NETWORKING FOR DEVOPS

What is a Network?

When two or more computers and computing devices connected together with each other through communication channels, such as cables or wireless media and sharing some files, then it is called a Network

A network is used to:

- Allow the connected devices to communicate with each other.
- Enable multiple users to share devices over the network, such as music and video servers, printers and scanners.

The Internet is the largest network in the world and can be called "the network of networks".

Types of Networks

There are different types of networks. But the main two are LAN and WAN

1. LAN (Local Area Network) - interconnects computer within a limited area, such as residences, schools. e.g. Wi-Fi, Ethernet
2. MAN (Metropolitan area network) - used in metropolitan area (cities).
3. WAN (Wide Area Network) - extends LAN over a large geographic area. e.g:- optical fiber cable
4. SONET (Synchronous Optical Network) - used in submarine.

Network Components:

1. Router: Think of this as a traffic controller. It directs information between different networks, like making sure the data from your home network finds its way to the websites you want to visit and back.

2. Switch: Like a postal sorting centre for your local network. It connects different devices within the same network (like your computer, printer, and smart TV) and makes sure data gets to the right device.

3. Modem: The translator between your home network and the internet. It converts the internet signal from your service provider into something your devices can understand.

4. Network Cable (Ethernet): The physical road that data travels on. Just like cars need roads, data needs cables to move between devices when using wired connections.

5. Wireless Access Point (WAP): Think of this as a radio tower for your network. It broadcasts your network signal wirelessly so devices can connect without cables. Your home WiFi router usually includes this.

6. Firewall: The security guard of your network. It watches data coming in and going out, blocking anything suspicious that might harm your network.

7. Network Card: Every device's ticket to join the network. It's like having the right pass to enter a club - without it, your device can't connect to the network. It is known as Network Interface Card which is used to connect your computer with the internet. It is wireless card preinstalled on motherboard now-a-days. It has a MAC (Media Access Control) address.

8. Server: Like a library of information and services. It stores files, runs applications, and provides services that other computers on the network can use.

What is Protocol?

A network protocol is a set of rules which is set up by people that determine how a particular data is transmitted between different devices in the same network.
e.g. HTTP, TCP, IP, FTP, SMTP etc.

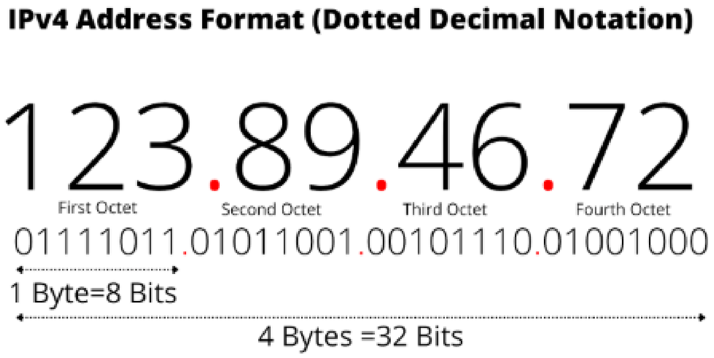
IP Address and its Types and Classes:

IP Address: An IP (Internet Protocol) address is a unique number assigned to each device on a network, allowing them to communicate with each other. Its like a device's "address" on the internet or local network.

Types of IP Addresses

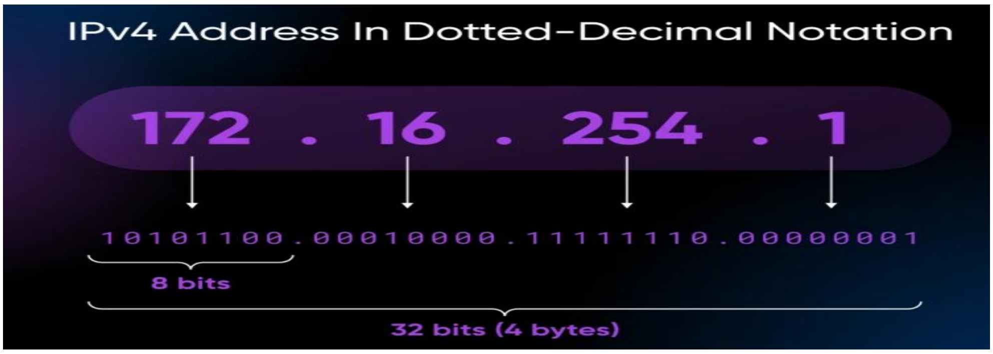
IPv4:

- 32-bit address, written as four numbers separated by dots (e.g., 123.89.46.7).
- This is a 32-bit IP address, means it contains a combo of 32 (1 and 0's). In this version of IP address there are 4 groups or Octets(8 bits), and each octet is represented by a decimal value in the address. It is easy to remember.
- Commonly used, but limited number of addresses (about 4.3 billion)



IPv6:

- 128-bit address, written in eight groups of hexadecimal numbers
- Provides a vastly larger pool of addresses, designed to replace IPv4 as it runs out.

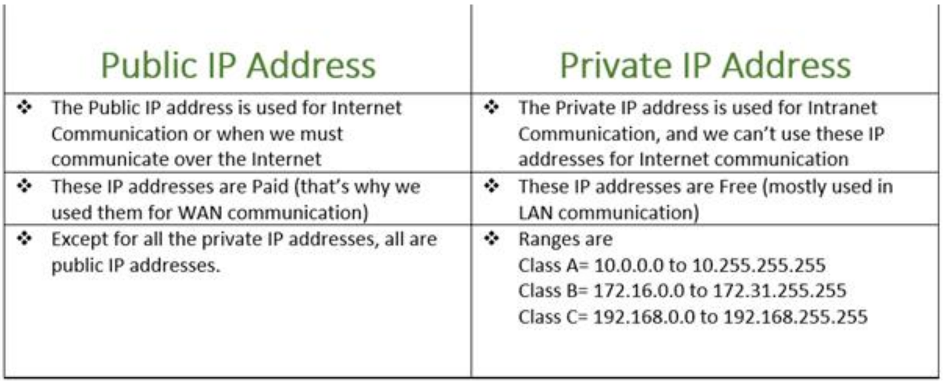


Public IP:

- Used to identify devices on the internet.
- Assigned by ISPs and accessible globally.

Private IP:

- Used within private networks (like home or office networks).
- Not accessible from the internet; usually in ranges like 192.168.x.x , 10.x.x.x , or 172.16.x.x - 172.31.x.x .



Public IP Address	Private IP Address
❖ The Public IP address is used for Internet Communication or when we must communicate over the Internet	❖ The Private IP address is used for Intranet Communication, and we can't use these IP addresses for Internet communication
❖ These IP addresses are Paid (that's why we used them for WAN communication)	❖ These IP addresses are Free (mostly used in LAN communication)
❖ Except for all the private IP addresses, all are public IP addresses.	❖ Ranges are Class A= 10.0.0.0 to 10.255.255.255 Class B= 172.16.0.0 to 172.31.255.255 Class C= 192.168.0.0 to 192.168.255.255

Static IP:

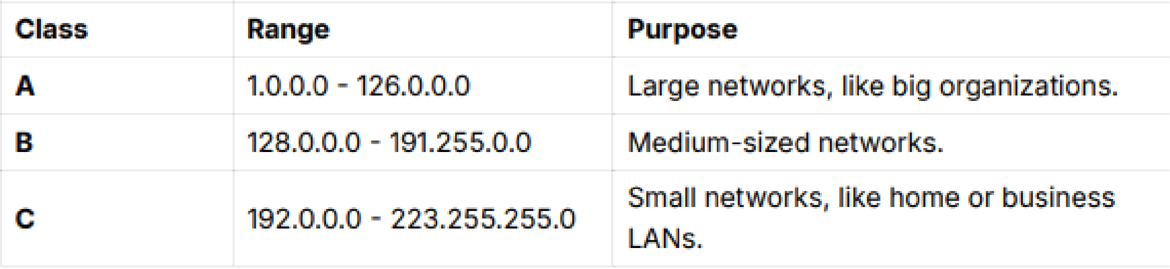
- Manually assigned, doesnt change.
- Often used for servers and devices that need a consistent address.

Dynamic IP:

- Automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server.
- Changes periodically; commonly used for home devices.

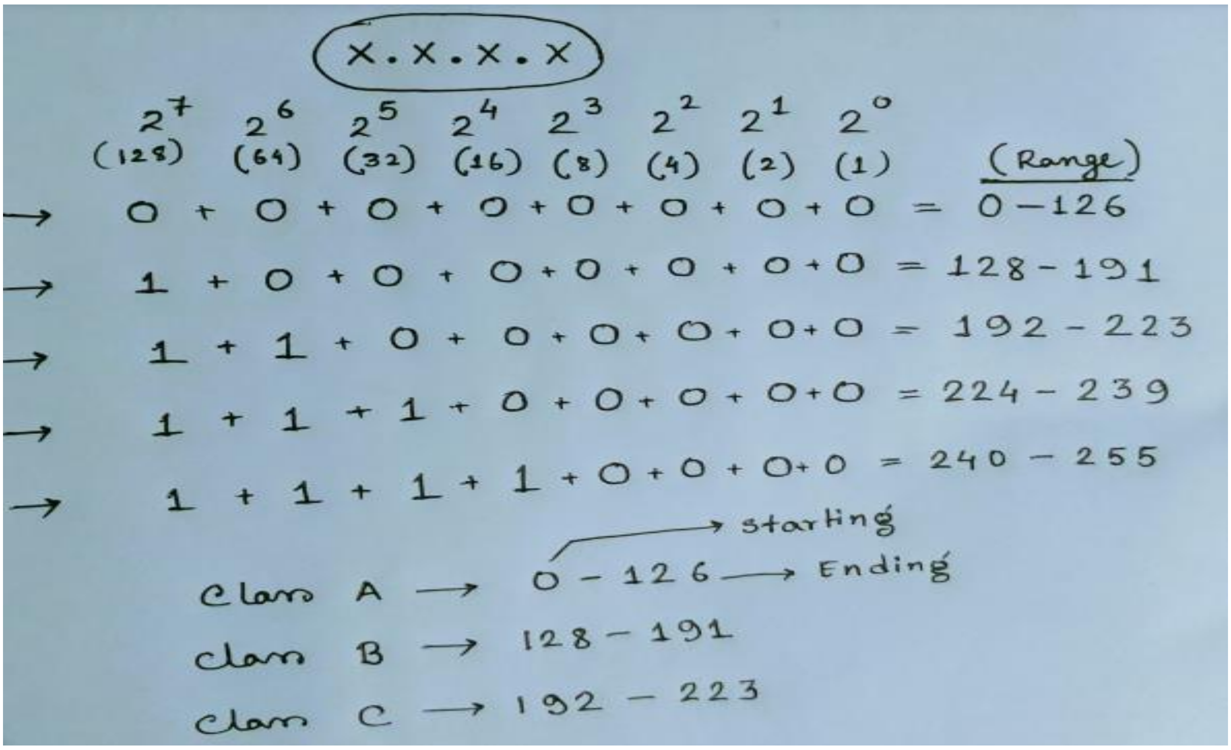
IP Address Classes (IPv4 Only)

There is an organization called IANA(Internet Assigned Numbers Authority) who divides the IP address into different classes. You have to know about binary to decimal conversion to understand this. IPv4 addresses are divided into five classes based on the starting number, which determines their usage in networks.



Class	Range	Purpose
A	1.0.0.0 - 126.0.0.0	Large networks, like big organizations.
B	128.0.0.0 - 191.255.0.0	Medium-sized networks.
C	192.0.0.0 - 223.255.255.0	Small networks, like home or business LANs.

D	224.0.0.0 - 239.255.255.255	Reserved for multicasting.
E	240.0.0.0 - 255.255.255.255	Experimental, used for research.



X.X.X.X

2^7 (128)	2^6 (64)	2^5 (32)	2^4 (16)	2^3 (8)	2^2 (4)	2^1 (2)	2^0 (1)	(Range)
→ 0 +	0 +	0 +	0 +	0 +	0 +	0 +	0	= 0 – 126
→ 1 +	0 +	0 +	0 +	0 +	0 +	0 +	0	= 128 – 191
→ 1 +	1 +	0 +	0 +	0 +	0 +	0 +	0	= 192 – 223
→ 1 +	1 +	1 +	0 +	0 +	0 +	0 +	0	= 224 – 239
→ 1 +	1 +	1 +	1 +	0 +	0 +	0 +	0	= 240 – 255

Class A → 0 – 126 (0 → starting, 126 → Ending)

Class B → 128 – 191

Class C → 192 – 223

Note:

- Class A addresses in IPv4 officially start from 1.0.0.0 and go up to 126.0.0.0. The address 0.0.0.0 is not part of the Class A range and has a special purpose in networking.is a special address, not part of the usable IP address range in Class A. The 127.0.0.0 to 127.255.255.255 range, especially 127.0.0.1, is reserved for loopback addresses in IPv4.

What is Loopback?

- Loopback address allows a device to communicate with itself.
- Its often used for testing network software on the local machine.

Key Points:

- 127.0.0.1 is commonly known as "localhost." Any IP address in the 127.x.x.x range will loop back to the same device.
- Useful for testing networking applications without needing an external network

IP address Network ID and Host ID:

There are two parts to an IP address Network ID and Host ID (Any device which gets the IP address is called a Host).

- The Network ID portion differs depending on the IP class
    - Class A : 1st octet is the Network ID.
    - Class B : 1st and 2nd octets are the Network ID.
    - Class C : 1st, 2nd, and 3rd octets are the Network ID.
- Direct Connection Devices with the same Network ID can connect without a router.
- Router Requirement Devices with different Network IDs need a router to connect.

Subnet:

A subnet or subnetwork is a smaller network inside a large network. Subnetting makes network routing much more efficient.

Example:

You have a network: **192.168.1.0/24**

- This means you have **256 IP addresses** (from 192.168.1.0 to 192.168.1.255).
- You want to divide this into **4 equal subnets** to organize your devices (e.g., one subnet for printers, one for computers, etc.).

Step 1: Divide the Network

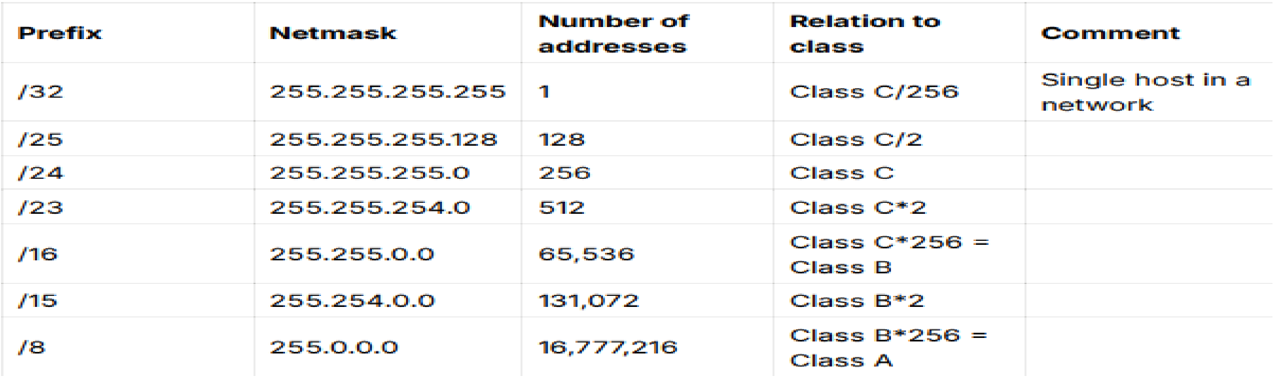
To create 4 subnets, each subnet will have **64 IP addresses**. Here's how the subnets look:

1. **192.168.1.0/26** → IPs: 192.168.1.0 to 192.168.1.63
2. **192.168.1.64/26** → IPs: 192.168.1.64 to 192.168.1.127
3. **192.168.1.128/26** → IPs: 192.168.1.128 to 192.168.1.191
4. **192.168.1.192/26** → IPs: 192.168.1.192 to 192.168.1.255

Step 2: Assign Subnets

- Subnet 1: For printers
- Subnet 2: For computers
- Subnet 3: For Wi-Fi devices
- Subnet 4: For servers

CIDR (Classless Inter-Domain Routing): CIDR Classless Inter-Domain Routing) is a method for allocating IP addresses and IP routing that replaces the older classful network system. It was introduced to improve IP address utilization and simplify routing.



Prefix	Netmask	Number of addresses	Relation to class	Comment
/32	255.255.255.255	1	Class C/256	Single host in a network
/25	255.255.255.128	128	Class C/2	
/24	255.255.255.0	256	Class C	
/23	255.255.254.0	512	Class C*2	
/16	255.255.0.0	65,536	Class C*256 = Class B	
/15	255.254.0.0	131,072	Class B*2	
/8	255.0.0.0	16,777,216	Class B*256 = Class A	

/0	0.0.0.0	4,294,967,296	Class A*256	0.0.0.0/0 means entire internet. Often used in public firewall rules

Network Models

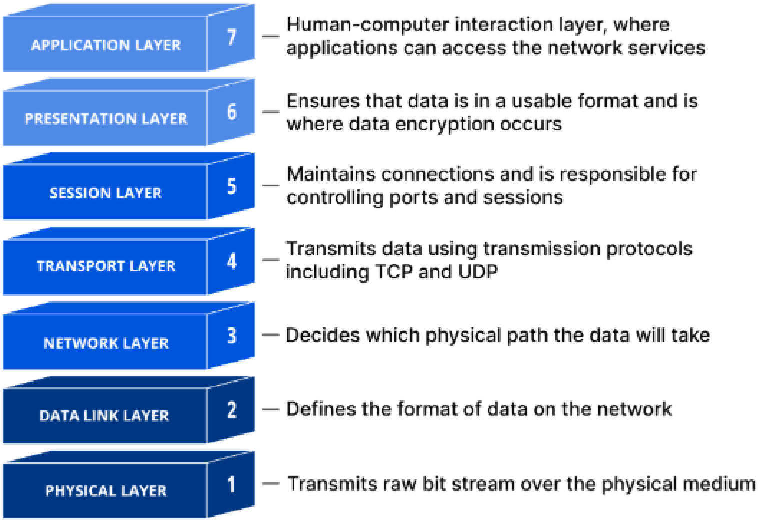
There are mainly two types of network model –

1. OSI Reference Model
2. TCP/IP Model

1. OSI Reference Model:

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

1. **Physical Layer** Handles the physical connection between devices, transmitting raw data as bits over cables, radio signals, etc.
2. **Data Link Layer** Manages data transfer between directly connected nodes. It handles error detection and flow control. Examples: Ethernet, Wi-Fi.
3. **Network Layer** Manages packet forwarding and routing through the network. Uses IP addressing. Example: IP Internet Protocol).
4. **Transport Layer** Ensures reliable data transfer with error correction and flow control. Examples: TCP, UDP.
5. **Session Layer** Establishes, maintains, and manages communication sessions between applications.
6. **Presentation Layer** Translates data formats to ensure compatibility between systems. Handles encryption and compression. Example: SSL/TLS.
7. **Application Layer** Interfaces directly with the user and provides network services like HTTP, FTP, SMTP.


APPLICATION LAYER
7
Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER
6
Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER
5
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
4
Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER
3
Decides which physical path the data will take
DATA LINK LAYER
2
Defines the format of data on the network
PHYSICAL LAYER
1
Transmits raw bit stream over the physical medium

Below is the list of protocols in each layer of the OSI model along with their port numbers (where applicable):

1. Application Layer (Layer 7)

- HTTP Port 80 Web browsing.
- HTTPS Port 443 Secure web browsing.
- SMTP Port 25 Sending email.
- FTP Ports 20, 21 File transfer.
- DNS Port 53 Domain name resolution.
- POP3 Port 110 Receiving email. IMAP Port 143 Receiving email.

2. Presentation Layer (Layer 6)

- SSL/TLS Port 443 for HTTPS, also used in other protocols): Encryption for secure data transmission.
- MIME Used for formatting email attachments.
- JPEG/PNG Image formats used to encode multimedia files.

3. Session Layer (Layer 5)

- PPTP Port 1723 Tunneling protocol for VPNs.
- NetBIOS Ports 137, 138, 139 Establishes sessions for network communications.

4. Transport Layer (Layer 4)

- TCP Reliable data transmission with acknowledgment.
- UDP Fast, connectionless data transmission without acknowledgment.
- SCTP Used for applications that require multiple data streams.

5. Network Layer (Layer 3)

- IP (IPv4/IPv6) Routing packets between source and destination.
- ICMP Error messaging and diagnostics (e.g., ping).
- IGRP Routing protocol used for sharing routing information.

6. Data Link Layer (Layer 2)

- Ethernet Defines physical addressing and channel access.
- PPP Used for point-to-point connections.
- HDLC For framing and error control on point-to-point links. ARP Resolves IP addresses to MAC addresses.

7. Physical Layer (Layer 1)

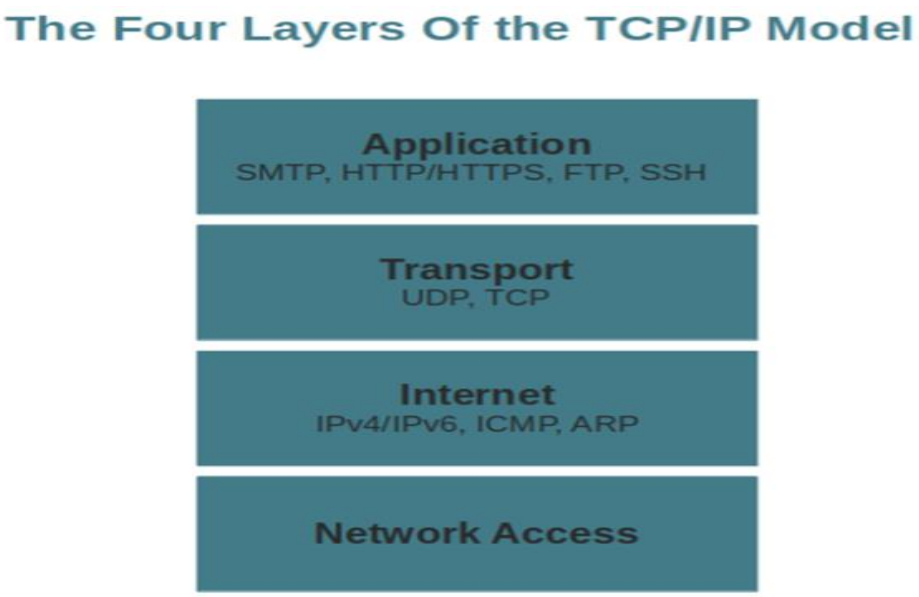
- Ethernet Physical signalling) Specifies electrical signals, cabling, etc.
- USB Used to physically connect devices.

2. TCP/IP Model: The TCP/IP model, also known as the Internet Protocol Suite, is a simplified version of the OSI model with only 4 layers instead of 7. This model is a real model which actually works in real. This model consists of 4 layers.

- Application Layer = Application Layer (Presentation Layer Session Layer) of OSI model
- Transport Layer

- Network Layer

Network Interface Layer = Data Link Layer Physical Layer) of OSI model



Web Services

- HTTP: Port 80 (TCP)
- HTTPS: Port 443 (TCP)
- HTTP Alternative: Port 8080 (TCP)
- HTTP Development: Port 3000 (TCP)

Database Ports

- MySQL/MariaDB: Port 3306 (TCP)
- PostgreSQL: Port 5432 (TCP)
- MongoDB: Port 27017 (TCP)
- Redis: Port 6379 (TCP)
- Elasticsearch: Port 9200 (HTTP), 9300 (TCP)

Remote Access

- SSH: Port 22 (TCP)
- Telnet: Port 23 (TCP, not recommended for security)

Email Related

- SMTP: Port 25 (TCP)
- SMTP Submission: Port 587 (TCP)
- SMTP SSL: Port 465 (TCP)

Container & Orchestration

- Docker Daemon: Port 2375 (without TLS), 2376 (with TLS)
- Kubernetes API: Port 6443 (TCP)
- Kubernetes Kubelet: Port 10250 (TCP)
- Kubernetes NodePort Range: 30000-32767

Monitoring & Logging

- Prometheus: Port 9090 (TCP)
- Grafana: Port 3000 (TCP)
-

File Transfer

- FTP: Port 21 (Control), Port 20 (Data) (TCP)
- SFTP: Port 22 (TCP)
- FTPS: Port 990 (TCP)

Common Protocols Used

- TCP (Transmission Control Protocol)

- UDP (User Datagram Protocol)

- HTTP/HTTPS (Hypertext Transfer Protocol/Secure)

- SMTP (Simple Mail Transfer Protocol)

- SSH (Secure Shell)

- FTP (File Transfer Protocol)

- AMQP (Advanced Message Queuing Protocol)

- gRPC (Google Remote Procedure Call)

- WebSocket

DNS (Domain Name System):

- DNS Domain Name System) translates human-readable domain names (e.g., www.example.com) into IP addresses (for example, 192.0.2.44.)
- Root DNS Server stores all the Top-level domain e.g : - .com, .in, .org, .io etc.
- DNS works like the phonebook of the internet, allowing humans to use readable names while machines use numerical addresses.

How DNS Works

- When you type a website address (e.g., www.example.com) into your browser, it needs to know the IP address of that server.

- The DNS process involves looking up the domain name and finding the corresponding IP address through multiple DNS servers.

Example: Visiting a Website

1. User Request:

You type www.example.com into your web browser.

2. DNS Query:

Your browser sends a request to a DNS server to get the IP address of www.example.com

3. DNS Resolution:

The DNS server checks if it has the IP address cached. If not, it contacts other DNS servers (root, TLD, and authoritative servers) to find the IP address.

4. IP Address Found:

Once the IP address (e.g., 93.184.216.34) is found, the DNS server sends it back to your browser.

5. Connecting to the Website:

The browser uses this IP address to connect to the web server, and the website loads on your screen .

Domains, Zones, and Delegation:

1. Domains

   Domains are like branches in a tree-like structure of the internet. The root domain is the highest level, followed by top-level domains TLDs) like .com , .org , etc. Subdomains (e.g., example.com) branch off from TLDs.

2. Zones

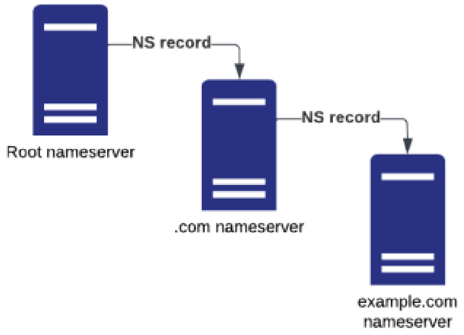
   A zone is a portion of the domain that is managed by a specific organization. For instance, .com is a zone controlled by Verisign. ICANN manages the root zone at the top of the DNS tree, while different organizations manage subdomains.

3. Delegation:

   Delegation allows one organization to hand over control of part of its domain to another organization. This is done using Nameserver NS records.

- For example, ICANN controls the root domain and delegates .com to Verisign.
- Verisign can then delegate control over example.com to "Example Ltd" by adding an NS record those points to their nameserver.

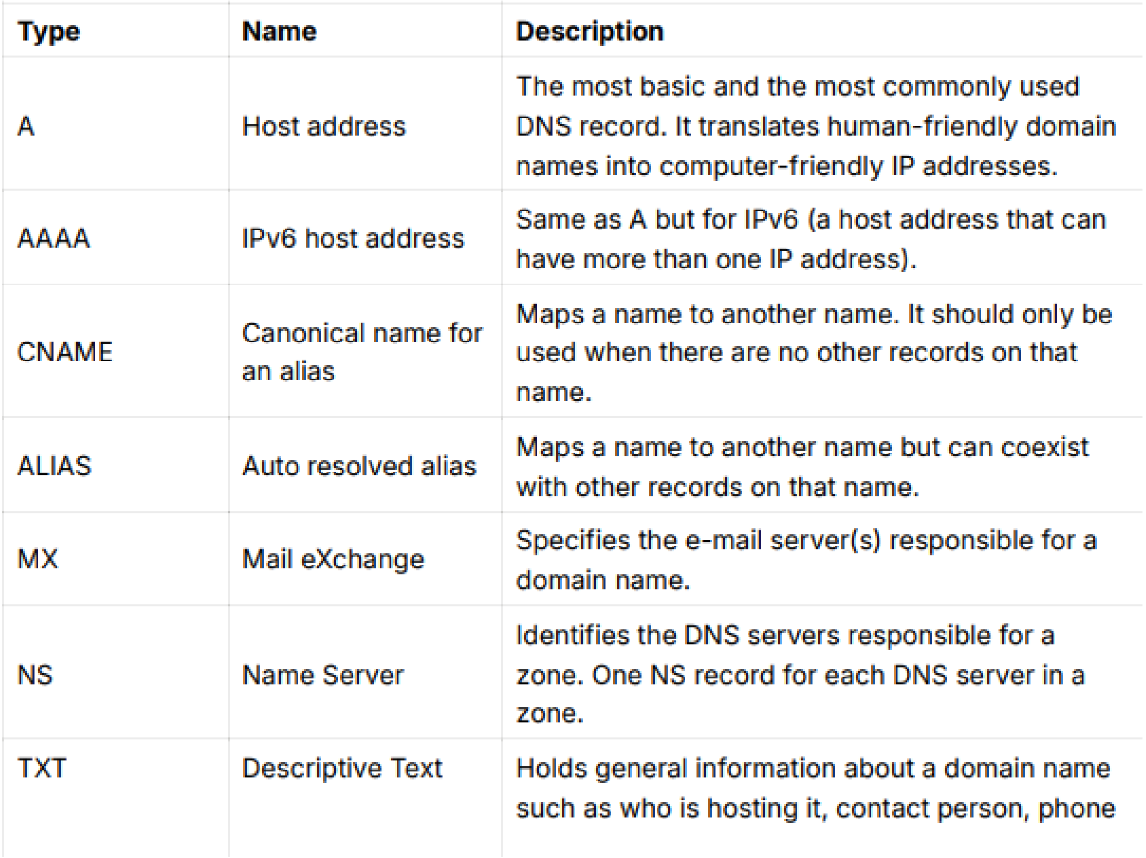
  The NS records direct traffic to the appropriate nameserver that manages a domain, allowing different parts of the DNS tree to be managed independently by different organization



DNS record types:

DNS records, also known as zone files, provide information about a domain. This includes the IP address that is associated with this domain and how to handle queries for it. Each DNS record has a time-to-live setting TTL which indicates how often a DNS server will refresh it.

Below are the most commonly used types of DNS records and their meaning:



Type	Name	Description
A	Host address	The most basic and the most commonly used DNS record. It translates human-friendly domain names into computer-friendly IP addresses.
AAAA	IPv6 host address	Same as A but for IPv6 (a host address that can have more than one IP address).
CNAME	Canonical name for an alias	Maps a name to another name. It should only be used when there are no other records on that name.
ALIAS	Auto resolved alias	Maps a name to another name but can coexist with other records on that name.
MX	Mail eXchange	Specifies the e-mail server(s) responsible for a domain name.
NS	Name Server	Identifies the DNS servers responsible for a zone. One NS record for each DNS server in a zone.
TXT	Descriptive Text	Holds general information about a domain name such as who is hosting it, contact person, phone

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network management protocol that automatically assigns IP addresses and other network configurations (such as subnet mask, gateway, DNS servers) to devices on a network.

Example:

- When you connect your laptop to a Wi-Fi network, a DHCP server assigns it an IP address automatically, allowing it to communicate with other devices on the network without manual configuration.

Network Components and Services

Routers and Switches

- Routers Connect different networks and direct data packets between them.
- Switches Connect devices within the same network and use MAC addresses to forward data to the correct device.

Firewalls

- Firewalls control incoming and outgoing network traffic based on predetermined security rules.

Load Balancers

Load balancers distribute incoming network traffic across multiple servers to ensure no single server becomes overwhelmed.

VPN

VPN Virtual Private Network) provides a secure connection between remote users and the corporate network over the internet.

Network Troubleshooting Tools:

1. ping

- Purpose: Test internet network connections.
- How It Works Uses the ICMP ECHO_REQUEST to get an ICMP ECHO_RESPONSE from a remote host.
- Usage For basic troubleshooting, you can run ping www.google.com to check network connectivity and see response times and packet loss

2. traceroute (or tracert on Windows)

- Purpose Track the route packets take to reach their destination.
- How It Works Sends UDP probes with increasing TTL values, showing each router along the route and the delay in reaching it.
- Usage Helps find which gateway is causing a delay by showing response times and where packets fail (indicated by).

3. telnet

- Purpose Test network connections and protocols. How It Works Attempts to establish a connection to a specified IP and port.
- Usage Test if a specific service is reachable, e.g., telnet google.com 443 .

4. curl

- Purpose Transfer data using multiple protocols, often for HTTP requests.
- Usage:
  - Basic GET request: curl http://example.com .
  - Check headers: curl -I http://example.com .
  - POST request: curl -X POST http://example.com .
  - Save response to file: curl http://example.com/file -o output.file .

5. dig (Domain Information Groper)

- Purpose Troubleshoot DNS problems and verify DNS records.
- How It Works Performs DNS lookups and displays information such as IP addresses.
- Usage: dig google.com to get information like IP addresses, TTL, and DNS record types.

6. netstat

Purpose Show network connections and port listening information.

Usage:

- netstat -lp List listening servers and their program names.
- netstat -a Show all active ports.
- netstat -r Show routing table.

7. nmap (Network Mapper)

- Purpose Discover hosts and services on a network.
- How It Works Sends raw packets to identify hosts, services, and operating systems.
- Usage:
  - Discover hosts: nmap -sn 172.31.44.35/20 .
  - Scan ports on a host: nmap -A 172.31.36.237 .

8. ssh (Secure Socket Shell)

- Purpose Securely connect to remote machines to execute commands.
- Usage:
  - Connect to a server: ssh username@hostname .
  - Secure and encrypted, used for remote management and file transfers.

9. scp (Secure Copy Protocol)

- Purpose Securely copy files between local and remote hosts.
- Usage:
  - Copy file to a remote server: scp localfile.txt user@remote:/path/to/destination .

These tools are invaluable for network diagnostics, troubleshooting, and secure communications, which are critical skills for any DevOps engineer.