Network Address Translation

For this article, and understanding of network addresses, subnets and ports is required.

Reasons for NAT

When communicating via the Internet, the TCP/IP protocols, along with UDP are the most used ones. There are two different flavors, the older IPv4 and the newer IPv6. Bot can basically be distinguished by the length the address of each host has. V4 uses 32 bits, which translates to a maximum of 4'294'967'294 possible hosts (if all were in one big subnet).

As you can imagine, 4 Billion Computers may sound a lot at first, but since nowadays many people have more than one computer device (one tablet, a smartphone, a PC, maybe a console, and you already have four devices in use, not counting the servers you are connecting to), this number quickly was identified as a little to short. IPv6 uses 128 bits of address space, which leads to a theoretical astronomical number of hosts of around 3 times 10 to the power of 38. That solves the problem with the address space once and for all. But as both protocols are still used, the old IPv4 still needed a solution for the problem of a lack of available addresses. If everyone had all the used devices on the public internet, the address space would have been exhausted years ago. The solution comes in form of a translation mechanism, that is usually facilitated by your router.

Mechanism

The router takes the function of a gateway, meaning, all internet connections have to go through it. Your local network is separated from the rest of the internet. It is using its own subnet, its own IP address space. Usually so-called private addresses are used, that are not routed through the internet (making them technically not reachable over the internet, but only on the local network). This way, certain IP addresses can be re-used for every one at home. They don't interfere with the rest of the internet.

But as this is kind of a separated, unreachable network, how do computers communicate to and with those, anyways? The answer lies in the Network Address Translation concept. Your router works as NAT. In principle, the following happens: Every package that is sent from your local network get's stripped of its source address (sender) and source port. Both are replaced with the address of the router on the other side, the internet, and another port. The router remembers which source address and port combination he gave which port on the internet side.

This way, the internet sees only the router's IP and some port he selected is opened for communication (temporarily). This saves up public IP addresses, making the IPv4 driven internet still feasible, even when working with actually far more than 4 Billion devices. Now when a package arrives, that is communicating with that port on the router's address, the router translates that back. It removes his own address and port and replaces it back again with the original address and port of the computer behind it in the local network and sends the package on it's way to the actual recipient. This way, one can communicate outwards without even noticing that there is something in-between, altering destination addresses and ports.

Now the only problem is, when an outside host tries to make contact with a computer behind the NAT, on the (private) local network, when there was no previous outward communication. The router won't have a port open for that connection and will refuse the connection altogether. This is where port forwarding becomes necessary.

Difference to a Firewall

There are many people, that mistakenly use the term „firewall“ for the NAT. That' is *not* the same thing. A NAT may serve a certain blocking role, as it won't relay packages, that are not part of an established connection. But this is more of a side effect. A real firewall can do a whole lot more, like package inspection (is the content of a received package somehow problematic) and discover certain ways of circumventing the NAT blocking. The difference, that is spottable most easy is the case of an out-going communication. This is never blocked by a NAT, nor are the replies to such a communication blocked. (This would in-fact make communication impossible.)

IPv6 still blocked

NAT mechanisms are not required for IPv6, as every host can have one or more (and usually has more than one) address at its disposable, making it addressable by itself also via the internet. A NAT is still not needed. Still, most routers block that kind of incoming communication anyways, as there are a security concerns when a computer is accessible directly from the world wide internet. But this is *not* the NAT (as there is never any translation of addresses involved), but simple blocking of communication. (This is far more close to a firewall, than the NAT is.) Many routers allow that to be turned off. Only do this, when you know what you are doing! When in doubt, only unblock the desired ports. (This is very often configured at the very same place in a router's configuration, as the NAT port forwarding.)

[Games Database] [Game Related Terms] [Network Terms]