IP Addresses: IP Addresses are numerical labels assigned to devices on a computer network. They serve as unique identifiers, enabling communication between devices. IP addresses allow data to be sent and received over the internet.

OSI Layers:

1) Physical Layer: The lowest layer, it deals with the actual transmission of raw binary data over physical media like cables.
2) Data Link Layer: This layer frames data into packets, adds MAC addresses, and ensures error-free transmission within a local network.
3) Network Layer: Responsible for routing packets across different networks using IP addresses. It determines the optimal path for data transmission, handles addressing, and manages network congestion.
4) Transport Layer: Manages end-to-end communication between hosts, ensuring reliable data delivery and error detection/correction. It divides data into segments, establishes connections, and manages flow control and congestion.
5) Session Layer: Establishes and manages sessions between applications for synchronized communication. It handles session establishment, maintenance, and termination, as well as synchronization and checkpointing.
6) Presentation Layer: Translates data formats between applications by handling data encryption, compression, and formatting. It deals with aspects like character encoding and data representation.
7) Application Layer: The topmost layer, it provides services directly to users. It encompasses various protocols and applications like web browsers, email clients, file transfer protocols, and virtual terminal emulations.

Classful IP Addressing: In classful IP addressing, the IP address space was divided into five classes: A, B, C, D, and E. Each class had a specific range of IP addresses.

1) Class A:
   Network ID range: 1.0.0.0 to 126.0.0.0
   Subnet mask: 255.0.0.0
   Host ID range: 1.0.0.1 to 126.255.255.254
2) Class B:
   Network ID range: 128.0.0.0 to 191.255.0.0
   Subnet mask: 255.255.0.0
   Host ID range: 128.0.0.1 to 191.255.255.254
3) Class C:
   Network ID range: 192.0.0.0 to 223.255.255.0
   Subnet mask: 255.255.255.0
   Host ID range: 192.0.0.1 to 223.255.255.254
4) Class D:
   Network ID range: 224.0.0.0 to 239.255.255.255
5) Class E:
   Network ID range: 240.0.0.0 to 255.255.255.255

IPv4 and IPv6 IP Addressing: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are two different versions of the Internet Protocol that are used to assign unique addresses to devices on a network.

IPv4: IPv4 addresses are 32-bit numbers and it provides a total of approximately 4.3 billion unique addresses (2^{32}). They are divided in 4 sections with each of 8 bits separated by a dot. Ex. “123.123.123.123”.

IPv6: IPv6 addresses are 128-bit numbers and it provides approximately about 340 undecillion unique addresses (2^{128}). They are divided into 8 sections with each of 16 bits separated by colons and they are represented in hexadecimal. Ex. “cdef:cdef:cdef:cdef:cdef:cdef:cdef:cdef”.

Why IPv6 addresses are being used instead of IPv4 addresses ?

The adoption of IPv6 addresses the limitations of IPv4 providing only a total of 4.3 billion (2^{32}) addresses(running out of IPv4 addresses), whereas IPv6 provides a total of 340 undecillion (2^{128}) ensuring address availability. Also, IPv6 supports new technologies and enhances security.

Explain ports and what are commonly used ports ?

Ports are numbered endpoints within a computer network that enable communication between devices. They allow multiple applications or services to share a single IP address by assigning them unique port numbers. Ports are categorized as either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) and are associated with specific protocols or services.

Ports:-

20:FTP, 22:SSH, 25:SMTP, 53:DNS, 80:HTTP

Static IP Address vs Dynamic IP Address

Static IP: A static IP address is manually assigned to a device and remains constant over time. It is typically configured by the network administrator or internet service provider or user.

Dynamic IP: A dynamic IP address is automatically assigned to a device by a DHCP (Dynamic Host Configuration Protocol) server and it changes every time the device connects to a network.

What are Load Balancer ? What are the different type of Load Balancers

Load balancers are devices or software components that distribute incoming network traffic across multiple servers or resources in order to optimize resource utilization, improve scalability, and ensure high availability and reliability of applications or services.

Advantages: Maximise resource utilisation, high availability, high reliability and scalability.

Types of Load Balancers (based on where they are used):

1) Application Load Balancer: Works at application layer and deals with HTTP and HTTPS.
2) Networks Load Balancer: Works at transport layer and deals with TCP and UDP.
3) Global Server Load Balancer: `Don't Know!`

Types of Load Balancer (based on the configuration):

1) Hardware Load Balancer: Dedicated device of load balancing.
2) Software Load Balancer: Application for load balancing.

   Ex. Nginx, Avi Vantage Software Load Balancer, Kemp LoadMaster, Barracuda Load Balancer ADC.

HTTP Status Codes: 200, 301, 400, 401, 403, 404, 405, 500, 501, 502 503, 504.

HTTP Status Codes:

200: OK, 301: Moved Permanently, 400: Bad Request,

401: Unauthorised response, 403: Forbidden Response,

404: Request Not Found, 405: Method Not Allowed,

500: Internal Server Error, 501: Not Implemented,

502: Bad Gateway, 503: Service Unavailable,

504: Gateway Timeout, 504: HTTP Version Not Supported.

Difference between Access Log and Error Log.

The Access Log and Error Log are both logs of web-servers and are used for maintenance of the servers.

Access Log: Access Log contains information about requests coming into the server.

Error Log: Error Log contains information about errors the webserver encounters while processing incoming requests.

Difference between Vertical Scaling and Horizontal Scaling.

Vertical Scaling: Vertical Scaling also known as Scaling-up refers to improving the performance by adding resources to existing hardware in the system.

Horizontal Scaling: Horizontal Scaling also known as Scaling-out refers to improving performance by adding another server to the system with is similar to the existing server.

Difference between Physical Server, Virtual Machine, Cloud VM and Docker.

Physical Server: A physical server refers to a dedicated hardware unit that typically includes components such as processors, memory, storage, and networking capabilities, providing computing resources for hosting and running applications.

Virtual Machine: A virtual machine is a software emulation of a computer system that allows multiple operating systems to run on a single physical machine. It provides isolated environments with their own virtualized hardware.

Cloud Virtual Machine: A cloud virtual machine (VM) is a virtualized computing instance that runs on a cloud service provider's infrastructure. It allows users to access and manage virtualized resources remotely over the internet.

Docker: Docker is an open-source platform that enables software to be packaged into lightweight, self-contained containers. These containers provide an isolated and consistent environment for applications to run.

Difference between JAR, WAR, EAR.

JAR: JAR stands for Java Archives. JAR file has Java class files, related metadata, and resources combined into a single file to execute a Java application.

WAR: WAR stands for Web Application Resource. WAR file contains files such as a servlet, JSP, HTML, JavaScript etc.

EAR: EAR stands for Enterprise Application Archive. EAR is a Java Enterprise Edition file that packs one or more modules into a single archive to deploy them on to an application server.

Difference between Application Server and Web Server.

Application Server: An Application Server hosts and executes application and does server-side processing and database access for clients.

Web Server: A Web Server is responsible for handling HTTP requests and delivering static web content to clients. They serve web pages, files and media content to web browsers.

Difference between Vagrant and Virtual Box.

Vagrant: Vagrant is a tool for managing and provisioning virtual environments. It acts as an abstraction layer on top of virtualization software like VirtualBox, allowing you to define and configure virtual environments using code.

Virtual Box: Virtual Box is a virtualization platform that allows you to create and run virtual machines (VMs) on your local system. It provides the foundation for running multiple operating systems simultaneously.