3 Network Address Translation (NAT)

Jacques Mock Schindler

20.08.2025

What is NAT?

Network Address Translation (NAT) is a process for automatically and transparently translating IP addresses in data packets. NAT enables multiple devices in a private network to communicate with the Internet via a single public IP address. This technology was developed to address the scarcity of IPv4 addresses while increasing the security of private networks.

In practice, this means that if you connect multiple devices (laptop, smartphone, smart TV) to the Internet at home, all of these devices share a single public IP address assigned to you by your Internet service provider.

How NAT works

Basic principle

NAT operates at layer 3 of the OSI model and changes the addresses in the IP header of data packets. The process works as follows:

1. **Outgoing connection:** A device on the private network (e.g. 192.168.1.10) sends a request to a server on the Internet.
2. **Address translation:** The NAT router replaces the private source IP address with its public IP address (e.g. 203.0.113.5).
3. **Table entry:** The router stores the assignment in a NAT table.
4. **Response:** When the server responds, the router uses the NAT table to forward the response to the correct device on the private network.

NAT table

The NAT table is at the heart of the process. It contains the following information:

- **Private IP address** (e.g. 192.168.1.10)
- **Private port** (e.g. 54321)
- **Public IP address** (e.g. 203.0.113.5)

- **Public port** (e.g. 12345)
- **Destination IP address** (e.g. 93.184.216.34)
- **Destination port** (e.g. 80)

Private IP address ranges

Special IP address ranges are reserved for private networks that are not routed on the public Internet:

- **10.0.0.0 to 10.255.255.255** (10.0.0.0/8) – 16,777,216 addresses
- **172.16.0.0 to 172.31.255.255** (172.16.0.0/12) – 1,048,576 addresses

- **192.168.0.0 to 192.168.255.255** (192.168.0.0/16) – 65,536 addresses

These ranges can be reused as often as desired in private networks, as they are only valid locally.

Types of NAT

1. Static NAT (one-to-one NAT)

With static NAT, a private IP address is permanently assigned to a public IP address. This is used when a server in the private network needs to be permanently accessible from the Internet.

Example: - Private: 192.168.1.100 ↔ Public: 203.0.113.10

2. Dynamic NAT

Dynamic NAT dynamically assigns private IP addresses from a pool of public IP addresses. The assignment is made as needed and is released again after a certain period of time.

3. Port Address Translation (PAT)

What is a port?

To understand how PAT works, we first need to understand the concept of ports. An IP address identifies a computer on the network – but many programs run simultaneously on a computer, all of which want to use network connections.

Analogy: Imagine the IP address as the postal address of a high-rise building. The port number then corresponds to the apartment number. Just as the post office knows which apartment a letter belongs to, the computer knows which program the data should be delivered to based on the port number.

Ports are 16-bit numbers (0 to 65,535) and are divided into three categories: - **Well-known ports (0-1023):** Reserved for standard services - Port 80: HTTP (websites) - Port 443: HTTPS (encrypted websites) - Port 22: SSH (secure connection) - Port 25: SMTP (email transmission) - **Registered**

ports (1024-49,151): For registered services - **Dynamic/private ports (49,152-65,535):** Freely usable

How PAT works

PAT, also known as NAT overload, is the most common form of NAT. Here, many private IP addresses share a single public IP address, with differentiation based on port numbers.

The router not only remembers which private IP address has established a connection, but also which port. This allows multiple devices to communicate simultaneously via the same public IP address.

Calculation example: With 16-bit port numbers, $2^{16} = 65,536$ ports are theoretically available. Minus the reserved ports (0-1023), this leaves approximately 64,512 usable ports for simultaneous connections. In practice, this means that a home router could theoretically manage over 64,000 simultaneous connections.

Advantages and disadvantages

Advantages

- **IP address savings:** A household with 20 devices only needs one public IP address
- **Security:** Private IP addresses are not directly accessible from the outside
- **Flexibility:** The internal network structure can be changed without affecting the public address

Disadvantages

- **End-to-end connectivity:** Direct connections between devices are made more difficult
- **Complexity:** Certain applications (e.g. VoIP, online gaming) require special configurations
- **Performance:** Address translation requires computing power and can cause delays

Practical example

Let's consider a typical home router:

1. **Your laptop** (192.168.1.15) opens the website www.example.com
2. **HTTP request:**
    - Source: 192.168.1.15:45678
    - Destination: 93.184.216.34:80
3. **NAT router translates:**
    - Source: 85.5.123.45:23456 (public IP)
    - Destination: 93.184.216.34:80
4. **Server responds:**

- Source: 93.184.216.34:80
- Destination: 85.5.123.45:23456

5. **Router translates back:**
    - Source: 93.184.216.34:80
    - Destination: 192.168.1.15:45678

Significance for the future

With the introduction of IPv6 and its 2^{128} possible addresses, NAT will theoretically become superfluous. In practice, however, NAT will continue to be used because:

- Many networks are still based on IPv4
- NAT provides additional security
- The transition to IPv6 is taking place gradually

NAT therefore remains an important technology for the modern Internet, solving both the address shortage and contributing to network security.