

NAT Example

NAT Client

The local machine using the Network Address Translation (NAT) router has a non-routable IP address, such as 192.168.1.2

The local machine can do normal TCP connections – the NAT router makes NAT work transparently.

Note that IP datagram from/to addresses represent the endpoints of the whole conversation

NAT Router

The NAT router has a local side (192.168.1.1) and a side connected to the Internet (1.1.1.1)

The NAT box translates the traffic going out and re-writes the from: so the datagram appears to be from the NAT box itself (1.1.1.1) using an random available port number (200 below).

In this way, all of the local machines share the NAT 1.1.1.1 connection to the Internet. Hosts out on the internet see the traffic coming from the NAT router itself (1.1.1.1).

When doing the re-write, the NAT box keeps a table of which port number is working for which local machine, so that when traffic comes in, it can be directed to the right local machine.

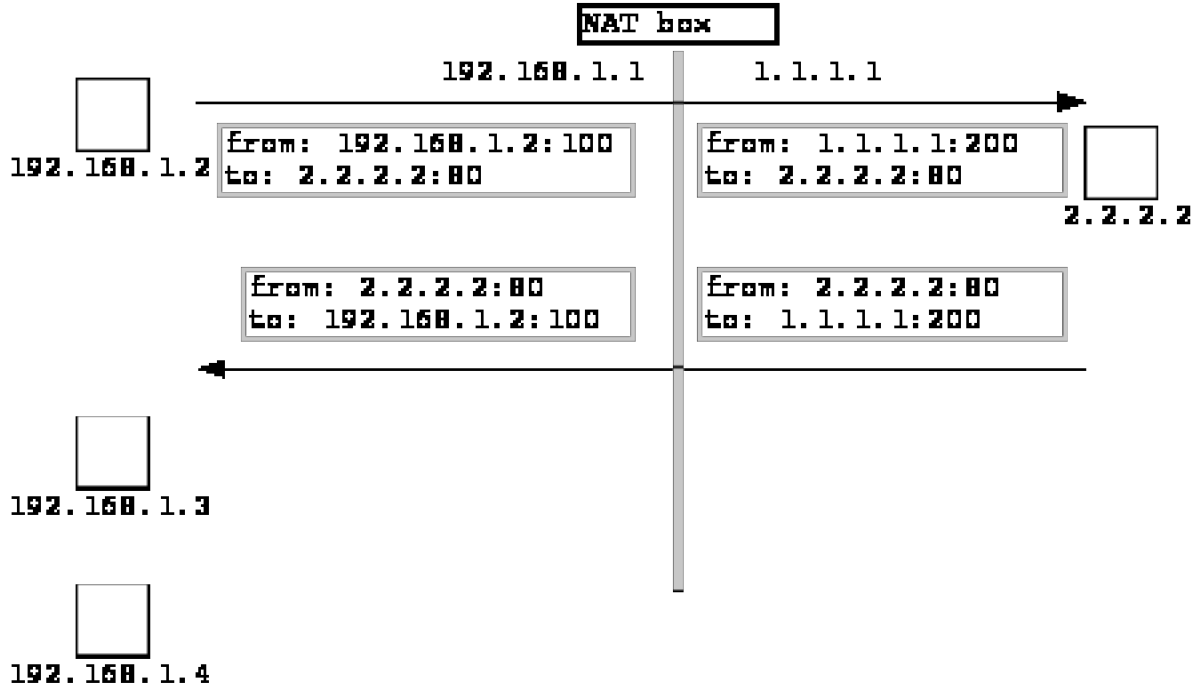
For the example below, the table might look something like...

connect to:2.2.2.2:80 using:1.1.1.1:200 for local: 192.168.1.2:100

When datagrams come in to the NAT box from the Internet, the NAT router re-writes the to: for the appropriate local machine.

NAT Example

Here we see local machine 192.168.1.2:100 sending a datagram to port 80 of 2.2.2.2 on the Internet. The ":100" represents the arbitrary port number chosen by the local machine for its end of the connection.



NAT Problems

1. NAT works for connections initiated from a local machine, but what about connections coming from outside?
Can set up mappings so port 80 connections go to local machine 1, port 110 connections go to local machine 2, ...
2. If the local machine honestly thinks its address is "192.168.1.2". But to the rest of the world, the address appears to be 1.1.1.1. If the local machine sends out a packet that includes as data something like "you can contact me later at my address: 192.168.1.2" , it's not going to work. The to/from in the datagram headers work because the NAT box knows to re-write it, but if the address is in the payload somewhere, the NAT router never gets a chance to fix it.

IPv6

The next generation IP system has 128 bit addresses, so in theory there's no need for NAT – every little device can just have its own address.

128 bits is so exponentially large, we will never run out of addresses.