

<LONG>Re: Dual NICs, Routing Problem

Source: <http://linux.derkeiler.com/Newsgroups/alt.os.linux.suse/2005-12/msg03062.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Wed, 28 Dec 2005 21:06:50 -0600
-

On 28 Dec 2005, in the Usenet newsgroup alt.os.linux.suse, in article <1135810804.980685.106810@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Tom Kersten wrote:

>Moe Trin wrote:

>> Do you have permission from BBN Communications to be using these
>> addresses?

>

>I have modified the IP addresses that my node is using. I am actually
>on a corporate network and the subnet is 10.x.x.x. So, for example,
>instead of 192.1.34, my subnet is actually 10.1.x.x. I changed the IP's
>just because it makes me leary...probably not necessary and may have
>created more harm than good. If so, I apologize.

OK – see RFC3330 which talks about this. 10.0.0.0/8 is RFC1918 IP space, and is totally irrelevant to the Internet at large. From outside the perimeter, you can't reach a 10.0.0.0/8 address, because no one knows where it might be, and RFC2827 recommends any packets with such addresses be silently discarded at the perimeter router.

>I will stick with the modified IP's just to prevent the confusion of
>switching to totally different range.

OK.

>>> 192.1.36.0 192.1.36.1 255.255.255.0 UG 0 0 0 eth0

>>

>> Wrong. 192.1.36.0 is directly attached to eth0 – no gateway needed.

>

>I don't understand why it won't work then. Having it set up the way it
>is listed above does not work. If I remove this entry, it still does
>not make it work.

What happens if you change it to

192.1.36.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

>But if I make the default gateway of the machine 192.1.36.1 it does work,
>but no external web requests are resolved correctly.

<LONG>Re: Dual NICs, Routing Problem

There can only be one default gateway (unless you are using extra stuff as mentioned in the Adv-Routing-HOWTO). A gateway is only needed to reach a network that is NOT directly attached to one of your interfaces. You have two (eth0 and eth1), and to speak to hosts on those networks, your kernel need only look at the routing table and choose the correct interface. NO GATEWAY IS INVOLVED.

>I am assuming you are referring to the 169.x address. I have removed
>that numerous times, but when I go into yast and modify the routing
>table (to troubleshoot), it puts this entry back in, so I have just
>left it because I was assuming it was not causing an issue.

Yeah, it's a windoze "feature" that allows for unconfigured systems on the local wire (usually because the MCSE screwed up the configuration of the DHCP server). There is an option in the network configuration scripts to disable this, but it's not part of this problem.

>This gateway is the way to the world. I am considering 'the world' as
>the internet. This gateway does not know anything about the 36 network.

That's a capital Internet, not the lower case internet (meaning the rest of the local networks). We don't care about the 36 network, because this system knows how to talk directly to it – just shove the packets out the eth0 interface.

>> Do all the hosts on 192.1.36.0 know that if they want to talk to any host on
>> 192.1.34.0, they have to send the packets to the gateway at 192.1.36.11?
>
>Just to make sure, I am assuming you meant 192.1.36.1. The 192.1.36.11
>IP is the IP I have assigned to eth0, which has just been given a
>static IP on the 192.1.36.x subnet.

Actually, I mean all hosts that will have a need to talk to a host on the '34' net.

>I don't really want all of the hosts on 192.1.36.0 to be able to talk
>to that network, if that's possible. I only want one node on the
>192.1.34.0 network to be able to talk to another single node on the
>192.1.36.0 network.

Those hosts that are on the 36 net that have to talk to the 34 net (and vice-versa) need to know where to send the packets in order to have them get through. Those that DON'T need this capability don't need to be told about it.

>If it ends up that the node in the DMZ (192.1.34.0 network) has to be
>able to talk to any machine in the private VLAN (192.1.36.0 network),
>that will be OK, but I only need it to talk to our DB server...and would
>ideally only want that channel of communication open between the networks.

<LONG>Re: Dual NICs, Routing Problem

My preference would be a dedicated network between extra NICs (using a cross-over cable) in both systems. We do that quite a lot to keep admin traffic off the "ordinary" net for example.

>Because I can't make ascii art ever turn out, here is a brief
>explanation of what I am trying to accomplish.

Big clue – fixed width fonts. OK, let's try this:

```
the world <--- DMZ ---> eth0 WebServer eth1 <--- secret net ---> eth0 DB_srvr
```

Here, the web server needs to know the IP of eth0 on the DataBase Server, and route requests to it over the cross-over cable of the "secret net". The DataBase Server can have a second NIC going to an inside NIC, but that's not relevant to this conversation (though it's a security problem in it's own right). On the web server, the routing table looks like this:

```
DMZ.net 0.0.0.0 255.255.whatever U 0 0 0 eth0
secret.net 0.0.0.0 255.255.whatever U 0 0 0 eth1
0.0.0.0 DMZ.gateway 0.0.0.0 UG 0 0 0 eth0
```

I'm ignoring absolute IP addresses and the loopback as not relevant. Fill in the blanks as required. On the database server, the routing table is

```
Inside.net 0.0.0.0 255.255.whatever U 0 0 0 eth1
secret.net 0.0.0.0 255.255.whatever U 0 0 0 eth0
```

If there is a way to the world using the inside net, there would be a default route using that, via eth1 – perhaps

```
0.0.0.0 Inside.gate 0.0.0.0 UG 0 0 0 eth1
```

Now notice – the DB server doesn't know anything about the DMZ, and the web server doesn't know about the inside net. The ONLY other network they both are aware of is that 'secret' net that connects the two. Again, notice that the ONLY gateway mentioned are those that lead to networks that are not directly attached to the individual hosts. IN THEORY, if the web server wanted to talk to SOME OTHER host on the inside network, it would send the packets out the DMZ gateway, to the Internet, which would then route them to the company firewall that protects the inside net from the big bad world, and so on. Replies would go the opposite route. NO TRAFFIC IS POSSIBLE between the Web Server and the inside net over the "secret.net", because the web server doesn't know it leads anywhere except to the DB server ONLY. Same bit from the inside net, in that they don't know of the existence of the 'secret.net', much less where it might lead. Any other hosts on the DMZ net also don't know of the 'secret.net' much less that an inside net even exists.

I mention that this is a security problem. There should be a firewall on the DB server, that only accepts DB requests from the eth1 address of the web server, AND NOTHING ELSE on that interface. Assuming both servers

<LONG>Re: Dual NICs, Routing Problem

are Linux, NEITHER SHOULD HAVE IPv4 FORWARDING ENABLED. They don't need it. The only traffic on that secret net is "locally generated packets" between the two servers. If you are running a firewall on the web server (I don't think I would), it should block all "new" (not DB) traffic from the DB server to prevent a covert channel. This actually should be handled by the firewall on the DB server, but what ever floats your boat.

>So, the 'thought' was that I would be able to set up a rule that any
>traffic that was headed to the 192.1.36.0 network would use gateway #1
>(192.1.36.1) and all other traffic would be sent out gateway #2 (the
>default gateway, 192.1.34.254).

Sounds like windoze _nomenclature_ The windoze routing table is a "baffle 'em with bullsh!t" situation – intentionally over complex to scare the sheep away from this technical stuff. They tend to misuse words, mainly because they invented IP networking 13 years after the rest of the world, and never understood what the words actually meant. The so-called "Gateway Address" is one example of microsoft's total lack of concept.

>Is this possible? I was told by our IT guys that it is not a problem in
>Windows, so I assumed it was an option in SuSe also. I am beginning to
>think it is not the correct way to set it up, but am not sure...

Hopefully, my long winded explanation makes sense to you. This is actually a trivial setup. If you wanted to have more hosts on the "secret net" (I would not), their routing tables would mention the secret net to allow them to talk to hosts on that net. I would NOT recommend adding a router, as that could be a security risk. If those additional hosts have to talk to the DMZ, or inside net, give them a second NIC to do so, and make sure they have appropriate firewall rules to prevent leaks.

Old guy
.

• *Follow-Ups:*

- ◆ **Re: <LONG>Re: Dual NICs, Routing Problem**
◇ From: Tom Kersten

• *References:*

- ◆ **Dual NICs, Routing Problem**
◇ From: Tom Kersten
- ◆ **Re: Dual NICs, Routing Problem**
◇ From: Tom Kersten
- ◆ **Re: Dual NICs, Routing Problem**
◇ From: Moe Trin
- ◆ **Re: Dual NICs, Routing Problem**
◇ From: Tom Kersten

<LONG>Re: Dual NICs, Routing Problem

- Prev by Date: ***Re: Visioneer 4400 USB scanner***
- Next by Date: ***Re: Where are the SuSE 9.2 Professional CD ISOs?***
- Previous by thread: ***Re: Dual NICs, Routing Problem***
- Next by thread: ***Re: <LONG>Re: Dual NICs, Routing Problem***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***