# 1. Basics of Networking

**Q1. Computer network kya hai aur kyun use hoti hai?**

- Network = Interconnected devices jo resources & data share karte hain.
- Use: Communication (email, WhatsApp), resource sharing (printers, files), remote access.

**Q2. Types of networks: LAN, MAN, WAN – example ke sath.**

- **LAN** (Local Area Network) → Small area, high speed (e.g., college lab, office).
- **MAN** (Metropolitan Area Network) → City-wide network (e.g., cable TV, city Wi-Fi).
- **WAN** (Wide Area Network) → Global scale (e.g., Internet).

**Q3. Hub vs Switch vs Router.**

- **Hub** → Layer 1, broadcasts to all, no intelligence.
- **Switch** → Layer 2, forwards using MAC, reduces collision domain.
- **Router** → Layer 3, forwards using IP, connects different networks.

**Q4. Unicast, Broadcast, Multicast, Anycast – examples.**

- **Unicast**: 1 → 1 (WhatsApp message).
- **Broadcast**: 1 → All (ARP request).
- **Multicast**: 1 → Many interested (IPTV, Zoom call).
- **Anycast**: 1 → Nearest one (DNS query).

**Q5. Circuit switching vs Packet switching.**

- **Circuit Switching**: Dedicated path, reserved bandwidth (Telephone).
- **Packet Switching**: Data split in packets, shared path (Internet).

**Q6. Peer-to-Peer vs Client-Server model.**

- **P2P**: All nodes equal, share resources (BitTorrent).
- **Client-Server**: Centralized server, clients request (Websites).

**Q7. What is bandwidth, latency, throughput?**

- **Bandwidth**: Max data transfer capacity (e.g., 100 Mbps).
- **Latency**: Delay (ms) in transmission.
- **Throughput**: Actual data achieved (e.g., 70 Mbps on 100 Mbps link).

**Q8. Half-duplex vs Full-duplex communication.**

- **Half**: One direction at a time (Walkie-talkie).
- **Full**: Both directions simultaneously (Telephone).

**Q9. What is multiplexing? Types (TDM, FDM).**

- Multiple signals on one channel.
- **TDM**: Time Division Multiplexing (time slots).
- **FDM**: Frequency Division Multiplexing (radio channels).

**Q10. What is demultiplexing?**

- Reverse of multiplexing: Receiver extracts original streams from combined signal.

# 2. OSI & TCP/IP Models

**Q11. What is the OSI model? Why is it important?**

- **OSI (Open Systems Interconnection)**: A 7-layer reference model for standardizing communication between systems.
- Importance: Breaks complex networking into layers → easier troubleshooting, standardization, protocol design.

**Q12. Name OSI layers in order.**
👉 Application → Presentation → Session → Transport → Network → Data Link → Physical.

**Mnemonic**: *All People Seem To Need Data Processing.*

**Q13. What is the function of each OSI layer with examples?**

- **Application** → Interface for end-users (HTTP, FTP, DNS).
- **Presentation** → Data translation, compression, encryption (SSL, JPEG).
- **Session** → Establish, maintain, terminate sessions (RPC, NetBIOS).
- **Transport** → Reliable delivery, error control (TCP/UDP).
- **Network** → Logical addressing, routing (IP, ICMP).
- **Data Link** → Error detection, MAC addressing (Ethernet, ARP).
- **Physical** → Transmission of bits (cables, NICs).

**Q14. TCP/IP model layers aur difference with OSI.**

- **TCP/IP Layers** → Application, Transport, Internet, Network Access.

- Difference:
    - OSI = 7 layers, theoretical model.
    - TCP/IP = 4 layers, practical implementation.
    - Example: HTTP (App), TCP (Transport), IP (Internet), Ethernet (Network Access).

**Q15. Encapsulation & Decapsulation process?**

- **Encapsulation**: Data wrapped layer by layer with headers/trailers (App → Transport → Network → Data Link → Physical).
- **Decapsulation**: Reverse process at receiver side.

**Q16. Difference between TCP & UDP (Transport layer).**

- **TCP**: Reliable, connection-oriented, error correction, ordered delivery (HTTP, FTP, Email).
- **UDP**: Unreliable, connectionless, faster, no ordering (Video streaming, DNS, VoIP).

**Q17. What is a port number? Well-known ports?**

- Port = Logical endpoint for process-to-process communication.
- **Examples**:
    - 21 FTP
    - 22 SSH
    - 25 SMTP
    - 53 DNS
    - 80 HTTP
    - 443 HTTPS

**Q18. What is socket?**

- Combination of **IP address + Port number** = socket.
- Example: `192.168.1.5:80`

**Q19. Explain connection establishment in TCP (3-way handshake).**

- Step 1: Client → SYN → Server
- Step 2: Server → SYN-ACK → Client

- Step 3: Client → ACK → Server
  👉 Connection established.

---

**Q20. What is 4-way termination in TCP?**

- Step 1: Client → FIN → Server
- Step 2: Server → ACK → Client
- Step 3: Server → FIN → Client
- Step 4: Client → ACK → Server
  👉 Connection closed.

# 3. IP Addressing & Subnetting

**Q21. What is an IP address? Types?**

- Unique identifier for devices in a network.
- **IPv4** (32-bit, e.g., 192.168.1.1), **IPv6** (128-bit, e.g., 2001:db8::1).
- Types: Public, Private, Static, Dynamic.

**Q22. Difference between IPv4 & IPv6.**

- IPv4: 32-bit, ~4.3B addresses, dotted decimal notation.
- IPv6: 128-bit, virtually unlimited addresses, hex notation, supports auto-configuration & better security (IPSec).

**Q23. What is subnetting? Why is it used?**

- Breaking large IP network into smaller networks.
- Uses: Efficient IP allocation, better security, reduces broadcast traffic.

**Q24. Explain Class A, B, C IP ranges.**

- **Class A** → 0.0.0.0 – 127.255.255.255 (/8 mask) → Big networks.
- **Class B** → 128.0.0.0 – 191.255.255.255 (/16) → Medium networks.
- **Class C** → 192.0.0.0 – 223.255.255.255 (/24) → Small networks.
- (D → Multicast, E → Research).

**Q25. Example: Company needs 600 hosts. Which subnet mask to use?**

- Formula: `2^n − 2 ≥ hosts`.

- 2^10 – 2 = 1022 → need 10 host bits.
- Subnet mask = **/22 (255.255.252.0)**

**Q26. What is CIDR notation?**

- Classless Inter-Domain Routing.
- IP address + prefix length.
- Example: `192.168.1.0/24` → 24 bits network, 8 bits host.

**Q27. What is a default gateway?**

- A router that forwards traffic from local network to external networks (e.g., Internet).

**Q28. What is ARP? Difference between ARP & RARP.**

- **ARP (Address Resolution Protocol)**: IP → MAC mapping.
- **RARP (Reverse ARP)**: MAC → IP mapping.

**Q29. What is ICMP? Use cases.**

- Internet Control Message Protocol (Layer 3).
- Used for error reporting & diagnostics.
- Example: `ping`, `traceroute`.

**Q30. Static routing vs Dynamic routing.**

- **Static**: Manual entry in routing table. Simple, less overhead.
- **Dynamic**: Auto-updates using protocols (RIP, OSPF, BGP). Scalable, efficient.

**Q31. Explain routing protocols: RIP, OSPF, BGP.**

- **RIP**: Distance-vector, hop count ≤ 15, slow convergence.
- **OSPF**: Link-state, fast convergence, large networks.
- **BGP**: Path-vector, used on the Internet, connects ISPs.

**Q32. What is NAT? Types?**

- **Network Address Translation**: Private ↔ Public IP conversion.
- **Types**: Static NAT, Dynamic NAT, PAT (Port Address Translation).

**Q33. Example: Why do we subtract 2 from total hosts formula (2^n – 2)?**

- 1 IP reserved for **network addresses**.
- 1 IP reserved for **broadcast address**.

**Q34. What is DHCP? How does it work?**

- Dynamic Host Configuration Protocol.
- Assigns IP automatically.
- Process: **DORA** → Discover → Offer → Request → Acknowledge.

**Q35. What is the difference between public & private IP ranges?**

- **Private**: For internal LAN (10.x.x.x, 172.16.x.x – 172.31.x.x, 192.168.x.x).
- **Public**: Globally routable, unique on Internet.

# 4. Protocols

**Q36. What is HTTP? Difference between HTTP & HTTPS.**

- **HTTP (Hypertext Transfer Protocol)** → Client-server communication for web. Port 80.
- **HTTPS** → HTTP + SSL/TLS encryption, secure communication. Port 443.

**Q37. What is DNS? How does it work?**

- **Domain Name System** → Converts domain names to IP addresses.
- Steps: Client → Resolver → Root server → TLD → Authoritative server → Response.
- Example: `google.com → 142.250.182.78`

**Q38. What is SMTP? Port numbers?**

- **Simple Mail Transfer Protocol** → Used to send emails.
- Ports: 25 (default), 587 (secure submission), 465 (SSL).

**Q39. Difference between POP3 & IMAP.**

- **POP3**: Downloads mail from server, deletes copy (Port 110).
- **IMAP**: Keeps mail on server, syncs across devices (Port 143, 993 SSL).

**Q40. What is FTP? Difference between FTP, SFTP, FTPS.**

- **FTP**: File Transfer Protocol, insecure (Port 21).
- **SFTP**: FTP over SSH, secure.
- **FTPS**: FTP + SSL/TLS encryption.

**Q41. What is DHCP? Explain the DORA process.**

- Dynamic IP assignment.
- **DORA**: Discover → Offer → Request → Acknowledge.

**Q42. What is SNMP?**

- **Simple Network Management Protocol** → Monitors and manages devices.
- Works on UDP port 161.
- Used by routers, switches, servers for health monitoring.

**Q43. What is Telnet? Why is SSH preferred?**

- **Telnet**: Remote login protocol, plaintext (Port 23).
- **SSH**: Secure Shell, encrypted remote login (Port 22).

**Q44. What is ICMP? Example commands.**

- Internet Control Message Protocol.
- Used for error messages & diagnostics.
- **Examples**: `ping`, `traceroute`.

**Q45. What is ARP? How does it work?**

- Address Resolution Protocol → Maps IP → MAC in local network.
- Uses broadcast request and unicast reply.

**Q46. What is RARP?**

- Reverse ARP → Maps MAC → IP.
- Rarely used now (DHCP replaced it).

**Q47. What is NTP?**

- **Network Time Protocol** → Synchronizes clocks across systems.
- Example: Ensures servers have same timestamps.

**Q48. What is LDAP?**

- **Lightweight Directory Access Protocol**.
- Used for accessing & maintaining distributed directory info (e.g., Active Directory).

**Q49. What is MQTT?**

- **Message Queuing Telemetry Transport** → Lightweight IoT protocol.
- Publisher-Subscriber model.

**Q50. What is gRPC?**

- Remote procedure call protocol, faster than REST.
- Uses HTTP/2 & Protobuf.

# 5. Firewall

**Q51. What is a firewall? Types?**

- **Firewall**: Security device/software that controls traffic based on rules.
- **Types**:
    - Packet-filtering (Layer 3, checks IP/port).
    - Stateful inspection (tracks sessions).
    - Application-level (deep packet inspection).
    - Next-gen firewalls (NGFW, with IDS/IPS).

**Q52. Difference between firewall & proxy.**

- **Firewall**: Protects network by filtering traffic.
- **Proxy**: Acts as an intermediary between client & server (can provide anonymity, caching, access control).

**Q53. What is VPN? Why is it used?**

- **Virtual Private Network**: Creates secure encrypted tunnels over the public Internet.
- Uses: Remote work, secure browsing, bypassing geo-blocks, enterprise intranet access.

**Q54. VPN protocols (basic overview).**

- **PPTP**: Old, insecure, fast.
- **L2TP/IPSec**: More secure, widely used.
- **OpenVPN**: Secure, open-source, uses SSL/TLS.
- **WireGuard**: Modern, lightweight, very fast.

**Q55. What is IDS & IPS?**

- **IDS (Intrusion Detection System)**: Monitors & alerts on malicious activity.
- **IPS (Intrusion Prevention System)**: Monitors + blocks suspicious activity.

**Q56. What is a DoS attack? Difference between DoS & DDoS.**

- **DoS (Denial of Service)**: Overwhelms server with traffic.
- **DDoS (Distributed DoS)**: Multiple systems attack simultaneously → much harder to stop.

**Q57. What is an MITM (Man-in-the-Middle) attack?**

- Attacker intercepts communication between two parties.
- Example: Fake Wi-Fi hotspot capturing login credentials.

**Q58. What is DNS spoofing / poisoning?**

- Attacker alters DNS responses → redirects users to malicious sites.

**Q59. What is ARP spoofing?**

- Attackers send fake ARP messages to associate their MAC with the victim's IP → intercepts traffic.

**Q60. What is SSL/TLS?**

- Encryption protocol securing data transfer.
- Provides **Confidentiality, Integrity, Authentication**.
- Example: HTTPS uses TLS.

**Q61. Symmetric vs Asymmetric encryption.**

- **Symmetric**: Same key for encryption & decryption (AES, DES). Fast, but key distribution problem.
- **Asymmetric**: Public key encrypts, private key decrypts (RSA, ECC). Slower, but secure key exchange.

**Q62. What is hashing? Examples.**

- One-way function to convert data → fixed hash value.
- Examples: MD5, SHA-256.
- Used in passwords, integrity checks.

**Q63. What is IPsec? Modes of operation.**

- Protocol suite for secure IP communication.

- **Transport mode**: Encrypts payload only.
- **Tunnel mode**: Encrypts the entire packet (used in VPN).

**Q64. What is Zero Trust Architecture?**

- Security model → “Never trust, always verify.”
- Even internal network traffic is verified & authenticated.

**Q65. Example: If your company’s server is under DDoS attack, what immediate steps would you suggest?**

- Block suspicious IP ranges (firewall rules).
- Use rate limiting.
- Redirect via CDN/DDoS protection service (Cloudflare, Akamai).
- Increase server redundancy (load balancing).

# 6. Congestion, Flow & Error Control

**Q66. What is a firewall? Types?**

- **Firewall**: Security device/software that controls traffic based on rules.
- **Types**:
    - Packet-filtering (Layer 3, checks IP/port).
    - Stateful inspection (tracks sessions).
    - Application-level (deep packet inspection).
    - Next-gen firewalls (NGFW, with IDS/IPS).

**Q67. Difference between firewall & proxy.**

- **Firewall**: Protects network by filtering traffic.
- **Proxy**: Acts as an intermediary between client & server (can provide anonymity, caching, access control).

**Q68. What is VPN? Why is it used?**

- **Virtual Private Network**: Creates secure encrypted tunnel over public Internet.
- Uses: Remote work, secure browsing, bypassing geo-blocks, enterprise intranet access.

**Q69. VPN protocols (basic overview).**

- **PPTP**: Old, insecure, fast.
- **L2TP/IPSec**: More secure, widely used.
- **OpenVPN**: Secure, open-source, uses SSL/TLS.
- **WireGuard**: Modern, lightweight, very fast.

**Q70. What is IDS & IPS?**

- **IDS (Intrusion Detection System)**: Monitors & alerts on malicious activity.
- **IPS (Intrusion Prevention System)**: Monitors + blocks suspicious activity.

**Q71. What is DoS attack? Difference between DoS & DDoS.**

- **DoS (Denial of Service)**: Overwhelms server with traffic.
- **DDoS (Distributed DoS)**: Multiple systems attack simultaneously → much harder to stop.

**Q72. What is an MITM (Man-in-the-Middle) attack?**

- Attacker intercepts communication between two parties.
- Example: Fake Wi-Fi hotspot capturing login credentials.

**Q73. What is DNS spoofing / poisoning?**

- Attacker alters DNS responses → redirects user to malicious site.

**Q74. What is ARP spoofing?**

- Attacker sends fake ARP messages to associate their MAC with victim's IP → intercepts traffic.

**Q75. What is SSL/TLS?**

- Encryption protocol securing data transfer.
- Provides **Confidentiality, Integrity, Authentication**.
- Example: HTTPS uses TLS.

**Q76. Symmetric vs Asymmetric encryption.**

- **Symmetric**: Same key for encryption & decryption (AES, DES). Fast, but key distribution problem.
- **Asymmetric**: Public key encrypts, private key decrypts (RSA, ECC). Slower, but secure key exchange.

**Q77. What is hashing? Examples.**

- One-way function to convert data → fixed hash value.
- Examples: MD5, SHA-256.
- Used in passwords, integrity checks.

**Q78. What is IPsec? Modes of operation.**

- Protocol suite for secure IP communication.
- **Transport mode**: Encrypts payload only.
- **Tunnel mode**: Encrypts entire packet (used in VPN).

**Q79. What is Zero Trust Architecture?**

- Security model → "Never trust, always verify."
- Even internal network traffic is verified & authenticated.

**Q80. Example: If your company's server is under DDoS attack, what immediate steps would you suggest?**

- Block suspicious IP ranges (firewall rules).
- Use rate limiting.
- Redirect via CDN/DDoS protection service (Cloudflare, Akamai).
- Increase server redundancy (load balancing).

# 8. Advanced / Real-World Concepts

**Q81. What is a Content Delivery Network (CDN)? Why is it used?**

- **CDN =** Globally distributed servers delivering content from nearest location.
- Benefits: Low latency, high availability, reduced bandwidth costs.
- Example: Netflix, YouTube, Cloudflare.

**Q82. What is Load Balancing? Types?**

- Technique to distribute workload across multiple servers/links.
- **Types**:
    - Round Robin
    - Least Connections
    - IP Hash

    - Geo Load Balancing
- Example: AWS Elastic Load Balancer.

**Q83. What is SDN (Software Defined Networking)?**

- Separates **control plane (routing decisions)** from **data plane (forwarding)**.
- Centralized controller manages the network (OpenFlow).
- Benefit: Programmable, flexible, reduces vendor lock-in.

**Q84. What is MPLS (Multi-Protocol Label Switching)?**

- Routing technique → uses **labels instead of IP lookup**.
- Faster packet forwarding, supports QoS (Voice/Video).
- Used by ISPs for VPNs & high-performance routing.

**Q85. What is QoS (Quality of Service) in networks?**

- Mechanism to prioritize traffic.
- Example: Video calls & VoIP get higher priority than email.
- Ensures **low latency, low jitter, controlled packet loss**.

**Q86. What is Proxy Server? Types?**

- **Proxy** = Middle server between client & Internet.
- **Types**:
    - Forward Proxy (hides client identity).
    - Reverse Proxy (hides server identity, load balancing).
    - Transparent Proxy (caching).
- Example: Nginx reverse proxy.

**Q87. What is NAT Traversal?**

- Technique to allow devices behind NAT to communicate over Internet.
- Used in: VPNs, VoIP (Skype/Zoom), P2P apps.

**Q88. What is Overlay Networking?**

- Virtual network built on top of another (physical) network.
- Used in cloud & containers (Docker overlay networks, Kubernetes).

**Q89. What is VPC (Virtual Private Cloud)?**

- Private isolated network in cloud.
- Example: In AWS, you create a VPC with subnets, route tables, security groups to simulate on-prem LAN.

**Q90. What is Anycast Routing? Where is it used?**

- Same IP advertised by multiple servers at different locations.
- Client automatically connects to **nearest server**.
- Used in: **DNS (Google DNS 8.8.8.8), CDNs, Cloud services.**

# 9. Wireless & Miscellaneous

**Q91. What is latency?**

- Delay between sender → receiver. Measured in ms.

**Q92. What is jitter?**

- Variation in packet delay. Critical for video/audio calls.

**Q93. What is throughput?**

- Actual achieved data transfer rate.

**Q94. MTU (Maximum Transmission Unit)?**

- Largest packet size that can be sent without fragmentation (Ethernet MTU = 1500 bytes).

**Q95. What is fragmentation in IP?**

- Splitting packets into smaller chunks when they exceed MTU.

**Q96. Difference between hub & switch?**

- Hub: Broadcasts to all (Layer 1).
- Switch: Forwards to correct MAC (Layer 2).

**Q97. Difference between switch & bridge?**

- Switch = multi-port bridge. Both work at Layer 2.

**Q98. Example of Layer 7 attack?**

- HTTP Flood (DDoS targeting web apps).

**Q99. Difference between stateful & stateless firewall?**

- Stateful: Tracks session info.
- Stateless: Filters packet by packet only.

**Q100. What is traceroute?**

- Diagnostic tool showing path packets take (uses ICMP TTL).

**Q101. What is TTL in IP header?**

- Time-To-Live = max hops packet can take before being discarded.

**Q102. What is DHCP lease time?**

- Time duration for which IP is assigned before renewal.

**Q103. What is sticky session in load balancing?**

- Ensures client always connects to same backend server.

**Q104. Difference between forward DNS & reverse DNS lookup?**

- Forward: Name → IP (google.com → 142.250.x.x).
- Reverse: IP → Name.

**Q105. What is Port Forwarding?**

- Redirecting traffic from one port/IP → another. Used in NAT & home routers.