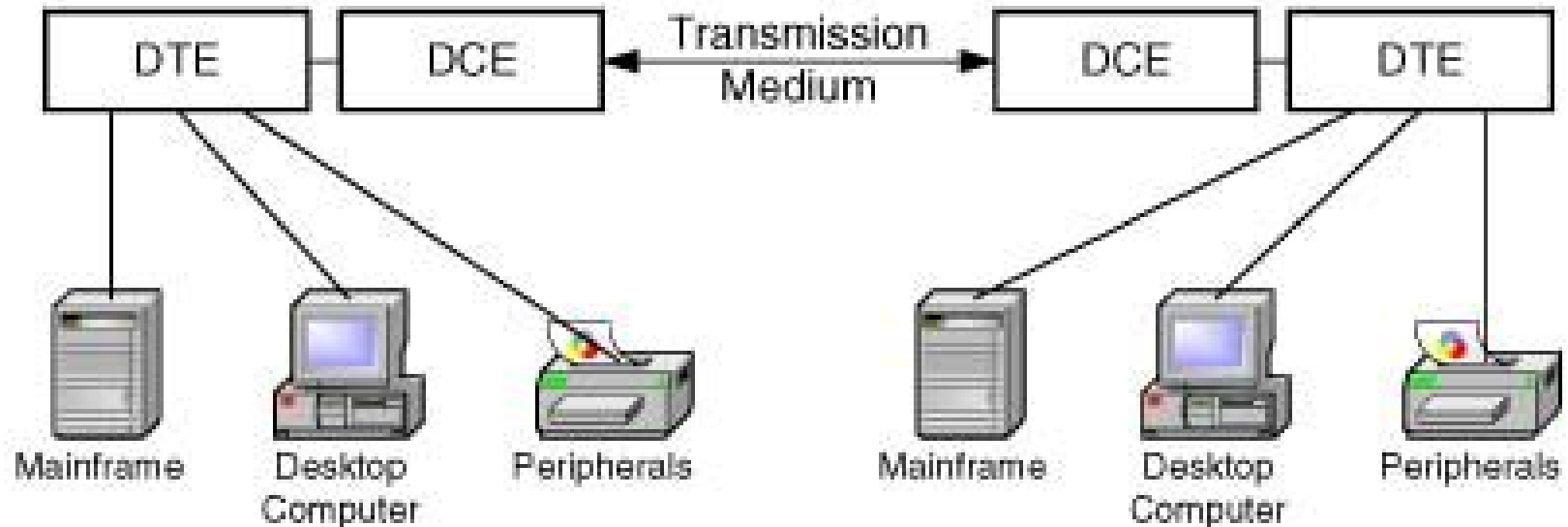


DATA  
COMMUNICATIONS

# Components of a Basic Data Communications Link

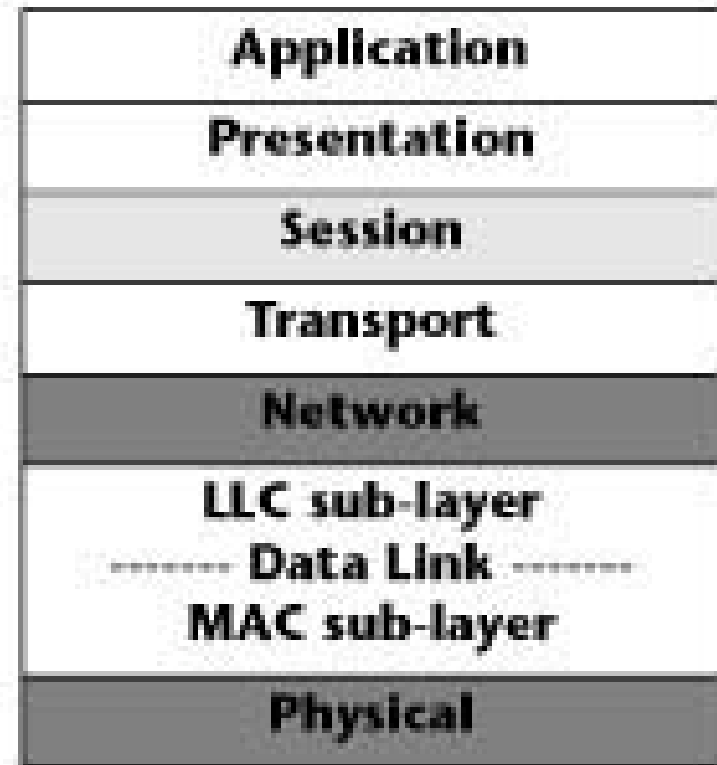


# Data Networks Terminology

- Data Network
  - Collaborative environment that provides worldwide access to corporate data
- Network Architecture
  - A coordinated set of guidelines that describe a communications environment
- DTE (Data Terminal Equipment)
  - Transmits and receives data; Examples: Desktop computer, Printer
- DCE (Data Communications Equipment)
  - Coupled to transmission medium; Examples: Router, Modem
- Interface
  - Provides handshaking from one layer to the next; Example: NIC
- Protocol Converter
  - Connects two systems at the same layer; Example: Bridge

# Open Systems Interconnect (OSI) Reference Model

- ISO recommends the Open Systems Interconnect (OSI) Model as a theoretical framework for communication between two machines in a LAN. It defines the parameters for communication hardware and software



# Physical Layer

- Interfaces network devices with transmission medium and provides the hardware a means of sending and receiving data
- Responsible for data coding (converting 0s and 1s into electrical or light pulses)
- Defines physical and electrical specifications for transmission

# Data Link Layer

- Data Link layer is divided into two parts:
  - Media Access Control (MAC) lower sub-layer
  - Logical Link Control (LLC) upper sub-layer
- MAC sub-layer
  - Specifies the access methods used, example IEEE 802
- LLC sub-layer
  - Brings various topologies together in a common format
  - Provides error-control and synchronization, common to all access methods, at the node-to-node basis

# Network Layer

- Defines network segmentation and network address scheme (IP/IPX)
- Handles routing and forwarding of the data
  - Virtual Circuit
    - Connection from sender to receiver is established on demand, and then functions as a point-to-point connection
  - Datagram
    - Packets are delivered individually, so they can take different routes and arrive at the destination at different times
    - Packets are reassembled at the destination

# Transport Layer

- Manages end-to-end control
- Assures end-to-end reliability and error-free data transfer
- Translates and manages message communication through sub-network
- Ensures data integrity and deals with packet sequencing
- Selects most cost-efficient communications service based on transmission parameters



# Session Layer

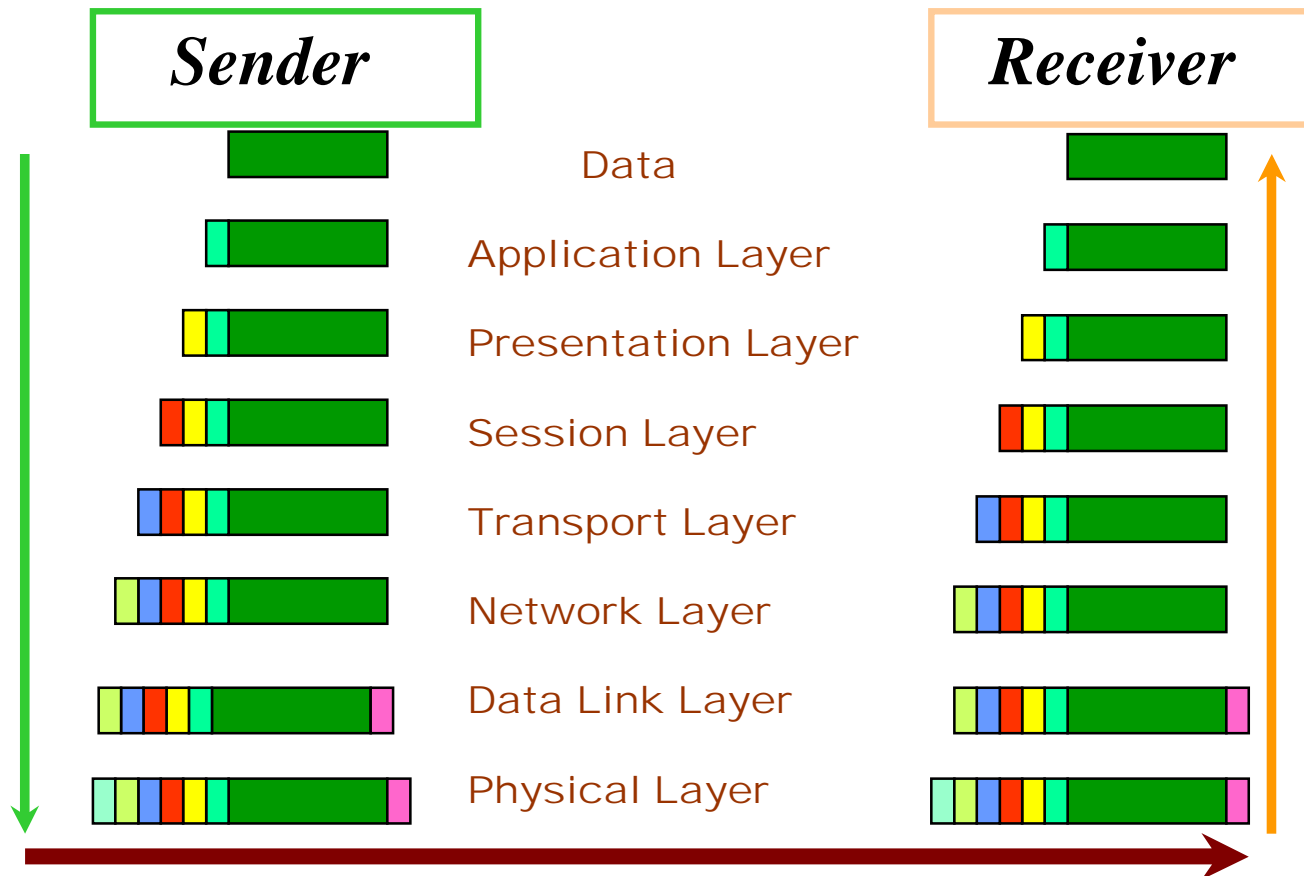
- Responsible for connection negotiation
- Authenticates and allows network access to users
- Establishes and maintains connection between applications at each end
- Synchronizes dialog between applications
- Handles crash recovery

# Presentation Layer

- Handles network security and architecture-independent data formats
- Provides data conversion, compression, and encryption
- Translates data format of sender to data format of receiver
- Commonly known as the syntax layer

# Application Layer

- Provides an interface to the end-user
- Manages program requests that require access to services provided by a remote system
- Identifies quality of service (QoS), user authentication, and other constraints on the data syntax



***Header/trailer information is added or removed as data passes from layer to layer.***

# Character Codes

- A byte is a string of 8 bits, which normally represents a character
- A character is a specific symbol or a string of 0s and 1s
- A character code refers to a way of converting alphabets, numbers, punctuation marks, and other special characters into a series of 0s and 1s
- There are several different character codes such as Baudot, EBCDIC (Extended Binary Coded Decimal Interchange Code), and ASCII (American Standard Code for Information Interchange)

# ASCII Character Code

- ASCII
  - ASCII was established to achieve compatibility between various types of data processing equipment
  - A standard seven-bit code that was proposed by ANSI in 1963, and finalized in 1968
  - With seven bits it is possible to differentiate  $2^7$  or 128 different patterns. The standard ASCII character set consists of 128 decimal numbers ranging from zero through 127 assigned to letters, numbers, punctuation marks, and the most common special characters

# Data Encoding Methods

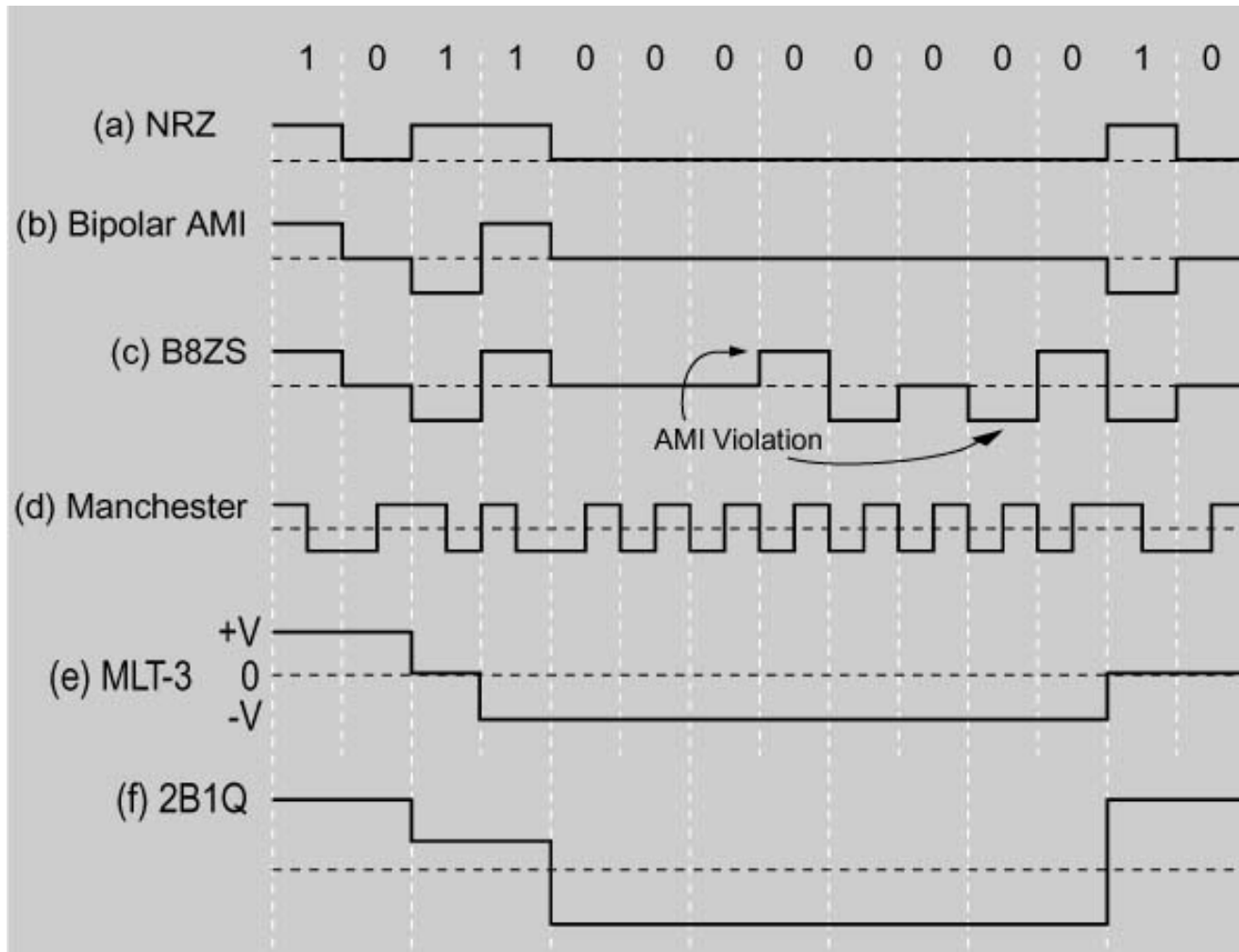
- **Data Encoding** deals with how best to transmit data (0s and 1s) across various media
- Popular Data Encoding Methods
  - NRZ (Non-Return to Zero)
  - Bipolar AMI ( Bipolar Alternate Mark Inversions)
  - B8ZS ( Bipolar with 8 Zero Substitution)
  - Manchester Encoding
  - Multi-Level Transition (MLT-3)
  - 4B/5B Encoding
  - 2B1Q ( 2 Binary 1 Quaternary)

# Shannon's Channel Coding Theorem

- Shannon's Channel Coding Theorem states that if the transmission rate is equal to or less than the channel capacity, then there exists a coding technique which enables transmission over the channel with an arbitrarily small frequency of errors



# Data Encoding Methods



# Non-Return to Zero (NRZ)

- NRZ is the simplest representation of digital signals
- One bit of data is transmitted per clock cycle
- Bit values of 1 and 0 are represented by high and low voltage signals, respectively
- Two downfalls of NRZ: 1. DC component, and 2. Inability to carry synchronization information along with the data
  - If a NRZ signal has a sequence of 1s, the signal cannot pass through electrical components, which conduct only when the signal is changing. The receiver will require an additional synchronization signal to determine how many 1s there are

# Bipolar Alternate Mark Inversions (Bipolar AMI)

- In Bipolar AMI, marks are analogous to 1s and spaces are analogous to 0s
- This means a logical one is represented by a signal and a logical zero is represented by no signal
- The Bipolar AMI solves the DC component problem by alternating the polarities of 1s
- However, Bipolar AMI signals can lose self-synchronization when transmitting a long string of 0s

# Bipolar with 8 Zero Substitution (B8ZS)

- This coding method takes care of the self-synchronization problem by *breaking the alternation rule* when it comes across a sequence of eight consecutive 0s
- This rule puts 1s in place of the fourth and fifth 0s and in places of the seventh and eighth 0s
- The first substitute incorrectly has the polarity of the previous 1, and the third substitute incorrectly has the polarity of the second substitute 1
- The receiver recognizes an intentional violation and concludes that there is a sequence of eight 0s

# Manchester Encoding

- Manchester encoding is implemented in Ethernet and Token Ring LAN technologies
- A 1 is indicated by a high to low transition in the middle of a pulse, while a 0 is indicated by a low to high transition in the middle of the pulse
- Unlike NRZ and Bipolar AMI, Manchester encoding has no DC component and is fully self-synchronizing
- Its drawback is that its bandwidth requirement is twice the baud rate
  - For 10 Mbps transmission, it operates at 20 MHz frequency

# 4B/5B Encoding

- Every 4-bit pattern is assigned a 5-bit code
- Instead of the 4-bits, the 5-bit code is transmitted
- The 5-bit code is picked such that there are at least two transitions in every 5-bit code
  - Therefore, an encoded stream will never contain more than 3 zeros in a row
  - This helps synchronization and leads to higher data transfer rates
- Used in Fast Ethernet and FDDI
- Gigabit Ethernet uses 8B/10B Encoding, based on the same principle, where an 8-bit pattern is assigned a 10-bit code

# 4B/5B Encoding Chart

Four Data Bits				Five-bit Code				
A3	A2	A1	A0	Q4	Q3	Q2	Q1	Q0
0	0	0	0	1	1	1	1	0
0	0	0	1	0	1	0	0	1
0	0	1	0	1	0	1	0	0
0	0	1	1	1	0	1	0	1
0	1	0	0	0	1	0	1	0
0	1	0	1	0	1	0	1	1
0	1	1	0	0	1	1	1	0
0	1	1	1	0	1	1	1	1
1	0	0	0	1	0	0	1	0
1	0	0	1	1	0	0	1	1
1	0	1	0	1	0	1	1	0
1	0	1	1	1	0	1	1	1
1	1	0	0	1	1	0	1	0
1	1	0	1	1	1	0	1	1
1	1	1	0	1	1	1	0	0
1	1	1	1	1	1	1	0	1

## 2 Binary 1 Quaternary (2B1Q)

- 2B1Q uses four distinct signaling levels, with data represented in two-bit units
- 2B1Q represents the distinction between bits per second and baud rate
- 2B1Q has been implemented in broadband technologies such as ISDN, SDSL and HDSL



# Error Detection and Correction





- Integrity of information is ensured in two steps:
  - Detecting errors when they occur at the receiver during transmission
  - Triggering retransmission or performing an error correction in the event that an error is detected

# Parity Checking

- One of the simplest error-detection schemes
- It refers to the use of parity bits to check that data has been transmitted accurately
- There two types of parity: odd and even
- Parity checking has limitations
  - It cannot detect an error when an even number of bits change in the same data unit

# Parity Checking

(with parity bits shown in boxes)

ASCII Character	Even Parity	Odd Parity
A	<span style="border: 1px solid black; padding: 2px;">0</span> 1000001	<span style="border: 1px solid black; padding: 2px;">1</span> 1000001
D	<span style="border: 1px solid black; padding: 2px;">0</span> 1000100	<span style="border: 1px solid black; padding: 2px;">1</span> 1000100
	 even parity bit 	 odd parity bit 
8	<span style="border: 1px solid black; padding: 2px;">1</span> 0111000	<span style="border: 1px solid black; padding: 2px;">0</span> 0111000
DEL	<span style="border: 1px solid black; padding: 2px;">1</span> 1111111	<span style="border: 1px solid black; padding: 2px;">0</span> 1111111

# Longitudinal Redundancy Check (LRC)

- Operates on a group of bytes
- Create a cross-grid matrix pattern to pinpoint a bad bit
- Produces a Block Check Character (BCC) to provide extra error-detection capabilities for a block of data
- Advantage
  - It is simple and improves the odds of detecting errors
  - Provides error correction at the receiver, which simply inverts the bad bit
- Disadvantage
  - It has significant overhead

# Example of LRC Implementation

Character	D	A	T	A		C	O	M	BCC
(LSB)	0	1	0	1	0	1	1	1	0
	0	0	0	0	0	1	1	0	1
ASCII	1	0	1	0	0	0	1	1	1
	0	0	0	0	0	0	1	1	1
Code	0	0	1	0	0	0	0	0	0
	0	0	0	0	1	0	0	0	0
(MSB)	1	1	1	1	0	1	1	1	0
Parity (odd)	1	1	0	1	0	0	0	1	1

LSB: Least Significant Bit  
 MSB: Most Significant Bit  
 BCC: Block Check Character

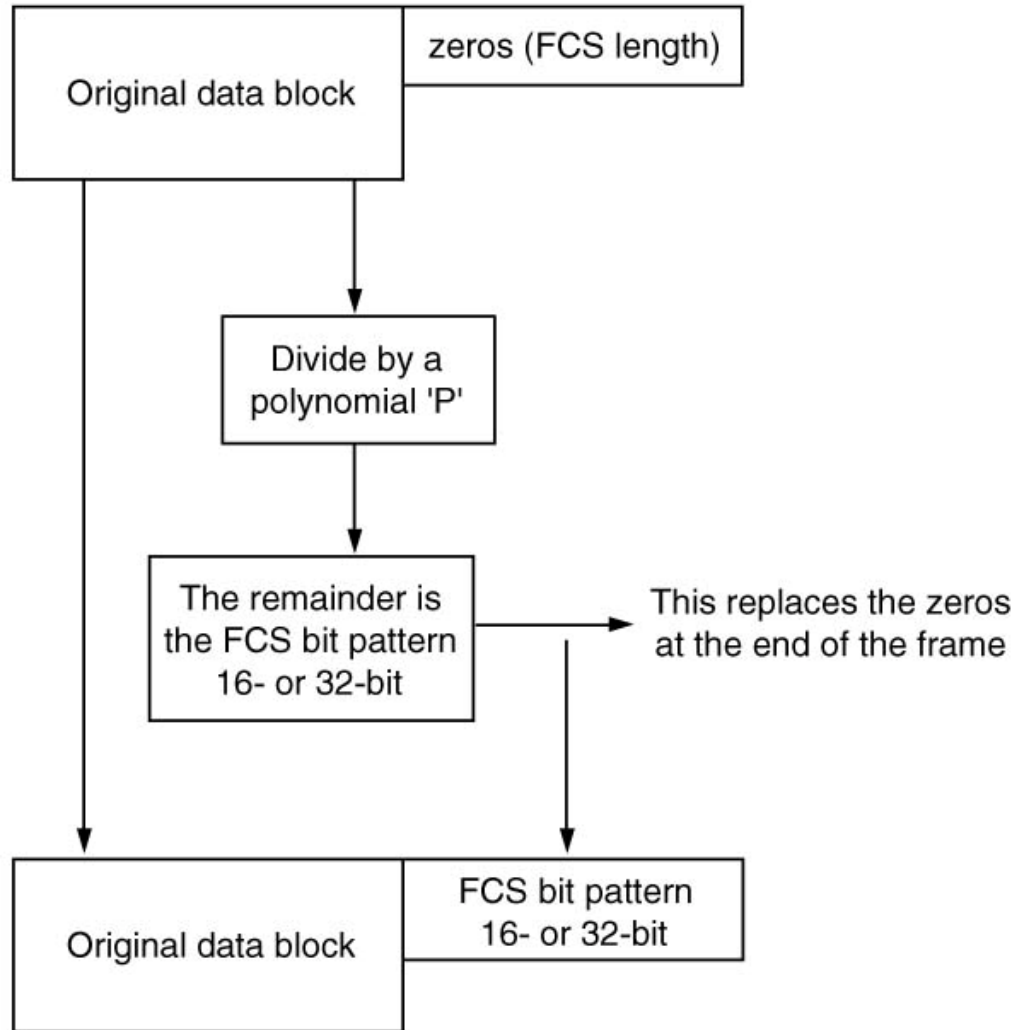
# Hamming Code

- Hamming Code is a error-detection-and-correction scheme for single-bit errors
- Generates several parity bits that are interspersed with data in a specific pattern
- One data bit affects more than one parity bit, so the bad bit can be detected
- Its error correction capability eliminates the need for retransmission
- It uses forward-error-correction
  - Error corrected by the receiving device

# Cyclic Redundancy Check (CRC)

- One of the most widely used, reliable, and efficient error-detection schemes
- Used in synchronous transmission where blocks of data can be several thousand bytes and where single bit errors occur less frequently as compared with multiple or burst errors
- CRC uses a unique mathematical algorithm, which is known to both the transmitter and the receiver
- The bit pattern (16 or 32 bits) that is used to verify the data is called a Frame Check Sequence (FCS)

# CRC Process Flowchart





# Data Link Protocols

- Data link layer deals with how data is logically packaged to cross from one user to another
- Data link protocols are divided into two broad categories:
  - Bit-oriented
    - Encode control information in single bits
    - HDLC is the most common bit-oriented protocol
  - Byte-oriented or Character-oriented
    - Encode control information in bytes
    - BISYNC is the most common byte-oriented protocol

# HDLC Bit-oriented Protocol

- HDLC
  - Allows every device to both send and receive information without being controlled by any other device, so that all devices have equal right to use the communication facility
  - Ethernet, Token Ring and FDDI are all based on the HDLC frame structure

Opening Flag	Station Address	Control Info.	Data Field	CRC	Closing Flag
-----------------	--------------------	------------------	---------------	-----	-----------------

## **An HDLC Frame Format**

An Opening Flag is a sequence of 8-bits, which marks the beginning of a packet, followed by a 16- or 32-bit Station Address. One to two bytes of control information describe the type of HDLC frame, routing parameters, and other packet identifiers. The variable Data Field or Raw Data is now inserted, followed by a 16- or 32-bit FCS (CRC) and a 8-bit Closing Flag, which marks the end of the HDLC frame. The HDLC frames are created by equipment that transmits the packet across the network.

# LAN Access Methods

- A LAN Access method describes how the devices access the network and share the transmission facilities
- By definition, a shared-media LAN has only one path to handle high-speed data. However, the total capacity of the path exceeds the transmission speed of any single station, so stations are usually unaware that they are sharing the medium.
- Popular LAN access methods are classified as non-contention or contention

# Polling and Selecting

- The Polling and Selecting access method is not very common because it requires the use of a central controller to execute and monitor the process

## **Polling:**

Polling refers to the process of a host computer asking an intelligent terminal if it has any data to send to the host computer. This task is typically accomplished by a front-end processor (FEP), which handles all the routine communications procedures for the host computer

## **Selecting:**

Selecting occurs when a host computer or a FEP sends data to a terminal after the terminal indicates that it is ready to accept data

# Token Passing

- Noncontention-based deterministic system
- A token circulates on the circuit from station to station
- The protocol controls which station can send messages by passing a token (3-bit frame) around the “ring”
- A transmitting station replaces the token with a message (a data frame with a modified token header)
- The message is passed from station to station until it reaches its destination station
- The receiving station makes a copy of the message and marks the token (header) to indicate it got the message
- The message continues around the ring until it reaches the sending station
- The sending station sees that the message was received and replaces it with a new token

# Carrier Sense Multiple Access (CSMA)

- Multiple Access
  - Any of the network devices can transmit data onto the network at will; there is no central controller
  - A broadcast network where all stations see all frames, regardless of whether they represent an intended destination
  - Each station must examine received frames to determine if the station is a destination. If so, the frame is passed to a higher protocol layer for appropriate processing
- Carrier Sense
  - Before sending data, stations listen to the network to see if it is already in use. If in use, the station wishing to transmit waits, otherwise it transmits

# CSMA/Collision Detection (CSMA/CD)

- Collision occurs when two stations listen for network traffic, hear none and transmit simultaneously damaging both transmissions
- Collision Detection enables stations to detect collisions, so they know when they must retransmit
- Used by Ethernet LANs



# CSMA/Collision Avoidance (CSMA/CA)

- Sender send a request-to-send (RTS) frame to receiver and indicates the time needed to complete data transmission
- Receiver send clear-to-send (CTS) frame, indicates time to complete data transmission and reserves channel for the sender
- Sender transmits the data and receiver responds with an ACK frame, ensuring reliable transmission
- RTS and CTS frames let other stations know of the data transmission so that collision is avoided
- Used by 802.11 wireless LANs

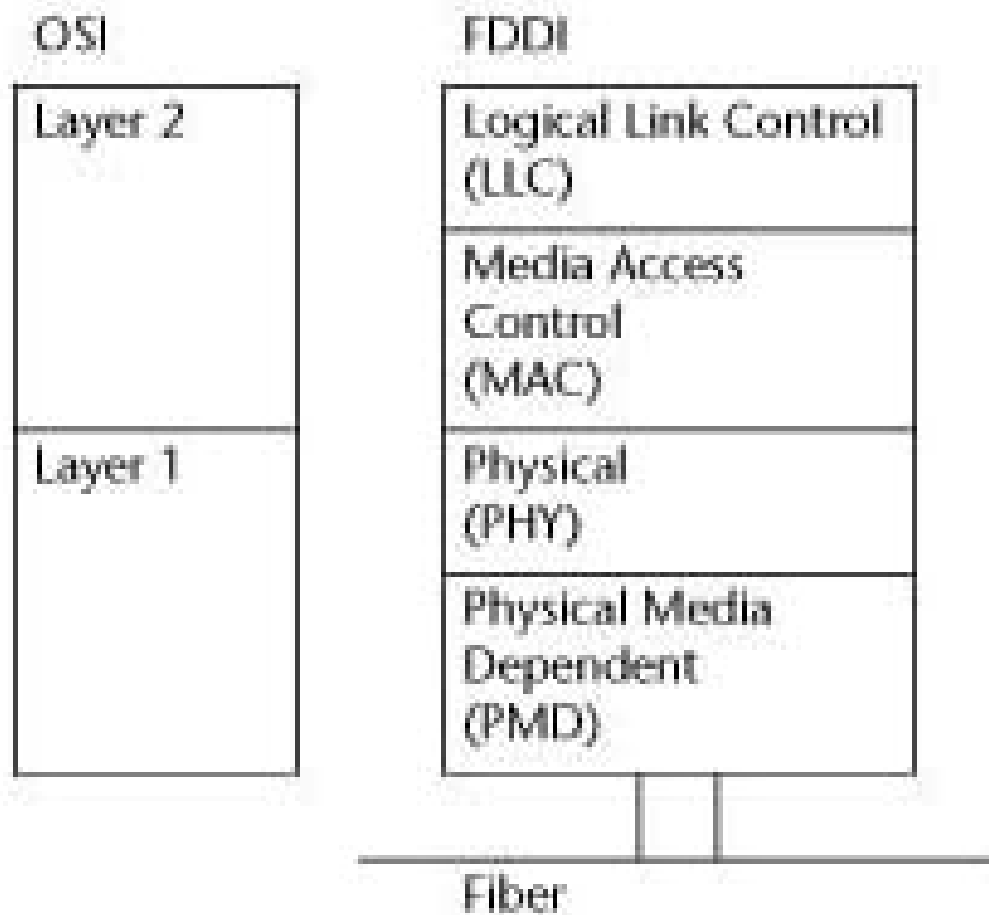
# LAN TECHNOLOGIES

- The ability to link a wide range of computers using a vendor-neutral network technology is an essential feature for today's LANs
- Most LANs must support a wide variety of computers purchased from different vendors, which requires a high degree of network interoperability
- Baseband LAN technologies include Token Ring, Ethernet, and Fiber Distributed Data Interface (FDDI)

# Token Ring

- IEEE 802.4 (Bus) or 802.5 (Ring) Standard for the Token Ring (Physical and Data Link Layers)
  - Protocol: Token Passing
  - Data Link Control Protocol: HDLC
  - Error Detection and Correction Method: CRC
  - Data Encoding Format: Differential Manchester
  - A MAU (Multistation Access Unit) transfers the token from port to port
  - Characteristics
    - Predictable response time even under heavy load
    - More robust compared with Ethernet, but also more expensive
    - Not very popular today due to its limited speed (16 Mbps)

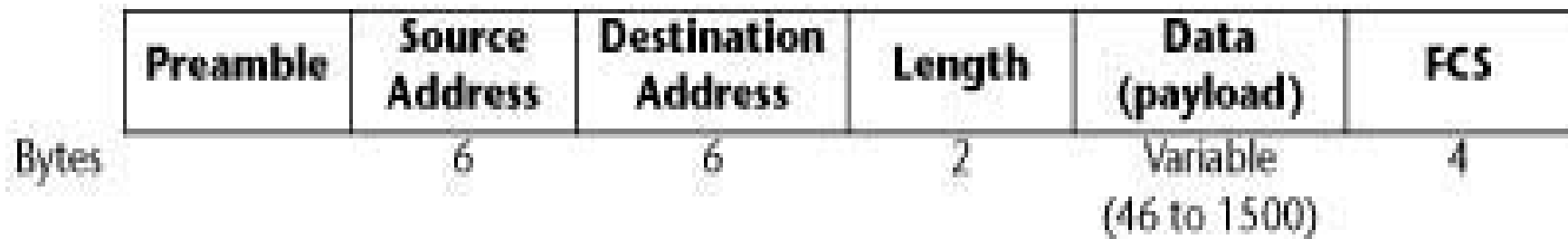
# FDDI



# Ethernet

- Formal specifications for Ethernet were published in 1980 by a multi-vendor consortium that created the DEC-Intel-Xerox (DIX) standard
- It marked a turning point in the evolution of experimental Ethernet into an open, production-quality system
- Ethernet and 802.3 have many common features
  - Protocol: CSMA/CD
  - Data Link Control Protocol: HDLC
  - Error Detection and Correction Method: CRC
  - Data Encoding Format: Differential Manchester

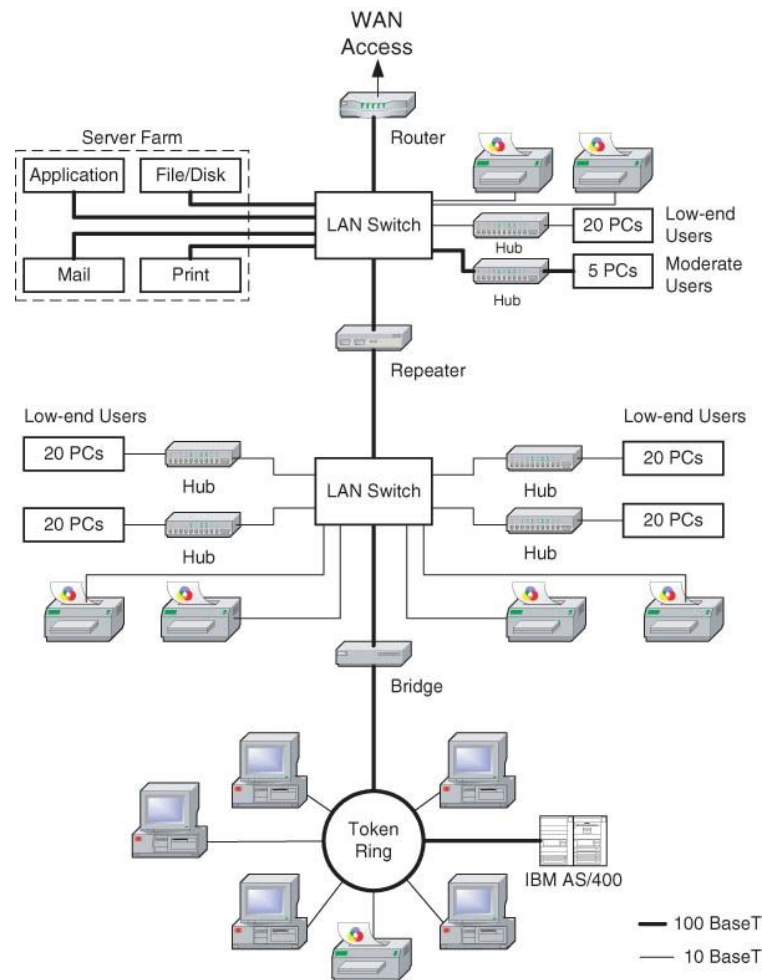
# Ethernet Frame Format



# Ethernet Frame

- Preamble
  - The alternating pattern of 1s and 0s tells receiving stations that a frame is coming. An additional byte serves to synchronize the frame-reception portions of all stations on the LAN.
- Destination and Source Addresses
  - Each address comprises of 6 bytes
- Length
  - Indicates the number of bytes of data
- Data
  - Payload or actual data, which can vary from 46 to 1500 bytes
- Frame Check Sequence (FCS)
  - Contains a four-byte CRC value
- Ethernet LANs are 10BaseT, 100BaseT, and 1000BaseT

# Typical 10BaseT and 100BaseT LAN Configuration





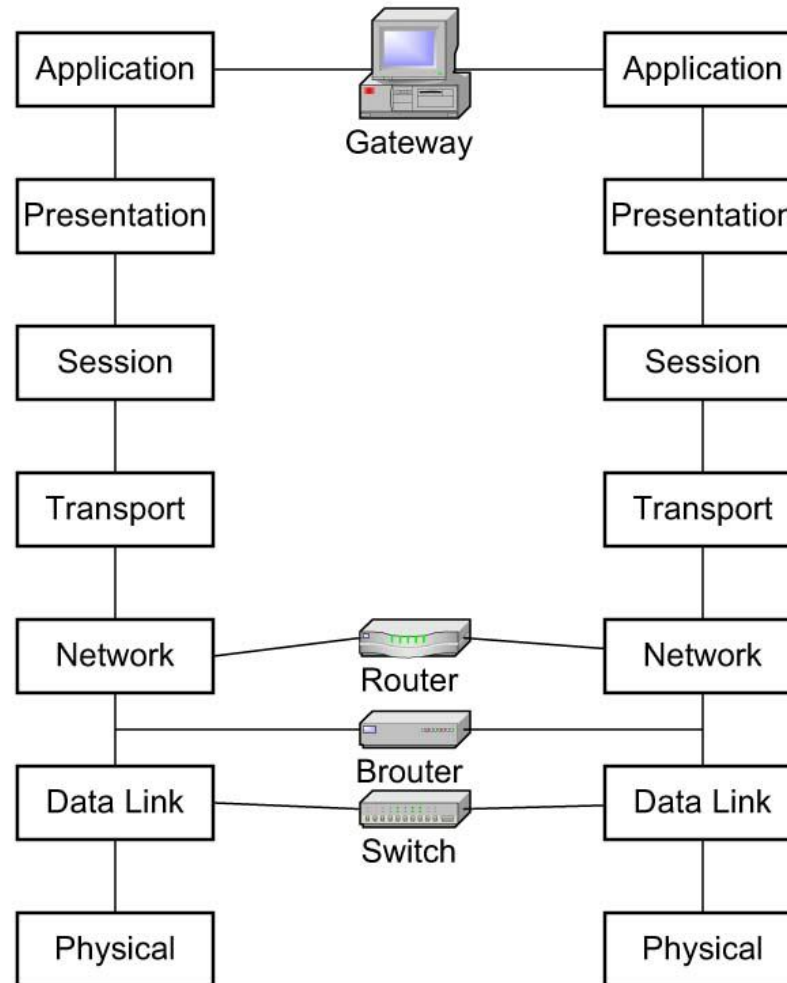
# LAN Configurations

- Client/Server
  - Most popular networking strategy
  - Servers provide special services to users
  - Clients make requests to use server resources
  - NIC enables a full-time, dedicated connection to the network
  - NOS controls the entire network
- Peer-to-Peer
  - Appropriate for a small group of users that may want to share some of their individual resources such as disk-drives, scanners and printers
  - NOS is installed on every machine that is part of the network

# Internetworking

- Internetworking is a comprehensive term for all the concepts, technologies, and generic devices that allow people and their computers to communicate across different kinds of networks
- Some Internetworking Devices are:
  - Repeaters
  - Bridges
  - Switches
  - Routers
  - Gateways

# Internetworking at various layers of the OSI model



# Repeaters

- A Repeater is the simplest and the least expensive internetworking device. It copies every messages it hears on LAN #1 to LAN #2, sometimes unnecessarily.
  - Operates at Layer 1 of the OSI model
  - It receives a signal, amplifies it, and then retransmits it along the next leg of the medium
  - If the two LANs connected with a repeater do not have a traffic problem, there is no need for a more complex approach. However, most LANs that are long enough to have reached their distance limitation probably have many users and there could be advantages to using more sophisticated devices than repeaters.

# Bridges

- A bridge is a device that operates at the data link layer of the OSI model
- It selectively forwards frames based on an examination of the MAC addresses in the frames
- It filters out the messages meant for the other stations
- A Bridge is used to interconnect networks using dissimilar protocols

# Characteristics of a Bridge

- A bridge connects one LAN to another LAN that uses the same protocol (for example, Ethernet or Token Ring)
- A transparent bridge automatically initializes itself and configures its own routing information after it has been enabled
- Since bridges buffer frames, it is possible to interconnect different segments which use different MAC protocols
- Subdividing the LAN into smaller segments, increases overall reliability and the network becomes easier to maintain
- Non-routable protocols like NETBEUI must be bridged
- Bridges help to localize network traffic by only forwarding data onto other segments as required (unlike repeaters)
- In complex networks, data may be sent over redundant paths, and the shortest path is not always taken

# Switch

- A switch is a device that is used to connect and distribute communications between a trunk line or backbone and individual nodes
- It operates at Layer 2 of the OSI model
- When you install a switch you are “collapsing the backbone” of the network
- A switch improves network performance
- Servers and Hubs may be connected to ports on the Switch
- Characteristics and Applications
  - Delivers more bandwidth
  - Simplifies network administration

# Router

- A “router” is a device that operates at the network layer of the OSI model
- It supports multiple protocols (such as TCP/IP, DecNet, SNA, IPX), and can be used to link LANs together locally or remotely as part of a WAN
- It controls network traffic and security in the process of delivering a message across one or more networks via the most appropriate path



# Characteristics of Routers

- Expensive piece of hardware
- Comes with its own administrative burden
- Can slow down the network
- Have a lower packet-filtering-and-forwarding rate as compared to switches
- Protocol-dependent and cannot handle protocols that are not routable
- The move now is towards implementing “switching routers”

# Gateways

- A Gateway is an inter-networking device that connects two or more computer networks that use different communications architectures
- Operates at Layer 7 of the OSI Model
- Compares and converts the communication protocols of one networking system with the communication protocols of another (usually proprietary) system
  - Example: Between Ethernet and SNA, where SNA (Systems Network Architecture) is the IBM Mainframe Protocol

# Channel Service Unit (CSU)

## Data Service Unit (DSU)

- Come in either stand-alone units or combination CSU/DSUs
- Their purpose is to encapsulate information into proper framing and ensure proper timing before connecting to the WAN
- At least one of these devices is required for any digital line termination
- CSU is used to connect a switched digital line such as a T-1 to a DCE device
  - Protects the line from electrical damage
  - Provides a way to test the circuit through loopback
- DSU is used to access dedicated lines

# Trunking

- Trunking lets companies increase the bandwidth from server to switch

