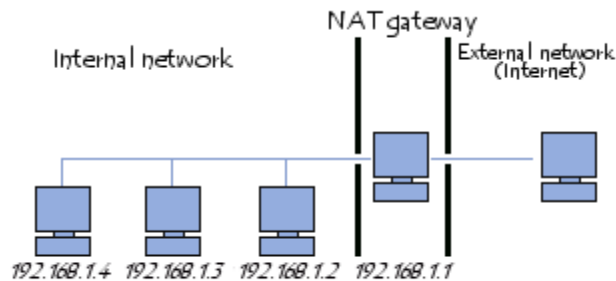


The principle of NAT

Network address translation or **NAT** was developed in order to respond to the shortage of IP addresses with IPv4 protocol (in time the IPv6 protocol will respond to this problem).

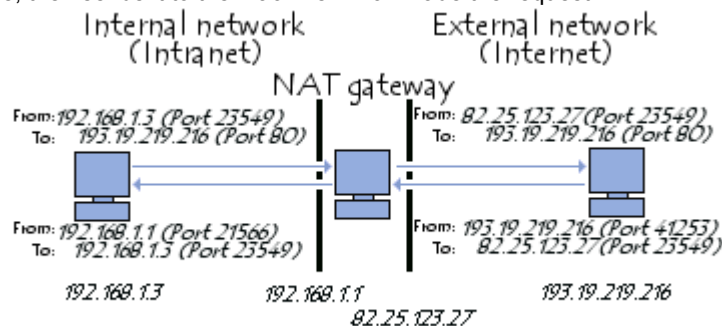
In fact, in IPv4 addressing the number of routable IP addresses (which are unique in the world) is not enough to enable all machines requiring it to be connected to the internet.

The principle of NAT therefore consists of using a gateway connection to the Internet, having at least one network interface connected to the internal network and at least one network interface connected to the Internet (possessing a routable IP address), in order to connect all the machines to the network.



It is a question of creating, at gateway level, a translation of packets coming from the internal network to the external network.

So, each machine on the network needing to access the Internet is configured to use the NAT gateway (by specifying the IP address of the gateway in the "Gateway" field with its TCP/IP parameters). When a network machine makes a request to the Internet, the gateway makes the request in its place, receives the response, then sends it to the machine which made the request.



Since the gateway completely conceals the internal addresses on the network, the network address translation mechanism provides a **secure** function. In fact, to an external observer of the network, all requests seem to come from the gateway IP address.

Address space

The organisation managing public address space (routable IP addresses) is the *Internet Assigned Number Authority (IANA)*. RFC 1918 defines a private address space enabling any organisation to allocate IP addresses to machines on its internal network without risk of entering into conflict with a public IP address allocated by IANA. These addresses known as non-routable relate to the following address ranges:

- Class A: range from 10.0.0.0 to 10.255.255.255;
- Class B: range from 172.16.0.0 to 172.31.255.255;
- Class C: range from 192.168.0.0 to 192.168.255.55;

All the machines on an internal network, connected to the internet via a router and not having a public IP address must use an address within one of these ranges. For small domestic networks, the address range from 192.168.0.1 to 192.168.0.255 is generally used.

Static translation

The principle of **static NAT** consists of linking a public IP address to a private internal IP address on the network. The **router** (or more precisely the **gateway**) thus allows a private IP address (for example 192.168.0.1) to be linked to a public routable IP address on the Internet and conducts the translation, in either direction, by changing the address in the IP packet.

Static network address translation therefore enables internal network machines to be connected to the Internet in a transparent way but does not resolve the problem of the lack of addresses insofar as n routable IP addresses are necessary to connect n machines to the internal network.

Dynamic translation

Dynamic NAT enables a routable IP address (or a reduced number of routable IP addresses) to be shared between several machines with private addresses. So seen from outside, all the machines on the internal network virtually possess the same IP address. This is the reason why the term "**IP masquerading**" is sometimes used to indicate dynamic network address translation.

In order to be able to "multiplex" (share) the different IP addresses on one or several routable IP addresses, dynamic NAT uses *Port Address Translation (PAT)*, i.e. the allocation of a different source port for each request in such a way as to be able to maintain a correspondence between the requests coming from the internal network and the responses of the machines on the Internet, all addressed to the router's IP address.

Port Forwarding

Network address translation only allows requests coming from the internal network to the external network, which means that it is impossible as such for an external machine to send a packet to a machine on the internal network. In other words, the internal network machines cannot operate as a server with regards to the external network.

For this reason, there is a NAT extension called "**port forwarding**" or *port mapping* consisting of configuring the gateway to send all packets received on a particular port to a specific machine on the internal network. So, if the external network needs to access a web server (port 80) operating on machine 192.168.1.2, it will be necessary to define a port forwarding rule on the gateway, redirecting all TCP packets received on port 80 to machine 192.168.1.2.

Port Triggering

The majority of client-server applications make a request over a remote host on a given port and open a port in return to recover the data. Nevertheless, certain applications use more than one port to exchange data with the server, this is the case for example with **FTP**, for which a connection is established by port 21, but data is transferred via port 20. So with NAT, after a connection request on port 21 by a remote FTP server, the gateway awaits a connection on a single port and will refuse the connection request on port 20 of the client.

There is a mechanism derived from NAT, called "**port triggering**", making it possible to authorise the connection to certain ports (*port forwarding*) if a condition (request) is fulfilled. It is therefore a question of conditional port forwarding, enabling a port to be opened only when an application requires it so it is not permanently left open.