

## Re: router causing ssh etc. slowdown?

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Fedora/2004-10/5050.html>

---

**From:** Stewart Nelson (*sn\_at\_scgroup.com*)

**Date:** 10/25/04

To: <fedora-list@redhat.com>

Date: Mon, 25 Oct 2004 22:21:40 +0200

>> *Most NAT routers don't work properly when you connect to a (forwarded)  
>> port on their public IP from a host on their own LAN.  
>>*

> *Would like to understand which NAT routers don't work and how they fail.*

> *I have found different NAT routers respond differently. For instance,  
> using a standard Linksys NAT router and a Netgear FVS 318 router (has  
> VPN support) produced different results. Systems connecting from the  
> LAN using the public IP address on the Linksys router would have their  
> packets redirected to the LAN retaining their local IP address as the  
> source.*

This is typical (incorrect) behavior, but IMO you also have a bug in the originating host's TCP stack if it works at all.

Let's say host A (192.168.0.2) starts a TCP connection from its port 1025 to 1.2.3.4 port 22. The router sends the SYN packet to host B (192.168.0.3) port 22, leaving the source IP address unchanged. Now, host B must send the ACK directly back to A; it has no information to do anything else. The router is not in the path of the reply, and cannot affect it. When A receives the ACK, it will have a source address of 192.168.0.3 — that's not the address it sent the SYN to, so the packet should be ignored, or answered with a RST. If the TCP connection gets opened, there is something wrong with host A.

> *The Netgear router would actually translate the source address  
> to the public IP address.*

That's how it should work.

> *This had some interesting implications for  
> SMTP and relaying for LAN based clients that were configured such that  
> they used the public IP address of the SMTP server.*

IMO, you should only do that if the NAT has a static public IP.

Fedora: Re: router causing ssh etc. slowdown?

Otherwise, your outgoing mails will often be rejected by servers that won't accept mail sent directly from dynamic addresses. If you do have a static address, it is easy to configure the SMTP server so that relays from the NAT's public address are trusted.

- > *I attribute this*
- > *difference to slightly different interpretations of the specs, the one*
- > *device performs the NAT prior to routing the packet back to the LAN*
- > *while the other device either recognizes the packet remains on the LAN*
- > *or reverses the NATing prior to sending the packet on to the*
- > *destination.*

IMO, there is only one correct way -- the router must set up the usual dynamic association for the outbound leg, and use its static (forwarding) association for the inbound leg. Both hosts will see the public IP as the source address of packets that they receive.

- > *As to why a NAT router would cause a slow down for ssh I don't know.*
- > *With the various linksys and netgear devices I have used I have not seen*
- > *a slow down in connectivity when using ssh, and I use ssh extensively*
- > *both locally and remotely.*

I don't either. It would be interesting if Ben would run Ethereal on his systems and see what the router is doing to his packets.

--Stewart

--

fedora-list mailing list  
fedora-list@redhat.com

To unsubscribe: <http://www.redhat.com/mailman/listinfo/fedora-list>