Comprehensive Computer Networking Notes – Fully Explained

---

1. Introduction to Computer Networking

A **computer network** is a set of interconnected devices that communicate and share resources using communication channels. Networking enables data transmission between systems regardless of distance or location.

Core Characteristics:

- **Connectivity:** Enables device-to-device communication.
- **Resource Sharing:** Multiple devices can share printers, storage, applications.
- **Scalability:** Networks can grow from 2 devices to millions (like the Internet).
- **Fault Tolerance:** Some networks use redundancy to avoid downtime.

Real-World Example:
An office network allows employees to share a single printer and access shared files stored on a central server, even if they are in different rooms.

Diagram Idea:
A small office with PCs connected to a switch, the switch linked to a router, and the router linked to the internet.

---

2. Network Fundamentals

Types of Networks:

- **LAN (Local Area Network):**
    - Covers small geographical area (office, school, home).
    - High speed (100 Mbps – 10 Gbps).
    - Controlled by a single organization.
    - Example: Your home Wi-Fi.
- **WAN (Wide Area Network):**

    - Covers large areas (cities, countries).
    - The Internet is the largest WAN.
    - Often managed by multiple organizations.
    - Example: Banking networks connecting branches nationwide.
- **MAN (Metropolitan Area Network):**
    - Covers a city or large campus.
    - Example: Cable TV networks.
- **WLAN (Wireless LAN):**
    - Wireless form of LAN using Wi-Fi standards (IEEE 802.11).
    - Example: Wi-Fi in coffee shops.

---

3. Network Topologies

The layout or structure of how network devices are connected.

- **Bus Topology:**
    - All devices connected to a single backbone cable.
    - Low cost but single cable failure brings network down.
    - Example: Older Ethernet networks.
- **Star Topology:**
    - All devices connected to a central hub/switch.
    - Easy troubleshooting; if one link fails, others stay up.
    - Example: Modern office LANs.
- **Ring Topology:**
    - Devices connected in a loop; data travels in one direction.
    - Failure of one device can disrupt entire network unless dual ring is used.
    - Example: Some MANs.
- **Mesh Topology:**

- Each device connects to all others.
- Very reliable, expensive to set up.
- Example: Military networks.

---

4. Network Devices

- **Hub:**
  - Broadcasts data to all devices.
  - Works at OSI Layer 1.
  - No intelligence.
- **Switch:**
  - Sends data only to the intended device using MAC addresses.
  - Works at Layer 2.
  - Increases efficiency.
- **Router:**
  - Connects different networks.
  - Works at Layer 3.
  - Uses IP addresses to forward data.
- **Access Point (AP):**
  - Extends wireless coverage.
  - Connects wireless devices to a wired network.
- **Firewall:**
  - Filters traffic based on rules.
  - Can be hardware or software.

---

5. Network Protocols

Definition:
Rules that govern how devices communicate over a network.

- **TCP/IP:** Foundation of internet communication.
- **HTTP/HTTPS:** Web page transfer; HTTPS adds encryption.
- **FTP:** File transfers between computers.
- **DNS:** Translates domain names to IP addresses.
- **SMTP/IMAP/POP3:** Email sending/receiving.

Example:
When you visit www.youtube.com, DNS resolves the name to an IP, HTTP fetches the site, and TCP ensures data arrives correctly.

---

6. OSI Model

A **conceptual framework** with 7 layers:

1. **Physical:** Cables, connectors, signals.
2. **Data Link:** MAC addresses, error detection.
3. **Network:** IP addressing, routing.
4. **Transport:** TCP/UDP, reliability.
5. **Session:** Manages communication sessions.
6. **Presentation:** Encryption, compression.
7. **Application:** User-facing services (web browsers, email).

Tip: Remember with "**Please Do Not Throw Sausage Pizza Away**".

---

7. TCP/IP Model

Real-world version of OSI with 4 layers:

1. **Network Access:** Physical + Data Link.
2. **Internet:** IP routing.
3. **Transport:** TCP/UDP.

4. **Application:** HTTP, FTP, SMTP, DNS.

---

8. IP Addressing & Subnetting

- **IPv4:** 32-bit addresses (e.g., 192.168.1.1).
- **IPv6:** 128-bit addresses (e.g., 2001:db8::1).
- **Subnetting:** Dividing a network into smaller parts.

Why Subnet?

- Better security.
- Reduced congestion.
- Department separation.

---

9. Network Routing Protocols

- **RIP:** Distance vector, max 15 hops.
- **OSPF:** Link state, uses cost metric.
- **EIGRP:** Hybrid protocol, Cisco proprietary.

---

10. Network Security Measures

- **Firewalls:** Block unwanted traffic.
- **VPN:** Encrypts communication.
- **ACLs:** Control who can access resources.
- **Encryption:** Protects data from interception.

---

11. Network Threats

- **Malware:** Virus, worm, ransomware.
- **Phishing:** Fake emails to steal credentials.
- **DDoS:** Flooding a server with traffic.

- **MITM:** Intercepting and altering communication.

---

12. Wireless Networking

- **Wi-Fi:** IEEE 802.11 standards.
- **Bluetooth:** Short-range, personal area networking.
- **5G:** High-speed mobile networking.

---

13. Network Management Tools

- **Ping:** Checks connectivity.
- **Traceroute:** Shows path packets take.
- **Wireshark:** Captures network traffic.
- **SNMP:** Monitors and manages devices.

---

14. Cloud Networking

- **Public Cloud:** AWS, Azure.
- **Private Cloud:** Internal organization use.
- **Hybrid Cloud:** Combination of both.

---

15. SDN & NFV

- **SDN:** Separates control plane from data plane.
- **NFV:** Runs network functions on virtual machines instead of hardware.

---

16. Network Architectures

- **Client-Server:** Centralized services.
- **Peer-to-Peer:** Direct device communication.

---

17. Quality of Service (QoS)

- Prioritizes important traffic.
- Example: VoIP over file downloads.

---

18. Network Simulation Tools

- **Cisco Packet Tracer:** For learning.
- **GNS3:** For professional network simulation.
- **NetSim:** Vendor-specific training.
