DAY - 1

Client Server Model

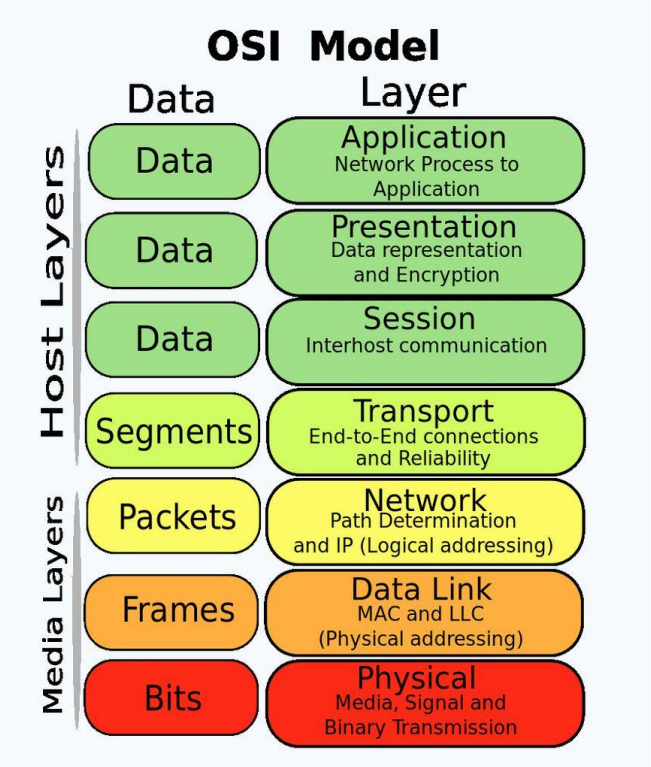
In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and delivers the data packets requested back to the client.

Client: When we say the word **Client**, it means to talk of a person or an organization using a particular service.

Server :A remote computer that provides information (data) or access to particular services.

OSI Model (Open Systems Interconnection Model)

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.
The OSI Model is widely used as a reference to understand how network systems function.



1)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.

2)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.**

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC. DLL also encapsulates Sender and Receiver's MAC address in the header.

3)Network Layer

The 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.**

4)Transport 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.

At the sender's side, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission.

It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application

5)Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices.

6)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.

Encryption/Decryption and compression also performed here.

7)Application Layer

Application Layer 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.

Data Flow

- **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.

Encoding: Transforms data into a different format to make it more human-readable and usable by different systems. Encoding is reversible, meaning that the same algorithm used to encode the data can be used to decode it.

Encryption:

Transforms data into an unreadable format to make it difficult for unauthorized users to decode. Encryption is reversible for authorized users who have a secret key.

TCP/IP PROTOCOL

TCP/IP stands for **Transmission Control Protocol/ Internet Protocol.** It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet. The internet protocol suite is commonly known as TCP/IP, as the foundational protocols in the suite are Transmission Control Protocol and Internet Protocol. It chooses how the information will be traded over the web through end-to-end communications that incorporate how the information ought to be organized into bundles (bundles of data), addressed, sent, and received at the goal. This communication protocol can also be utilized to interconnect organize devices in a private network such as an intranet or an extranet.

TCP/IP Layers:

- **Application Layer** An application layer is the topmost layer within the TCP/IP model. When one application layer protocol needs to communicate with another application layer, it forwards its information to the transport layer.
- **Transport Layer** It is responsible for the reliability, flow control, and correction of data that is being sent over the network. There are two protocols used in this layer are User Datagram Protocol and Transmission control protocol.
- It add sequence number and checksum
- **Internet/Network Layer** It is the third layer of the TCP/IP Model and also known as the Network layer. The main responsibility of this layer is to send the packets from any network, and they arrive at the goal irrespective of the route they take.
- It adds its own header to each TCP segment contain source address and destination IP address.

- **Network Access Layer** It is the lowest layer of the TCP/IP Model. It is the combination of the Physical Layer and the Data link layer which present in the OSI Model. Its main responsibility is to the transmission of information over the same network between two devices.

Public IP:
IP Address which will known globally

ICMP(Internet Control Message Protocol)
The protocol is at the network layer. It is mostly utilized on network equipment like routers and is utilized for error handling at the network layer.

ARP(Address Resolution Protocol)
Used to resolve the IP Addresses to MAC Address.
Devices use ARP to acquire the MAC Address for a device.If device A wants to communicate with device B.
Firstly the device A will first look at its internal list called an ARP cache if it has already have MAC Address.
If it has not then A will broadcast the message on network asking every device which computer has the specific IP Address asked them the MAC Address
Which Computer has the matching IP Address will send the MAC Address after that device A will store the MAC Address in ARP cache(table).

NIC(Network Interface Card)
A NIC allows a computer to send and receive data with other devices on a network, such as routers or switches.

Fiber Optic Cables

Fiber Optic cables carrying data at highspeed

Submarine Cables

Submarine cables are specialized under sea cables that transmit data across sea oceans forming the backbone of global internet infrastructure. These cables carry the majority of international communications, including internet traffic, telephone calls and private data transfers.

Types of area networks – LAN, MAN and WAN

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. MAN has a range of 5-50km. It connects two or more computers that are apart but reside in the same or different cities.

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country.

MODEM

It connects your local network to the **internet**. It's necessary for accessing the web and converts the internet signal from your ISP (Internet Service Provider) into a usable form for your devices.

It converts the input analog signal to a digital signal and directs it to the computer and vice versa.

Minimal security

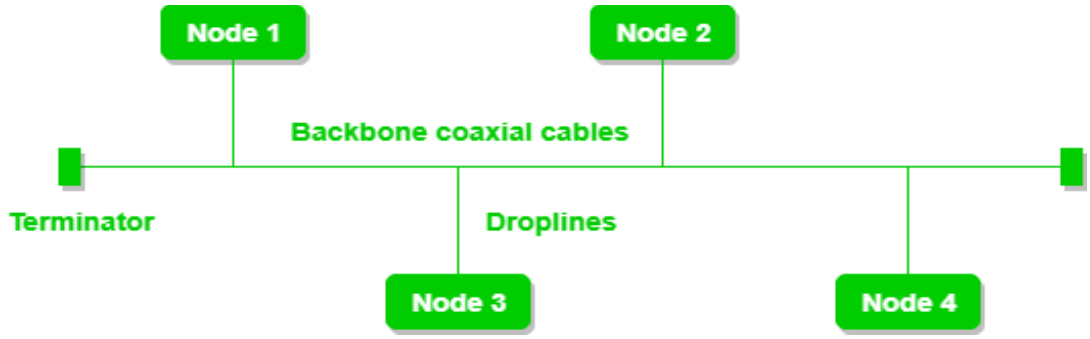
ROUTER

It directs the flow of **data packets** between different devices in your network. A router helps manage how data travels between devices and ensures that it reaches the correct destination.

Network Topology

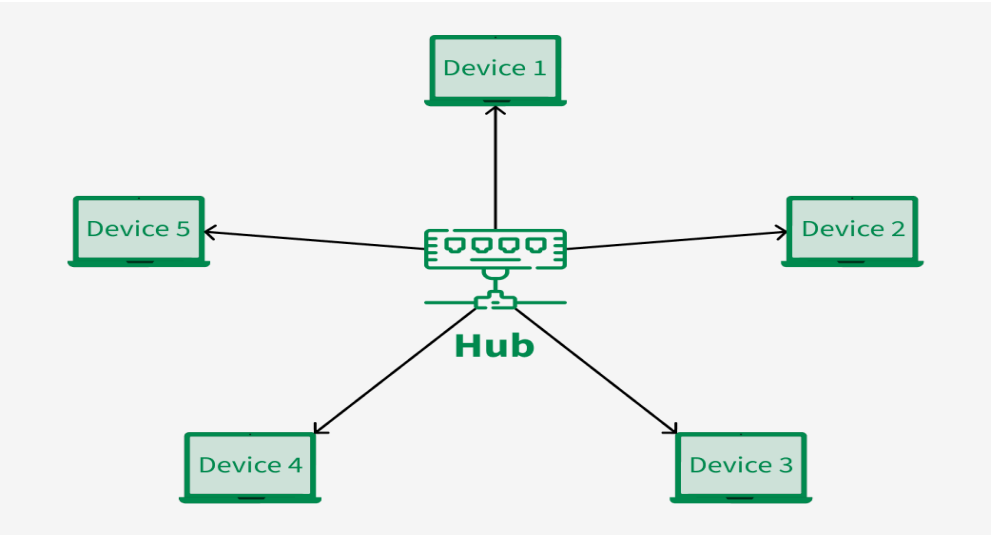
1)Bus Topology

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



2)Star Topolgy

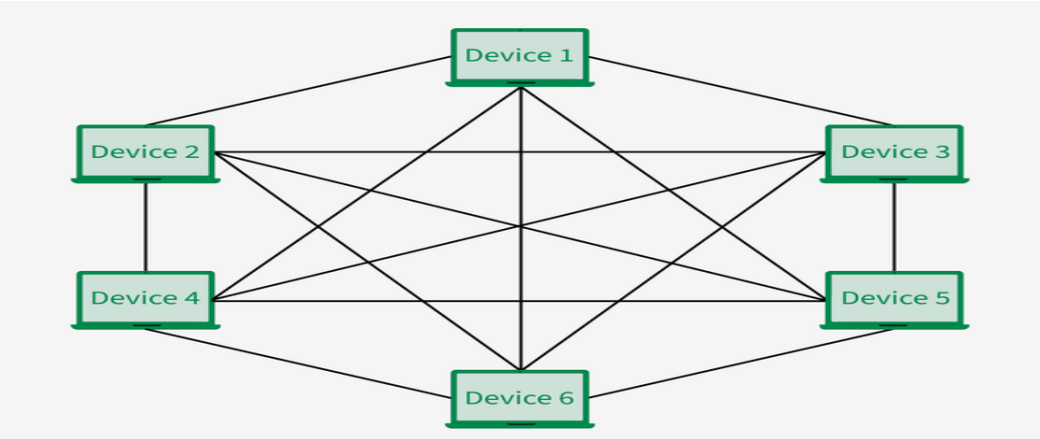
In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node all other nodes are



connected to central node.

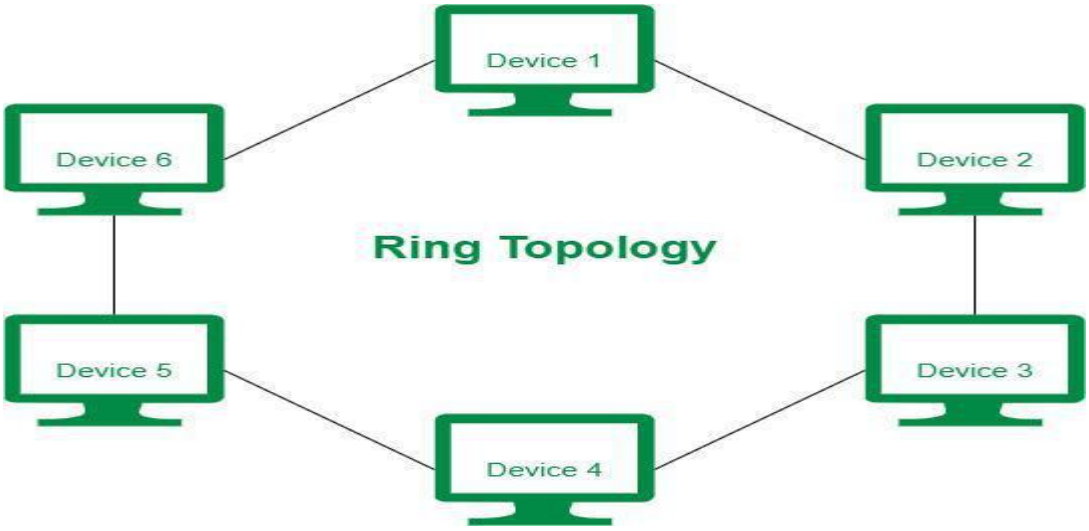
3)Mesh Topology

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.



Ring Topology

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



Peer-to-Peer (P2P) Architecture

Peer-to-peer (P2P) architecture is a decentralized computing model where network participants share resources directly with each other without the need for a centralized server.

A socket can be regarded as a basic network entity that allows devices to communicate over a network with the use of data.

combination of IP and port.

A port is an access point where protocols are used in a network to locate the particular processes or services within a device.

Scalability

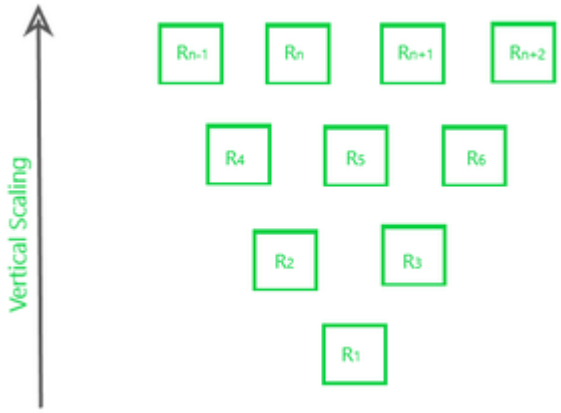
Cloud scalability is used to handle the growing workload where good performance is also needed to work efficiently with software or applications.

Example: Consider you are the owner of a company whose database size was small in earlier days but as time passed your business does grow and the size of your database also increases, so in this case you just need to request your cloud service vendor to scale up your database capacity to handle a heavy workload.

Types of Scalability:

1. Vertical Scalability (Scale-up/scale down) –

In this type of scalability, we increase the power of existing resources in the working environment in an upward direction.



2)Horizontal Scalability(scale in/scale out)

In this kind of scaling, the resources are added in a horizontal row.

Cloud Elasticity: Elasticity refers to the ability of a cloud to automatically expand or compress the infrastructural resources on a sudden up and down in the requirement so that the workload can be managed efficiently.

HTTP Methods

The Hypertext Transfer Protocol (HTTP) is designed to enable communications between clients and servers.

GET – Retrieve data

POST – Create data

PUT – Update data

DELETE – Remove data

DAY - 2

- HTTP error/status codes //Stateless Protocol
  common code like
  200 - ok
  404 - not found
  500 - internal server error

- **Cookies**
  Small amount of txt file
  saved when you visit the web site
  This help the website to remember info about your visit

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.

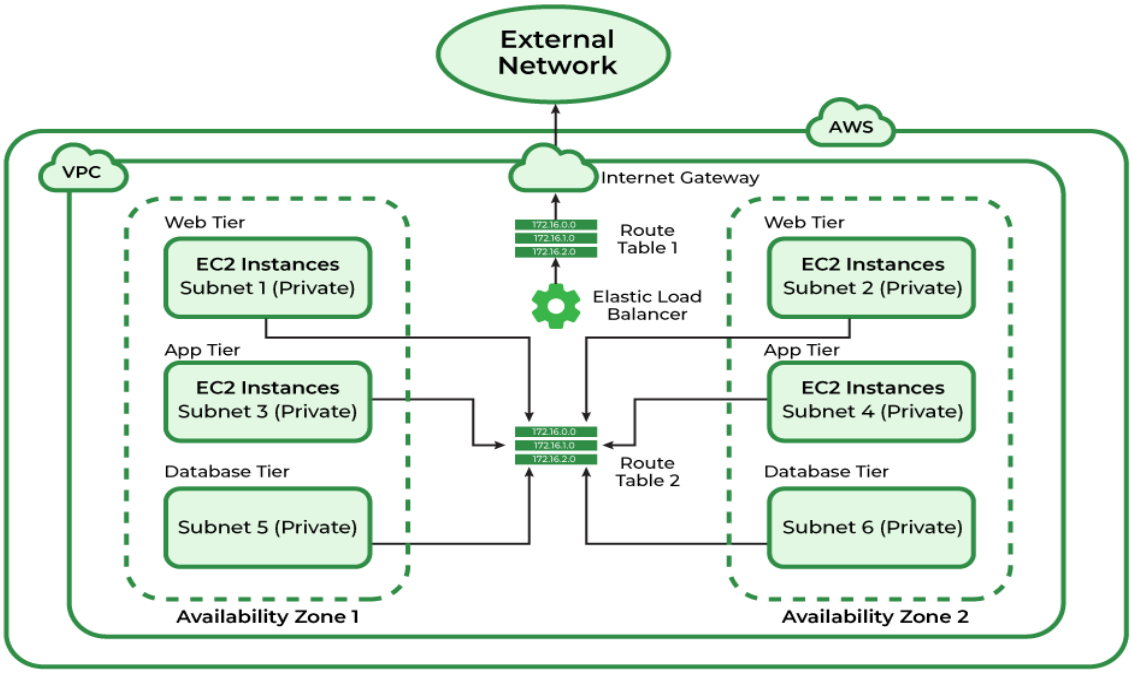
Example: AWS might have a region named **us-east-1** (North Virginia), and Google Cloud might have a region called **us-central1** (Iowa).

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



NAT(Network Address Translation)

This is commonly used when internal devices with private IP addresses want to access external resources on the internet. It is a technique that translates source IP addresses generally when connecting from a private IP address to a public IP address.

Static NAT - also known as **one-to-one NAT**, is a type of NAT where a **single private IP address** is mapped to a single public IP address.

Dynamic NAT maps **private IP addresses** to a pool of **public IP addresses**

However, this mapping is not fixed like Static NAT. Instead, when a device in the private network wants to communicate with the internet, a public IP address is dynamically assigned from the pool of available public IP addresses.

PAT, also known as **Overloading or Network Address Port Translation (NAPT)**, is a form of **many-to-one NAT**.With PAT, multiple private IP addresses can be mapped to a **single public IP address**, but with the addition of **port numbers** to differentiate between different connections.

DNAT(Destination Network Address Translation)

DNAT, as the name suggests, is a technique that translates the destination IP Address generally when connecting from a public IP address to a private IP address.

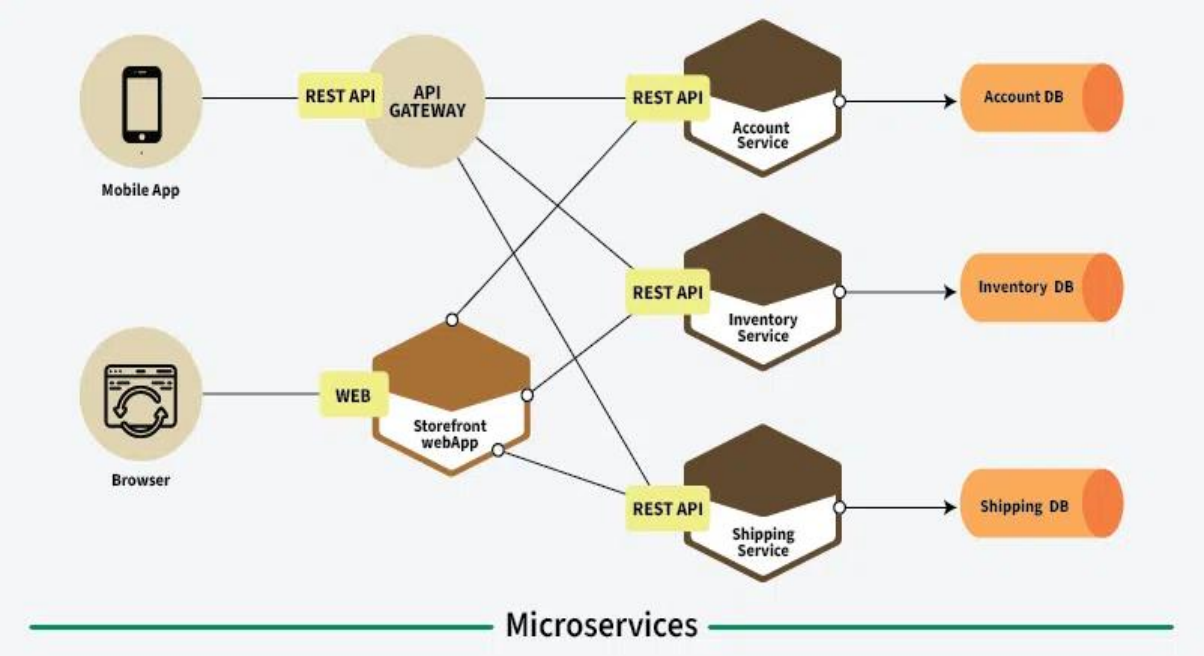
Symmetric-key encryption

In symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure.

Asymmetric-key encryption

one key is used to encrypt data and the second one is used to decrypt an encrypted text. The second key is kept highly secret, while the first one which is called a public key can be freely distributed among the service's users.

Microservices Architecture



Monolithic – A Single Application having all its services together.

Authentication- Authentication is the process of verifying the identity of a user or system.

Authorisation- Authorization is the process of determining what actions or resources an authenticated user or system is allowed to access.

API Gateway- Acts as a central entry point for external clients also they manage requests, authentication and route the requests to the appropriate microservice.

Service Discovery - Keeps track of the locations and addresses of all microservices, whether they are alive or not.

Load Balancer - Distributes incoming traffic across multiple service instances and prevent any of the microservice from being overwhelmed.

Synchronous Communication: Services communicate in real-time, waiting for a response before proceeding.

Asynchronous Communication: Services interact without waiting for an immediate response.

1) **Queue Model** – It is a common pattern in asynchronous communication where messages are placed into a queue for later processing. This is ideal for scenarios where tasks need to be executed, but not immediately, and where tasks are handled by one or more workers at different times.

2)**Notification model/Public subscribe model –** Subscriber send notifications to one or more recipients, without the need for immediate acknowledgment or interaction from the recipient.

DAY – 3

Firewall

It will know incoming traffic(Ingress) and outgoing traffic(egress)

Filter based IP address port

firewall restricts access to these services by controlling what external IPs or networks can interact with the system,

stateless firewall is a simpler type of firewall that inspects packets individually, without keeping track of the state of active connections. Looks at each packet **individually**. It doesn't track whether the packet is part of an ongoing communication.

stateful firewall, on the other hand, keeps track of the **state** of active connections and uses this information to make more informed decisions about which packets should be allowed or denied. It keeps track of the context of the traffic—this means that it can understand whether packets are part of an established connection or a new connection.

IPSec(IP Security)

IP Security (IPSec) refers to a collection of communication rules or protocols used to establish secure network connections. Internet Protocol (IP) is the common standard that controls how data is transmitted across the internet. IPSec enhances the protocol security by introducing **encryption** and **authentication**.

Threat - is a malicious act that seeks to steal or damage data or discompose the digital network or system.

vulnerability is a flaw in a system’s design, security procedures, internal controls, etc., that can be exploited by cybercriminals.

Risk - is a potential consequence of the loss or damage of assets or data caused by a cyber threat.

Reverse proxy is a server that acts as an intermediary between client requests and backend services. The reverse proxy routes client requests to the appropriate microservice, often based on the URL, headers, or other request information.

IPV4

IPv4 has a 32-bit address length

Address representation of IPv4 is in decimal

In IPv4 checksum field is available

IPv4 consists of 4 fields which are separated by addresses dot (.)

IPV6

IPv6 has a 128-bit address length

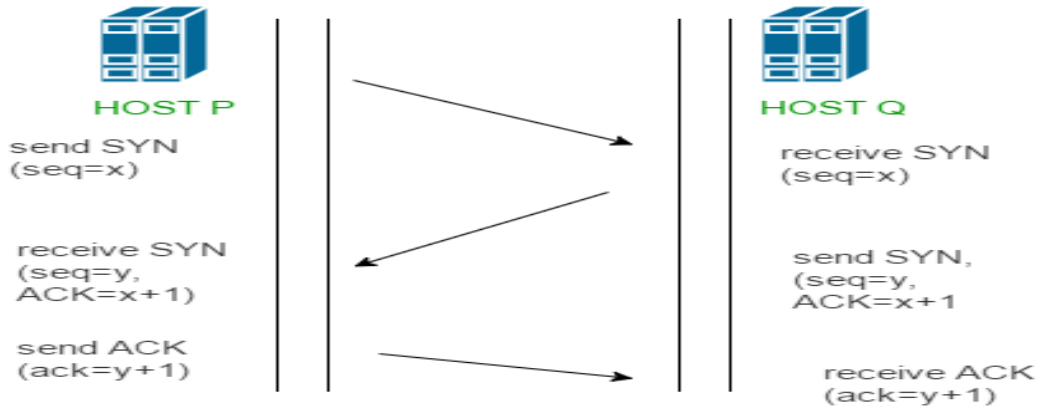
It supports Auto and renumbering address configuration

In IPv6 checksum field is not available

IPv6 consists of 8 fields, which are separated by a colon (:)

3 way handshaking

The TCP 3-Way Handshake is a fundamental process used in the TCP to establish a reliable connection between a client and a server before data transmission begins. This handshake ensures that both parties are synchronized and ready for communication.



- **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.

PAT(personal access token)

Instead of giving user id and password you can share PAT.

A **server farm** is a large collection of servers housed in a single location, typically used to handle a high volume of traffic or to provide redundant services. It is essentially a group of servers that work together to provide services such as web hosting, data processing, or application delivery

- Scalable, load balancing, reliable

Router - A **router** is a network device used to **connect different networks** (typically LANs to WANs or different subnets) and direct data packets between them.

Switch - A **switch** is a network device used to connect devices within a **local area network (LAN)**.

Hub - Hubs do not scale well for large networks

A **hub** is a basic network device that connects multiple computers or devices within a **local area network (LAN)**.

Port

For instance, imagine your MAC Address or IP Address as the PIN code of the nearest Post Office and your house address as a Port. Whenever any parcel is sent to you it gets received by the nearest post office and then it is identified by your address where to deliver that parcel. Similarly in a computer data is first received using their IP or MAC address then it is delivered to the application whose port number is with the data packets.

Port is a logical address of a 16-bit unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.

Port forwarding / Port Mapping whatever request come on port allow incoming traffic on that port to be forwarded to device.

VLAN (Virtual Local Area Network) is a logical grouping of devices or computers on a network that are configured to communicate as if they are on the same physical network, even if they are actually on different switches or in different physical locations.

Gateway - help to connect two different network(local network to large network)

Bridge – is a device used to connect two or more **similar networks** or network segments

Wi-Fi - It is a technology that allows devices like smartphones, laptops, and other electronic devices to connect to the internet or local area networks (LANs) wirelessly, using radio waves instead of physical cables. Wi-Fi operates on **IEEE 802.11 standards**, which define the communication protocols and frequencies for wireless networks.

- **Frequency Bands**: Wi-Fi typically operates on **2.4 GHz** and **5 GHz** frequency bands, offering different ranges and speeds.
- **Access Points (APs)**: Devices connect to Wi-Fi through wireless **access points** that are connected to the network (either via a wired Ethernet cable or another wireless method).

DHCP(Dynamic Host Control Configuration) – It is a network protocol that automatically assigns **IP addresses** and other network configuration information (like subnet mask, gateway, and DNS servers) to devices on a network, without the need for manual configuration.

How It Works:

1)A device (e.g., a computer or smartphone) requests an IP address from the DHCP server.

2)The DHCP server assigns an available IP address from a predefined range (called a **pool**) and sends the information back to the device.

3)The device uses this information to configure its network settings and communicate on the network.

12 Factors Application

1) Codebase

One codebase tracked in version control (e.g., Git), with many deploys. There should be a single codebase for the app, and it should be stored in a version control system. The same codebase can be deployed to different environments (e.g., development, staging, production).

2)**Dependencies** - The app should declare all of its dependencies (e.g., libraries) explicitly, ensuring that it doesn't rely on the underlying system environment. Tools like Docker and virtual environments help isolate dependencies.

3)**Config -** Configuration such as database connection strings, API keys, and environment settings should not be stored in the codebase but in environment variables, making it easier to change settings across different environments.

4)**Backing Services** - Services like databases, message queues, and file storage should be treated as external, attachable resources. They can be swapped without changing the app code (e.g., replacing a local database with a cloud service).

5)**Build, Release, Run -** The process of building the app (compiling code, installing dependencies) should be separated from deployment and runtime. This ensures a clear separation of concerns.

6)**Processes -** Apps should be run in stateless processes, meaning they should not store data locally between requests. Any data needed should be stored in external services (e.g., databases, caches).

7)**Port Binding**- The app should be self-contained, and it should expose a service (e.g., web server) through a specific port, rather than relying on an external web server.

8)**Concurrency** - Applications should scale by running multiple instances of processes. This allows the app to handle more traffic or tasks without affecting the existing infrastructure.

9)**Disposability -** Apps should be able to start up quickly and shut down gracefully. This allows for efficient scaling, deployment, and handling of failures.

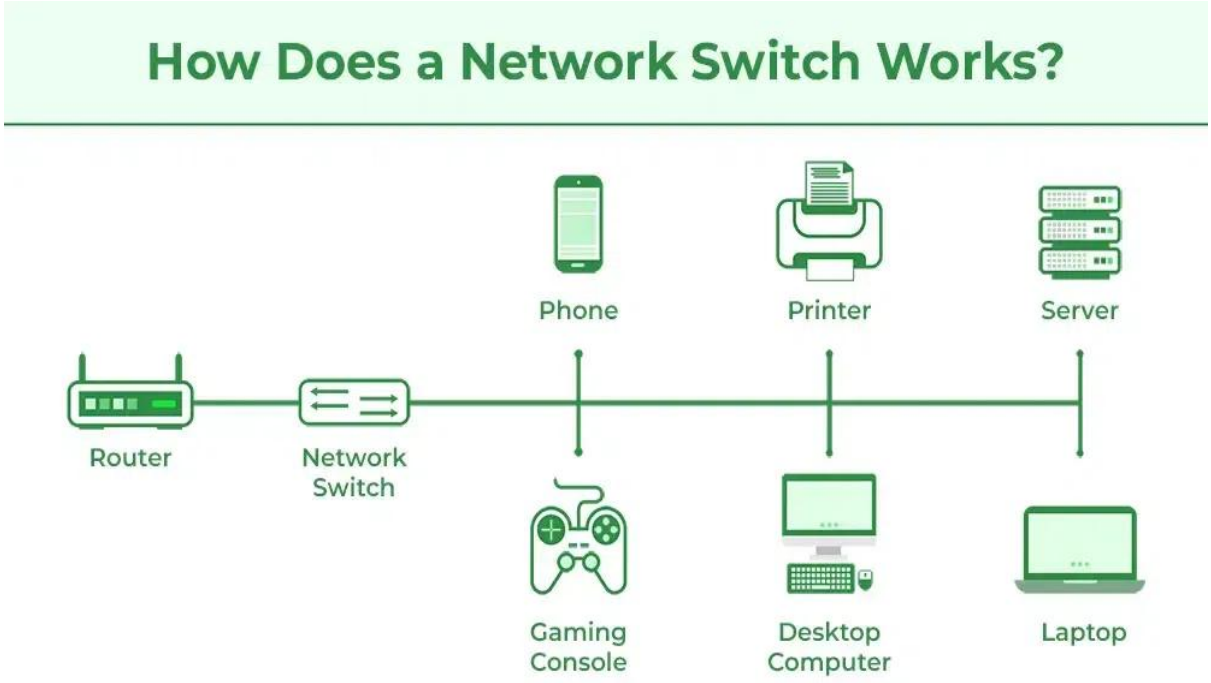
10)Dev – Prod Parity - The development, staging, and production environments should be as similar as possible to avoid discrepancies between environments that could lead to bugs or deployment issues.

11)Logs - Logs should be treated as streams of events, allowing the app to output logs to standard output or external systems.

12)Admin Processes - Any administrative or management tasks (e.g., database migrations, scripts) should be run as one-off processes.

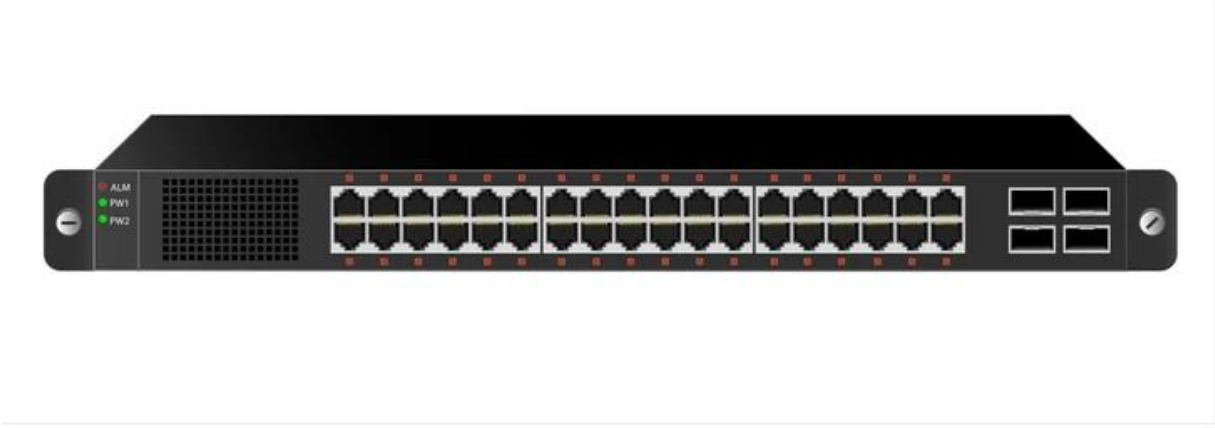
Network Switch

A network switch is a device that connects devices (like computers, printers, etc.) in a local area network (LAN) and forwards data between them based on MAC (Media Access Control) addresses.



When the source wants to send the data packet to the destination, the packet first enters the switch and the switch reads its header and finds the MAC address of the destination to identify the device then it sends the packet out through the appropriate ports that lead to the destination devices.

Switch establishes a temporary connection between the source and destination for communication and terminates the connection once the conversation is done.



Switches operate by using **MAC addresses** to forward data.
Learning: Switches learn MAC addresses by examining incoming data frames.
Forwarding: Based on the MAC address table, the switch forwards data to the correct device.
Filtering: Switches can also filter traffic and avoid unnecessary data broadcast.

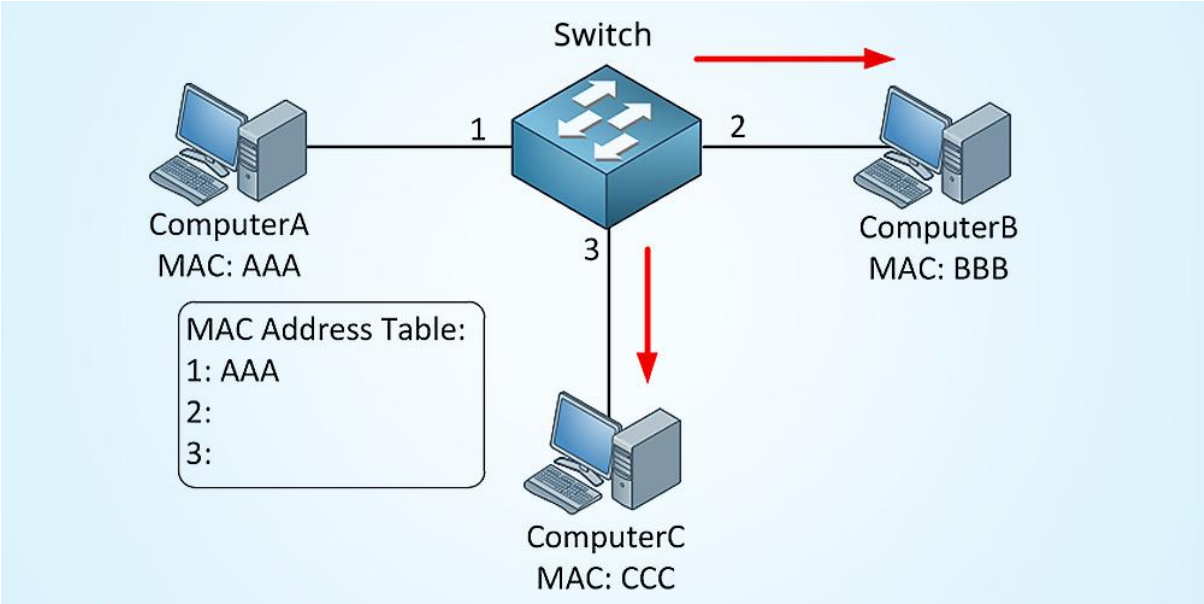


Diagram illustrating the forwarding process using MAC addresses.

Types of switches

1) Layer 2 switches

A Layer 2 switch operates at Layer 2 of OSI model, which is the Data Link Layer. The switch forwards data packets depending on the devices' MAC (Media Access Control) addresses that are in its network. Most commonly they are found in Local Area Networks (LAN).

2)Layer 3 switches

A **Layer 3 Switch** is similar to a regular switch but with added routing capabilities. While a standard switch works only at **Layer 2** (the Data Link Layer) and forwards data within the same network, a **Layer 3 switch** can also route data between different networks or subnets using **IP addresses**, just like a **router**.

Difference Between Network Switch and Router

Network Switch	Router
Network Switch works on Layer 2 of the OSI Model.	The router is primarily a device of Layer 3 of the OSI Model.
The resource is shared among multiple devices with the help of a single LAN using a network switch.	Data is moved between two or more computers with the help of a router.
Network switches uses data frames.	Routers use data packets.
Switches only work in a Wired network connection.	Router works with both wired and Wi-Fi networks.
Switches use MAC Addresses for transferring data to the proper destination.	Routers use IP Addresses for the same work.

Difference Between Network Switch and Hub

Network Switch	Hub
Network Switch is a device of layer 2 of the OSI Model.	Hub is a physical device of Layer 1 of the OSI Model.
Network Switch is a little more complex than a Hub.	Hub is a simple device as compared to Network Switch.
Network Switch easily manages data in and out, hence less communication collision.	Communication Collisions usually happen in a Hub.
Network Switches transfer data together by connecting devices.	The main task of Hub is to connect all nodes of the network.
Switches prevent collision with the help of Ethernet Frames.	Hubs cannot help in preventing collisions.

Advantages of using switches

- **Improved Network Performance**: Switches reduce network congestion by directing traffic to the right devices.
- **Security:** Preventing unauthorized access to other devices.
- **Scalability**: Easier to expand networks by adding more devices without significant performance loss.
- **Cost-Efficiency**: Switches are more cost-effective and provide better performance than hubs.

Day – 5