

odd tcpdump output w/ 6.0-BETA2 ...

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2005-08/0185.html>

From: Matthew Grooms (*mgrooms_at_shrew.net*)

Date: 08/23/05

Date: Tue, 23 Aug 2005 12:01:52 -0500

To: freebsd-net@freebsd.org

Is anyone else seeing this issue? I get useless output from tcpdump (no header or protocol decode) but only when I specify a filter on the command line.

For example ...

```
root@hole# tcpdump -ne -i pflog0 src or dst www.21.com
tcpdump: WARNING: BIOCPROMISC: Network is down
tcpdump: WARNING: pflog0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on pflog0, link-type PFLOG (OpenBSD pflog file), capture size
96 bytes
11:33:05.172950 [[pflog]
11:33:05.222612 [[pflog]
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
```

... or ...

```
root@hole# tcpdump -i xl0 src or dst www.21.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on xl0, link-type EN10MB (Ethernet), capture size 96 bytes
11:33:32.920031 [[ether]
11:33:35.203998 [[ether]
11:33:35.375459 [[ether]
11:33:35.555475 [[ether]
11:33:35.728465 [[ether]
11:33:36.077081 [[ether]
^C
6 packets captured
67 packets received by filter
0 packets dropped by kernel
```

... but with no filter ...

freebsd-net: odd tcpdump output w/ 6.0-BETA2 ...

```
root@hole# tcpdump -i xl0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on xl0, link-type EN10MB (Ethernet), capture size 96 bytes
11:35:15.224237 IP 66-90-165-114.dyn.grandenetworks.net.ssh >
fw1.seton.org.62909: P 507679271:507679463(192) ack 1455983273 win 65535
11:35:15.342434 IP fw1.seton.org.62909 >
66-90-165-114.dyn.grandenetworks.net.ssh: . ack 192 win 63760
11:35:15.371456 arp who-has 24-155-229-142.dyn.grandenetworks.net tell
24-155-229-254.dyn.grandenetworks.net
11:35:15.374214 arp who-has 66-90-146-196.dyn.grandenetworks.net tell
66-90-147-254.dyn.grandenetworks.net
11:35:15.496867 arp who-has 24-155-108-156.dyn.grandenetworks.net tell
24-155-109-254.dyn.grandenetworks.net
11:35:15.509748 arp who-has 24-155-108-208.dyn.grandenetworks.net tell
24-155-109-254.dyn.grandenetworks.net
11:35:15.533528 arp who-has 66-90-245-22.dyn.grandenetworks.net tell
66-90-245-254.dyn.grandenetworks.net
^C11:35:15.554105 arp who-has 216-188-225-208.dyn.grandenetworks.net
tell 216-188-225-254.dyn.grandenetworks.net
```

```
8 packets captured
65 packets received by filter
0 packets dropped by kernel
```

... I did compile a custom kernel but haven't cvsup'ed any source since it was installed from the iso. Would like to cvsup and rebuild the kernel and userland but am restricted on disk space. Does anyone know what collections are considered minimal to sync and rebuild or do I really need to cvsup src-all?

Thanks,

-Matthew

freebsd-net@freebsd.org mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-net>
To unsubscribe, send any mail to "freebsd-net-unsubscribe@freebsd.org"