Network Address Translation

NAT is a technology widely used nowadays. It was first applied in 1994 on the PIX (Private Internet Exchange) firewall product by John Mayes, and its main objective was to solve the issue of the limited number of IPv4 addresses. The engineers who designed IPv4 addresses could not realize how widespread the technology would become. Therefore, it was limited to only about 4 billion unique addresses, which turned out to be too few for vast devices that required IP addresses to access the internet.

There are two types of IPv4 addresses- public and private. As inferred from the name, Public IPs are used to access the internet. Therefore, they should be globally unique. In contrast, private IPs are used internally. Consequently, they should be unique only in the network. As the number of public IPs is strictly limited, our routers assign our devices private IP addresses. But then, how could these devices access the internet? And here is where the NAT comes to help. NAT translates Private IPv4 addresses into public ones and vice versa when receiving packets. NAT works in the OSI model's Network Layer(Layer 3).

When a device wants to send a packet to another device outside one subnet, it sets the destination MAC address to the MAC address of the router it is connected to, but assigns the destination IP address to the address it wants to reach. Then the router changes the source IP address to its public IP address and adds a line in the NAT forwarding table. After the request is sent to its destination and the destination device responds to that request, it mentions the router's public address as the destination address. When the router receives the response packet, it sends it directly to the device's private IP that requested it. The way the router does so is through the NAT forwarding table. When the router gets the packet, it checks the port on which it received the packet and matches it with the IP address that initially sent the request.

Though NAT is a crucial technology now, it will be optional. Ideally, every device should have its public IP address, and there should be no distinction between public and private addresses, so the routers would use their resource only for routing. Engineers solved this problem by implementing IPv6, which has approximately 3.4x1038 unique addresses, so that every device can have its own public IP. However, its implementation is a challenging task. For the global switch to IPv6, every device should support it, which still needs to be achieved. However, IPv6 standards were accepted over 20 years ago.