

problems with tcpdump filter on a switch mirroring port, 6.2 RELEASE-p4

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2007-04/msg02144.html>

- *From:* Philipp Gaschütz <philipp@xxxxxxxxxx>
 - *Date:* Sun, 29 Apr 2007 16:14:21 +0200
-

Hi,

we have a strange problem with tcpdump on a vanilla FreeBSD 6.2-RELEASE-p4 box, which we are trying to use as a traffic sniffing/IDS/whatever device.

The box has 2 NICs, em0 and em1

em0 is normally configured with an inet address.

em1 is connected to a port on the same switch (HP Procurve 2824), which is configured to be a mirror port of all other ports and configured like this:

```
ifconfig em1 polling monitor promisc
```

ie only a network sniffing device.

while issuing a "ping 81.91.161.70",

"tcpdump -nli *em0* host 81.91.161.70" works like expected (traffic is sent to the default gw via em0, switch copies the data to em1):

```
15:54:05.790877 IP XXX.XXX.XXX.XXX > 81.91.161.70: ICMP echo request, id 35620, seq 0, length 64
15:54:05.801690 IP 81.91.161.70 > XXX.XXX.XXX.XXX: ICMP echo reply, id 35620, seq 0, length 64
```

However, issuing the same ping, but tcpdump'ing on em1 only results in

```
# tcpdump -nli em1 host 81.91.161.70
```

```
15:56:00.512614 IP XXX.XXX.XXX.XXX > 81.91.161.70: ICMP echo request, id 40484, seq 0, length 64
15:56:01.548077 IP XXX.XXX.XXX.XXX > 81.91.161.70: ICMP echo request, id 40484, seq 1, length 64
```

ie. no replies are captured by tcpdump

Initially I thought this was somehow connected to the monitoring port on the switch not working as expected. However:

```
# tcpdump -nli em1 | grep 81.91.161.70
```

```
15:57:48.447530 IP XXX.XXX.XXX.XXX > 81.91.161.70: ICMP echo request, id 41508, seq 0, length 64
15:57:48.458767 IP 81.91.161.70 > XXX.XXX.XXX.XXX: ICMP echo reply, id 41508, seq 0, length 64
```

problems with tcpdump filter on a switch mirroring port, 6.2 RELEASE-p4

ie. tcpdump without a filter captures the packets just fine.

I have tried to disable monitor and polling and also gave em1 an inet address, without success.

The box itself idles at 99% when running tcpdump.

I have ammended the following sysctls (also without success):

net.bpf.bufsize: 4194304

net.bpf.maxbufsize: 8388608

Has anyone seen something like this before?

Thanks

Philipp

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"