28th of Dec. 2025

Network Address Translation (NAT)

Network Address Translation (NAT) is a process that enables one, unique IP address to represent an entire group of computers. In network address translation, a network device, often a router or NAT firewall, assigns a computer or computers inside a private network a public address. In this way, network address translation allows the single device to act as an intermediary or agent between the local, private network and the public network that is the internet. NAT's main purpose is to conserve the number of public IP addresses in use, for both security and economic goals.

How Network Address Translation (NAT) Works

To communicate with the internet, a networking system requires a unique IP address. This 32-bit number identifies and locates the network devices so a user can communicate with it.

Network address translation permits a single device, such as a NAT firewall or router or other network address translation device, to act as an agent between the public network and private networks - the internet and any local networks. This allows an entire group of devices to be represented by a single unique IP address when they do anything outside their network.

NAT works like a large company's receptionist, with specific instructions on which calls and visitors to keep out, make wait, or send through, and where the should go. For example, you can tell the receptionist not to forward any visitors or calls without your request until you're waiting for something specific; you can then leave instructions about letting that particular client communication through.

The client calls the company's main number, because that public-facing number is the only one whom anyone knows. They tell the receptionist they need to speak with you, and the receptionist

a) checks the instructions and knows you want the call forwarded, and
b) matches your extension with a list to send the information to the right place. The caller never gets your private line.

Network address translation works similarly. The request arrives at the public IP address and port, and the NAT instructions send it where it

should go without revealing the private IP addresses of the destination.

Types of Network Address Translation

There are many forms of NAT and it can function in several ways

1. Static NAT (One-to-One Mapping) : Static NAT maps unregistered IP addresses using 1 to 1 network address translation to match up with registered IP addresses. It is particularly useful when a device needs to be accessible from outside the network.

2. Dynamic NAT (many-to-many from a pool) : This form of NAT selects a target from a group of registered IP addresses and maps an unregistered IP address to the registered version. When the outgoing traffic arrives at the router, the router replaces the destination IP address with a free global IP address from the pool. When the return traffic comes back to the order router, the router replaces the mapped global IP address with the source IP address.
Dynamic NAT is mostly used in networks that need outbound internet connectivity.

3. Port Address Translation (PAT) (many-to-one) : PAT is a type of dynamic NAT that maps multiple internal IP addresses to a single external IP address via port numbers. This is many-to-one mapping. When a computer connects to the internet, the router assigns it a port number that it then appends to the computer's internal IP address, in turn giving the computer a unique IP address. When a second computer connects to the internet, it gets the same external IP address but a different port number.
PAT is mostly used in home networks.

Note: for static NAT, when outgoing traffic arrives at the router, the router replaces the destination IP address with the mapped global IP. When the return traffic comes back to the router, the router replaces the mapped global IP address with the source IP address.
Static NAT is mostly used for in servers that need to be accessible from the internet, such as web servers and email servers.