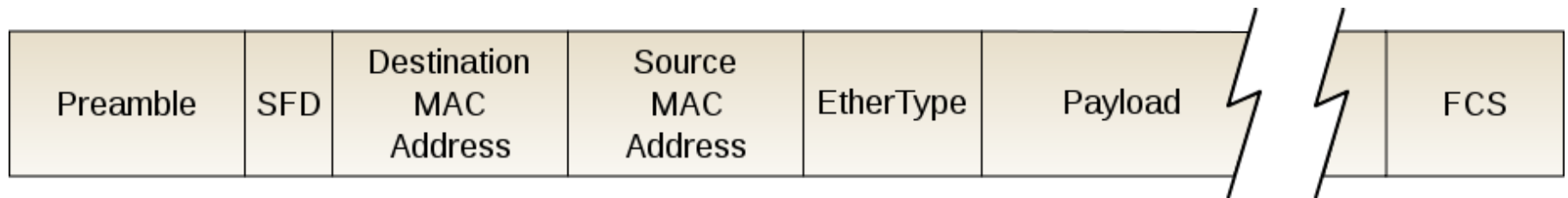






Ethernet Frame

- Computer Networking Technology for LAN and Large Area Network
- Ethernet: It is a LAN protocol that is used in Bus and Star topologies and implements CSMA/CD as the medium access method

Ethernet Frame Format



- 
- Preamble
 - 7-Octets 10101010 value
 - start frame delimiter
 - 1 Octets
 - Header
 - Mac Destination
 - 6 octets
 - Destination MAC Address
 - Mac Source
 - Source Mac Address
 - 6 Octets

- 
- PayLoad
 - 1500 bytes | octets
 - FCS
 - Frame Check Sequences
 - 4 octets



Ethernet Frame Details

- The Preamble - This consists of seven bytes, all of the form "10101010". This allows the receiver's clock to be synchronised with the sender's.
- The Start Frame Delimiter - This is a single byte ("10101011") which is used to indicate the start of a frame.
- The Destination Address - This is the address of the intended recipient of the frame. The addresses in 802.3 use globally unique hardwired 48 bit addresses.
- The Source Address - This is the address of the source, in the same form as above.
- The Length - This is the length of the data in the Ethernet frame, which can be anything from 0 to 1500 bytes.
- Data - This is the information being sent by the frame.
- Checksum - This is used for error detection and recovery.



Draw the Frame Format for Ethernet II and IEEE 802.3 ??

- Homework



Ethernet Cont'd..

- computer networking technologies for local area (LAN) and larger networks
- Frame Format of Ethernet is already discussed in slide 96-101

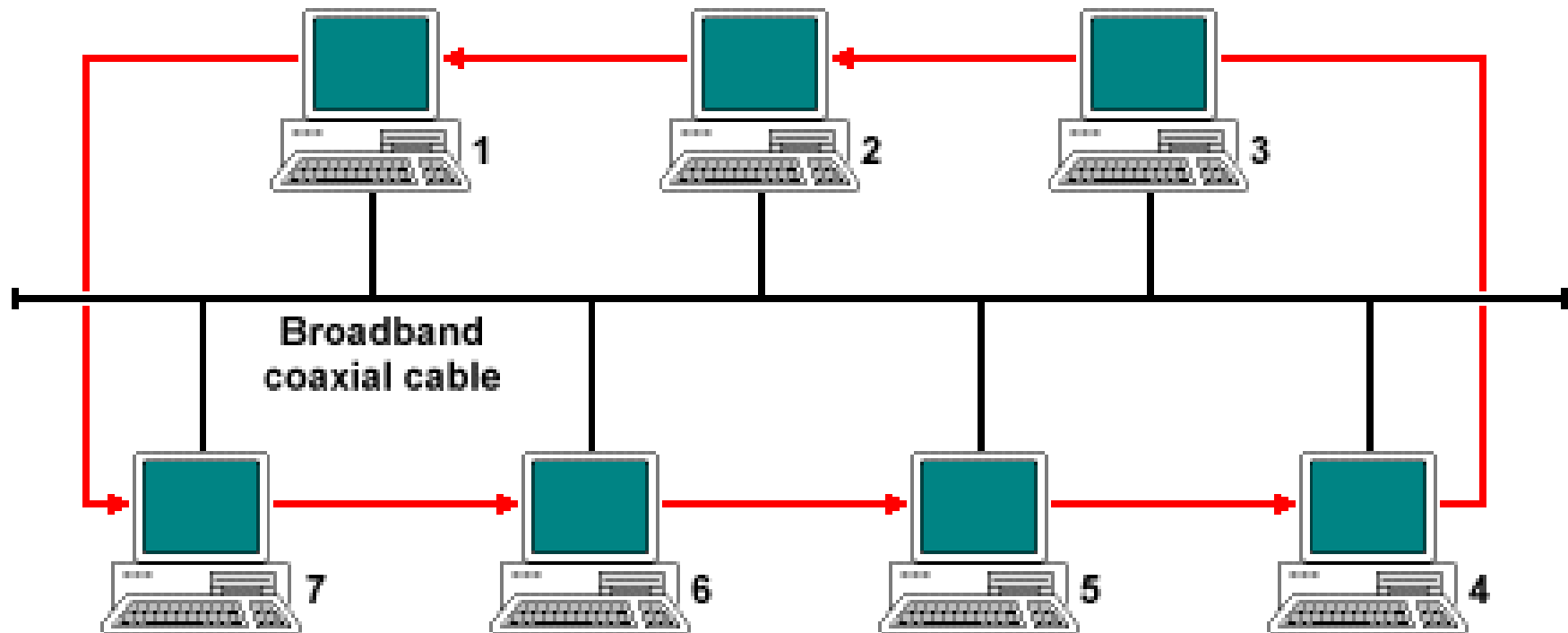
Ethernet Types

- Ethernet
 - Speed 10 Mbps
- Fast Ethernet
 - Also called 802.3u
 - Identified by 100BaseTx
 - Maximum Speed 100 Mbps
- Gigabit Ethernet
 - Speed 1000 Mbps
- Ten GigabitEthernet
 - 10 Gbps
- Note: For More resources:http://www.rhyshaden.com/eth_intr.htm

Token Bus: 802.4

- Token is passed around the network nodes
- Node possessing the token may transmit
- If node doesn't have anything to send, the token is passed to the next node on the virtual ring
- Each node must know the address of its neighbour in the ring
- utilized a copper coaxial cable to connect multiple end stations.
- Token Bus Limitations
 - failure in the bus caused all the devices unable to communicate with the rest of the network.
 - Adding more stations to the bus was somewhat difficult

Token Bus Cont'd..

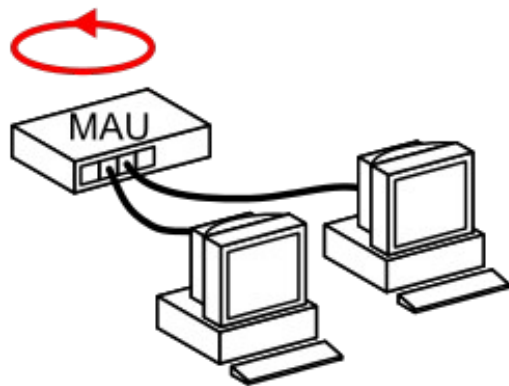




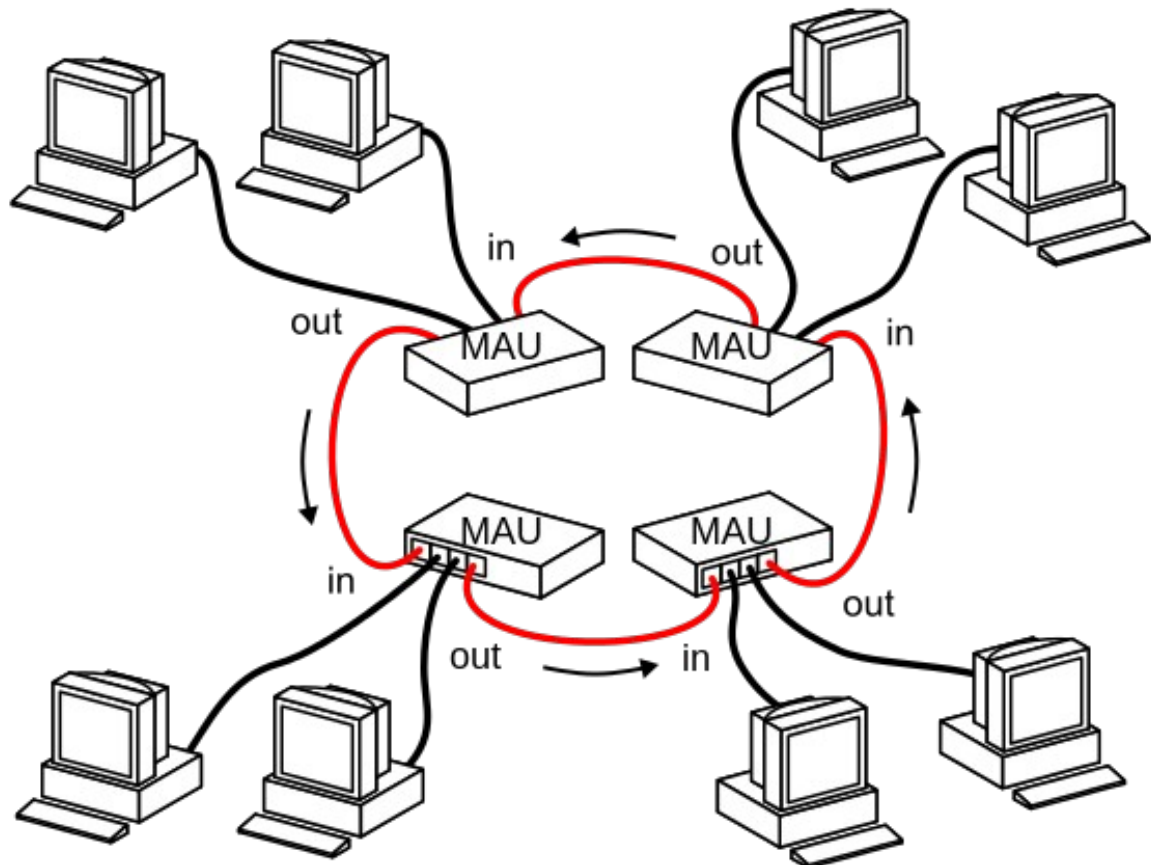
Token Ring: 802.5

- Used Special three-byte frame called Token
 - Token travels around the ring
- Token Ring uses a **ring based topology** and passes a token around the network to control access to the network wiring.
- Token ring frame travel completely around the loop
- All nodes are connected in a ring or Star topology
- maximum speed of 16 Mbps

Token Ring



a)



b)



Virtual Circuit Switching

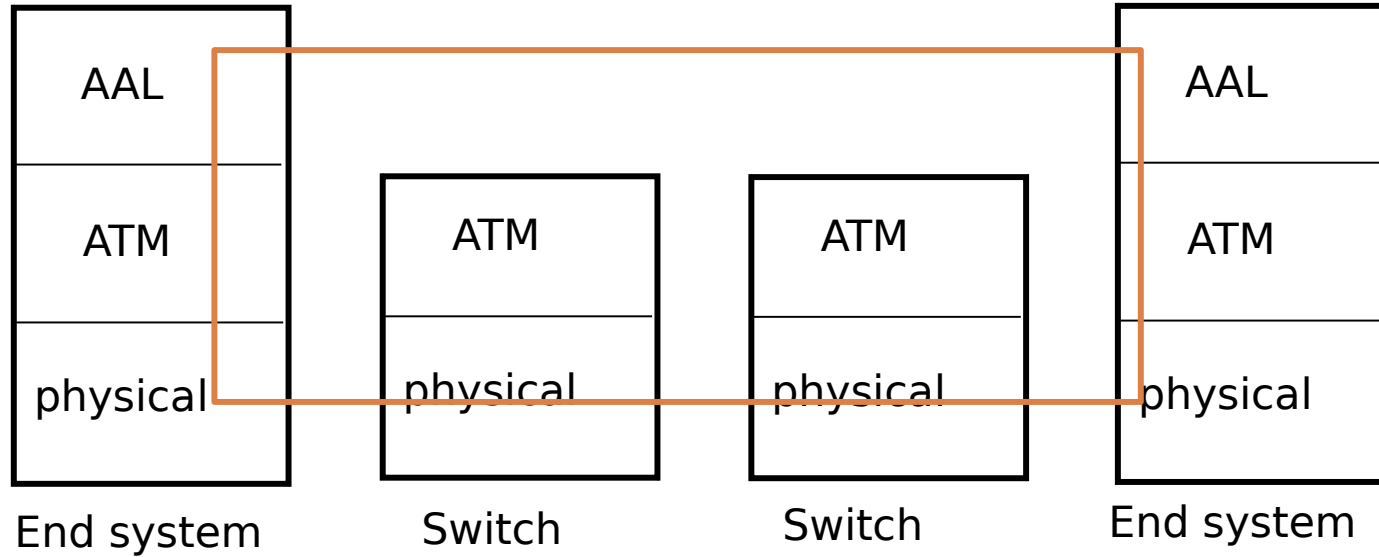
- ATM
- Frame Relay
- X.25



ATM : Asynchronous Transfer Mode

- 1990s Standard for High Speed for Broadband Integrated Service Digital Network Architecture.
- Data Rate => 155 Mbps to 622 Mbps and Higher.
- Goal => Integrated Voice, Video and Data Transport.
- Provide QoS Requirements for Integrated Traffic.
- Root of Next Generation Telephony.
- Fixed Length Packets => Cells (Uses Virtual Circuit Approach).

ATM : Architecture ??



ATM Network

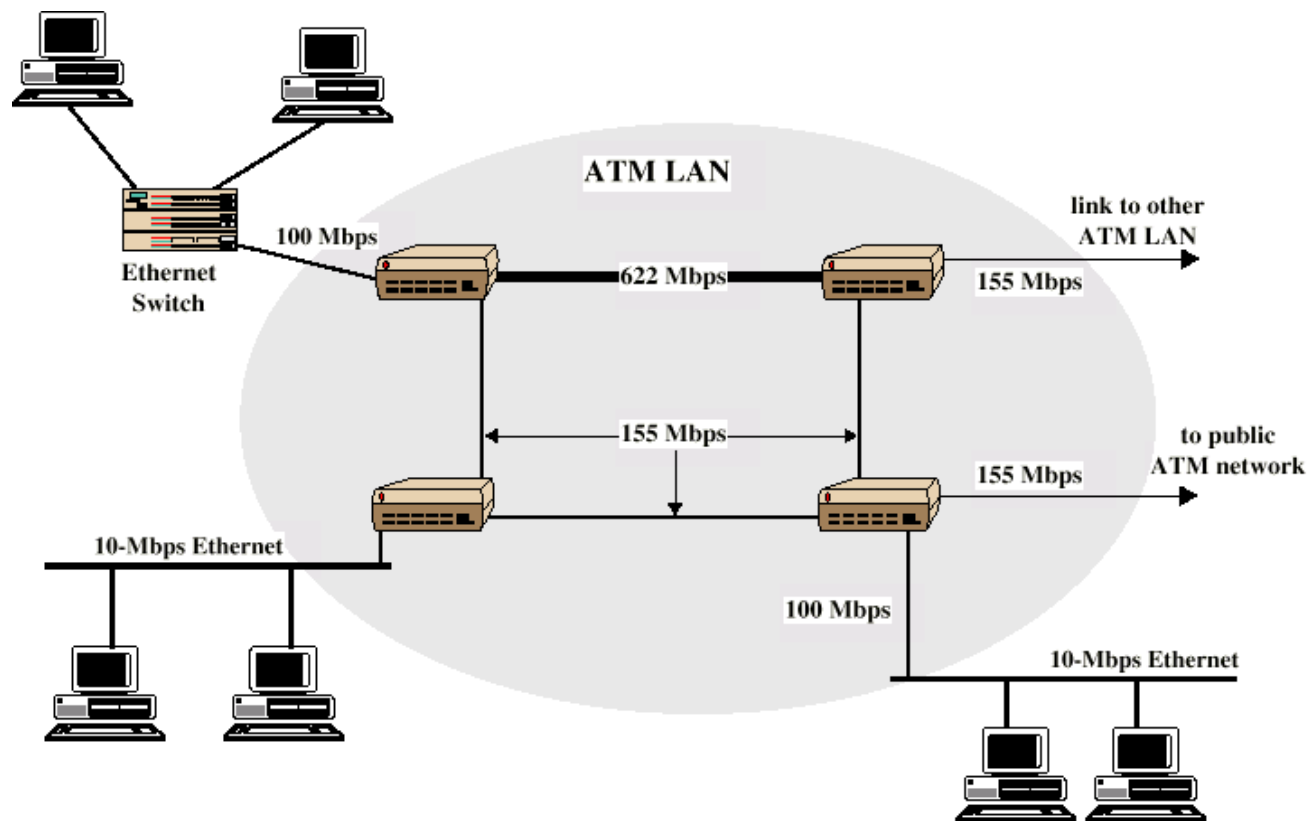


Figure 14.11 Example ATM LAN Configuration



ATM : Protocol Architecture

AAL (ATM Adaptation Layer)

- Used only at edge of ATM Network.
- Data Segmentation Reassembly.
- Analogous to Internet Transport Layer.

ATM Layer

- Analogous to Internet Network Layer.
- Cell Switching and Routing.

Physical Layer

- Analogous to Internet Physical Layer.



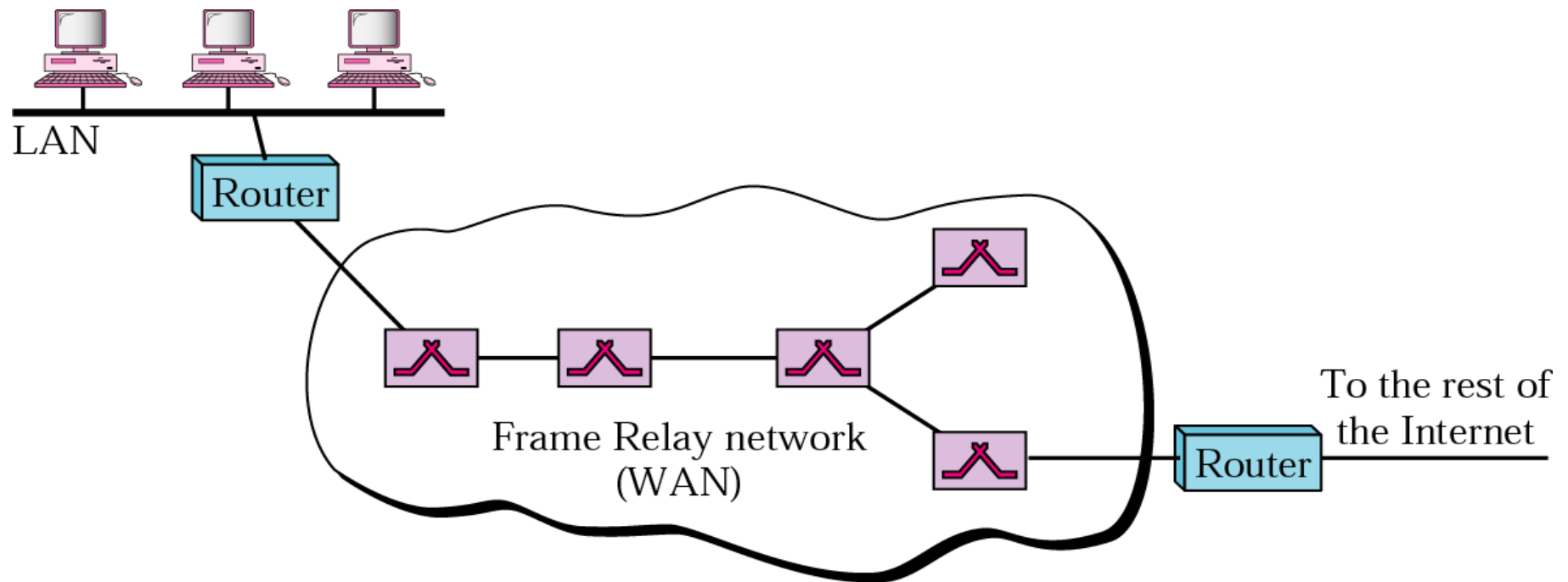
Frame Relay

- It is a Virtual Circuit Wide Area Networks.
- Designed to respond for new type of WAN in late 1980s.
- Prior to Frame Relay => X.25 were Used.

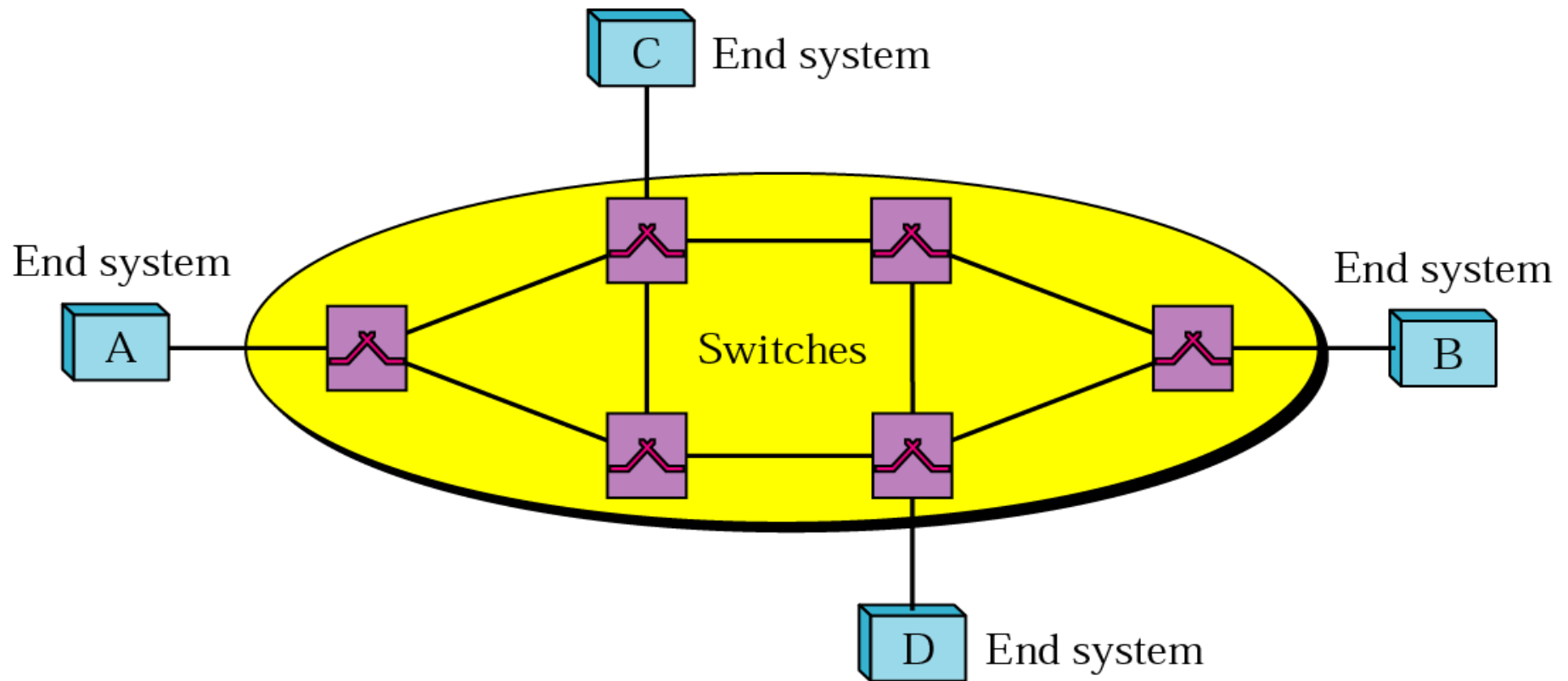
- Demerits of X.25
 - ✓ Low Data Rate (64 Kbps).
 - ✓ Flow and Error Control at Data Link Layer and Network Layer.
 - ✓ X.25 has its own Network Layer.

- Frame Relay Operates at Higher Speed (1.54 Mbps).
- It Operates in Physical and Data Link Layers.
- Can be easily used as a backbone Network.

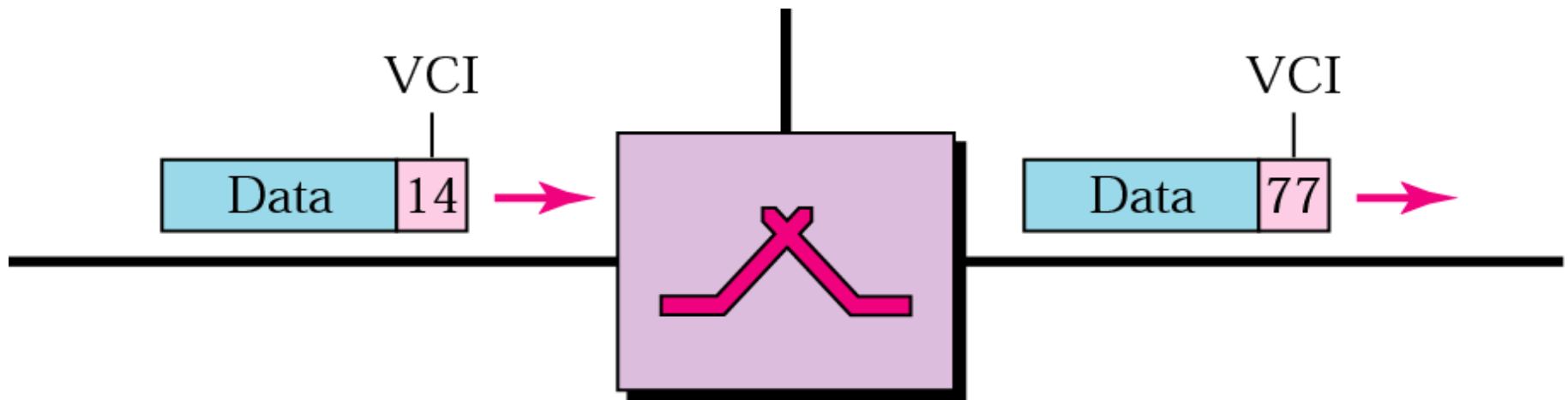
Frame Relay Network



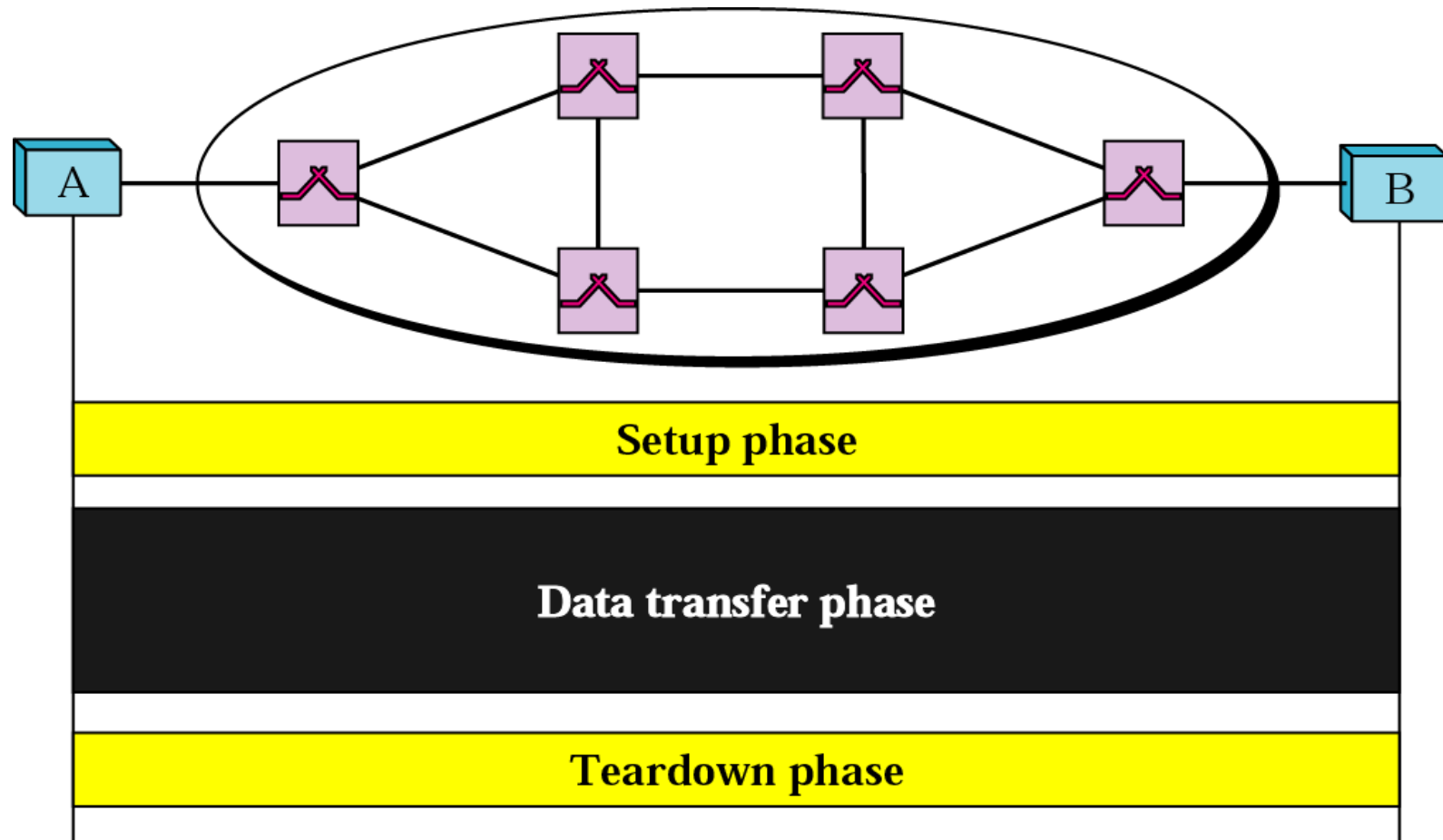
Frame Relay Networks: Virtual Circuit Wide Area Network



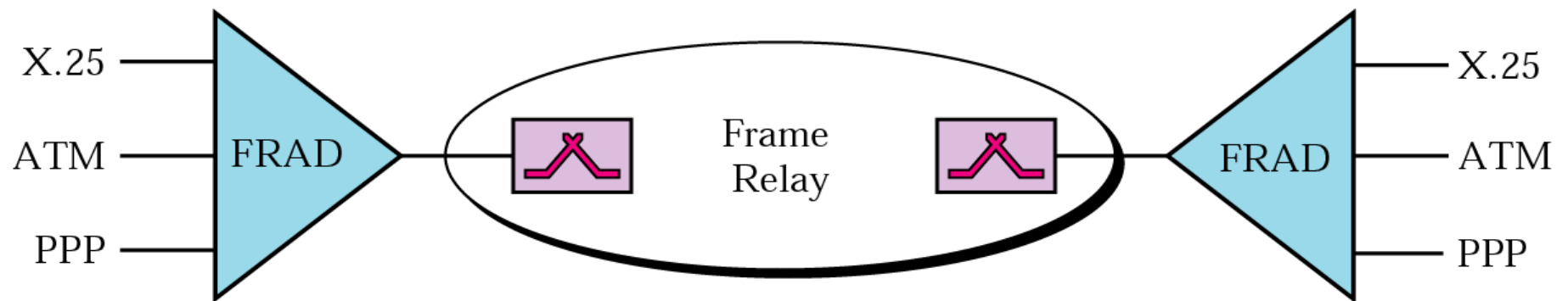
Frame Relay: VCI: Virtual Connection Identifier



VCI Phases: Three Phases of VCI



FRAD: Frame Relay Assembler Disassembler



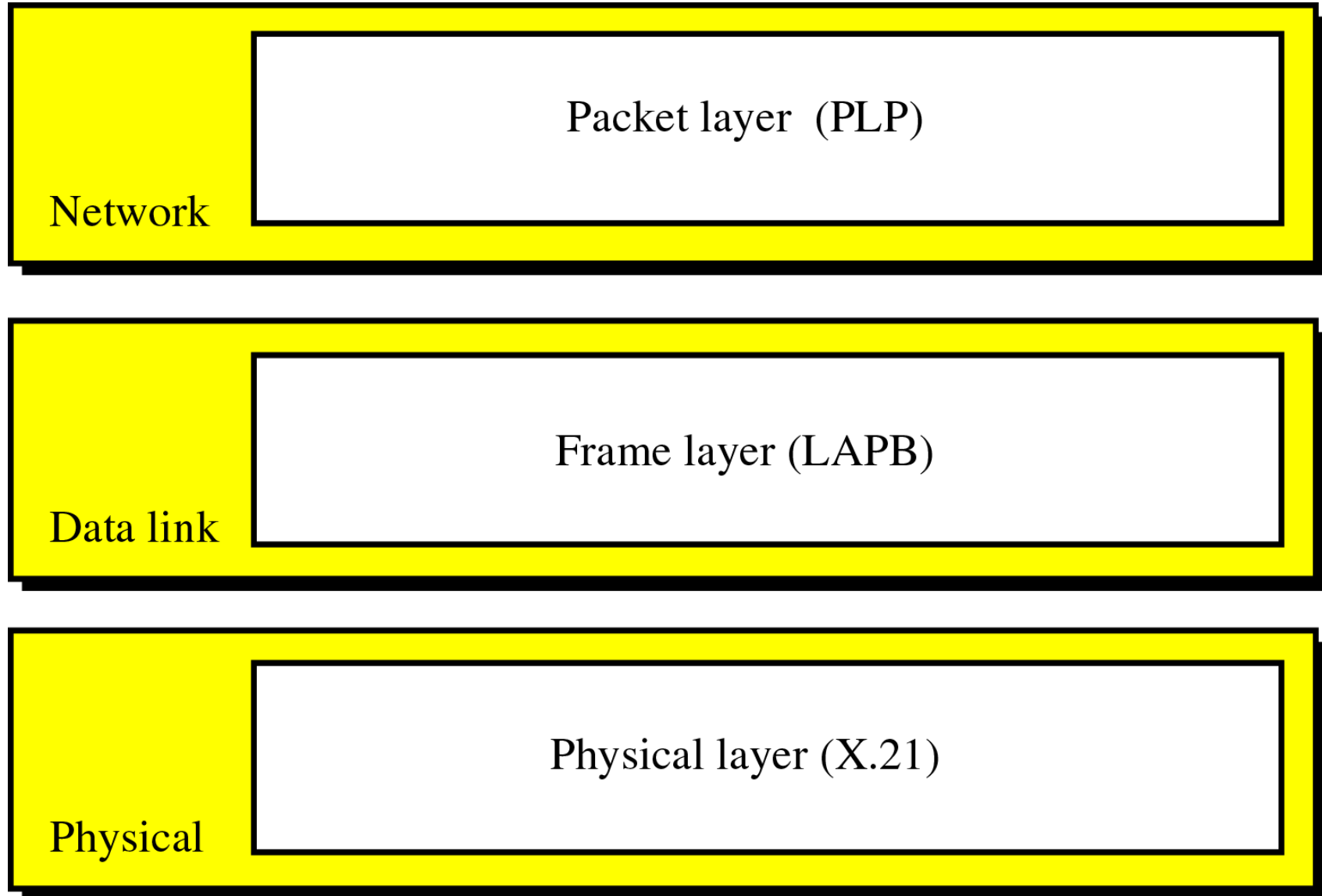


X.25

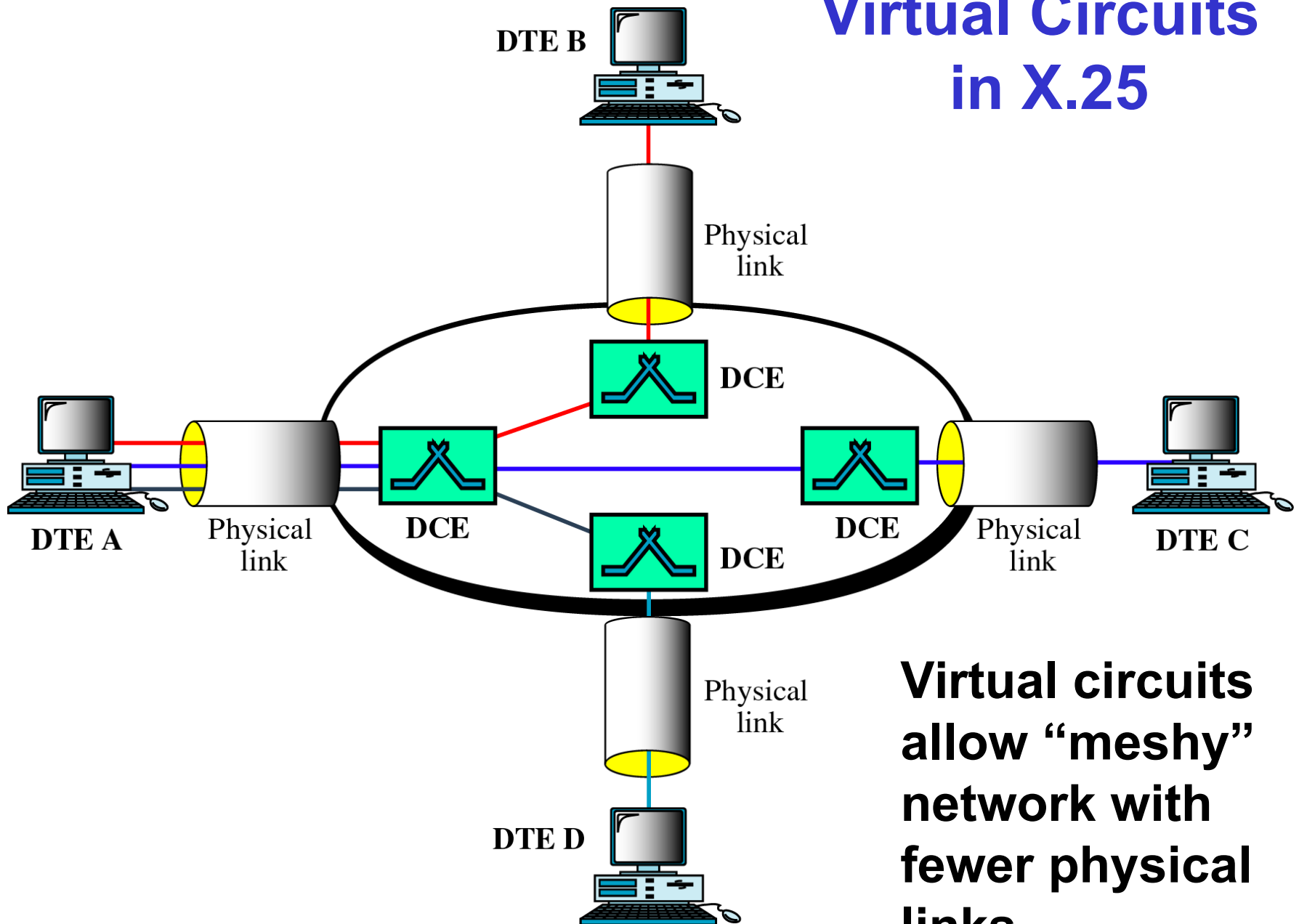
- Was the first popular packet switched network
- Allowed for the setup of data connections at speeds between 300bps to about 56kbps.
- Uses the “Virtual Circuit” concept.
 - Connection oriented packet switch.
- Still used for low bandwidth transactions
 - credit cards / Point-of-Sale (POS) transactions.
 - Telemetry networks.

Figure 17-2

X.25 Layers in Relation to the OSI Layers



Virtual Circuits in X.25



PSTN: Public Switched Telephone Network

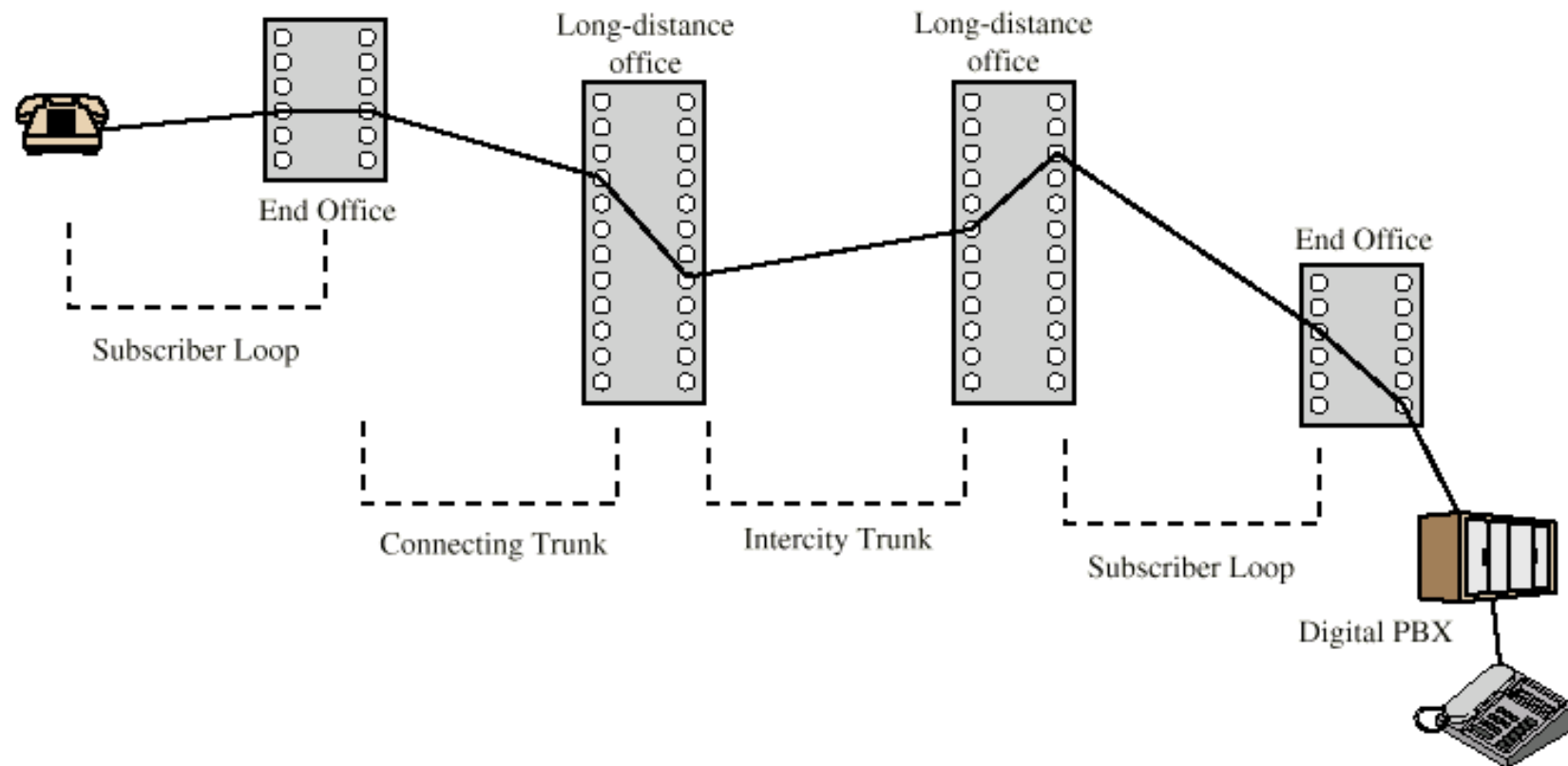


Figure 9.2 Example Connection Over a Public Circuit-Switching Network



Thank You