

## Re: Liunx and DSL routing

**Source:** <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2004-07/0276.html>

---

**From:** Will Hall (*culdespamsac\_at\_yahoo.com*)

**Date:** 07/07/04

Date: 7 Jul 2004 11:06:40 -0700

Abdullah Ramazanoglu <ar018@yahoo.com> wrote in message  
Thanks for your comments – have added mine below (oh God, am I going  
to suffer the wrath of anti-top-posters?)

news:<40ead17c\$0\$23874\$14726298@news.sunsite.dk>...

> *Will Hall wrote:*

>

>> *I've been trying to figure this one out for a while and am getting  
>> my small brain into knots – so hopefully one of you guys (girls?)  
>> can shed some light.*

>>

>> *I run two Linux mail servers in different locations, but with  
>> similar setups: Each with static IP address (block of 4), DSL  
>> modem/router fed by the same ISP (PPPoA). The linux server has 2  
>> NICs, eth0 for private LAN (DHCP, NAT etc for Windows and Mac  
>> clients) and eth1 which is connected to the modem/router.*

>>

>> *For server A:*

>> *Public IPs are aaa.aaa.aaa.156–159 (I assume 156 is the network  
>> address, 157/158 are standard routeable addresses and 159 is the  
>> broadcast?)*

>

> *All of them are routable public addresses.*

>

>> *The modem is a Zyxel prestige 650R–31 with NAT/DHCP off and, as  
>> instructed by the ISP, has been configured to have a LAN address  
>> of aaa.aaa.aaa.158, subnet mask 255.255.255.252.*

>>

>> *The linux box (Slackware 9.1) is then configured to have:*

>> *IPADDR[0]="195.168.1.100"*

>> *NETMASK[0]="255.255.255.0"*

>>

>> *IPADDR[1]="aaa.aaa.aaa.157"*

>> *NETMASK[0]="255.255.255.252"*

>>

>> *GATEWAY="aaa.aaa.aaa.158"*

>>

>> *Which gives the routing table as:*

```
> >
> > aaa.aaa.aaa.156 0.0.0.0 255.255.255.252 U 0 0 0
> > eth1
> > 192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0
> > eth0
> > 127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0
> > lo
> > 0.0.0.0 aaa.aaa.aaa.158 0.0.0.0 UG 1 0 0
> > eth1
> >
>
> Waste of IP addresses though it works.
```

>From what I know, the basics are this: As I'm running a public mail server (amongst others) I need the public IP address aaa.157 assigned to eth1 on the server. The modem/router is assigned aaa.158 so the 255.255.255.252 netmask will happily sit between the two. Where I am confused is the difference between the modem WAN and LAN addresses.

```
>
> >
> >
> > So, to configure the router, I just telnet the gateway,
> > aaa.aaa.aaa.158 and everything is fine. This gateway is also
> > accessible to the outside world.
> >
> > Now, the second mail server is configured as follows:
> >
> > Server B:
> > Public IPs are bbb.bbb.bbb.76-79
> > Modem is a DLink DSL-300G+ with NAT and DHCP turned off. The
> > configuration is less flexible with this modem/router and fires up
> > with the following information (which I cannot change!)
> >
> > IP Address bbb.bbb.bbb.77
> > Gateway bbb.bbb.bbb.78
> > Connection Type PPPoA
> > Encapsulation VC Mux
> >
> > So in order to route to the modem I manually add the 192.168.0.1
> > route (see blow)
> >
> > The linux box (Slackware 9.1) is then configured as:
> > IPADDR[0]="195.168.2.100"
> > NETMASK[0]="255.255.255.0"
> >
> > IPADDR[1]="bbb.bbb.bbb.77"
> > NETMASK[1]="255.255.255.252"
> >
> > GATEWAY="bbb.bbb.bbb.78"
> >
```

> > *Which gives the routing table as:*  
> > *192.168.0.1 0.0.0.0 255.255.255.255 UH 0 0 0*  
> > *eth1*  
> > *bbb.bbb.bbb.76 0.0.0.0 255.255.255.252 U 0 0 0*  
> > *eth1*  
> > *192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0*  
> > *eth0*  
> > *127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0*  
> > *lo*  
> > *0.0.0.0 bbb.bbb.bbb.78 0.0.0.0 UG 1 0 0*  
> > *eth1*  
> >  
> >  
> >  
> *I am assuming modem's internal address is 77, since gateway is*  
> *specified as 78, implying the external address. But this*  
> *contradicts with your gateway settings in linux unless your modem*  
> *does proxy-arp the external interface to LAN (an unneeded*  
> *complication).*  
> *Your eth1 address is also 77 clashing with modem's IP address.*  
> *Then the 76 in routing table: Who is it? According to what is*  
> *presented above there is no 76 in your network.*  
> *Then the 192.168.0.1 in the routing table...*  
> >  
> *I don't see how this setup can ever work.*

It does. The 192.168.0.1 route is just so I can gain access to the modem's web interface from the LAN.

> >  
> > *This configuration also works fine!! But, I cannot "see" the*  
> > *gateway from the outside. ie nothing from nmap, cannot telnet –*  
> > *but this might be a security feature of the modem. I can telnet*  
> > *into it (via 192.168.0.1) but the commands are not exactly*  
> > *intuitive.*  
> >  
> > *So modem's LAN interface has two addresses (bbb.77 and 0.1) which*  
> > *means that your modem has IP aliasing feature (and enabled) at the*  
> > *LAN port? This suggests me that you have enabled DMZ mode on your*  
> > *modem and one of the LAN addresses is for DMZ network.*

Haven't touched any settings for aliasing or DMZ

> >  
> > *All in all, the whole setup seems incorrect, overly complicated and*

That's why I'm posting this!

> *fragile to me. I would suggest following one of two ways:*  
> >  
> > *1. Use your modem in bridge mode, exposing your server directly to*  
> > *internet and using up only one public IP address. In bridge mode*  
> > *the modem is a stupid piece of electronics (no ppp, no userid, no*  
> > *firewall, no NAT, no IP addresses, nothing but just raw ADSL*  
> > *connection to telco) like a dialup fax/modem. All the intelligence*

> *has to be implemented by the server. So you must run a pppoe  
> program to do all these (roaming penguen's "rp-pppoe" is probably  
> included in your distro). Your modem will not have any IP addresses  
> and the only public IP address will be assumed by the server, which  
> will be the one that your modem is getting now from ISP for its  
> external interface. Since you will be fully exposed to internet (as  
> you currently are), you will have to apply all the relevant  
> security measures. Some modems also have "half-bridge" mode,  
> handling the connection details (which would have been done by  
> rp-pppoe otherwise) but still providing bridge behavior. This could  
> be more convenient/easy to operate.*

I don't want to use bridge mode as I want to be able to perform  
reconnects to the ADSL service without touching the server, so I want  
the username/password authentication and negotiation on the modem.

>  
> *2. Or use your modem in router mode and route specific ports (NAT)  
> or all ports (DMZ) to your server. Here Linux box has only one  
> ethernet card, sharing the same LAN with other clients. If you use  
> DMZ mode of the modem, (depending on the modem) you have 2 aliased  
> networks on the same physical LAN segment: One is 192.168.x.0  
> (clients) the other is 192.168.y.0 (DMZ). Ethernet on linux has two  
> addresses, one for LAN, the other for modem. And your modem routes  
> all incoming connection requests to DMZ network (to your server).  
> The server is still exposed to internet, but somewhat more securely  
> because traffic first passes through the firewall on the modem.  
> Mind you, the term "DMZ" may change meaning from one modem to  
> another. Some means real DMZ with different network addresses,  
> others mean just forwarding all the ports. If you run only a few  
> services you might also consider plain port forwarding. In this  
> case modem and server don't have a second, aliased network address.  
> And everybody on the LAN, including modem and server have the same  
> network address (192.168.x.0), but your modem routes incoming  
> connection request to specific ports to the Linux server (with or  
> without translating port numbers). Security is more enhanced  
> because both you have the firewall on modem, and also you are  
> exposing the bare minimum, just required ports, of your server to  
> internet.*

I don't see any need for a DMZ. eth1 is "public" and eth0 is "private"  
with iptables doing the firewalling, port forwarding, syslogs etc. I'm  
happy that security is tight as only the required ports are visible to  
the outside world.

>  
>>  
>> *If you're still following this then thank you – I've nearly got to  
>> my point....*  
>>  
>> *Question: The difference is the LAN IP setup: the first has a  
>> routeable public IP and the second has a private address. Which is*

> > *correct? Exactly where do the gateways actually live?*  
> > *If I use bridging mode, do I need to bother with 4 IP addresses?*  
> >  
> > *Thanks for your help*  
> >  
> > *Will*