Public IP address :

- a unique identifier that lets device find each others and share their information

- there are three types of public IP addresses which are

1) static : is assigned to a single entity whether a user, machine, website or server, usually used when a accessing a device from a distance

2) dynamic : may change depending on your isp and various network settings

3) shared : is assigned to a group of devices by the isp

Private IP address :

is more like a nickname is known by a group of friends

devices using private IP addresses can only freely communicate with in shared internal network and cannot directly connected to the internet or be accessed from it

example – three routers without a public IP address connecting to the internet while their sim cards all of the routers have different IP addresses however they are all seen as 84.15.186.115

---------- IPv4 ----------

IPv4, or Internet Protocol version 4, is the original addressing system of the Internet, introduced in 1983. It uses a 32-bit address scheme, which theoretically allows for over 4 billion unique addresses (2^32). IPv4 addresses are typically displayed in decimal format, divided into four octets separated by dots. For example, 192.168.1.1 is a common IPv4 address you might find in a home network.

IPv4 Address Format

IPv4 Address Format is a 32-bit Address that comprises binary digits separated by a dot (.)

Characteristics of IPv4

- **32-bit address length**: Allows for approximately 4.3 billion unique addresses.
- **Dot-decimal notation**: IP addresses are written in a format of four decimal numbers separated by dots, such as 192.168.1.1.
- **Packet structure**: Includes a header and payload; the header contains information essential for routing and delivery.
- **Checksum fields**: Uses checksums in the header for error-checking the header integrity.
- **Fragmentation**: Allows packets to be fragmented at routers along the route if the packet size exceeds the maximum transmission unit (MTU).
- **Address Resolution Protocol (ARP)**: Used for mapping IP network addresses to the hardware addresses used by a data link protocol.
- **Manual and DHCP configuration**: Supports both manual configuration of IP addresses and dynamic configuration through DHCP (Dynamic Host Configuration Protocol).

- **Limited address space**: The main limitation which has led to the development of IPv6 to cater to more devices.
- **Network Address Translation (NAT)**: Used to allow multiple devices on a private network to share a single public IP address.
- **Security**: Lacks inherent security features, requiring additional protocols such as IPSec for secure communications.

Drawbacks of IPv4

- **Limited Address Space** : IPv4 has a limited number of addresses, which is not enough for the growing number of devices connecting to the internet.
- **Complex Configuration** : IPv4 often requires manual configuration or DHCP to assign addresses, which can be time-consuming and prone to errors.
- **Less Efficient Routing** : The IPv4 header is more complex, which can slow down data processing and routing.
- **Security Issues** : IPv4 does not have built-in security features, making it more vulnerable to attacks unless extra security measures are added.
- **Limited Support for Quality of Service (QoS)** : IPv4 has limited capabilities for prioritizing certain types of data, which can affect the performance of real-time applications like video streaming and VoIP.
- **Fragmentation** : IPv4 allows routers to fragment packets, which can lead to inefficiencies and increased chances of data being lost or corrupted.
- **Broadcasting Overhead** : IPv4 uses broadcasting to communicate with multiple devices on a network, which can create unnecessary network traffic and reduce performance.

---------- IPv6 ----------

Another most common version of the Internet Protocol currently is IPv6. The well-known IPv6 protocol is being used and deployed more often, especially in mobile phone markets. IPv6 was designed by the Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding IPv4 due to the global exponentially growing internet of users.

IPv6 stands for Internet Protocol version 6. IPv6 is the new version of Internet Protocol, which is way better than IPv4 in terms of complexity and efficiency. IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 Address Format

IPv6 Address Format is a 128-bit IP Address, which is written in a group of 8 hexadecimal numbers separated by colon (:).

To switch from IPv4 to IPv6, there are several strategies:

- **Dual Stacking** : Devices can use both IPv4 and IPv6 at the same time. This way, they can talk to networks and devices using either version.
- **Tunneling** : This method allows IPv6 users to send data through an IPv4 network to reach other IPv6 users. Think of it as creating a “tunnel” for IPv6 traffic through the older IPv4 system.
- **Network Address Translation (NAT)** : NAT helps devices using different versions of IP addresses (IPv4 and IPv6) to communicate with each other by translating the addresses so they understand each other.

Characteristics of IPv6

- IPv6 uses 128-bit addresses, offering a much larger address space than IPv4's 32-bit system.
- IPv6 addresses use a combination of numbers and letters separated by colons, allowing for more unique addresses.
- The IPv6 header has fewer fields, making it more efficient for routers to process.
- IPv6 supports Unicast, Multicast, and Anycast, but no Broadcast, reducing network traffic.
- IPv6 allows flexible subnetting (VLSM) to divide networks based on specific needs.
- IPv6 uses Neighbor Discovery for MAC address resolution instead of ARP.
- IPv6 uses advanced routing protocols like OSPFv3 and RIPng for better address handling.
- IPv6 devices can self-assign IP addresses using SLAAC, or use DHCPv6 for more control.
- IPv6 handles fragmentation at the sender side, not by routers, improving speed.

Difference Between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
It can generate 4.29×10^9 address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
IPv4 supports VLSM(Variable Length subnet mask).	IPv6 does not support VLSM.
Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

TCP

What is Transmission Control Protocol (TCP)?

is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

Features of TCP

- TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- TCP implements an error control mechanism for reliable data transfer.
- TCP takes into account the level of congestion in the network.
-

Applications of TCP

- **World Wide Web (WWW)** : When you browse websites, TCP ensures reliable data transfer between your browser and web servers.
- **Email** : TCP is used for sending and receiving emails. Protocols like **SMTP** (Simple Mail Transfer Protocol) handle email delivery across servers.
- **File Transfer Protocol (FTP)** : FTP relies on TCP to transfer large files securely. Whether you're uploading or downloading files, TCP ensures data integrity.
- **Secure Shell (SSH)** : SSH sessions, commonly used for remote administration, rely on TCP for encrypted communication between client and server.
- **Streaming Media** : Services like Netflix, YouTube, and Spotify use TCP to stream videos and music. It ensures smooth playback by managing data segments and retransmissions.

Advantages of TCP

- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on Operating System .
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.
-

Disadvantages of TCP

- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.
- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

UDP

What is User Datagram Protocol (UDP)?

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.

Features of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching .
- UDP is used for some routing update protocols like RIP(Routing Information Protocol) .
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
-

Application of UDP

- **Real-Time Multimedia Streaming** : UDP is ideal for streaming audio and video content. Its low-latency nature ensures smooth playback, even if occasional data loss occurs.
- **Online Gaming** : Many online games rely on UDP for fast communication between players.
- **DNS (Domain Name System) Queries** : When your device looks up domain names (like converting "www.example.com" to an IP address), UDP handles these requests efficiently .
- **Network Monitoring** : Tools that monitor network performance often use UDP for lightweight, rapid data exchange.
- **Multicasting** : UDP supports packet switching, making it suitable for multicasting scenarios where data needs to be sent to multiple recipients simultaneously.
- **Routing Update Protocols** : Some routing protocols, like RIP (Routing Information Protocol), utilize UDP for exchanging routing information among routers.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.
-

Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.
    - UDP cannot have the mechanism to track the sequence of data.
    - UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
    - UDP can drop packets in case of detection of errors.
    -

Which Protocol is Better: TCP or UDP?

The answer to this question is difficult because it totally depends on what work we are doing and what type of data is being delivered. UDP is better in the case of online gaming as it allows us to work lag-free. TCP is better if we are transferring data like photos, videos, etc. because it ensures that data must be correct has to be sent. In general, both TCP and UDP are useful in the context of the work assigned by us. Both have advantages upon the works we are performing, that's why it is difficult to say, which one is better.