

# Computer Networks

Lecture by:

Jalauddin Mansur

# Chapter 3: Data Link Layer

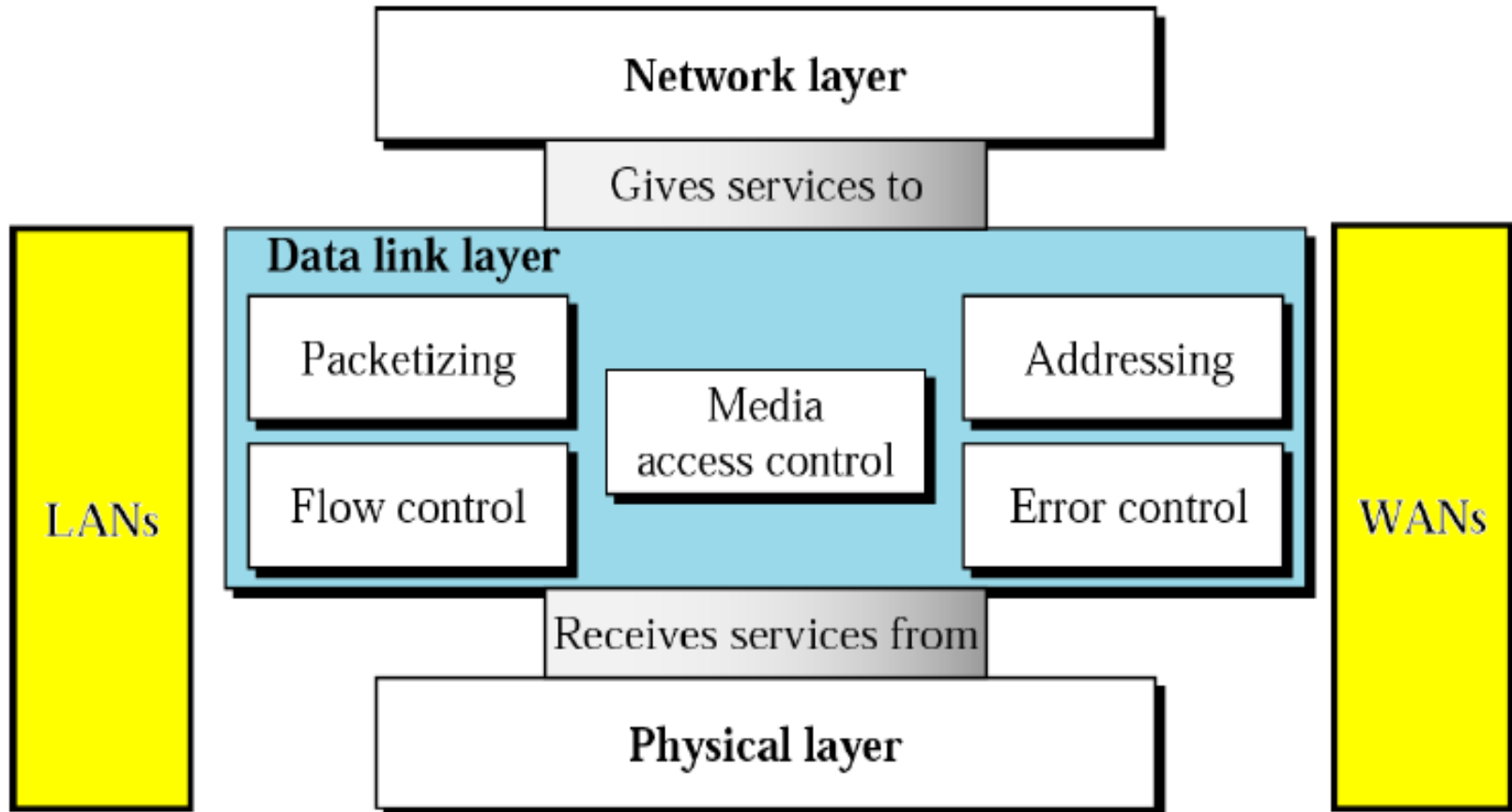
## Topics:

- Functions of Data Link Layer
- Framing
- Error Detection and Correction
- Flow Control
- Examples of Data Link Protocol: HDLC, PPP
- The Medium Access Sub-layer
- The channel allocation problem
- Multiple Access Protocols
- Ethernet
- Networks : FDDI, ALOHA, VLAN, CSMA/CD, IEEE 802.3, IEEE 802.4, IEEE 802.5 and IEEE 802.11

# Data Link Layer : Basic

- Data link layer is layer 2 in OSI Model
- The Data Link Layer sits between the Network Layer and the Physical Layer.
- The DLL provides an interface for the Network Layer to send information from one machine to another.
- To the Network Layer, it looks as though the path to the new machine happens at the DLL level, when it is really happening at the physical level.
- Concerned with local delivery of frames between devices on the same LAN/WAN

# Data Link Layer : Position

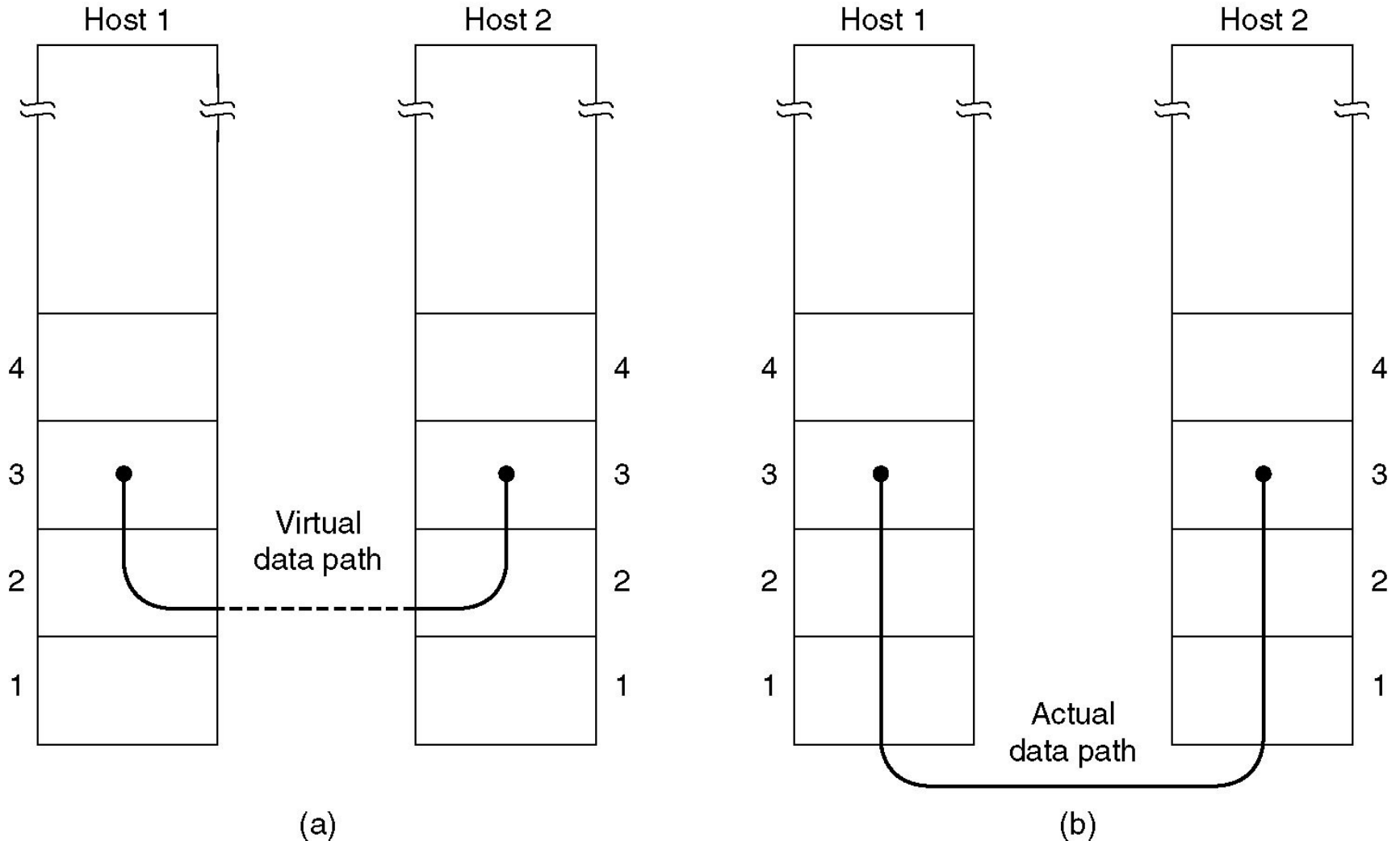


# Data Link Layer : Functions

The data link layer has three specific functions:

1. Provide a well-defined interface to the network layer.
2. Deal with transmission errors.
3. Regulate the flow of data (so that slow receivers are not overloaded).

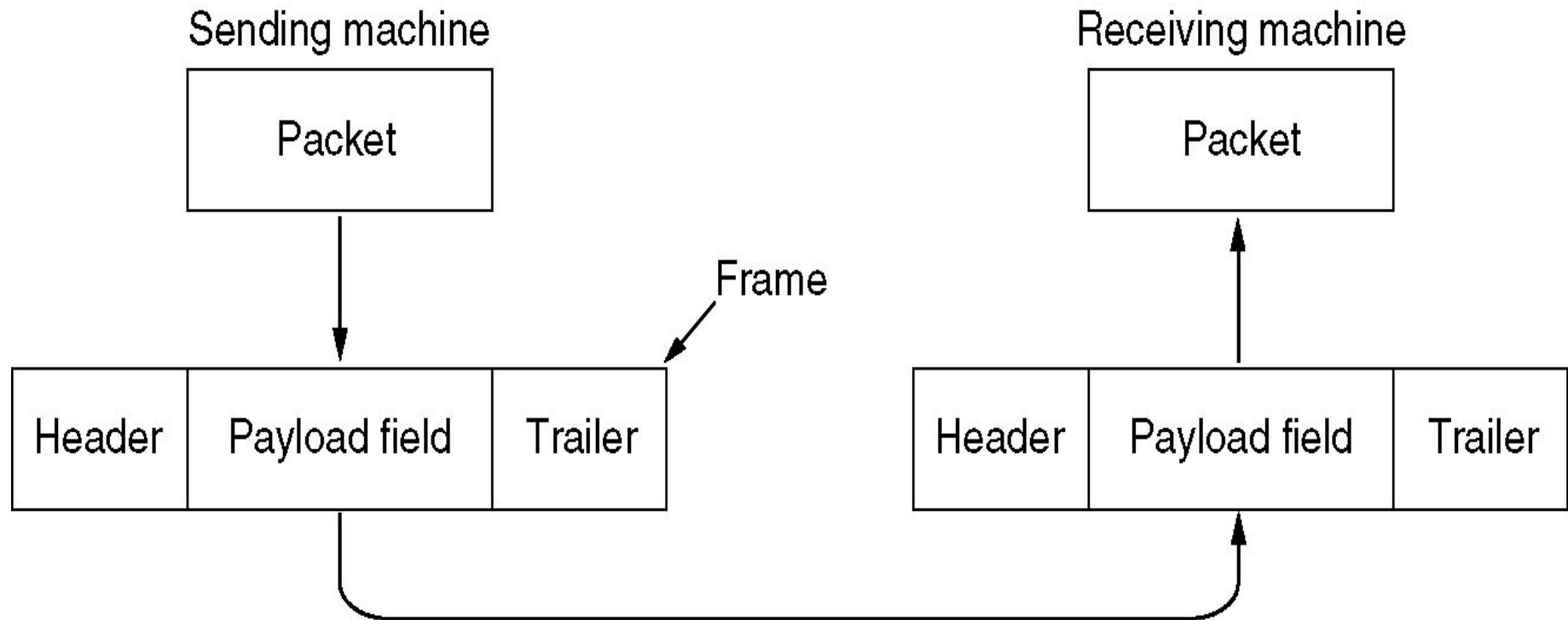
# Data Flow



# How data is moved

- The DLL is responsible for taking the **packets** of information that it receives from the Network Layer and putting them into **frames** for transmission.
- Each frame holds the payload plus a header and a trailer (overhead).
- It is the frames that are transmitted over the physical layer.

# Packets and Frames



# DLL Services

- The Data Link Layer can offer many different services.
- These services can vary from system to system.
- Common services:
  - Unacknowledged connectionless service.
  - Acknowledged connectionless service.
  - Acknowledged connection-oriented service.

# Unacknowledged Connectionless Service

- No acknowledgement from the receiving machine.
- No logical connection is set up between the two machines.
- The DLL will make no attempt to detect the loss of or recover a lost frame.
- This service is useful for low error rate networks and for real-time traffic where late data is worse than no data.

# Acknowledged Connectionless Service

- The receiver acknowledges the arrival of each frame.
- If it hasn't arrived correctly (or within the correct time) it can be resent.
- This is a useful service when the connection is unreliable (such as wireless)
- There is no requirement for such an acknowledgement service to be implemented by the Data Link Layer.

# Acknowledged Connection-Oriented Service

- A connection is established between the two machines.
- The frames are then transmitted and each frame is acknowledged.
- The frames are guaranteed to arrive only once and in order.
- This is the same as a “reliable” bit stream.
- The connection is released once the communication is complete.

# Link Layer Services (More)

- Framing, link access:
  - encapsulate datagram into frame, adding header, trailer
  - channel access if shared medium
  - “MAC” addresses used in frame headers to identify source, destination
    - different from IP address!
- Reliable delivery between adjacent nodes
  - seldom used on low bit error link (fiber, some twisted pair)
  - wireless links: high error rates

# Link Layer Services contd..

- *Flow Control:*
  - pacing between adjacent sending and receiving nodes
- *Error Detection:*
  - errors caused by signal attenuation, noise.
  - receiver detects presence of errors:
    - signals sender for retransmission or drops frame
- *Error Correction:*
  - receiver identifies *and corrects* bit error(s) without resorting to retransmission
- *Half-duplex and full-duplex*
  - with half duplex, nodes at both ends of link can transmit, but not at same time

# Framing

- Translates the physical layer's raw bit stream into discrete units called *frames*
- encapsulating a network layer datagram into frame
- Frame is a data on the Layer 2 of the OSI model
- The Process of creating Frames by the Data Link Layer is known as Framing.

# Types of Framing

- Fixed size Framing
- Variable size Framing
- Fixed size Framing
  - Have Fixed Length
  - No need to define boundaries for Frames
  - Example
    - ATM Frames (54 byte cells)
- Variable Size Framing
  - Not Fixed Size
  - Need a way to define the end of the frame and the beginning of the next frame

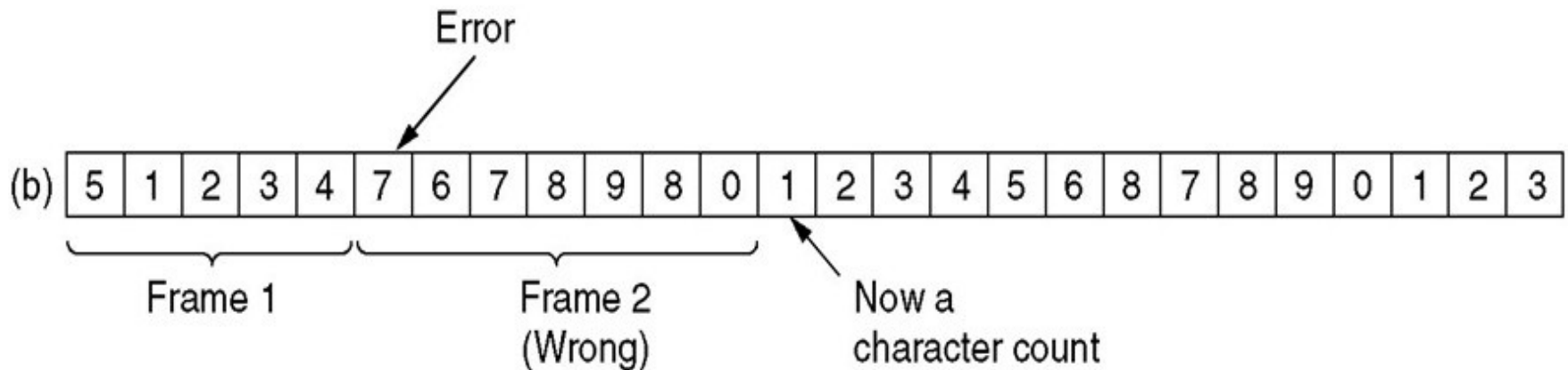
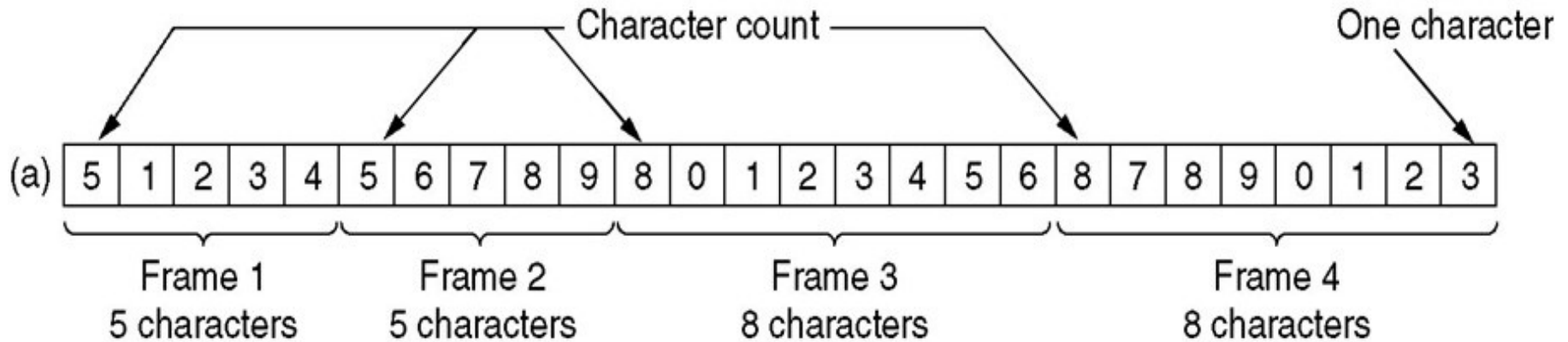
# Different types of Variable Size Framing

1. Character count
2. Flag bytes with byte stuffing
3. Starting and ending flags, with bit stuffing
4. Physical layer coding violations

# Character Count

- We use 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
- This method can cause problems if the count is garbled in transit.
- The receiver will not know where to pick up and the sender will not know how much to resend.
- This method is rarely used anymore.

# Character Count Example

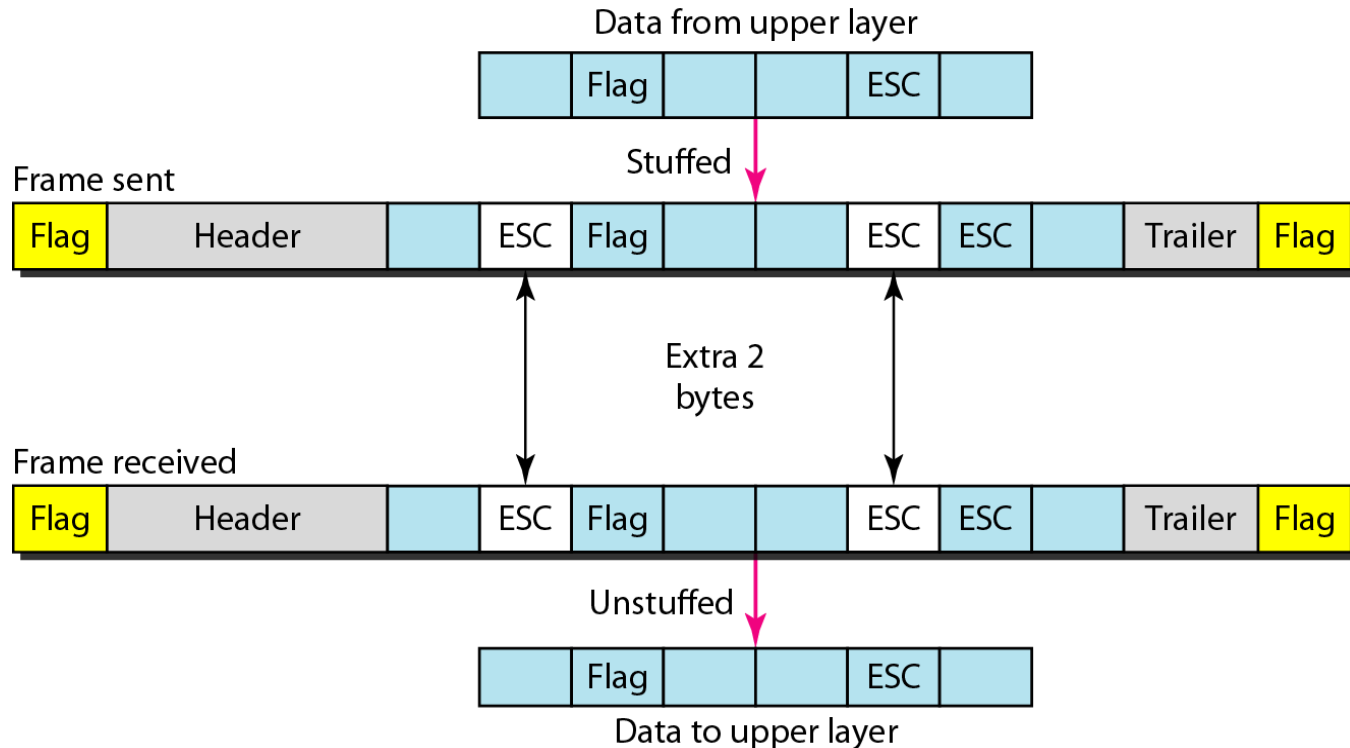


# Flag Bytes (with byte stuffing!)

- Frames begin and end with special bytes.
- Often used are the same start/end flag.
- If the receiver gets “lost”, it just looks for a pair of flag bytes to denote the end of one frame and the start of the next.
- What happens if the “flag” byte is accidentally transmitted in the message ? or message contains flag byte?

## Byte stuffing and unstuffing

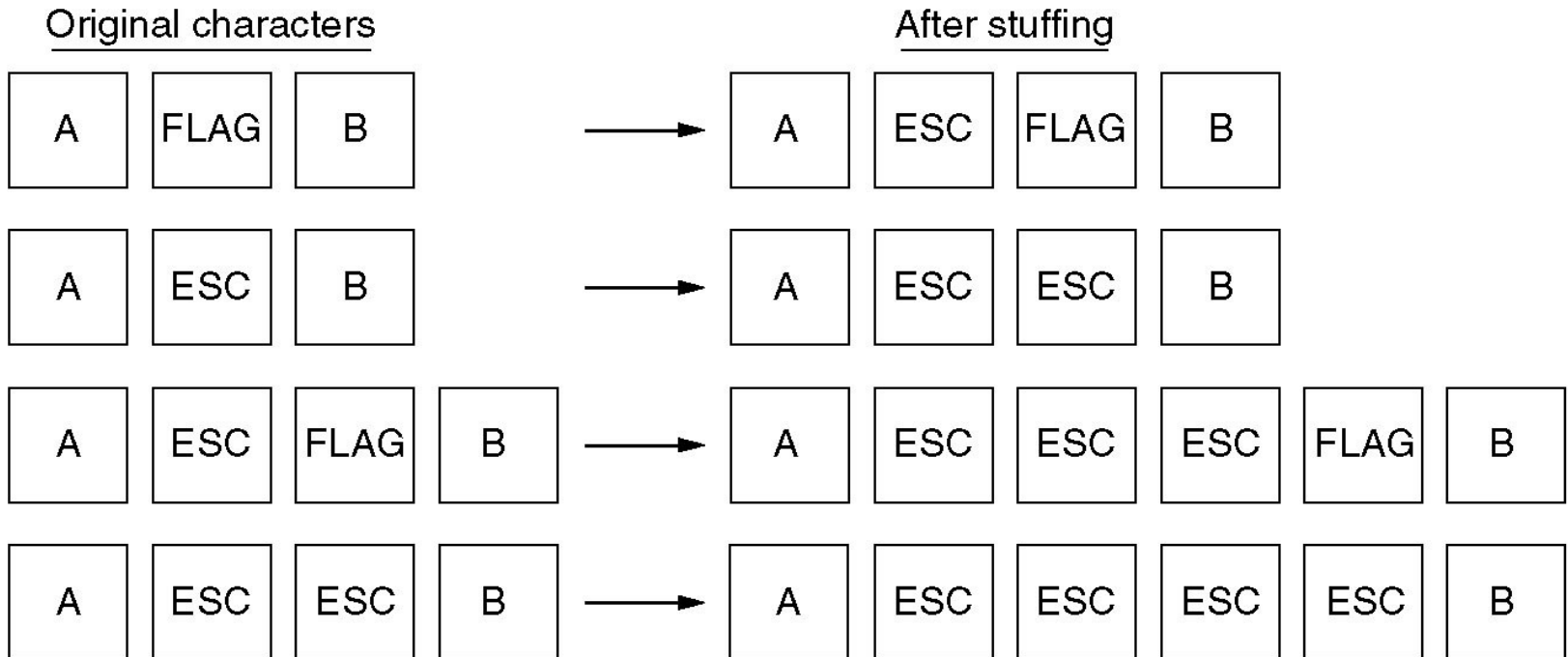
Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.



# Example of Byte Stuffing



(a)



(b)


# Bit Stuffing

- We could have problems with two machines communicating where one uses 8-bit characters and one uses 16-bit characters.
- We stuff **bits** instead of bytes.
- Most DLL protocols use a combination of character count with another method for extra safety. This increases the chances of catching an error.
- 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 de-stuffs the 0 bit.
- The boundary between two frames can be determined by locating the flag pattern.

# Framing – bit stuffing

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

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



Stuffed bits

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

Bit stuffing

(a) The original data.

(b) The data as they appear on the line.

(c) The data as they are stored in receiver's memory after destuffing.

## Framing → Bit Stuffing

Use reserved bit patterns to indicate the start and end of a frame.

For instance, use the 4-bit sequence of 0111 to delimit consecutive frames. A frame consists of everything between two delimiters.



Problem: What happens if the reserved delimiter happens to appear in the frame itself? If we don't remove it from the data, the receiver will think that the incoming frame is actually two smaller frames!

Solution: Use *bit stuffing*. Within the frame, after every occurrence of two consecutive 1's insert 0. E.g., append a zero bit after each pair of 1's in the data. This prevents 3 consecutive 1's from ever appearing in the frame.

Likewise, the receiver converts two consecutive 1's followed by a 0 into two 1's, but recognizes the 0111 sequence as the end of the frame.

# 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

# Error Control

- We use bit and byte stuffing as a method for detecting and determining errors in the data that we send.
- We also have to deal with making sure that the frames make it to their destination.
- The receiver sends back a control frame acknowledging the received frame and the condition of the frame.
- A timeout can occur if the acknowledgement doesn't arrive, resulting in the frame being resent.
- Resending the frame can also cause problems – what happens when the same frame is received twice?
- We can also sequentially number the frames to prevent this problem.

# Error Control contd..

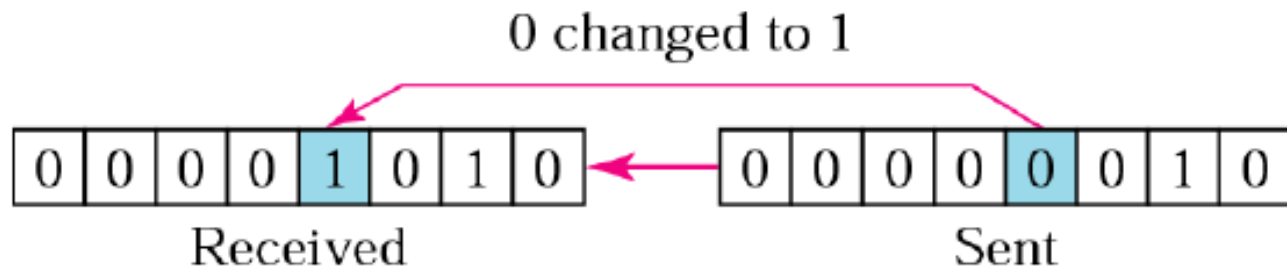
- Error control in the data link layer is based on automatic repeat request, which is the retransmission of data
- Error control includes both error detection and error correction

# Error Control Mechanism

- Error Detection
  - CRC (Cyclic Redundancy Check)
  - Parity Check
  - CheckSum
- Error Correction
  - Hamming codes
  - Binary convolutional codes
  - Reed-Solomon codes
  - Low-Density Parity Check codes

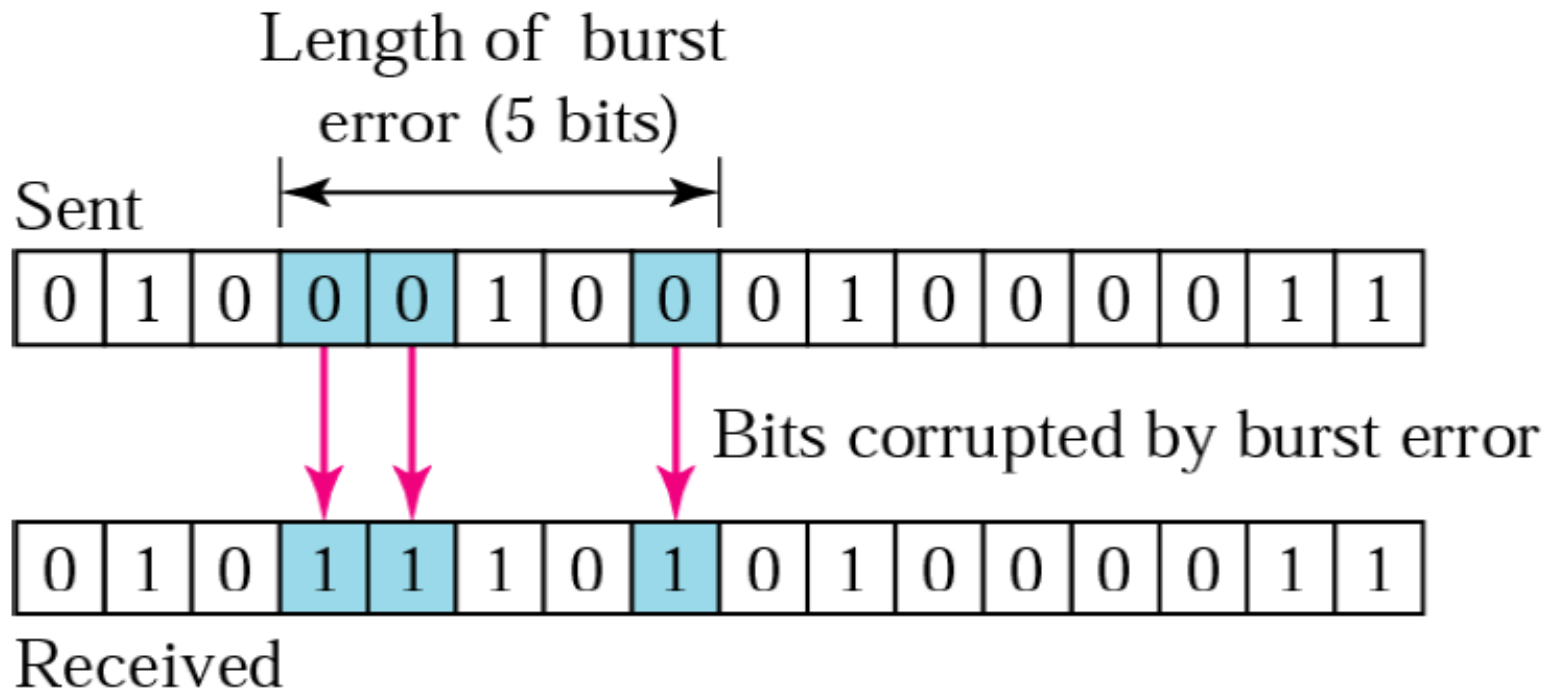
# Error

- Changes in bits results in Error
- Types of Error
  - Single Bit Error
  - Burst Error
- Single Bit Error
  - Occurs 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

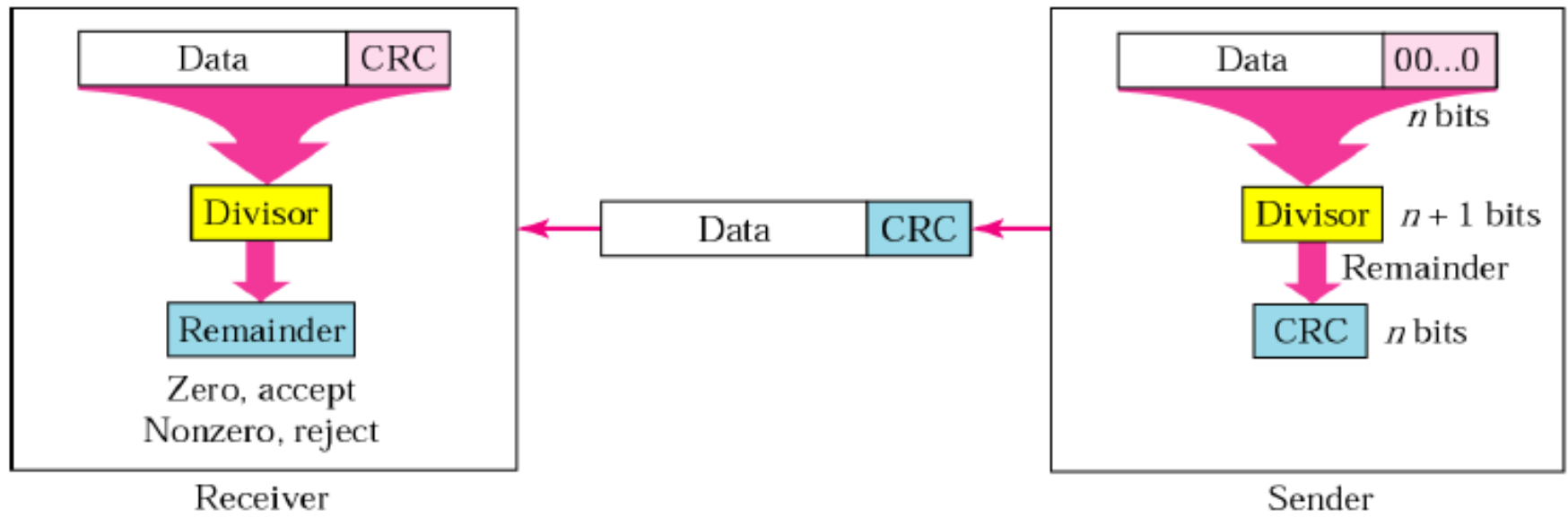


# Error Detection Method

- 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

# CRC (Cyclic Redundancy Check)

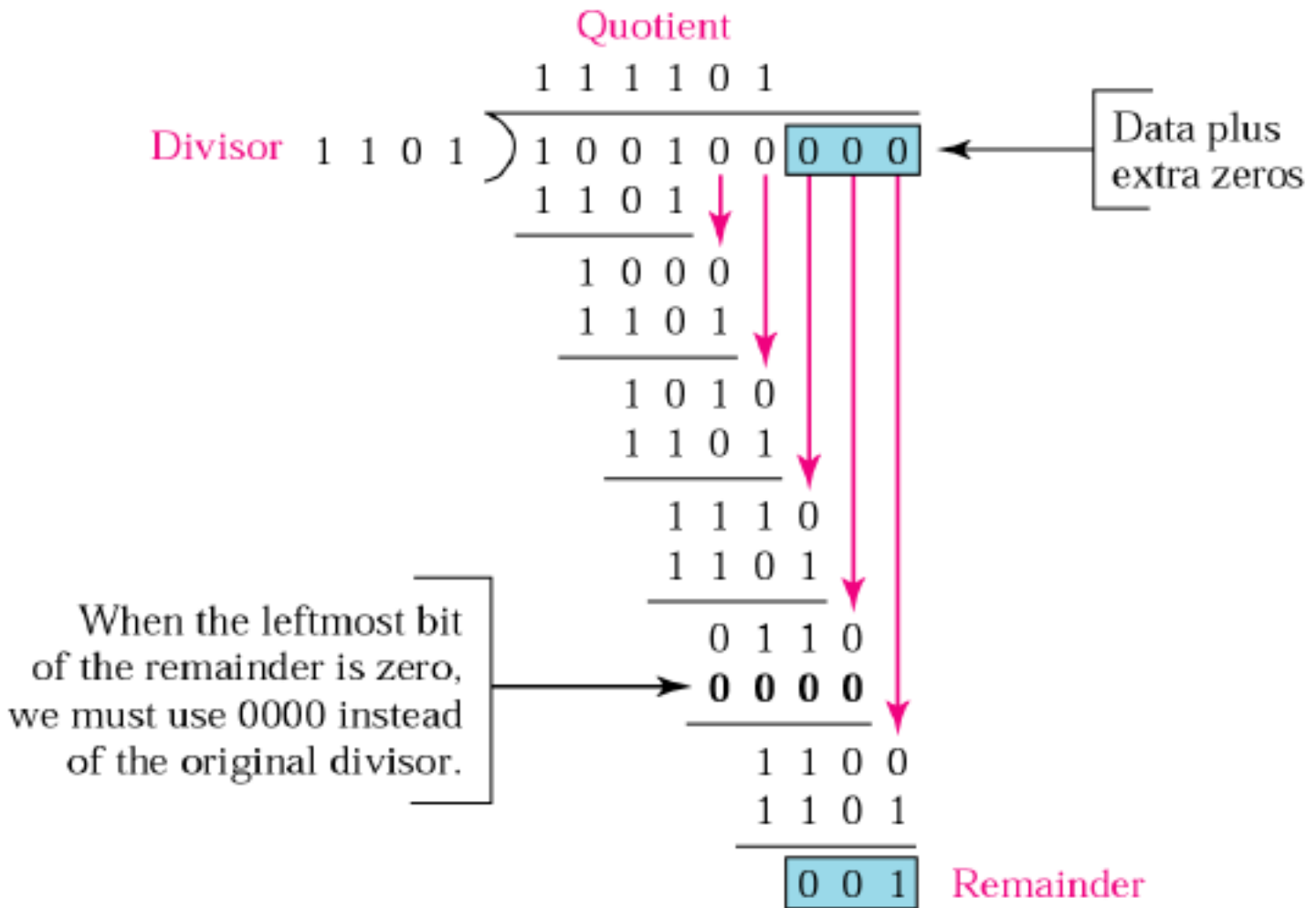
- Given a  $k$ -bit frame or message, the transmitter generates an  $n$ -bit sequence, known as a frame check sequence (FCS), so that the resulting frame, consisting of  $(k+n)$  bits, is exactly divisible by some predetermined number.
- The receiver then divides the incoming frame by the same number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



# CRC

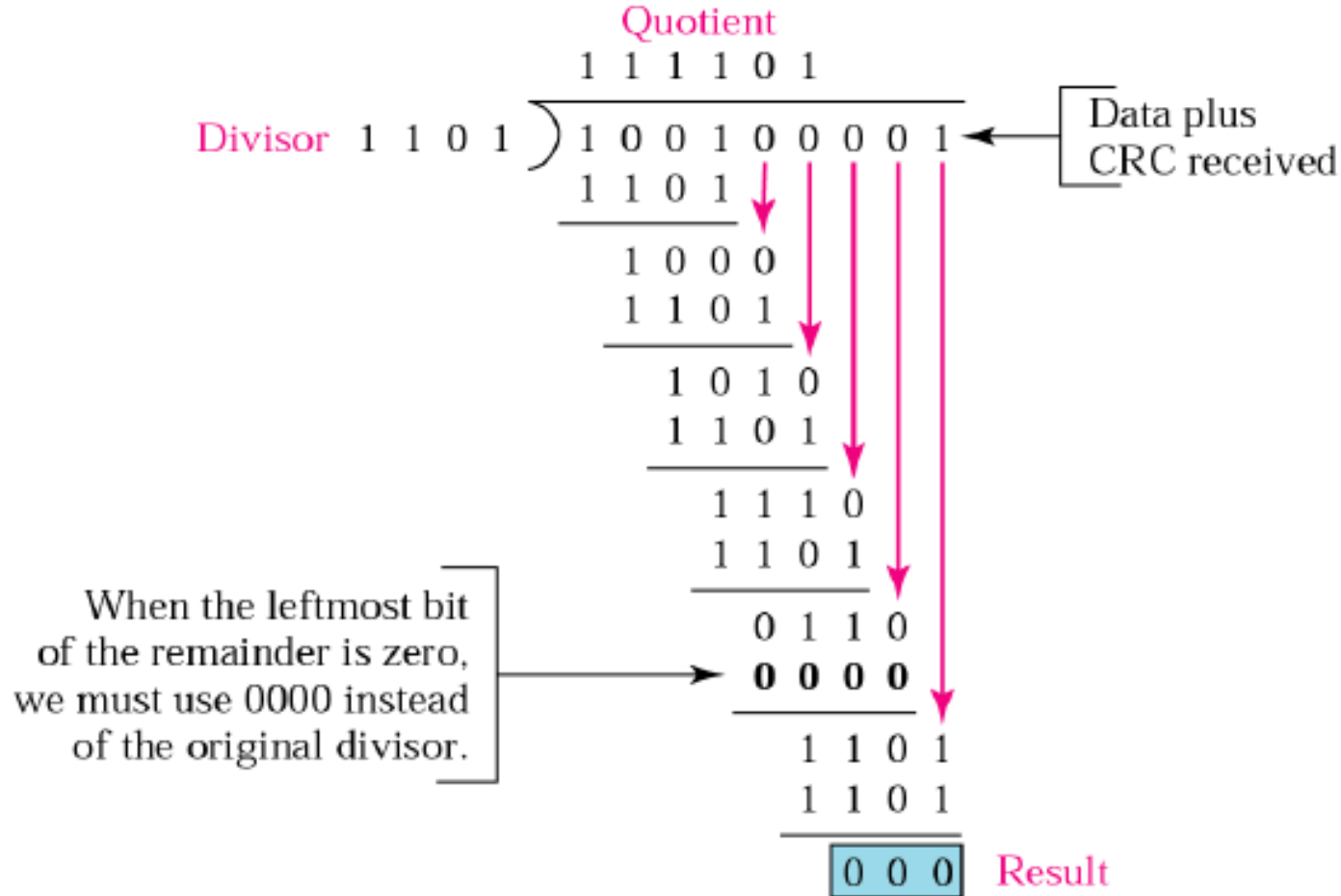
- The data or polynomial is appended with number of zeros equal to the degree of generator (divisor).
- The polynomial formed is divided by the divisor.
  - Modulo-2 division is used, i.e, XOR is used during division while subtracting
- The remainder of the division will be the value of CRC that will replace the data plus extra zeros i.e., remainder is added to the appended polynomial .
- This value is now transmitted to the receiver as the transmitted frame.
- At the receiver side, the data string and the CRC value is divided by the same value of divisor in the sender part.
- Then the remainder determines either to accept or reject the received data bit string.
  - If the remainder is zero, the data will be accepted else it will be rejected.

# CRC Encoding



**Figure : CRC Encoding or CRC Generator Example**

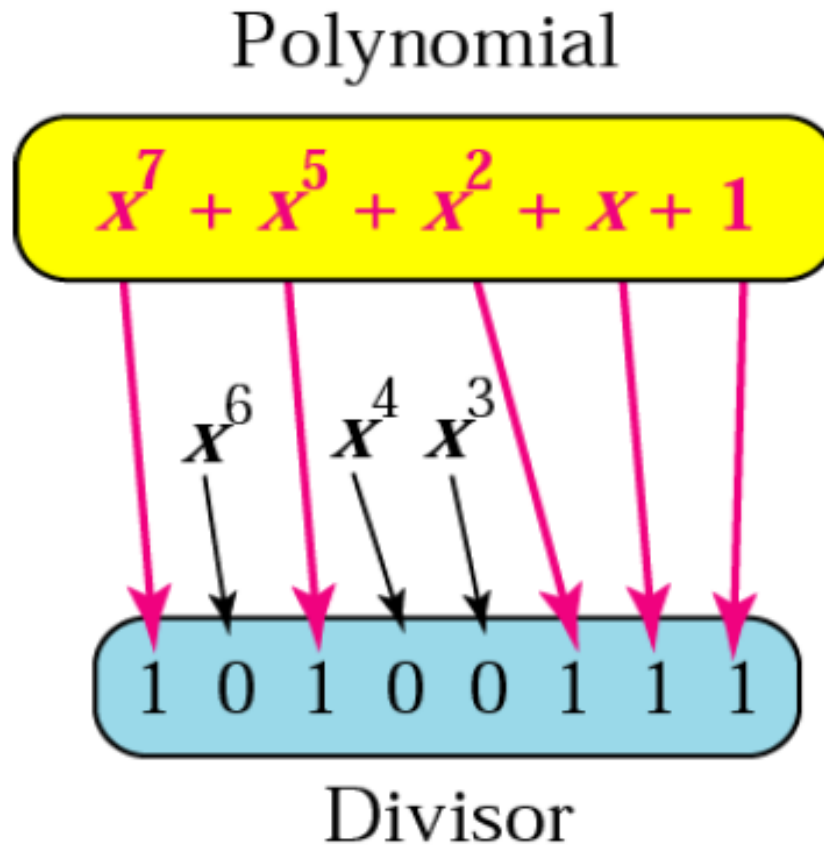
# CRC Decoding



**Figure : CRC Decoding or CRC Checker Example**

Note : 000 Remainder Indicates - No errors in Data during transmission

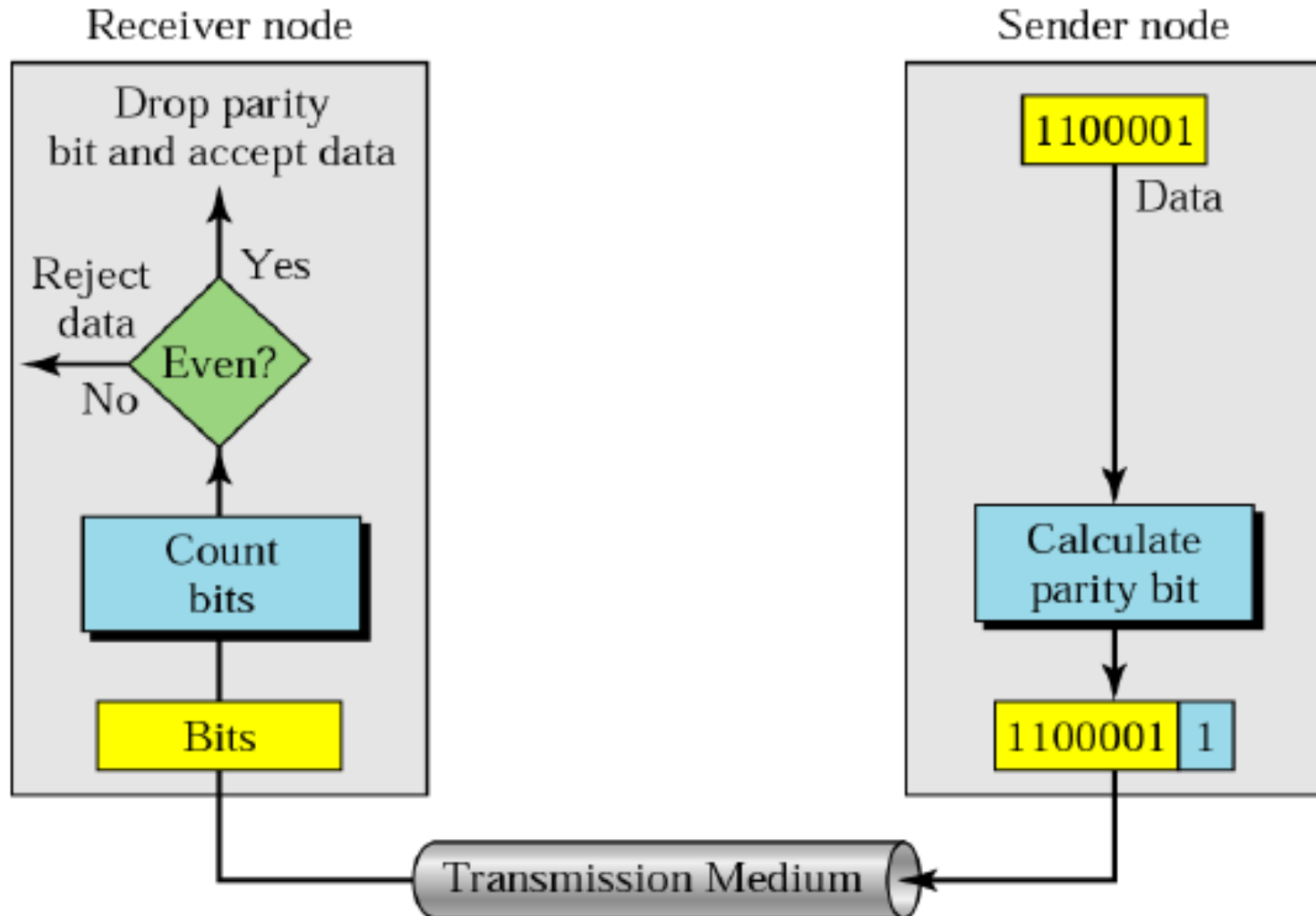
# Polynomial Representing Standard Divisor



# Standard Polynomials

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

# Parity Check :Even Parity

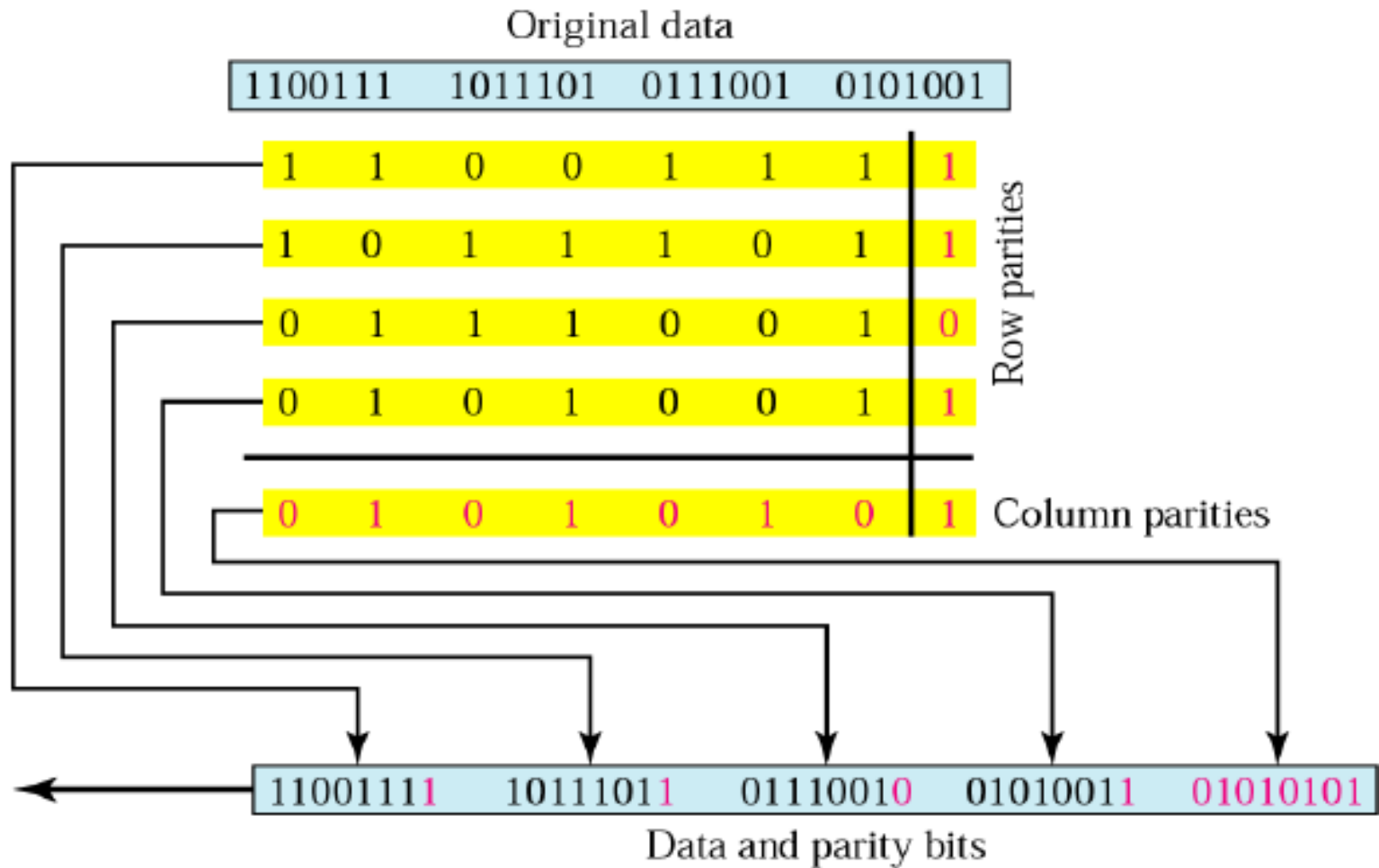


- Note: In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd-parity).
- ODD Parity : Class work

# Examples

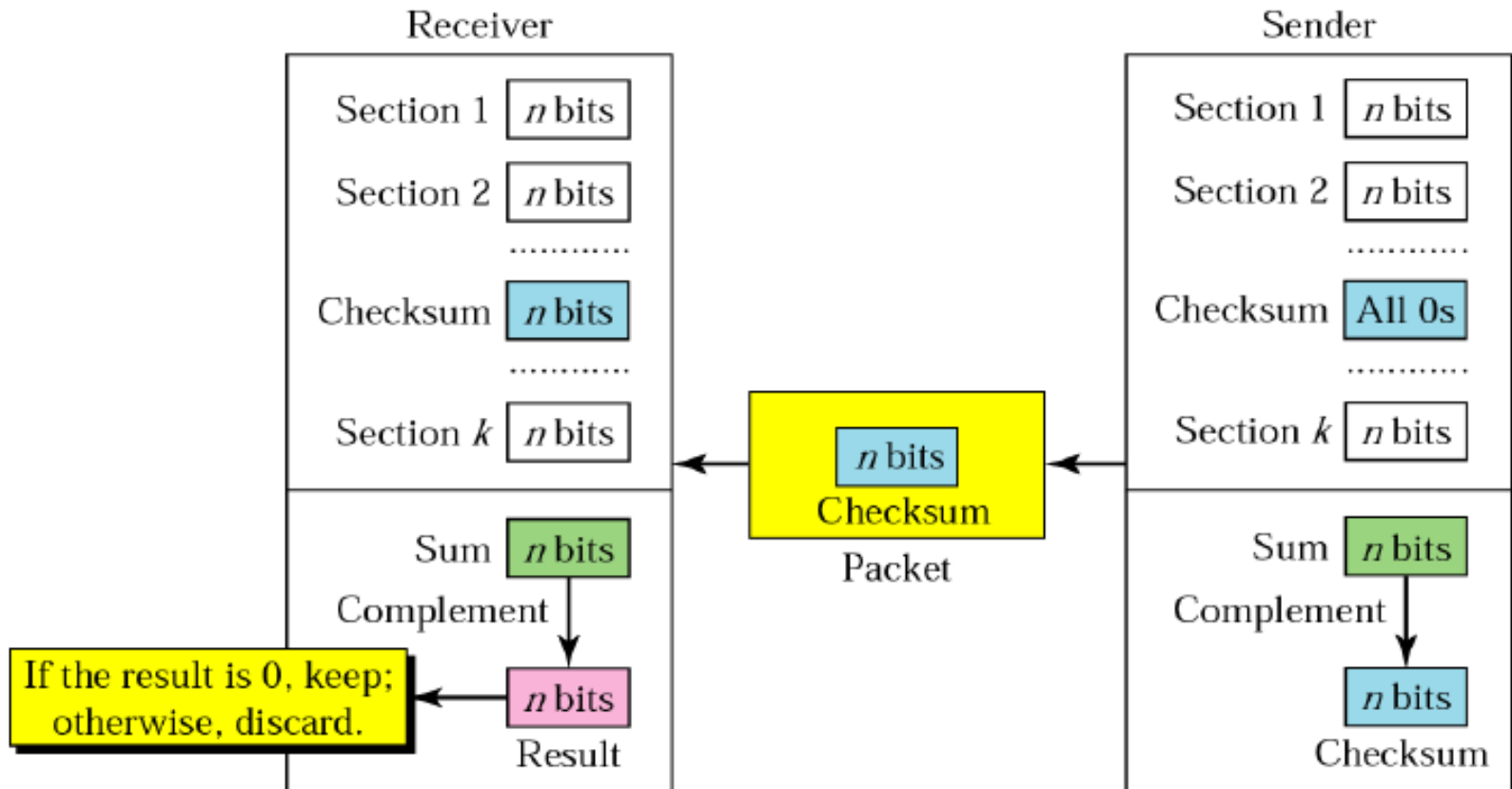
- Now suppose the word is received by the receiver without being corrupted in transmission.
  - 11101110 11011110 11100100 11011000 11001001
  - The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4, 4). The data are accepted.
- Now suppose the word is corrupted during 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



# Checksum

- The checksum is usually placed at the end of the message, as the complement of the sum function.
- This way, errors may be detected by summing the entire received codeword, both data bits and checksum.
- If the result comes out to be zero, no error has been detected



# 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

- Forward Error Control (FEC)
  - each block transmitted contains extra information which can be used to detect the presence of errors
  - and determine the position in the bit stream of the errors.
- Backward (Feedback) Error Control (BEC)
  - Also called Automatic Repeat Request (ARQ)
  - extra information is sufficient to only detect the presence of errors.
  - If necessary, a retransmission control scheme is used to request that another copy of the erroneous information be sent.

# Hamming Codes

## Steps for Hamming Codes

- An information of 'm' bits are added to the redundant bits to form 'm+r'
- The location of each 'm+r' is assigned a decimal value
- The 'r' bits are placed in the position  $2^0, 2^1, \dots, 2^{k-1}$
- At the receiving end parity bits are recalculated. The decimal value of parity bits determines the position of an error

## Hamming Distance:

- The number of bit positions in which two code words differ is called the Hamming distance ( $d$ ).
  - Example :  $W1=10001001$ ,  $W2=10110001$ , then  $d(W1, W2) = 3$
  - The minimum Hamming distance (or “minimum distance”) of the scheme is the *smallest number of bit errors that changes one valid codeword into another*
  - This scheme can detect any combination of  $\leq D-1$  bit errors and correct any combination of strictly less than  $D/2$  bit errors

suppose only 4 valid code words are:

- **00000 00000, 00000 11111, 11111 00000, and 11111 11111**
- Minimum distance is  $D=5$ , so any combination of  $\leq 4$  bit errors can be detected and any combination of  $\leq 2$  bit errors can be corrected, but 3 bit errors can't be properly corrected.
- If 00000 00000 transmitted,  $W=00000\ 00011$  received:  **$d(W, C1)=2$ ,  $d(W, C2)=3$ ,  $d(W, C3)=7$ , and  $d(W, C4)=8$  receiver takes  $C1=00000\ 00000$  as transmitted codeword (errors corrected)**
- If 00000 00000 transmitted,  $X=00000\ 00111$  received:  **$d(X, C1)=3$ ,  $d(X, C2)=2$ ,  $d(X, C3)=8$ , and  $d(X, C4)=7$  receiver takes  $C2=00000\ 11111$  as transmitted codeword (in this case, error correction fails)**

# Redundancy bit calculation in Hamming Code

$r_1$  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.

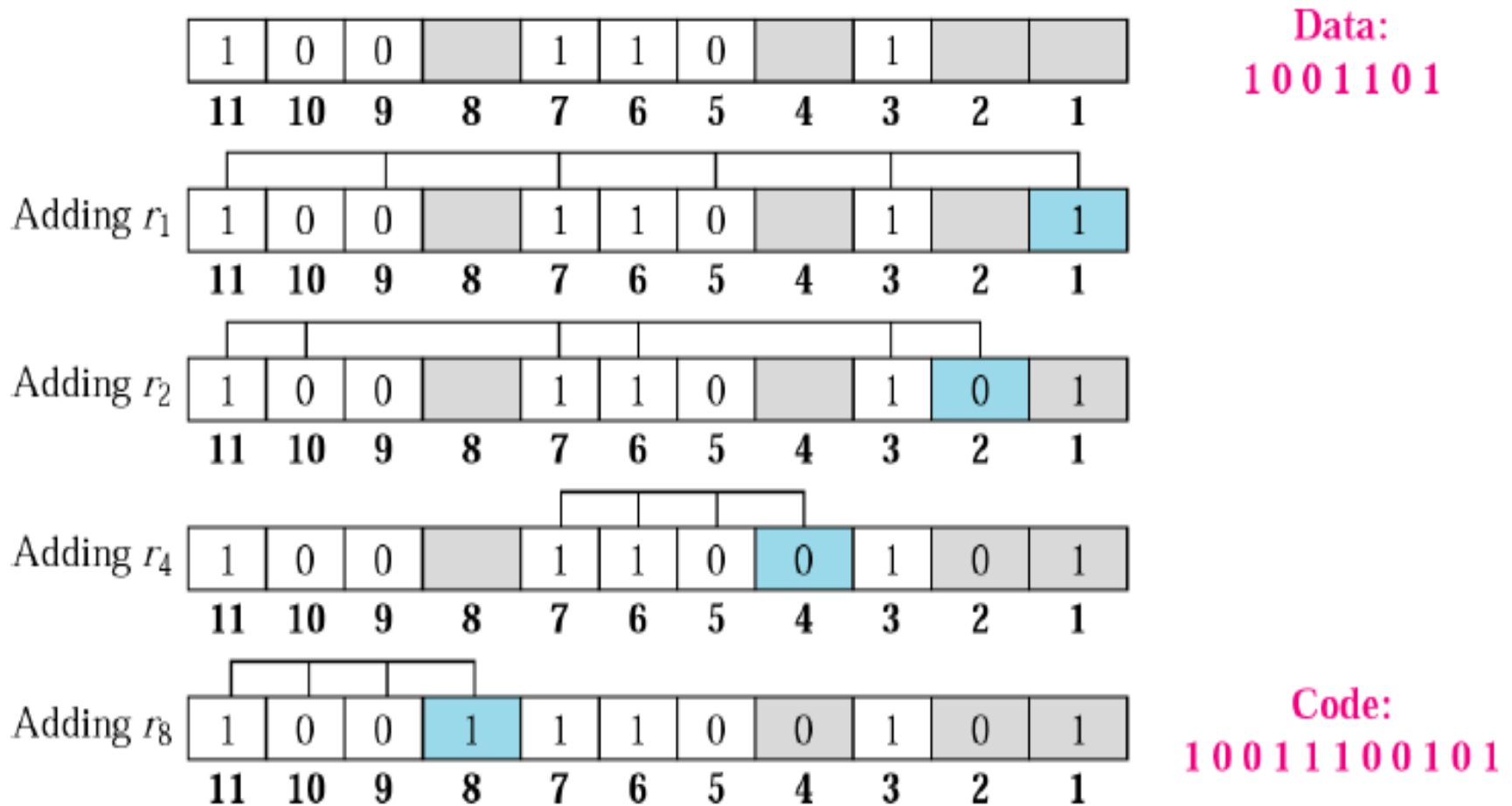
				7	6	5	4			
d	d	d	$r_8$	d	d	d	$r_4$	d	$r_2$	$r_1$

$r_8$  will take care of these bits.

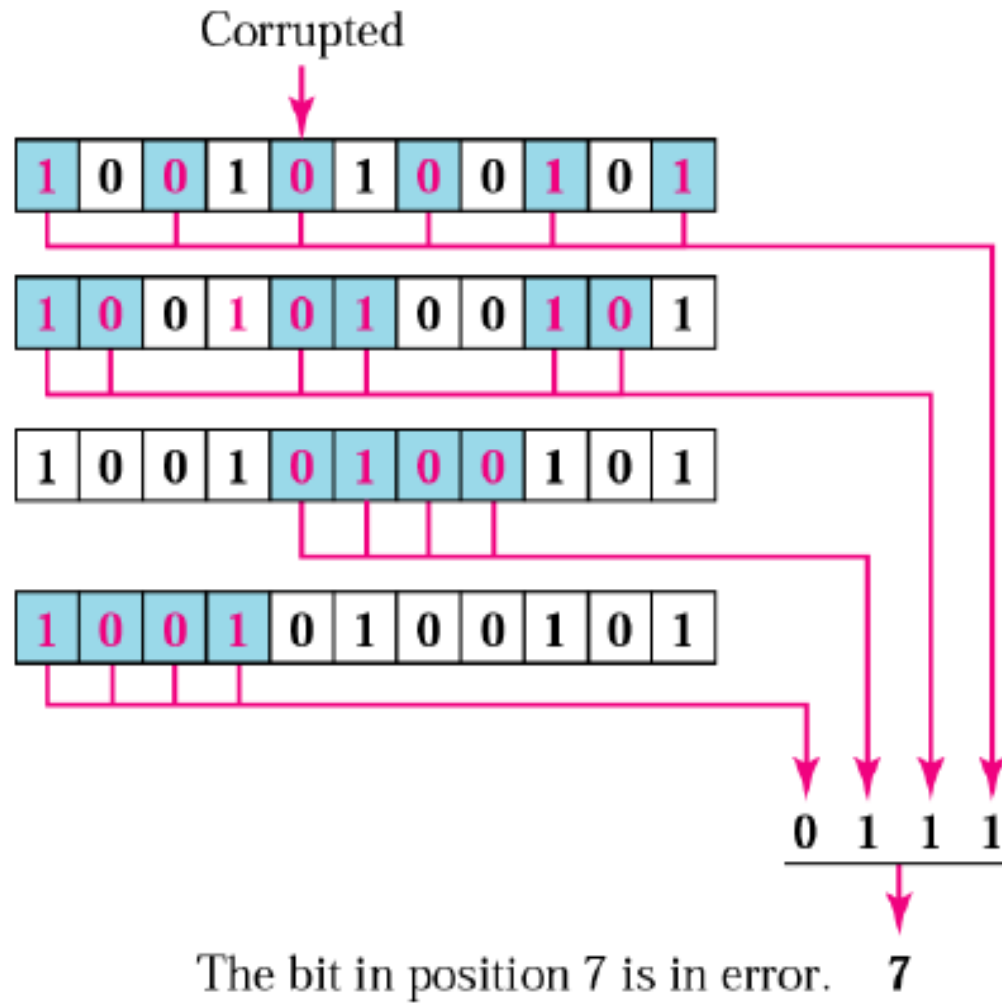
11	10	9	8							
d	d	d	$r_8$	d	d	d	$r_4$	d	$r_2$	$r_1$

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

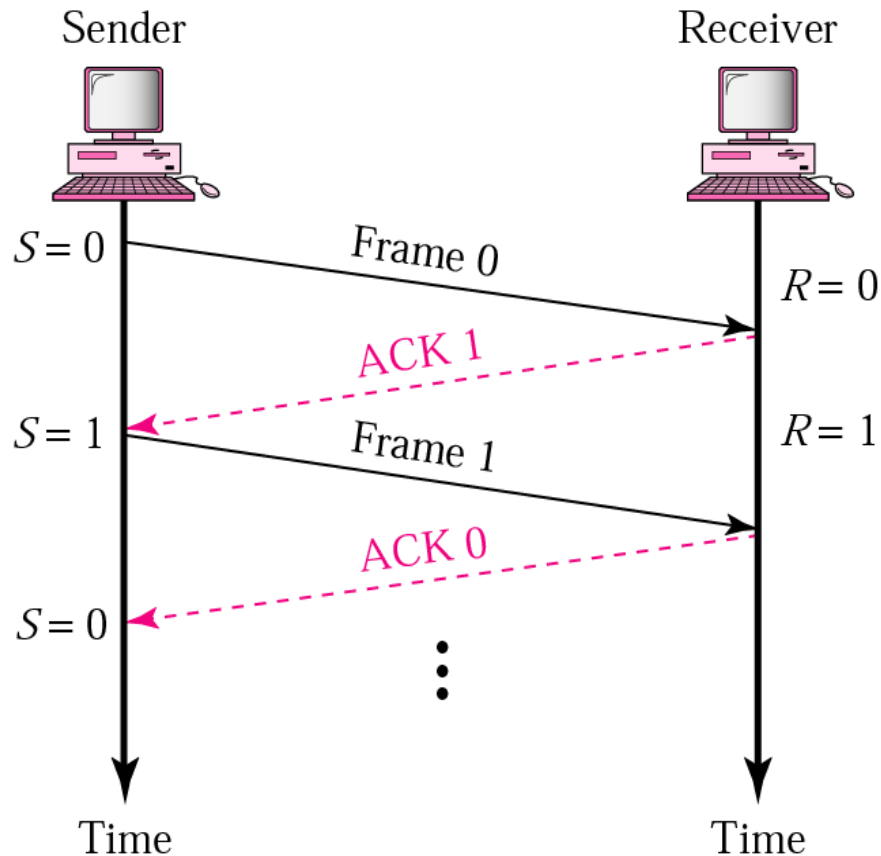
# Flow Control

- We must deal with the issue where the sender is sending data at a higher rate than the receiver can receive the data.
- There are two approaches to this problem:
  - feedback-based flow control
    - feedback is used to tell the sender how the receiver is doing **or** to send another frame
  - rate-based flow control
    - the transfer rate is fixed by the sender
    - this is not used often in the DLL

# Stop and Wait protocol

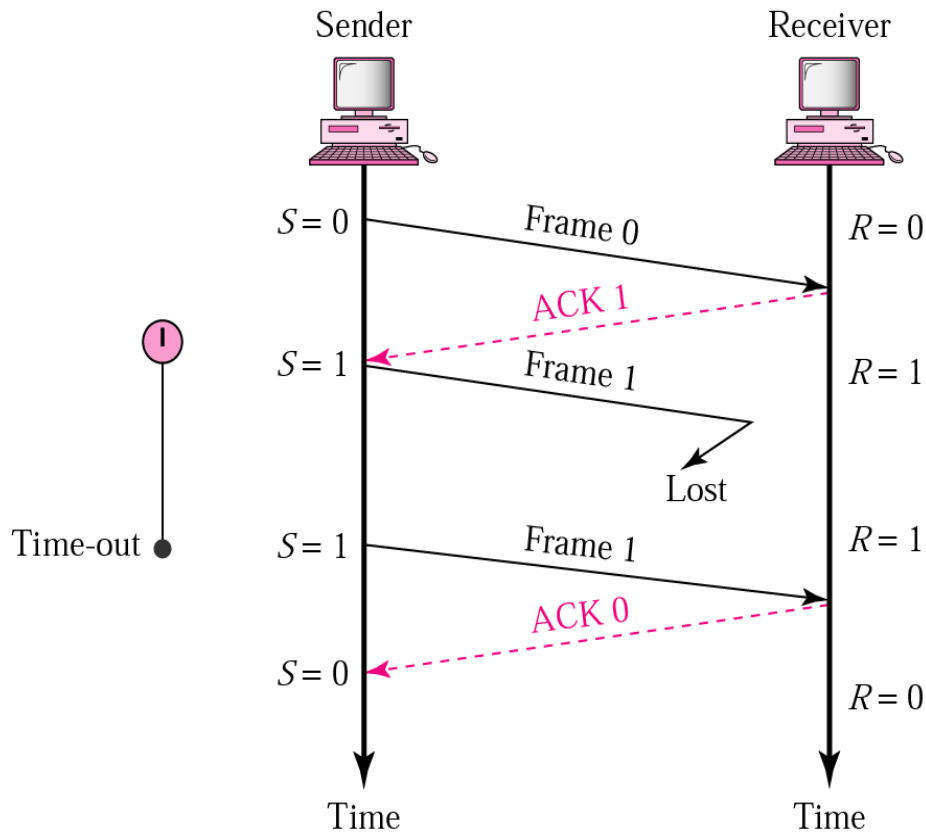
- If data frames arrive at the receiver site faster than they can be processed,
  - The frames must be stored until their use
  - Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources.
  - This may result in either the discarding of frames or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

# Stop and Wait: Normal Operation



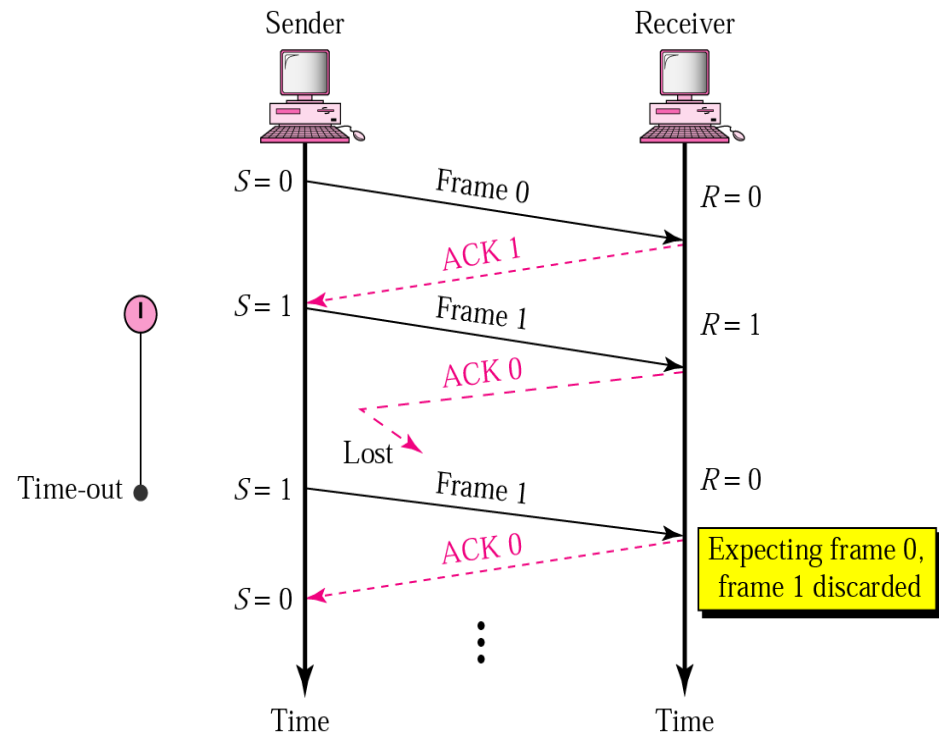
- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.
- Sender has a control variable ( $S$ ) that holds the number of the recently sent frame. (0 or 1)
- Receiver has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



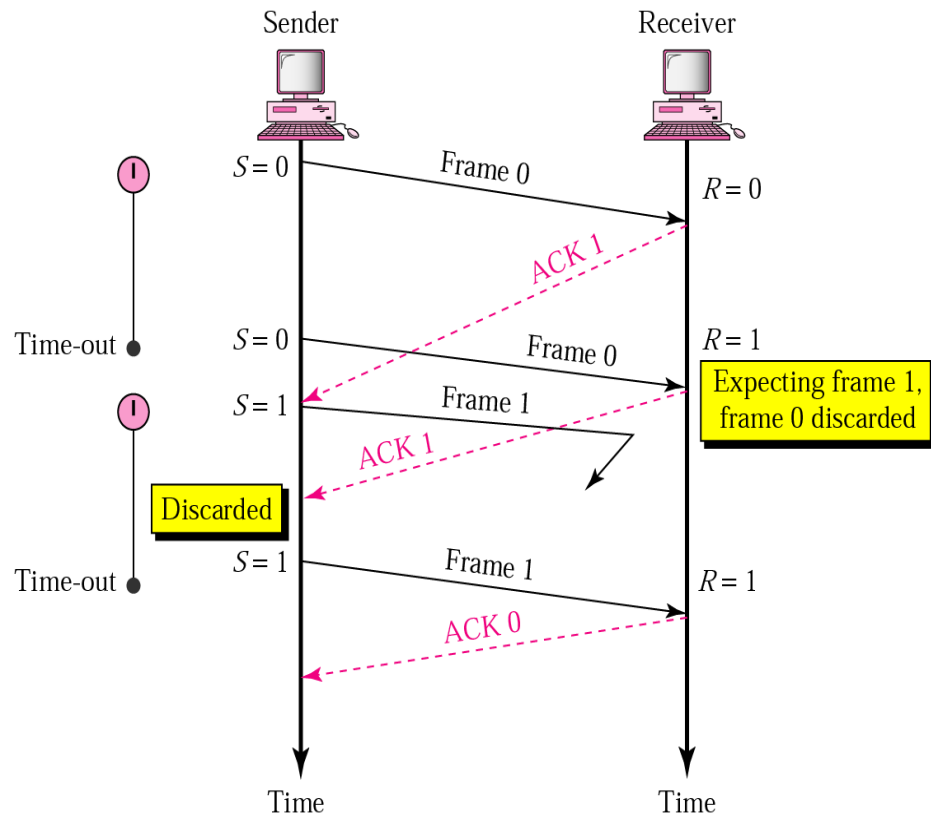
- When a receiver receives a damaged frame, it discards it and keeps its value of  $R$ .
- After the timer at the sender expires, another copy of frame 1 is sent.

# 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

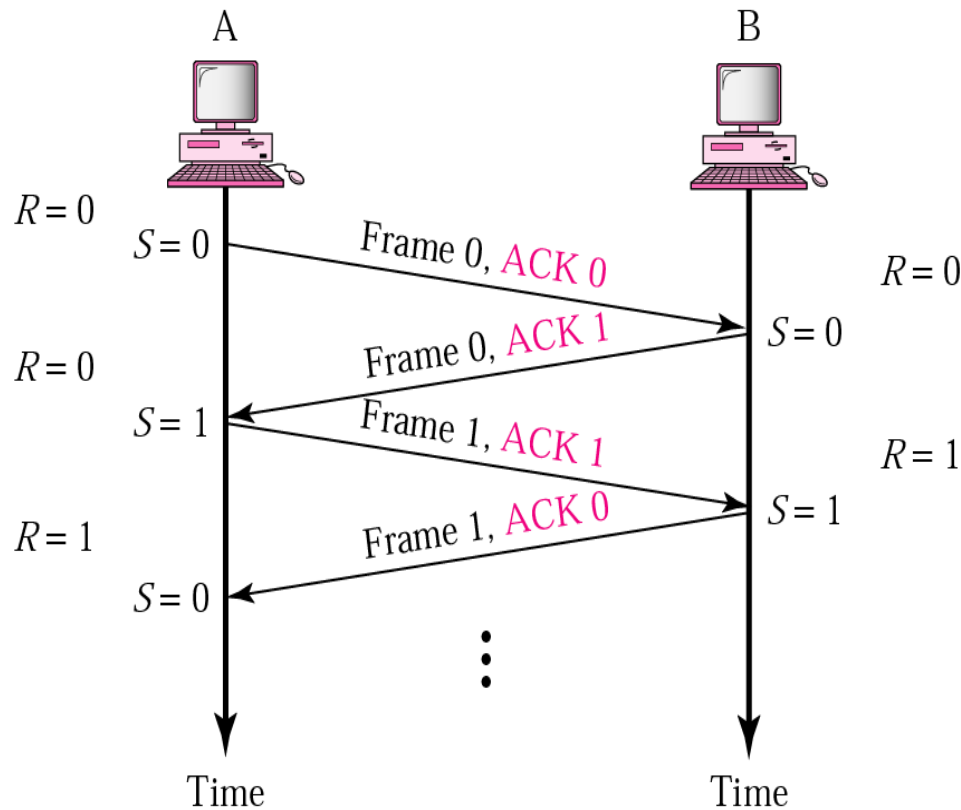


- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However,  $R=1$  means receiver expects to see frame 1. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

# 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.

# 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.

# Sliding Window Protocol - Sending

- The sender has a “window” of frames that it can be sending at any point in time.
- The larger the window, the more frames that it can have “on the go” at once.
- All of the frames in the window must be buffered in case one must be resent.
- The size of the sending window does not have to match the receiver, nor must it remain a constant size.

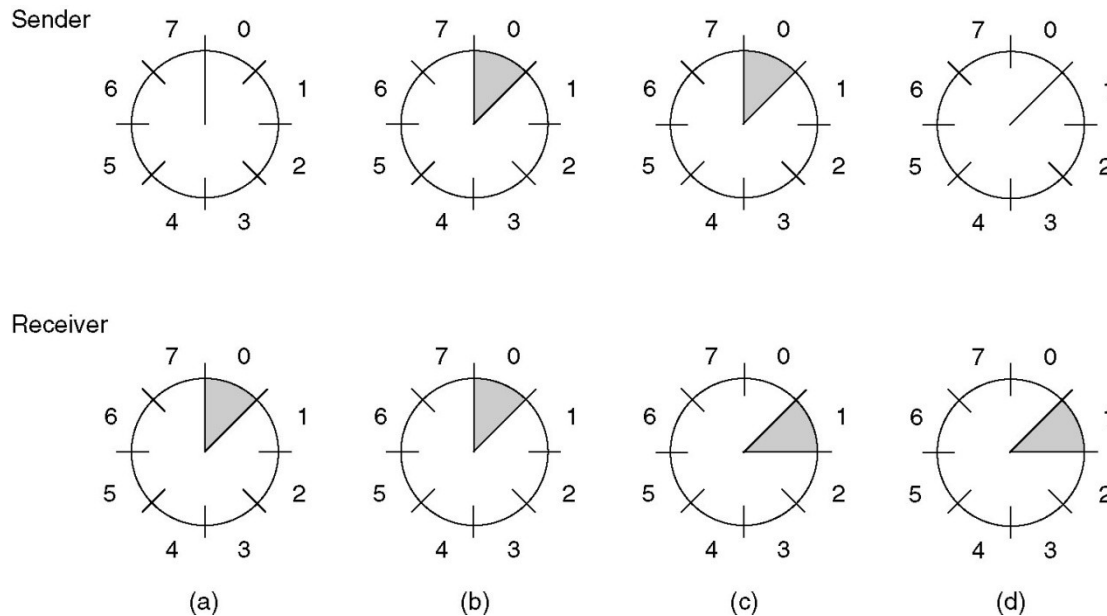
# Sliding Window - Receiving

- This is the window of frames that the receiver is allowed to receive at any point in time.
- A receiving window of 1 means that the frames must be received one-at-a-time and in order.
- A receiving window larger than 1 results in buffering of frames at the receiver end.
- Anything outside of the receiving window is automatically discarded.
- Anything inside the window can be accepted.

# Sliding Window - Receiving

- If the sequence number is equal to the lower edge of the window, then that frame is acknowledged and the packet passed to the network layer.
- Other buffered data, if it now has the sequence number of the lower edge of the window, will also be passed to the network layer.
- As the lower edge is received, the window moves.

# Sliding Window Protocols



A sliding window of size 1, with a 3-bit sequence number.

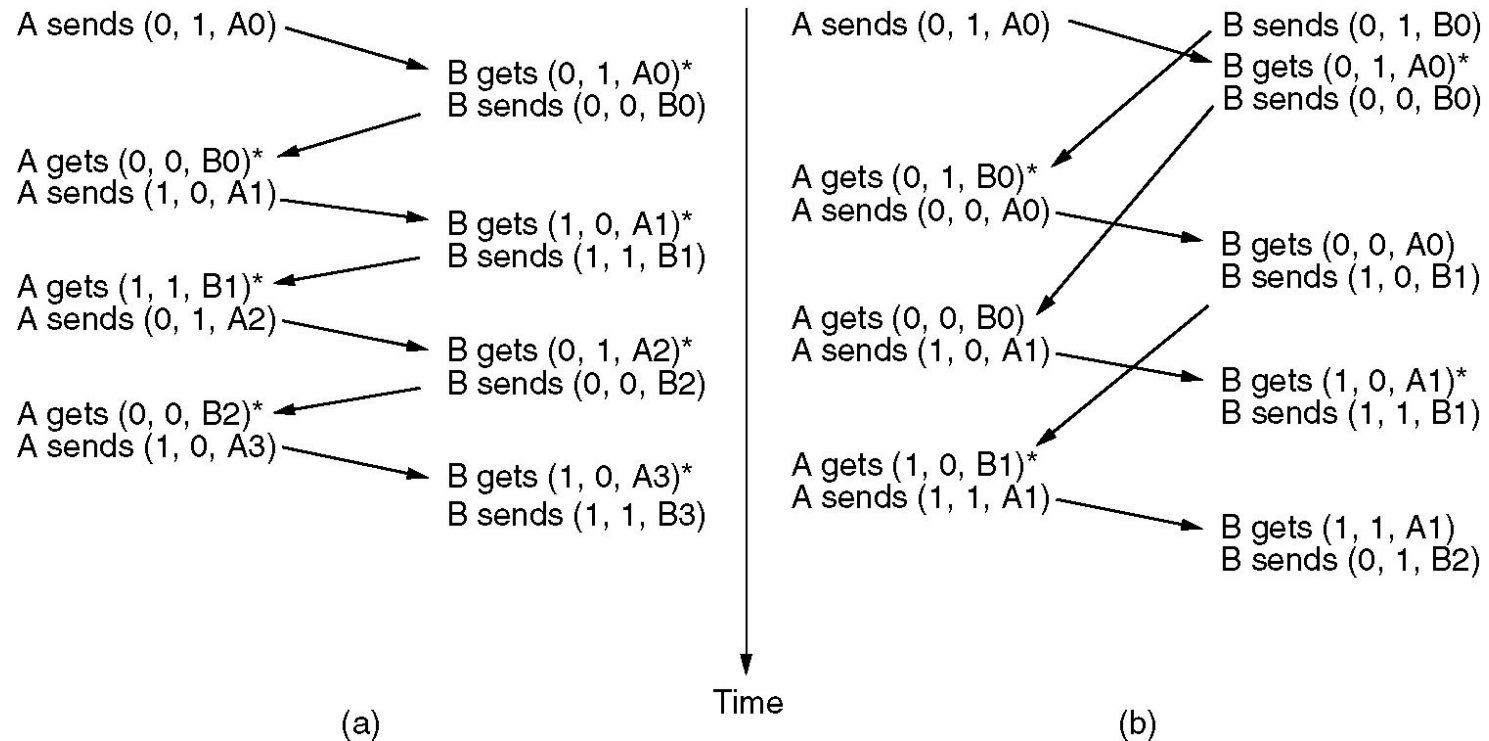
(a) Initially.

(b) After the first frame has been sent.

(c) After the first frame has been received.

(d) After the first acknowledgement has been received.

# One-Bit Sliding Window Protocol



Two scenarios for protocol 4. **(a)** Normal case. **(b)** Abnormal case. The notation is (seq, ack, packet number). An asterisk indicates where a network layer accepts a packet.

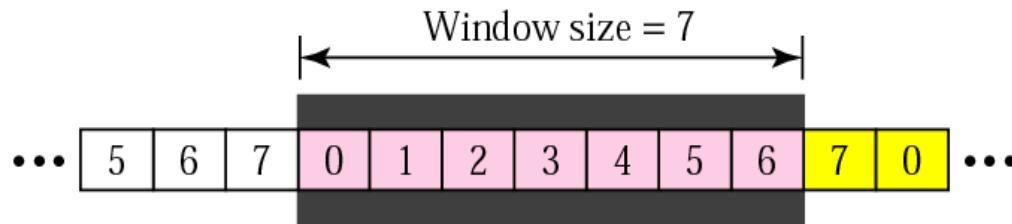
# Go-Back-N ARQ

- 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
- In case of lost or corrupt frame, retransmit from lost frame

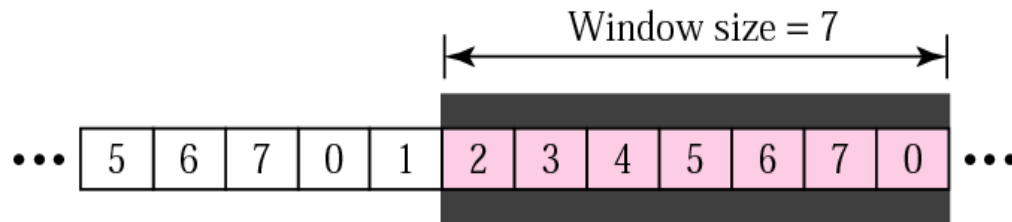
# Sequence Number

- 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



a. Before sliding

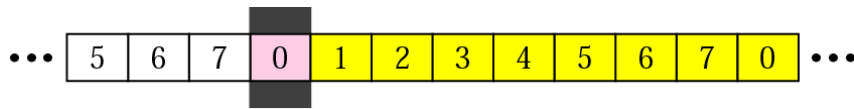


b. After sliding two frames

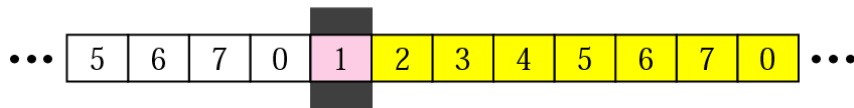
- Sliding window Define the range of Sequences Number
- Here Sender Sliding window define the window size=7
- Total Number of Frames that can be sent without receiving ACKs is 7

# Go-Back-N ARQ : Receiver sliding window

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



a. Before sliding

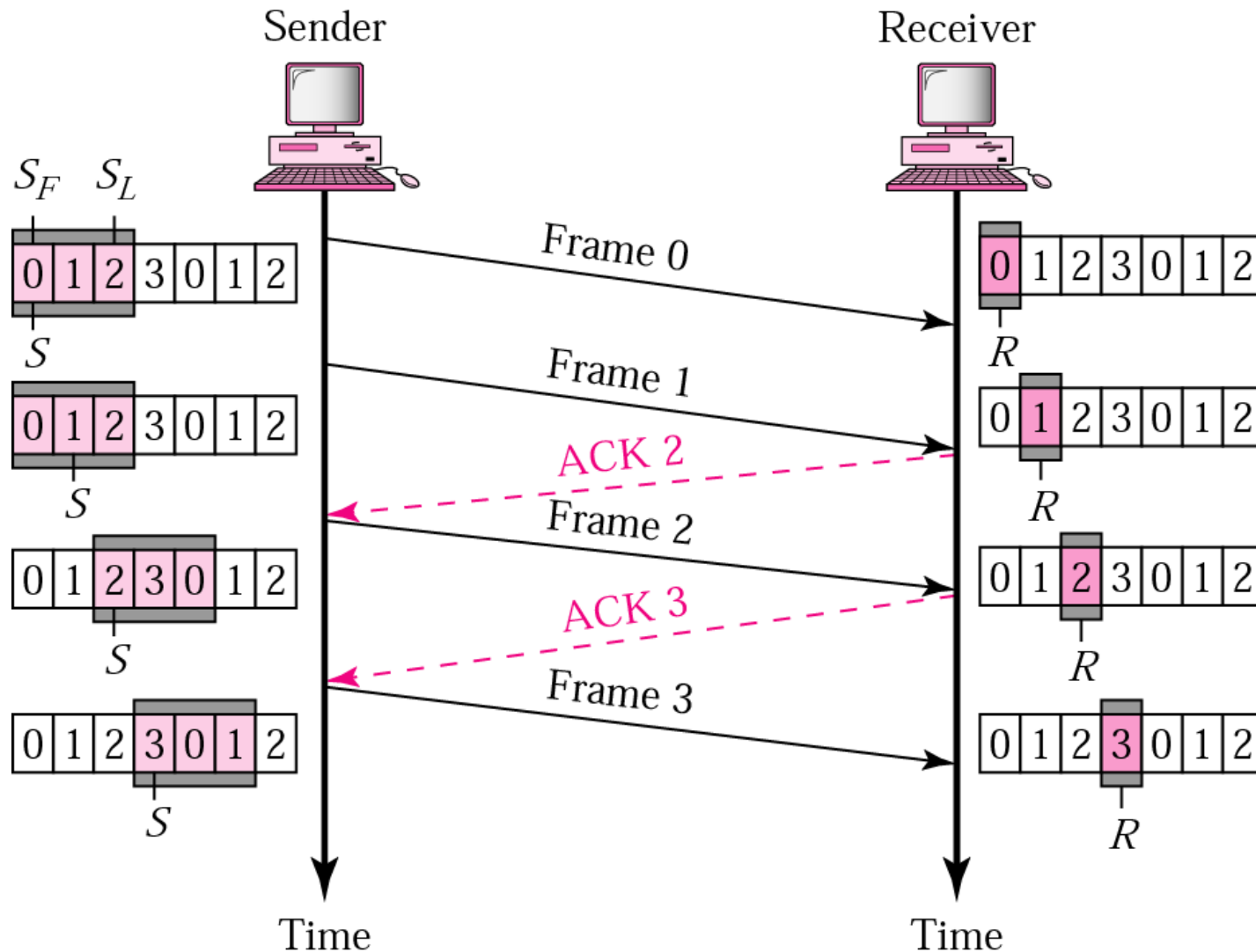


b. After sliding

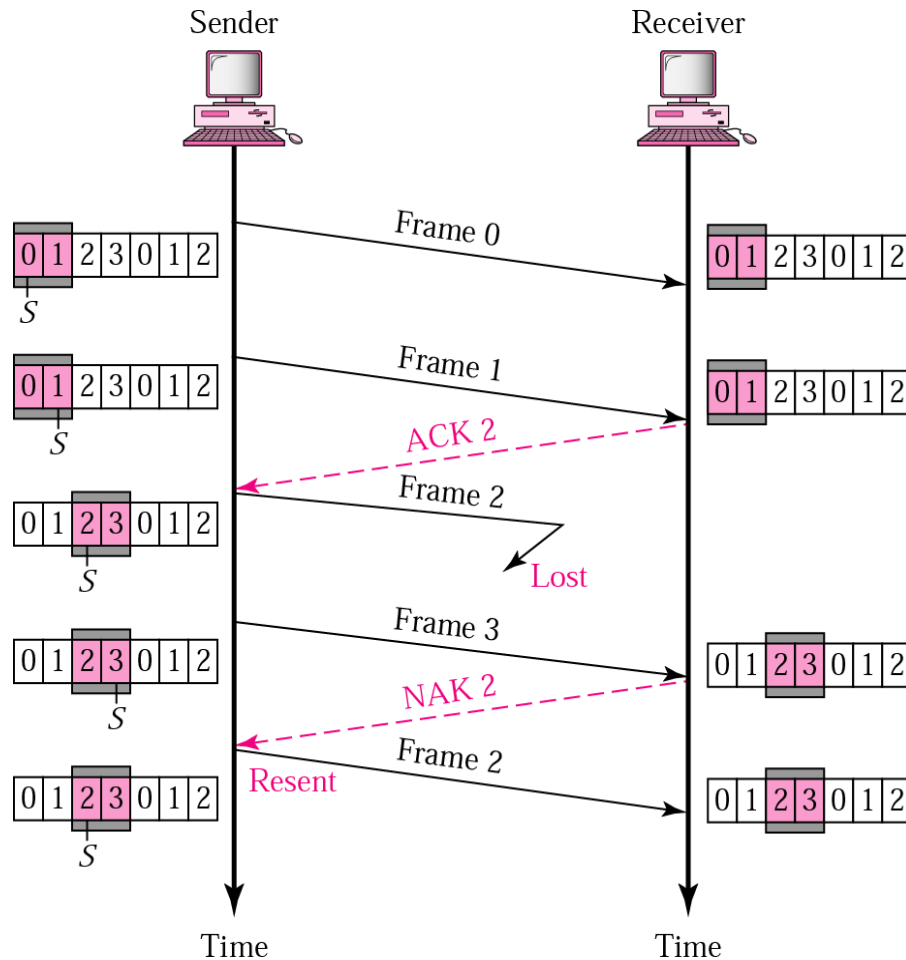
# Control Variables

- 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



# Selective Repeat Request



*Fig: Selective Repeat Request, lost frame*

- Sometimes also called Selective Reject ARQ (SREJ)
- Only retransmit frames that are lost
  - Negative acknowledgment NAK (SREJ)
  - Time out
- 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 Send window and Receive window are Same

# Pipelining and a Bad Frame

- **Pipelining** is the process of putting multiple frames on the connection without receiving any acks for them. Assuming that they all arrive safely, it is much faster than sending them with **stop-and-wait**.
- What happens when we get a bad frame?
- **Go back N** – Ask the sender to go back and start retransmitting from the lost frame.
- **Selective repeat** – Ask the sender to repeat the particular frames that were lost.

# Overlapping Windows

- We have to make sure that there is no overlap between the two windows that may cause error. Error can occur when retransmitted frames can look like new frames.
- To ensure there is no overlap, the number of frames should be, at most,  $\frac{1}{2}$  of the range of sequence numbers.

# Example Data Link Protocol

- IBM introduced **SDLC** – Synchronous Data Link Control – and submitted it to ANSI and ISO for acceptance as US and International standards.
- ANSI modified it to be **ADCCP** – Advanced Data Communication Control Procedure
- ISO modified it to be **HDLC** – High-level Data Link Control.

# HDLC

- Most widely used data link control protocol
- Bit oriented protocol using bit stuffing
- Supports half and full duplex communication over point-to-point and multipoint links.
- HDLC Defines :
  - Three types of stations,
  - Two link configurations and
  - Three data transfer modes

# Station Types

- **Primary station**
  - Responsible to control the operation of link
  - Frames issued by primary are called commands
- **Secondary station**
  - Operates under control of primary
  - Frames issued by secondary are called responses
- **Combined station**
  - A combination of above
  - Issues commands and responses

# Link Configurations

- Unbalanced
  - Consists of one primary and one or many secondary stations
  - Primary is responsible for controlling secondary
  - Primary maintains and establishes link and responsible for error recovery
- Balanced
  - Consists of two combined stations
  - Can be used on point to point lines only
  - Stations are peer and share equal responsibility for error recovery and line management

# Data Transfer Modes

- **Normal Response Mode (NRM)**
  - Used with unbalanced configuration
  - Primary may initiate data transfer
  - Secondary can transmit data only as a response
  - Used on point-to-point and multi-point links
- **Asynchronous Response Mode (ARM)**
  - Used with unbalanced configuration
  - Secondary station may initiate data transfer without explicit permission from the primary. Primary still responsible for overall control
  - Rarely used

- **Asynchronous Balanced Mode (ABM)**
  - Used with balanced configuration
  - Any combined station may initiate data transfer without permission from the other
  - Most widely used because more efficient on full duplex point to-point link

# HDLC Frame format



## HDLC Frame Types



- **Information Frames (I-Frame)**

Used to transmit user data and control info

- **Supervisory Frames (S-Frame)**

Used to transmit only control info

- **Un-numbered Frames (U-Frame)**

Reserved for system maintenance (link management)

# PPP

- It is the most commonly used data link protocol.
- It is used to connect the home PC to the ISP server.
- It provides error detection.
- It defines Link Control Protocol (LCP) for:
  - Establishing the link between two devices.
  - Maintaining this established link.
  - Configuring this link.
  - Terminating this link after the transfer.

# PPP : Frame Format

01111110	11111111	00000011				01111110
Flag	Address	Control	Protocol	Information	FCS	Flag
1 Byte	1 Byte	1 Byte	1 or 2 Byte	Variable	2 or 4 Byte	1 Byte

**Flag Field:** It marks the beginning and end of the PPP frame. Flag byte is 01111110.

**Address:** 11111111, which means all stations can accept the frame

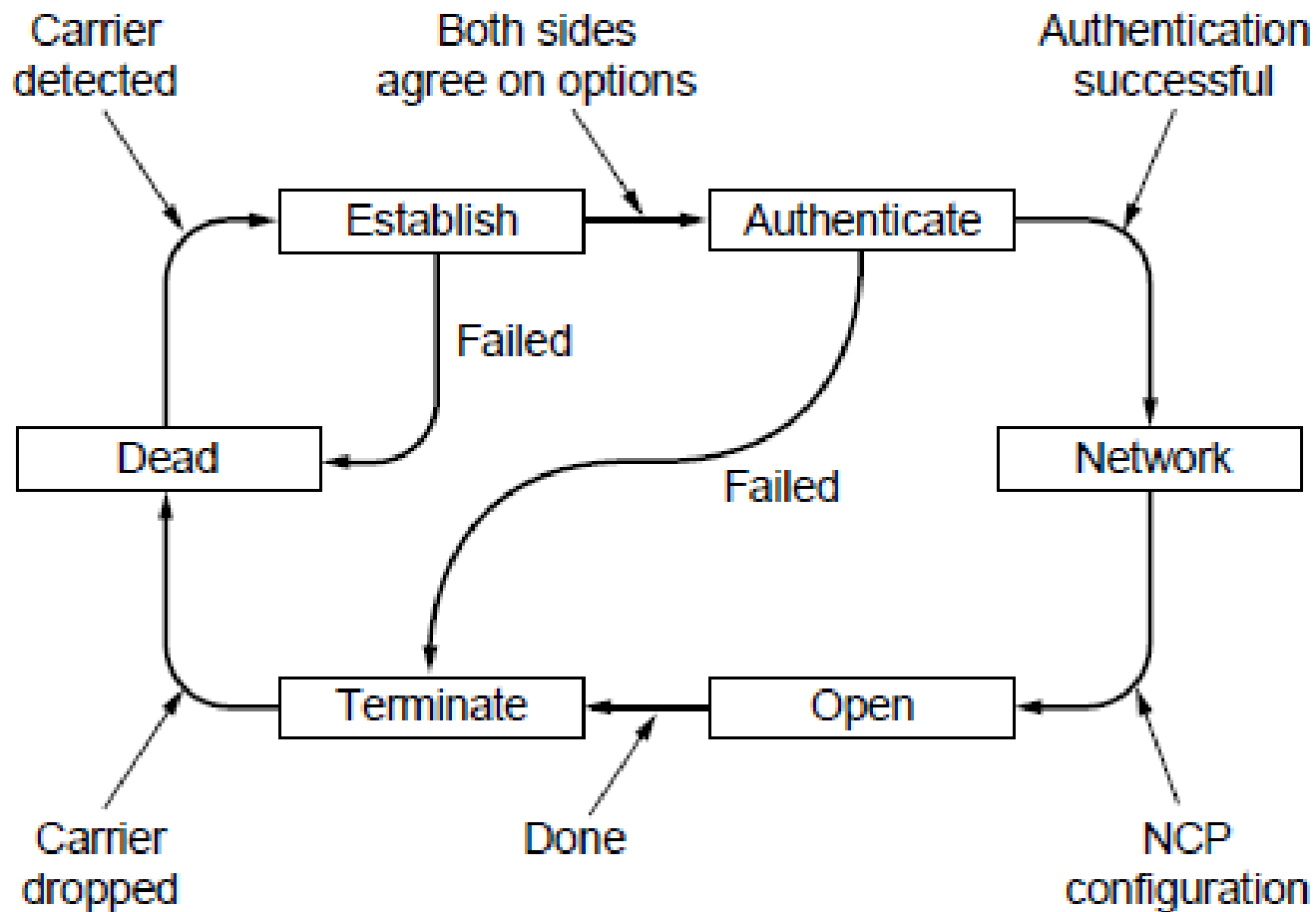
**Control Field:** It is also of 1 byte. The value is always 00000011 to show that the frame does not contain any sequence number and there is no flow control or error control

**Protocol field:** tells what kind of packet is in payload

**Information Field:** Its length is variable. It carries user data or other information.

**FCS Field:** It stands for Frame Check Sequence. It contains checksum. It is either 2 bytes or 4 bytes.

# PPP : Operation/Phases



# PPP Contd..

- PPP uses several other protocols to establish link, authenticate users and to carry the network layer data:
- The various protocols used are:
  - Link Control Protocol
  - Authentication Protocol
  - Network Control Protocol

## **Link Control Protocol**

- It is responsible for establishing, maintaining, configuring and terminating the link.

## **Authentication Protocol**

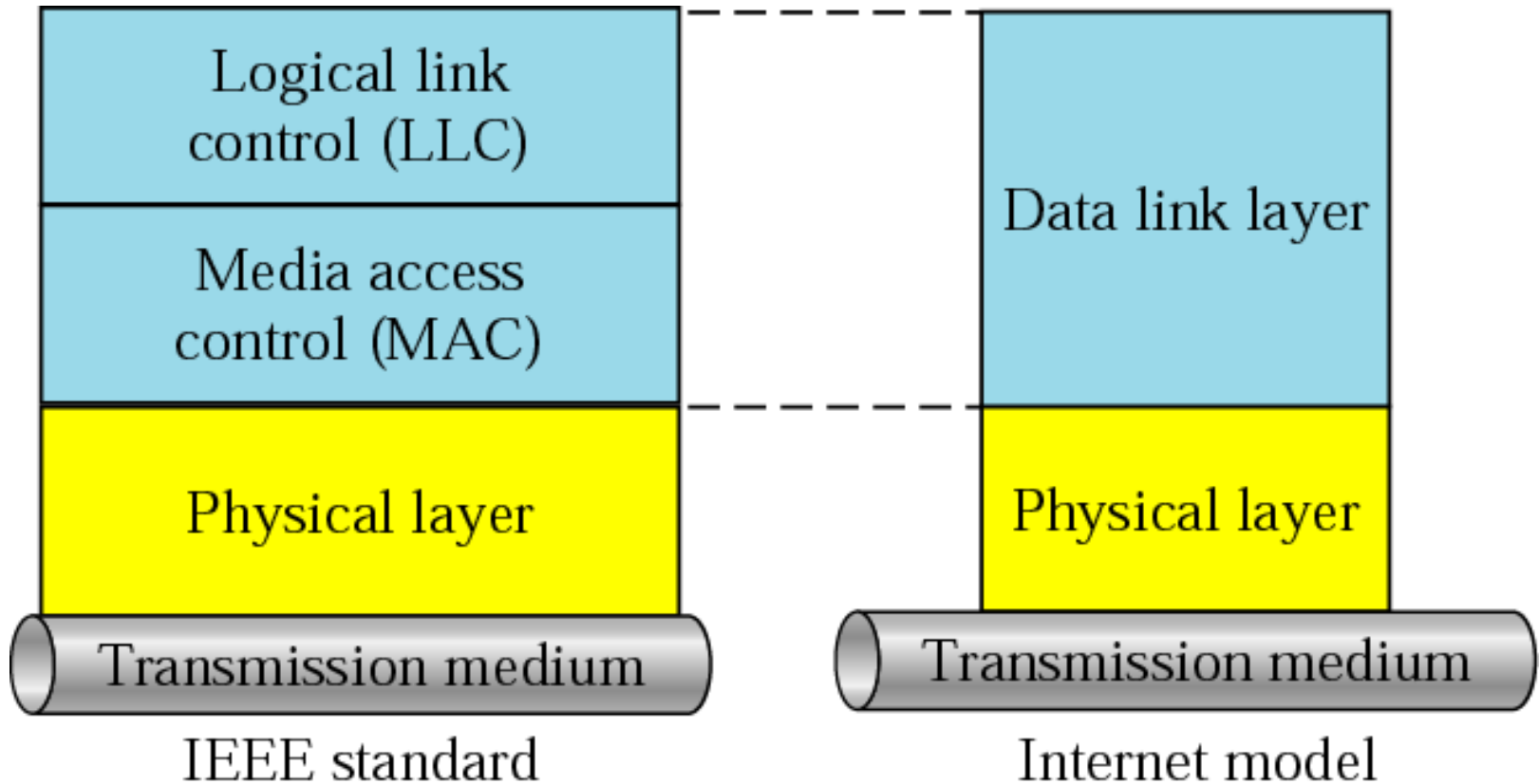
- Authentication protocol helps to validate the identity of a user who needs to access the resources.

## **Network Control Protocol (NCP)**

- After establishing the link & authenticating the user, PPP connects to the network layer.
- This connection is established by NCP.
- Therefore, NCP is a set of control protocols that allow the encapsulation of the data coming from the network layer.
- After the network layer configuration is done by one of the NCP, the user can exchange data from the network layer.

# The Medium Access Control Sub-layer

- LLC and MAC SubLayer Overview



# 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 control
- The LLC sub-layer acts as an interface between the media access control (MAC) sub-layer and the network layer

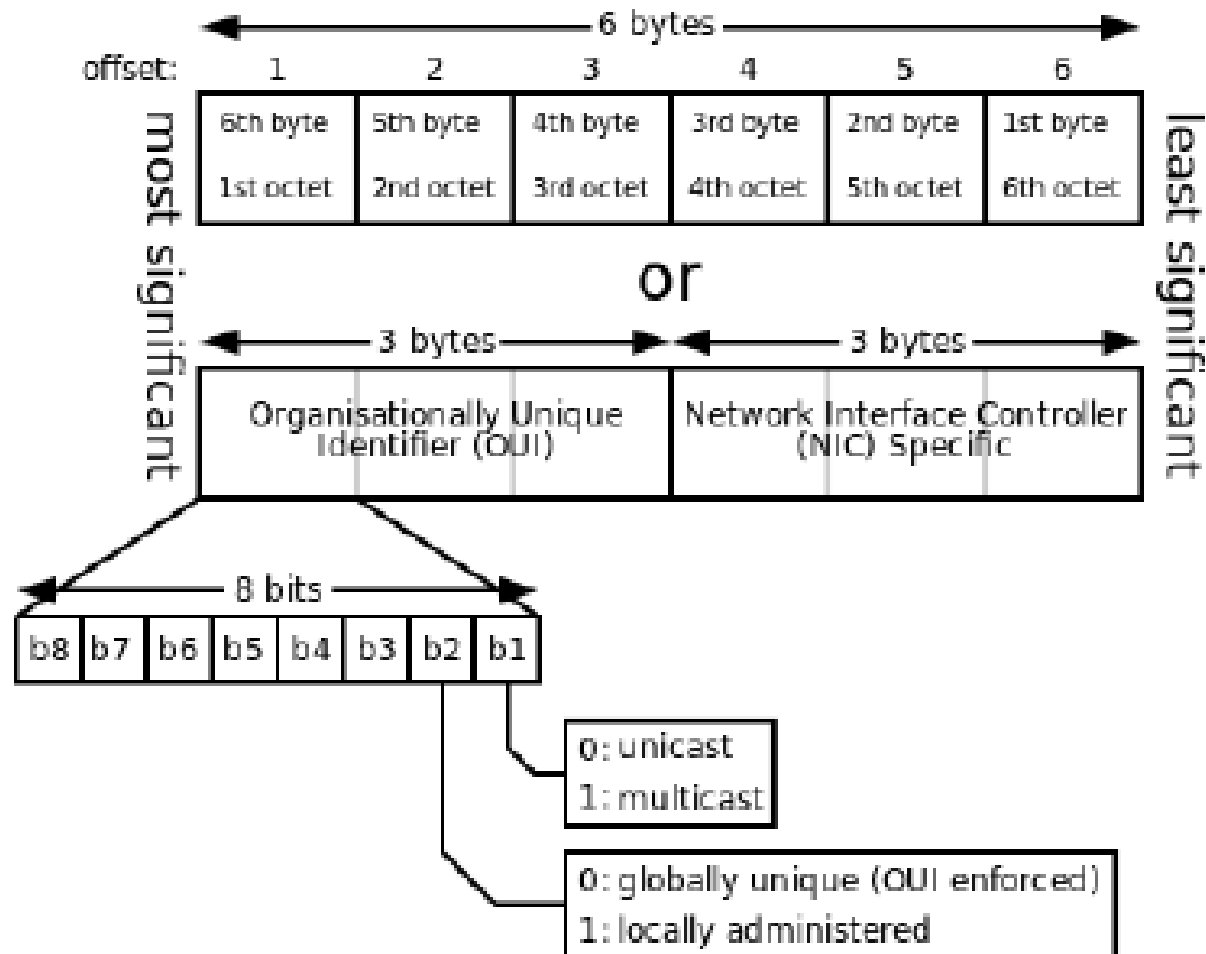
# Media Access Control

- Provides addressing and channel access control mechanisms
- Functions performed in the MAC sub-layer
  - End Devices Addressing Mechanism
    - Using physical address
- Channel access control mechanism
  - CSMA/CD, CSMA/CA

# 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
  - Lower 3 bytes represent the Device ID

# MAC contd..



# The channel allocation problem

- In broadcast networks, single channel is shared by several stations.
- This channel can be allocated to only one transmitting user at a time.
- There are two different methods of channel Allocations:
  - Static Channel Allocation
  - Dynamic Channel Allocation

# Static Channel Allocation

- In this method, a single channel is divided among various users either on the basis of frequency or on the basis of time.
- It either uses FDM (Frequency Division Multiplexing) or TDM (Time Division Multiplexing).
- In FDM, fixed frequency is assigned to each user, whereas, in TDM, fixed time slot is assigned to each user.

# Dynamic Channel Allocation

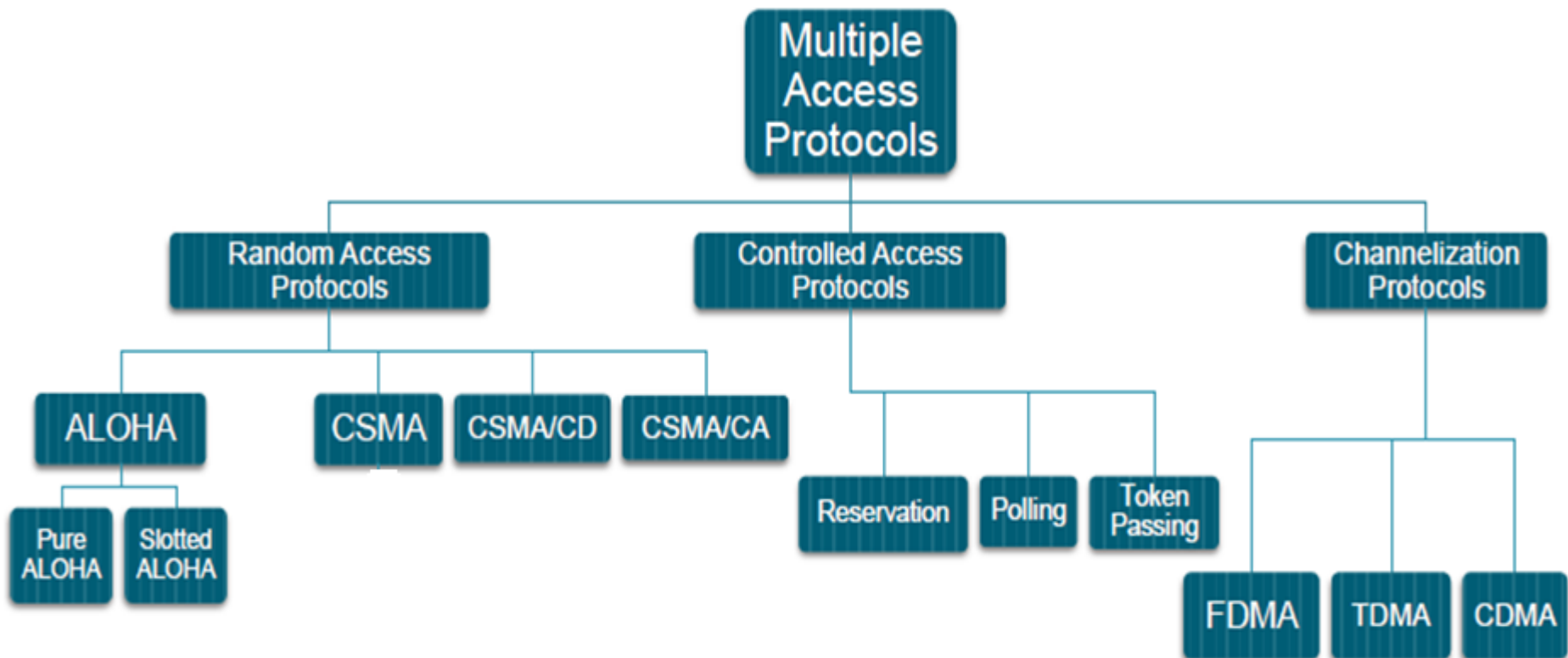
- In this method, no user is assigned fixed frequency or fixed time slot.
- All users are dynamically assigned frequency or time slot, depending upon the requirements of the user.

## Assumptions for Dynamic Channel Allocation

1. Independent traffic: independent stations
2. Single channel: available for all communication. All stations can transmit/receive on/from it. The stations are equally capable.
3. Observable Collisions: All stations can detect a collision.
4. Continuous or slotted time (for transmission)
5. Carrier sense or no carrier sense: With carrier sense, stations can tell if the channel is in use before trying to use it.

# Multiple Access Protocols

- Distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit



# Random Access Protocols

- In this method, there is no control station.
- Any station can send the data.
- There is no scheduled time for a stations to transmit. They can transmit in random order.
- The various random access methods are:
  - ALOHA
  - CSMA (Carrier Sense Multiple Access)
  - CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  - CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

# ALOHA

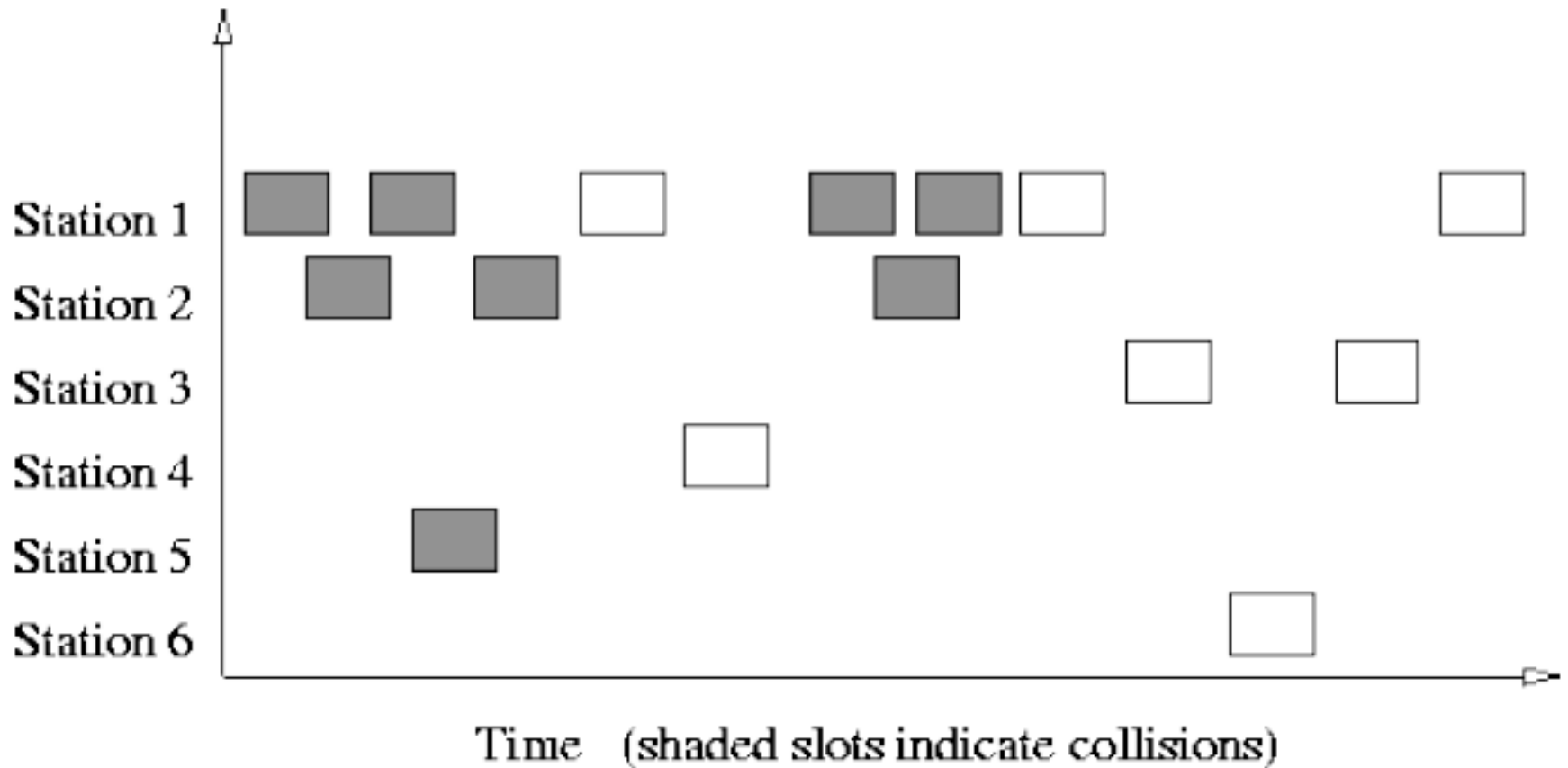
- Any terminal is allowed to transmit without considering whether channel is idle or busy
- If packet is received correctly, the base station transmits an acknowledgement.
- If no acknowledgement is received,
  - it assumes the packet to be lost
  - it retransmits the packet after waiting a *random time*
- There are two different versions of ALOHA:
  - Pure ALOHA
  - Slotted ALOHA

# Pure ALOHA

- In pure ALOHA, stations transmit frames whenever they have data to send.
- When two stations transmit simultaneously, there is collision and frames are lost.
- In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame has been lost.

- If the frame is lost, station waits for a random amount of time and sends it again.
- This waiting time must be random, otherwise, same frames will collide again and again.
- Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost.
- If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.

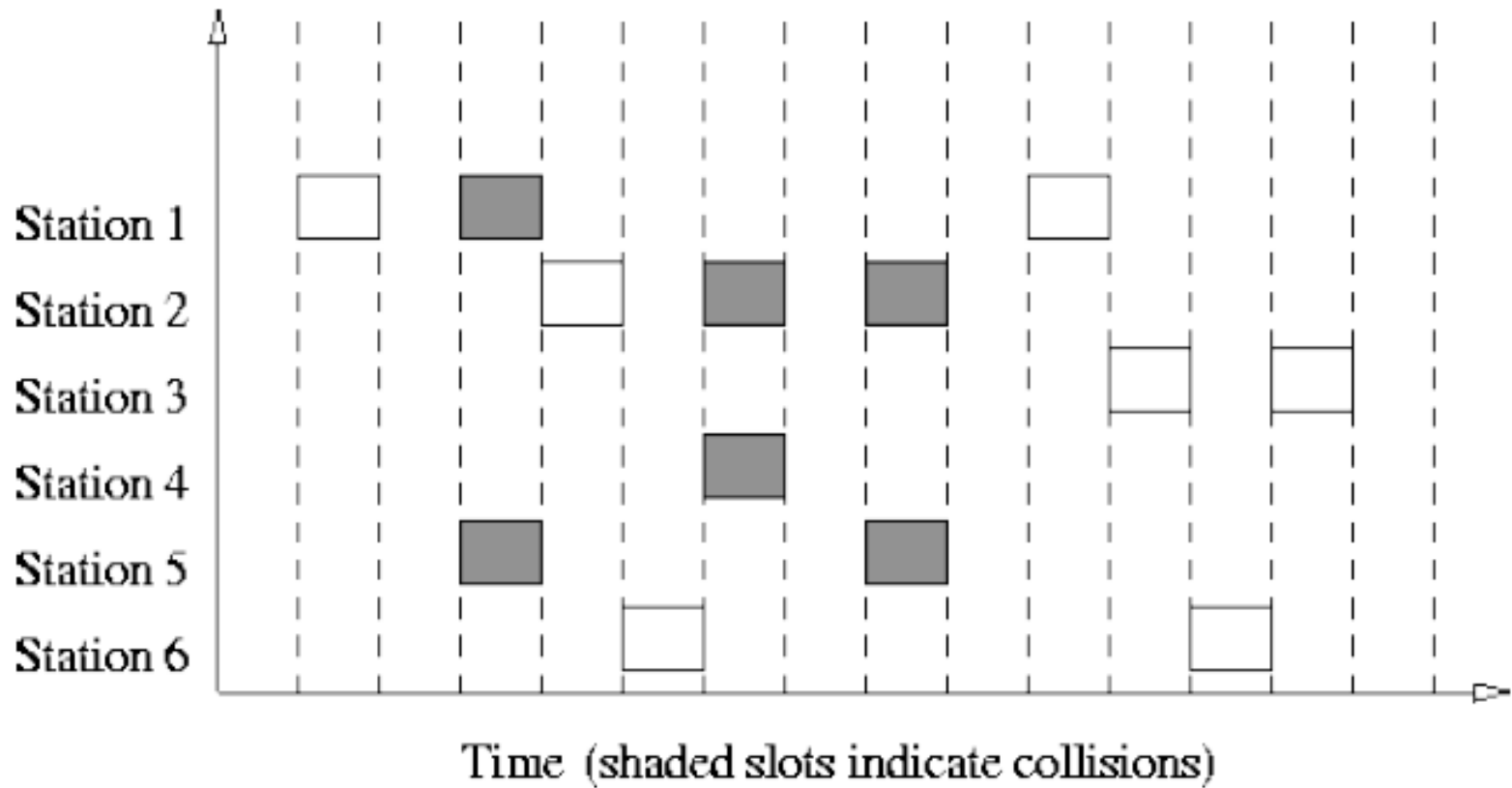
# Pure ALOHA



# Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
- In slotted ALOHA, time of the channel is divided into intervals called slots.
- The station can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot.
- There is still a possibility of collision if two stations try to send at the beginning of the same time slot.

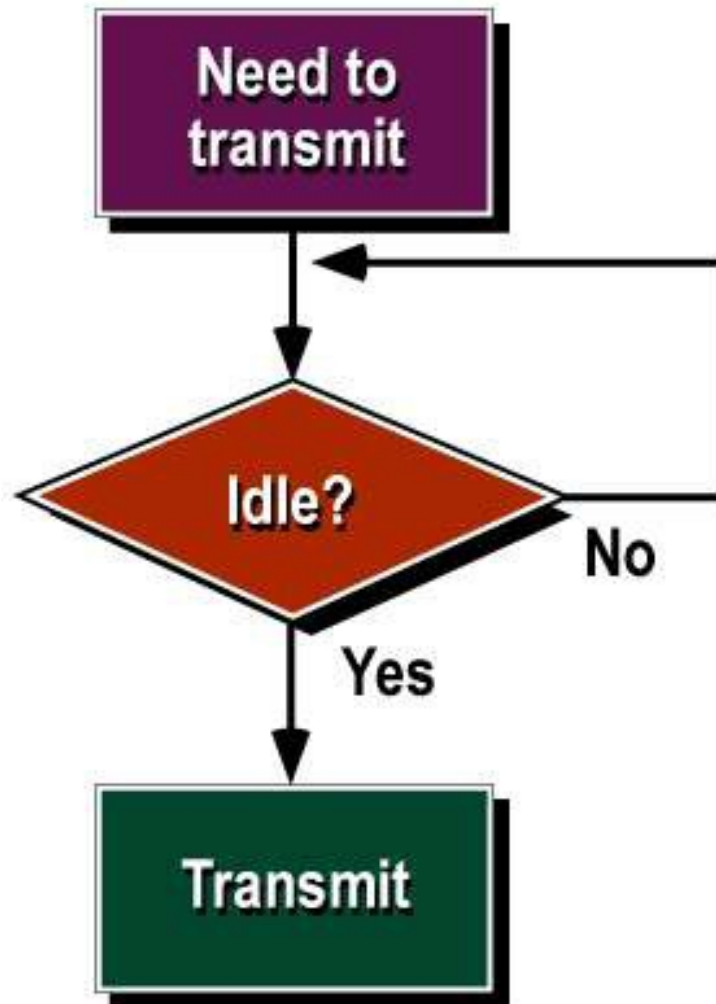
# Slotted ALOHA



# CSMA

- CSMA was developed to overcome the problems of ALOHA i.e. to minimize the chances of collision.
- 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

# CSMA Contd..



# CSMA Contd..

- The chances of collision still exists because of propagation delay.
- There are three different types of CSMA protocols:
  - 1-Persistent CSMA
  - Non-Persistent CSMA
  - P-Persistent CSMA

# 1-Persistent CSMA

- In this method, station that wants to transmit data, continuously senses the channel to check whether the channel is idle or busy.
- If the channel is busy, station waits until it becomes idle.
- When the station detects an idle channel, it immediately transmits the frame.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

# Non-Persistent CSMA

- A station that has a frame to send, senses the channel.
- If the channel is idle, it sends immediately.
- If the channel is busy, it waits a random amount of time and then senses the channel again.
- It reduces the chance of collision because the stations wait for a random amount of time .
- It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

## P-Persistent CSMA

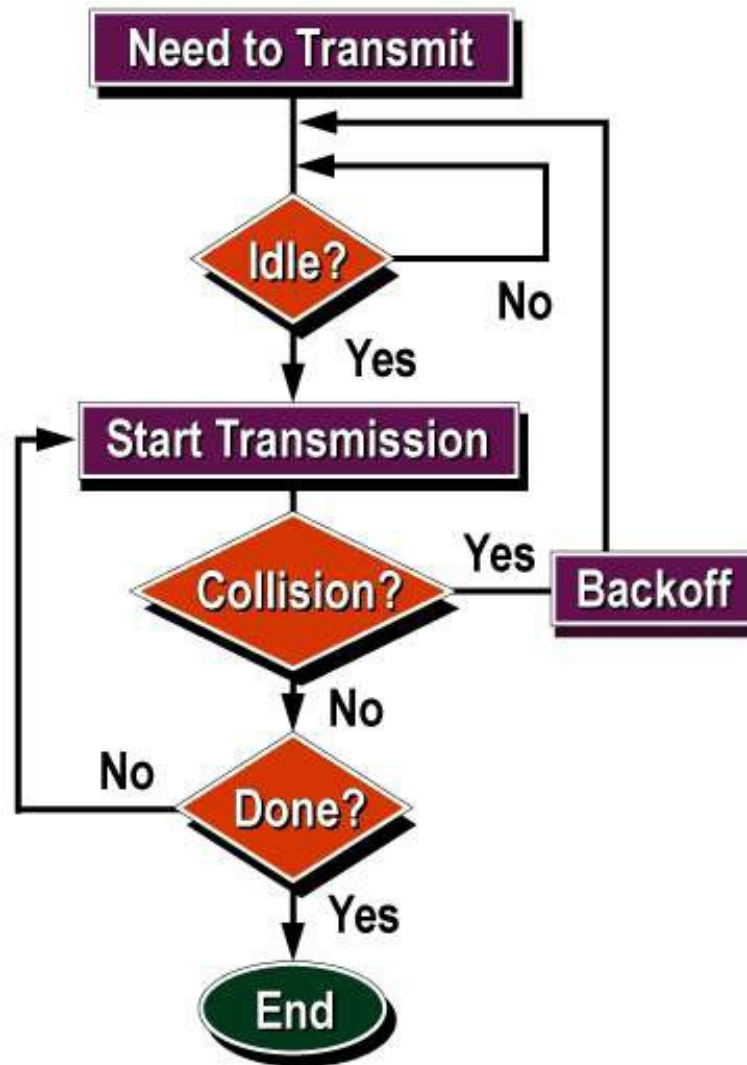
- In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time.
- When a station is ready to send, it senses the channel.
- If the channel is busy, station waits until next slot.
- If the channel is idle, it transmits the frame.

# CSMA/CD

- CSMA with Collision Detection
- In this protocol, the station senses the channel before transmitting the frame. If the channel is busy, the station waits.
- Additional feature in CSMA/CD is that the stations can detect collisions.
- The stations abort their transmission as soon as they detect collision.
- In CSMA/CD, the station that sends its data on the channel, continues to sense the channel even after data transmission.

- If collision is detected, the station aborts its transmission and waits for a random amount of time & sends its data again.
- As soon as a collision is detected, the transmitting station release a ***jam signal***.
- Jam signal alerts other stations. Stations are not supposed to transmit immediately after the collision has occurred.

# CSMA/CD Contd..



# CSMA/CA

- CSMA with Collision Avoidance
- This protocol is used in wireless networks because they cannot detect the collision.
- So, the only solution is collision avoidance.
- It avoids the collision by using three basic techniques:
  - Inter-frame Space
  - Contention Window
  - Acknowledgements

# CSMA/CA



# Interframe Space

- Whenever the channel is found idle, the station does not transmit immediately.
- It waits for a period of time called Interframe Space (IFS).
- When channel is sensed idle, it may be possible that some distant station may have already started transmitting.
- Therefore, the purpose of IFS time is to allow this transmitted signal to reach its destination.
- If after this IFS time, channel is still idle, the station can send the frames.

# Contention Window

- Contention window is the amount of time divided into slots.
- Station that is ready to send chooses a random number of slots as its waiting time.
- The number of slots in the window changes with time.
- It means that it is set of one slot for the first time, and then doubles each time the station cannot detect an idle channel after the IFS time.

# Acknowledgment

- Despite all the precautions, collisions may occur and destroy the data.
- Positive acknowledgement and the time-out timer helps guarantee that the receiver has received the frame.

# Controlled Access Protocol

- In this method, the stations consult each other to find which station has a right to send.
- A station cannot send unless it has been authorized by other station.
- The different controlled access methods are:
  - Reservation
  - Polling
  - Token Passing

# Reservation

- In this method, a station needs to make a reservation before sending data.
- The time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.
- When a station needs to send a frame, it makes a reservation in its own slot.
- The stations that have made reservations can send their frames after the reservation frame.

# Polling

- Polling method works in those networks where primary and secondary stations exist.
- All data exchanges are made through primary device even when the final destination is a secondary device.
- Primary device controls the link and secondary device follow the instructions.

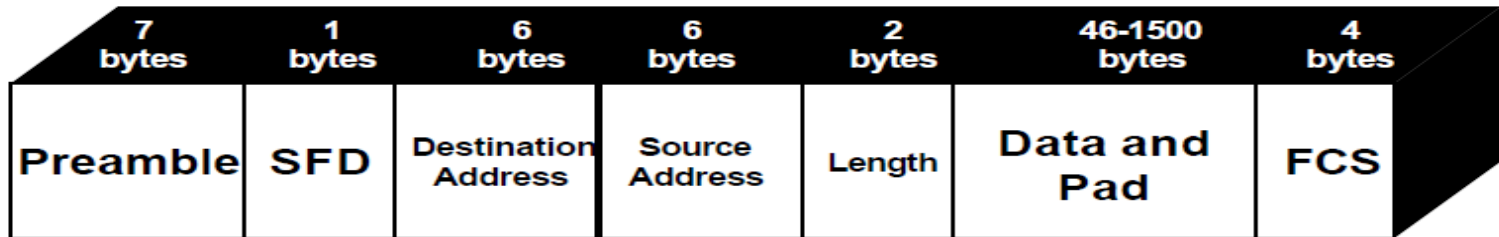
# Token Passing

- Token passing method is used in those networks where the stations are organized in a logical ring.
- In such networks, a special packet called token is circulated through the ring.
- Whenever any station has some data to send, it waits for the token. It transmits data only after it gets the possession of token.
- After transmitting the data, the station releases the token and passes it to the next station in the ring.
- If any station that receives the token has no data to send, it simply passes the token to the next station in the ring.

# Ethernet

- Ethernet has been a relatively inexpensive, reasonably fast, and very popular LAN technology for several decades.
- Ethernet uses the CSMA/CD access method to handle simultaneous demands.
- The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps.
- Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second.

# Ethernet Frame format



- The Preamble - This consists of seven bytes, all of the form "10101010". This allows the receiver's clock to be synchronized 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.

# FDDI → Fiber Distributed Data Interface

- data rate :100Mbps, used as a backbone
- With multi-mode fiber any given ring segment can be up to 200 km in length.
- A total of 1000 stations can be connected with a maximum separation of 2 km.
- two complete rings to overcome failures

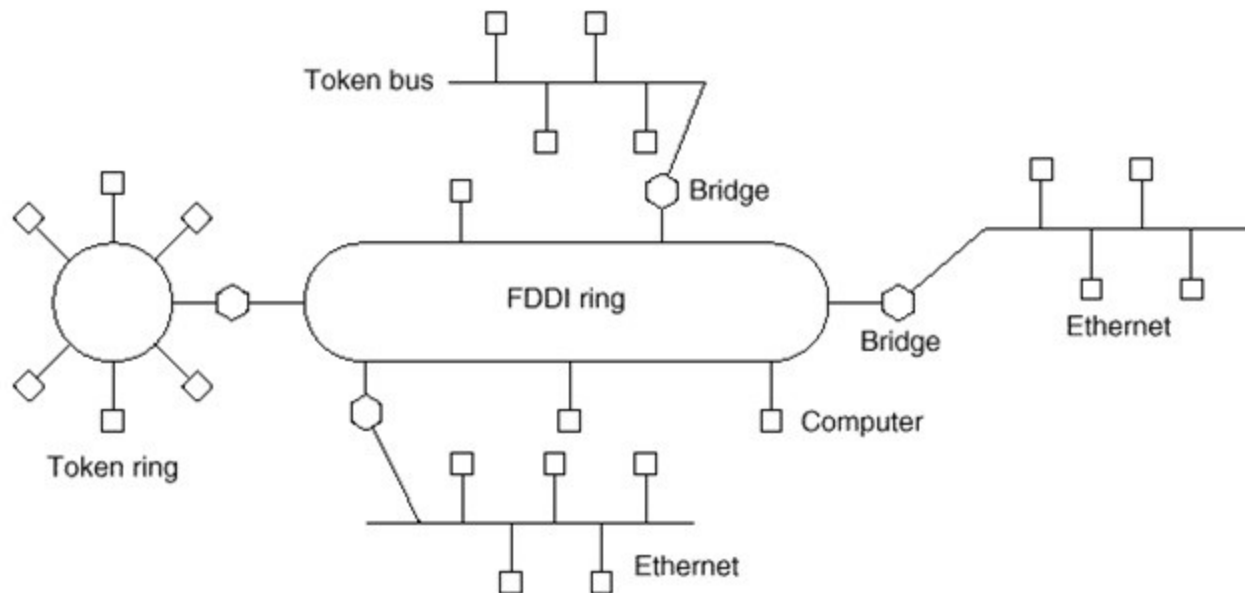
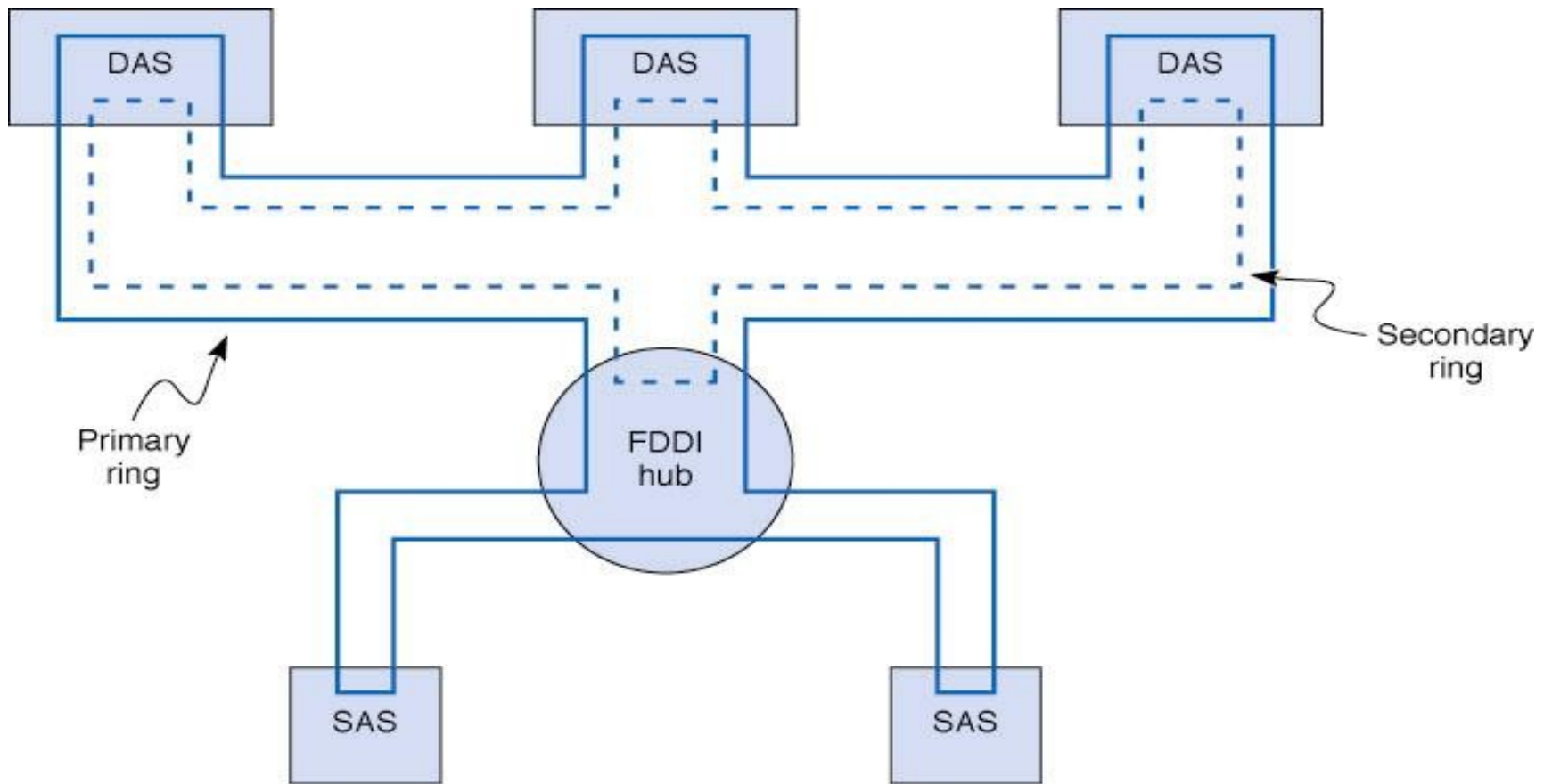


Fig: FDDI ring being used as a backbone to connect LANs and computers

# FDDI Topology

- FDDI uses both a physical and logical ring topology capable of attaching a maximum of 1000 stations over a maximum path of 200 km. A repeater is needed every 2 km.
- FDDI uses dual counter-rotating rings (called the primary and secondary). Data normally travels on the primary ring.
- Stations can be attached to the primary ring as single attachment stations (SAS) or both rings as dual attachment stations (DAS).



DAS: Dual-attachment station  
SAS: Single-attachment station

Fig : Optical cable topology for an FDDI local area network.

# FDDI's Self Healing Rings

- An important feature of FDDI is its ability to handle a breaks in the network by forming a single temporary ring out of the pieces of the primary and secondary rings.
- Once the stations detect the break, traffic is rerouted through a new ring formed out of the parts of the primary and secondary rings not affected by the break.
- The network then operates over this temporary ring until the break can be repaired.
- Next figure shows how the failure is managed.

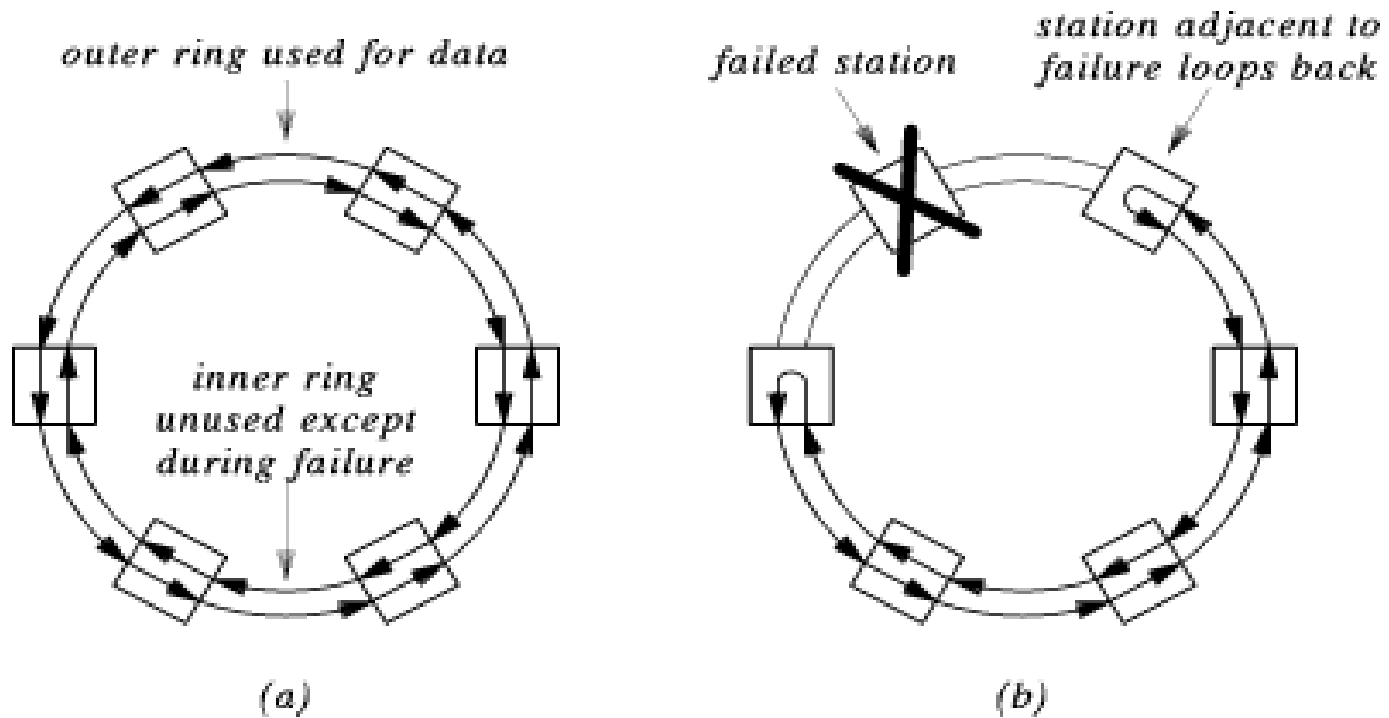


Fig : Managing a broken circuit

# FDDI Media Access Control

- FDDI uses a token passing system. Computers wanting to send packets wait to receive a token before transmitting.
- Multiple packets can be attached to the token as it moves around the network.
- When a station receives the token, it looks for attached packets addressed to it and removes them from the incoming packet.
- If the station wants to send a packet it attaches it to the token and sends the token with its attached packets to the next station.
- This controlled access technique provides a higher performance level at high traffic levels compared to a contention-based technique like Ethernet.

# FDDI Message Delineation

- The FDDI frame can be broken into three parts:
- **Frame Start:** like Ethernet, the frame begins with a **preamble** (8-bytes in this case) and a 1-byte **start delimiter**.
- **Frame Body:** the main body of the frame includes the following fields:
  - 1-byte **frame control field** (used for the token)
  - 2 or 6 byte fields for the **destination and source addresses** (6 bytes is more common)
  - the **data field** contains 0-4500 bytes of data
  - the **frame check sequence (FCS)** used in error control.
- **Frame End:** the frame ends with a 1-byte **end delimiter** and a 2-byte **frame status** field.

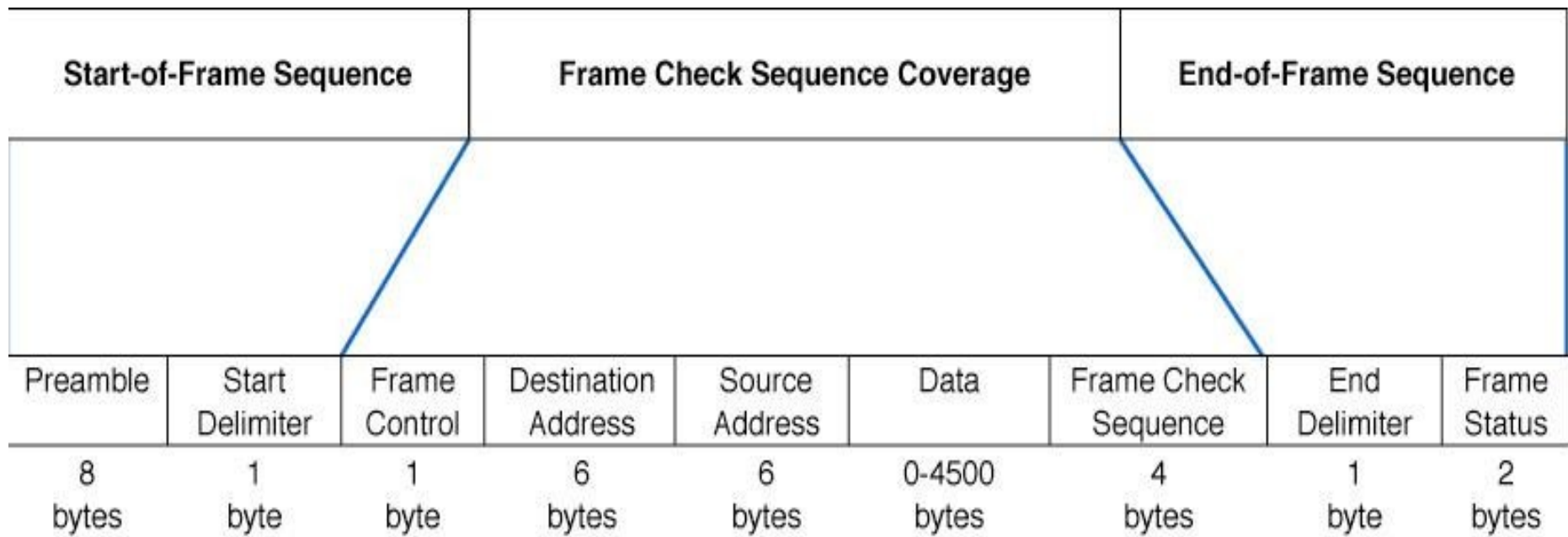


Fig : FDDI frame layout

# Virtual LANs

- VLANs are a new type of LAN architecture using intelligent, high-speed switches.
- Unlike other LAN types, which physically connect computers to LAN segments, VLANs assign computers to LAN segments by software.
- VLANs have been standardized as IEEE 802.1q and IEEE 802.1p.
- The two basic designs are:
  - Single-switch VLANs
  - Multiswitch VLANs

# Single Switch VLANs

- With single switch VLANs, computers are assigned to VLANs using special software, but physically connected together using a large physical switch.
- Computers can be assigned to VLANs in four ways:
  - **Port-based VLANs** assign computers according to the VLAN switch port to which they are attached
  - **MAC-based VLANs** assign computers according to each computer's data link layer address
  - **IP-based VLANs** assign computers using their IP-address
  - **Application-based VLANs** assign computers depending on the application that the computer typically uses. This has the advantage of allowing precise allocation of network capacity.

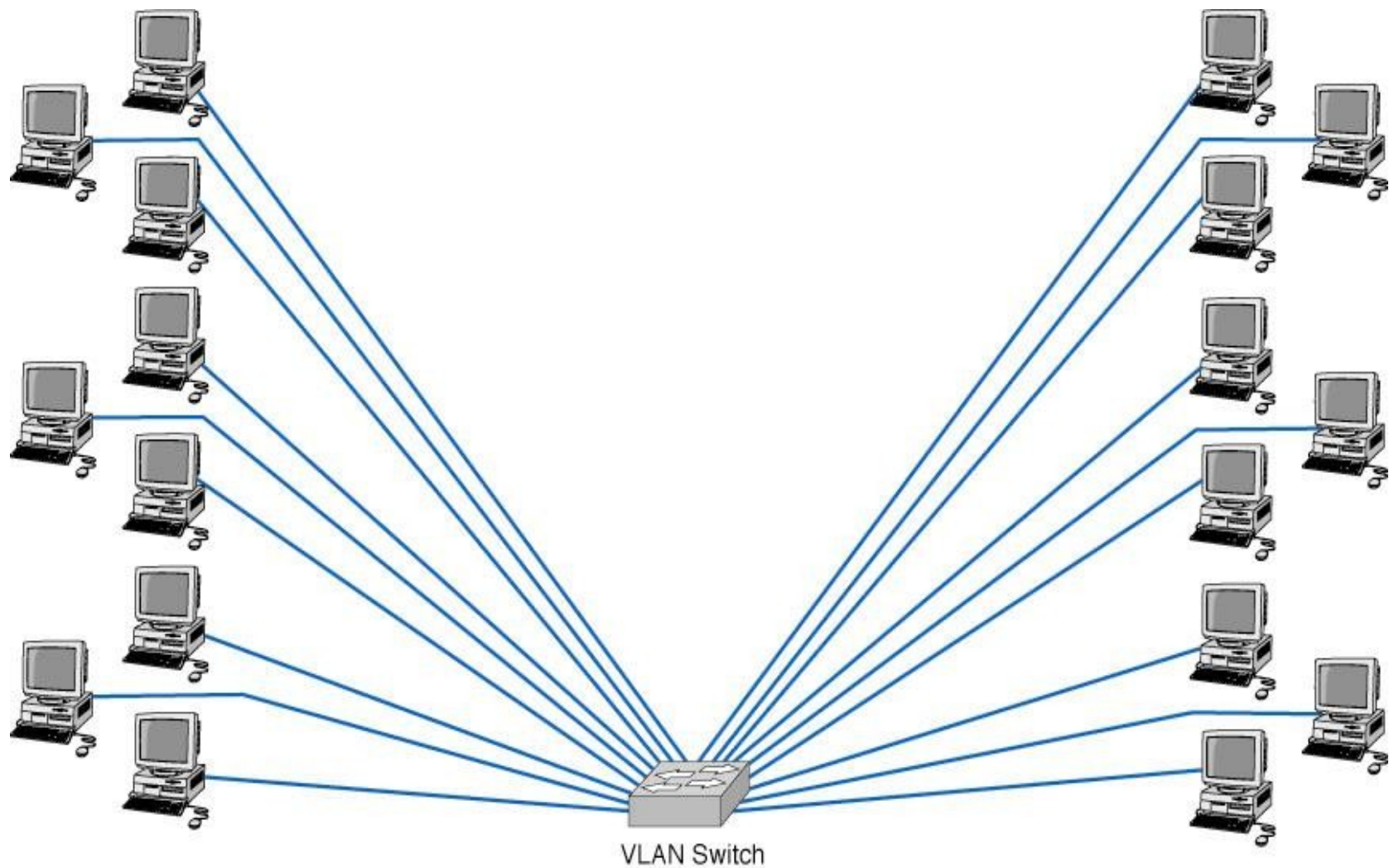


Fig : Single-switch VLAN architecture

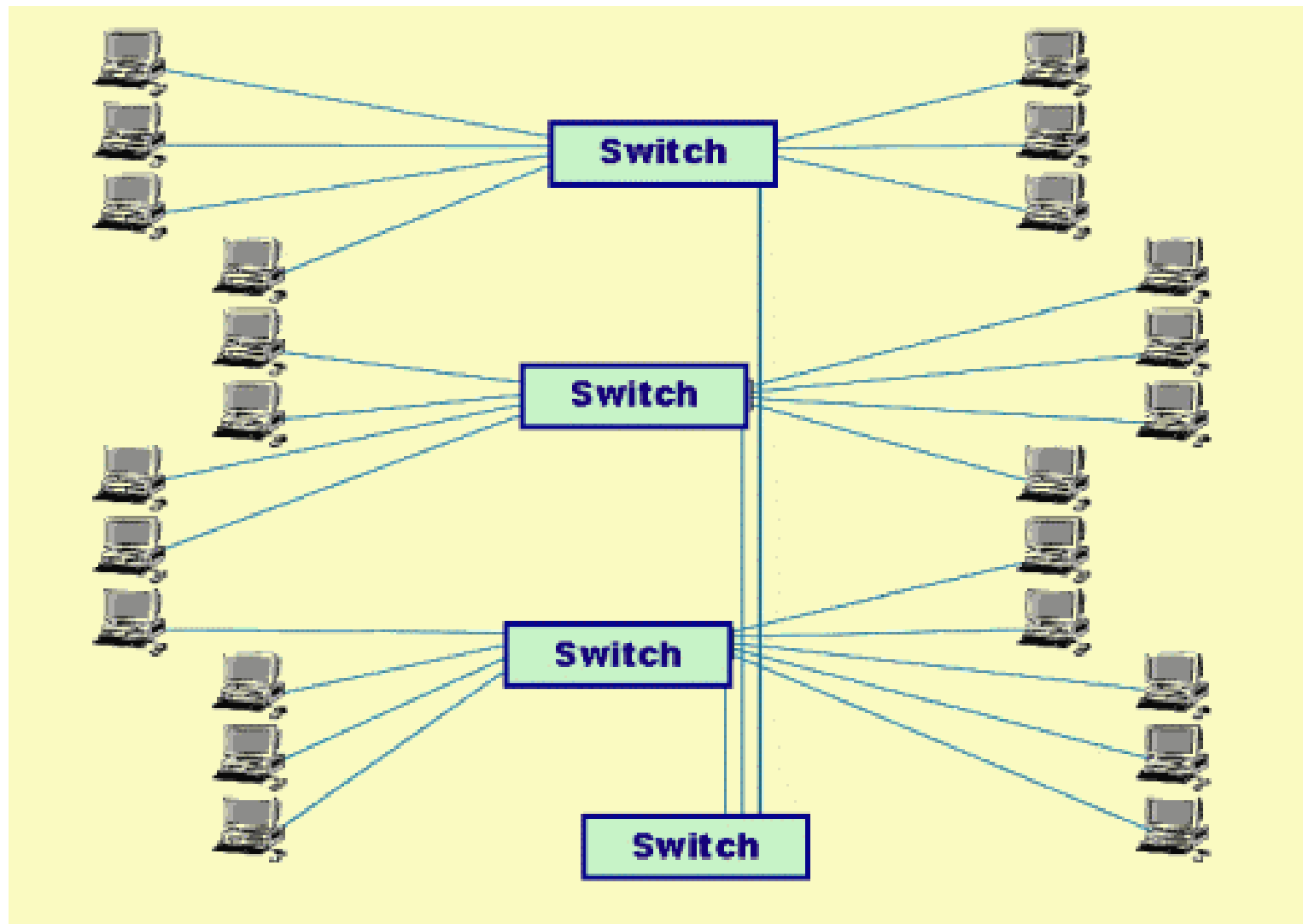


Fig : Multi-switch VLAN

# IEEE LAN Standards

- **IEEE 802.3**                      **Ethernet (CSMA/CD)**
- **IEEE 802.4**                      **Token Bus**
- **IEEE 802.5**                      **Token Ring**
- IEEE 802.6                      Metropolitan Area Networks
- IEEE 802.7                      Broadband LANs
- IEEE 802.8                      Fiber Optic LANs
- IEEE 802.9                      Integrated Data and Voice Networks
- **IEEE 802.11**                      **Wireless Networks**
- IEEE 802.14                      Cable TV

# IEEE 802.3 : Ethernet(CSMA/CD)

- The IEEE standard for Ethernet is 802.3
- Ethernet operates in two areas of the OSI model
  - the lower half of the data link layer, which is known as the MAC sub layer,
  - and the physical layer.
- The CSMA/CD is the access method used in Ethernet to detect and avoid collision in network.

- The 802.3 standard describes the operation of the MAC sub-layer in a bus LAN that uses carrier sense, multiple access with collision detection (CSMA/CD).
  - Beside carrier sensing, collision detection and the binary exponential back-off algorithm, the standard also describes the format of the frames and the type of encoding used for transmitting frames.
  - The minimum length of frames can be varied from network to network.
  - The standard also makes some suggestions about the type of cabling that should be used for CSMA/CD bus LANs.
- The 802.3 CSMA/CD bus LAN is said to be a **non-deterministic** network. This means that no host is guaranteed to be able to send its frame within a reasonable time.
  - When the network is busy, the number of collisions rises dramatically and it may become very difficult for any hosts to transmit their frames.

## 802.3 cabling

<i>Name</i>	<i>Cable type</i>	<i>Speed/Distance</i>	<i>Signaling</i>
• 10Base 2	Thin Ethernet (Coax)	10 Mbps/ 185 m	Base band
• 10Base 5	Thick Ethernet (Coax)	10 Mbps/ 500 m	Base band
• 10Base-T	UTP	10 Mbps/ 100m	Base band
• 100Base-TX	UTP	100 Mbps/ 100m	Base band
• 100Base-FX	Fiber	100 Mbps/ 228-412m	Base band
• 1000Base-T	UTP	1000Mbps/ 100 m	Base Band

Note: Ethernet Frame format can be discussed in 802.3 standard which has been already covered

# IEEE 802.4 : Token Bus

## Evolution of 802.4

- 802.3 suffer from the difficulty of large delay in getting the access and at the same time
- poor performance under heavy load.
- There are also no priorities in 802.3, making them unsuited for real time systems.
- Token passing protocols were proposed and were found to be very attractive for situations with heavy load.

- The basic idea is to generate a token in the network
- Only the holder of the token can transmit.
- Thus with one token, only one station can transmit at a time, eliminating collisions totally.
- Normally a token can be held by a user for a prescribed time only after which it has to be passed to the next station.
  - If the user finishes his transmission before his token holding time is over, he passes the token to the next user.

# A Token Bus Layout

Speeds of 1,5 and 10 Mbps were possible

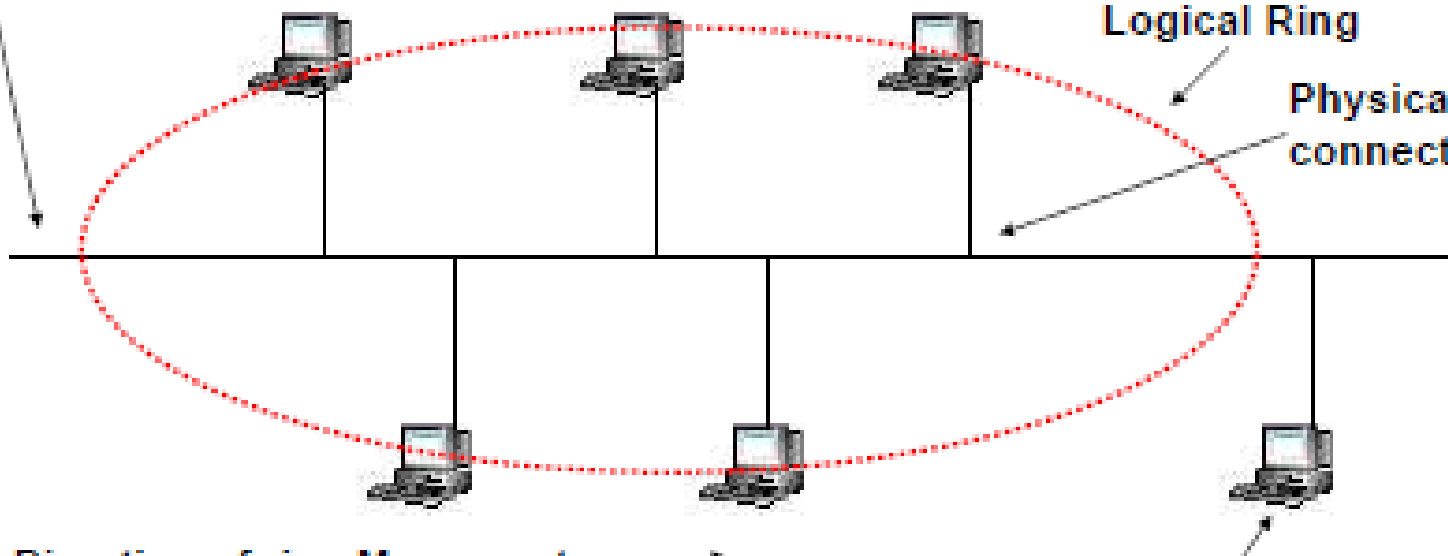
Broadband coaxial  
cable

Logical Ring

Physical  
connection

Direction of ring Movement →

Station outside the  
Ring



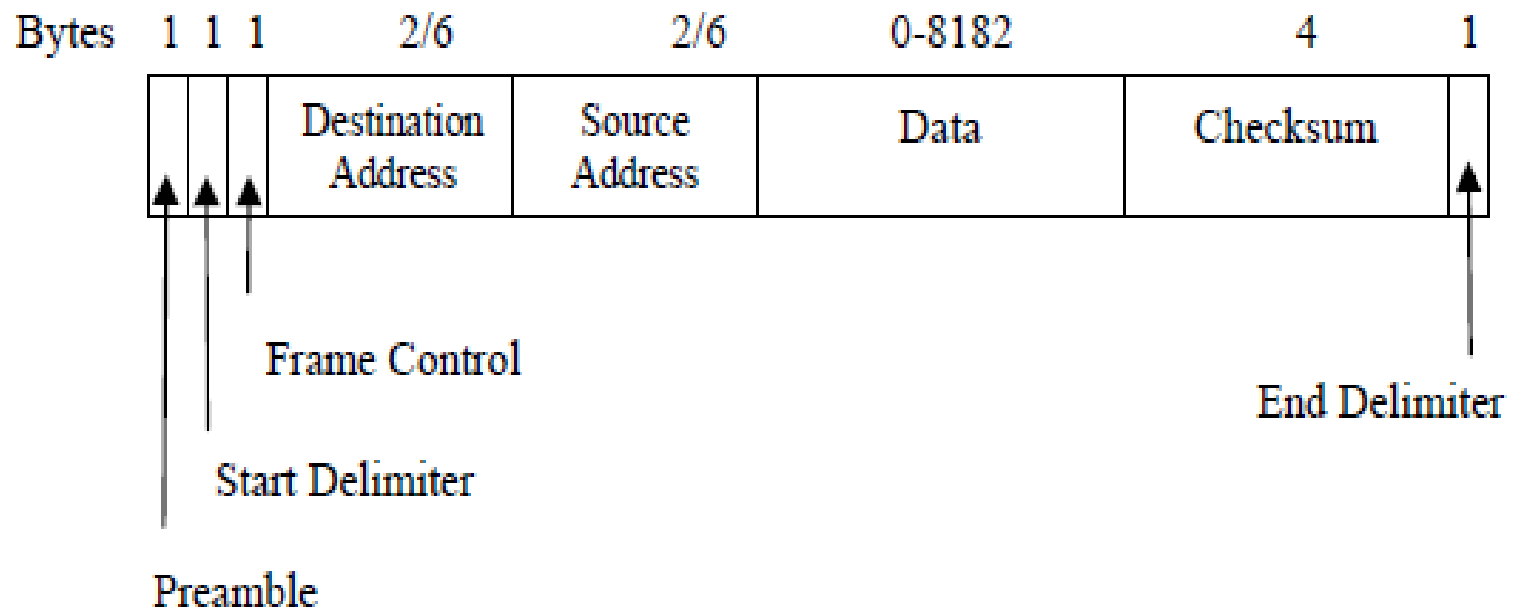


Fig : IEEE 802.4 Frame format

## 802.4 Frame format contd..

- The preamble is used to synchronize the receiver's clock.
- The start and end delimiter fields are used to mark the frame boundaries.
- The frame control field is used to distinguish data frames from control frames.
- For data frames, it carries the frame's priority.
  - The token bus defines four priority classes-0, 2, 4 and 6 for traffic, with 0 the lowest and 6 the highest.

- For the control frame, the frame control field is used to specify the frame type.
  - The allowed types include token passing
  - and various ring maintenance frames,
    - mechanism for letting new stations enter the ring,
    - the mechanism for allowing stations to leave the ring

# IEEE 802.5 : Token Ring

- Ring is not a broadcast medium but a collection of point-to-point links forming a circle.
- Rings can be based on twisted pair, coaxial or a fiber optics cable.
- Channel access problem is solved with the help of a special frame called a “Token”.
- A free token circulates the ring when all stations are idle.
- A station wishing to transmit must wait until it detects a free token passing by.

- It then seizes the token by changing the token bit to transform it into the start-of-frame sequence for a data frame.
- The data to be transmitted is then appended.
- The frame on the ring will make a round trip and then removed by the transmitting station.

## USE OF WIRE CENTERS

- Cable breaks can lead to ring failure
- This problem can be resolved with the help of a Wire Center.
- A wire center has bypass relays which draw current from the station
- If a station is powered down the relays close thereby removing the station from the ring and maintaining the ring
- Relays can be operated by software for network management
- wire centers make the ring a star-shaped ring.

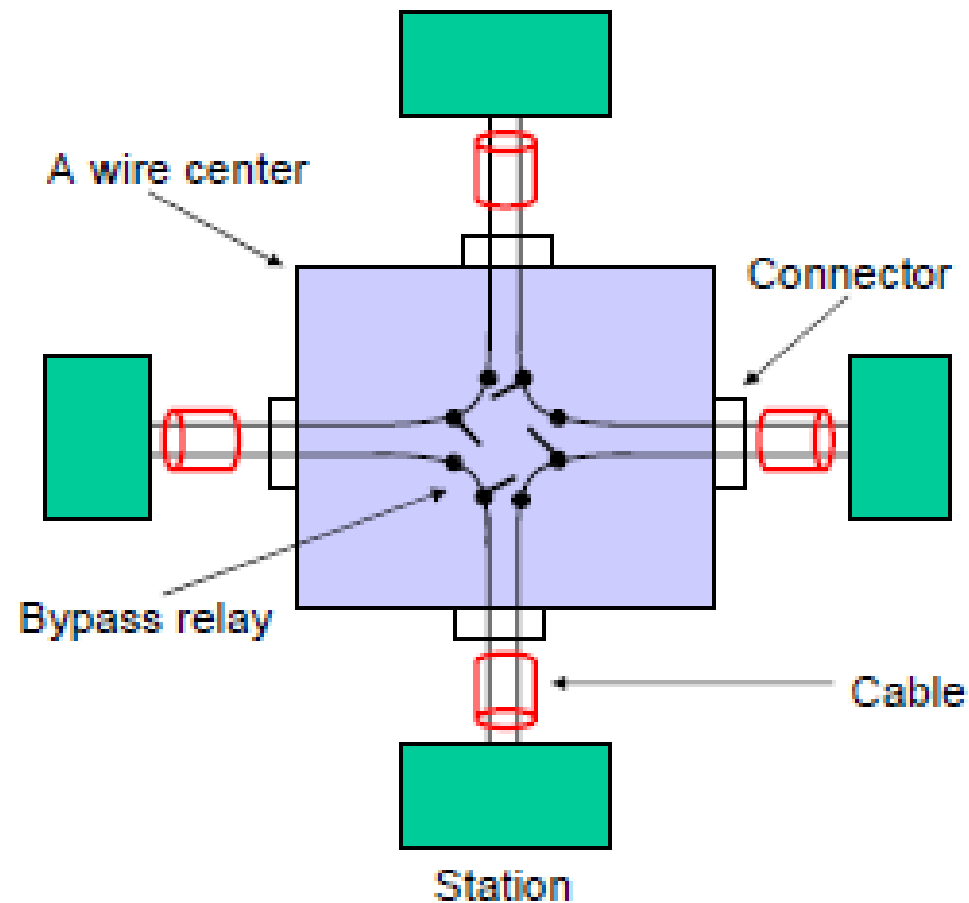


Fig : Four stations connected to a wire center

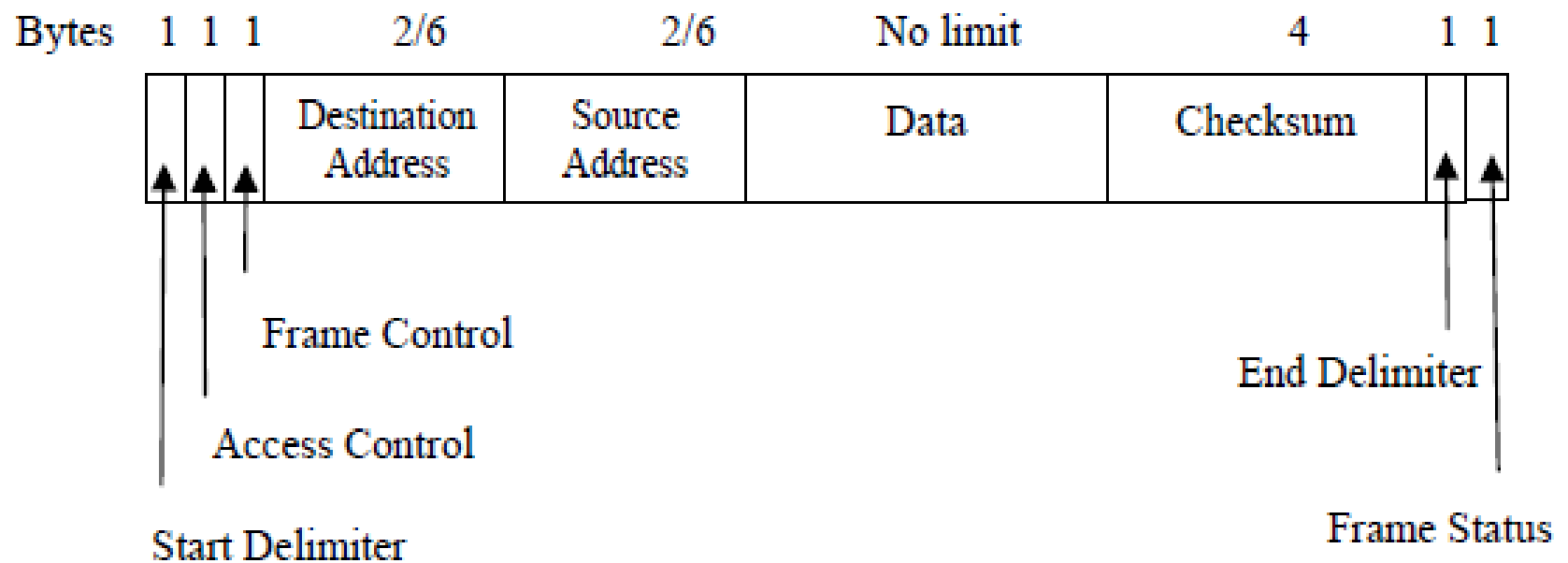


Fig : IEEE 802.5 Frame Format

- The starting and ending delimiter fields mark the beginning and ending of the frame.
- The access control byte contains the token bit, and also the monitoring bit, priority bits and reservation bits.
- The frame control byte, distinguishes data frames from various possible control frames.
- The frame status byte contains A and C bits.

<b>A</b>	<b>C</b>	<b>Significance</b>
----------	----------	---------------------

0	0	Destination not present or not powered up
1	0	Destination present but frame not accepted
1	1	Destination present and frame copied.

# IEEE 802.11: Wireless LANs

- Use CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
- A station wishing to transmit shall first sense the medium.
- If the medium is busy, the station shall defer until the end of the current transmission.
- After deferrals, the station shall select a random back off interval and shall decrement the back off interval counter while the medium is idle.
- If the medium is idle, after any deferrals or back offs, prior to data transmission, RTS/CTS short frames are exchanged.

All 802.11 frames are composed of the following components:

Preamble	PLCP Header	MAC Data	CRC
----------	-------------	----------	-----

Physical Layer Convergence Procedure (PLCP)

- Defined Data rate
- packet length

The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information used by the PHY Layer to decode the frame.

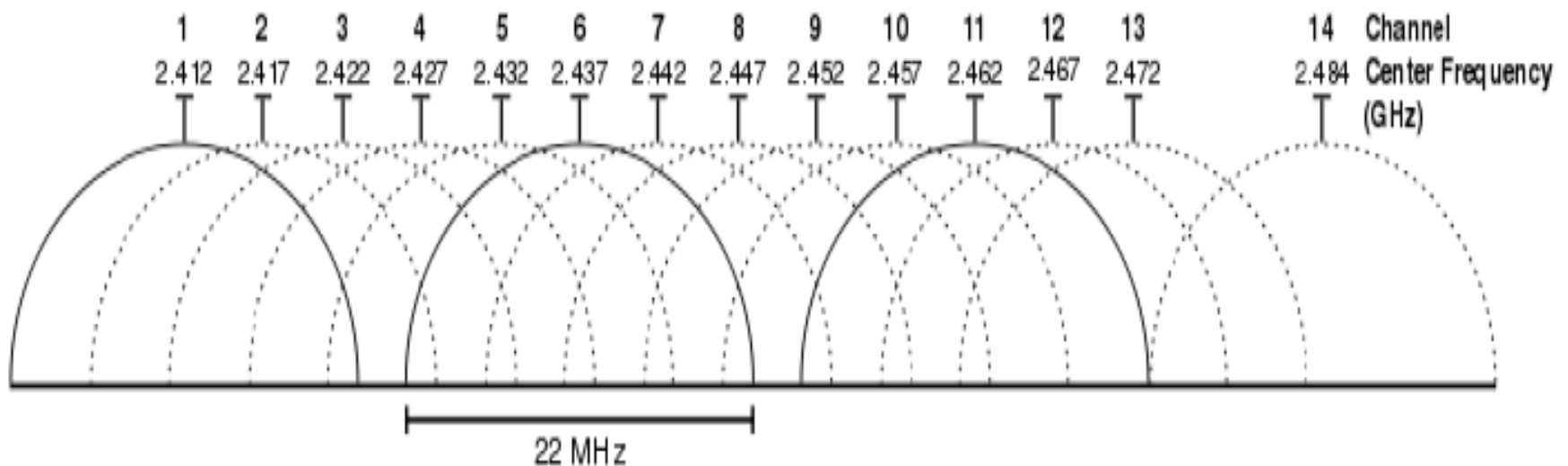
## Wireless LAN Throughput by IEEE Standard

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
IEEE 802.11b	11 Mbps	5 Mbps
IEEE 802.11g	54 Mbps	25 Mbps (when .11b is not present)
IEEE 802.11a	54 Mbps	25 Mbps
IEEE 802.11n	Up to 600 Mbps	Up to 400 Mbps
IEEE 802.11ac	Up to 867 Mbps with 2 antennas and 80 MHz; Up to 1.3 Gbps with 3 antennas and 80 MHz	Up to 600 Mbps with 2 antennas and 80 MHz; Up to 900 Mbps with 3 antennas and 80 MHz
IEEE 802.11ad	At least 1.1 Gbps (up to 4.6 Gbps in some first generation products)	Up to 700 Mbps for 1.1 Gbps OTA (up to 3 Gbps for 4.6 Gbps OTA)

# 802.11b Standard

- Operate at 2.4 GHz range
- Throughput up to 11 Mbit/s using the same 2.4GHz band (Theoretically)
- CSMA/CA media access method is used
- Use DSSS Modulation Techniques
- 802.11b devices suffer interference from other products operating in the 2.4 GHz band
  - microwave ovens, Bluetooth, cordless phone

- Maximum 14 channels
- 11 channels (1-11) are allowed to use
- 3 non overlapping channels 1, 6, 11
- Amendments to 802.11b are
  - 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be



# 802.11g Standard

- Extension of 802.11b
- Extended throughput up to 54 Mbit/s
- Using the same 2.4 GHz band as 802.11b.
- 802.11g hardware is fully backwards compatible with 802.11b hardware
- modulation scheme used in 802.11g is OFDM

# 802.11a Standard

- Completely different from 11b and 11g.
- Shorter range than 11b and 11g.
- Runs in the 5 GHz range, so less interference from other devices.
- Has 12 channels, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about 27 Mbps max
- Uses frequency division multiplexing
- Improvements to 802.11a are
  - 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

# 802.11n Standard

- Wireless networking standard
- uses multiple antennas to increase data rates
- Maximum data rate from 54 Mbit/s to 600 Mbit/s
- Use OFDM and MIMO technologies
- RF Band (GHz) 2.4 or 5

# IEEE 802.11ac and 802.11ad Standard

- IEEE 802.11ac will deliver its throughput over the 5 GHz band, which also uses 5 GHz band offering bandwidth of 3.46 Gbps
- IEEE 802.11ad, targeting shorter range transmissions, will use the unlicensed 60 GHz band with 6.7 Gbps bandwidth
- Through range improvements and faster wireless transmissions, IEEE 802.11ac and ad will:
  - Improve the performance of high definition TV (HDTV) and digital video streams in the home and advanced applications in enterprise networks

Thank You !!!