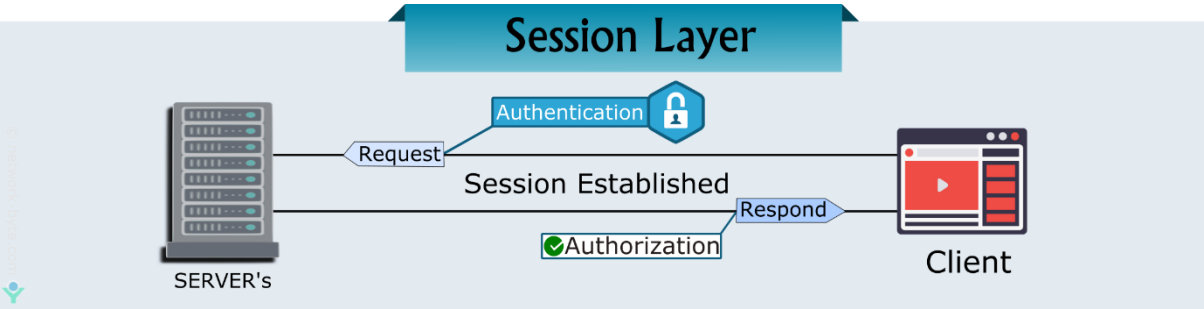
1.OSI (Open Systems Interconnection)

- **Application Layer:** Applications create the data.
- **Presentation Layer:** Data is formatted and encrypted.
- **Session Layer:** Connections are established and managed.
- **Transport Layer:** Data is broken into segments for reliable delivery.
- **Network Layer**: Segments are packaged into packets and routed.
- **Data Link Layer:** Packets are framed and sent to the next device.
- **Physical Layer:** Frames are converted into bits and transmitted physically.

SESSION LAYER

Session layer is used to establish connection between devices.

Session layer ensures that data is properly synchronized, organized, and managed during communication between two systems.



1) Session establishment
   The session layer is responsible for initiating, establishing, and maintaining a session between two communicating devices or applications. It provides mechanisms to ensure that the session is active and ready for data exchange.
   Authentication
   Authorization

2) Dialog Control
   The session layer provides full-duplex, half-duplex, or simplex communication between devices.

3) Synchronization
   The session layer provides synchronization services to ensure that the communication between devices is consistent. It can insert checkpoints into the data stream, allowing the communication to resume from the last checkpoint in case of a failure or interruption.

   Checkpoints: If an error occurs, data transfer can resume from the last checkpoint without needing to retransmit all the data again.

HTTP Cokkies example Authorization
Authentication: Cookies are commonly used for storing session identifiers (like session_id) after a user logs in. This allows the user to stay logged in across different pages or visits without re-entering credentials.

NetBIOS
RPC (Remote Procedure Call)
PPTP (Point-to-Point Tunneling Protocol)

Layer	Working	Protocol Data Unit	Protocols
1 – Physical Layer	Establishing Physical Connections between Devices.	Bits	USB, SONET/SDH, etc.
2 – Data Link Layer	Node to Node Delivery of Message.	Frames	Ethernet, PPP, etc.
3 – Network Layer	Transmission of data from one host to another, located in different networks.	Packets	IP, ICMP, IGMP, OSPF, etc.
4 – Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segments (for TCP) or Datagrams (for UDP)	TCP, UDP, SCTP, etc.
5 – Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Data	NetBIOS, RPC, PPTP, etc.
6 –	Data from the	Data	TLS/SSL, MIME, JPEG,

Layer	Working	Protocol Data Unit	Protocols
Presentation Layer	application layer is extracted and manipulated in the required format for transmission.		PNG, ASCII,
7 – Application Layer	Helps in identifying the client and synchronizing communication.	Data	FTP, SMTP, DNS, DHCP, etc.

2. **Encoding**

Encoding is the process of converting data from one format into another, typically for the purpose of standardization, efficient transmission, or storage. It does not use keys, it can be easily decoded.

3. **Encryption**

hb(ciphertext) using an algorithm and a key. This transformation ensures that the data remains confidential and secure, protecting it from unauthorized access, even if intercepted during transmission, it cannot be easily decoded.

What is an IP Address?

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

4. **ARP** (Address Resolution Protocol)

ARP (Address Resolution Protocol) is a protocol used in computer networks to map a device's IP address (Internet Protocol address) to its MAC address (Media Access Control address). This mapping is necessary because while IP addresses are used for routing data between devices on a network, the actual transmission of data between devices on the same local network (LAN) relies on MAC addresses, which are unique hardware addresses assigned to network interface cards (NICs).

5. **IGMP** (Internet Group Management Protocol)

IGMP is a network-layer protocol used by hosts and adjacent routers on an IP network to manage the membership of multicast groups. Multicast allows one-to-many communications, where data is sent from a single sender to multiple receivers in an efficient manner, as opposed to broadcasting to all devices or unicasting to a single device.

6. **ICMP** (Internet Control Message Protocol)

ICMP is a network layer protocol used to send control messages and error reporting in Internet Protocol (IP) networks. It is an essential protocol for diagnosing and troubleshooting network issues.

7.Networking terms & devices

Node: node is any device or point that can send, receive, or forward data

Hosts: A host is any device that has an IP address and can be a source or destination for data on a network.

Client: device that requests services or resources from a server.

Servers: device that provides resources, data, or services to clients.

Protocol: A set of rules that define how data is transmitted and handled between devices in a network.

8.**LAN/MAN/WAN**

LAN (Local Area Network) A Local Area Network (LAN) is a network that spans a small geographic area, such as a home, office, or building. It is typically used to connect devices like computers, printers, servers, and other networked devices within a limited physical area.

MAN (Metropolitan Area Network) A Metropolitan Area Network (MAN) is a larger network that spans a city or a large campus and is typically used to connect multiple LANs within a metropolitan area.

WAN (Wide Area Network) A Wide Area Network (WAN) is a network that covers a large geographic area, often spanning multiple cities, regions, or even countries. WANs are used to connect multiple LANs and MANs, allowing devices from different locations to communicate with each other. The internet itself is the largest example of a WAN.

9. **Modem/Router**

Modem

A modem (short for Modulator-Demodulator) is a device that connects your home or office network to the internet through your Internet Service Provider (ISP). It converts digital signals from your computer or network into analog signals.

Router

A router is a device that routes data between your modem and all the devices on your local network. Routers often include security features like firewalls to protect your internal network from outside threats.

10. **HTTP (Hypertext Transfer Protocol) Methods**

GET: The GET method is used to request data from a specified resource.

POST: creating a resource. POST requests typically include a request body, which contains the data to be submitted.

PUT: The PUT method is used to update a resource on the server.

DELETE: The DELETE method is used to delete a specified resource from the server.

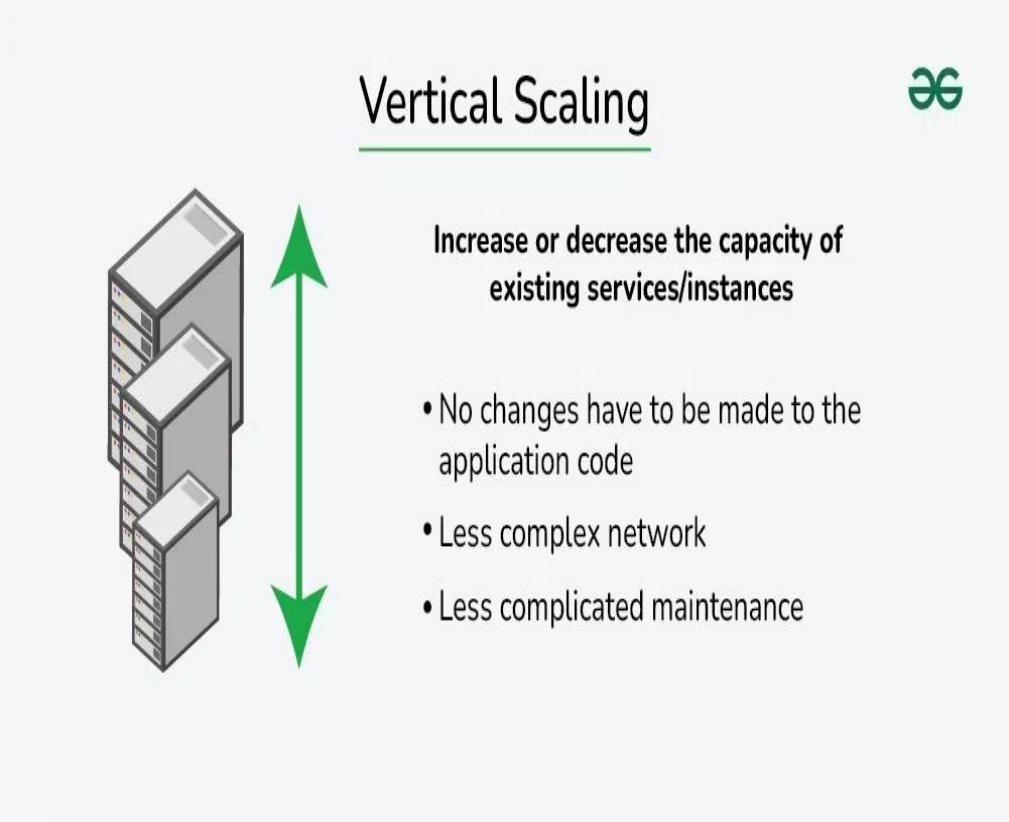
11.**Scalability**

Scalability is the capacity of a system to support growth or to manage an increasing volume of work. When a system's workload or scope rises, it should be able to maintain or even improve its performance, efficiency, and dependability. This is known as scalability.

1. Vertical Scaling

Vertical scaling, also known as scaling up, refers to the process of increasing the capacity or capabilities of an individual hardware or software component within a system.

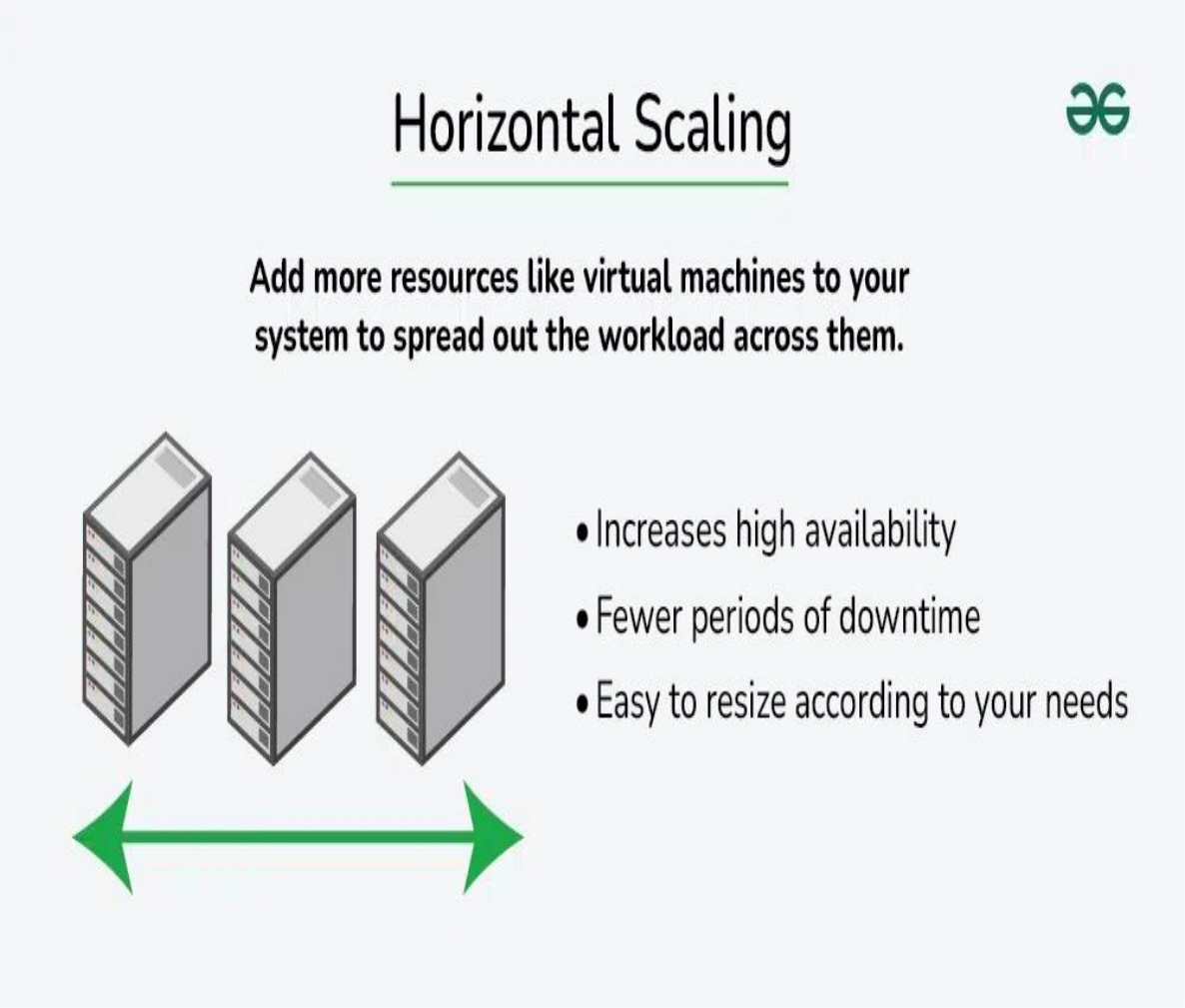
- You can add more power to your machine by adding better processors, increasing RAM, or other power-increasing adjustments.
- Vertical scaling aims to improve the performance and capacity of the system to handle higher loads or more complex tasks without changing the fundamental architecture or adding additional servers.



2.Horizontal Scaling

Horizontal scaling, also known as scaling out, refers to the process of increasing the capacity or performance of a system by adding more machines or servers to distribute the workload across a larger number of individual units.

- In this approach, there is no need to change the capacity of the server or replace the server.
- Also, like vertical scaling, there is no downtime while adding more servers to the network



Data transfer: In nat case more than one request how it handle it , I think there will be table to consider for each request

12) Network Topology

1) Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable.

2) Star Topolgy

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node all other nodes are connected to central node.

3) Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links.

4) Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighbouring devices.

DAY 2

HTTP Response code

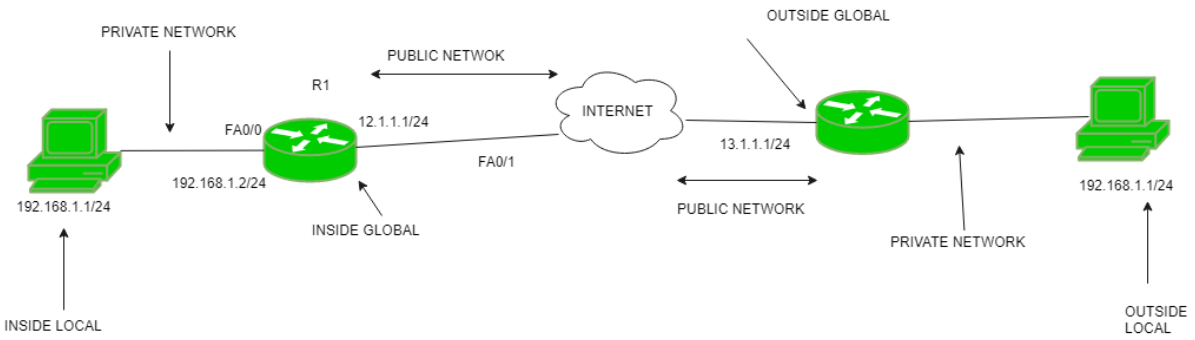
1. Informational responses $(100 - 199)$
2. Successful responses $(200 - 299)$
3. Redirection messages $(300 - 399)$
4. Client error responses $(400 - 499)$
5. Server error responses $(500 - 599)$

Cookies

Cookies are used to track the history of pages you visit

Network Address Translation (NAT)

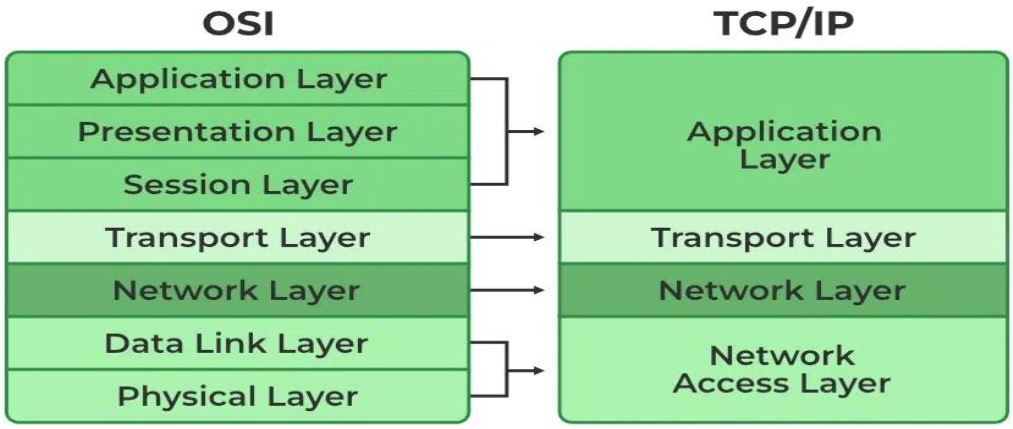
NAT is a process in which one or more local IP addresses are translated into one or more Global IP addresses and vice versa to provide Internet access to the local hosts. It also does the translation of port numbers, i.e., masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.



TCP/IP

- ***Network Interface Layer****: Handles the physical transmission of data over a network.*
- ***Internet Layer****: Manages the routing of data packets across the network.*
- ***Transport Layer****: Ensures reliable data transmission between devices.*

  Application Layer*: Provides protocols for specific data communication services on a process-to-process level*



VPN(Virtual Private Network)

A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet.

1)Remote Access VPN It permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private.

2) Site-to-Site VPN A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

3). Cloud VPN

A Cloud VPN is a virtual private network that allows users to securely connect to a cloud-based infrastructure or service

4). Mobile VPN

Mobile VPN is a virtual private network that allows mobile users to securely connect to a private network.

5). SSL VPN

SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses the SSL protocol to secure the connection between the user and the VPN server.

6.Double VPN

Two VPN Instead of one VPN.

Check Sum

A value used to verify data integrity ensuring it hasn't been altered during data transmission. In communication it will count the no. of packets .

ICMP – Error detection /reporting Network layer protocol

Ping

Ping (Packet Internet Groper) is a method for determining communication latency between two networks or ping is a method of determining the time it takes for data to travel between two devices or across a network. Ping sends an ICMP Echo Request to a network interface and then waits for a response. When the ping command is executed, a ping signal is delivered to the provided address. When the target host receives the echo request, it answers with an echo reply packet.

Traceroute It shows you the complete route to a destination address, gives the number of hops.

Subnetting It is the process of dividing a large network into smaller networks called as "subnets."

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily.

Different Parts of IP Address

An IP address is made up of different parts, each serving a specific purpose in identifying a device on a network. In an IPv4 address, there are four parts, called "octets," which are separated by dots (e.g., 192.168.1.1).

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

In class C the first 3 octets are network bits so it remains as it is.

• For Subnet-1: The first bit which is chosen from the host id part is zero and the range will be except for the first bit which is chosen zero for subnet id part.

• Thus, the range of subnet 1 is: 193.1.2.0 to 193.1.2.127

• Subnet id of Subnet-1 is : 193.1.2.0

• The direct Broadcast id of Subnet-1 is: 193.1.2.127

• The total number of hosts possible is: 126 (Out of 128)

• 2 id's are used for Subnet id & Direct Broadcast id)

• The subnet mask of Subnet- 1 is: 255.255.255.128

Thus, the range of subnet-2 is: 193.1.2.128 to 193.1.2.255

VPC(Virtual Private Cloud)

VPC can be referred to as the private cloud inside the cloud. It is a logical grouping of servers in a specified network.

A Region is a geographical area where cloud providers (e.g., AWS, Google Cloud) have data centers to run services. Each region is physically isolated from others to ensure fault tolerance and stability.

Example: AWS might have a region named us-east-1 (North Virginia), and Google Cloud might have a region called us-central1 (Iowa).

Availability Zone (AZ) is a distinct, isolated location within a region, typically representing a data center or a group of data centers. Each region consists of multiple AZs that are connected by high-speed private links. Example: The us-east-1 region in AWS has several availability zones, such as us-east-1a, us-east-1b, and us-east-1c.

A Subnet is a logical division of a VPC's IP address range. It allows you to partition the network within a region and organize resources into smaller, manageable segments.

VPC has the CIDR block 10.0.0.0/16 you might create multiple subnets like:

- 10.0.1.0/24 for a public subnet - doubt
- 10.0.2.0/24 for a private subnet - doubt

DAY 3

FIREWALL

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.

Accept: allow the traffic

Reject: block the traffic but reply with an “unreachable error”

Drop: block the traffic with no reply

FILTER BASED ON IP ADDRESS, PORT NUMBER OR PROTOCOL

	Stateless Packet Filtering Firewalls	**Stateful Packet Filtering Firewalls**
1.	The stateless firewalls are designed to protect networks based on static information such as	Stateful firewalls filter packets based on the

	Stateless Packet Filtering Firewalls	Stateful Packet Filtering Firewalls
	source and destination.	full context of the connection.
2.	It uses some predefined packet filtering rules, the packets are judged based on that, if it conforms to the predefined rules then it is considered to be “safe” and allowed to pass through. If the conditions are not met, the packet is considered to be “unidentified” or “malicious” and it will be blocked.	It uses the concept of a state table where it stores the state of legitimate connections. Stateless firewall filters are only based on header information in a packet but stateful firewall filter inspects everything inside data packets, the characteristics of the data, and its channels of communication.
3.	Less secure than stateless firewalls.	Stateful firewalls are more secure.
4.	Cheaper or cost-efficient.	Expensive as compared to stateless firewall
5.	Faster than Stateful packet filtering firewall.	Slower in speed when compared to Stateless firewall.
6.	For small businesses, a stateless firewall could be a better option, as they face fewer threats and also have a limited budget in hand.	For larger enterprises, a stateful firewall would be a smarter option, as they have larger outgoing traffic that needs monitoring and enough money to afford it. Stateful firewalls offer dynamic packet filtering, so they can provide a thick security layer to mitigate attacks.

API Gateway

An API Gateway is a server or service that acts as an intermediary between a client (such as a web or mobile application) and multiple backend services (often microservices). It provides a unified entry point for accessing different APIs, making it easier for clients to interact with multiple services without

needing to know the specifics of each one.

Personal Access Token (PAT)

PATs are used as an alternative to traditional username/password authentication, and they provide a more secure and flexible way of authenticating users or applications.

Server Farm

A server farm is a large collection of servers that work together to provide a high level of computing power and storage capacity for various applications, websites, and services. These servers are usually housed in a data center and are configured to work as a unified system, often using load balancing, redundancy, and virtualization technologies to ensure scalability, high availability, and reliability.

IPSec (Internet Protocol Security)

IPSec (Internet Protocol Security) is a suite of protocols used to secure IP communications by authenticating and encrypting each IP packet in a communication session. It is commonly used to implement Virtual Private Networks (VPNs) and to protect data traffic across untrusted networks, such as the internet.

IPSec operates at the Network Layer (Layer 3) of the OSI model and can secure communication between devices such as routers, firewalls, and gateways, as well as between hosts (e.g., computers, servers). Its primary purpose is to ensure data confidentiality, integrity, and authenticity.

Threat, Vulnerability, and Risk in Cybersecurity

Threat: A threat refers to any potential danger or event that could exploit a vulnerability and cause harm to a system, network, or data.

Vulnerability: A vulnerability is a weakness or flaw in a system, network, application, or process that can be exploited by a threat actor to gain unauthorized access or cause harm.

Risk: Risk is the potential impact of a threat exploiting a vulnerability, expressed in terms of likelihood and consequences.

Reverse Proxy

A reverse proxy is a server that sits between client devices and a backend server.

IPV4/IPV6

IPV4

- IPv4 is a 32-bit address.
- IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).
- IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.
- It supports manual and DHCP configuration.

IPV6

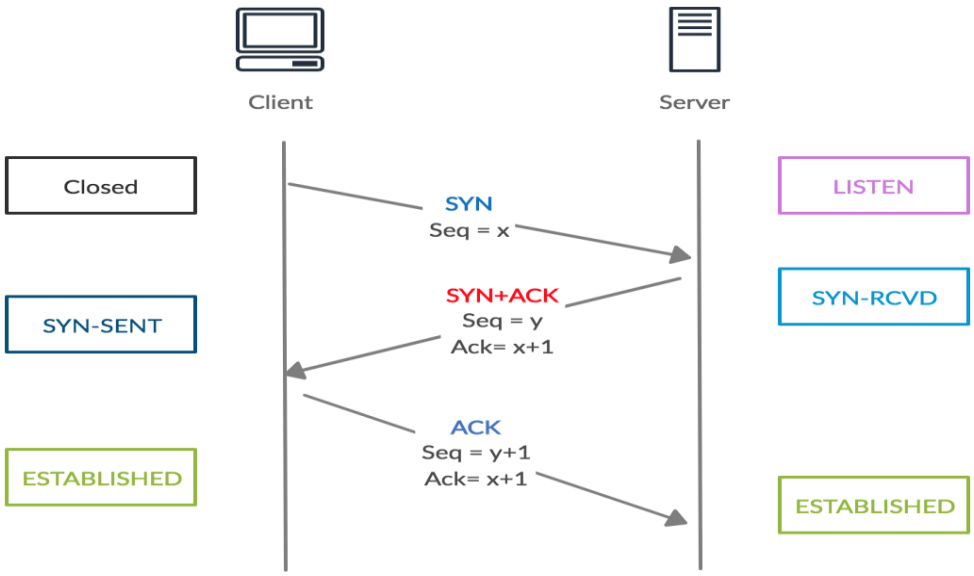
- IPv6 is a 128-bit address.

• IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.

• IPv6 does not contain classes of IP addresses.

• It supports manual, DHCP, auto-configuration, and renumbering.

3-Way Handshake



• SYN (client to server)

• SYN-ACK (server to client)

• ACK (client to server)

41. DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign IP addresses and other network configuration information to devices (known as clients) on a network.

42. Switch and Router

Switch

A switch is a network device that connects multiple devices (like computers, printers, and servers) within a local area network (LAN) and uses MAC addresses to forward data packets between devices.

Router

Definition:

A router is a device that connects multiple networks together, typically a local area network (LAN) and

the internet, and forwards data packets between them using IP addresses.

43.Port forwarding

Port forwarding is a network configuration technique used to allow external devices or services to access specific services or devices within a private internal network. It works by redirecting communication requests from an external IP address (often the public IP address of a router) to a specific device or service on the internal network, using a particular port number.

44.Hub and switch

Hub:

A hub is a basic networking device that connects multiple devices in a network, enabling them to communicate with each other. It operates at Layer 1 (Physical Layer) of the OSI model and is often referred to as a "network hub".

Switch:

A switch is a more advanced network device that connects devices within a local network and uses MAC addresses to forward data only to the intended recipient. It operates at Layer 2 (Data Link Layer)

of the OSI model.

45. VLAN (Virtual Local Area Network)

A VLAN (Virtual Local Area Network) is a logical grouping of devices within a physical network, allowing them to communicate as if they are on the same local network, regardless of their actual physical location. VLANs enable network administrators to segment networks into smaller, more manageable parts, improving security, performance, and organization.

DAY 4

DATA CENTER

In a dedicated space with strong security levels, where enterprises or organizations store and share large amounts of data, is known as a data center.

Key components

- **Servers** (compute power)

  Servers are the backbone of any data center, responsible for running applications, managing data, and providing services to clients or users. These can include web servers, database servers, application servers, and storage servers.

- **Storage systems** (data management)

  Data storage systems hold and manage large volumes of data within a data center. This can include both primary data (active data) and backup or archival data.

- **Networking equipment** (communication)

  Networking equipment connects all the components of a data center, ensuring communication between servers, storage systems, and external networks.(Router, Switch, Firewall)

- **Power supply and backup systems** (reliable operation)

Ensures that the data center operates continuously without interruption due to power failures.

- **Cooling systems** (temperature regulation)

  Servers and other IT equipment generate a lot of heat, so cooling systems are necessary to maintain an optimal operating temperature.

- **Security systems** (physical and cybersecurity)

  Protects the physical and logical infrastructure of the data center from unauthorized access, theft, and cyber threats.

Types of Data centers

- **On premise Data Center**
- The organization owns the data center and is responsible for managing, maintaining, and upgrading the infrastructure.
- The company has complete control over how it is configured and customized to meet specific requirements.
- The data center is located within the organization's own premises.
- High initial investment.
- **Colocation Data Center**
- A third-party data center where businesses can rent space, power, cooling, and network connectivity for their IT infrastructure.
- Lower investment
- Shared infrasructure
- **Cloud Data Center**
- Data centers operated by cloud service providers (e.g., AWS, Google Cloud, Microsoft Azure) that host and manage virtualized resources and services.
- Pay-as-you-go model.
- High scalability

Storage Types

• **Direct Attached Storage (DAS)**:

* DAS refers to storage devices that are directly attached to a single computer or server, without being connected to a network. It is typically used for personal or small-scale applications.

* How it works: DAS storage is directly connected via interfaces such as USB, SATA, SAS, or Thunderbolt.

* Local storage directly attached to servers.

*Lack of scalability

*Potential to lost data

*Device specific

* Examples: External hard drives, internal hard drives, SSDs (Solid-State Drives).

• **Network Attached Storage (NAS)**:

*NAS is a storage device connected to a network, allowing multiple users and devices to access data over the network. It's often used for centralized file storage and sharing.

*How it works: NAS devices typically use Ethernet or Wi-Fi to connect to a local area network (LAN), and they present storage over protocols like SMB/CIFS (Windows), NFS (Linux/Unix), or AFP (Apple).

*File-based storage accessible over a network.

*Moderate scalability and perfomance

*Examples: Synology NAS, QNAP NAS, WD My Cloud.

• **Storage Area Networks (SAN)**:

*SAN is a high-speed network that connects storage devices (such as disk arrays) with servers, enabling block-level data access. Unlike NAS, which provides file-level access, SAN provides block-level access to data, typically used for large-scale enterprise applications.

*How it works: SANs often use Fibre Channel, iSCSI, or FCoE (Fibre Channel over Ethernet) to connect storage devices and servers. Data is accessed as blocks rather than files.

*High-speed network of storage devices, often used for large-scale enterprise data storage.

*Examples: EMC VMAX, NetApp FAS, Dell PowerMax

TYPES OF STORAGES

PRIMARY STORAGE

Primary storage refers to the storage that is directly accessible by the CPU and is used to store data and instructions that are actively being processed.

1. **RAM (Random access memory)**

   Description: RAM is the most common type of primary storage and is used to store data and instructions that the CPU needs to access quickly while performing tasks.

   Characteristics:

- Fast read and write access.
- Volatile memory (data is lost when power is turned off).
- Temporarily stores data being processed by running applications.

1. **ROM(Read only memory)**

Definition: ROM is a type of non-volatile memory used in computers and other electronic devices to store permanent data or instructions that are not meant to be altered or modified during normal operation.

Characteristics:

- Non volatile
- Read only
- Slower access

SECONDARY STORAGE

1. **HDD (Hard Disk Drives)**
2. **SSD (Solid-State Drives)**

Description: HDDs are mechanical storage devices that use spinning disks to read/write data. They are widely used for long-term storage.

Characteristics:

1. Larger capacity compared to primary storage.
2. Slower read/write speeds due to mechanical components.
3. Non-volatile (data persists even without power).

Description: SSDs are storage devices that use flash memory to store data, providing faster read/write speeds compared to HDDs.

Characteristics:

1. Faster than HDDs but generally more expensive.
2. Larger capacity compared to primary storage.
3. Non-volatile, retains data without power.

OPTICAL DISC

- An **optical disc** is a storage medium that uses laser light to read and write data on a reflective surface.
- Optical discs are widely used for storing data such as software, music, videos, and backups.
- Example : CD, DVD, Floppy Disc

RAID LEVELS

RAID 0 (Striping)

- **Configuration**: Data is split into blocks and distributed across multiple disks (at least 2).
- **Redundancy**: No redundancy—if one drive fails, all data is lost.
- **Performance**: High performance, as data is read and written in parallel to multiple drives.
- **Capacity**: Total capacity is the sum of the capacities of all disks.
- **Use Case**: Suitable for applications requiring high performance and where data loss is not critical (e.g., temporary data, non-essential files).

RAID 1 (Mirroring)

- **Configuration**: Data is duplicated (mirrored) across two or more disks.
- **Redundancy**: High redundancy—if one drive fails, the data is still available from the other drive(s).
- **Performance**: Good read performance (because the system can read from multiple disks), but write performance is similar to a single disk.
- **Capacity**: Total capacity is the size of one drive (since data is duplicated).
- **Use Case**: Suitable for situations where data integrity is critical and write performance is not as important (e.g., personal computers, critical data storage).

RAID 5 (Striping with Parity)

- **Configuration**: Data is striped across multiple disks (at least 3), with parity information distributed across all disks.
- **Redundancy**: Moderate redundancy—if one disk fails, the data can be rebuilt using the parity data from the remaining disks.
- **Performance**: Good read performance, but write performance is slower compared to RAID 0 and RAID 1 due to the overhead of parity calculations.
- **Capacity**: Total capacity is the sum of all disks minus one (because one disk is used for parity).
- **Use Case**: Suitable for applications that require a balance of redundancy, performance, and storage capacity (e.g., file servers, databases).

RAID 6 (Striping with Double Parity)

- **Configuration**: Similar to RAID 5 but with **two sets of parity data**, which are stored across different disks (requires at least 4 disks).
- **Redundancy**: High redundancy—can tolerate the failure of **two disks** simultaneously without data loss.
- **Performance**: Read performance is good, but write performance is slower than RAID 5 because of double parity calculations.
- **Capacity**: Total capacity is the sum of all disks minus two (because two disks are used for parity).
- **Use Case**: Suitable for environments where data protection is more important than write performance (e.g., critical business data storage).

RAID 10 (RAID 1+0)

- **Configuration**: Combines the features of RAID 1 and RAID 0. Data is mirrored (RAID 1) and then striped (RAID 0).

- **Redundancy**: High redundancy—can tolerate the failure of one disk per mirrored pair.
- **Performance**: High performance for both read and write operations, as data is striped (RAID 0) and mirrored (RAID 1).
- **Capacity**: Total capacity is the sum of half of the disks (since data is mirrored).
- **Use Case**: Suitable for applications that require both high performance and redundancy (e.g., databases, high-performance servers).

BACKUP AND RECOVERY

A **backup** is the process of creating a duplicate copy of data that can be restored in case the original data is lost, corrupted, or inaccessible.

TYPES OF BACKUP

Full Backup

- **Definition**: A full backup is a complete copy of all selected data. It copies everything, including all files, folders, and system data (depending on the configuration).
- **How It Works**: Every time a full backup is performed, all data is backed up in its entirety, regardless of whether it has changed since the last backup.

Incremental Backup

- **Definition**: An incremental backup only backs up the data that has changed since the **last backup** (whether it was a full backup or the most recent incremental backup).
- **How It Works**: After an initial full backup, subsequent incremental backups only capture changes made to files since the last backup. This can be multiple times over a period.

Differential Backup

- **Definition**: A differential backup captures all the changes made since the last **full backup**. Unlike incremental backups, differential backups do not rely on previous differential backups, but only on the full backup.

Mirror Backup

- **Definition**: A mirror backup creates an exact copy (or "mirror") of the selected data. It is similar to a full backup but continuously synchronizes data between the source and the backup location.

3-2-1 BACKUP STRATEGY

The **3-2-1 backup strategy** is a widely recommended method for ensuring robust data protection and recovery. It helps mitigate the risks of data loss from various types of disasters (e.g., hardware failure, cyberattacks, accidental deletions). This strategy involves creating multiple copies of data and storing them in different locations to increase redundancy and resilience.2 Copies stores in two different media types and one in offsite.

BASIC SERVER COMPONENTS

- **MOTHER BOARD:** A **motherboard** is the central printed circuit board (PCB) in a computer that connects and allows communication between various hardware components. It serves as the backbone of the computer, providing essential connections for components like the **CPU, RAM**
- **CPU**
- **RAM**
- **NIC**
- **STORAGE DRIVE**

LOAD BALANCING

- **ROUND ROBIN: Round Robin** is one of the simplest and most commonly used load balancing algorithms. It is a method used to distribute client requests (or traffic) across a group of servers or resources in a circular order.
- **LEAST CONNECTION: Least Connections** is a dynamic load balancing algorithm that directs incoming traffic to the server with the **fewest active connections** at the time of the request. This method is designed to distribute load based on the number of active connections each server is currently handling, aiming to prevent overloading any single server.
- **LEAST RESPONSE TIME: Least Response Time** is a dynamic load balancing algorithm that routes incoming client requests to the server with the **quickest response time** at the moment of the request. The goal of this algorithm is to optimize user experience by sending traffic to the server that is not only least loaded but also currently capable of processing requests the fastest.
- **SOURCE IP HASHING: Source IP Hashing** is a load balancing algorithm that uses the **client's IP address** to determine which server in the pool should handle a particular request. The key idea behind this approach is to ensure that requests from the same client IP address are always directed to the same backend server, creating session persistence (also called sticky sessions).
- **WEIGHTED ROUND ROBIN: Weighted Round Robin (WRR)** is an enhancement of the traditional **Round Robin** load balancing algorithm. In **Weighted Round Robin**, each server in the pool is assigned a **weight** that reflects its capacity or performance. The load balancer distributes incoming requests across the servers, but it gives more requests to servers with higher weights, effectively allowing more powerful servers to handle more traffic.

TYPES OF LOAD BALANCER

HARDWARE LOAD BALANCER

Hardware load balancer is a physical appliance designed specifically for load balancing tasks. It is a dedicated device with specialized hardware and software to handle traffic distribution efficiently.

SOFTWARE LOAD BALANCER

A software load balancer is a software application that runs on general-purpose hardware (such as a server or virtual machine) to perform load balancing tasks. It uses algorithms and protocols to distribute traffic among multiple servers.

CONFIDENTIALITY

Confidentiality is one of the core principles of **information security**, ensuring that sensitive information is only accessible to those authorized to view it. It involves preventing unauthorized individuals, organizations, or systems from accessing data, ensuring that private and personal information is protected from exposure or misuse.

INTEGRITY

Integrity refers to the concept of maintaining and assuring the accuracy, consistency, and trustworthiness of data throughout its lifecycle. It ensures that data is not altered, tampered with, or corrupted—either accidentally or maliciously—while it is being stored, transmitted, or processed.

AVAILABILITY

Availability refers to the concept of ensuring that information, systems, and services are accessible and usable by authorized individuals when needed.