0.what Devops do?

1.OSI

2.layers of OSI

3.TCP

4.IP Protocol,Public vs Private IP

5.UDP,ICMP,ARP

6.DNS Server

7.HTTP/HTTPS

8.FTP

9.SMTP

10.Ports

11.IP address ,MAC Address

12.Switches,bridge

13.scalability(scale up and down) vs elasticity

0.**what Devops do?**

DevOps is a software development methodology that combines and automates the work of software development and IT operations teams to accelerate the delivery of higher-quality applications and services

.The term "DevOps" is a combination of "development" and "operations," reflecting its goal of unifying these traditionally separate roles.

1.**OSI:**The OSI (Open Systems Interconnection) Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the International Organization for Standardization (ISO). The OSI Model consists of 7 layers and each layer has specific functions and responsibilities.

2.**Layers:**

Physical Layer: The lowest layer of the OSI reference model is the Physical Layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Common physical layer devices are Hub, Repeater, Modem, and Cables.

Data Link Layer: The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame. Switches and Bridges are common Data Link Layer devices.

Network Layer: network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet. Network layer is implemented by networking devices such as routers and switches.

Transport Layer: The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as Segments. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

Session Layer: Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Presentation Layer: The presentation layer is also called the Translation layer. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are JPEG, MPEG, GIF, TLS/SSL, etc.

Application Layer: At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.

3.**TCP** : TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

4.**IP**

Here, IP stands for **internet protocol**. It is a protocol defined in the TCP/IP model used for sending the packets from source to destination. The main task of IP is to deliver the packets from source to the destination based on the IP addresses available in the packet headers. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source and destination information.

An IP protocol provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP and UDP/IP, so internet protocol is also known as TCP/IP or UDP/IP.

Types of IP addresses

IPv4 addresses are divided into two categories:

- **Public address:** The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet.

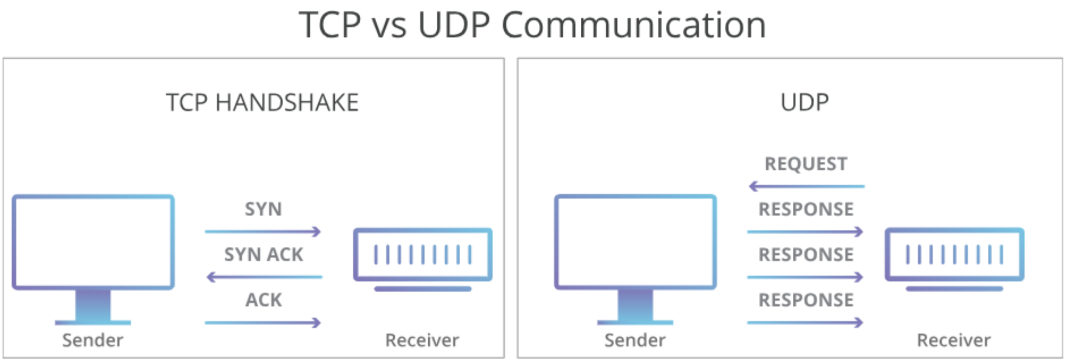
- **Private address:** A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address.

5.**UDP**

The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred. This allows data to be transferred very quickly, but it can also cause packets to become lost in transit — and create opportunities for exploitation in the form of DDoS attacks.

Like all networking protocols, UDP is a standardized method for transferring data between two computers in a network. Compared to other protocols, UDP accomplishes this process in a simple fashion: it sends packets (units of data transmission) directly to a target computer, without establishing a connection first, indicating the order of said packets, or checking whether they arrived as intended. (UDP packets are referred to as ‘datagrams’.)

TCP vs. UDP



UDP is faster but less reliable than TCP, another common transport protocol. In a TCP communication, the two computers begin by establishing a connection via an automated process called a ‘handshake.’ Only once this handshake has been completed will one computer actually transfer data packets to the other.

UDP communications do not go through this process. Instead, one computer can simply begin sending data to the other:

In addition, TCP communications indicate the order in which data packets should be received and confirm that packets arrive as intended. If a packet does not arrive — e.g. due to congestion in intermediary networks — TCP requires that it be re-sent. UDP communications do not include any of this functionality.

These differences create some advantages. Because UDP does not require a ‘handshake’ or check whether data arrives properly, it is able to transfer data much faster than TCP.

However, this speed creates tradeoffs. If a UDP datagram is lost in transit, it will not be re-sent. As a result, applications that use UDP must be able to tolerate errors, loss, and duplication.

(Technically, such packet loss is less a flaw in UDP than a consequence of how the Internet is built. Most network routers do not perform packet ordering and arrival confirmation by design, because doing so would require an unfeasible amount of additional memory. TCP is a way of filling this gap when an application requires it.)

ICMP

ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.

Since the IP protocol lacks an error-reporting or error-correcting mechanism, information is communicated via a message. For instance, when a message is sent to its intended recipient, it may be intercepted along the route from the sender. The sender may believe that the communication has reached its destination if no one reports the problem. If a middleman reports the mistake, ICMP helps in notifying the sender about the issue.

Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility.

ARP

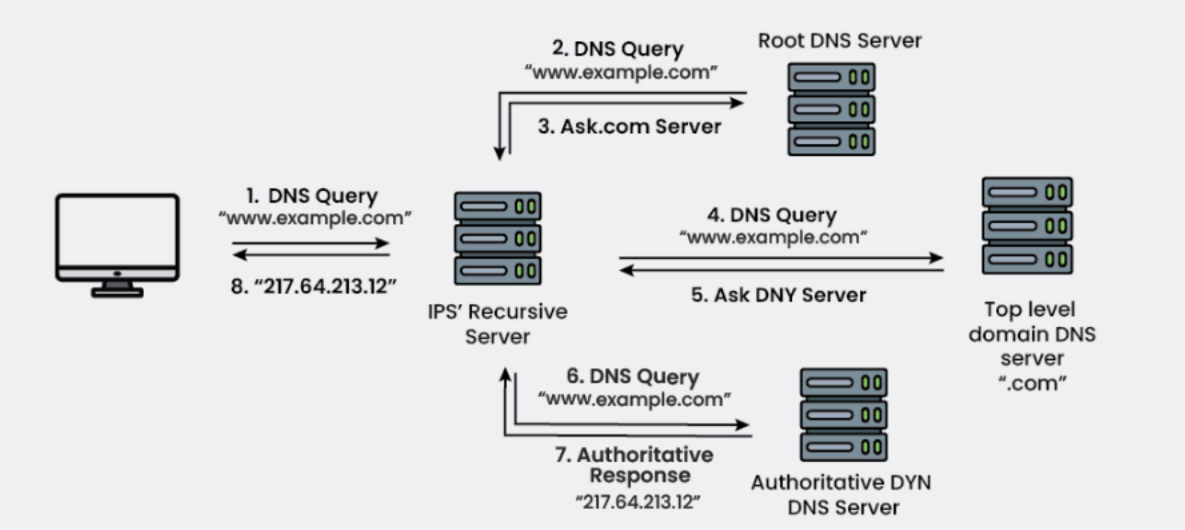
ARP stands for **Address Resolution Protocol**, which is used to find the MAC address of the device from its known IP address. This means, the source device already knows the IP address but not the MAC address of the destination device. The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address. So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.

Suppose two devices (device A and device B) want to communicate with each other. The device A already knows the IP address of the Device B. But in order to communicate with the device B, device A still needs the MAC address of the device B. The **IP address** is used to locate a device on a local area network and the **MAC address** is used to identify the actual device. The device A first look at its internal list known as ARP cache (table) to check if the IP address of the device B already consists of its MAC address or not. If the ARP table consists of the MAC address of the device B, then device A simply use that MAC address and start communication.

If the table does not consist of the MAC address of device B, then device A sends an ARP broadcast message on the network to know which device has that specific IP address and ask for the MAC address of that particular device. Then the device that has matching IP address to the source address sends an ARP response message that consists of the MAC address of the device B. When device A obtains the MAC address of the device B, it will store the information in the ARP cache (table). The ARP cache is used to make the network more efficient. It stores the IP address of the device along with its MAC address. The stored information is used when device A wants to communicate with device B on a network, and it does not need to broadcast a message on the network again. It will simply check the ARP cache for the entries and then use it for communication.

DNS server

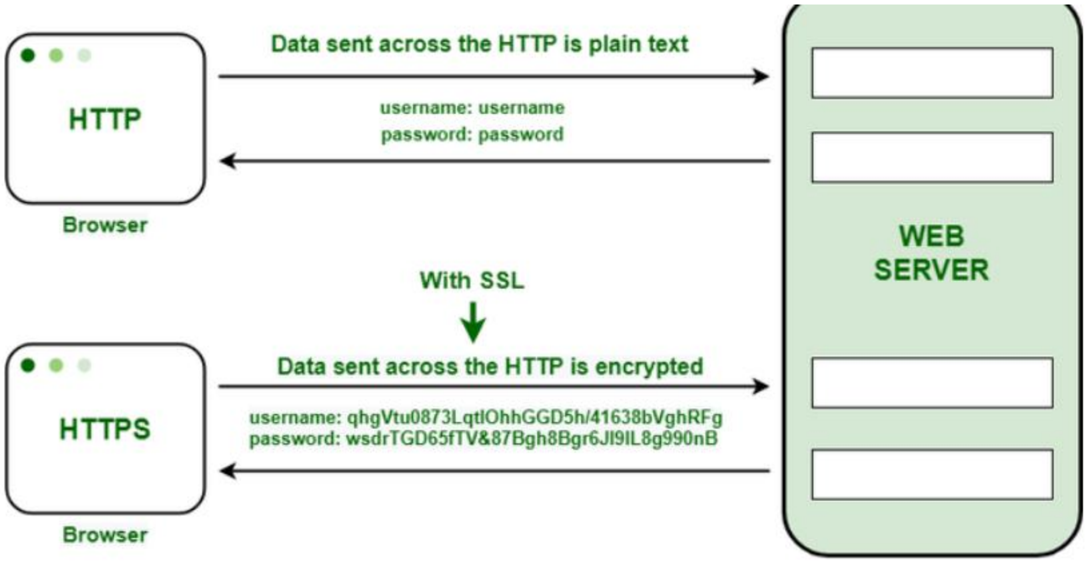
The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as ‘google.com’ or ‘nytimes.com’ into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with origin servers or CDN edge servers to access website information. This all happens thanks to DNS servers: machines dedicated to answering DNS queries.



HTTP: HTTP (Hypertext Transfer Protocol) is a fundamental protocol of the Internet, enabling the transfer of data between a client and a server. It is the foundation of data communication for the World Wide Web.
HTTP provides a standard between a web browser and a web server to establish communication. It is a set of rules for transferring data from one computer to another.

HTTPS: Hypertext Transfer Protocol Secure is a protocol that is used to communicate between the user browser and the website. It also helps in the transfer of data. It is the secure variant of HTTP.

HTTPS establishes the communication between the browser and the web server. It uses the **Secure Socket Layer** (SSL) and **Transport Layer Security** (TLS) protocol for establishing communication. The new version of SSL is **TLS(Transport Layer Security)**.
HTTPS uses the conventional HTTP protocol and adds a layer of SSL/TLS over it. The workflow of HTTP and HTTPS remains the same, the browsers and servers still communicate with each other using the HTTP protocol. However, this is done over a secure SSL connection. The SSL connection is responsible for the encryption and decryption of the data that is being exchanged to ensure data safety.


HTTP
Browser
Data sent across the HTTP is plain text
username: username
password: password
WEB SERVER
With SSL
HTTPS
Browser
Data sent across the HTTP is encrypted
username: qhgVtu0873LqtlOhhGGD5h/41638bVghRFg
password: wsdrTGD65fTV&87Bgh8Bgr6JI9IL8g990nB

SMTP

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is an always-on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection through port 25. After successfully establishing a TCP connection the client process sends the mail instantly.

Port: A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Ports allow computers to easily differentiate between different kinds of traffic: emails go to a different port than webpages, for instance, even though both reach a computer over the same Internet connection.

Suppose Bob transfers an MP3 audio recording to Alice using the File Transfer Protocol (FTP). If Alice's computer passed the MP3 file data to Alice's email application, the email application would not know how to interpret it. But because Bob's file transfer uses the port designated for FTP (port 21), Alice's computer is able to receive and store the file.

Meanwhile, Alice's computer can simultaneously load HTTP webpages using port 80, even though both the webpage files and the MP3 sound file flow to Alice's computer over the same WiFi connection.

IP and MAC address

MAC addresses are hardware identifiers, while IP addresses represent network locations. Together, they ensure proper data routing on the internet.
The main difference between MAC and IP address is that MAC Address is used to ensure the physical address of the computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identifies the connection of the network with that device takes part in a network.

Switch

Switches may operate at one or more layers of the OSI model. They may operate in the data link layer and network layer; a device that operates simultaneously at more than one of these layers is known as a *multilayer switch*.

A Switch can check the errors before forwarding the data, which makes it more efficient and improves its performance. A switch is the better version of a hub. It is a multi-port bridge device.

Bridge

A bridge operates at the data link layer of the OSI model. It can read only the outmost hardware address of the packet but cannot read the IP address. It reads the outmost section of the data packet to tell where the message is going. It reduces the traffic on other network segments. It does not send all the packets. So, a bridge can be programmed to reject packets from a particular network.

Scalability refers to a system's ability to handle increasing workloads by adding resources. It ensures that a system can maintain its performance as demand grows, allowing businesses to expand operations without experiencing performance degradation or downtime[1]. Scalability is typically used in environments where the workload increases predictably and requires a persistent deployment of resources[2].

Elasticity

Elasticity refers to the ability of a system to dynamically adjust its resource allocation in response to changing demands. This includes automatically scaling resources up or down based on factors like workload fluctuations, user demand, or performance requirements.

Types of Scalability

1. **Vertical Scalability (Scale-up)**: Increasing the power of existing resources in an upward direction.
2. **Horizontal Scalability (Scale-out)**: Adding more resources in a horizontal row.
3. **Diagonal Scalability**: A combination of both vertical and horizontal scalability

- **Resource Allocation**: Scalability involves adding or removing resources manually, while elasticity automatically scales resources based on demand[2].
- **Timing**: Scalability usually occurs reactively, whereas elasticity scales resources dynamically in real-time[2].
- **Management**: Scalability typically requires human intervention, while elasticity minimizes manual involvement through automation[2].
- **Flexibility**: Scalability offers flexibility in scaling but may not be instantaneous, whereas elasticity provides instant and automated resource adjustments[2].
- **Use Cases**: Scalability is commonly used in systems with predictable workload patterns, while elasticity is ideal for applications with highly variable workloads[2].

Load Balancer: A **load balancer** is a networking device or software application that distributes incoming traffic across multiple servers to ensure high availability, efficient utilization of resources, and improved performance. It acts as a "traffic cop" sitting in front of your servers, routing client requests across all servers to prevent any single server from being overwhelmed.