

Can't route through Linux box

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux/2004-02/0674.html>

From: Fred Smyth (fred_at_mail.vcoms.net)

Date: 02/26/04

Date: Thu, 26 Feb 2004 05:46:43 -0600

I'm trying to setup a linux box (Kernel 2.4.18) to act as a server/router.

We have an SDSL connection with a few static IP's. With the following setup, I can ping the sdsl router 66.80.220.65 from the linux system. I Can ping any of the PC's (66.80.220.67,68,69,70) from the linux system. I can ping the linux system (66.80.220.66,71) from any of the PC's.

Problem is: I cannot ping the SDSL router(66.80.220.65) from any of the PC's.

Here is ifconfig

```
eth0 Link encap:Ethernet HWaddr 00:A0:CC:5E:F9:9D
      inet addr:66.80.220.71 Bcast:66.255.255.255 Mask:255.255.255.255
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:18 errors:0 dropped:0 overruns:0 frame:0
      TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:1458 (1.4 Kb) TX bytes:1040 (1.0 Kb)
      Interrupt:5 Base address:0xd000
```

```
eth1 Link encap:Ethernet HWaddr 00:30:48:23:B5:DF
      inet addr:66.80.220.66 Bcast:66.255.255.255 Mask:255.255.255.255
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:693 errors:0 dropped:0 overruns:0 frame:0
      TX packets:525 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:69481 (67.8 Kb) TX bytes:365582 (357.0 Kb)
      Interrupt:9 Base address:0x2000
```

```
lo Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:96 errors:0 dropped:0 overruns:0 frame:0
      TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:10525 (10.2 Kb) TX bytes:10525 (10.2 Kb)
```

comp.os.linux: Can't route through Linux box

Kernel IP routing table

```
Destination Gateway Genmask Flags Metric Ref Use Iface
66.80.220.65 0.0.0.0 255.255.255.255 UH 0 0 0 eth1
66.80.220.67 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
66.80.220.69 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
66.80.220.68 0.0.0.0 255.255.255.255 UH 0 0 0 eth0
66.80.220.70 0.0.0.0 255.255.255.255 UH 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 66.80.220.65 0.0.0.0 UG 1 0 0 eth1
```

I striped the firewall configuration down to this, to see if I had some issue here. But even with this it no go.

```
#!/bin/sh
INTERNALIF="eth0"
INTERNALNET="66.80.220.64/27"
DIALUPIF="ppp+"
INTERNALBCAST="66.80.220.95"
EXTERNALIF="eth1"

# Pathnames
DMESG="/bin/dmesg"
IPTABLES="/usr/sbin/iptables"
MODPROBE="/sbin/modprobe"

#####
#Insert modules– should be done automatically if needed
# dmesg -n 1 #Kill copyright display on module load
/sbin/modprobe ip_tables
/sbin/modprobe iptable_filter
/sbin/modprobe ip_contrack
/sbin/modprobe ip_contrack_ftp
/sbin/modprobe ip_contrack_irc

#
## Flush everything, start from scratch
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD
$IPTABLES -t nat -F

## Setting default filter policy
$IPTABLES -P INPUT ACCEPT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD ACCEPT
#
#

#Disabling IP Spoofing attacks.
echo 2 > /proc/sys/net/ipv4/conf/all/rp_filter
```

Can't route through Linux box

comp.os.linux: Can't route through Linux box

```
#Don't respond to broadcast pings
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

#Enable forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

#Block source routing
echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route

#Kill timestamps. These have been the subject of a recent bugtraq thread
echo 0 > /proc/sys/net/ipv4/tcp_timestamps

#Enable SYN Cookies
echo 1 > /proc/sys/net/ipv4/tcp_syncookies

#Kill redirects
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects

#Enable bad error message protection
echo 1 > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

#Log martians (packets with impossible addresses)
#RiVaL said that certain NICs don't like this. Comment out if necessary.
echo 1 > /proc/sys/net/ipv4/conf/all/log_martians

#Set out local port range
echo "32768 61000" > /proc/sys/net/ipv4/ip_local_port_range

#Reduce DoS'ing ability by reducing timeouts
# ccv..Don't know if this breaks something so out for now.
#echo 30 > /proc/sys/net/ipv4/tcp_fin_timeout
#echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_time
#echo 1 > /proc/sys/net/ipv4/tcp_window_scaling
#echo 0 > /proc/sys/net/ipv4/tcp_sack
#echo 1280 > /proc/sys/net/ipv4/tcp_max_syn_backlog

exit 0
```

Thanks in advance for your help. I know I'm over looking something obvious, but I just can't find it.

Fred