

RE: 2 NIC's on same network, possible?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-07/1008.html>

From: Burton M. Strauss III (*BStrauss_at_acm.org*)

Date: 07/29/03

To: <security-basics@securityfocus.com>

Date: Tue, 29 Jul 2003 11:08:51 -0500

No, you're wrong. The two – addresses and routing – are separate albeit related.

First, (to clean up one bit of confusion in the replies) 192.168.0.6/24 means a host address of 192.168.0.6 with a 255.255.255.0 mask – that is the 192.168.0 portion is the network address and .6 the host.

In the absence of fancy, load balancing software, let's look at how routing works (this is for Linux, but most network stacks work pretty much the same).

Internal to the Linux kernel is a routing table. It tells the network stack what to do with each packet.

```
# ip route show
192.168.0.0/24 dev eth0 proto kernel scope link src 192.168.0.36
127.0.0.0/8 dev lo scope link
default via 192.168.42.1 dev eth0
```

or, in it's more common format:

```
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use
Iface
192.168.0.0 * 255.255.255.0 U 0 0 0 eth0
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
default homeportal.gate 0.0.0.0 UG 0 0 0 eth0
```

Read this as follows...

Destination 192.168.0.0, genmask 255.255.255.0 – that's the network 192.168.0
iface – eth0 – that's the card #
metric – that's the 'goodness' of this route for the specified destination.
(or as defined in man route,
" Metric The 'distance' to the target (usually counted in hops). It

SecurityFocus BASICS: RE: 2 NIC's on same network, possible?

is

not used by recent kernels, but may be needed by routing
dae-
mons."

Similarly, the 'default' route is my router. What this means is that packets for anywhere else, not otherwise specified, should be stuffed out eth0, with the expectation that the 'gateway' (router), named homeportal.2wire.net, will pick them up and forward them on.

For each packet, the table is processed from most specific to least specific, and the first match wins.

So a packet to 192.168.0.5 matches rule 1 and gets stuffed out eth0
A packet to 127.0.0.1 matches rule 2 and gets stuffed out lo
A packet to 4.2.2.1 matches rule 3 (the default or 'last resort') and gets stuffed out eth0 also.

Say you now enable your eth1 NIC. The single interaction between having two NICs with identical network address portions (the 192.168.0 part) is that they can't have the same metric. Since the metric is used for sorting the table, the route table becomes:

```
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use
Iface
192.168.0.0 * 255.255.255.0 U 0 0 0 eth0
192.168.0.0 * 255.255.255.0 U 1 0 0 eth1
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
default homeportal.gate 0.0.0.0 UG 0 0 0 eth0
```

See the two routes to 192.168.0.0? But with different metrics??

Same rules apply...

A packet -> 192.168.0.5 matches rule 1 and gets stuffed out eth0
A packet to 127.0.0.1 matches rule 2 and gets stuffed out lo
A packet to 4.2.2.1 matches rule 3 (the default or 'last resort') and gets stuffed out eth0 also.

Suppose that 2nd NIC is really a private link to your database server, 192.168.0.14/24. You could add the special route to the routing table (see man route for the add syntax), to create a table that looks like this:

```
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use
Iface
192.168.0.14 * 255.255.255.255 U 0 0 0 eth1
192.168.0.0 * 255.255.255.0 U 0 0 0 eth0
```

RE: 2 NIC's on same network, possible?

SecurityFocus BASICS: RE: 2 NIC's on same network, possible?

```
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
default homeportal.gate 0.0.0.0 UG 0 0 0 eth0
```

Looks weird, right... but it works.

A packet → 192.168.0.14 matches rule 1 and gets stuffed out eth1
A packet → 192.168.0.5 matches rule 2 and gets stuffed out eth0
A packet to 127.0.0.1 matches rule 3 and gets stuffed out lo
A packet to 4.2.2.1 matches rule 4 (the default or 'last resort') and gets stuffed out eth0 also.

Now it gets weird if somebody is trying to reach YOU on the 2nd NIC. Why?
Because the routing decision is address based, not NIC based.

So a packet TO the address of the 2nd NIC (192.168.0.7) is received on the 2nd NIC. The reply, addressed say to 192.168.0.5 again, is sent VIA the 1st NIC (1st match in the routing rules wins!). Unless the sender also has this kind of funky routing table.

THIS is what leads to the 'rule' that you can't have two NICs with the same network portions, because if they're really NOT connected identically, you'll lose traffic, and if you're not really, really careful with routine rules (wait for it) (yes) you'll lose traffic.

Given that the entire 192.168.0.0/16 space is reserved for private networks (RFC 1918), you're a lot better off using another network (say 192.168.1.0/24) for the private link and let the regular and automatic routing rules apply.

But if you really get into specialized network design, sometimes you have to do this kind of scary junk...

-----Burton

-----Original Message-----

From: Vineet Mehta [mailto:vineet@linux.com.kw]
Sent: Sunday, July 27, 2003 9:49 AM
To: security-basics@securityfocus.com
Subject: 2 NIC's on same network, possible?

Hi all,

My colleague has a Linux machine which has 2 NIC's on it. What he did was assign the IP's 192.168.0.6/24 and 192.168.0.7/24 to the NIC's. And he was trying to ping the network but was getting errors (i dont know the errors).

```
-----
| Switch |
|_____|
||
```

RE: 2 NIC's on same network, possible?

SecurityFocus BASICS: RE: 2 NIC's on same network, possible?

```
||
||
-----
| NIC1 NIC2 |
|192.168.0.6/24 192.168.0.7/24|
| Machine |
|-----|
```

I tried explaining him like this:->

Configuring the machine's network like this is not a big problem, coz other machines on the network can still see these 2 IP's. But his machine will not be able to reach other machines on the network coz 2 NIC's point to the same network so Linux kernel would be confused for which NIC to use to send packets. If by any means we set the route to use ANY one NIC to reach the network then there will be no errors.

Am i right in this, or this is not possible AT ALL? I took my thought from the concept of IP Aliasing.

Thanks in advance for any help.

Regards,

```
--
Vineet Mehta
Network Security Consultant
Kuwait Linux Company
Kuwait
Ph-2412552/2463633
<vineet [at] linux [dot] com [dot] kw>
www.linux.com.kw
```

```
-----
-----
-----
-----
```