DevOps

08/01/2025

CI/CD: Continuous Integration / Continuous Delivery

Fundamentals of networking

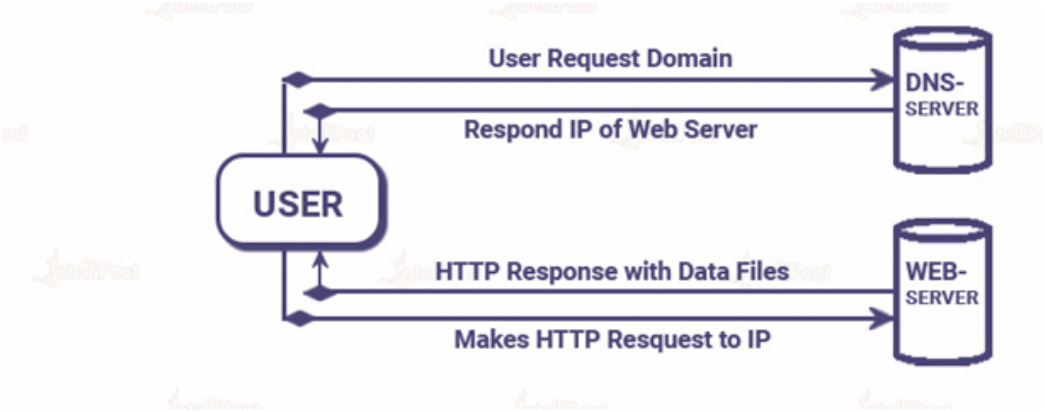
Client Server Architecture:

Client: Electronic Devices

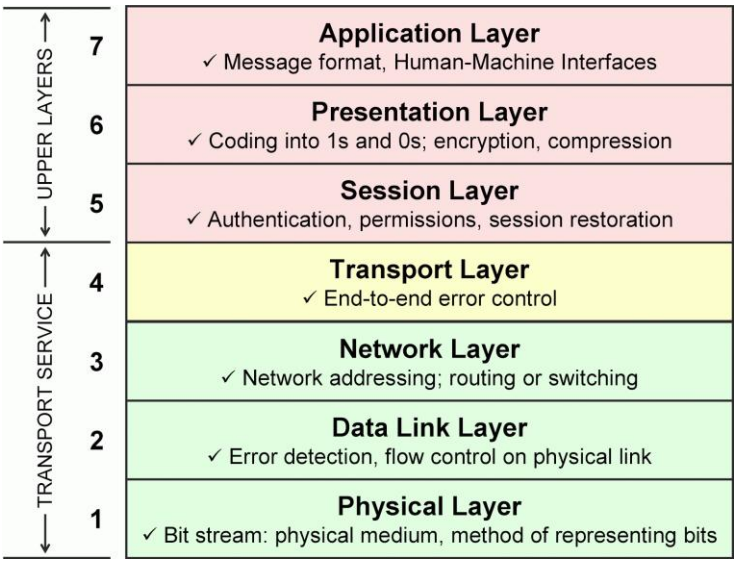
Server

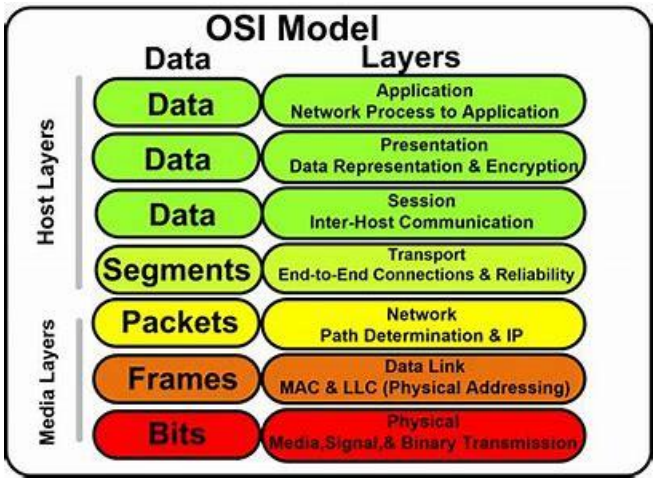
In this architecture, the client sends requests and server responds to the request of the clients.

Ex: Mail Servers, Web Servers



OSI Model (Open System Inter Connection):





OSI Model was developed by the International Organization for Standardization (ISO).

Physical Layer :

It is responsible for the actual physical connection between the devices. Responsible for transmitting individual bits from one node to another.

Infrastructure

Data Format: Bits

Data Link Layer: It is responsible for the node-to-node delivery of the message.

It has two Sub layers.

LLC (Logical Link Control)

Media Access Control (MAC)

Data Format: Frames

Network Layer: It is responsible for the transmission of data from one host to other in the network. Determining the best route for delivery

IP address Mapping -

Data Format: Packets

Windowing

Transport Layer: provides services to the application layer. Choosing right delivery method
Data Format- Segments

Protocols: TCP, UDP

Session Layer: Establishing a connection between tow devices.

Data Format - Data

Presentation Layer: Translation layer. The data extracted from the application layer will be converted into suitable format required for transmission in the network.

Formatting the letter/package

Ex: JPEG, GIF, MPEG

Application Layer: Produces data

Data Format- Data

Protocols: SMTP, FTP, DNS

Application Layer : Creates 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:

It is the process of converting data into a specific format that can be easily understood by different systems.

Encoding is without key.

Encryption:

It is the process of converting readable data (plaintext) into an unreadable format (ciphertext) using algorithms and keys.

Encryption is with key

Case Study: Transferring an email

The OSI model layers involved in the Process of sending an Email from Sender to Receiver.

Case 1 (Sender to Receiver):

1) **Application Layer:** A Separate Email is created by the Application Layer using the SMTP protocol. The Application layer places a header (encapsulation) field that contains information such as screen size and fonts, and passes the data to the Presentation layer.

2) **Presentation Layer:** This layer places header information. The text in the message is converted to ASCII. The Presentation layer will then pass the new data to the Session layer.

3) **Session Layer:** This Layer will start a new and separate session for communication between the devices and manages the flow of data in the same session only and data received from previous layer is sent to the Transportation Layer.

4) **Transportation Layer:** Here the Data received is broken into segments of Data and pushes them forward to Network Layer.

5) **Network Layer**: This Layer stores the Source and Destination addresses so a network is formed, it converts the segments received into packets.

6) **Data Layer:** The data of the packets is converted into Frames. Then the data is send to Physical Layer.

7**) Physical Layer**: The data of the Frames is converted into bit stream (the information is in binary 0's and 1's) and eventually the data is reached to the Receiver's end (teacher).

Case 2 (Receiver to Sender):

1) **Physical Layer:** The received data from the sender which is in bit stream is converted to frames and passed to Data Layer.

2) **Data Layer:** The Data Layer merges all the frames information and makes those into packets.

3) Network Layer: The packets are converted to segments and pushed forward to Transportation Layer.

4) Transportation Layer: Those received segments are combined into a single data element.

5) Session Layer: The single Data element obtained from the Transportation Layer is maintained and flowed as per the communication built in the session.

6) Presentation Layer: This Layer removes the necessary compression that were made with the Data and passes the new Data obtained to Application Layer.
7) Application Layer: The Layer will showcase the readable data at the receiver's end and eventually the email is sent and received successfully.

TCP (Transmission Control Protocol): Connection oriented protocol. Lies between Application and Network Layers. Ensures reliable and efficient data transmission over the internet.

IP (Internet Protocol): useful for sending data from one device to another over the internet. Responsible for addressing and routing packets of data.

Public IP: Understood by globally

Private IP:

Elastic IP: It is a static IPv4 address designed for dynamic cloud computing, primarily used in Amazon Web Services (AWS)

ICMP (Internet Control Message Protocol): *Network Layer protocol. It is used for error handling at the network layer.*

ARP (Address Resolution Protocol): Converting IP address into MAC address. Network Layer protocol.

IGMP (Internet Group Management Protocol): It is used by hosts and adjacent routers for multicasting communication with IP Networks.

HTTP: 80 (Web Browsing)

HTTPS: 443

NIC: Network Interface Card

Submarine Cable Map are optical fibre cables under oceans that enable global internet connectivity.

Networking Terms and Devices:

Nodes: A node is a physical or logical connection point in a computer network

Hosts: A host is a computer or other device that communicates with other hosts on a network.

Protocols: Set of Instructions and rules

Types of Networks:

LAN (Local Area Network) :
MAN (Metropolitan Area Network)
WAN (Wide Area Network)

****Why Cluster Deployment ?**

Scalability

Horizontal(Scale Out/ Scale In): Adding more machines

Load Balancer: To adjust the work load between the machines

Service Discovery: It is the technology that allows applications and microservices to **automatically detect services and devices on a computer network**

Vertical (Scale Up/ Scale Down): Adding/decreasing the capacity of the machine

Elasticity: Elasticity, on the other hand, refers to the ability of a system to dynamically adjust its resource allocation in response to changing demands

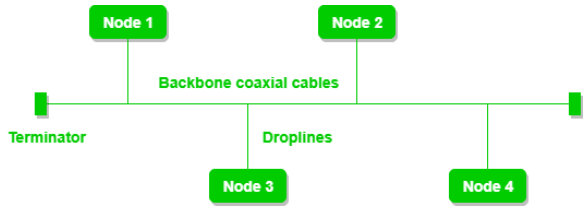
Application should be stateless to scale horizontally

Modem : Converts signals for internet access

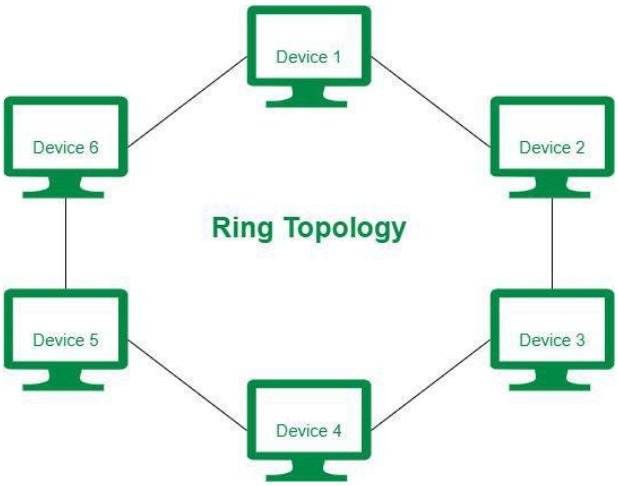
Router: Directs data between networks

Network Topologies

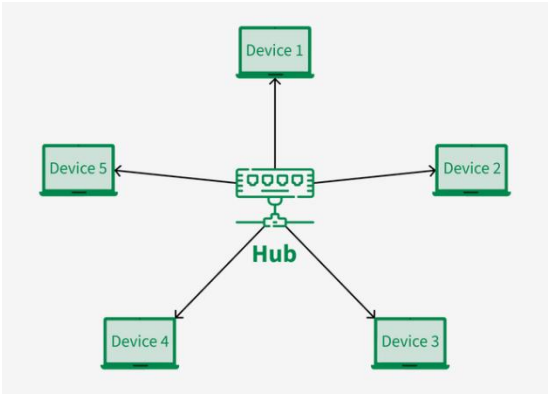
Bus Topology:



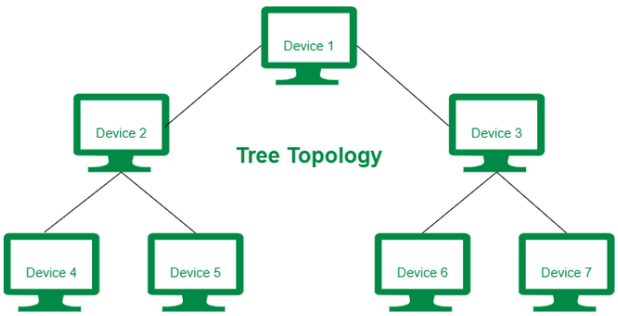
Ring Topology:



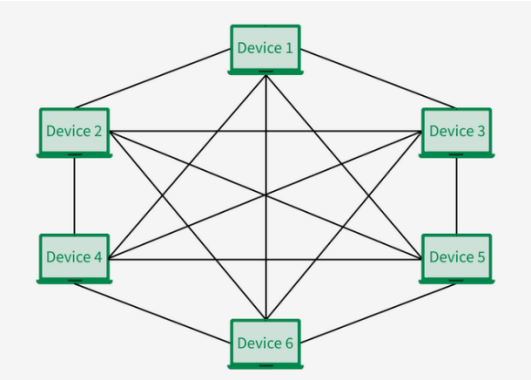
Star Topology:



Tree Topology



Mesh Topology



Peer to Peer Architecture: In this architecture each node acts as client and server.

Socket: Combination of IP address and port

Port: It is a number assigned to uniquely identify a connection endpoint

HTTP (Hyper Text Transfer Protocol):

Methods:

GET: Retrieves data

POST: Send data

PUT: Update data

DELETE: Remove data

****Richardson Maturity Model:**

‘

09/01/2025

HTTP Error/Status Codes

1xx – Informational Response

2xx – Success

3xx – Redirection

4xx – Client Errors

5xx – Server Errors

1. 200 (Success/ Ok)
2. 301 (Permanent Redirect)
3. 302 (Temporary Redirect)
4. 304 (Not Modified)
5. 400 (Bad Request)

Cookies: Cookies are small text files of information created/updated when visiting a website and stored on the user's web browser.

Different Types of cookies:

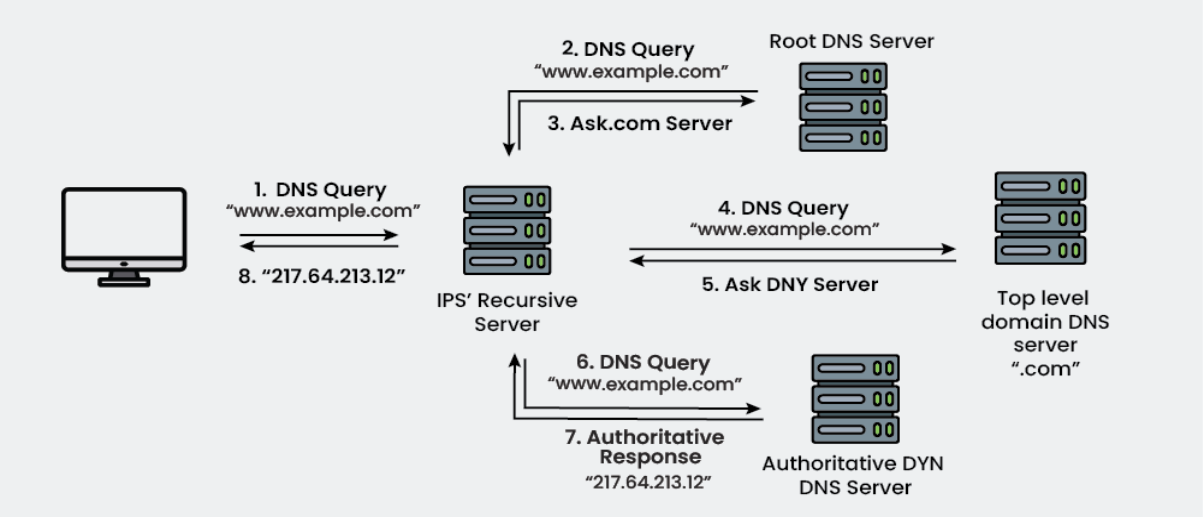
Session Cookies: Session cookies are also known as temporary cookies which are present as long as the user browser is open.

Persistent Cookies: Stored more than session cookies for a specific period of time like less than 6 months

First party Cookies: These cookies are set by the website that you are currently visiting

Third party cookies: These cookies are set by the domains that you are not visiting. Mostly used for cross-site tracking and advertising purposes.

DNS



VPN (Virtual Private Network): allows a user to connect to a private network over the Internet securely and privately.

Types of VPNs

Remote Access VPNs: Allows a user to connect to a private network and access its services and resources remotely.

Site to site VPNs: Connects two or more networks together.

Cloud VPNs: Provides secure connections to cloud-based resources

Mobile VPNs: Designed for mobile devices.

SSL VPNs: Uses SSL encryption for secure access.

Double VPNs: A double VPN connection is one where an internet connection is run through two VPN servers operated by the same VPN service, one after the other.

Checksum: Error Detection scheme used in IP, TCP, UDP.

In this checksum, the data is divided into K segments each of 'm' bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. At the reciever's end, all data segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero the data is accepted otherwise discarded.

Ex:

If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.

Sender Site:

10101001 subunit 1

00111001 subunit 2

11100010 sum (using 1s complement)

00011101 checksum (complement of sum)

Data transmitted to Receiver is:

10101001 00111001 || 00011101

Receiver Site:

10101001 subunit 1

00111001 subunit 2

00011101 checksum

11111111 sum

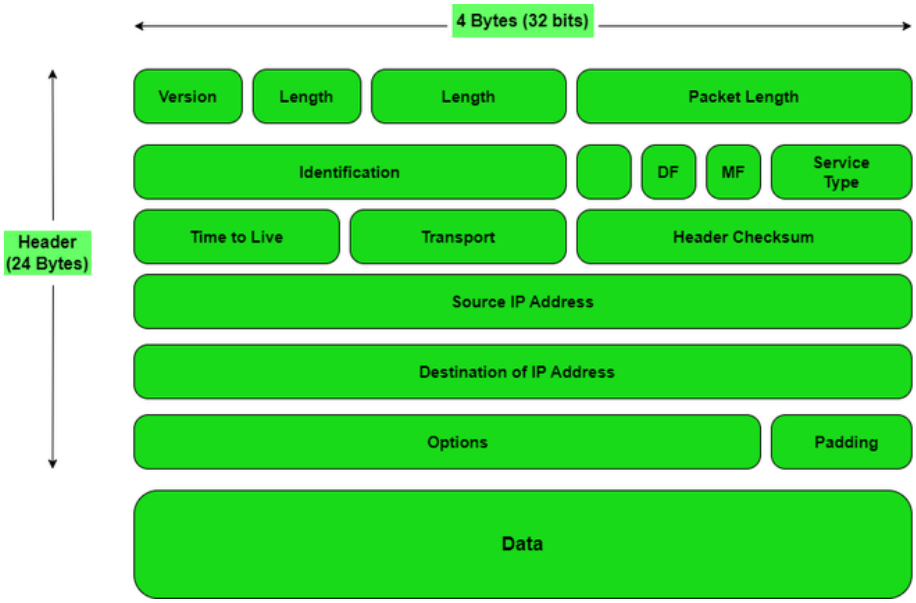
00000000 sum's complement

Result is zero, it means no error.

Internet Protocol: responsible for delivering packets from the source host to the destination host based on their IP addresses.

IP Building Blocks

IP Packet Structure: IP packet is the basic unit of data transmission in an IP Network.



ICMP, PING, TraceRoute

ICMP: Used to find errors

Ping: check the reachability of a server

ICMP Echo Request

Working:

When you run a Ping command, it sends **Internet Control Message Protocol (ICMP)** echo requests to the target IP address or domain. The recipient responds with an **echo reply**, and Ping calculates the time it took for the packet to travel to the destination and back. The result is displayed in terms of **round-trip time (RTT)**, usually measured in milliseconds (ms).

TraceRoute: used to trace the path that packets take from your computer to a remote server or host.

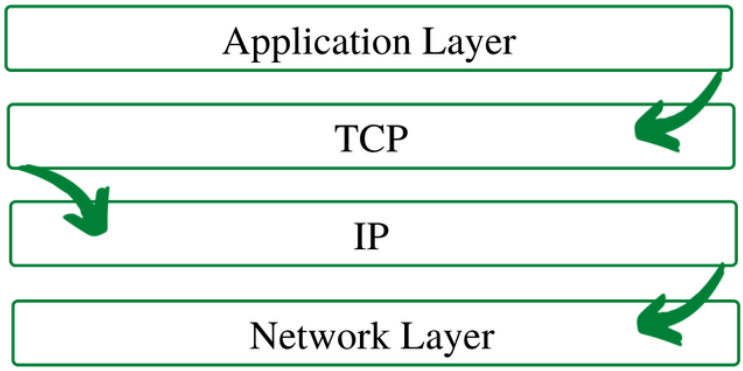
Working:

works by sending **ICMP Echo Requests** (or other types of packets, depending on the OS) with an initial **Time To Live (TTL)** value. TTL is a field in the packet header that limits the number of hops the packet can make before being discarded. Each time a packet reaches a router or hop, the router decreases the TTL by 1 and sends a message back to the sender. If TTL expires, the router sends back a **Time Exceeded** message.

By gradually increasing the TTL, traceroute determines the path of the packet across the network and displays the **round-trip time** for each hop, allowing you to see the exact path and performance at each step.

ARP (Address Resolution Protocol): Maps IP addresses to MAC addresses, data link layer

TCP : Connection Oriented protocol for communications



Application Layer

Transport Layer

Network Layer

Data Link Layer

IP Addressing and Subnetting

CIDR Notation	Subnet Mask	Subnet Bit	Usable Hosts
/32	255.255.255.255	0	1
/31	255.255.255.254	1	2
/30	255.255.255.252	2	4
/29	255.255.255.248	3	8
/28	255.255.255.240	4	16
/27	255.255.255.224	5	32
/26	255.255.255.192	6	64
/25	255.255.255.128	7	128
/24	255.255.255.0	8	256

Network Architecture and Models

NAT (Network Address Translation): 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.

NATTING
DENATTING

Default Route: It is the route which is sent when all possible ways are closed.

SSL (Secure Socket Layer): provides security to the data that is transferred between web browser and server.

TLS (Transport Layer Security): Derived from a SSL.

PAT (Personal Access Token)

****Difference Between SSL & TLS ??**

Symmetric 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.

Examples: AES, DES, 3DES

The Mathematical Representation is as follows-

P = D (K, E(K, P))

where K –> encryption and decryption key

P –> plain text

D –> Decryption

E(K, P) –> Encryption of plain text using K

Asymmetric Encryption: one key is used to encrypt data and the second one is used to decrypt an encrypted text. (Public Key & Private Key)

Ex: RSA, Diffie-Hellman

The Mathematical Representation is as follows-

P = D (K, E(K, P))

where K –> encryption and decryption key

P –> plain text

D –> Decryption

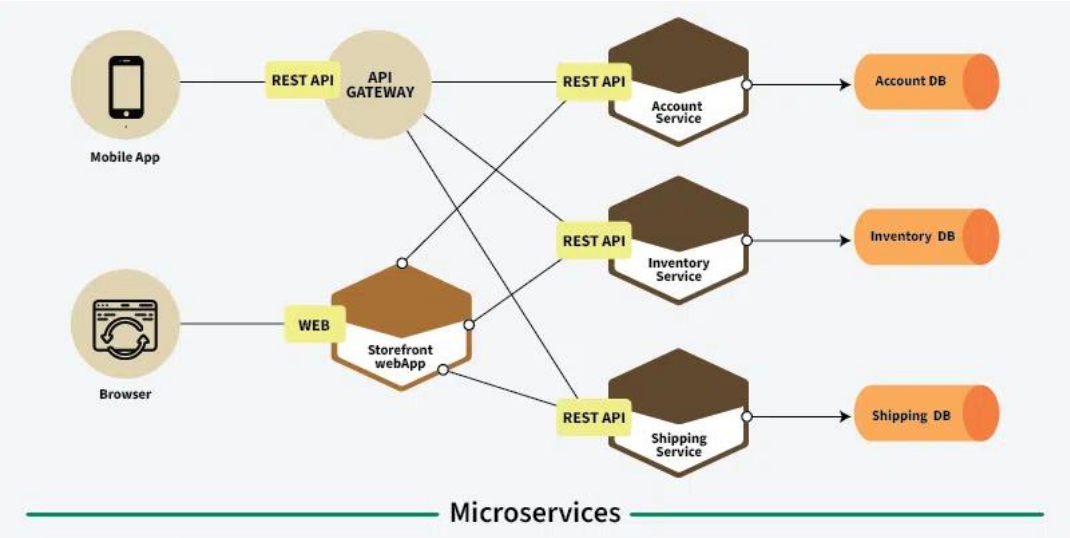
E(K, P) –> Encryption of plain text using K

Microservices

Load Balancing: Path based routing, Service Level Routing

Monolith: Everything packaged into single.

Microservice: is a small, loosely coupled service that is designed to perform a specific business function and each microservice can be developed, deployed, and scaled independently.



Synchronous Communication: Waiting for response.

Asynchronous Communication: Not waiting for response.

Different types of Asynchronous Communication:

1. Publish Subscribe Model: In this model the user should subscribe to the topic. If something has come then the user is notified.
2. Queue Model: In this model subscriber goes and check every time whether they got something or not
   Ex: SQS

Splunk: is the "Google for log files" heavyset enterprise tool that was the first log analysis software

ELK: The ELK Stack is a set of three open-source products—Elasticsearch, Logstash and Kibana—all developed and maintained by Elastic

DynaTrace

Externalizing logs

Event Sync

Scheduling

10/1/2025

Firewalls: Acts like a security guard. It is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization.

Checks

Ingress, egress

Filter

based on IP address.

Port

Protocol

Types of Firewalls:

1. **Packet Filtering Firewall:** It is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports.
2. **Stateful Inspection Firewall:** These firewalls are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient.

Stateful Firewalls

Stateless Firewalls

Server Farm:

Collection of physical servers that work together to deliver services, applications or data.

IPSec (Internet Protocol Security): Suite of protocols designed to secure networks. It is important because it helps to keep your data safe and secure when you send it over the internet.

Threat: A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system.

Vulnerability: It is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals

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

Risk = Vulnerability x Threat

Defence in Depth: It is an information security approach in which a series of security mechanisms and controls are thoughtfully layered throughout a computer network to protect the CIA and data.

Reverse Proxy: It is a server that sits in front of web servers and forwards client (e.g. web browser) requests to those web servers.

IPv4 vs IPv6

IPv4:

32 Bit

IPv6:

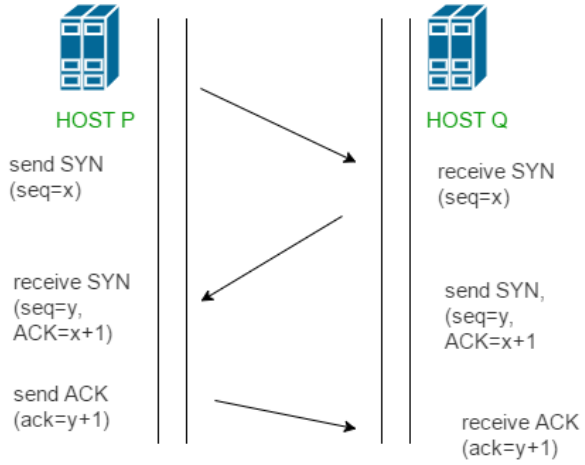
128 Bit

Hexadecimal

Offers more built-in security features.

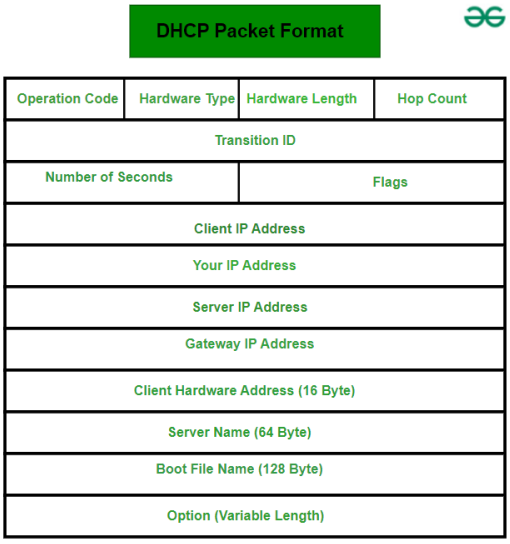
CIDR (Classless Inter Domain Routing): It is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses.

3-Way Handshake: It is used to establish a connection between two clients.



WiFi 802.11:

DHCP (Dynamic Host Configuration Protocol): it is a network protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices (such as computers, smartphones, and printers) on a network.



FTP (File Transfer protocol)

Richardson Maturity Model

12 Factor App:

I. Codebase

One codebase tracked in revision control, many deploys

II. Dependencies

Explicitly declare and isolate dependencies

III. Config

Store config in the environment

IV. Backing services

Treat backing services as attached resources

V. Build, release, run

Strictly separate build and run stages

VI. Processes

Execute the app as one or more stateless processes

VII. Port binding

Export services via port binding

VIII. Concurrency

Scale out via the process model

IX. Disposability

Maximize robustness with fast startup and graceful shutdown

X. Dev/prod parity

Keep development, staging, and production as similar as possible

XI. Logs

Treat logs as event streams

XII. Admin processes

Run admin/management tasks as one-off processes

VLAN (Virtual Local Area Network): It is a logical grouping of devices within a network that allows them to communicate as if they were on the same physical LAN, even if they are not.

WLS (Windows Subsystem for Linux): Windows Subsystem for Linux (WSL) is a feature of Windows that allows you to run a Linux environment on your Windows machine, without the need for a separate virtual machine or dual booting

Port Forwarding: Port forwarding is a network technology procedure that enables external devices to access services on a private network.

SMTP/IMAP/POP3

Linters

11/01/2025

Data Centre: A data center is a centralized facility equipped with computing resources such as servers, storage systems, networking equipment, and cooling infrastructure that is used for the delivery of cloud services over the Internet.

Key Components:

- **Servers**: Physical or virtual machines running applications and services.
- **Storage Systems**: Hardware or cloud-based solutions used to store data.
- **Network Equipment**: Routers, switches, and other devices used to connect systems within and outside the data centre.
- **Power Infrastructure**: Uninterrupted power supply, power distribution units, etc., to ensure constant power availability.
- **Cooling Systems**: Air conditioning, cooling towers, and related technologies to maintain an optimal temperature.
- **Security Systems**: Physical security, network security, firewalls, surveillance, etc., to safeguard the data centre.

Types of Data Centre:

On-Premises Data Centre:

- **Owned and Operated**: Owned and managed by the organization.
- **Complete Control**: Full control over hardware, software, and security.
- **High Initial Investment**: Significant upfront costs for infrastructure.
- **Suitable for**: Organizations with high security and compliance needs.

Colocation Data Centre:

- **Rented Space**: Companies rent space in a third-party data centre.
- **Lower Investment**: Lower capital costs than building an on-premises data centre.
- **Shared Infrastructure**: Resources are shared with other clients.

Cloud Data Centre:

- **IaaS, PaaS, SaaS**: Provides infrastructure, platform, and software services.
- **Virtualized Infrastructure**: Provides virtualized resources over the internet.
- **Pay as You Go**: Scalable, pay-per-use model.
- **High Scalability**: Easily scalable depending on demand.

Key Considerations of Data Centres:

- **Reliability**: Ensuring continuous uptime and availability.
- **Security**: Protecting data and physical assets from threats.
- **Scalability**: Ability to scale infrastructure as demand grows.
- **Energy Efficiency**: Reducing power consumption and carbon footprint.

- **Disaster Recovery**: Ability to recover from hardware failure or disasters.

Data Centre Infrastructure

1. **Power Infrastructure:**
    - **Uninterruptible Power Supply (UPS)**: Ensures power continuity during outages.
    - **Power Distribution Units (PDU)**: Distributes electricity to servers and systems.
    - **Power Monitoring**: Tracks power usage and ensures efficiency.
    - **Redundancy**: Backup systems (e.g., generators) to ensure uptime.
2. **Cooling Infrastructure:**
    - **Air Conditioning Units**: Maintain temperature within optimal levels.
    - **Cooling Towers**: Help remove excess heat from the data centre.
    - **Hot and Cold Aisle Containment**: Separates hot and cold air to optimize cooling efficiency.
3. **Space Management:**
    - **Modular Design**: Flexible infrastructure that can expand as needed.
    - **Cable Management**: Organized routing and management of cables.
    - **Raised Floors**: Provides space for cables and air circulation beneath the floor.

Types of Data Storage:

- **Primary Storage**: Direct access storage for active data (e.g., hard drives, SSDs).

Types of Storage:

- **DAS (Direct Attached Storage)**: Directly connected storage to a server or computer.
- **NAS (Network Attached Storage)**: Storage that is connected to a network and can be accessed by multiple devices.
- **SAN (Storage Area Network)**: High-speed network connecting servers to storage devices.

RAID (Redundant Array of Independent Disks):

1. **RAID 0 (Striping)**: Data is divided and stored across multiple disks for improved performance (no redundancy).
2. **RAID 1 (Mirroring)**: Data is duplicated across two or more disks for redundancy.
3. **RAID 5 (Block-level Striping with Parity)**: Data is striped across multiple disks, with parity distributed for redundancy (needs at least 3 disks).
4. **RAID 6 (Block-level Striping with Double Parity)**: Similar to RAID 5, but with two sets of parity for added fault tolerance (needs at least 4 disks).
5. **RAID 10 (Combination of RAID 1 and RAID 0)**: Combines the mirroring of RAID 1 and the striping of RAID 0 for both performance and redundancy (needs at least 4 disks).

Backup and Recovery:

Recovery Time Objective: target time within which a system or application must be restored after an outage.

Recovery Point Objective: The maximum amount of data loss that an organization can tolerate

Backup Types:

- **Full Backup**: A complete backup of all data.
- **Incremental Backup**: Backs up only the data changed since the last backup (full or incremental).
- **Differential Backup**: Backs up data changed since the last full backup.

Backup Strategies:

3-2-1 Backup Strategy:

Keep 3 copies of data.

Store on 2 different types of media (e.g., hard drive and cloud).

Keep 1 copy off-site for disaster recovery

Servers:

- **Types of Servers:**

- **Dedicated Servers**: Servers dedicated to a single organization.

- **Virtual Servers**: Multiple virtual machines run on a physical server, sharing resources.

Load Balancing:

Distributes traffic across multiple servers to ensure high availability and performance.

Load Balancing Methods:

- **Round Robin**: Distributes traffic evenly to all servers.
- **Least Connection**: Directs traffic to the server with the fewest active connections.
- **Least Response Time**: Routes traffic to the server with the fastest response time.
- **Source IP Hashing**: Routes traffic based on the source IP address.
- **Weighted Round Robin**: Routes more traffic to servers with higher capacities.

Types of Load Balancers:

- **Hardware Load Balancers**: Physical devices used to distribute traffic.
- **Software Load Balancers**: Load balancing done via software on general-purpose hardware.