One of the rules of connecting to the internet is that every host needs an IP address, if we have 4 hosts (A, B, C, D), they can all send and receive data to each other as long as they each have an IP address. When host A sends data to host B, host A’s source IP addresses is stamped alongside host B’s IP address which is used as the destination, then since host B receives the data with host A having stamped the data with its source IP address, host B is able to send a response back.

IPv4 addresses are 32 bits split into 4 octets, the computer sees IP addresses as (example): 1011 0111.0110 0101. 1000 0010. 0011 0001. We simplify this into 4 octets as decimal numbers, so we see it as 151.101.130.49. Every IP address is just a unique combination of 32 1’s and 0’s. This means that there is a finite number of IP addresses. Since we have 32 bits each and each bit can either be a 1 or a 0, we can calculate the total combination of IP addresses by doing 2^32, 2 represents either 1 or 0, and 32 represents the amount of bits in an IP address. The total number of IPv4 addresses is 4.2 billion.

The original intention of the internet was for every host to have a unique IP address, but eventually we would run out of IP addresses.

The long-term solution for this was to create an IPv6 addressing scheme which has 128 bits giving us a significantly larger addresses space, however moving from IPv4 to IPv6 is a very long process. IPv6 came out in 1998, in 2020 only 25% of the world was on IPv6, in 2025-2026 around 49% of the world is on IPv6.

We have another solution to stretch the IPv4 address space which is NAT.

NAT creates a set of IP addresses that are reusable:

* 10.0.0.0/8 – any IP in range of 10.#.#.# (from 10.0.0.0 to 10.255.255.255)
* 172.16.0.0/12 - any IP in range of 172.16.#.# (from 172.16.0.0 to 172.31.255.255)
* 192.168.0.0/16 - any IP in range of 192.168.#.# (from 192.168.0.0 to 192.168.255.255)

The above addresses are known as private IPv4 addresses which are also referred to as RFC 1918 addresses because that is the document that formalised those addresses.

So, the problem of running out of IPv4 addresses is gone because we can reuse those addresses as necessary. All remaining addresses are known as public IP addresses, NAT translates private IP addresses into unique public IP addresses. Lets see how this conserves IP address space.

NEXT PAGE

A house with a router

AI-generated content may be incorrect.

This home wifi network is using the internal address space of 192.168.1.0/24. Each device in this network has its own IP address. Since each device is connected to the internet, each device must have an IP address (which they do). When the devices send data over the internet, the router is translating all the device addresses to the public IP address (210.20.6.98). This allows those 5 devices to all use one IP address. All 5 devices are sharing one IP address (the routers one), this gives us a 5:1 ratio of conserved IP address space.

We can take this a step further, it is very likely that the many houses within a neighbourhood is using the same private IP address space (192.168.1.0/24) for their internal wifi network. And as long as each of those routers are translating private addresses into unique public addresses, we will have no problem with communicating to other devices on the internet:

A house with a router

AI-generated content may be incorrect.

One of the rules after NAT is that any communication on the internet must be from public addresses to public addresses, any traffic that includes a private IP address will be dropped. So, if a host from the first house on the right (with the private address) is sending data to host C, after the data passes the router, the router translates the private IP address into a public address, and as far as the internet is concerned, it is a public address speaking to a public address. When the traffic comes back to the router, the router will then untranslated the packet to pass it back to the host with the private IP.