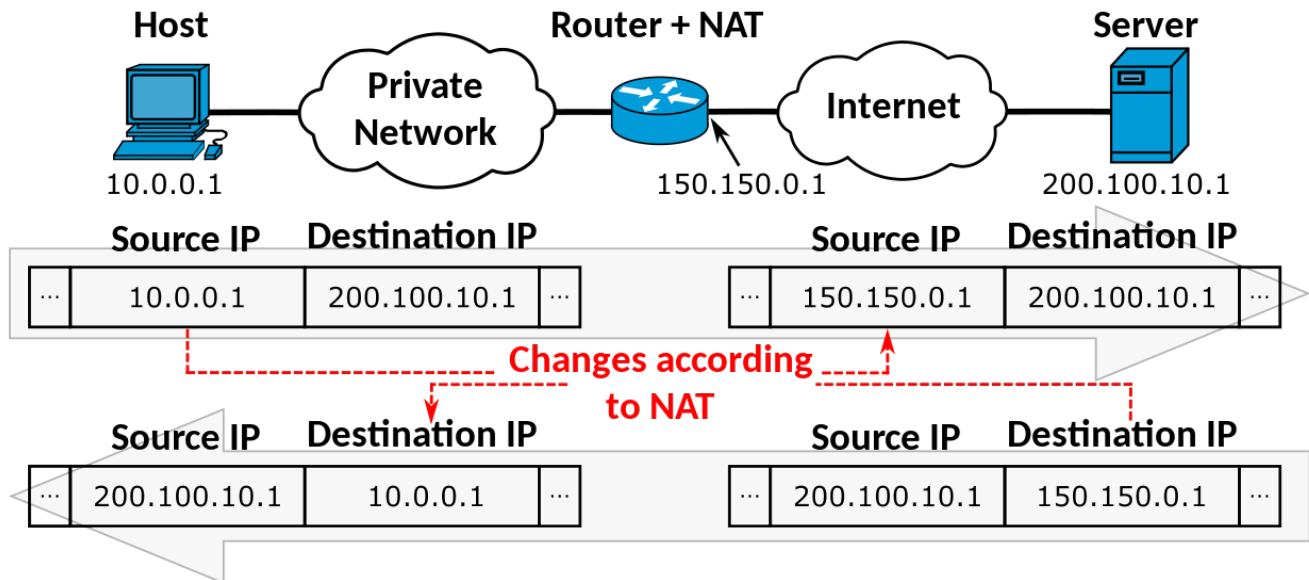


Network: Types of NAT address translation

Excerpted from Ostrowski, K. (2025). Lexicon: Computer networks - For engineers and technicians (1.0). Zenodo. <https://doi.org/10.5281/zenodo.15341381>

Lexicon: Computer Networks



Representation of SNAT translation between WAN and LAN

Address Translation (SNAT) in IP networks is a technique for mapping IP addresses from one address space to another. It is particularly useful for managing network addressing, providing security and enabling communication between different networks. There are several methods of address translation, the most commonly used of which are: SNAT (Source Network Address Translation), DNAT (Destination Network Address Translation) and PAT (Port Address Translation).

SNAT (Source Network Address Translation)

SNAT is the process of translating the source address in IP packets. It is mainly used in scenarios where internal devices (e.g. computers on the local network) want to communicate with an external network (e.g. the Internet), but do not have public IP addresses. With SNAT, outgoing packets from the internal network are altered to look like they are coming from a device with a public IP address. A typical example is a router acting as a default gateway, which converts private IP addresses into a single public address.

Practical applications of SNAT:

- Connecting internal devices to the Internet using a single public IP address.
- Masking the true source address to protect the privacy of internal devices.
- Optimising the use of public IP addresses in the case of limited available resources.

DNAT (Destination Network Address Translation)

DNAT is the process of translating the destination address in IP packets. It is used when packets arriving on the network need to be routed to the appropriate internal devices, even though they have private IP addresses. It is most commonly used in scenarios where internal servers need to be accessible from the Internet, such as a web server, FTP server, or mail server. With DNAT, the router or firewall changes the destination addresses of the packets, redirecting them to the appropriate internal servers.

Practical applications of DNAT:

- Sharing internal servers (e.g. web servers, FTP) on the Internet.
- Directing incoming traffic to different servers depending on the destination port (e.g. HTTP to one server, FTP to another).
- Enabling communication with devices with private IP addresses in external environments.

PAT (Port Address Translation)

PAT, also known as *NAT with port translation*, is a technique in which multiple internal devices use a single public IP address, but different outgoing connections are identified by port number. It is the most common form of NAT, used in situations where there are multiple devices on the local network but only one public IP address. Each outgoing connection from the internal network is assigned a unique port number, allowing multiple outgoing connections from a single IP address to be differentiated.

Practical applications of PAT:

- Enabling multiple devices on a local network to use a single public IP address.
- Efficient management of a limited number of public IP addresses.
- Use in home routers where multiple devices access the internet via a single public IP address.

DMZ (Demilitarised Zone)

DMZ, or *demilitarised zone*, is a network segment that lies between an external network (e.g. the Internet) and an internal corporate network. It is a specially designated zone that houses servers that need to be accessible from both the internal network and the Internet, such as web, FTP and mail servers. The purpose of the DMZ is to increase security, as it allows servers that need to be accessible from the outside to be separated from the internal network, protecting it from direct access from the Internet.

Practical applications of DMZ:

- Isolating Internet-accessible servers (e.g. web servers, mail servers) from the internal corporate network.
- Increasing the security of the organisation by segmenting network traffic.
- Providing access control to sensitive resources, restricting access to internal servers from the outside.

Summary

Address translation in IP networks is an essential element in managing network traffic, ensuring security and the efficient use of available address resources. Techniques such as SNAT, DNAT, PAT and the DMZ concept allow effective access control and communication management between different network segments. Through the use of these technologies, it is possible to both ensure the privacy of internal devices and make network resources available to the outside in a secure and controlled manner.