Computer Networks

Notes by
Kamal Kishor
(HandNotes)

Sr. No	Chapters	Page No
1	Introduction to Computer Networks (Basics, Types, History, Topologies)	1-9
2	Network Models (OSI, TCP/IP)	10-12
3	Physical Layer (Media, Encoding, Switching)	13-20
4	Data Link Layer (Error/Flow Control, MAC)	21-25
5	Network Layer (IP Addressing, Routing)	26-30
6	Transport Layer (TCP/UDP)	31-34
7	Application Layer (HTTP, FTP, SMTP, DNS)	35-37
8	Network Security (Threats, Defense)	38-41
9	Wireless Networks (Wi-Fi, Bluetooth, Mobile)	42-44
10	Network Management (SNMP)	45

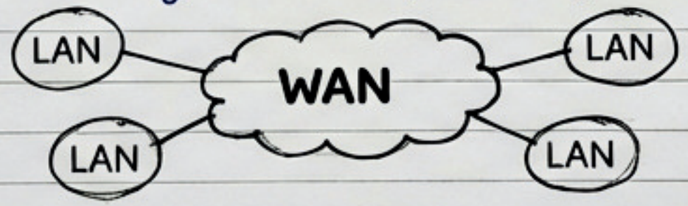
1. Introduction to Computer Networks

1.1 What is a Computer Network?

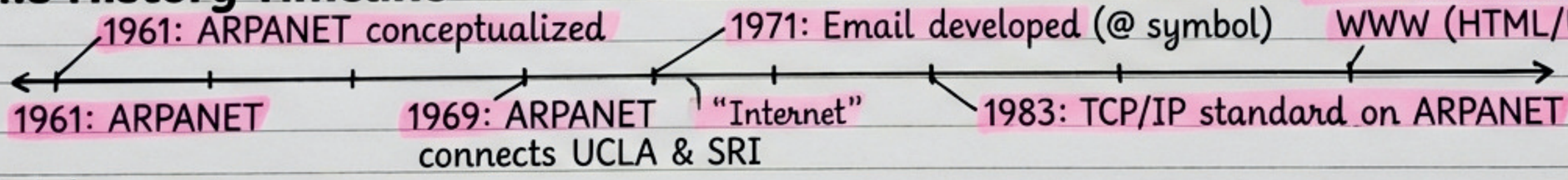
A computer network is an interconnection among two or more computers or computing devices to share data and resources. Nodes include servers, desktops, laptops, cellular phones.

1.2 Types of Networks

- PAN (Personal Area Network): Range ~10m. Wired (USB) or Wireless (Bluetooth). E.g., Phone to Laptop.
- LAN (Local Area Network): Room, building, campus. High speed (Ethernet 10Mbps - 1Gbps). Private ownership.
- MAN (Metropolitan Area Network): City-wide (e.g., Cable TV). Distance 30-40km. Connects multiple LANs.
- WAN (Wide Area Network): Country/Continent (Internet). Connects LANs/MANs via wired/wireless media.



1.3 History Timeline



1.4 Importance

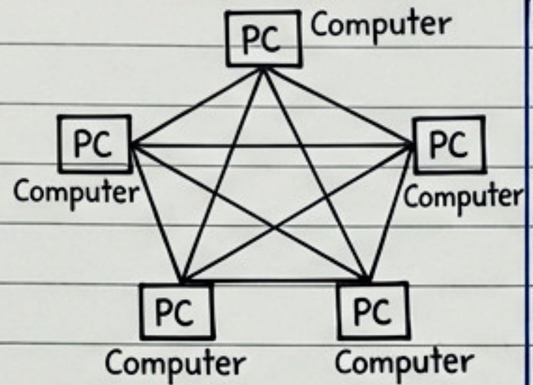
- Business communication
- Resource sharing (Printers, Storage)
- Cost-effective
- File sharing
- Overcoming geographical separation

1.5 Network Topologies

1. Mesh Topology

Every device connected to every other. Robust, secure, handles heavy traffic.

Drawback: Expensive cabling, complex.

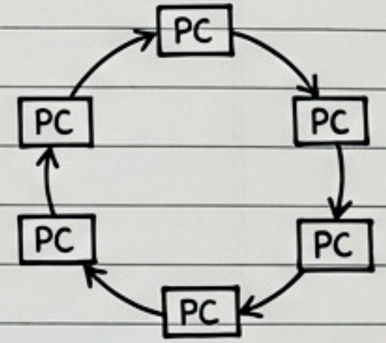


2. Ring Topology

Nodes connected in a closed loop.

Unidirectional flow.

Token passing.

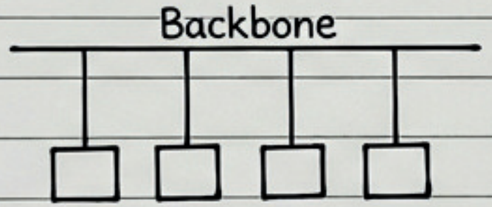


3. Bus Topology

Single backbone wire.

Easy install, cheap.

Failure of backbone = total failure.

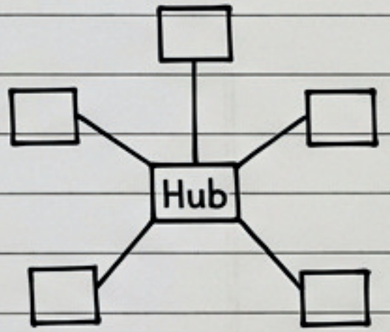


4. Star Topology

All nodes connect to central Hub/Switch.

Efficient, easy to fix.

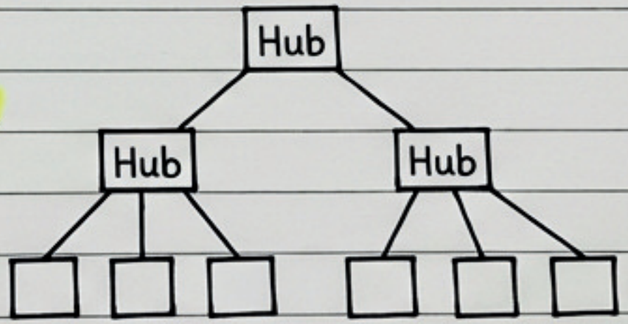
Hub failure = critical.



5. Tree/Hybrid Topology

Hierarchical (Star of Stars).

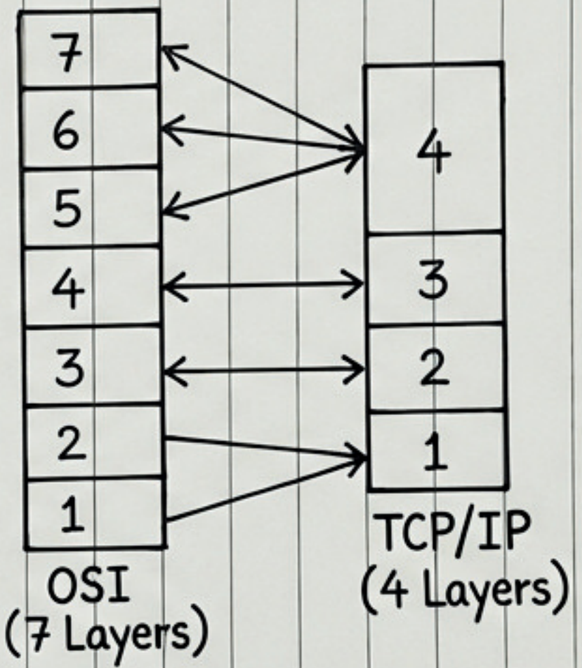
Used in WANs.



2. Network Models (The Blueprint)

2.1 OSI Model (7 Layers)

7. **Application**: User interface (HTTP, SMTP)
6. **Presentation**: Encryption, Compression
5. **Session**: Dialogue control
4. **Transport**: Reliability, Segments (TCP/UDP)
3. **Network**: Routing, Packets (IP)
2. **Data Link**: Error detection, Frames (MAC)
1. **Physical**: Transmission of raw bits, Cables



2.2 TCP/IP Model (4 Layers)

4. **Application**: Combines Session, Presentation, App
3. **Transport**: Host-to-host (TCP/UDP)
2. **Internet**: Routing (IP, ICMP)
1. **Network Interface**: Physical hardware/MAC

Comparison

	OSI	TCP/IP
1.	7 Layers	4 Layers
2.	Theoretical/Reference Model	Practical/Implementation Model
3.	Strict boundaries	Flexible

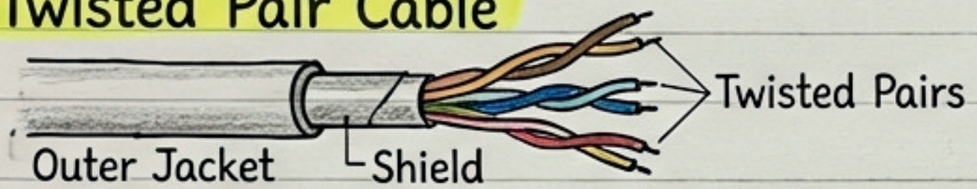
PREMIUM
classmate

3. Physical Layer - Transmission Media

Function: Transmitting raw bits over media.

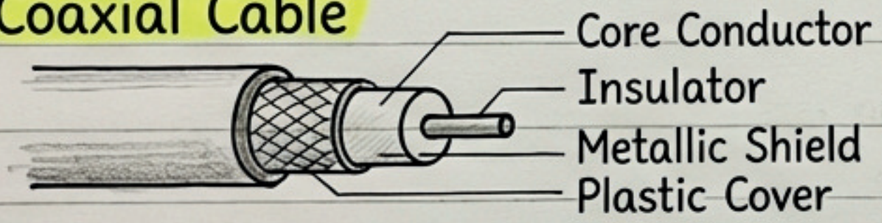
① Wired Media

① Twisted Pair Cable



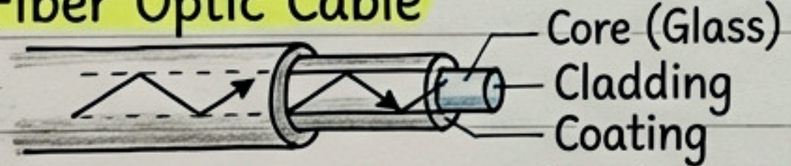
UTP (Unshielded) vs STP (Shielded).
Used in LAN/Telephony. Low cost, limited distance.

② Coaxial Cable



High bandwidth, Cable TV, Internet.

③ Fiber Optic Cable

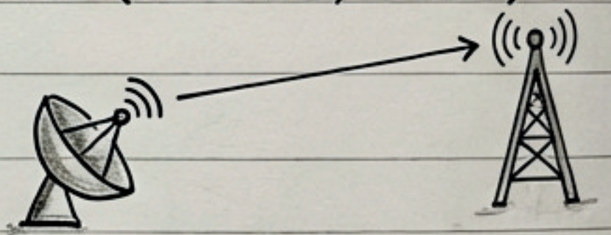


Uses light. Highest speed & distance.
Single Mode (SMF) vs Multi Mode (MMF).

② Wireless Media

✓ **Radio Waves**: Omni-directional (AM/FM, Wi-Fi). Wide coverage.

✓ **Microwaves**: Line-of-sight required (Satellites, Towers).



✓ **Infrared**: Short range, secure (TV Remotes). Cannot pass walls.

3. Signals, Multiplexing & Switching

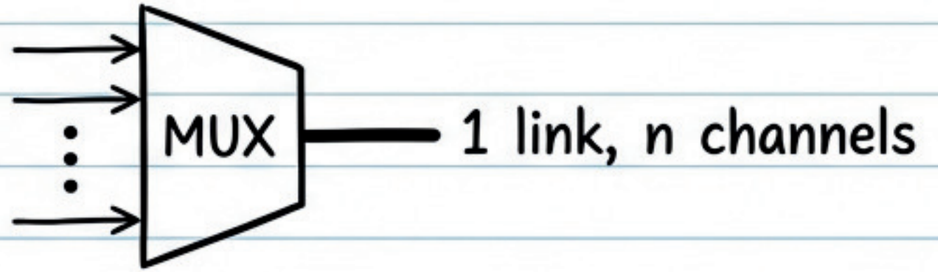
3.3 Encoding & Modulation

Encoding: Digital data → Digital signals (e.g., NRZ, Manchester).
Modulation: Digital/Analog data → Analog signals.
Techniques: AM (Amplitude), FM (Frequency), PM (Phase).

Hand-drawn sketch

3.4 Multiplexing (Sharing the Channel)

FDM: Frequency Division (Cable TV).
TDM: Time Division (Telephony).
CDM: Code Division (Cellular).



3.5 Switching

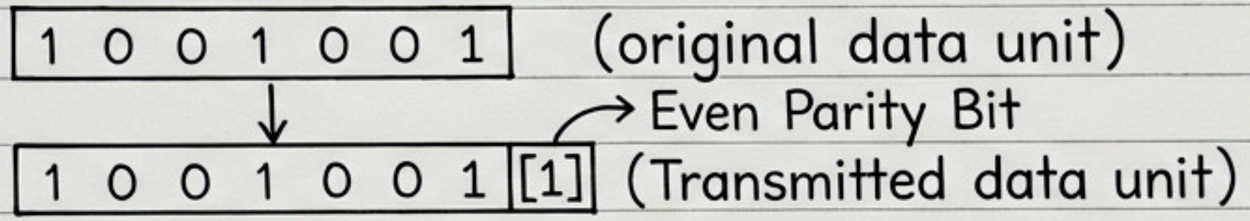
Circuit Switching: Dedicated physical path (Old Telephone).
Continuous flow, inefficient for bursty data.
Packet Switching: Data broken into packets. Shared paths (Internet).
Efficient, robust.

4. Data Link Layer - Error & Flow Control

Functions: Error detection, Flow control, Framing, Access control.

4.2 Error Detection Techniques

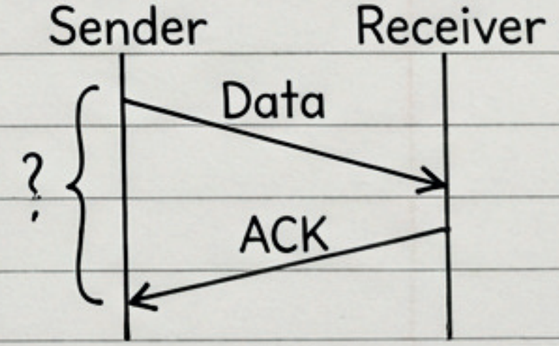
1. Parity Check: Add 1 bit. Even Parity (total 1s is even) / Odd Parity.



2. CRC (Cyclic Redundancy Check): Uses polynomial division. Good for burst errors.
3. Hamming Code: Error *correction*. Formula: $2^r \geq m + r + 1$.

4.3 Flow Control Protocols

1. Stop-and-Wait: Sender transmits one frame, waits for ACK. Simple but inefficient.
2. Sliding Window: Allows multiple frames in transit. Efficient.



4.4 MAC Sub-Layer & Standards

Role: Coordinates access to shared media to avoid collisions.

1. CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
   ↳ Used in: Wired Ethernet.
   → Algorithm: 1. Sense channel.
   2. Transmit if idle.
   3. If collision occurs, stop & retry after random backoff.

2. CSMA/CA (Collision Avoidance)
   ↳ Used in: Wireless (Wi-Fi).
   → Algorithm: Cannot detect collisions easily. Uses ACK to confirm success.
   Senses channel before sending.

3. Ethernet Standards (IEEE 802.3)
   - Standard Ethernet: 10 Mbps.
   - Fast Ethernet: 100 Mbps.
   - Gigabit Ethernet: 1 Gbps.

4. Wireless LAN (IEEE 802.11)
   - Operates using CSMA/CA.
   - Frequencies: 2.4 GHz / 5 GHz.

5. Network Layer - IP Addressing

notes by ~kamal kishor

Role: Logical addressing and path determination.

5.3 IPv4 Addressing

- 32-bit address. Format: Dot-decimal (e.g., 192.168.1.1).

Class A:	1.0.0.0 to 126... (Large networks)
Class B:	128... to 191... (Medium)
Class C:	192... to 223... (Small/LAN)
Class D:	Multicast / Class E: Reserved

5.4 IPv6 Addressing

- 128-bit address. Format: Hexadecimal (e.g., 2001:0db8...)
- Why? Solves IPv4 address exhaustion.

5.5 Subnetting

- Dividing a large network into smaller sub-networks.
- Subnet Mask: Determines Network vs Host portion.
- CIDR Notation: e.g., 192.168.1.0/24. → 192.168.1.0/24
- Benefits: Reduces broadcast traffic, improves security.

5. Routing & Protocols

Routing Algorithms

Static	Dynamic
Manually configured. Good for small networks.	**Adapts automatically.** - **Distance Vector:** Bellman-Ford alg. Periodic updates. Protocol: **RIP** (Metric: Hops). - **Link State:** Dijkstra's alg. Complete map. **Protocol:** **OSPF** (Metric: Cost/Speed). - **BGP:** Path vector protocol for the Internet (Autonomous Systems).

Helper Protocols

- **ICMP** (Internet Control Message Protocol): Diagnostics (Ping, Echo). Error reporting.
- **NAT** (Network Address Translation): Converts Private IP ↔ Public IP. Conserves IPv4.
- **ARP** (Address Resolution Protocol): Maps IP Address → MAC Address.

6. Transport Layer

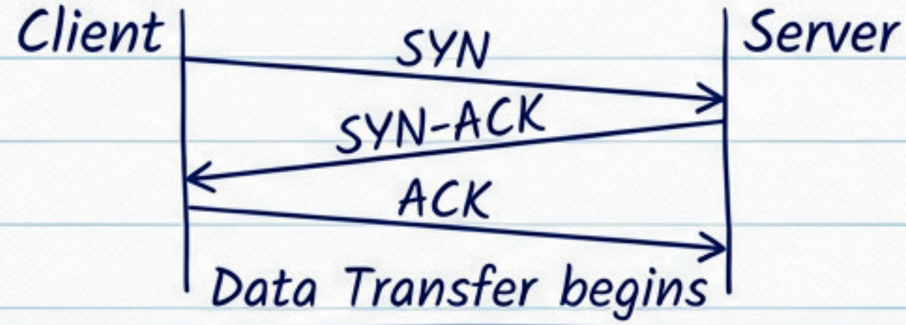
notes by
~kamal kishor

Role: End-to-end delivery, segmentation, reliability.

6.2 TCP (Transmission Control Protocol)

- Connection-oriented, Reliable, Ordered.
- Uses: Web (HTTP), Email, File Transfer.

TCP 3-Way Handshake



6.3 UDP (User Datagram Protocol)

- Connectionless, Unreliable, Fast.
- Uses: Streaming, Gaming, VoIP, DNS.

6.4 Ports & Sockets

- Socket = IP Address + Port Number.
- Well-known Ports: HTTP (80), FTP (21).

7. Application Layer Protocols

Role: Interface for users to access network services.

Web Protocols

- HTTP (HyperText Transfer Protocol): Foundation of WWW.
- HTTPS: Secure HTTP using SSL/TLS encryption.
- WWW: Interlinked hypertext documents.
- URL (Uniform Resource Locator): Address of resource.

File Transfer

- FTP: Standard file transfer.
- SFTP: Secure FTP (uses SSH).

Email Protocols

- SMTP: Sending email (Push).
- POP3: Retrieving email (Download & Delete).
- IMAP: Accessing email (Sync across devices).

DNS (Domain Name System)

- Translates Domain Names (google.com) → IP Addresses.
- Like the "Phonebook" of the internet.

8. Network Security - Threats

Premium Classmate

Goal (CIA Triad): Confidentiality, Integrity, Availability.

Common Threats

1. Malware: Malicious software. Viruses, Worms, Ransomware, Spyware.

2. Phishing: Social engineering (fake emails) to steal credentials.
3. DDoS (Distributed Denial of Service): Overwhelming a server with excessive traffic.
4. Man-in-the-Middle (MitM): Intercepting communication between two parties.
5. SQL Injection: Injecting malicious code into database inputs.

8. Defense & Cryptography

Premium classmate

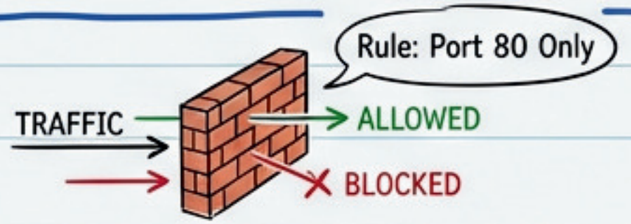
8.3 Cryptography

↳ **Symmetric Encryption:** Single key for encrypt/decrypt (e.g., AES). Fast.

↳ **Asymmetric Encryption:** Public Key (Encrypt) + Private Key (Decrypt) (e.g., RSA).

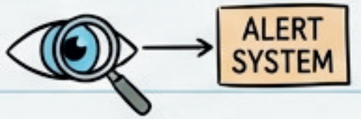
↳ **Digital Signatures:** Verify authenticity.

8.4 Defense Tools



↳ **Firewalls:** Filter traffic based on rules (Packet filtering).

↳ **IDS** (Intrusion Detection System): Monitors for suspicious activity.



8.5 Protocols & VPN

↳ **VPN** (Virtual Private Network): Secure tunnel over public internet.

↳ **SSL/TLS:** Secures web traffic (HTTPS).

↳ **IPSec:** Secures IP packets (used in VPNs).

9. Wireless & 10. Management

9. Wireless Networks

- Wi-Fi Standards (IEEE 802.11):
  - a -> b -> g -> n (MIMO) -> ac -> ax (Wi-Fi 6)
- Bluetooth: Short range (10m), Piconets. BLE for IoT.
- Mobile Generations:
  - 3G: Broadband.
  - 4G (LTE): IP-based, High speed.
  - 5G: Ultra-fast, Low latency, Massive IoT.

10. Network Management (SNMP)

- Simple Network Management Protocol.
- Components: Manager (NMS) <-> Agent (Managed Device).
- Operations: Get (Read), Set (Write), Trap (Alert).

End of Notes