1. Difference between http:// and https://

HTTP and HTTPS are both protocols for communication but they are different in several ways and the main difference is security.

HTTP (Hypertext Transfer Protocol) is the basic protocol used to transfer data over the web. It does not encrypt the data, so information is sent in plain text, which makes it vulnerable to interception by attackers.

HTTPS (HTTP Secure) is the secure version of HTTP. It uses SSL/TLS encryption to encrypt the data being transferred between the client and server

This ensures:

Confidentiality: Data is encrypted.
Integrity: Data cannot be modified during transmission.
Authentication: Confirms the website is legitimate via SSL certificates.

2. What is an API Gateway?

An API Gateway is a server that acts as an entry point for all client requests to a set of backend services or microservices.

Key Functions of an API Gateway:

Request Routing: Forwards client requests to the appropriate backend service.
Authentication & Authorization: Validates tokens (like JWT) before allowing access.
Load Balancing: Distributes incoming traffic to multiple service instances.

3 What is SSL/TLS?

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols used to secure communication over a network—especially the internet.

For example, when you visit a website with https://, TLS ensures that the communication is private and protected from attackers.

How it works (Brief):

When you visit a website using https://, the browser initiates a TLS handshake.
The server sends its SSL/TLS certificate.
The client (browser) verifies it, and they agree on an encryption method.
A secure encrypted channel is established for communication

4. What is a Reverse Proxy?

A reverse proxy is a server that sits in front of backend servers and forwards client requests to those servers. Unlike a forward proxy, which works on behalf of clients, a reverse proxy works on behalf of servers.

Key Responsibilities of a Reverse Proxy:

Load Balancing: Distributes client requests across multiple backend servers.
Security: Hides internal server details and can filter malicious requests.
Caching: Stores frequently requested responses to improve performance.

Compression: Reduces the size of responses to improve speed.

5. What is a Load Balancer?

A Load Balancer is a system (software or hardware) that distributes incoming network traffic across multiple servers to ensure no single server is overwhelmed and that the application remains highly available, reliable, and scalable.

Key Functions of a Load Balancer:

Traffic Distribution: Balances traffic among servers using algorithms like:Round Robin,Least Connections,IP Hash

High Availability: Redirects traffic if a server goes down, ensuring uptime.

SSL Termination: Can decrypt SSL/TLS traffic before passing it to backend servers.

Scalability: Helps handle more users by spreading the load across servers.

6. What is ARP (Address Resolution Protocol)?

ARP (Address Resolution Protocol) is a network protocol used to map an IP address to a MAC address in a local area network (LAN).

When a device wants to communicate with another device on the same network, it knows the destination IP address but needs the corresponding MAC address to send the Ethernet frame. ARP is used to resolve this.

How ARP Works (Briefly):

The sender broadcasts an ARP request:

"Who has IP 192.168.1.10? Tell me your MAC address."

The device with that IP replies with an ARP response:

"I have IP 192.168.1.10, and my MAC address is 00:1A:2B:3C:4D:5E."

The sender stores this mapping in its ARP cache for future use

7. What is the difference between Horizontal and Vertical Scaling?

Horizontal Scaling and Vertical Scaling are two strategies used to improve a system's performance and handle increased load.

1. Horizontal Scaling (Scale Out):

Involves adding more machines or instances to your system

You distribute the load across multiple servers.

Adding more application servers behind a load balancer.

2. Vertical Scaling (Scale Up):

Involves increasing the resources (CPU, RAM, Storage) of an existing machine.

You make a single server more powerful.

Upgrading from 8 GB RAM to 32 GB RAM on a server.

8. What is caching? how does a website is cached ?

Caching is the process of storing copies of data in a temporary storage location so future requests for that data can be served faster without recomputing or refetching it from the original source.

How a Website is Cached?

User visits a site.

Browser checks its cache: if a resource is fresh (based on headers), it uses the cached version.

If not cached or expired, it requests the server/CDN.

Server/CDN(Content Delivery Network) might serve cached content or regenerate and cache it for next time.

Benefits of Caching:

Faster load times
Reduced server load
Better user experience
Cost-efficient for high-traffic websites

9. What is VIP (Virtual IP) in Computer Networks?

A Virtual IP (VIP) is an IP address that doesn’t belong to a specific physical interface, but is instead used by one or more devices for redundancy, load balancing, or failover purposes.

Load Balancing: In web servers, a VIP is used by a load balancer to represent a pool of backend servers.

High Availability (HA): VIPs are used so that if one server fails, another can take over the VIP and continue serving clients.

or,

How VIP Works:

A cluster of servers shares one VIP.

Only one server actively uses the VIP at a time.

If the active server fails, the VIP is quickly reassigned to a standby server.

Clients continue to connect to the same IP, unaware of any changes in the backend.

10. REST API vs HTTP API?

While both REST API and HTTP API use the HTTP protocol, they are not the same. A REST API is a type of HTTP API, but not all HTTP APIs are RESTful.

1. HTTP API:

Generic term for any API that uses HTTP methods (GET, POST, PUT, DELETE).

Commonly used for building lightweight or custom-designed web services.

2. REST API (Representational State Transfer):

A REST API is a specific type of HTTP API that follows REST (Representational State Transfer) principles, such as statelessness, resource-based URLs, and using standard HTTP methods in a consistent way.

A specific architectural style for designing networked applications.

Built on top of HTTP with strict rules and principles.

```
eg. GET /users – Fetch list of users
    POST /users – Create a new user
    PUT /users/1 – Update user with ID 1
    DELETE /users/1 – Delete user with ID 1
```

/users is the resource, and we perform different actions using HTTP methods, not by changing the URL name.

11. What is a Container in Computer Networks?

A container is a lightweight, portable, and isolated runtime environment that packages an application with all its dependencies, libraries, and configurations.

This means the application can run consistently across different environments—whether it's on a developer’s laptop, a testing server, or a production machine.

Unlike virtual machines, containers share the host OS kernel, making them faster and more resource-efficient. Tools like Docker are commonly used to create and manage containers.

Containers help in achieving DevOps goals like continuous integration and deployment by ensuring the software runs the same everywhere.”

12. Containerization vs Virtualization?

Both Containerization and virtualization run multiple isolated environments on a single physical machine, but they differ in architecture and efficiency.

Virtualization uses a hypervisor to create Virtual Machines (VMs), each virtual machinee(VM) has its own full guest operating system, making them heavier and slower to boot.

In contrast, containerization shares the host OS kernel with isolated applications present in lightweight containers, which make it faster, more efficient, and ideal for microservices and CI/CD workflows. Containers are managed by tools like Docker and Kubernetes,

Hypervisors:

A hypervisor is a software layer (also called a Virtual Machine Monitor - VMM) that creates and manages virtual machines (VMs) by abstracting and sharing the physical hardware of a host machine.

It allows multiple operating systems to run simultaneously and independently on the same physical hardware.

Example: Running Ubuntu and Windows side by side using a hypervisor.

13. Performance vs Scalability ?

Performance:

Performance refers to how efficiently a system handles its current workload — focusing on speed, response time, throughput, and resource utilization

Example: how fast a webpage loads or how many requests per second a server can handle under current conditions.

Scalability:

scalability is about how well a system can grow and maintain performance as the workload increases — such as more users, data, or transactions.

Scalability is achieved either by vertical scaling (adding more power to existing machines) or horizontal scaling (adding more machines to distribute the load)

Example: Can your web app handle 10x more users if you add more servers?

14. Latency vs Throughput?

Latency and throughput are two key metrics used to evaluate system or network performance, but they measure different aspect

Latency refers to the delay between sending a request and receiving a response, often measured in milliseconds — it’s like the reaction time of a system.

For example, if you click a link and the server responds in 100ms, the latency is 100ms

Throughput measures the amount of data or number of requests a system can process in a given time, such as requests per second or Mbps.

It's about capacity — for instance, a server that handles 10,000 requests per second has high throughput.

While low latency gives fast responses, high throughput ensures the system can handle large volumes

15. 2G vs 3G vs 4G vs 5G?

These are generations of mobile network technologies, each improving over the previous in terms of speed, latency, capacity, and capabilities.

2G: First digital network - supported calls and SMS.

3G: Introduced mobile internet, video calls, and faster downloads.

4G: Made HD streaming, gaming, and fast browsing possible.

5G: Enables real-time applications like autonomous cars, IoT, and smart cities with massive speed and ultra-low latency.

16. How does a VPN work?

A VPN (Virtual Private Network) creates a secure, encrypted tunnel between your device and a remote VPN server, ensuring that your online activity remains private and protected.

🔧 How It Works (Step-by-Step):

When we connect to a VPN, our internet traffic is encrypted by the VPN client on our device and sent to the VPN server, which then decrypts it and forwards it to the intended website using its own IP address — effectively hiding your real IP.

The response from the website follows the same path in reverse: it goes back to the VPN server, gets encrypted, and is finally decrypted on your device, making the entire session secure from hackers or surveillance.

This not only protects your data on public Wi-Fi but also allows anonymous browsing and access to geo-restricted content.

17. Gateway vs Router?

A router and a gateway are both networking devices, but they serve different roles.

A router connects multiple devices within the same type of network and directs data packets along the best path, commonly used in homes and offices to route traffic from internal devices to the internet.

For example, your Wi-Fi router connects your phone, laptop, and TV to each other and to the web.

A gateway connects two different networks that may use different communication protocols, acting as a protocol translator.

It enables communication between systems that otherwise couldn’t understand each other, like connecting a corporate network to a cloud service or converting analog phone signals to digital VoIP.

A router manages traffic within or between similar networks, while a gateway bridges different networks or technologies, often operating across multiple OSI layers.

18. NIC vs MAC Address?

1. NIC (Network Interface Card):

A hardware component that allows a device (computer, printer, etc.) to connect to a network.

It can be wired (Ethernet) or wireless (Wi-Fi).

It operates on the Data Link Layer (Layer 2) and Physical Layer (Layer 1) of the OSI model.

Every NIC has a unique MAC address.

Example:

The LAN port on your laptop or the Wi-Fi chip is a NIC.

2. MAC Address (Media Access Control Address):

A unique identifier assigned to a NIC by the manufacturer.

It's a 12-digit hexadecimal number (e.g., 00:1A:2B:3C:4D:5E).

It helps in identifying the device on a local network (LAN).

Used by switches to forward data to the correct device.

Example:

If you check your phone's Wi-Fi settings, you'll find its MAC address, linked to its NIC

MAC address is the unique ID assigned to that hardware for device-level identification on a network.

19. Public vs Private IP Address?

IP addresses are used to uniquely identify devices on a network and are categorized into public and private based on their scope of access.

A public IP address is assigned by your Internet Service Provider (ISP) and is globally unique, allowing devices or networks to be accessible over the internet—typically used by routers, web servers, or any service that needs internet access.

For example, 49.207.192.10 is a public IP visible on sites like whatismyip.com.

A private IP address is used within local networks (like your home or office) and is not routable on the internet. Devices such as laptops, phones, or printers are assigned private IPs like 192.168.1.10 by a router using DHCP.

the public IP connects your network to the outside world, while private IPs help internal devices communicate securely within the local network.

20. What is Multiplexing in Networking?

Multiplexing is the process of combining multiple data signals into one for efficient transmission over a single medium — saving time, bandwidth, and cost.

To send multiple streams of data simultaneously over a single communication channel without interference.

Bandwidth refers to the maximum amount of data that can be transmitted over a network connection in a given amount of time, typically measured in bits per second (bps)

21. Modem vs Router?

📡 1. Modem (Modulator-Demodulator):

Connects your home/office network to the Internet via your ISP.
Converts digital signals ↔ analog signals (over phone lines, cable, or fiber).
Has one public IP address assigned by the ISP.
Can only connect to one device directly (unless combined with a router).

📶 2. Router:

Distributes the internet from the modem to multiple devices (wired or wireless).
Assigns private IP addresses to devices on the local network.
Manages traffic, provides firewall, and enables Wi-Fi.
Often includes NAT (Network Address Translation) to allow multiple devices to share one public IP.
Example:
Your Wi-Fi router at home that connects your phone, laptop, and smart TV.

A modem brings the internet into your network from the ISP, while a router distributes it to multiple devices, often wirelessly.

22. How does Bluetooth work?

Bluetooth is a short-range wireless communication technology used to connect devices over a secure, low-power radio frequency.

How It Works:

Bluetooth uses radio waves in the 2.4 GHz range to send data wirelessly.
Devices first pair by sharing a code to create a secure connection.
Once connected, they can communicate directly without internet or cables.
It uses low power and short range (usually up to 10 meters).
It can connect one device to many others in a small network (called a piconet).

23. How Does a Hotspot Work?

A hotspot is a feature that allows a device (like a smartphone or router) to share its internet connection with other nearby devices using Wi-Fi.

How It Works:

A device (e.g. smartphone) connects to the internet using mobile data (4G/5G).
It creates a Wi-Fi signal like a mini router.
Other devices (laptop, tablet) connect to that Wi-Fi signal.
The internet from the mobile data is shared with connected devices.

A hotspot turns a device into a Wi-Fi access point, allowing it to share its internet connection with other devices wirelessly.

24. How Does Email Work?

Email is a way to send and receive messages electronically over the Internet using a set of protocols.

🔧 How It Works (Simplified):

Writing & Sending:
You write an email using an email client (like Gmail or Outlook) and hit send.

Sending Server (SMTP):
Your email client sends the message to the SMTP server (Simple Mail Transfer Protocol), which handles outgoing mail.

Routing:
The SMTP server looks up the recipient's email server using DNS (Domain Name System).

Receiving Server (POP3/IMAP):
The recipient's email server receives and stores the message.
POP3 downloads emails to the recipient's device.
IMAP syncs emails between the server and device.

Reading:
The recipient uses their email client to retrieve and read the message.

25. How Does File Transfer Work?

File transfer is the process of sending data files from one device to another over a network.

🔧 How It Works (Simplified):

Initiation:
The sender selects the file to send and starts the transfer using a protocol or app (like FTP, HTTP, or peer-to-peer apps).

Breaking into Packets:
The file is split into small data packets to be sent over the network efficiently.

Sending Packets:
Packets travel from the sender to the receiver through routers and switches on the network.

Receiving & Reassembling:
The receiver collects all packets and reassembles them into the original file.

Acknowledgment & Error Checking:
The receiver sends acknowledgments to confirm receipt and requests retransmission if packets are lost or corrupted.

26. How Does an ATM Work?

An ATM (Automated Teller Machine) allows bank customers to perform financial transactions like cash withdrawals, deposits, and balance inquiries without visiting a bank branch.

🔧 How It Works (Simplified):

User Authentication:
You insert your debit/credit card and enter your PIN to verify your identity.

Transaction Request:
You choose a transaction type (e.g., withdraw cash).

Communication with Bank:
The ATM sends your request and credentials to the bank’s central server via a secure network.

Verification & Approval:
The bank verifies your account balance and PIN, then sends back an approval or denial.

Cash Dispensing / Service Execution:
If approved, the ATM dispenses cash or completes the requested service.

Transaction Logging:
The transaction is recorded both in the ATM and the bank’s system for accountability.

27. How Do Packets Travel in a Network?

Data sent over a network is broken into small units called packets, which travel from the source to the destination through various devices like routers and switches.

🔧 How Packets Travel (Simplified Steps):

Data is Broken into Packets:
A large message (e.g. a file or webpage) is divided into smaller packets, each containing:

Part of the data
A header (source/destination IP, sequence number, etc.)

Packets Enter the Network:
The sender’s device sends packets to the local router or gateway.

Routing Through the Internet:

Routers use the destination IP address to decide where to send each packet next.

Packets may take different paths to reach the destination (best path based on speed, load, or cost).

Arrival and Reassembly:

At the destination, packets are collected and reassembled in order using their sequence numbers.

Missing or corrupted packets are requested again using protocols like TCP.

Acknowledgment (if TCP):

The receiver sends back an ACK (Acknowledgment) to confirm successful delivery.