# Q&A Top 50 In Computer Network

## 1. What is a computer network?

A computer network is a collection of interconnected devices (computers, servers, routers) that can share data and resources.

## 2. What is a LAN?

LAN stands for Local Area Network, which connects devices within a limited geographical area, such as an office or home.

## 3. What is a WAN?

WAN stands for Wide Area Network, which connects devices over a large geographical area, typically using public networks.

## 4. What is the OSI model?

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes network communication into seven layers.

## 5. What is TCP/IP?

TCP/IP is a set of protocols used to enable communication on the internet and most computer networks.

## 6. What is IP address?

An IP address is a unique numerical label assigned to each device on a network, enabling them to be identified.

## 7. What is subnetting?

Subnetting is dividing a large network into smaller subnetworks for efficient IP address allocation.

## 8. What is DHCP?

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network.

## 9. What is DNS?

DNS (Domain Name System) translates human-readable domain names into IP addresses.

## 10. What is ARP?

ARP (Address Resolution Protocol) resolves IP addresses to MAC addresses on a local network.

## 11. What is a router?

A router is a networking device that forwards data packets between different networks.

## 12. What is a switch?

A switch is a networking device that connects devices within a local network and forwards data between them.

## 13. What is a gateway?

A gateway is a device that connects different network types, enabling communication between them.

## 14. What is bandwidth?

Bandwidth is the maximum data transfer rate of a network or internet connection.

## 15. What is latency?

Latency is the delay in data transmission between two points on a network.

## 16. What is a firewall?

A firewall is a security device that filters and controls incoming and outgoing network traffic.

## 17. What is NAT?

NAT (Network Address Translation) converts private IP addresses to public IP addresses for internet communication.

## 18. What is VPN?

VPN (Virtual Private Network) creates a secure encrypted connection over a public network, ensuring privacy.

## 19. What is a proxy server?

A proxy server acts as an intermediary between clients and the internet, enhancing security and performance.

## 20. What is a MAC address?

A MAC address is a unique identifier assigned to each network interface card (NIC).

## 21. What is ICMP?

ICMP (Internet Control Message Protocol) handles error messages and network diagnostics.

## 22. What is a broadcast address?

A broadcast address is used to send data to all devices on a network.

## 23. What is a subnet mask?

A subnet mask identifies the network and host portions of an IP address.

## 24. What is the difference between TCP and UDP?

TCP (Transmission Control Protocol) is connection-oriented and ensures reliable data delivery,

while UDP (User Datagram Protocol) is connectionless and faster but may not guarantee delivery.

## 25. What is port number?

A port number identifies specific processes or services on a device within a network.

## 26. What is a MAC flooding attack?

A MAC flooding attack overloads the switch’s MAC address table, causing it to act like a hub, making data visible to all devices.

## 27. What is a man-in-the-middle attack?

A man-in-the-middle attack intercepts communication between two parties to eavesdrop or manipulate data.

## 28. What is a denial-of-service (DoS) attack?

A DoS attack floods a network or service with excessive traffic, causing it to become unavailable.

## 29. What is VLAN?

VLAN (Virtual LAN) logically segments a physical LAN into multiple virtual LANs for security and traffic management.

## 30. What is STP?

STP (Spanning Tree Protocol) prevents network loops in redundant switch connections.

## 31. What is QoS?

QoS (Quality of Service) prioritizes network traffic to ensure specific data types receive better service.

## 32. What is the difference between half-duplex and full-duplex?

In half-duplex, data can be transmitted or received, but not simultaneously, whereas in full-duplex, data can be transmitted and received simultaneously.

## 33. What is PoE?

PoE (Power over Ethernet) delivers power to network devices over the Ethernet cable.

## 34. What is the purpose of traceroute?

Traceroute is used to identify the path and latency of data packets between two points on a network.

## 35. What is a DMZ?

DMZ (Demilitarized Zone) is a separate network that provides an additional layer of security between the internet and an internal network.

## 36. What is network congestion?

Network congestion occurs when the network experiences heavy traffic, leading to reduced performance.

## 37. What is a packet?

A packet is a unit of data transmitted over a network.

## 38. What is a collision domain?

A collision domain is a network segment where data collisions can occur on shared media, like in Ethernet hubs.

## 39. What is CSMA/CD?

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is an Ethernet protocol to detect and resolve data collisions.

## 40. What is IEEE 802.11?

IEEE 802.11 is a standard for wireless LAN technology (Wi-Fi).

## 41. What is a MAC filtering?

MAC filtering restricts network access based on MAC addresses.

## 42. What is a network topology?

Network topology defines the physical or logical layout of devices and their connections in a network.

## 43. What is the purpose of a subnet?

Subnets help divide a large network into smaller segments for easier management and improved security.

## 44. What is SDN?

SDN (Software-Defined Networking) separates the control plane and data plane, enabling centralized network management.

## 45. What is a network protocol?

A network protocol is a set of rules defining how devices communicate and exchange data on a network.

## 46. What is ARP poisoning?

ARP poisoning (spoofing) is a cyber attack that alters ARP tables to redirect traffic to a malicious device.

## 47. What is network virtualization?

Network virtualization enables the creation of virtual networks using software-based techniques.

## 48. What is multiplexing?

Multiplexing combines multiple data streams into a single channel for more efficient data transmission.

## 49. What is a gateway router?

A gateway router connects networks with different protocols, enabling communication between them.

## 50. What is the purpose of ICMP Echo Request and Reply?

ICMP Echo Request (ping) sends a packet to check if a host is reachable, and ICMP Echo Reply responds if the host is available.