Computer Networking -

Definition

Computer Networking is the practice of connecting multiple computing devices (computers, servers, mobile devices, IoT devices, etc.) to share data, resources, and services over wired or wireless communication channels.

Purpose

- **Data Sharing** → Transfer files, messages, media between devices.
- **Resource Sharing** → Use printers, storage, and internet from one central point.
- **Communication** → Enable real-time or delayed communication.
- **Centralized Management** → Control, monitor, and update devices from a single location.

Basic Components

1. **Nodes** → Devices on the network (PC, router, server, smartphone).
2. **Links** → Communication paths (Ethernet cables, Wi-Fi signals, fiber optic).
3. **Protocols** → Rules for communication (TCP/IP, HTTP, FTP).
4. **Networking Devices** →
    - **Router** → Connects different networks.
    - **Switch** → Connects devices in a local network.
    - **Hub** → Basic device for data broadcasting.
    - **Firewall** → Secures network traffic.

Types of Networks (By Scale)

- **LAN (Local Area Network)** → Small area like office/home.
- **MAN (Metropolitan Area Network)** → City-wide network.
- **WAN (Wide Area Network)** → Large scale, connects multiple cities or countries (e.g., Internet).
- **PAN (Personal Area Network)** → Very small range like Bluetooth.

Network Topologies

- **Bus** → Single cable connection.
- **Star** → All devices connected to a central switch.
- **Ring** → Devices connected in a loop.
- **Mesh** → Each device connects to every other device.

Protocols in Networking

- **TCP/IP** → Internet communication.
- **HTTP/HTTPS** → Web communication.
- **FTP/SFTP** → File transfer.
- **SMTP/IMAP/POP3** → Email.

- **DNS** → Domain name to IP mapping.

Importance in Ethical Hacking

- Understanding how data flows helps in sniffing, spoofing, and intrusion testing.
- Helps identify vulnerabilities in network configuration.
- Essential for penetration testing, exploiting weak protocols, and securing communications.

📝 Short Notes: Computer Networking

- **Definition** → Interconnection of devices to share resources & data.
- **Purpose** → Data sharing, resource sharing, communication, central management.
- **Components** → Nodes, Links, Protocols, Networking Devices.
- **Types** → LAN, MAN, WAN, PAN.
- **Topologies** → Bus, Star, Ring, Mesh.
- **Protocols** → TCP/IP, HTTP, FTP, SMTP, DNS.
- **Ethical Hacking Use** → Understanding data flow, sniffing, spoofing, penetration testing.

Types of Networks -

1. LAN (Local Area Network)

- **Coverage:** Small area (office, home, school).
- **Speed:** High (100 Mbps – 10 Gbps).
- **Ownership:** Usually private.
- **Use Case:** File sharing, printer sharing within an office.
- **Security Risks:** Unauthorized access from inside users, malware spread.

2. MAN (Metropolitan Area Network)

- **Coverage:** City or large campus.
- **Speed:** Moderate to high (10 Mbps – 1 Gbps).
- **Ownership:** Can be public or private.
- **Use Case:** Connects multiple LANs in a city (e.g., city-wide Wi-Fi).
- **Security Risks:** Data interception if not encrypted.

3. WAN (Wide Area Network)

- **Coverage:** Large geographical areas (countries, continents).
- **Speed:** Lower than LAN but improving (1 Mbps – 1 Gbps+).
- **Ownership:** Often public (Internet).
- **Use Case:** Internet, corporate branch connections.

- **Security Risks:** Man-in-the-middle attacks, DDoS, packet sniffing.

4. PAN (Personal Area Network)

- **Coverage:** Very short range (few meters).
- **Speed:** Varies (Bluetooth ~2 Mbps, USB much higher).
- **Ownership:** Always private.
- **Use Case:** Mobile-to-headset, phone-to-laptop.
- **Security Risks:** Bluetooth hacking (Bluejacking, Bluesnarfing).

5. WLAN (Wireless Local Area Network)

- **Coverage:** Similar to LAN but wireless.
- **Technology:** Wi-Fi (IEEE 802.11).
- **Use Case:** Wireless office/home networks.
- **Security Risks:** Weak Wi-Fi passwords, WEP encryption crack.

6. SAN (Storage Area Network)

- **Coverage:** Specialized network for data storage devices.
- **Use Case:** Datacenter storage, backups.
- **Security Risks:** Unauthorized access to sensitive data.

7. VPN (Virtual Private Network)

- **Coverage:** Virtual network over the Internet.
- **Use Case:** Secure remote access, anonymity.
- **Security Risks:** Weak VPN encryption or misconfiguration.

8. CAN (Campus Area Network)

- **Coverage:** Multiple LANs in a university or corporate campus.
- **Use Case:** Connecting departments/buildings.
- **Security Risks:** Internal data leaks.

📝 Short Notes: Types of Networks

- **LAN** → Small area, high speed, private.
- **MAN** → City-wide, connects multiple LANs.
- **WAN** → Country/continent scale, includes Internet.
- **PAN** → Personal range (Bluetooth, USB).
- **WLAN** → Wireless LAN using Wi-Fi.
- **SAN** → Storage device network for data centers.
- **VPN** → Secure virtual network over Internet.
- **CAN** → Multiple LANs in a campus.

How LAN, MAN & WAN Work -

1. LAN (Local Area Network) – Working

- **Setup:**
  - Devices (PCs, printers, servers) connect via Ethernet cables or Wi-Fi.
  - A **switch** or **hub** acts as the central connection point.
  - A **router** may connect the LAN to the Internet.
- **Communication:**
  - Uses **MAC addresses** at the data link layer for local communication.
  - **TCP/IP** is used for data transfer across devices.
- **Data Flow:**
  - Packets travel from one device to another within milliseconds.
  - Limited to a local scope, so it's fast and low-latency.
- **Security Concerns:**
  - If someone plugs into the network physically or hacks Wi-Fi, they can sniff traffic with tools like **Wireshark**.

2. MAN (Metropolitan Area Network) – Working

- **Setup:**
  - Connects multiple LANs across a city using fiber optic cables, microwave links, or wireless connections.
  - Often uses **service providers** or **municipal infrastructure**.
- **Communication:**
  - Uses high-speed backbone connections (like **Metro Ethernet**) to link LANs.
  - Can operate using ring or mesh topologies for redundancy.
- **Data Flow:**
  - Data passes through **routers and switches** across multiple locations.
  - Managed by ISPs or local authorities.
- **Security Concerns:**
  - Traffic may pass through public infrastructure → requires **VPN or encryption** to prevent interception.

3. WAN (Wide Area Network) – Working

- **Setup:**
  - Connects LANs and MANs across countries or continents.
  - Uses undersea fiber optic cables, satellites, and cellular networks.
  - Managed by multiple ISPs and telecom companies.
- **Communication:**
  - Uses the **Internet backbone** with routing protocols like **BGP (Border Gateway Protocol)**.
  - Data is split into packets and routed via the fastest/available path.
- **Data Flow:**

    - Packets travel through multiple intermediate devices like routers, gateways, and firewalls before reaching the destination.
- **Security Concerns:**
    - Susceptible to **MITM attacks, DDoS, packet sniffing, routing manipulation** if security is weak.

Ethical Hacking Relevance

- **LAN:** Good target for penetration testing inside offices; can sniff or spoof ARP.
- **MAN:** Test for data leaks between sites; check encryption.
- **WAN:** Test public-facing servers, firewalls, and VPN gateways.

📝 Short Notes: How They Work

- **LAN:**
    - Small area; devices connected via switch/router.
    - Uses MAC addresses & TCP/IP.
    - Very fast, low latency.
    - Risk: Unauthorized access, packet sniffing.
- **MAN:**
    - Connects LANs across a city using fiber/microwave.
    - Uses Metro Ethernet & backbone links.
    - Risk: Public infrastructure interception.
- **WAN:**
    - Connects countries/continents via ISPs, satellites, fiber.
    - Uses BGP & Internet backbone.
    - Risk: MITM, DDoS, routing attacks.

Important Entities in Computer Networking -

In networking, entities refer to the main components, devices, and elements that make communication possible.

1. Networking Devices

- **Router → Connects different networks (LAN to WAN), forwards data packets based on IP addresses.**
- **Switch → Connects devices within a LAN, forwards data based on MAC addresses.**
- **Hub → Broadcasts data to all devices (less secure & outdated).**
- **Access Point → Enables wireless (Wi-Fi) connections.**

- **Firewall → Filters incoming/outgoing traffic for security.**
- **Gateway → Acts as an entry/exit point between networks.**
- **Modem → Converts digital data to analog (for phone lines) or vice versa.**

2. Networking Protocols

- **TCP/IP → Base protocol for Internet communication.**
- **HTTP/HTTPS → For web browsing (HTTPS is secure).**
- **FTP/SFTP → For file transfers.**
- **SMTP/IMAP/POP3 → For email.**
- **DNS → Translates domain names to IP addresses.**
- **DHCP → Assigns IP addresses automatically.**

3. Addresses & Identifiers

- **IP Address → Unique identifier for devices (IPv4/IPv6).**
- **MAC Address → Hardware-based address for each network interface.**
- **Port Numbers → Identifies specific processes/services (e.g., 80 for HTTP).**
- **Subnet Mask → Defines network & host portions of an IP address.**

4. Transmission Media

- **Wired → Ethernet cables (Cat5, Cat6), fiber optic cables.**
- **Wireless → Wi-Fi, Bluetooth, satellite, infrared.**

5. Network Models & Layers

- **OSI Model → 7 layers (Physical → Application).**
- **TCP/IP Model → 4 layers (Network Access → Application).**

6. Network Services

- **DNS Service → Converts domain names to IP.**
- **VPN Service → Secure tunnel over the Internet.**
- **Proxy Server → Acts as intermediary for requests.**

Ethical Hacking Relevance

- **Knowing these entities helps in footprinting (finding devices & services), scanning (detecting open ports, IP ranges), and exploitation (attacking vulnerable services or devices).**

📝 Short Notes: Important Networking Entities

- **Devices: Router, Switch, Hub, Access Point, Firewall, Gateway, Modem.**
- **Protocols: TCP/IP, HTTP/HTTPS, FTP, SMTP, DNS, DHCP.**
- **Identifiers: IP Address, MAC Address, Port Number, Subnet Mask.**
- **Media: Wired (Ethernet, Fiber), Wireless (Wi-Fi, Bluetooth).**
- **Models: OSI (7 layers), TCP/IP (4 layers).**

- **Services: DNS, VPN, Proxy.**

IP Addresses -

1. Definition

An **IP address (Internet Protocol address)** is a unique numerical label assigned to each device connected to a network that uses the Internet Protocol for communication.
It serves **two main purposes**:

1. **Identification** → Uniquely identifies a device.
2. **Location Addressing** → Indicates the device's position in a network.

2. Types of IP Addresses

A. Based on Version

- **IPv4 (Internet Protocol version 4)**
  - 32-bit address, written as four decimal numbers (0–255) separated by dots.
  - Example: 192.168.1.1
  - Total: ~4.3 billion addresses.
- **IPv6 (Internet Protocol version 6)**
  - 128-bit address, written in hexadecimal, separated by colons.
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - Total: ~340 undecillion addresses.

B. Based on Usage

- **Private IP Address** → Used within local networks (not routable on the internet).
  - IPv4 Ranges:
    - 10.0.0.0 to 10.255.255.255
    - 172.16.0.0 to 172.31.255.255
    - 192.168.0.0 to 192.168.255.255
- **Public IP Address** → Assigned by ISP, used for internet communication.
- **Static IP** → Fixed IP address that does not change.
- **Dynamic IP** → Assigned temporarily by DHCP and changes over time.

3. IP Address Classes (IPv4)

- **Class A** → 1.0.0.0 – 126.0.0.0 (Large networks)
- **Class B** → 128.0.0.0 – 191.255.0.0 (Medium networks)
- **Class C** → 192.0.0.0 – 223.255.255.0 (Small networks)
- **Class D** → 224.0.0.0 – 239.255.255.255 (Multicast)

- **Class E** → 240.0.0.0 – 255.255.255.255 (Research)

4. Special IP Addresses

- **Loopback Address** → 127.0.0.1 (Test your own machine).
- **Broadcast Address** → Sends data to all devices in a network.
- **APIPA Address** → 169.254.x.x (When DHCP fails).

5. IP in Ethical Hacking

- **Footprinting** → Identify target's public IP.
- **Scanning** → Detect active hosts & open ports.
- **Exploitation** → IP-based access restrictions can be bypassed if exposed.
- **Tracking** → IP logs help trace activity.

📝 Short Notes: IP Addresses

- **Definition:** Unique number identifying a device on a network.
- **Versions:** IPv4 (32-bit), IPv6 (128-bit).
- **Usage Types:** Private, Public, Static, Dynamic.
- **IPv4 Classes:** A (large), B (medium), C (small), D (multicast), E (research).
- **Special:** Loopback (127.0.0.1), Broadcast, APIPA (169.254.x.x).
- **Hacking Use:** Recon, scanning, exploitation.

MAC Addresses -

1. Definition

- **MAC Address** (**Media Access Control Address**) is a **unique hardware identifier** assigned to a network interface card (NIC) by the manufacturer.
- It works at the **Data Link Layer (Layer 2)** of the OSI model.
- Written in **hexadecimal**, usually in MM:MM:MM:SS:SS:SS or MM-MM-MM-SS-SS-SS format.
  - Example: 00:1A:2B:3C:4D:5E

2. Purpose

- **Uniquely identify** a device on a local network.
- Used by switches to forward data to the correct device.
- Helps in controlling network access (MAC filtering).

3. Structure

- **First 3 bytes (OUI - Organizationally Unique Identifier):** Identify manufacturer (e.g., Intel, Cisco).
- **Last 3 bytes (NIC-specific):** Unique serial number for the device.

4. Types of MAC Addresses

- **Unicast MAC** → Sent to one specific device.
- **Multicast MAC** → Sent to a group of devices.
- **Broadcast MAC** → Sent to all devices (FF:FF:FF:FF:FF:FF).

5. MAC Address vs IP Address

Feature	MAC Address	IP Address
Layer	Data Link (Layer 2)	Network (Layer 3)
Assigned By	Manufacturer (hardware)	ISP or Admin (software)
Format	Hexadecimal	Decimal (IPv4) / Hex (IPv6)
Changeable	Yes, via spoofing	Yes, easily

6. MAC Address in Ethical Hacking

- **MAC Filtering Bypass:** Change your MAC to match an allowed device.
- **Anonymity:** MAC spoofing hides your real device identity.
- **Network Recon:** Identify devices/manufacturers in a LAN.
- **Tracking:** Networks can track a device via its MAC if unchanged.

7. Tools for MAC Address Operations

- **Linux:** ifconfig eth0 hw ether <new-mac> or macchanger
- **Windows:** Device Manager → Network Adapter → Properties → Network Address.
- **Wireshark:** Capture MACs in packets for analysis.

📝 Short Notes: MAC Addresses

- **Definition:** Unique hardware ID for network card; Layer 2.
- **Format:** Hexadecimal, 00:1A:2B:3C:4D:5E.
- **Parts:** OUI (manufacturer) + NIC-specific serial.
- **Types:** Unicast, Multicast, Broadcast.
- **Hacking Uses:** MAC spoofing, filtering bypass, device tracking.
- **Tools:** macchanger, ifconfig, Wireshark.

Ports in Networking -

1. Definition

- In networking, a **port** is a **virtual endpoint** for sending and receiving data between devices.
- It's identified by a **port number** (0–65535) assigned to a specific process/service.
- Works at the **Transport Layer** of the OSI model (Layer 4).
- Common protocols using ports: **TCP** and **UDP**.

2. Purpose

- **Distinguish services** running on the same device.
- Enable **simultaneous connections** to multiple services.
- Help routing data to the correct application.

3. Port Ranges

1. **Well-Known Ports (0–1023)** → Reserved for standard services.
   - Example: HTTP (80), HTTPS (443), FTP (21), SSH (22).
2. **Registered Ports (1024–49151)** → Used by user-registered applications.
   - Example: MySQL (3306), RDP (3389).
3. **Dynamic/Ephemeral Ports (49152–65535)** → Temporary ports for client connections.

4. Common Ports & Their Uses

Port	Protocol	Service
20/21	TCP	FTP (File Transfer)
22	TCP	SSH (Secure Shell)
23	TCP	Telnet
25	TCP	SMTP (Email)
53	TCP/UDP	DNS
80	TCP	HTTP
110	TCP	POP3 (Email)
143	TCP	IMAP (Email)
443	TCP	HTTPS
3306	TCP	MySQL
3389	TCP	RDP (Remote Desktop)

5. TCP vs UDP Ports

- **TCP** → Connection-oriented, reliable, used for web, email, SSH.
- **UDP** → Connectionless, faster, used for streaming, VoIP, DNS.

6. Ports in Ethical Hacking

- **Port Scanning:** Identify open ports on a target using tools like **Nmap**.
- **Service Enumeration:** Find what service & version runs on a port.
- **Exploitation:** Attack vulnerable services on specific ports.
- **Pivoting:** Use open ports to access internal networks.

7. Tools for Port Analysis

- **Nmap** → nmap -p 1-65535 <target> (full port scan).
- **Netstat** → Check active ports on your own machine.
- **Wireshark** → Capture and analyze port-based traffic.

📝 Short Notes: Ports in Networking

- **Definition:** Virtual endpoint for network communication (Layer 4).
- **Range:** 0–65535.
- **Types:** Well-known (0–1023), Registered (1024–49151), Dynamic (49152–65535).
- **Common Ports:** 21 (FTP), 22 (SSH), 53 (DNS), 80 (HTTP), 443 (HTTPS).
- **TCP vs UDP:** TCP reliable, UDP faster.
- **Hacking Use:** Scanning, enumeration, exploitation.
- **Tools:** Nmap, Netstat, Wireshark.