

Re: Can't seem to get packets to route

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2003-08/1581.html>

From: A. Trent Foley (*helpme_at_trentfoley.com*)

Date: 08/23/03

Date: Fri, 22 Aug 2003 21:14:24 -0500

On Sat, 23 Aug 2003 01:30:48 +0000, David Efflandt wrote:

> Path:

> *internal1.nntp.ash.giganews.com!border3.nntp.ash.giganews.com!border2.nntp.
> ash.giganews.com!border1.nntp.ash.giganews.com!firehose2!nntp4!intern1.nntp
> .aus1.giganews.com!border1.nntp.aus1.giganews.com!nntp.giganews.com!feed2.n
> ews.rcn.net!rcn!news.maxwell.syr.edu!news.xnet.com!efflandt
> From: efflandt@xnet.com (David Efflandt)
> Newsgroups: comp.os.linux.networking
> Subject: Re: Can't seem to get packets to route
> Date: Sat, 23 Aug 2003 01:30:48 +0000 (UTC)
> Organization: XNet Information Systems, Inc.
> Lines: 36
> Message-ID: <slrnbkdgu8.g7n.efflandt@typhoon.xnet.com>
> References: <pan.2003.08.22.19.49.09.8412@snl.com>
> NNTP-Posting-Host: typhoon.xnet.com
> X-Trace: flood.xnet.com 1061602248 11812 198.147.221.66 (23 Aug 2003
> 01:30:48 GMT)
> X-Complaints-To: abuse@xnet.com
> NNTP-Posting-Date: Sat, 23 Aug 2003 01:30:48 +0000 (UTC)
> User-Agent: slrn/0.9.7.0 (SunOS)
> Xref: intern1.nntp.aus1.giganews.com comp.os.linux.networking:425166
> MIME-Version: 1.0
> Content-Type: text/plain*

>
>

> On Fri, 22 Aug 2003 14:49:10 -0500, Anonymous <Nobody> wrote:

>> I currently have my network as a 192.168.xx.xx nonroutable behind a
>> single routable ip using a linux box doing nat. I've been doing this
>> for years and have had no troubles.

>>

>> I am switching providers and now have 8 routable ips all in the same /24
>> subnet. This is new ground for me and I'm having troubles. I'm
>> guessing that the root of my problem is in my subnetting. I am trying
>> to set up a new router with 3 nics - one for my isp connection, one for
>> a dmz, and one for my lan. Once I get the routing working, I will worry
>> about setting up netfilter. I don't have the entire /24 to myself, but
>> my new isp seems to be blocking addresses not assigned to me. So, I

comp.os.linux.networking: Re: Can't seem to get packets to route

>> *think it is safe to subnet the /24 any way I wish. This may be my
>> problem... I took a look at my ip addresses and came up with the
>> following:*

- >
- > *What is the actual netmask or significant bits of your IP block? Typically*
- > *with 255.255.255.248 netmask (/29) your 8 IPs end up as network IP, WAN*
- > *IP, 5 usable IPs and broadcast IP. Although, creative networking may be*
- > *able to utilize more than 5 of them. Your internet interface should*
- > *likely have netmask 255.255.255.255, bcast same as its IP, host route to*
- > *gw, and default route to gw (which is typical for my adsl ISP), since the*
- > *only IP you need to route to locally in that direction is the default gw.*
- >
- > *Using unauthorized public IPs can cause a good deal of confusion,*
- > *especially when that network overlaps your assigned IP range. For example*
- > *you would need to masquerade the unauthorized IPs for them to access the*
- > *internet, but not your authorized IPs.*
- >
- > *So you should likely have your 2nd nic as DMZ (your assigned public IPs*
- > *with 255.255.255.248 netmask), and 3rd nic as private IPs masqueraded to*
- > *the internet as the IP of your internet interface. This would make*
- > *everything much easier to figure out and keep straight.*

Thanks for the quick response.

First of all, my main purpose in doing this is to stop using NAT. I want every machine on my network to have a routable address. But, for the sake of simplifying firewall rules, I wanted to have two segments — one very protected, and one not very protected. I could plug my broadband link straight in to my switch and then configure each machine with a separate firewall. I tested this on a couple of computers and it worked just fine, but I want a central firewall/proxy/vpn/router to ease administration and to reduce potential errors.

I get 8 usable ip addresses with my new ISP (Speakeasy). They are all on the same /24 subnet. I was kind of suprised by this as I expected to get a /29 with 5 usable, as you mentioned. However, each of these 8 I get are usable and are subnetted by my ISP in the same /24. I have provisioned only 5 of them so far since that is my current need. I did the subnet analysis shown above of the addresses they assigned to me to see if I could break them up cleanly into subnets. I was able to make three subnets out of them. The only place where I am using addresses that are not assigned to me are on the internal interfaces on the router (a.b.c.62 and a.b.c.254, and by subnetting, a.b.c.128, a.b.c.63, and a.b.c.32).

Thanks,
-Trent