COMPUTER NETWORKING

Name : Dipankar Thorat
Course : Computer Engineering
College : K.J Somaiya Polytechnic
Place : Mumbai , India
E-mail : dipankar.t@somaiya.edu

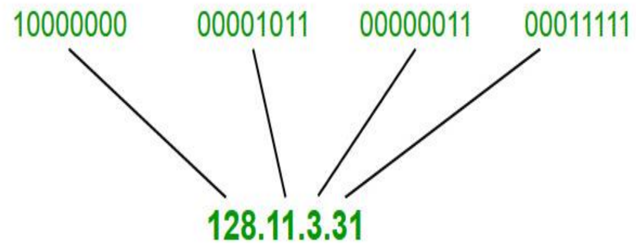
Name : Vedant Shetye
Course : Computer Engineering
College : K.J Somaiya Polytechnic Place : Mumbai , India
E-mail : vedant.shetye@somaiya.edu

Name : Swayam Patel
Course : Computer Engineering
College : K.J Somaiya Polytechnic Place : Mumbai , India
E-mail : swayam.patel@somaiya.edu

ABSTRACT: THE FOLLOWING PAPER CONSISTS OF ALL THE INFORMATION REGARDING IP ADDRESSING. IT HAS THE FORMAT OF IP ADDRESS, SUBCLASSES, WORKING, AND TYPES.

INTRODUCTION TO IP ADDRESSING

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network. In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works. An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.



IP ADRESS

- *Decimal Dotted Notation*

- *The 32 bit IP address is divided into five sub-classes:*
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 address is divided into **two parts**:

- Network ID
- Host ID

WORKING OF IP ADDRESS

The working of IP addresses is similar to 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.

- 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.

HOW DOES DNS MATCH DOMAIN NAMES TO IP ADDRESSES?

Nobody types IP addresses into a browser search field; we use domain names like Network World, CNN or Twitter. The Domain Name System, or DNS, another part of the Internet protocol suite, makes sure that requests made using domain names reach the correct IP address. You can think of DNS as representing a more user-friendly layer on top of the IP-address infrastructure. However, the IP address remains the fundamental way that internet-connected devices are found, and in some circumstances a domain name can correspond to multiple servers with different IP addresses.

HOW ARE IP ADDRESSES ASSIGNED?

As the International Assigned Numbers Authority (IANA) puts it, "Both IPv4 and IPv6 addresses are generally assigned in a hierarchical manner," and IANA is at the top of the hierarchy. IANA assigns blocks of IP addresses to regional internet registries (you can see which address ranges go with which regions here).
The regional registries in turn assign smaller blocks to national registries, and so on down the line, with blocks eventually being assigned to individual internet service providers (ISP), which in this context include mobile phone companies. It's the ISPs that assign specific IP addresses to individual devices, and there are a couple of ways they can do this.

TYPES OF IP ADDRESS ?

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: 179.123.113.90

IPv6: But, 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 much 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 actually more than enough for upcoming future generations.

IPv6 can be written as:

2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b

WHAT'S THE DIFFERENCE BETWEEN IPV4 AND IPV6 ADDRESSES?

There are two versions of IP addresses: IPv4 and IPv6, and they have different formats, the major difference between them being that it's possible to create vastly more unique IPv6 addresses (2128) than IPv4 addresses (232).

IPv4 addresses are written in four parts separated by dots like this: 45.48.241.198. Each part written in conventional Base 10 numerals represents an eight-bit binary number from 0 to 255.

Each of these four numbers separated by dots is written in standard decimal notation. But computers fundamentally deal with numbers in binary (using zeroes and ones, and each of the numbers in an IPv4 address represents an 8-bit binary number, which means that none of them can be higher than 255 (111111 in binary).

It's quite likely that you've seen IP addresses like that one before since they've been around since 1983. The newer version of the protocol, IPv6, is slowly displacing IPv4, and it's addressing looks like this: **2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b**

WHAT ARE PUBLIC VS. PRIVATE IP ADDRESSES?

We've been talking about IP addresses and potentially running out of them as if there were one set of addresses for the entire planet, with no repeats. But that's not strictly true. In fact, it's probably not true for most devices you use in a day-to-day basis and not all of the 4.3 billion IPv4 addresses are available to publicly connected devices.

A typical home or corporate network connects to the public internet via a router, and it's this router that's assigned an IP address by the ISP. From the perspective of the outside world, all traffic from devices on that local network are coming from that public IP address; but inside the network, each device (including the router) has a local private IP address, usually assigned by the router via DHCP.

These addresses are considered private because they're only used for directing packets within the local, private network, and can't be seen by anyone outside the network. As result, the same IP address can be used on an infinite number of private networks without causing confusion. In fact, there are blocks of IP addresses specifically set aside for use on these private networks. (For small home networks, addresses starting with 192.168 are quite common.)

The job of the router is to alter the origin and destination IP addresses in each packet's headers as needed as it passes between the private network and the public internet, a process known as network address translation, or NAT.

There are several methods for doing this. One common way is to associate each device on the internal network with a network port that is listed in the packet header. That port information determines the final destinations of incoming packets that have all been addressed to the public-facing IP address assigned to the router.

This discussion is specific to IPv4 addresses, and the boom in local networks has been in a big factor in staving off a total IPv4 address drought even as network-connected devices multiply in every home.

IPv6 addresses, on the other hand, are so plentiful that it's assumed that these kinds of private networks will be unnecessary after universal IPv6 adoption. However, if you want to set up a private internal IPv6 network that connects to the internet via IPv4, there are also private IPv6 address ranges you can use

IP ADDRESS SECURITY THREATS:

Cybercriminals or digital crackers various ways to hack your IP address. The two commonly used techniques include social engineering and online stalking.

Social engineering :

Hackers can practice social engineering techniques to trick you into disclosing your device's IP address. For example, they will connect you through email, Skype, or a similar instantaneous messaging app, that accepts IP addresses to communicate and pass information. If you chat with these anonymous people using these messaging applications, it is essential to note that they can get your IP address. Cybercriminals can use a third-party tool named Skype Resolver, with the help of which they can locate your IP address using your username.

Online Stalking :

Attackers can get crack your IP address by simply tracking your online activities. Any online activity can disclose your IP address, i.e., from using an instant messaging app to playing online games to discussing a topic on any digital websites and forums. Once they gain access to your IP address, criminals can visit an IP address tracking website (whatismyipaddress.com), they will enter your IP address there, and in no seconds, they can track your current location. They won't stop till this; they can further cross-check it with other available information to verify whether the IP address is connected with you particularly. Social networking sites such as instagram, LinkedIn, facebook are used to verify the information of your location gathered by the attacker.

REFERENCE

- https://www.wikipedia.org
- https://www.geeksforgeeks.org
- https://www.kaspersky.com