Internet Protocol Address

Overview

All the computers of the world on the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine to deliver that particular file or webpage that I am requesting. In technical terms, that address is called IP Address or Internet Protocol Address.

Let us understand it with another example, like if someone wants to send you a mail then he/she must have your home address. Similarly, your computer too needs an address so that other computers on the internet can communicate with each other without the confusion of delivering information to someone else's computer. And that is why each computer in this world has a unique IP Address. Or in other words, an IP address is a unique address that is used to identify computers or nodes on the internet. This address is just a string of numbers written in a certain format. It is generally expressed in a set of numbers, for example 192.155.12.1. Here each number in the set is from 0 to 255 range. Or we can say that a full IP address ranges from 0.0.0.0 to 255.255.255.255. And these IP addresses are assigned by IANA (known as Internet Corporation For Internet Assigned Numbers Authority).

Working of IP Address

The working of IP addresses is like other languages. It can also use some set of rules to send information. Using these protocols, we can easily send and receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them.

- Your device directly requests your Internet Service Provider which then grants your device access to the web.
- And an IP Address is assigned to your device from the given range available.
- Your internet activity goes through your service provider, and they route it back to you, using your IP address.
- Your IP address can change. For example, turning your router on or off can change your IP Address.
- When you are out from your home location your home IP address doesn't accompany you. It changes as you change the network of your device.

Types of IP Address

IP Address is of two types:

1. IPv4: Internet Protocol version 4. It consists of 4 numbers separated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-

255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8-digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately = 4,294,967,296 can be assigned with IPv4.
IPv4 can be written as:

189.123.123.90

Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let's understand it with a simple example. If you must find a word from a language dictionary, how long will it take? Usually, you will take less than 5 minutes to find that word. You can do this because words in the dictionary are organized in alphabetical order. If you must find the same word from a dictionary that doesn't use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionary with one billion words without order can be so disastrous, then you can imagine the pain behind finding an address from 4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes:

IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

The 0.0.0.0 is a Non-routable address is that indicates an invalid, or inapplicable end-user address.
A loopback address is a distinct reserved IP address range that starts from 127.0.0.0 ends at 127.255.255.255 through 127.255.255.255 is the broadcast address for 127.0.0.0/8. The loopback addresses are built into the IP domain system, enabling devices to transmit and receive the data packets. The loopback address 127.0.0.1 is generally known as localhost.
2. IPv6: There is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are many more devices in the world to be connected to the internet. So, gradually we are making our way to IPv6 Address which is a 128-bit IP address. In human-friendly form, IPv6 is written as a group of 8 hexadecimal numbers separated with colons (:). But in the

computer-friendly form, it can be written as 128 bits of 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which are more than enough for upcoming future generations.
IPv6 can be written as:

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Classification of IP Address

An IP address is classified into the following types:

1. Public IP Address: This address is available publicly and it is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses are of two types,

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you with an IP Address from the range of available IP Addresses. Now, your device has an IP Address, and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time you try to connect to the internet with the same device, your provider provides you with different IP Addresses to the same device and from the same available range. Since IP Address keeps on changing every time you connect to the internet, it is called a Dynamic IP Address.

- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are used by DNS servers. What are DNS servers? These are computers that help you to open a website on your computer. Static IP Address provides information such as device is located on which continent, which country, which city, and which Internet Service Provider provides internet connection to that device. Once we know who the ISP is, we can trace the location of the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. Private IP Address: This is an internal address of your device which are not routed to the internet and no exchange of data can take place between a private address and the internet.

3. Shared IP addresses: Many websites use shared IP addresses where the traffic is not huge and very controllable, they decide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers use the same IP address (within a single mail server) to cut down the cost so that they could save the time the server is idle.

4. Dedicated IP addresses: A dedicated IP Address is an address used by a single company or an individual which

gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP address that is black-listed due to spam.

Lookup IP Address

To know your public IP, you can simply search “What is my IP?” on google. Other websites will show you equivalent information: they will see your public IP address because, by visiting the location, your router has made an invitation/request and thus revealed the information. The location IP location goes further by showing the name of your Internet Service Provider and your current city.

Finding your device’s private IP Address depends on the OS or platform you are using.

- **On Windows:** Click Start and type “cmd” in the search box and run the command prompt. In the black command prompt dialog box type “ipconfig” and press enter. You will be able to see your IP Address there.
- **On Mac:** Go to system preferences and select Network, you will be able to see the information regarding your network which includes your IP Address.

IP Address Security Threat

Each IP address is associated with virtual ports in a computer that acts as a doorway that allows web applications or websites to send and receive data or information on your device. If after the connection is terminated the ports remain open somehow, might allow hackers to get into your device. Once, a hacker gets access to your device remotely through various tools and viruses, they would be able to access all your stored files and data and your computer hardware as well, which includes your webcam, mic, speaker, and all your browsing history, your emails and saved passwords. These are some serious threats from which we need to be extra careful.

Various online activities can reveal your IP address from playing games or accepting bad cookies from a trap website or commenting on a website or forum. Once they have your IP, there are websites that help them get a decent idea of your location. They can further use social media websites to track your online presence and cross verify everything that they got from these sites and use your information for their benefits or can sell these data collected on the dark web which can further exploit you.

The worst which I have seen in my friend's pc got infected while he was installing an application that he downloaded from a pirated website. The moment he hit install, several command prompt boxes started appearing, tens of commands started running and after a while, it was back to normal. Some malware was installed in the process. After a

few days, someone was trying to log in to his social media account and other accounts using his computer as a host pc (his own IP address) but his computer was idle. The hacker was using his pc and his network, i.e., his IP address to do some serious stuff. He formatted his computer then and there, secured all his emails and other accounts, and changed all the passwords and all the security measures that had to be taken.

Cybercriminals use different techniques to get hands-on with your IP address and know your location, get into your network and hack into your computers. For instance, they will find you through Skype which uses IP addresses to speak. If you are using these apps, it's important to notice that your IP address might be vulnerable. Attackers can use the various tools, where they will find your IP address. Some of the threats are: Online stalking, downloading illegal content using your IP address, tracking your location, directly attacking your network, and hacking into your device.

Protect and Hide IP Address

To secure and hide your IP address from unwanted people always remember the following points:

- Use a proxy server.
- Use a virtual private network (VPN) when using public Wi-Fi, you are traveling, working remotely, or just want some privacy.

- Change privacy settings on instant messaging applications.
- Create unique passwords.
- Beware of phishing emails and malicious content.
- Use a good and paid antivirus application and keep it up to date.
- When you are using public Wi-Fi in a cafe or station or anywhere, you must hide your IP address by using VPN. Getting your IP from public Wi-Fi is just a cakewalk for these hackers and they are very good at stealing all your information while using your computer's address. There are different phishing techniques in which they email you, call you, and SMS you about giving vital information about you. They give links to vicious websites which are pre-rigged. The moment you open these websites, they steal all your device's information revealing all the information about you and your device which is to be kept private. These leaks help hackers to exploit your device and install or download some spyware and malware on your device. But using a good anti-virus gives you web security as well, which will prevent those websites from launching and warn you about the information being passed to these websites.
- It is also not recommended to use torrent or pirated websites which are a threat to your online identity and can compromise your device or emails or any other information about you.