## Basic Networking Questions

1. **What is a network?**
   - A network is a collection of computers and devices connected together to share resources and communicate.
2. **What is the difference between a hub, a switch, and a router?**
   - A hub broadcasts data to all devices on a network, a switch forwards data to specific devices based on MAC addresses, and a router connects different networks and routes data between them.
3. **What is an IP address?**
   - An IP address is a unique identifier assigned to each device on a network, allowing it to communicate with other devices.
4. **What is the difference between IPv4 and IPv6?**
   - IPv4 uses 32-bit addresses, allowing for about 4.3 billion unique addresses, while IPv6 uses 128-bit addresses, allowing for a vastly larger number of unique addresses.
5. **What is a subnet?**
   - A subnet is a smaller network within a larger network, created by dividing an IP address space into smaller segments.
6. **What is a DNS?**
   - The Domain Name System (DNS) translates human-readable domain names (like www.example.com) into IP addresses.
7. **What is DHCP?**
   - The Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses and other network configuration parameters to devices on a network.
8. **What is a firewall?**
   - A firewall is a security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
9. **What is NAT?**
   - Network Address Translation (NAT) is a technique used to translate private IP addresses to a public IP address, allowing multiple devices to share a single public IP.
10. **What is a VPN?**
    - A Virtual Private Network (VPN) creates a secure, encrypted connection over a less secure network, such as the Internet.

## Intermediate Networking Questions

11. **What is the OSI model?**

- The OSI (Open Systems Interconnection) model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

12. **What is TCP/IP?**
    - TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of communication protocols used for the Internet and similar networks.
13. **What is the difference between TCP and UDP?**
    - TCP (Transmission Control Protocol) is connection-oriented and ensures reliable data transmission, while UDP (User Datagram Protocol) is connectionless and does not guarantee delivery.
14. **What is a MAC address?**
    - A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications at the data link layer.
15. **What is a VLAN?**
    - A Virtual Local Area Network (VLAN) is a logical grouping of devices on a network, allowing them to communicate as if they were on the same physical network, regardless of their actual location.
16. **What is a proxy server?**
    - A proxy server acts as an intermediary between a client and a server, forwarding requests and responses to improve security, performance, or anonymity.
17. **What is the purpose of the ARP protocol?**
    - The Address Resolution Protocol (ARP) is used to map IP addresses to MAC addresses, allowing devices to communicate on a local network.
18. **What is a network topology?**
    - Network topology refers to the arrangement of different elements (links, nodes, etc.) in a computer network. Common topologies include star, ring, bus, and mesh.
19. **What is bandwidth?**
    - Bandwidth is the maximum rate of data transfer across a network path, usually measured in bits per second (bps).
20. **What is latency?**
    - Latency is the time it takes for data to travel from the source to the destination, often measured in milliseconds (ms).

## Advanced Networking Questions

21. **What is a load balancer?**
    - A load balancer distributes network or application traffic across multiple servers to ensure no single server becomes overwhelmed, improving performance and reliability.
22. **What is a network protocol?**

   - A network protocol is a set of rules and conventions for communication between network devices.

23. **What is the difference between a public and a private IP address?**

    - Public IP addresses are routable on the Internet, while private IP addresses are used within private networks and are not routable on the Internet.

24. **What is a port?**

    - A port is a virtual point where network connections start and end, identified by a number (e.g., HTTP uses port 80).

25. **What is ICMP?**

    - The Internet Control Message Protocol (ICMP) is used for error messages and operational information exchange in network devices.

26.** What is a network packet?**

    - A network packet is a formatted unit of data carried by a packet-switched network, containing both control information and user data.

27. **What is the purpose of the TCP three-way handshake?**

    - The TCP three-way handshake establishes a connection between a client and server by synchronizing sequence numbers and confirming the connection.

28. **What is a network switch?**

    - A network switch is a device that connects devices within a local area network (LAN) and uses MAC addresses to forward data to the correct destination.

29. **What is a network bridge?**

    - A network bridge connects two or more network segments, allowing them to function as a single network while filtering traffic.

30. **What is a network gateway?**

    - A network gateway is a device that connects two different networks and translates communication between them, often serving as a point of entry and exit.

31. **What is the difference between a stateful and stateless firewall?**

    - A stateful firewall tracks the state of active connections and makes decisions based on the context of the traffic, while a stateless firewall treats each packet in isolation.

32. **What is a DMZ in networking?**

    - A Demilitarized Zone (DMZ) is a physical or logical subnetwork that contains and exposes external-facing services to an untrusted network, typically the Internet.

33. **What is the purpose of the DHCP lease?**

    - A DHCP lease is a temporary assignment of an IP address to a device, allowing it to use the address for a specified period before it must renew the lease.

34. **What is a subnet mask?**

- A subnet mask is a 32-bit number that divides an IP address into the network and host portions, determining which part of the address identifies the network.

35. **What is the purpose of the ping command?**
    - The ping command is used to test the reachability of a host on a network and measure the round-trip time for messages sent to the destination.
36. **What is a network sniffer?**
    - A network sniffer is a tool that captures and analyzes packets traveling over a network, useful for troubleshooting and monitoring network traffic.
37. **What is the difference between a static and dynamic IP address?**
    - A static IP address is manually assigned and does not change, while a dynamic IP address is assigned by a DHCP server and can change over time.
38. **What is the purpose of the traceroute command?**
    - The traceroute command is used to track the path that packets take from one host to another, identifying each hop along the way.
39. **What is a wireless access point?**
    - A wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi.
40. **What is the role of the transport layer in the OSI model?**
    - The transport layer is responsible for providing reliable or unreliable delivery of data, error recovery, and flow control between end systems.

## Networking Security Questions

41. **What is SSL/TLS?**
    - SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols designed to provide secure communication over a computer network.
42. **What is a man-in-the-middle attack?**
    - A man-in-the-middle attack occurs when an attacker intercepts and potentially alters the communication between two parties without their knowledge.
43. **What is a denial-of-service (DoS) attack?**
    - A denial-of-service attack aims to make a network service unavailable by overwhelming it with traffic or exploiting vulnerabilities.
44. **What is WPA2?**
    - WPA2 (Wi-Fi Protected Access 2) is a security protocol used to secure wireless networks, providing stronger data protection and network access control.
45. **What is a security policy in networking?**
    - A security policy is a formal document that outlines how an organization protects its physical and information technology assets.

46. **What is the purpose of network segmentation?**

    - Network segmentation involves dividing a network into smaller, manageable sections to improve performance and enhance security.

47. **What is a security incident response plan?**

    - A security incident response plan is a documented strategy for responding to and managing security incidents to minimize damage and recover quickly.

48. **What is the role of encryption in networking?**

    - Encryption protects data by converting it into a coded format that can only be read by authorized parties, ensuring confidentiality and integrity.

49. **What is a digital certificate?**

    - A digital certificate is an electronic document used to prove the ownership of a public key, issued by a trusted certificate authority (CA).

50. **What is the purpose of a network audit?**

    - A network audit is a comprehensive assessment of a network's security, performance, and compliance with policies, helping to identify vulnerabilities and areas for improvement.