

## Re: tcpdump broken after rh9 2.4.20–27.9 kernel upgrade

**Source:** <http://linux.derkeiler.com/Mailing-Lists/RedHat/2003-12/1133.html>

---

**From:** Robert Brown ([eli\\_at\\_typhoon.xnet.com](mailto:eli_at_typhoon.xnet.com))

**Date:** 12/27/03

To: [redhat-list@redhat.com](mailto:redhat-list@redhat.com)

Date: Fri, 26 Dec 2003 19:12:48 -0600 (CST)

I just ran a quick check, and I see the same symptoms when running tcpdump from another box, so it is not box-specific. As I said before, it looks like promiscuous mode isn't working -- either that or my hubs just transmogrified (Calvin & Hobbes word) into switches, which I rather doubt.

All the NICs on the network are operating in forced 100baseT half-duplex mode and are connected thru a hub rather than a switch, so that the sniffers will see everything. Only the WILD NICs run in 10baseT half duplex mode, for compatibility with the bridge that connects me to the internet. The relevant lines in the /etc/modules.conf file on the NIDS box looks like this:

```
alias eth0 8139too
alias eth1 8139too
alias eth2 8139too
options 8139too 0x100,0x100,0x10
```

Strangely enough, even though I cannot see pings from box A to box B when sniffing on box C, I still see arps. This further causes me to suspect that something is wrong with promiscuous mode.

Robert Brown writes:

- > *I did the upgrade by downloading the rpm files to my server, and then*
- > *running the install from a script, as I have several systems that I*
- > *must maintain. I did not use up2date; I used essentially the*
- > *[scripted] manual process.*
- >
- > *While I have only tried tcpdump on one system, my NIDS, I have*
- > *observed that in every case, the old kernel images were purged.*
- >
- > *BTW My NIDS box has 3 ethernet NICs in it, and only one has an*
- > *assigned address, as the other 2 are used for packet sniffing to feed*
- > *the NIDS. The NIC with an address is also in promiscuous mode, and*
- > *sniffs the LAN behind the DMZ. The other 2 NICs sniff, thru a*

RedHat: Re: tcpdump broken after rh9 2.4.20-27.9 kernel upgrade

```
> read-only cable, the DMZ, and the WILD zones.
> -----
>
> Harry Hoffman writes:
> > Hmm,
> >
> > I updated via up2date and my tcpdump works fine. Also, my old kernel wasn't
> > removed automatically...
> > I'm not quite sure that this really helps but at the very least you know that
> > different things are being seen :-(
> >
> > Do you have other systems that this has happened to or is this the only one?
> >
> > HTH,
> > Harry
> >
> > Quoting Robert Brown <eli@typhoon.xnet.com>:
> >
> > *> Robert Brown writes:
> > *> > I use tcpdump as a component of an network monitoring tool and to feed
> > *> > the snort intrusion detection system. I have done so for several
> > *> > years. After upgrading from the 2.4.20-24.9 to the 2.4.20-27.9
> > *> > kernel, my tcpdump no longer functions properly. It is acting like
> > *> > perhaps the promiscuous mode is not taking effect, even though an
> > *> > ifconfig shows all the monitored interfaces to be in promiscuous
> > *> > mode.
> > *> >
> > *> > Has anybody else seen this? Is there a fix?
> > *>
> > *> Unfortunately, the 2.4.20-27.9 upgrade, unlike previous rh9 upgrades,
> > *> took it upon itself to automatically delete all earlier versions of
> > *> the kernel from the system, so I cannot simply edit
> > *> /boot/grub/grub.conf to default to the older kernel.
> > *>
> > *> I think somebody at Red Hat maybe had a little too much holiday happy
> > *> juice just before that release was tested... :-<
> > *>
> >
> >
> > --
> > Harry Hoffman
> > hhoffman@ip-solutions.net
> >
> >
#-----#
> > # Harry: version 4.0a #
> > # Known bugs: #
> > # 1) Verbal output may occur before data processing is complete. #
> > # 2) Loudspeaker option may activate without being invoked. #
> > # 3) Other bugs as reported #
> >
```

RedHat: Re: tcpdump broken after rh9 2.4.20-27.9 kernel upgrade

```
#-----#
>>
>> -----
>> This mail sent through IpSolutions: http://www.ip-solutions.net/
>>
>>
>> --
>> redhat-list mailing list
>> unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe
>> https://www.redhat.com/mailman/listinfo/redhat-list
>>
>
>
> --
> redhat-list mailing list
> unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe
> https://www.redhat.com/mailman/listinfo/redhat-list
>
--
redhat-list mailing list
unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe
https://www.redhat.com/mailman/listinfo/redhat-list
```