NAT

Network **A**ddress **T**ranslation – a primer.

Author: Tom Kistner

Requirements: Basic IP Protocol Knowledge

What does NAT do ?

- Every IP packet carries a SOURCE and DESTINATION address in its header.
- **NAT alters one (or even both) of the IP header addresses.**
- If the SOURCE address is replaced, we talk about Source NAT (SNAT).
- If the DESTINATION address is tampered with, we have a case of Destination NAT (DNAT).

Why do people use NAT ?

Today, NAT is used primarily for

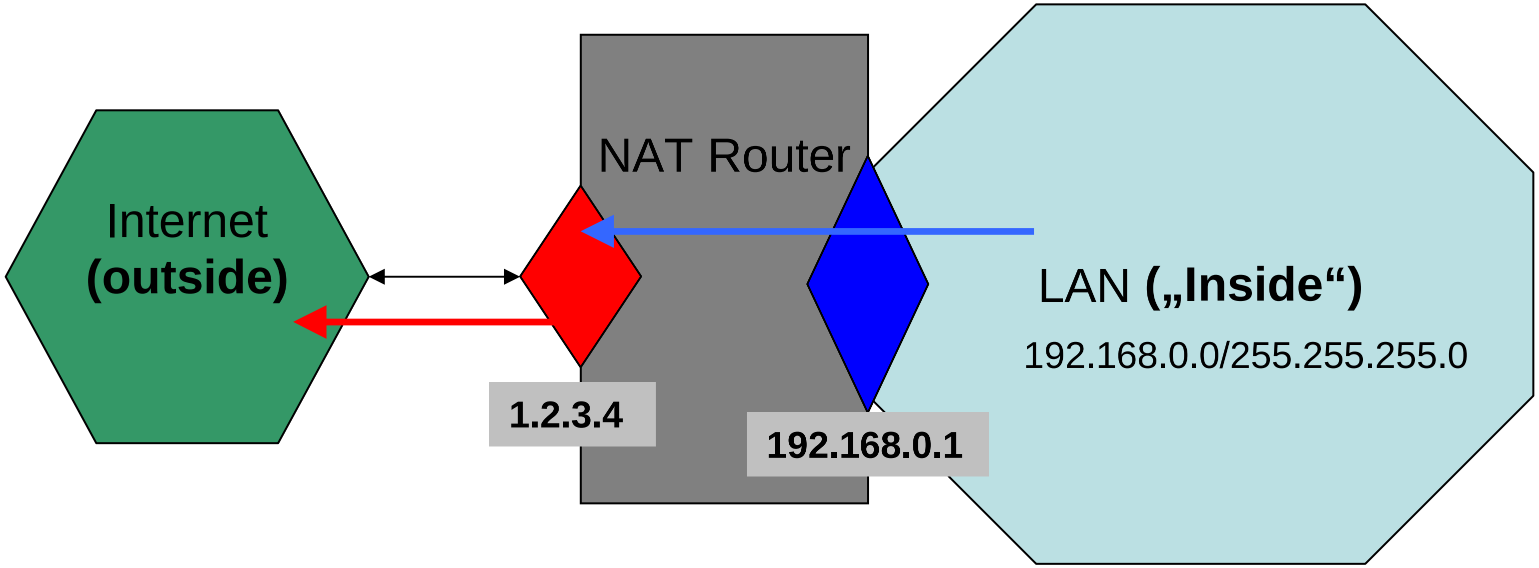
- Attaching private Networks to public Networks (uses SNAT).
- „Hiding“ or „Relocation“ of Network Services (uses DNAT).

What is Masquerading ?

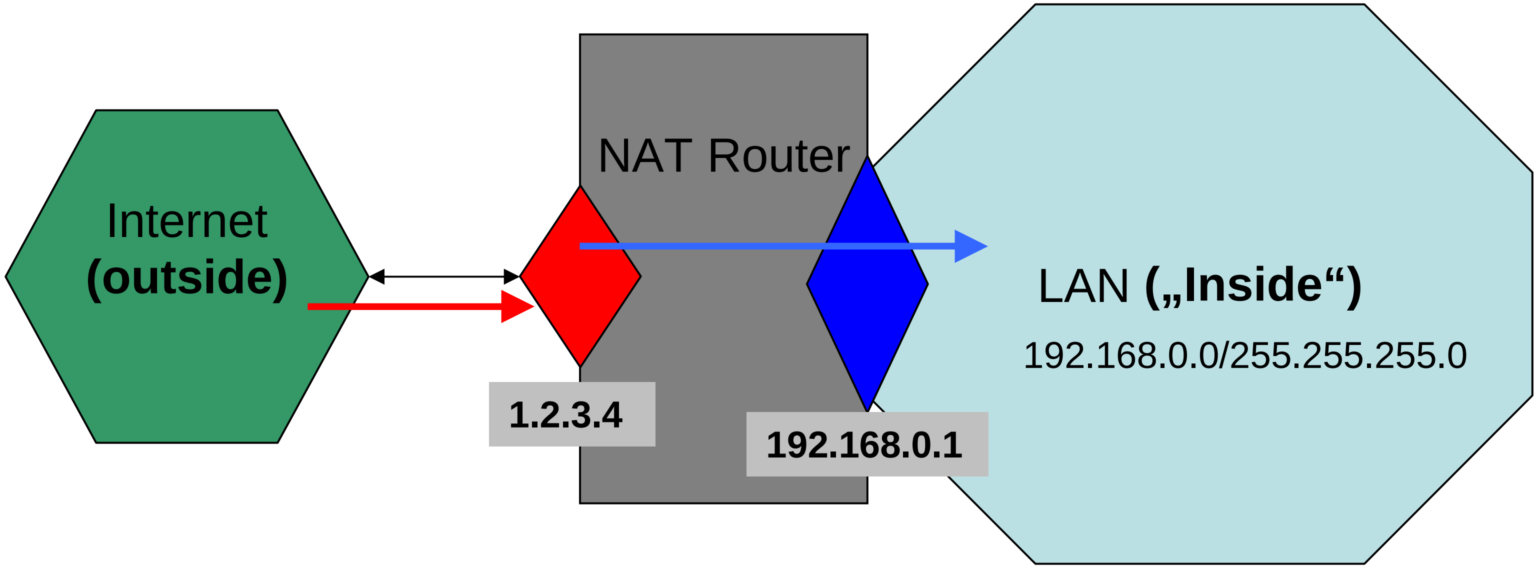
- Masquerading is a special case of SNAT, where a router replaces the source address of in-transit („outgoing“) IP packets with the address of its outbound interface. The router will typically translate more than one source address into his interface address (meaning he has more than one client „behind“ him), and he is able to „remember“ the original source addresses, so he can transparently manage multiple connections for multiple clients at the same time.

A practical SNAT example

We have a LAN using a private Class C IP network, connected to the via a router. Since the private IP addresses are not routed **on the Internet**, we have to apply **SNAT** on the routers **external interface**. The routers **internal interface** serves as the default gateway for the LAN.



We add a rule to the router, telling him to replace the source address of all packets **crossing his external interface from inside to outside** with (in this case, his own) IP address **1.2.3.4**.

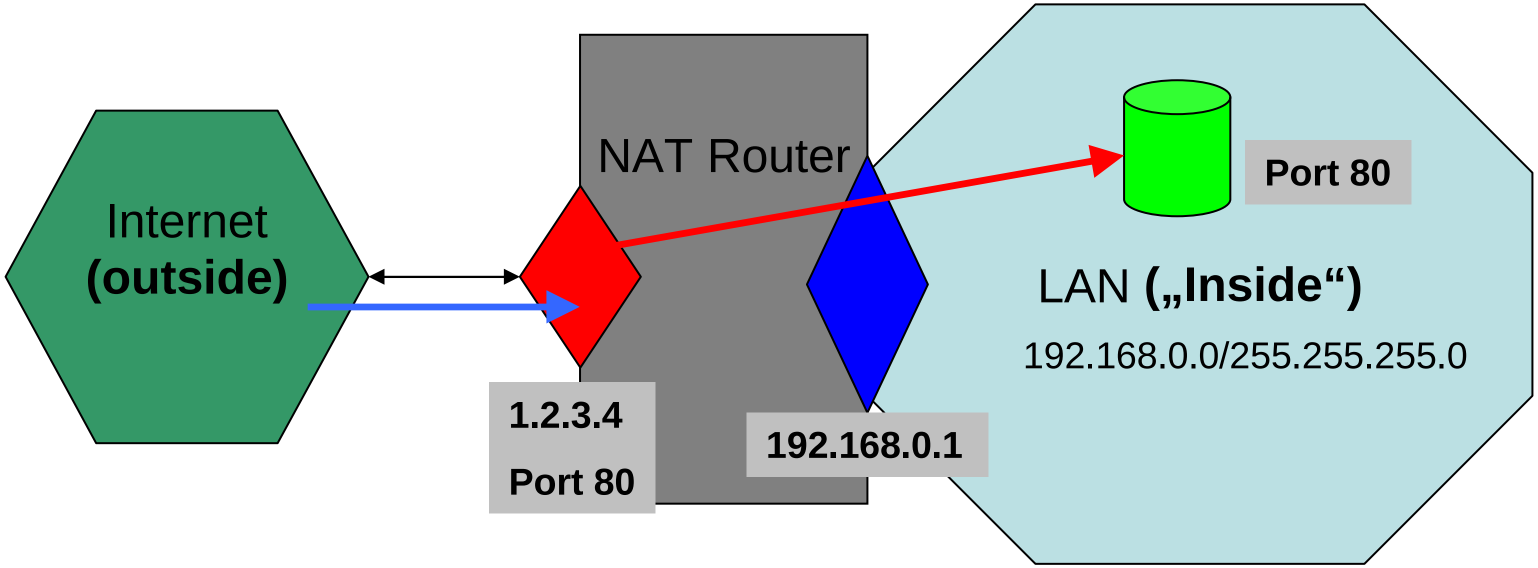


Once the request gets answered from the Internet host, the NAT router will receive the reply packets and will forward them to the client on the LAN.
This already shows one of the downsides of simple SNAT: the Internet server won’t be able to **initiate** a connection to a client on the LAN, since it’s own destination address is not routeable on the Internet. Some people see this as a security feature, which it is not (RFC1631 also has some words on this).
Another Note: If the IP of the outgoing Interface is dynamic (instead of the static 1.2.3.4) and the rule on the NAT router dynamically translates into the current IP, then this example would show **Masquerading**.

A simple, practical DNAT example

In this scenario, we look at a setup, where we have a network server running in the LAN, providing a network service (here: HTTP on Port 80) with an address in the 192.168.0.0/24 range. Now we want to make this service accessible to hosts on the Internet.

To do this we add a rule on the NAT router to translate the Destination Address of incoming packets, destined for HIS address on Port 80, into the address of the real network server on the LAN. The packets then get forwarded. Answer packets from the network server will the treated by replacing the source address.



NAT trivia

- Practical DNAT implementations can map all iterations of single IPs/IP Networks with single Ports/Port ranges TO single IPs/IP Networks with single Ports/Port ranges. For example, you could use a “Single IP/Port to IP Network/Port” as a load balancing mechanism.
- Adding a SNAT rule will also do DNAT on the reverse data path, and doing DNAT will add SNAT on the “way back”, so the difference is only in how the initial connection setup is handled.
- Many NAT routers run special software to enable the translation of more complicated application protocols (in Linux, these are the ip_masq_xxx modules, for example).
- NAT is not a firewall. Many people mean NAT when they say “I am behind a firewall”. This is not exactly true.
- NAT was developed to overcome the limitations of the IPv4 address space. Thanks to NAT, we can still use IPv4 on the internet today.

The Dark site of NAT

If NAT is such a wonderful thing, why does not everyone use it ?

- NAT requires CPU processing power. That adds latency to the network. With simple translations, this is not much of a problem, but with very large translation tables, it will become an issue.
- NAT increases the probability of miss-addressing, especially in more complicated application protocols (for example FTP).
- NAT breaks other applications completely, or at least makes them difficult to run (IPSEC comes to mind).
- NAT hides the identity of hosts. While this has the benefit of privacy, it is generally a negative effect.

References

- RFC 1631 gives more (and more advanced) examples.

  http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc1631.html