**1. What is a Computer Network?**

* **Answer**: A computer network is a collection of interconnected devices, such as computers, servers, and networking hardware, that communicate with each other to share resources, such as files, internet access, and applications.
* **Example**: A home Wi-Fi network where multiple devices (laptops, smartphones, tablets) are connected to a single router to access the internet.

**2. What are the different types of networks?**

* **Answer**: The main types of networks are:
  + **LAN (Local Area Network)**: Covers a small geographic area, like a home, office, or building.
  + **WAN (Wide Area Network)**: Spans a large geographic area, often a country or continent. The Internet is the largest WAN.
  + **MAN (Metropolitan Area Network)**: Covers a city or a large campus.
  + **PAN (Personal Area Network)**: Used for connecting devices within the range of an individual person, typically within a range of a few meters.
* **Example**: A company’s internal network is an example of a LAN, whereas the internet is an example of a WAN.

**3. What is the OSI Model? Describe its layers.**

* **Answer**: The OSI (Open Systems Interconnection) Model is a conceptual framework used to understand network interactions in seven distinct layers:
  1. **Physical Layer**: Deals with the physical connection between devices and the transmission of binary data as electrical, optical, or radio signals.
  2. **Data Link Layer**: Ensures error-free data transfer between adjacent network nodes by framing data and controlling access to the medium.
  3. **Network Layer**: Handles packet forwarding, including routing through different routers.
  4. **Transport Layer**: Ensures end-to-end communication, error checking, and data flow control (e.g., TCP, UDP).
  5. **Session Layer**: Manages sessions or connections between applications.
  6. **Presentation Layer**: Translates data between the application layer and the network, encrypts and decrypts data, and compresses data.
  7. **Application Layer**: Provides network services directly to applications (e.g., HTTP, FTP, SMTP).
* **Example**: When you load a web page, the HTTP request operates at the Application Layer, while the transmission of data packets over the network involves the Physical, Data Link, and Network layers.

**4. What is an IP Address? Differentiate between IPv4 and IPv6.**

* **Answer**: An IP address is a unique identifier assigned to each device connected to a network, allowing devices to communicate with each other.
  + **IPv4**: Uses a 32-bit address format, allowing approximately 4.3 billion unique addresses (e.g., 192.168.1.1).
  + **IPv6**: Uses a 128-bit address format, providing a vastly larger number of addresses (about 3.4 x 10^38), intended to replace IPv4 due to address exhaustion (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
* **Example**: An IPv4 address looks like 192.168.1.1, while an IPv6 address looks like 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

**5. What is a MAC Address, and how is it different from an IP Address?**

* **Answer**: A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications at the Data Link Layer of a network. Unlike an IP address, which is assigned by the network and can change, a MAC address is hardware-specific and does not change.
* **Example**: A MAC address looks like 00:1A:2B:3C:4D:5E and is usually found on a device's network interface card (NIC).

**6. Explain the difference between TCP and UDP.**

* **Answer**: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are transport layer protocols.
  + **TCP**: Provides reliable, ordered, and error-checked delivery of data (e.g., used for web browsing, email). It establishes a connection before data is transferred.
  + **UDP**: Provides a faster, connectionless service with no guarantee of delivery, ordering, or error-checking (e.g., used for video streaming, online gaming).
* **Example**: Web browsers use TCP to ensure that all data is received correctly, while online games often use UDP to minimize latency.

**7. What is DNS, and how does it work?**

* **Answer**: DNS (Domain Name System) is a system that translates human-readable domain names (like [www.example.com](http://www.example.com)) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network.
* **Example**: When you type www.example.com in your browser, DNS servers resolve this domain to its IP address, allowing your browser to load the website.

**8. What is a subnet mask, and why is it used?**

* **Answer**: A subnet mask is used in IP networks to divide an IP address into two parts: the network part and the host part. It determines which portion of the IP address refers to the network and which refers to the host.
* **Example**: A common subnet mask for a Class C network is 255.255.255.0, indicating that the first three octets (24 bits) are the network portion, and the last octet (8 bits) is the host portion.

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

* **Answer**: A default gateway is a device (usually a router) that routes traffic from a local network to other networks, typically the internet. It serves as an access point or IP router that a networked computer uses to send information to a device in another network.
* **Example**: In a home network, the router is the default gateway that connects your local devices to the internet.

**10. What is NAT, and why is it used?**

* **Answer**: NAT (Network Address Translation) is a method used in routers to translate private (not globally unique) IP addresses into a single public IP address (and vice versa) to access the internet. It is used to conserve global IP address space and provide an extra layer of security by hiding internal IP addresses.
* **Example**: A home router assigns private IP addresses (e.g., 192.168.1.x) to devices in the network and translates these to the public IP address assigned by the ISP when accessing the internet.

**11. What are HTTP and HTTPS?**

* **Answer**:
  + **HTTP (Hypertext Transfer Protocol)**: A protocol used for transmitting hypertext (like web pages) over the internet. It is stateless and not encrypted, making it less secure.
  + **HTTPS (Hypertext Transfer Protocol Secure)**: An extension of HTTP that uses SSL/TLS to encrypt data between the web server and the client, providing a secure communication channel.
* **Example**: A website with a login page uses HTTPS to ensure that login credentials are securely transmitted.

**12. What is a firewall, and what are its types?**

* **Answer**: A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
  + **Types**:
    - **Packet-Filtering Firewalls**: Inspects packets and permits or denies them based on source and destination addresses, ports, or protocols.
    - **Stateful Inspection Firewalls**: Tracks the state of active connections and makes decisions based on the state and context of the traffic.
    - **Proxy Firewalls**: Acts as an intermediary for requests from clients seeking resources from other servers.
    - **Next-Generation Firewalls (NGFW)**: Provides deeper inspection capabilities by including features like application awareness, intrusion prevention, and advanced threat detection.
* **Example**: A firewall configured to block all traffic except for web and email traffic (HTTP, HTTPS, and SMTP) to secure a corporate network.

**13. Explain what VPN is and how it works.**

* **Answer**: A VPN (Virtual Private Network) extends a private network across a public network, allowing users to send and receive data as if their computing devices were directly connected to the private network. VPNs use tunneling protocols and encryption to secure data transmission.
* **Example**: Employees working remotely can use a VPN to securely access their company's internal network over the internet.

**14. What is ARP?**

* **Answer**: ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address on a local area network. When a device wants to communicate with another device on the same network, it uses ARP to find the physical address corresponding to the IP address.
* **Example**: If a computer wants to send a packet to another computer in the same network but only knows the IP address, it will use ARP to find out the MAC address.

**15. What is the difference between a hub, switch, and router?**

* **Answer**:
  + **Hub**: A basic networking device that connects multiple devices in a LAN. It broadcasts incoming traffic to all connected devices, regardless of the destination.
  + **Switch**: More intelligent than a hub, it forwards traffic only to the device(s) it is intended for, using MAC addresses to determine the correct destination.
  + **Router**: Connects multiple networks (e.g., LAN to WAN), directing data packets based on IP addresses. It also provides internet connectivity and can perform network address translation (NAT).
* **Example**: In a home network, a router connects to the ISP’s network and provides internet access to various devices through a switch or hub.

**16. What is a load balancer, and why is it used?**

* **Answer**: A load balancer is a device or software that distributes network or application traffic across multiple servers to ensure no single server becomes overwhelmed, improving responsiveness and availability.
* **Example**: A load balancer is used in a web application architecture to distribute incoming requests evenly among several web servers to maintain performance and reliability.

**17. What is network latency, and what factors can affect it?**

* **Answer**: Network latency is the time it takes for data to travel from the source to the destination across a network. It is usually measured in milliseconds (ms).
* **Factors affecting latency**:
  + **Distance**: The physical distance between devices increases latency.
  + **Network Congestion**: High traffic can lead to delays.
  + **Transmission Medium**: The type of cables or wireless signals used (e.g., fiber optics vs. copper).
  + **Network Devices**: The number and type of devices (routers, switches) data must pass through.
* **Example**: High latency in a video call can cause delays and reduce the quality of communication.

**18. What is network topology, and what are the different types?**

* **Answer**: Network topology refers to the arrangement of various elements (links, nodes, etc.) in a computer network. The main types are:
  + **Bus Topology**: All devices share a single communication line.
  + **Star Topology**: All devices connect to a central hub or switch.
  + **Ring Topology**: Devices are connected in a circular sequence.
  + **Mesh Topology**: Every device is connected to every other device.
  + **Tree Topology**: A combination of star and bus topologies, forming a hierarchical structure.
* **Example**: A star topology is common in home networks where all devices connect to a central router or switch.

**19. What is DHCP, and how does it work?**

* **Answer**: DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices in a network, allowing them to communicate efficiently.
* **Example**: When you connect a device to a Wi-Fi network, DHCP assigns an IP address to your device automatically without manual configuration.

**20. What is a VLAN, and why would you use it?**

* **Answer**: A VLAN (Virtual Local Area Network) is a subgroup within a network that combines devices into a single broadcast domain, regardless of their physical location. VLANs are used to segment a network into distinct groups to improve security and performance.
* **Example**: In an office, VLANs can be used to separate the finance department's devices from the HR department's devices for security and network management purposes.

**21. What is a Proxy Server, and how does it work?**

* **Answer**: A proxy server acts as an intermediary between a client and the internet. It can provide various functionalities like content filtering, security, privacy, and caching to improve speed.
* **Example**: A school network might use a proxy server to block access to specific websites and cache frequently accessed web pages to reduce bandwidth usage.