🌐 Networking Fundamentals

A Complete Guide for Interview Preparation & Professional Development

1. Basics of Networking

IP Addressing

> **What is an IP Address?** A unique identifier for devices on the internet or local network, following Internet Protocol rules for data transmission.

- **IPv4 vs IPv6:** IPv4 uses 32-bit addresses (~4.3 billion addresses), while IPv6 uses 128-bit addresses (vastly larger space)
- **Public vs Private IP:** Public IPs are globally unique and internet-routable; private IPs are for local networks only
- **Subnetting & CIDR:** Divides networks into smaller segments; CIDR notation (e.g., `/24`) indicates network size

MAC Addressing

- **MAC Address:** A 48-bit unique identifier for network interface cards (e.g., `00:1A:2B:3C:4D:5E`) operating at the data link layer
- **MAC vs IP:** MAC addresses handle local network communication within the same segment, while IP addresses enable routing across different networks globally

DNS (Domain Name System)

> **How DNS Works:** Translates human-readable domain names (e.g., `www.example.com`) into IP addresses (e.g., `192.168.1.1`)

- **A Record:** Maps domain to IPv4 address
- **AAAA Record:** Maps domain to IPv6 address

- **CNAME Record:** Creates an alias pointing one domain to another
- **MX Record:** Specifies mail servers for email delivery
- **DNS Resolution:** The process of converting domain names into IP addresses through DNS server queries

2. Network Models

OSI Model (Open System Interconnection)

- **7 Layers:** Physical (hardware) → Data Link (MAC, switches) → Network (IP routing) → Transport (TCP/UDP) → Session (connection management) → Presentation (data translation) → Application (user applications)
- **Layer Functions:** Each layer performs specific tasks like error detection, routing, and data formatting
- **Protocol Examples:** Ethernet (Data Link), IP (Network), TCP/UDP (Transport), HTTP/FTP (Application)

TCP/IP Model

- **4 Layers:** Network Interface (physical) → Internet (IP addressing) → Transport (TCP/UDP) → Application (protocols)
- **Comparison:** TCP/IP is a more practical, simplified version of the OSI model

3. Protocols

TCP vs UDP

- **TCP (Connection-oriented):** Reliable delivery with error checking, used for web pages and file transfers
- **UDP (Connectionless):** Faster but less reliable, ideal for video streaming and gaming
- **Three-way Handshake:** TCP establishes connections via SYN → SYN-ACK → ACK sequence

HTTP/HTTPS

- **HTTP:** Transfers web data without encryption
- **HTTPS:** Secures data transfer using SSL/TLS encryption
- **SSL/TLS:** Encryption protocols that protect data from interception

File Transfer & Remote Access

- **FTP:** File Transfer Protocol (unencrypted)
- **SFTP:** Secure File Transfer Protocol over SSH
- **SSH:** Secure Shell for encrypted remote system access

Email Protocols

- **SMTP:** Simple Mail Transfer Protocol for sending emails
- **POP3:** Downloads emails to local device
- **IMAP:** Allows multi-device email access with server synchronization

4. Networking Devices

Router vs Switch vs Hub

- **Router:** Routes data between different networks
- **Switch:** Connects devices within the same network using MAC addresses
- **Hub:** Broadcasts data to all connected devices (less efficient)

Firewalls

- **Purpose:** Filter network traffic to protect against threats
- **Stateful:** Tracks connection states for intelligent filtering
- **Stateless:** Examines each packet independently

Load Balancers

- **Purpose:** Distributes traffic across multiple servers to prevent overload
- **Round-robin:** Sequential distribution

- **Least connections:** Directs to least busy server

Other Devices

- **Gateway:** Connects different networks and translates protocols
- **Proxy Server:** Intermediary between clients and servers
- **NAT:** Allows multiple local devices to share one public IP

5. Network Security

VPN (Virtual Private Network)

- **How it Works:** Encrypts data for secure remote network access
- **Site-to-Site:** Connects entire networks
- **Remote Access:** Connects individual users to networks

IDS/IPS

- **IDS:** Intrusion Detection System monitors and alerts on suspicious activity
- **IPS:** Intrusion Prevention System actively blocks detected threats

Encryption

- **Symmetric:** Same key for encryption/decryption (e.g., AES)
- **Asymmetric:** Public/private key pair (e.g., RSA)

DDoS Protection

- **Attack Method:** Overwhelms servers with traffic causing service denial
- **Protection:** Rate limiting, traffic filtering, and CDN absorption

6. Advanced Concepts

CDN (Content Delivery Network)

- **How it Works:** Caches content on global servers, delivering from closest location
- **Benefits:** Reduces latency and improves load times

BGP (Border Gateway Protocol)

- **Purpose:** Routes data between autonomous systems on the internet
- **Role:** Determines optimal paths for internet data routing

NAT Types

- **SNAT:** Source Network Address Translation
- **DNAT:** Destination Network Address Translation
- **PAT:** Port Address Translation

Cloud Networking

- **VPC:** Virtual Private Cloud - isolated network environment
- **Subnets:** Subdivisions within a VPC
- **Route Tables:** Control traffic flow between subnets

7. Practical Tools

Diagnostic Tools

- **Ping:** Tests connectivity with ICMP echo requests
- **Traceroute:** Maps network path and identifies each hop
- **Wireshark:** Captures and analyzes network packets for troubleshooting

Command-Line Tools

- **Netcat (nc):** Creates connections, sends/receives data, troubleshoots networks
- **Curl/Wget:** Makes HTTP requests, tests APIs, downloads files