1. Basics of Networking

---

1. What is a computer network?

A computer network is a group of interconnected computers and other devices that can share resources and exchange information. Networks allow communication between devices like computers, printers, and servers.

2. Types of networks (LAN, MAN, WAN, PAN, VPN).

- **LAN (Local Area Network)**: A network that connects devices in a limited area, like a home, school, or office building. It's typically privately owned and managed. **Example**: Computers in a single office building connected to a central server.
- **MAN (Metropolitan Area Network)**: A network that spans a city or large campus. It's larger than a LAN but smaller than a WAN. **Example**: A network connecting multiple university campuses within a city.
- **WAN (Wide Area Network)**: A network that covers a broad area, often connecting networks across different cities, countries, or even continents. The internet is the largest WAN. **Example**: A company with offices in London and New York connected via a private network.
- **PAN (Personal Area Network)**: A network that connects personal devices within a small range, typically around a person. **Example**: A smartphone connected to a Bluetooth headset.
- **VPN (Virtual Private Network)**: A secure, encrypted connection over a public network (like the internet), allowing users to access a private network remotely. **Example**: An employee working from home using a VPN to securely access the company's internal network.

3. Difference between client-server and peer-to-peer networks.

Feature	Client-Server	Peer-to-Peer (P2P)
Centralization	Central server manages resources and provides services.	No central server; all devices are equal peers.
Security	Centralized security and access control.	Security is managed individually on each device.
Scalability	Easy to add more clients; performance may depend on server capacity.	Scalability can be difficult to manage.

Performance	Can be faster due to a dedicated server.	Performance can degrade as more peers join the network.
Example	A web server providing web pages to client browsers.	File-sharing applications like BitTorrent.

4. What is bandwidth and latency?

- **Bandwidth** is the maximum amount of data that can be transferred over a network connection in a given amount of time, typically measured in bits per second (bps). Think of it as the **width of a pipe**; a wider pipe allows more water (data) to flow through. High bandwidth means more data can be sent at once.
- **Latency** is the time delay for a data packet to travel from its source to its destination, measured in milliseconds (ms). Think of it as the **speed of water** moving through the pipe. Low latency is crucial for real-time applications like online gaming or video calls.

5. Difference between hub, switch, and router.

- **Hub**: A simple, Layer 1 device that connects multiple devices on a single network. It broadcasts all incoming data to all connected devices, making it inefficient and prone to network collisions.
- **Switch**: A more intelligent Layer 2 device that learns the MAC addresses of connected devices. It forwards data only to the intended destination device, reducing network traffic and collisions.
- **Router**: A Layer 3 device that connects different networks together. It uses IP addresses to route data packets between networks (e.g., your home network to the internet).

6. What is a MAC address vs IP address?

Feature	MAC Address	IP Address
Layer	Data Link Layer (L2)	Network Layer (L3)
Purpose	Uniquely identifies a network interface card (NIC) on a local network.	Uniquely identifies a device on a network (local or global).

Format	48-bit hexadecimal (e.g., `00:1A:2B:3C:4D:5E`).	32-bit (IPv4) or 128-bit (IPv6) numbers.
Assignment	Hard-coded by the manufacturer.	Assigned dynamically by a DHCP server or manually.
Scope	Local to a single network segment.	Global; used for routing across different networks.
Analogy	Like a person's physical street address (fixed).	Like a person's mailing address (can change).

7. Difference between IPv4 and IPv6.

Feature	IPv4	IPv6
Address Size	32 bits	128 bits
Address Format	Dotted-decimal (e.g., `192.168.1.1`).	Colon-hexadecimal (e.g., `2001:0db8:85a3:0000:0000:8a2e:0370:7334`).
Address Space	~4.3 billion addresses.	Vastly larger, virtually unlimited.
Header	Larger header with optional fields.	Simplified, more efficient header.
Security	Optional IPsec.	IPsec is built-in and mandatory.

Key Reason	To address the depletion of IPv4 addresses.	Provides a future-proof, larger address space.

8. What is DNS? How does it work?

DNS (Domain Name System) is a hierarchical system that translates human-readable domain names (like google.com) into machine-readable IP addresses (like 172.217.164.142).

How it works:

1. You type a URL into your browser.
2. Your computer checks its local DNS cache. If not found, it queries a **recursive DNS resolver** (usually your ISP's server).
3. The resolver queries a **root name server**.
4. The root server directs the resolver to a **Top-Level Domain (TLD) name server** for .com.
5. The TLD server directs the resolver to the **authoritative name server** for google.com.
6. The authoritative server provides the IP address for google.com to the resolver.
7. The resolver sends the IP address back to your computer.
8. Your computer can now connect to the web server at that IP address.

9. What is DHCP?

DHCP (Dynamic Host Configuration Protocol) is a network management protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network. It eliminates the need for manual IP configuration, preventing addre[1]ssing conflicts and simplifying network administration. When a new device connects, it broadcasts a request, and a DHCP server responds with an available IP address, subnet mask, default gateway, and DNS server addresses.

10. What is ARP (Address Resolution Protocol)?

ARP (Address Resolution Protocol) is a protocol used to map an IP address to a physical MAC address on a local network. When a device wants to send a data packet to another device on the same network, it knows the destination's IP address but needs its MAC address to send the data frame. The sending device broadcasts an ARP request with the destination's IP address. The device with that IP address replies with its MAC address, allowing communication to proceed.

---

2. OSI & TCP/IP Models

---

11. What is the OSI model? Explain all 7 layers.

The **OSI (Open Systems Interconnection)** model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven distinct layers. It helps to understand how different technologies work together.

1. **Physical Layer (L1)**: Deals with the physical transmission of raw bit streams over a communication medium. This includes cabling, connectors, and electrical signals.
2. **Data Link Layer (L2)**: Provides reliable data transfer between adjacent network nodes. It handles error detection, correction, and flow control. This layer uses MAC addresses.
3. **Network Layer (L3)**: Responsible for logical addressing (IP addresses) and routing data packets across different networks.
4. **Transport Layer (L4)**: Ensures reliable and ordered delivery of data between processes on different hosts. It handles segmentation, reassembly, flow control, and error checking. TCP and UDP operate here.
5. **Session Layer (L5)**: Establishes, manages, and terminates connections (sessions) between applications. It provides synchronization and dialog control.
6. **Presentation Layer (L6)**: Translates data from the application format to a common intermediate format for transmission and vice versa. It also handles data encryption and compression.
7. **Application Layer (L7)**: Provides network services for end-user applications. This is where user interaction with the network happens. Protocols like HTTP, FTP, and SMTP operate here.

12. What is the TCP/IP model? Explain all 4/5 layers.

The **TCP/IP model** is a four- or five-layer conceptual model used for the Internet and most modern networks. It's more practical and widely used than the OSI model.

1. **Network Access Layer (or Link Layer)**: Combines the Physical and Data Link layers of the OSI model. Deals with all aspects of physical transmission, including hardware addressing (MAC addresses).
2. **Internet Layer**: Corresponds to the OSI's Network Layer. It's responsible for logical addressing (IP addresses) and routing data packets across networks. IP, ICMP, and ARP operate here.
3. **Transport Layer**: Corresponds to the OSI's Transport Layer. Manages end-to-end communication and data delivery. TCP and UDP are the main protocols.
4. **Application Layer**: Combines the OSI's Session, Presentation, and Application layers. This layer provides network services to applications. Protocols like HTTP, SMTP, and DNS operate here.

13. Difference between OSI and TCP/IP models.

Feature	OSI Model	TCP/IP Model

Standard	A theoretical, conceptual model.	A practical, functional model used for the Internet.
Layers	7 layers.	4 or 5 layers.
Protocol Dependence	Protocols were developed after the model.	Model was developed based on existing protocols.
Flexibility	Less flexible; strict separation of layers.	More flexible; layers are more loosely defined.
Security	Security is an afterthought, not inherent to the model.	Security (like IPsec) is an integral part of the model.
Example	Academic and theoretical discussions.	The foundation of the Internet and real-world networking.

14. Which protocols work at which OSI layers?

- **Layer 7 (Application)**: HTTP, HTTPS, FTP, SMTP, DNS, SSH, Telnet.
- **Layer 6 (Presentation)**: JPEG, GIF, MPEG (data formatting).
- **Layer 5 (Session)**: NetBIOS, RPC, PPTP.
- **Layer 4 (Transport)**: TCP, UDP.
- **Layer 3 (Network)**: IP, ICMP, ARP, RIP, OSPF.
- **Layer 2 (Data Link)**: Ethernet, PPP, Wi-Fi.
- **Layer 1 (Physical)**: Coaxial cable, Fiber optic cable, DSL.

15. What is encapsulation and decapsulation?

Encapsulation is the process where a protocol adds its control information (header and sometimes a trailer) to the data it receives from the layer above. As data moves down the protocol stack, each layer encapsulates the data from the layer above it, adding its own header. For example, at the Transport layer, TCP adds a header to the data, creating a **segment**. This segment is then passed to the Network layer, where IP adds another header, creating a **packet**.

Decapsulation is the reverse process. As data moves up the protocol stack at the destination, each layer removes its corresponding header, revealing the data for the layer above. For example, the Network layer removes the IP header to reveal the TCP segment, which is then passed to the Transport layer.

16. What is MTU (Maximum Transmission Unit)?

The **MTU (Maximum Transmission Unit)** is the largest size of a data packet that can be transmitted over a specific network layer protocol without being fragmented. The standard MTU for Ethernet is **1500 bytes**. If a data packet is larger than the MTU of a network link, it must be fragmented into smaller pieces, which can lead to performance degradation.

17. What is fragmentation in networking?

Fragmentation is the process of breaking a large data packet into smaller packets (fragments) to be transmitted over a network link that has a smaller MTU than the original packet. These fragments are then reassembled at the destination. While fragmentation allows large packets to traverse networks, it adds processing overhead and can make the connection less efficient. For this reason, modern networks and protocols (especially IPv6) try to avoid fragmentation.

18. Explain TCP vs UDP (detailed differences).

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection	Connection-oriented. Requires a 3-way handshake to establish a connection.	Connectionless. No handshake is required.
Reliability	Highly reliable. Guarantees delivery, order, and error checking.	Unreliable. No guarantee of delivery or order.
Overhead	High overhead due to extensive headers, acknowledgments, and state management.	Low overhead; small header and no state management.
Speed	Slower due to reliability mechanisms.	Faster and more efficient due to less overhead.
Flow Control	Yes. Prevents the sender from overwhelming the receiver.	No. The receiver may drop packets if it's too busy.

Congestion Control	Yes. Manages network congestion to prevent collapse.	No. It keeps sending data regardless of congestion.
Use Cases	Web browsing (HTTP), email (SMTP), file transfer (FTP).	Video streaming, online gaming, DNS, VoIP.

19. What is a 3-way handshake in TCP?

The **3-way handshake** is a process used by TCP to establish a reliable connection between a client and a server. It ensures that both sides are ready to send and receive data.

1. **SYN (Synchronize)**: The client sends a packet with the SYN flag set to the server, proposing to establish a connection.
2. **SYN-ACK (Synchronize-Acknowledge)**: The server receives the SYN, sets the SYN and ACK flags, and sends a packet back to the client, acknowledging the request and indicating it is ready to connect.
3. **ACK (Acknowledge)**: The client receives the SYN-ACK, sets the ACK flag, and sends a final packet back to the server, acknowledging its readiness. The connection is now established.

20. What is a 4-way termination in TCP?

The **4-way termination** is the process of closing a TCP connection gracefully. It allows both sides to end the connection independently.

1. **FIN (Finish)**: One side (e.g., the client) sends a packet with the FIN flag set to the other side, indicating it has no more data to send.
2. **ACK (Acknowledge)**: The receiver (server) acknowledges the FIN, but it can still send data to the client (the connection is half-closed).
3. **FIN (Finish)**: The server, once it has no more data to send, sends its own FIN packet to the client.
4. **ACK (Acknowledge)**: The client acknowledges the server's FIN, and the connection is fully closed.

---

3. IP Addressing & Routing

---

21. What is subnetting? Why do we need it?

Subnetting is the process of dividing a large IP network into smaller, more manageable sub-networks (subnets). We use a **subnet mask** to distinguish the network portion of an IP address from the host portion.

Why we need it:

- **Reduces Network Congestion**: By segmenting the network, broadcast traffic is confined to its subnet, reducing network overhead.

- **Improves Security**: Subnets can be isolated from each other using firewalls and routers, allowing for more granular security policies.
- **Efficient IP Address Management**: Subnetting allows for better use of a limited number of IP addresses. Instead of assigning an entire class of IP addresses to a small network, you can create a smaller subnet.
- **Simplifies Administration**: Smaller, well-defined subnets are easier to manage and troubleshoot.

22. Difference between public and private IP addresses.

- **Public IP Address**: An IP address that is globally unique and routable on the public internet. It's assigned to your network by your ISP (Internet Service Provider).
- **Private IP Address**: An IP address that is not routable on the public internet. It's used for devices within a private network (like your home or office). The Internet Assigned Numbers Authority (IANA) has reserved specific address ranges for private use:
    - **Class A**: `10.0.0.0` to `10.255.255.255`
    - **Class B**: `172.16.0.0` to `172.31.255.255`
    - **Class C**: `192.168.0.0` to `192.168.255.255`

23. What is NAT (Network Address Translation)?

NAT (Network Address Translation) is a method used by routers to map multiple private IP addresses on a local network to a single public IP address. It allows devices on a private network to access the internet. When a device on the private network sends a request to the internet, the router replaces the private source IP address with its public IP address before forwarding the packet. This process is reversed for incoming packets.

24. Difference between static and dynamic routing.

- **Static Routing**: A manual process where a network administrator configures a router's routing table with fixed paths to specific networks.
    - **Pros**: Simple to set up in small networks, highly secure.
    - **Cons**: Not scalable, requires manual updates, and doesn't adapt to network changes.
- **Dynamic Routing**: A more automated process where routers use routing protocols (like RIP, OSPF, BGP) to automatically discover network paths and update their routing tables.
    - **Pros**: Scalable, adapts to network topology changes, and requires less manual intervention.
    - **Cons**: More complex to set up, requires more processing power, and can be less secure.

25. Difference between unicast, multicast, and broadcast.

- **Unicast**: **One-to-one** communication. A data packet is sent from a single source to a single, specific destination. **Example**: A web browser requesting a web page from a web server.

- **Multicast**: **One-to-many** communication. A data packet is sent from a single source to a select group of multiple receivers who have explicitly joined the group. **Example**: A live video stream being sent to multiple subscribed viewers.
- **Broadcast**: **One-to-all** communication. A data packet is sent from a single source to all devices on the same local network segment. **Example**: An ARP request to find the MAC address of a device.

26. What is CIDR (Classless Inter-Domain Routing)?

CIDR (Classless Inter-Domain Routing) is a method for allocating and addressing IP addresses that replaces the traditional classful addressing system (A, B, C). It uses a CIDR notation (e.g., `192.168.1.0/24`) where the number after the slash indicates the number of bits in the network portion of the address. This allows for more flexible and efficient use of IP address space by creating subnets of varying sizes.

27. What is default gateway?

A **default gateway** is the IP address of the router on a local network that acts as the entry and exit point for all data packets going to and from other networks. When a device wants to send data to a destination outside its local network (e.g., to the internet), it sends the packet to the default gateway, which then routes it to the appropriate destination.

28. Difference between IPv4 classes (A, B, C, D, E).

Class	First Octet Range	Default Subnet Mask	Use Case
A	`1` to `126`	`255.0.0.0` (`/8`)	Large networks (e.g., major corporations).
B	`128` to `191`	`255.255.0.0` (`/16`)	Medium-sized networks (e.g., universities).
C	`192` to `223`	`255.255.255.0` (`/24`)	Small networks (e.g., home offices).
D	`224` to `239`	N/A	Multicast addresses.

E	240 to 255	N/A	Reserved for experimental purposes.

Note: Classful addressing is largely replaced by CIDR today.

29. What is a routing table?

A **routing table** is a data table stored in a router or a networked computer that lists the routes to various network destinations. It contains information like the destination network, the next-hop router's IP address, and the outgoing network interface to use. Routers use this table to determine the most efficient path for a data packet to reach its destination.

30. Difference between distance vector and link-state routing.

- **Distance Vector Routing**: A routing protocol where each router maintains a table of distances (e.g., hop count) to other networks in the topology. Routers periodically share their entire routing table with their immediate neighbors.
    - **Example**: RIP (Routing Information Protocol).
    - **Characteristics**: Simple, but slow to converge and prone to routing loops.
- **Link-State Routing**: A more advanced routing protocol where each router creates a complete map of the entire network topology. Routers only share information about their local connections and link status with all other routers in the network.
    - **Example**: OSPF (Open Shortest Path First).
    - **Characteristics**: More complex, but faster to converge and less prone to routing loops.

---

4. TCP/UDP & Transport Layer

---

31. What is TCP? Features of TCP.

TCP (Transmission Control Protocol) is a connection-oriented, reliable transport layer protocol. It provides a reliable, ordered, and error-checked delivery of data between applications.

Key Features:

- **Reliability**: Guarantees delivery using acknowledgments (ACKs) and retransmissions.
- **Connection-Oriented**: Requires a 3-way handshake to establish a connection before data transfer.
- **Sequencing**: Segments are numbered to ensure they are reassembled in the correct order at the destination.
- **Flow Control**: Uses a sliding window mechanism to prevent a fast sender from overwhelming a slow receiver.
- **Congestion Control**: Manages network congestion to prevent network collapse.
- **Full-Duplex**: Allows data to be sent and received simultaneously.

32. What is UDP? Where is it used?

UDP (User Datagram Protocol) is a connectionless, unreliable transport layer protocol. It's a "best-effort" protocol that sends data without any prior setup or guarantee of delivery.

Where it is used:

UDP is ideal for applications where speed is more important than reliability and where small data loss is acceptable.

- **Live Video and Audio Streaming**: A dropped frame is better than a delayed one.
- **Online Gaming**: Low latency is critical.
- **DNS (Domain Name System)**: A quick, single request-response is more efficient with UDP.
- **VoIP (Voice over IP)**: Real-time voice calls.

33. Difference between TCP and UDP.

(See question 18 for a detailed table of differences).

34. What are ports in networking? Common port numbers.

Ports are logical numbers used by the Transport Layer to identify a specific process or application on a host. They allow multiple applications on a single machine to communicate over a network simultaneously. A combination of an IP address and a port number (IP:Port) is called a **socket**.

Common Port Numbers:

- **80**: HTTP (Hypertext Transfer Protocol)
- **443**: HTTPS (HTTP Secure)
- **21**: FTP (File Transfer Protocol)
- **22**: SSH (Secure Shell)
- **25**: SMTP (Simple Mail Transfer Protocol)
- **53**: DNS (Domain Name System)
- **23**: Telnet
- **110**: POP3 (Post Office Protocol 3)

35. What is socket programming?

Socket programming is a method of building network applications by using sockets as communication endpoints. A **socket** is an abstract representation of a communication endpoint that allows a program to send and receive data over a network. It provides a standard API (like the BSD sockets API) for network communication. A typical socket program involves creating a socket, binding it to an address and port, and then listening for connections (for a server) or connecting to a remote socket (for a client).

36. What is flow control in TCP?

Flow control is a TCP mechanism that prevents a sender from overwhelming a receiver by sending data faster than the receiver can process it. TCP uses a **sliding window** protocol, where the receiver advertises the size of its available buffer space (the "window size") in its

acknowledgment packets. The sender is only allowed to send data that fits within this advertised window, ensuring the receiver has enough capacity to handle the incoming data.

37. What is congestion control in TCP?

Congestion control is a TCP mechanism that prevents network collapse by regulating the rate at which data is sent when the network is congested. TCP uses a **congestion window** (cwnd) to limit the number of unacknowledged packets that can be in flight. If the network is congested (e.g., indicated by dropped packets or timeouts), TCP reduces its sending rate. If packets are being successfully acknowledged, it gradually increases its sending rate, probing for the network's capacity.

38. Explain slow start and congestion avoidance.

Slow start and **congestion avoidance** are two phases of TCP's congestion control algorithm.

- **Slow Start**: This phase begins when a TCP connection is established. The congestion window (cwnd) starts at a small value (e.g., 1 or 10 segments) and increases exponentially (by one segment for every acknowledgment received). This rapid increase allows the connection to quickly reach a fair share of the network bandwidth.
- **Congestion Avoidance**: When the congestion window reaches a predetermined threshold (ssthresh), the algorithm shifts to the congestion avoidance phase. In this phase, the congestion window increases linearly (by one segment for a full round-trip time of acknowledgments), not exponentially. This prevents the sender from overwhelming the network, as it's a more cautious approach to probing for available bandwidth.

39. What are TCP flags (SYN, ACK, FIN, RST, PSH, URG)?

TCP flags are control bits in the TCP header that specify the purpose of the segment and the state of the connection.

- **SYN (Synchronize)**: Initiates a connection (part of the 3-way handshake).
- **ACK (Acknowledge)**: Acknowledges received data.
- **FIN (Finish)**: Indicates that the sender has no more data to send and wants to terminate the connection.
- **RST (Reset)**: Abruptly terminates a connection, usually due to an error.
- **PSH (Push)**: Forces the immediate delivery of buffered data to the application.
- **URG (Urgent)**: Indicates that the segment contains urgent data that should be processed immediately.

40. Difference between persistent and non-persistent HTTP connections.

- **Non-Persistent HTTP**: A new TCP connection is established for every single resource (e.g., an HTML file, an image, a CSS file) requested from the server. The connection is closed after the transfer is complete.
    - **Pros**: Simple.
    - **Cons**: High overhead due to repeated 3-way handshakes and slower loading times.

- **Persistent HTTP**: A single TCP connection is established and kept open for multiple requests and responses. The client can request multiple resources (e.g., an HTML file and its images) over the same connection.
    - **Pros**: Lower overhead, faster loading times.
    - **Cons**: The server needs to keep the connection open, consuming resources.

---

5. Application Layer Protocols

---

41. What is HTTP? Difference between HTTP and HTTPS.

- **HTTP (Hypertext Transfer Protocol)**: A stateless, application-layer protocol used for transmitting web pages and other resources from a web server to a web browser. It's the foundation of the World Wide Web.
- **HTTPS (Hypertext Transfer Protocol Secure)**: An extension of HTTP that uses **SSL/TLS (Secure Sockets Layer/Transport Layer Security)** for encryption.
    - **Encryption**: HTTPS encrypts all communication between the client and server, protecting data from eavesdropping. HTTP is plain text and unencrypted.
    - **Security**: HTTPS provides data integrity and authentication (ensuring you are talking to the correct server).
    - **Port**: HTTP uses port 80; HTTPS uses port 443.

42. Explain SMTP, IMAP, and POP3.

These are application-layer protocols for email.

- **SMTP (Simple Mail Transfer Protocol)**: Used for **sending** email from a client to a server or between email servers. It's the "postman" of the email world.
- **IMAP (Internet Message Access Protocol)**: Used for **retrieving** emails from a server. It keeps emails on the server, allowing multiple devices to access and synchronize the same mailbox. It's a good choice for users who check their email from multiple locations.
- **POP3 (Post Office Protocol 3)**: Also used for **retrieving** emails. It typically downloads emails from the server to the client and deletes them from the server. This can lead to issues if you access your email from different devices.

43. What is FTP and SFTP?

- **FTP (File Transfer Protocol)**: A standard protocol for transferring files between a client and a server. It uses two separate connections: a **control connection** (for commands) and a **data connection** (for file transfers). FTP is unencrypted and insecure.
- **SFTP (SSH File Transfer Protocol)**: A secure version of FTP that runs on top of the **SSH (Secure Shell)** protocol. All data, including authentication information and file transfers, is encrypted. SFTP is much more secure and widely used today.

44. What is SSH?

SSH (Secure Shell) is a cryptographic network protocol used to securely operate network services over an unsecured network. It provides a secure channel over an unsecured network by using strong encryption. It's commonly used for remote command-line login and for executing commands on a remote server.

45. What is Telnet?

Telnet is an older application protocol used to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. Unlike SSH, Telnet is **unencrypted**, meaning all data, including login credentials, is sent in plain text. It is now considered insecure and has been largely replaced by SSH for remote administration.

46. What is SNMP?

SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring devices on a network, such as routers, switches, and servers. An SNMP manager can query a device's "agent" to collect information (e.g., CPU usage, network traffic) and can also be used to configure the device.

47. What is MQTT protocol?

MQTT (Message Queuing Telemetry Transport) is a lightweight, publish-subscribe messaging protocol. It's designed for use in low-bandwidth, high-latency, and unreliable networks, making it ideal for **IoT (Internet of Things)** devices. It operates on top of TCP and is very efficient, with a small code footprint and minimal network bandwidth requirements.

48. What is gRPC? Difference with REST.

- **gRPC (gRPC Remote Procedure Call)** is a high-performance, open-source framework developed by Google for creating APIs. It's based on **HTTP/2** and uses **Protocol Buffers** for serializing structured data.
- **REST (Representational State Transfer)** is an architectural style for designing APIs. It's based on HTTP and uses standard methods like GET, POST, PUT, and DELETE to operate on resources.
    - **Data Format**: gRPC uses Protocol Buffers (a binary format), which are more efficient and smaller than REST's typical JSON or XML format.
    - **Protocol**: gRPC uses HTTP/2, which supports multiplexing (multiple requests over a single connection) and server-side streaming. REST traditionally uses HTTP/1.1, which requires a new connection for each request (non-persistent) or uses a persistent connection.
    - **Performance**: gRPC is generally faster and more efficient for internal microservices communication. REST is more suitable for public-facing APIs due to its simplicity and browser compatibility.

49. Difference between WebSocket and HTTP.

- **HTTP**: A request-response protocol. A client sends a request, and the server sends a response, and then the connection is closed (in non-persistent HTTP). It's stateless and designed for one-way communication initiated by the client.

- **WebSocket**: A protocol that provides a **full-duplex**, persistent communication channel over a single TCP connection. Once the connection is established (via an initial HTTP handshake), both the client and server can send data to each other at any time. This makes it ideal for real-time applications like chat, live sports updates, and online games.

50. What is CDN (Content Delivery Network)?

A **CDN (Content Delivery Network)** is a geographically distributed network of proxy servers and their data centers. Its purpose is to provide high-speed content delivery to users by caching content (like images, videos, and web pages) at a location closer to the user. This reduces latency and improves website performance. For example, a user in London accessing a website hosted in New York might have the website's content served from a CDN server in London, reducing the data's travel time.

---

6. Network Security

---

51. What is a firewall? Types of firewalls.

A **firewall** is a network security device (hardware or software) that monitors and controls incoming and outgoing network traffic based on a predefined set of security rules. It acts as a barrier between a trusted internal network and an untrusted external network (like the internet).

Types of Firewalls:

- **Packet-filtering Firewall**: The most basic type. It inspects individual packets and allows or denies them based on rules like source/destination IP address, port number, and protocol.
- **Stateful Inspection Firewall**: More advanced. It tracks the state of active connections and can make more intelligent decisions. It's faster and more secure than packet-filtering firewalls.
- **Application-level Gateway (Proxy Firewall)**: Acts as a proxy between the client and server. It inspects the content of the data at the application layer and can provide deep packet inspection.
- **Next-Generation Firewall (NGFW)**: Combines traditional firewall features with advanced functionalities like deep packet inspection, intrusion prevention systems, and application awareness.

52. What is SSL/TLS?

- **SSL (Secure Sockets Layer)**: An older cryptographic protocol for securing communication over a network. It has been largely replaced by TLS.
- **TLS (Transport Layer Security)**: The successor to SSL. It provides authentication and data encryption between a client and a server. When you visit a website with `https://`, your browser and the web server use SSL/TLS to create a secure, encrypted connection.

53. Difference between symmetric and asymmetric encryption.

- **Symmetric Encryption**: Uses a **single key** for both encryption and decryption. Both the sender and receiver must have this shared secret key. It's fast and efficient. **Example**: AES, DES.
- **Asymmetric Encryption (Public Key Cryptography)**: Uses a **pair of keys**: a **public key** for encryption and a **private key** for decryption. The public key can be shared with anyone, while the private key must be kept secret. It's slower but solves the key distribution problem of symmetric encryption. **Example**: RSA, ECC.

54. What is a VPN?

A **VPN (Virtual Private Network)** creates a secure, encrypted connection (a "tunnel") over a public network (the internet). It masks your IP address and encrypts your traffic, protecting your data from being intercepted or monitored. VPNs are commonly used to securely access corporate networks from a remote location or to enhance online privacy.

55. What is IPsec?

IPsec (Internet Protocol Security) is a suite of protocols that provides security at the Network Layer (L3) of the TCP/IP model. It encrypts and authenticates all IP packets, providing a secure method for transferring data. IPsec is often used to implement VPNs.

56. What are DoS and DDoS attacks?

- **DoS (Denial-of-Service) Attack**: A cyber-attack where the attacker tries to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. This is typically done by flooding the target with a high volume of traffic from a single source.
- **DDoS (Distributed Denial-of-Service) Attack**: A DoS attack but from multiple, distributed sources. The attacker uses a network of compromised devices (a "botnet") to flood the target with traffic, making it much harder to block and mitigate.

57. What is man-in-the-middle attack?

A **man-in-the-middle (MITM) attack** is a type of cyberattack where the attacker secretly relays and alters the communication between two parties who believe they are communicating directly with each other. For example, an attacker can position themselves between a user's browser and a web server, intercepting and reading all of the user's unencrypted data.

58. What is DNS spoofing?

DNS spoofing (also known as DNS cache poisoning) is a type of attack where the attacker corrupts a DNS resolver's cache, causing it to return an incorrect IP address for a domain name. This redirects users to a malicious website (often a phishing site) instead of the legitimate one.

59. What is ARP spoofing?

ARP spoofing is a type of MITM attack where the attacker sends forged ARP messages to a local network. This allows the attacker to associate their own MAC address with the IP

address of another device (like the default gateway), causing all traffic from the target device to be sent to the attacker first, who can then intercept, modify, or drop the data.

60. What is zero trust architecture?

Zero trust architecture is a security model that assumes no user, device, or network is trustworthy by default, whether inside or outside the network. Instead of trusting devices based on their location (e.g., inside the corporate network), every access request is verified. It operates on the principle of "never trust, always verify."

---

7. Wireless & Modern Networking

---

61. Difference between Wi-Fi and Ethernet.

Feature	Wi-Fi (Wireless)	Ethernet (Wired)
Connection	Wireless; uses radio waves.	Wired; uses physical cables (e.g., Cat5e, Cat6).
Speed	Varies, but generally slower than wired.	Typically faster and more stable.
Reliability	Prone to interference and signal loss.	Highly reliable; no interference from other devices.
Security	Requires strong encryption (WPA3) to be secure.	More inherently secure; requires physical access to the network.
Mobility	High mobility; allows devices to roam.	No mobility; devices are physically tethered.

62. What is 4G vs 5G networking?

- **4G (Fourth Generation)**: The mobile network standard that introduced high-speed mobile internet, enabling applications like video streaming and mobile gaming.
- **5G (Fifth Generation)**: The next generation of mobile networking.
    - **Speed**: Significantly faster than 4G (up to 100x faster).
    - **Latency**: Ultra-low latency (under 1ms). This is crucial for real-time applications like self-driving cars and remote surgery.

    - **Capacity**: Can support a much higher number of connected devices, making it suitable for IoT.

63. What is hotspot vs tethering?

- **Hotspot**: A mobile device (like a smartphone) acts as a wireless access point, sharing its cellular data connection with other devices via Wi-Fi.
- **Tethering**: A mobile device shares its cellular data connection with a single other device, typically a laptop, via a physical USB cable or Bluetooth. Tethering is generally more stable and efficient than a hotspot.

64. What is Bluetooth Low Energy (BLE)?

Bluetooth Low Energy (BLE) is a wireless personal area network technology designed for very low power consumption. It's a key technology for the Internet of Things (IoT), wearables, and smart devices. Unlike classic Bluetooth, which is designed for continuous streaming, BLE is optimized for devices that send small amounts of data infrequently.

65. What is IoT networking?

IoT (Internet of Things) networking refers to the network infrastructure that connects a vast number of physical devices (e.g., sensors, smart appliances) to the internet and to each other. It often involves a mix of different networking technologies (Wi-Fi, Bluetooth, Zigbee, cellular networks) and protocols (MQTT, CoAP) that are designed to be lightweight and energy-efficient for constrained devices.

66. What is edge computing vs cloud computing in networking?

- **Cloud Computing**: Processing and storage of data happens on remote servers in large data centers. Data is sent from the device to the cloud, processed, and then a response is sent back.
- **Edge Computing**: The processing and storage of data happens closer to the data source (the "edge" of the network), often on the device itself or a local gateway.
    - **Pros**: Reduces latency, saves bandwidth, and improves privacy.
    - **Use Case**: Ideal for real-time applications like autonomous vehicles or industrial robotics where low latency is critical.

67. What is SDN (Software Defined Networking)?

SDN (Software Defined Networking) is an architectural approach that separates the network's control plane from the data plane. The **control plane** (the "brain") is centralized and managed by a software controller, while the **data plane** (the "muscles") simply forwards data based on the controller's instructions. This allows network administrators to manage the entire network centrally and programmatically, making it more flexible and scalable.

68. What is NFV (Network Function Virtualization)?

NFV (Network Function Virtualization) is the concept of virtualizing network services (like routers, firewalls, and load balancers) that have traditionally run on dedicated hardware. These network functions are instead run as software on standard, general-purpose servers.

- **Benefits**: Reduces hardware costs, allows for faster deployment of new services, and provides greater flexibility.

69. Difference between MPLS and VPN.

- **MPLS (Multiprotocol Label Switching)**: A high-performance routing technique used in telecommunications networks. It directs data packets using short path labels rather than complex IP addresses, which can be faster. It's often used by large enterprises to create a private network across a service provider's infrastructure.
- **VPN (Virtual Private Network)**: A technology that uses encryption to create a secure tunnel over a public network. VPNs can be built on top of any public network, including an MPLS network. While MPLS is a core routing technology, VPN is an overlay technology that focuses on security and privacy.

70. What is mesh network?

A **mesh network** is a network topology where each node (device) is connected to one or more other nodes. This creates multiple paths for data to travel from a source to a destination.

- **Pros**: Highly resilient and reliable because if one path fails, another can be used.
- **Cons**: Can be more complex to set up and manage, and more expensive due to the number of connections.
- **Use Cases**: Home automation (smart lights, sensors), military applications, and large campus networks.

---

8. Network Devices & Tools

---

71. What is a hub, switch, router, modem?

- **Hub**: A basic L1 device that broadcasts all incoming data to all connected devices.
- **Switch**: An intelligent L2 device that forwards data only to the intended destination using MAC addresses.
- **Router**: A L3 device that connects different networks and routes data packets using IP addresses.
- **Modem (Modulator-Demodulator)**: A device that converts digital data from a computer into an analog signal for transmission over an analog medium (like a telephone line or coaxial cable) and vice versa. It's the device that connects your home network to your ISP's network.

72. Difference between L2 and L3 switch.

- **L2 (Layer 2) Switch**: Operates at the Data Link Layer. It forwards data based on **MAC addresses**. It's used to connect devices within a single LAN.

- **L3 (Layer 3) Switch**: Operates at both the Data Link Layer and the Network Layer. It can forward data based on **IP addresses**, which means it can route traffic between different VLANs or subnets. A L3 switch is essentially a hybrid device with both switching and basic routing capabilities.

73. What is a load balancer?

A **load balancer** is a network device or software that distributes incoming network traffic across a group of backend servers. This ensures that no single server is overloaded, improving application performance, reliability, and scalability. It can also perform health checks on servers and direct traffic away from unhealthy ones.

74. What is proxy server vs reverse proxy?

- **Proxy Server (Forward Proxy)**: Acts as an intermediary between a client and a server. It receives requests from clients and forwards them to the server. It can be used for things like content filtering, caching, and improving privacy. **The client knows about the proxy.**
- **Reverse Proxy**: Acts as an intermediary between the server and the client. It receives requests from the internet and forwards them to one or more internal servers. It can be used for load balancing, SSL termination, and security. **The client does not know about the proxy; it thinks it is talking directly to the server.**

75. What is gateway in networking?

A **gateway** is a network node that serves as an entry and exit point for data going from one network to another. It typically operates at all seven layers of the OSI model and can translate data between different protocols. A router is a type of gateway that specifically handles the routing of packets between networks. Your home router acts as a gateway connecting your LAN to the internet.

76. What is IDS and IPS (Intrusion Detection/Prevention)?

- **IDS (Intrusion Detection System)**: A system that monitors network traffic for suspicious activity or policy violations and generates alerts. It's like a security camera; it observes and reports but does not actively stop the attack.
- **IPS (Intrusion Prevention System)**: A system that not only detects but also actively **blocks** or prevents malicious activity in real time. It's like a security guard; it observes, identifies a threat, and then takes action to stop it.

77. What is traceroute?

`traceroute` (or `tracert` on Windows) is a network diagnostic tool that shows the path (the sequence of routers or "hops") a data packet takes from a source to a destination. It measures the round-trip time for each hop, which can help in troubleshooting network latency and identifying where a connection is failing.

78. What is ping command?

`ping` is a command-line utility used to test the reachability of a host on an IP network. It sends an **ICMP (Internet Control Message Protocol)** Echo Request to the target host and

waits for an Echo Reply. It also measures the round-trip time of the packets and reports on any packet loss, which helps determine if a host is up and accessible.

79. What is nslookup/dig?

- **nslookup**: A command-line tool used for querying the **DNS (Domain Name System)** to obtain domain name or IP address mapping or other DNS records. It's a useful tool for troubleshooting DNS-related issues.
- **dig (Domain Information Groper)**: A more advanced and flexible command-line tool for querying DNS. It provides more detailed information and is preferred by network administrators.

80. What is Wireshark?

Wireshark is a free and open-source network protocol analyzer. It allows you to "sniff" or capture network packets in real time and display them in a human-readable format. It's an invaluable tool for network troubleshooting, analysis, software development, and security auditing.

---

9. Advanced Concepts

---

81. What is QoS (Quality of Service)?

QoS (Quality of Service) is a set of technologies that manages network traffic to ensure that certain types of data (e.g., voice, video) are prioritized over others. It works by setting aside network resources or giving priority to critical traffic, guaranteeing a certain level of performance (e.g., minimum bandwidth, low latency) for specific applications.

82. What is MPLS (Multiprotocol Label Switching)?

MPLS (Multiprotocol Label Switching) is a data-carrying mechanism for high-performance telecommunications networks. It directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. MPLS provides a flexible and scalable way to route data and is often used to create virtual private networks (VPNs) and traffic engineering.

83. Difference between circuit switching and packet switching.

- **Circuit Switching**: A dedicated, end-to-end communication path (a "circuit") is established before data transfer begins. All data travels along this single, continuous path.
    - **Pros**: Guaranteed bandwidth and low latency.
    - **Cons**: Inefficient use of bandwidth (the circuit is reserved even if no data is being sent), and a failure in one part of the circuit can terminate the connection. **Example**: Traditional telephone networks.
- **Packet Switching**: Data is broken into small packets, and each packet is sent independently across the network. Packets can take different routes to reach the destination.
    - **Pros**: Efficient use of bandwidth, highly resilient to network failures.

- **Cons**: Potential for variable latency and packet loss. **Example**: The Internet.

84. What is ATM (Asynchronous Transfer Mode)?

ATM (Asynchronous Transfer Mode) is a switching technique for telecommunications networks that transmits data in fixed-size cells (53 bytes). It's a connection-oriented technology that combines the best of circuit switching (guaranteed QoS) and packet switching (efficiency). While once a popular choice for high-speed networks, it has been largely superseded by Ethernet and IP-based technologies.

85. What is BGP (Border Gateway Protocol)?

BGP (Border Gateway Protocol) is a standardized exterior gateway protocol used for routing between autonomous systems (AS) on the internet. It's the "internet's backbone" routing protocol. BGP is responsible for exchanging routing information between large networks (e.g., those of ISPs and large corporations), allowing them to direct traffic efficiently and reliably across the globe.

86. What is OSPF (Open Shortest Path First)?

OSPF (Open Shortest Path First) is a widely used **link-state routing protocol** for internal routing within a single autonomous system (AS). OSPF routers build a complete topology map of the network and use Dijkstra's algorithm to calculate the shortest path to each destination. It's known for its fast convergence and efficiency.

87. What is RIP (Routing Information Protocol)?

RIP (Routing Information Protocol) is an older and simpler **distance-vector routing protocol**. It uses **hop count** as its metric to find the shortest path. RIP is limited by a maximum hop count of 15, making it unsuitable for large networks. It's slow to converge and prone to routing loops, which is why it has been largely replaced by OSPF and other protocols.

88. What is multicast routing?

Multicast routing is a networking technique used to efficiently send a single stream of data from a source to multiple, specific destinations simultaneously. Unlike broadcast (which sends to everyone) and unicast (which sends to one), multicast sends data only to a group of interested receivers. This is highly efficient for applications like live video streaming and online gaming.

89. What is ICMP (Internet Control Message Protocol)?

ICMP (Internet Control Message Protocol) is a protocol used by network devices, like routers, to send error messages and operational information. It's not used for data transfer but for network diagnostics and control. `ping` and `traceroute` commands rely on ICMP.

90. What is Anycast?

Anycast is a network addressing and routing method where data is routed from a sender to the **"nearest"** of a group of potential receivers identified by the same destination address.

This is a crucial technology for large-scale distributed services like DNS, where a client's request is directed to the closest available server.

---

10. Cloud & Distributed Networking

---

91. What is CDN and how does it work?

(See question 50). A **CDN (Content Delivery Network)** is a distributed network of servers that caches content closer to end-users. When a user requests content (like a video or image), the CDN directs the request to the server nearest to the user, reducing latency and bandwidth consumption on the origin server.

92. What is DNS load balancing?

DNS load balancing is a method of distributing network traffic across multiple servers by configuring the DNS to resolve a single domain name into multiple IP addresses. When a client requests the domain, the DNS server can respond with a different IP address from the list each time (e.g., using a round-robin approach), spreading the traffic across the servers.

93. Difference between vertical scaling and horizontal scaling in networks.

- **Vertical Scaling (Scaling Up)**: Increasing the capacity of a single machine by adding more resources (e.g., more CPU, RAM, or storage).
    - **Pros**: Simpler to implement.
    - **Cons**: Limited by the maximum capacity of a single machine, and a single point of failure.
- **Horizontal Scaling (Scaling Out)**: Adding more machines to a system to distribute the workload.
    - **Pros**: Highly scalable, no single point of failure.
    - **Cons**: More complex to manage, requires a load balancer.

94. What is Kubernetes networking?

Kubernetes networking is the set of rules and components that enables communication between containers, pods, and services within a Kubernetes cluster and with the external world. Key concepts include:

- **Pod IP Addresses**: Each pod gets a unique IP address within the cluster.
- **Service**: A stable IP address and DNS name that load balances traffic to a set of pods.
- **Ingress**: A way to manage external access to services in the cluster.

95. What is service mesh (Istio, Linkerd)?

A **service mesh** is a dedicated infrastructure layer for handling service-to-service communication in a microservices architecture. It provides a way to manage, control, and observe communication. It's often implemented by deploying a lightweight proxy (a "sidecar") alongside each service.

- **Benefits**: Offloads complex networking tasks like load balancing, security, and monitoring from the application code.
- **Examples**: Istio, Linkerd.

96. What is API Gateway in cloud networking?

An **API Gateway** is a central entry point for all client requests to a backend service. It acts as a single point of contact, routing requests to the appropriate microservices. It can also handle cross-cutting concerns like authentication, rate limiting, and caching, simplifying the client's interaction with the backend.

97. How does load balancing work in AWS/GCP/Azure?

Cloud providers offer sophisticated load balancing services (e.g., **AWS Elastic Load Balancer (ELB)**, **Google Cloud Load Balancing**, **Azure Load Balancer**). These services automatically distribute incoming traffic across a pool of compute instances (e.g., virtual machines, containers) in different availability zones. They can perform health checks, use various algorithms (e.g., round-robin, least-connections), and automatically scale to handle varying traffic loads.

98. What is VPC (Virtual Private Cloud)?

A **VPC (Virtual Private Cloud)** is a private, isolated network within a public cloud (like AWS, GCP, or Azure). It provides a logically isolated virtual network where you can launch and manage your cloud resources (e.g., virtual servers, databases) in a controlled environment. You have full control over the IP address range, subnets, routing tables, and security groups.

99. What is hybrid cloud networking?

Hybrid cloud networking is a network model that connects a private, on-premises network to one or more public cloud networks. This allows organizations to leverage the scalability and flexibility of the public cloud while maintaining control over sensitive data and applications in their private data center. It often uses technologies like VPNs or dedicated connections (e.g., AWS Direct Connect) to create a secure link.

100. Difference between monolithic, SOA, and microservices communication in networks.

- **Monolithic**: All components of an application are tightly coupled and run as a single process. Communication is simple, usually via function calls.
- **SOA (Service-Oriented Architecture)**: The application is composed of loosely coupled services that communicate over a network. This is often done via an **Enterprise Service Bus (ESB)**, which acts as a central intermediary.
- **Microservices**: The application is broken down into a collection of very small, independent services. Communication is typically done via lightweight, simple APIs (e.g., REST, gRPC). Network latency and reliability become critical, and a **service mesh** is often used to manage this complex inter-service communication.