Physical and Data Link Layer

Message Switching	The entire message is stored and forwarded.	No need for a dedicated path.	Delays due to store-and-forward.	Email systems

Transmission Media

The medium through which data is transmitted from one device to another.

Wired Media

Type	**Description**	**Speed**	**Cost**	**Use Case**
Twisted Pair	Two insulated copper wires twisted together.	Up to 10 Gbps	Low	LANs, telephone lines
UTP	No shielding, common in Ethernet cables (Cat5e, Cat6).			
STP (Shielded Twisted Pair)	Shielding reduces interference.			
Coaxial Cable	Copper core with insulation and shielding.	Up to 1 Gbps	Medium	Cable TV, broadband
Fiber Optic Cable	Uses light signals to transmit data.	Up to 100+ Gbps	High	High-speed backbone, long distances, ISPs

Wireless Media

Type	Description	Range	Speed	Use Cases
Radio Waves	Omnidirectional, used in Wi-Fi and Bluetooth	Short to Medium	Medium	WLANs, mobile phones
Microwaves Unidirectional	Unidirectional, needs line-of-sight	Long	High	Satellite links, cellular
Infrared (IR)	Line-of-sight, no penetration through walls	Very short	Low	Remote controls
Satellite	Signals bounce off satellites in orbit	Global	Medium to High	Global communication

Switching Techniques

Switching is a technique used to transmit data across a network from source to destination. It determines how data is routed and delivered between network devices.

Comparison of Switching Techniques:

Technique	**Description**	**Advantage**	**Disadvantage**	**Use Case**
Circuit Switching	The dedicated communication path is established before data transfer.	Consistent and reliable connection.	Wastes bandwidth when idle.	Traditional telephone networks
Packet Switching	Data is divided into packets sent independently.	Efficient use of bandwidth.	Packets may arrive out of order.	Internet, VoIP

Framing

Framing is the process of dividing a continuous stream of data into manageable chunks called **frames** for transmission.

Purposes:

- Synchronization
- Error Detection
- Flow Management

Framing Techniques:

Technique	Description
Character Count	The frame starts with a count of the number of characters in the frame.
Byte Stuffing	Special characters added to distinguish data from control info (e.g., FLAG -> ESC FLAG).
Bit Stuffing	Inserts 0 after a sequence of 5 continuous 1s to avoid confusion with frame delimiters.
Clock-based (SONET)	Uses synchronization signals to mark frame boundaries.

Error Detection

1. Types of Errors in Networking

Error Type	Description	Example
Single-bit	One bit is flipped (0→1 or 1→0)	0101 → 0111
Burst Error	Multiple consecutive bits are corrupted	001100 → 110011

2. Common Error Detection Techniques

A. Parity Check

- **Concept:** Adds an extra bit (parity bit) to make the total number of 1s **even (even parity)** or **odd (odd parity)**.
- **Types:**
  - **Even Parity:** The Total number of 1s (including parity bit) must be even.
  - **Odd Parity:** The Total number of 1s (including parity bit) must be odd.
- **Example (Even Parity):**
  - Data: 1101 (3 bits → odd)
  - Parity bit added: 1 (to make total 1s = 4 → even)
  - Sent: 11011
- **Limitation:** Detects only an **odd number of bit errors** (fails if two bits flip).

B. Checksum

- **Concept:** The Sender computes a checksum (sum of data bytes) and appends it to the data. The receiver recalculates and compares.
- **Steps:**
  1. Divide data into fixed-size segments (e.g., 16-bit words).
  2. Sum all segments (ignore overflow).
  3. Take **1's complement** (invert bits) → Checksum.
  4. Append checksum to data.

  Limitation: Weak against certain errors (e.g., reordered data).

C. Cyclic Redundancy Check (CRC)

- **Concept:** Uses polynomial division to generate a checksum (CRC code).
- **Steps:**
  1. Choose a predefined **generator polynomial** (e.g., $x^3 + x + 1 \rightarrow 1011$).
  2. Append n zeros to the data (where n = degree of polynomial).
  3. Divide modified data by the polynomial (using XOR).
  4. Append remainder (CRC) to original data.

 Advantage: Detects **all single-bit, double-bit, and odd-length burst errors**.

D. Hamming Code

- **Concept:** Adds redundant bits to detect and correct single-bit errors.
- **Steps:**
  1. Insert parity bits at positions that are powers of 2 (1, 2, 4, 8...).
  2. Calculate parity for overlapping bit groups.
- **Example (4-bit data → 7-bit Hamming code):**
  - Data: 1001
  - Encoded: _ _ 1 _ 0 0 1 (positions 1,2,4 are parity bits)
  - Calculate parity:
    - P1 (positions 1,3,5,7): ? + 1 + 0 + 1 → Even parity → 0
    - P2 (positions 2,3,6,7): ? + 1 + 0 + 1 → Even parity → 0
    - P4 (positions 4,5,6,7): ? + 0 + 0 + 1 → Odd parity → 1
  - Final Hamming code: 0011001
- **Error Correction:** The Receiver recalculates parity to locate and flip the erroneous bit.

3. Comparison of Techniques

Method	Detects Single-bit?	Detects Burst Errors?	Corrects Errors?	Overhead
Parity	Yes	No (if even # of bits)	No	Low
Checksum	Yes	Partial	No	Medium
CRC	Yes	Yes (up to certain length)	No	Medium
Hamming	Yes	No	Yes (single-bit)	High

Real-World Applications

- **Parity:** Used in RAM error detection.
- **Checksum:** TCP/IP headers, UDP.
- **CRC:** Ethernet, Wi-Fi, ZIP files.
- **Hamming Code:** ECC memory, satellite communication.

MAC Protocols: CSMA/CD & CSMA/CA

1. Introduction to MAC Protocols

MAC (Media Access Control) protocols determine how devices share a communication channel to avoid collisions.

- **Used in:** Ethernet (wired) and Wi-Fi (wireless).
- **Goal:** Ensure fair and efficient transmission.

---

2. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Used in: Wired networks (Ethernet - IEEE 802.3).

How CSMA/CD Works

1. **Carrier Sense (CS):**
   - Device checks if the medium (cable) is free before sending.
2. **Multiple Access (MA):**
   - Multiple devices share the same medium.
3. **Collision Detection (CD):**
   - If two devices transmit simultaneously, → **collision is detected**.
   - Devices **stop**, wait for a random backoff time, then retry.

Key Features

✓ **Half-duplex mode** (devices can't send & receive simultaneously).
✓ **Collision detected via voltage spikes**.
✓ **Binary Exponential Backoff Algorithm:**

- After a collision, wait time = **random (0 to 2^n - 1) × slot time** (where n = # of collisions).

Limitations

- **Not suitable for wireless networks** (hidden terminal problem).
- **Inefficient in large networks** (long propagation delays).

---

3. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Used in: Wireless networks (Wi-Fi - IEEE 802.11).

How CSMA/CA Works

1. **Carrier Sense (CS):**
   - Device checks if the channel is idle.
2. **Collision Avoidance (CA):**
   - Uses **RTS/CTS (Request to Send / Clear to Send)** to reserve the channel.
   - Waits for **DIFS (DCF Interframe Space)** before transmitting.
3. **Random Backoff Timer:**
   - If busy, waits for a **random time (contention window)** before retrying.

Key Features

✓ **Full-duplex not required** (avoids collisions proactively).
✓ **Uses ACK frames** for successful transmission confirmation.
✓ **Handles hidden terminal problem** via RTS/CTS.

Limitations

❌ **Overhead due to RTS/CTS/ACK frames**.
❌ **Slower than CSMA/CD** due to avoidance mechanisms.

---

4. Comparison: CSMA/CD vs. CSMA/CA

Feature	CSMA/CD (Ethernet)	CSMA/CA (Wi-Fi)
Medium	Wired	Wireless
Collision Handling	Detects collisions	Avoids collisions
Duplex Mode	Half-duplex	Doesn’t require full-duplex
Mechanism	Listens while transmitting	Uses RTS/CTS/ACK
Efficiency	Faster in wired networks	Slower due to overhead
Backoff Algorithm	Binary Exponential	Similar, but with DIFS/SIFS

---

5. Real-World Applications

- **CSMA/CD:** Classic Ethernet (10BASE5, 10BASE2), **not used in modern Gigabit Ethernet** (full-duplex).
- **CSMA/CA:** Wi-Fi (802.11a/b/g/n/ac/ax), Bluetooth.