Computer Networks

Basic Terminologies:

1. **IP (Internet Protocol):** IP stands for Internet Protocol, a fundamental communication protocol that facilitates the transmission of data across networks. It provides a set of rules governing how data packets should be addressed, routed, and fragmented, ensuring reliable and efficient delivery between devices over the internet or any interconnected network. IP addresses uniquely identify devices on a network and enable them to communicate with each other.
2. **Proxy:** A proxy acts as an intermediary between a client (such as a web browser) and a server. It receives requests from clients seeking resources (like web pages) and forwards those requests to the appropriate servers. Proxies can also provide additional functionalities like caching, security, or anonymity.
3. **Client:** In networking, a client refers to a device or software that requests services or resources from a server. Examples include computers, smartphones, or any device that uses services provided by servers.
4. **Server:** A server is a computer or device that provides resources, data, services, or functionality to other computers or devices, known as clients, over a network. Servers respond to requests made by clients, providing access to files, web pages, emails, or other resources.
5. **Peer:** In networking, a peer refers to any device or entity that is of equal standing or operates at the same level within a network. Peers can communicate directly with each other without relying on a central server.
6. **Host:** A host can refer to any device (such as a computer or server) connected to a network that has its own IP address and can send or receive data within that network or across the internet.
7. **Packet:** A packet is a unit of data that travels across a network. It consists of the data being transmitted along with additional information like the source and destination addresses, error-checking codes, and sequencing details.
8. **Frame:** In networking, a frame is a unit of data at the data link layer of the OSI model. It encapsulates packets for transmission over a physical network medium

and includes details such as MAC addresses, error checking, and synchronization information.

9. **Segment:** In networking, a segment refers to a portion of data generated by a host for transmission across a network. Segments are specifically associated with the transport layer (Layer 4 in the OSI model), where they are created by segmenting larger messages or data into smaller, manageable units for transmission.
10. **Local Host:** It refers to the computer or device that an individual is currently using. It is typically identified by the IP address "127.0.0.1" in IPv4 (or "::1" in IPv6) and is used to access the networking services available on that particular device. When a program or service refers to the "localhost," it means the device itself. This address is often used to test networking programs or access services running on the same machine.

Types of Networks (on the basis of scope)

1. **Personal Area Network (PAN):**
    - **Definition:** A PAN is a network focused on connecting devices around an individual person, typically within a range of a few meters.
    - **Characteristics:** PANs are used for personal convenience and might use technologies like Bluetooth, infrared, or Wi-Fi Direct.
    - **Example:** When a smartphone connects via Bluetooth to wireless headphones, a smartwatch, and a laptop simultaneously, forming a network around the user, it constitutes a PAN.
2. **Local Area Network (LAN):**
    - **Definition:** A LAN is a network that covers a small geographical area, such as a single building, office, or campus. It allows computers and devices to share resources and information within a confined space.
    - **Characteristics:** LANs are typically owned, controlled, and managed by a single organization. They offer high data transfer rates and low latency.
    - **Example:** In an office, all computers, printers, servers, and other devices connected to the same Wi-Fi router or Ethernet switch form a LAN. This network

facilitates internal communication, file sharing, and resource access among employees.

3. **Metropolitan Area Network (MAN):**
    - **Definition:** A MAN covers a larger geographical area, like a city or a town, interconnecting multiple LANs within that region.
    - **Characteristics:** MANs bridge the gap between LANs and WANs. They might use technologies like fiber optics, microwave links, or leased lines.
    - **Example:** A university campus network connecting various departments, libraries, and administrative offices spread across a city could be considered a MAN. It facilitates data sharing and communication within the institution.
4. **Wide Area Network (WAN):**
    - **Definition:** A WAN spans a vast geographical area, connecting multiple LANs, MANs, or other WANs across cities, countries, or continents.
    - **Characteristics:** WANs use public or private networks and might rely on leased lines, satellites, or the internet for connectivity. They typically have lower data transfer rates compared to LANs.
    - **Example:** The internet itself is the largest WAN. It connects billions of devices worldwide, allowing users to access resources, websites, and services from anywhere with an internet connection.

Routers, Switches, Hubs & Bridges

Feature	Router	Switch	Hub	Bridge
Device Function	Routes data packets between different networks	Forwards data packets within a single network based on MAC addresses	Broadcasts data to all devices in the network	Connects network segments, forwarding traffic based on MAC addresses
Layer in OSI Model	Operates at the Network Layer (Layer 3)	Operates at the Data Link Layer (Layer 2)	Operates at the Physical Layer (Layer 1)	Operates at the Data Link Layer (Layer 2)
Packet Handling	Uses IP addresses for	Uses MAC addresses for	Broadcasts packets to all	Uses MAC addresses for

Feature	Router	Switch	Hub	Bridge
	routing	forwarding	connected devices	forwarding
Broadcasts	Does not forward broadcasts between networks	Does not forward broadcasts between ports	Broadcasts data to all connected ports	Does not forward broadcasts between segments

Unicast, Broadcast & Multicast

● **Unicast:** It refers to the transmission of data from a single sender to a specific individual receiver. The data packet is intended for and delivered to only one destination device within the network.
Example: Imagine sending a personal message to a friend using a messaging app. When you send the message, it goes directly to your friend, and only your friend receives and reads it. Unicast is like a one-to-one communication, where data is sent from a single sender to a single receiver.
● **Broadcast:** It involves the transmission of data from a single sender to all devices within the network. The data packet is duplicated and sent to all devices, regardless of whether they need the information or not.
Example: Think of a public announcement made over a loudspeaker in a crowded place. Everyone within the range of the loudspeaker can hear the message simultaneously. Broadcast is like a one-to-all communication, where data is sent from a single sender to all devices within the network.
● **Multicast:** It is the transmission of data from a single sender to a select group of recipients. The data packet is copied and delivered only to those devices that have joined the multicast group, indicating their interest in the data.
Example: Picture a teacher in a classroom sharing a specific message with a group of students who are working on a project together. Multicast is like a one-to-many communication, where data is sent from a single sender to a specific group of receivers who are interested in the information.

Network Topology

Aspect	Ring	Mesh	Bus	Star
Definition	Circular or ring-like topology	Interconnected topology where	Linear topology where all devices	Centralized topology where

Aspect	Ring	Mesh	Bus	Star
	where each device connects to exactly two other devices forming a closed loop.	every device has direct point-to-point links with every other device in the network.	are connected to a single backbone cable.	all devices connect to a central hub or switch.
Cost	Moderate cost due to the required cabling and devices, but fewer cables compared to mesh topology.	High cost due to the extensive cabling required for direct connections between every device.	Low cost as it requires minimal cabling, but additional devices may degrade the signal.	Moderate cost for the central hub/switch, and cabling to connect devices to the hub.
Security	Moderate security as data flows in a specific direction; however, a single point failure can disrupt the entire network.	High security due to multiple paths and direct connections, enabling better isolation and control.	Low security as data is broadcast along the backbone, received by all devices.	Moderate security as the hub can be a potential single point of failure, but easier to control access centrally.
Scalability	Limited scalability due to the closed-loop structure; adding or removing devices can disrupt the ring.	Highly scalable with excellent potential for expansion due to multiple paths for data to travel.	Limited scalability due to signal degradation as additional devices are added.	Easily scalable by adding new devices without disrupting existing connections.
Fault Tolerance	Vulnerable to single point failures; a failure at any point can disrupt the entire network.	High fault tolerance as multiple paths ensure network resilience; faults in one path don’t affect the entire network.	Moderate fault tolerance; a single cable failure can affect the entire network.	Moderate fault tolerance; failure of the central hub can disrupt the network, but individual device failures may not impact others.

Internet Protocol (IP)

An Internet Protocol (IP) address serves as a distinctive identifier assigned to each device connected to the internet. It is a numeric label that enables devices utilizing the internet to communicate and share information with pinpoint accuracy. Whether computers are interacting over the internet or within local networks, they rely on IP addresses to precisely direct data to specific destinations. These addresses facilitate seamless communication by uniquely labeling each connected device, ensuring data reaches its intended target across global or localized networks.

▼ Classes of IPs

1. **Class A Addresses:**
   - **Range:** IP addresses in Class A have their first bit set to 0. The first octet represents the network portion, and the remaining three octets represent the host portion. An IP address in Class A ranges from 0.0.0.0 to 127.255.255.255.
   - **Usage:** Class A addresses are typically assigned to large networks due to their capacity for a vast number of hosts. However, due to the limited number of available Class A networks, they are relatively scarce.
2. **Class B Addresses:**
   - **Range:** Class B IP addresses start with the first two bits set to 10. The first two octets represent the network portion, and the remaining two octets represent the host portion. IP addresses in Class B range from 128.0.0.0 to 191.255.255.255.
   - **Usage:** Class B addresses are commonly used by medium-sized organizations or institutions that require a moderate number of networks and hosts.
3. **Class C Addresses:**
   - **Range:** IP addresses in Class C have their first three bits set to 110. The first three octets represent the network portion, and the last octet represents the host portion. Class C addresses range from 192.0.0.0 to 223.255.255.255.
   - **Usage:** Class C addresses are often utilized by smaller networks or home networks due to their ability to provide a large number of networks with a relatively smaller number of hosts per network.

4. **Class D Addresses:**
    - **Range:** Class D IP addresses start with the first four bits set to 1110. These addresses are specifically reserved for multicast group purposes. Class D addresses range from 224.0.0.0 to 239.255.255.255.
    - **Usage:** Class D addresses are utilized for multicast group communication, enabling data transmission to multiple recipients simultaneously.
5. **Class E Addresses:**
    - **Range:** Class E IP addresses begin with the first four bits set to 1111. These addresses were initially designated for experimental and research purposes. Class E addresses range from 240.0.0.0 to 255.255.255.255.
    - **Usage:** Class E addresses are not intended for standard IP routing and are reserved for experimental use, not commonly used in public networks.

It's essential to note that the concept of IP classes is no longer used for IP address assignment due to the adoption of CIDR. CIDR allows for more efficient and flexible allocation of IP addresses.

NOTE: I highly recommend watching GATE Smasher' s explanation on this topic to completely understand the underlying concept. This is a very important topic if the interviewer is interested in checking networking fundamentals.

▼ Reserved IP addresses

1. **Loopback Address:**
    - **Definition:** A loopback address is an IP address that allows a device to send and receive data to itself. The most commonly used loopback address is 127.0.0.1, which is a part of the loopback address range 127.0.0.0/8.
    - **Purpose:** It's used for testing network software or services on a device without affecting the network or communicating with other devices. This address allows a computer to verify that its networking software is working correctly.
2. **Link-Local Address:**
    - **Definition:** A link-local address is an IP address assigned to a network interface when no other IP address configuration is available. In IPv4, the

link-local address range is 169.254.0.0/16, and in IPv6, it uses the prefix fe80::/10.

- **Purpose:** Link-local addresses are typically assigned automatically when a device is unable to obtain an IP address through DHCP or other manual configuration methods. These addresses facilitate communication on a local network segment, allowing devices to communicate with each other on the same physical network when no other IP configuration is available.

3. **Broadcast Address:**
    - **Definition:** The broadcast address is the highest address within a network range. In a network with the address range 192.168.1.0/24, the broadcast address would be 192.168.1.255.
    - **Purpose:** Used to send data simultaneously to all devices within the network. When data is sent to the broadcast address, it reaches all hosts within that network.

▼ IPv4 vs. IPv6

Feature	IPv4	IPv6
Address Length	32 bits	128 bits
Address Representation	Decimal format (e.g., 192.168.1.1)	Hexadecimal format (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Configuration	Manual and DHCP	Autoconfiguration (Stateless or DHCPv6)
Address Types	Public and Private	Global unicast, Unique local, Link-local, Multicast
Address Exhaustion	Depletion of available addresses	Expanded address space to accommodate growth
Fragmentation	Routers and devices perform fragmentation	Fragmentation handled at the source
Security	Limited built-in security	Enhanced security features (IPSec integration)

IPv6, the successor to IPv4, was introduced primarily due to the limitations and challenges faced by IPv4. Several key reasons prompted the development and implementation of IPv6:

1. **Address Exhaustion:** IPv4 uses 32-bit addresses, providing approximately 4.3 billion unique addresses. With the rapid expansion of the internet and the proliferation of connected devices, the pool of available IPv4 addresses became insufficient. IPv6's 128-bit addressing scheme offers an immensely larger address space (3.4 x 10^38 addresses), ensuring an abundant supply of unique addresses to accommodate the growing number of devices worldwide.
2. **Enhanced Functionality:** IPv6 offers improvements in various aspects compared to IPv4. It incorporates features like more efficient routing, simpler header formats, improved support for multicast communication, and enhanced security features, including the integration of IPSec (Internet Protocol Security) as a fundamental component of the protocol.
3. **Autoconfiguration and Plug-and-Play:** IPv6 includes features for easier network setup and configuration. With stateless address autoconfiguration, devices can automatically assign themselves a unique address without the need for manual configuration or DHCP (Dynamic Host Configuration Protocol) servers. This facilitates easier plug-and-play functionality, especially for mobile devices and IoT devices.
4. **Transition and Coexistence:** IPv6 was designed with transitional mechanisms to facilitate the coexistence of IPv4 and IPv6 networks during the migration process. This allows gradual adoption and interoperability between the two protocols, enabling a smooth transition without disrupting existing IPv4 networks.

Overall, the introduction of IPv6 was driven by the need to overcome the limitations of IPv4, such as address exhaustion, and to meet the requirements of a rapidly expanding and evolving internet landscape, ensuring continued growth, scalability, and improved functionality for global network infrastructure.

Network Address Translation (NAT)

NAT stands for network address translation. It’s a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.

The core functionality of NAT involves the translation of IP addresses, enabling multiple devices within a local network to share a single public IP address for communication over the internet. Here's an overview of how NAT works:

1. **Private and Public Addresses:**

Feature	**Public IP Addresses**	**Private IP Addresses**
Usage	Assigned to devices connected directly to the Internet	Used within private networks (LANs, home networks, corporate intranets)
Address Range	Globally unique, assigned by ISPs	Reserved address ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
Scalability	Limited availability due to IPv4 address exhaustion	Abundantly available within local networks
Security Implication	Directly exposed to the Internet, security measures required	Hidden from external networks, basic security through obscurity
Examples	IP addresses assigned to servers, routers, public-facing devices	IP addresses assigned to computers, printers, devices within a local network

2. **Translation Process:**

   - **Outgoing Traffic:** When a device within the private network initiates communication with the internet, NAT translates its private IP address to the public IP address of the NAT device. This translation involves replacing the source IP address and port number of outgoing packets with the NAT device's public IP address and unique port number.
   - **Reverse Translation:** When the response returns from the internet, the NAT device uses stored mapping information to reverse the translation process. It changes the destination IP address and port back to the original private IP address and port, ensuring the response reaches the correct device within the private network.

Benefits of NAT:

1. **Address Conservation:** NAT allows multiple devices within a private network to share a single public IP address. This helps conserve public IPv4 addresses, which are limited in availability.
2. **Basic Security:** Since devices in the private network use private IP addresses, they are not directly reachable from the internet. NAT acts as a basic firewall by hiding

internal IP addresses, providing a level of security by obscurity.

Overall, NAT facilitates the interaction of devices with private IP addresses within a local network to communicate with external servers or services over the internet by translating their private addresses to a single public IP address, thereby enabling efficient use of limited IPv4 addresses.

OSI Model

1. Physical Layer (Layer 1):

- Involves the transmission and reception of unstructured raw data bits through a physical medium like copper wires, fiber optics, or wireless channels.
- Defines specifications for electrical, mechanical, and functional connections to the network.

Examples: Voltage levels, cable types (twisted pair, coaxial, fiber optics), connectors (RJ45, BNC), and signal encoding (Manchester encoding, NRZ).

2. Data Link Layer (Layer 2):

- Manages the flow of data frames between devices connected on the same local network.
- Includes the Logical Link Control (LLC) sublayer for error checking and the Media Access Control (MAC) sublayer for addressing and managing access to the network medium.
- Handles framing, error detection, flow control, and access control to the physical medium.

Examples: Ethernet switches, MAC addresses, error detection (CRC), and data frame formats.

3. Network Layer (Layer 3):

- Focuses on routing and forwarding data packets across different networks.
- Provides logical addressing (IP addressing) to devices, determines optimal routes for data, and ensures successful delivery of packets.
- Handles packet switching, addressing, routing protocols (OSPF, BGP), and fragmentation/reassembly.

Examples: Routers, IP addresses, Internet Protocol (IPv4, IPv6).

4. Transport Layer (Layer 4):

- Manages end-to-end communication between devices.
- Ensures reliable and ordered delivery of data by providing error detection, flow control, and data segmentation/assembly.
- Includes protocols such as TCP (Transmission Control Protocol) for reliable and connection-oriented communication and UDP (User Datagram Protocol) for faster but unreliable communication.

Examples: TCP, UDP, port numbers, flow control mechanisms.

5. Session Layer (Layer 5):

- Establishes, manages, and terminates communication sessions between applications running on different devices.
- Handles session establishment, synchronization, checkpointing, and termination.
- Controls dialogues and maintains sessions for data exchange.

Examples: Session control, NetBIOS, RPC (Remote Procedure Call).

6. Presentation Layer (Layer 6):

- Deals with data representation and translation for application-layer compatibility.
- Handles data compression, encryption, and conversion between different data formats.
- Converts data between different character encodings and formats to ensure compatibility.

Examples: Encryption protocols (SSL/TLS), data compression algorithms (ZIP, JPEG), ASCII to Unicode conversion.

7. Application Layer (Layer 7):

- Provides network services directly to end-users or applications.
- Contains protocols and interfaces that allow user applications to interact with the network.

- Includes various protocols for services such as file transfer (FTP), web browsing (HTTP), email (SMTP), and remote access (SSH).

Examples: HTTP, FTP, SMTP, DNS, DHCP.

TCP/IP Model

The TCP/IP model, also known as the Internet Protocol Suite, is a conceptual framework defining the functions and protocols used for communication on the internet. It consists of four interconnected layers, which differ slightly from the OSI model. Here's a technical breakdown of the TCP/IP model:

1. Network Interface Layer (Link Layer):

- Similar to the Data Link Layer in the OSI model.
- Handles the physical transmission of data on the network medium.
- Responsible for accessing the network hardware and addressing using MAC addresses.

Examples: Ethernet, Wi-Fi, ARP (Address Resolution Protocol).

2. Internet Layer (Network Layer):

- Corresponds to the OSI Network Layer.
- Focuses on routing packets across different networks and logical addressing.
- Provides logical addressing using IP addresses and determines the best path for data transmission.
- Protocols include IP (Internet Protocol), ICMP (Internet Control Message Protocol), and routing protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol).

3. Transport Layer:

- Combines functionalities of the OSI Transport Layer and higher.
- Provides end-to-end communication between devices across the network.
- Manages reliable and connection-oriented communication (similar to OSI's Transport Layer).

- Includes TCP (Transmission Control Protocol) for reliable data transmission and UDP (User Datagram Protocol) for connectionless and faster data transfer.

4. Application Layer:

- Corresponds to the top three layers (Session, Presentation, and Application) of the OSI model.
- Provides network services directly to user applications.
- Contains protocols for various applications and services like HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), and more.

The TCP/IP model serves as the basis for the modern internet and is widely used in networking. It organizes network communication into layers that interact with each other through well-defined protocols, allowing different devices and systems to communicate effectively across the internet.

▼ Application Layer Protocols

1. **HTTP (Hypertext Transfer Protocol):**
    - Used for transmitting web pages and data on the World Wide Web.
    - Operates over TCP port 80.
    - Responsible for fetching and displaying web content in browsers.
2. **HTTPS (Hypertext Transfer Protocol Secure):**
    - Similar to HTTP but operates over a secure encrypted connection (SSL/TLS).
    - Operates over TCP port 443.
    - Provides secure communication for sensitive data transmission, used for secure online transactions, login pages, etc.
3. **IMAP (Internet Message Access Protocol):**
    - Allows access and retrieval of emails from a remote server.
    - Operates over TCP port 143 or encrypted port 993 (IMAPS).

- Offers more advanced email management features compared to POP3.

4. **POP3 (Post Office Protocol version 3):**
   - Retrieves emails from a mail server to a client device.
   - Operates over TCP port 110 or encrypted port 995 (POP3S).
   - Downloads emails from the server and often deletes them by default.
5. **FTP (File Transfer Protocol):**
   - Used for transferring files between devices on a network.
   - Operates over TCP ports 20 (data transfer) and 21 (control).
   - Supports uploading, downloading, and managing files on servers.
6. **SMTP (Simple Mail Transfer Protocol):**
   - Used for sending email messages between servers on the internet.
   - Operates over TCP port 25.
   - Handles outgoing mail transfer from a client or server to another mail server.
7. **DNS (Domain Name System):**
   - Translates domain names into IP addresses and vice versa.
   - Operates over UDP (User Datagram Protocol) on port 53.
   - Resolves domain names to their corresponding IP addresses for internet navigation.
8. **DHCP (Dynamic Host Configuration Protocol):**
   - Assigns IP addresses and network configurations dynamically to devices on a network.
   - Operates over UDP on port 67/68.
   - Facilitates automatic IP address allocation to devices upon connection to a network.
9. **SSH (Secure Shell):**
   - Provides secure, encrypted communication between devices.

- Operates over TCP port 22.
- Enables secure remote access, command execution, and file transfer over an insecure network.

10. **Telnet:**
    - Provides remote access to devices' command-line interface.
    - Operates over TCP port 23.
    - Allows users to interact with devices remotely, but lacks encryption, making it less secure than SSH.

▼ Transport Layer Protocols

TCP (Transmission Control Protocol):

- **Function:** TCP is a connection-oriented protocol that ensures reliable and ordered data delivery between devices over an IP network. It offers error checking, acknowledgment of received data, and retransmission of lost packets. TCP breaks data into segments and numbers each segment for reassembly at the receiving end.
- **Key Characteristics:**
  - Reliable: Guarantees that data arrives intact and in the correct order.
  - Connection-oriented: Establishes a connection between devices before transmitting data.
  - Flow control and congestion avoidance: Manages data flow to prevent overwhelming the receiver or network congestion.
  - Slower compared to UDP due to additional features like error correction and acknowledgment.

UDP (User Datagram Protocol):

- **Function:** UDP is a connectionless protocol that offers faster, but less reliable, data transmission. It doesn't ensure delivery or order of packets and lacks built-in error-checking mechanisms. UDP is suitable for time-sensitive applications that prioritize speed over reliability.

- **Key Characteristics:**
  - Unreliable: Doesn't guarantee delivery or packet order.
  - Connectionless: Doesn’t establish a connection before sending data.
  - Faster than TCP due to minimal overhead and fewer error-checking features.
  - Used in applications like real-time video streaming, online gaming, DNS, and VoIP.

TCP/IP (Transmission Control Protocol/Internet Protocol):

- **Function:** TCP/IP is a suite of communication protocols that form the foundation of the internet. It consists of various protocols, including TCP, UDP, IP, ICMP, and others. TCP/IP provides the framework for data transmission and addressing on the internet.
- **Key Characteristics:**
  - Provides the core protocols for transmitting data over the internet.
  - IP handles addressing and routing, while TCP and UDP manage data transfer.
  - Ensures interoperability between different types of computers and networks.
  - Defines how data should be formatted, addressed, transmitted, routed, and received.

ICMP (Internet Control Message Protocol):

- **Function:** ICMP is used for diagnostic and error-reporting functions in IP networks. It sends control messages between network devices to report errors, check network connectivity, perform diagnostics, and handle routing issues.
- **Key Characteristics:**
  - Not used for regular data transmission but for network management and troubleshooting.
  - Reports errors (e.g., unreachable hosts) by sending ICMP messages to the source.

    - Includes tools like ping (to check network connectivity) and traceroute (to trace the route taken by packets).

▼ Network Layer Protocols

1. OSPF (Open Shortest Path First):

- **Function:** OSPF is an Interior Gateway Protocol (IGP) used within autonomous systems (AS) or networks to determine the best paths for routing IP packets. It calculates the shortest path (based on cost) between routers using the Dijkstra algorithm and maintains a database of network topology.
- **Key Characteristics:**
    - Dynamic routing protocol for internal networks (e.g., within an organization).
    - Supports variable-length subnet masking (VLSM) and classless addressing.
    - Provides faster convergence and scalability compared to distance vector protocols.
    - Utilizes areas to scale large networks and reduce routing overhead.

2. RIP (Routing Information Protocol):

- **Function:** RIP is one of the oldest distance vector routing protocols used for routing within small to medium-sized networks. It employs the Bellman-Ford algorithm to determine the best path to a destination based on hop count (number of routers).
- **Key Characteristics:**
    - Limited to small networks due to its slow convergence and hop count metric.
    - Broadcasts routing table updates at regular intervals (30 seconds).
    - Supports classful addressing and doesn't support VLSM or CIDR.
    - May experience routing loops and has limitations in larger networks.

3. ARP (Address Resolution Protocol):

- **Function:** ARP is used to map an IP address to a MAC address within a local network. When a device wants to communicate with another device on the same subnet, but only knows its IP address, it sends an ARP request to discover the MAC address corresponding to that IP.

- **Key Characteristics:**
  - Resolves IP addresses to MAC addresses for communication within the same subnet.
  - Operates at the data link layer (Layer 2) of the OSI model.
  - Devices maintain an ARP cache to store recently resolved IP-to-MAC mappings for faster communication.
  - Essential for Ethernet networks to establish direct communication between devices.

Packet Traversal in OSI Model

1. Physical Layer (Layer 1):

- Handles the physical transmission of data using copper cables, fiber optics, or wireless signals.
- Converts data into electrical signals, light pulses, or radio waves for transmission.

2. Data Link Layer (Layer 2):

- Creates frames that include source and destination MAC addresses and LLC error codes.
- Performs error checking and may retransmit data if necessary.
- Uses ARP (Address Resolution Protocol) to determine MAC addresses.

3. Network Layer (Layer 3):

- Adds a new header with source and destination IP addresses to the packet.
- Routes packets based on destination IP addresses, determining the best path.
- Determines the next-hop router for forwarding packets.

4. Transport Layer (Layer 4):

- Ensures end-to-end communication and reliable data delivery.
- Divides data into segments or datagrams and assigns sequence numbers.

- Establishes connections (TCP) or operates connectionlessly (UDP).

5. Session Layer (Layer 5):

- Establishes, manages, and terminates communication sessions between applications.
- Sets up, maintains, and closes connections as needed.

6. Presentation Layer (Layer 6):

- Responsible for data formatting, encryption, and compression.
- Converts data into a standardized format understandable by both sender and receiver.
- Applies encryption to secure data.

7. Application Layer (Layer 7):

- Generates and processes data by applications running on the source device.
- Formats data into messages or requests suitable for the application being used.
- Examples include sending emails, accessing websites, etc.

Network Commands

1. Ping (Packet Internet Groper):

- **Function:** Ping is a command-line utility used to test connectivity between devices. It sends ICMP Echo Request messages to a target device and waits for an ICMP Echo Reply. This utility helps in checking if a destination host is reachable and measures the round-trip time (RTT) for packets.
- **Usage:** `ping <IP address or domain>` or `ping <hostname>`

2. Netstat (Network Statistics):

- **Function:** Netstat is a command-line tool used to display network connections, routing tables, interface statistics, and various network-related information. It provides information on active network connections, listening ports, routing tables, and network protocol statistics.
- **Usage:** `netstat [-a] [-b] [-n] [-r]`

3. Ipconfig (Internet Protocol Configuration):

- **Function:** Ipconfig is a Windows command used to display the IP configuration details of a device, including IP address, subnet mask, default gateway, and MAC address. It provides information about the current network configuration of a computer.
- **Usage:** `ipconfig` or `ipconfig /all`

4. Tracert (Trace Route):

- **Function:** Tracert is a command-line tool used to trace the route that packets take from the local device to a specified destination. It shows the path taken by packets and measures the round-trip time (RTT) to each intermediate network device (router) along the way.
- **Usage:** `tracert <IP address or domain>` or `tracert <hostname>`

5. NSLookup (Name Server Lookup):

- **Function:** NSLookup is a command-line tool used to query DNS (Domain Name System) servers to obtain domain name or IP address information. It is helpful in performing DNS lookups, resolving domain names to IP addresses, and vice versa.
- **Usage:** `nslookup <domain>` or `nslookup <IP address>`

Working of ARP

Scenario: Device A wants to send data to Device B using its IP address.
ARP Request (Resolution):
● Device A checks its ARP cache (a table that stores IP-to-MAC mappings) to see if it already knows the MAC address of Device B for the given IP address.
● If the MAC address is not in the cache, Device A sends an ARP request broadcast packet to the local network. This broadcast is sent to all devices on the same network segment, asking for the MAC address associated with the target IP address (belonging to Device B).

ARP Reply (Resolution):
● Device B receives the ARP request and checks if the IP address in the request matches its own.
● If it matches, Device B responds with an ARP reply packet, which includes its MAC address.

● The ARP reply is sent directly to the requesting device (Device A) since the MAC address of Device A is included in the ARP request.

Updating ARP Cache:

● Once Device A receives the ARP reply from Device B, it updates its ARP cache with the IP-to-MAC mapping of Device B.

● This mapping is stored in the ARP cache for a certain period of time (ARP cache timeout), after which it might be cleared to ensure that outdated information doesn't cause communication issues.

Sending Data:

● Now that Device A knows the MAC address of Device B, it encapsulates the data it wants to send in a data packet with the MAC address of Device B in the Ethernet header.

● The data packet is then sent to the local network, and switches or routers forward it to Device B using its MAC address.

Communication:

● Device B receives the data packet, processes it, and responds as needed.

Working of DHCP

DHCP, or Dynamic Host Configuration Protocol, is a network protocol used to automatically assign IP addresses.

Scenario: Setting Up a New Device on a Network

Device Initialization:

● Imagine you've just bought a new laptop and want to connect it to your home network.

● The laptop's network settings are initially configured to obtain an IP address automatically.

DHCP Client Initialization:

● When you power on the laptop and connect it to your home Wi-Fi, it doesn't have an IP address yet.

● The laptop broadcasts a DHCP Discover message to the local network, indicating that it's looking for an IP address and network configuration.

DHCP Server Discovery:

● Your home network has a DHCP server, which receives the discover message from the laptop.

● The DHCP server is responsible for managing IP addresses and configuration settings for devices on the network.

DHCP Offer:
● The DHCP server responds with a DHCP Offer message.
● The Offer includes an available IP address (e.g., 192.168.1.5) and other configuration options like subnet mask (e.g., 255.255.255.0), gateway IP (e.g., 192.168.1.1), and DNS server IPs (e.g., 8.8.8.8).
DHCP Client Request:
● The laptop receives the Offer and evaluates the provided information.
● It sends a DHCP Request message to the DHCP server, confirming that it wants to use the offered IP address and configuration.
DHCP Server Acknowledgment:
● The DHCP server receives the Request and verifies that the IP address is still available.
● If the IP address is available, the server sends a DHCP Acknowledge (ACK) message to the laptop.
● The ACK message confirms the allocation of the IP address 192.168.1.5 and provides the final configuration details.
Configuration:
● The laptop configures its network settings based on the information provided in the ACK message.
● It sets its IP address to 192.168.1.5, subnet mask to 255.255.255.0, gateway to 192.168.1.1, and DNS server(s) to 8.8.8.8.

Working of DNS

The Domain Name System (DNS) is a hierarchical and distributed naming system used to translate human-readable domain names (like example.com) into IP addresses and vice versa. It plays a crucial role in internet communication by facilitating the mapping of domain names to their corresponding IP addresses.

1. DNS Resolver:

- When a user types a domain name into a web browser, the device starts the DNS resolution process by querying a DNS resolver. This resolver can be local (like your ISP's DNS server) or configured manually (like Google's public DNS servers).
- The resolver checks its cache for the requested domain's IP address. If it's not there or has expired, the resolver proceeds with the DNS resolution process.

2. Root Servers:

- If the DNS resolver doesn’t have the IP address in its cache, it contacts a root DNS server. There are 13 sets of root servers worldwide, each managed by different organizations.
- The root servers don’t store information about every domain; instead, they maintain information about the authoritative DNS servers for each top-level domain (TLD), like .com, .net, .org, etc.

3. Top-Level Domain (TLD) Servers:

- The root server provides the DNS resolver with the IP address of the authoritative name server responsible for the specific TLD requested (e.g., .com, .org, etc.).
- The resolver then contacts the TLD server, which holds information about the authoritative name servers for second-level domains (SLDs) within that TLD.

4. Authoritative Name Servers:

- The TLD server directs the resolver to the authoritative name server responsible for the requested domain (e.g., example.com).
- The authoritative name server contains specific domain information, such as IP addresses, associated with that domain.
- There are typically multiple authoritative name servers for redundancy and load distribution.

5. DNS Resolution and Response:

- The resolver queries the authoritative name server for the IP address associated with the requested domain.
- The authoritative name server responds to the resolver with the corresponding IP address.
- The resolver caches this information for future use and sends the IP address to the user's device, enabling it to establish a connection with the requested website or service.

HTTP vs. HTTPS

Feature	HTTP	HTTPS
Security	Operates over a non-secure connection; data transmitted in plain text, vulnerable to interception.	Adds an extra layer of security by using encryption (SSL/TLS protocols) to protect data exchanged.
Protocol	Standard protocol for transferring web page data over the internet.	Extension of HTTP with added security protocols (SSL/TLS) for data protection.
Port	Operates over port 80 by default.	Operates over port 443 by default.
URL Scheme	URLs begin with "http://".	URLs start with "https://".
Trust & Authentication	Does not provide authentication of the website's identity.	Provides authentication of the website's identity using SSL certificates.

▼ SSL vs. TLS

Secure Sockets Layer (SSL) is a communication protocol, or set of rules, that creates a secure connection between two devices or applications on a network. SSL is technology your applications or browsers may have used to create a secure, encrypted communication channel over any network. However, SSL is an older technology that contains some security flaws. Transport Layer Security (TLS) is the upgraded version of SSL that fixes existing SSL vulnerabilities. TLS authenticates more efficiently and continues to support encrypted communication channels.

POODLE Attack: The POODLE attack, specifically targets SSL 3.0, an outdated encryption protocol used to protect internet connections.

This attack took advantage of a weakness in SSL 3.0's cipher block chaining (CBC) mode, exploiting a vulnerability in how this protocol handled data padding. By forcing a connection to use SSL 3.0 and tampering with the encrypted data, attackers could intercept and decipher sensitive information transmitted between a user's web browser and a server.

Here's how it worked: Attackers downgraded the connection to use SSL 3.0, manipulated the encrypted data, and exploited errors in SSL 3.0's padding mechanism. Through a series of trial and error attempts, they could decrypt parts of the secure communication, potentially accessing sensitive data like login credentials or personal information.

This vulnerability posed a significant risk to data confidentiality because SSL 3.0's flawed design allowed attackers to decipher encrypted information.

To address this security threat, security experts recommended disabling support for SSL 3.0 on servers and web browsers and switching to more secure protocols like TLS (Transport Layer Security). TLS provides enhanced security features and stronger encryption, making it much harder for attackers to intercept and decrypt sensitive information exchanged between users and servers.

As a result, many websites, browsers, and online services swiftly dis

Reverse Proxy and Load Balancer

Reverse Proxy: A reverse proxy serves as an intermediary between clients and servers, providing security, caching, and content optimization.

Load Balancer: A load balancer evenly distributes incoming traffic across multiple servers, ensuring efficient resource utilization, scalability, and high availability.

Feature	Reverse Proxy	Load Balancer
Client Interaction	Receives client requests and forwards to backend servers, masking server details from clients.	Directs incoming requests to multiple servers based on load-balancing algorithms.
Caching & Security	Can cache static content, enhance security by filtering and protecting against threats.	Focuses on evenly distributing traffic and ensuring high availability, less involved in caching or modifying content.
Health Monitoring	Limited health checks to ensure servers are operational for routing traffic.	Performs regular health checks to detect and redirect traffic from failed or unhealthy servers.

Working of Email

When Alice finishes composing her email to Bob and clicks "Send," her email client begins the sending process. Firstly, it performs a Domain Name System (DNS) lookup to locate the Mail Exchange (MX) records for Bob's domain, which specify the servers handling incoming emails for example.com.

Subsequently, Alice's email client establishes an SMTP (Simple Mail Transfer Protocol) connection with the Mail Exchange (MX) server responsible for example.com, transmitting the email along with sender details, the subject, and the message content.

Upon arrival at Bob's email server (MX server), the email is stored in Bob's mailbox for later access.

To read his emails, Bob accesses his email server through either the Internet Message Access Protocol (IMAP), allowing him to view emails directly on the server, or the Post Office Protocol version 3 (POP3), which downloads emails to his local device for viewing.

HTTP Status Codes

HTTP status codes are standardized responses provided by web servers to communicate the outcome of a client's request to access a web resource. These three-digit codes convey specific information about the success, failure, or the nature of the response during HTTP transactions. These codes are divided into several categories, each with its own range of codes representing different outcomes:

1xx Informational Response:

- 100 Continue: The server confirms the initial part of the request, allowing the client to continue sending the remainder.
- 101 Switching Protocols: The server is changing the protocol (e.g., HTTP to WebSocket) as requested by the client.

2xx Success:

- 200 OK: The server successfully processed the request and returns the requested content.
- 201 Created: The request has been fulfilled, resulting in the creation of a new resource.

3xx Redirection:

- 301 Moved Permanently: The requested resource has been permanently moved to a new URL.
- 302 Found: The requested resource has been temporarily moved to a different URL.

4xx Client Error:

- 400 Bad Request: The server cannot process the client's request due to invalid syntax or a malformed request.
- 401 Unauthorized: The client needs to authenticate itself before accessing the resource.
- 403 Forbidden: The server understands the request but refuses to authorize it.

5xx Server Error:

- 500 Internal Server Error: A generic error message indicating an issue on the server that prevented it from fulfilling the request.
- 502 Bad Gateway: The server, while acting as a gateway or proxy, received an invalid response from an upstream server.
- 503 Service Unavailable: The server is currently unavailable due to overload or maintenance.

Firewall

A firewall is a security mechanism, either hardware or software-based, that acts as a barrier between trusted internal networks and untrusted external networks (e.g., the internet). Its primary role is to monitor and control incoming and outgoing network traffic based on predefined security rules.

Types of Firewalls:

1. **Packet Filtering Firewall (Network Layer - Layer 3):**
   - Operates at the Network Layer (Layer 3) of the OSI model.
   - Examines packet headers (source/destination IP addresses, port numbers, protocol types) to allow/block packets.
   - Filters traffic quickly but lacks the ability to inspect packet contents.
2. **Stateful Inspection Firewall (Transport Layer - Layer 4):**
   - Operates at the Transport Layer (Layer 4).
   - Tracks active network connections' state to analyze traffic context.
   - Allows only legitimate traffic based on established connection information.
3. **Application Layer Firewall (Application Layer - Layer 7):**

- Operates at the Application Layer (Layer 7).
- Offers advanced filtering capabilities, examining packet content and application-specific data.
- Blocks specific application-layer protocols and provides granular control over applications and user activities.

4. **Proxy Firewall (Application Layer - Layer 7):**
   - Functions at the Application Layer as an intermediary between clients and servers.
   - Hides the actual client IP address from the server by acting as a data intermediary.
   - Enhances security and anonymity by obscuring client information from the server.
5. **Next-Generation Firewall (NGFW):**
   - Integrates traditional firewall features with advanced security functions.
   - Incorporates intrusion prevention, application control, deep packet inspection, and SSL decryption.
   - Operates across multiple OSI model layers, offering comprehensive and sophisticated network security capabilities.

TCP 3-Way Handshake

The TCP (Transmission Control Protocol) 3-way handshake is a fundamental process for establishing a reliable and stable connection between two devices over a network. It's the method by which TCP ensures both ends are ready to exchange data before initiating communication.

TCP 3-Way Handshake Steps:

SYN (Synchronize):

- The process begins with the client (initiating device) sending a TCP segment to the server (receiving device). This segment contains a SYN flag (Synchronize) set to 1 and an initial sequence number (ISN) to start the communication.

- The client requests to establish a connection by sending a packet with the SYN flag set and an initial sequence number (randomly chosen).

SYN-ACK (Synchronize-Acknowledge):

- Upon receiving the SYN segment, the server acknowledges the client's request by sending its own TCP segment. This segment also has the SYN flag set to 1 and an acknowledgment number (ACK) value equal to the client's ISN incremented by 1.
- Additionally, the server chooses its own ISN and sends it along with the ACK of the client's ISN.

ACK (Acknowledge):

- Finally, the client acknowledges the server's response by sending an acknowledgment back. The ACK packet contains the server's ISN incremented by 1, confirming that the server received the acknowledgment.

The termination of a TCP (Transmission Control Protocol) connection is a process known as the TCP connection termination or TCP teardown. It involves the orderly closing of an established connection between two devices.

TCP Connection Termination Process (4-Way Handshake):

1. **Initiation of Termination:**
    - Either the client or server initiates the termination by sending a TCP segment with the FIN (Finish) flag set, indicating the desire to close the connection.
2. **Acknowledgment of Termination Request:**
    - The receiving party acknowledges the termination request by sending an ACK (Acknowledgment) segment back to the initiator. At this point, the receiving side also sends its own FIN segment to start closing its side of the connection.
3. **Acknowledgment of Termination Completion:**
    - The initiator acknowledges the received FIN segment from the other side with an ACK segment. This acknowledgment indicates that it's ready to

terminate its side of the connection as well.

4. **Completion of Termination:**
    - Finally, the receiving side acknowledges the ACK sent by the initiator. Both sides have now acknowledged the termination request, and the connection is fully closed.

Subnetting

Subnetting is a networking technique used to divide a single, large network into smaller, more manageable sub-networks or subnets. It involves partitioning an IP network into several smaller sub-networks to improve performance, manage network traffic, and enhance security.

Advantages of Subnetting:

1. **Efficient Network Management:** Subnetting allows network administrators to organize and manage network resources more effectively by dividing a large network into smaller segments. This facilitates better control and monitoring of traffic flow within each subnet.
2. **Reduced Network Traffic:** By breaking down a large network into smaller subnets, broadcast traffic is confined within each subnet, preventing it from flooding the entire network. This helps reduce unnecessary network congestion and improves overall performance.
3. **Enhanced Security:** Subnetting enables the implementation of network security measures more effectively. Firewalls, access control lists (ACLs), and other security mechanisms can be applied at the subnet level, providing better protection against unauthorized access and potential security threats.

Disadvantages of Subnetting:

1. **Complexity in Planning:** Subnetting requires careful planning and design to allocate IP addresses effectively. Poor planning or mismanagement during subnetting can lead to IP address depletion or inefficient use of address space.
2. **Potential for Subnet Overhead:** When creating multiple subnets, there might be some overhead in managing and configuring additional routers, switches, or network devices required for the increased segmentation.

Default Subnet Masks:

Below is a table showing default subnet masks corresponding to different IP address classes:

Class	Default Subnet Mask	CIDR Notation
Class A	255.0.0.0	/8
Class B	255.255.0.0	/16
Class C	255.255.255.0	/24

These default subnet masks represent the default subnetting divisions for IP address classes A, B, and C. However, subnetting allows flexibility to further divide these classes into smaller subnets by using custom subnet masks, also known as Variable Length Subnet Masks (VLSM), allowing networks to be more efficiently utilized based on specific requirements.

Example 1

Subnet: 192.168.1.0/24

Binary Representation: 11111111 11111111 11111111 00000000

Decimal Representation of Binary: 255.255.255.0 (Default subnet mask for a Class C network)

Total Hosts: 2^(32-24) = 256

Active Hosts: Total Hosts - 2 = 254 (Subtracting network and broadcast addresses)

Network ID (First Address): 192.168.1.0

Broadcast ID (Last Address): 192.168.1.255 (Range from 192.168.1.0 to 192.168.1.255 includes 256 integers)

Example 2

Subnet: 192.168.1.16/28

Binary Representation: 11111111 11111111 11111111 11110000

Decimal Representation of Binary: 255.255.255.240

Total Hosts: 2^(32-28) = 16

Active Hosts: Total Hosts - 2 = 14 (Subtracting network and broadcast addresses)

Network ID (First Address): 192.168.1.16

Broadcast ID (Last Address): 192.168.1.31 (Range from 192.168.1.16 to 192.168.1.31 includes 16 integers)

Note: I highly recommend watching GATE Smashers for proper understanding of subnetting and the questions asked from it. No notes can help you understand it better than videos.

These notes cover the most prominent topics I encountered in interviews (particularly cyber security interviews). They don't cover the computer networks topic as a whole. The purpose of these notes is to help people who have a decent idea about computer networks to refresh their concepts or as a means for last minute interview preparation.

I hope you find these helpful and I wish you **Best of Luck** for your interviews.