

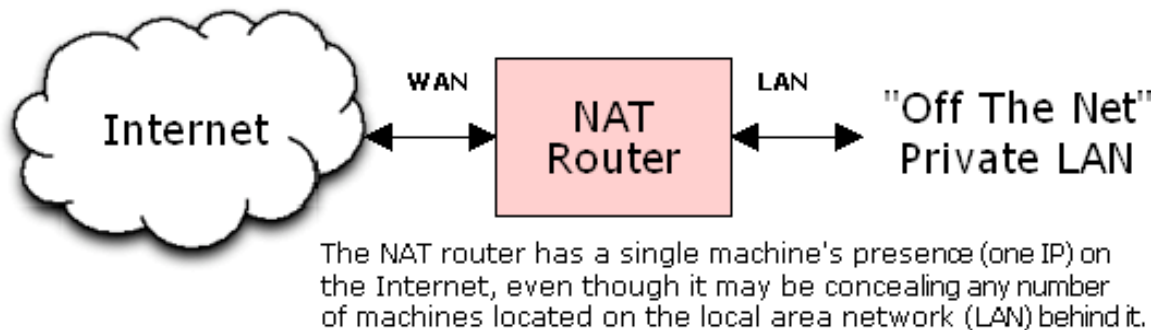
NAT: Network Address Translation

Ben Woodruff

CPT 216 181

Abstract

NAT, short for Network Address Translation is a technology that allows one or more nodes to hide behind and “share an IP” with a network device. This device is typically a router. This adds a layer of security because the devices that are not behind the NAT device do not know the IP addresses of the devices behind it, and can’t route them. The IP addresses are generally in the private address space (192.168.x.x, 10.x.x.x, or 172.16-31.x.x).

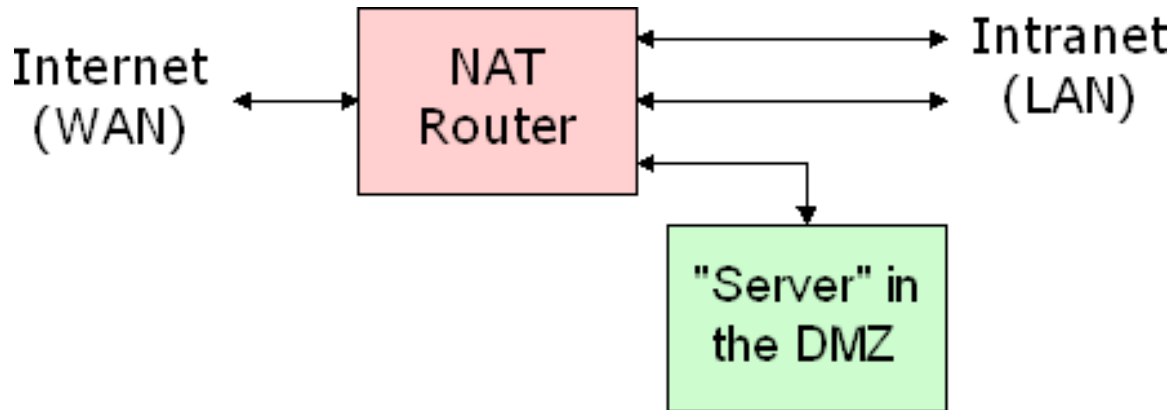


(Gibson, 2006)

In order for NAT to work the source or destination IP address and the checksum of the packet needs to be re-written by the NAT device. Because of this, NAT can have a negative impact on the performance of a network. However, due to the limited address space of IPv4, the current standard, most internet-connected networks do implement some kind of NAT (Wikipedia, 2008).

There are two kinds of NAT. PAT or Port Address Translation is the more complex, but more common kind. This technology involves “mapping” ports to specific machines (also commonly referred to as forwarding). This would allow you to, for example, run a web server on port 80 on one node, and a mail server on ports 25 and 110 on a different node. Most consumer level routers use this technology, but the terminology isn’t standardized (even within the same brand). The other NAT, basic NAT, does not do port mapping. It only does address translation (Wikipedia,

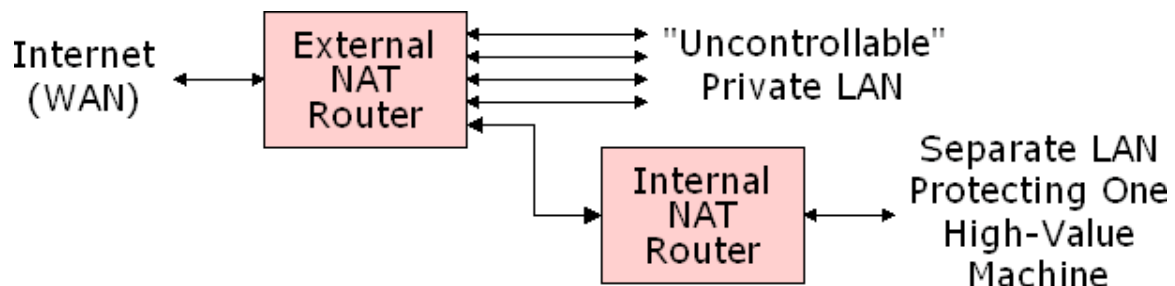
2008). This feature is also commonly available in consumer level routers, and is often labeled “DMZ” – although it is slightly different than the definition of DMZ that we generally work with (where you are using a three legged router). As you can see from the diagram below, this type of DMZ is less secure than using a three-legged router because the DMZ host is still part of your internal LAN.



(Gibson, 2006)

Often NAT routers are used as a firewall. The reason for this is because, in general, unless you have a port forwarded to one of your clients, nodes on the internet are not able to interact with (or attack), or even see your client nodes.

In the case where you are going to have a DMZ, or an unprotected wireless access point, you can setup a second NAT router within your internal network to protect high-value clients from the unprotected clients (Gibson, 2006).



(Gibson, 2006)

The way this could work is that you would setup your unprotected wireless router as the “External NAT Router,” and place your DMZ host (if any) directly behind that.

Then you would place your other machines (machines that are more mission critical and require a higher security level) behind what is labeled as the “Internal NAT Router.”

NAT can be confused with proxying technology, as they have a similar function (masking the client’s IP address by providing the server’s instead), but they are different technologies. One of the primary differences is that proxy servers are not transparent. The client node knows that it is making its requests to a proxy server, but it does not know when NAT is occurring (Tyson).

NAT is an important part of most every network. It provides a means for client nodes to talk to the internet without having a separate publically addressable IP for them. NAT also adds a layer of security through obscurity.

Works Cited

Gibson, S. (2006, Aug 8). *NAT - The Security of Network Address Translation*. Retrieved from GRC: <http://www.grc.com/nat/nat.htm>

Tyson, J. (n.d.). *How Stuff Works*. Retrieved from Nat Security: <http://computer.howstuffworks.com/nat5.htm>

Wikipedia. (2008). *Network address translation*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Network_address_translation