175 Cabot Street – Suite 210
Lowell, MA 01854 USA
www.cspi.com
NASDAQ: CSPI

How do I run Linux tcpdump with the Sniffer10G software?

Model:

ARC Series B & C Network Adapters (10G-PCIE2-8B2-2S & 10G-PCIE2-8C2-2S)

Software:

Sniffer10G

Operating System:

Supports the Linux operating system.

Information:

Instructions for using Linux tcpdump with Sniffer10G v2/v3 (if you are using Ubuntu 14.04 and Sniffer10G v2, refers to Note 5 below).

1. Verify that your tcpdump has a dynamically linked libpcap:

```
%ldd `which tcpdump` | grep pcap
```

   If your tcpdump statically links libpcap, then you'll see no output. Otherwise, you'll see something like:

```
libpcap.so.0.9.4 => /usr/lib64/libpcap.so.0.9.4
(0x00000034c1400000)
```

   If you saw no output above, continue onwards to step 2. If you saw the output above, skip to step 3 (running tcpdump with LD_LIBRARY_PATH set).

2. Building a new tcpdump:

   Make sure you have libpcap-devel installed.

```
% %sudo yum install libpcap-devel
```

   Download and build tcpdump:

```
% wget http://www.tcpdump.org/release/tcpdump-4.1.1.tar.gz
%tar zxf tcpdump-4.1.1.tar.gz
%cd tcpdump-4.1.1/
% ./configure
% make
```

3. Running tcpdump with LD_LIBRARY_PATH set:

   Determine what libpcap version your tcpdump expects:

```
%ldd tcpdump | grep pcap
libpcap.so.0.9.4 => /usr/lib64/libpcap.so.0.9.4
(0x00000034c1400000)
```

   Make a symlink to that version in **/opt/snf/lib.** Assuming your version is 0.9.4:

```
%sudo ln -s /opt/snf/lib/libpcap.so
/opt/snf/lib/libpcap.so.0.9.4
```

   Set LD_LIBRARY_PATH to prefer the Sniffer10G-compatible libpcap:

   csh/tcsh:

```
% setenv LD_LIBRARY_PATH /opt/snf/lib
```

   bash:

```
$ export LD_LIBRARY_PATH=/opt/snf/lib
```

4. Set SNF_DEBUG_MASK=3 to know if incoming packets are going through Sniffer10G.

csh/tcsh:

```
% setenv SNF_DEBUG_MASK 3
```

bash:

```
$ export SNF_DEBUG_MASK=3
```

5. Run tcpdump on the snf0 interface:

```
% tcpdump -ni snf0

tcpdump: verbose output suppressed, use -v or -vv for full
protocol decode
listening on snf0, link-type EN10MB (Ethernet), capture size 65535 bytes
09:13:10.065406 IP 192.168.1.32 > 192.168.1.250: ICMP echo request, id
21865, seq 7, length 64
09:13:11.065142 IP 192.168.1.32 > 192.168.1.250: ICMP echo request, id
21865, seq 8, length 64
09:13:12.065889 IP 192.168.1.32 > 192.168.1.250: ICMP echo request, id
21865, seq 9, length 64
09:13:13.065632 IP 192.168.1.32 > 192.168.1.250: ICMP echo
request, id
21865, seq 10, length 64
09:13:14.065374 IP 192.168.1.32 > 192.168.1.250: ICMP echo request, id
21865, seq 11, length 64

5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

Caveat: Please be aware that while Sniffer10G can support up to 14.8 Mpps, tcpdump will print output to standard out, which will severely limit achievable packet rates.

Notes:

1. If there are problems opening the snf0 device, verify that ldd is showing **/opt/snf/libpcap** and **/opt/snif/libsnf**.

```
%ldd ./tcpdump
libpcap.so.0.9.4 => /opt/snf/lib/libpcap.so.0.9.4
(0x00002b058049a000)
libc.so.6 => /lib64/libc.so.6 (0x00000034c1000000)
libsnf.so.0 => /opt/snf/lib/libsnf.so.0 (0x00002b05806de000)
/lib64/ld-linux-x86-64.so.2 (0x00000034c0c00000)
libpthread.so.0 => /lib64/libpthread.so.0
(0x00000034c1c00000)                                    librt.so.1 =>
/lib64/librt.so.1 (0x00000034c2400000)
```

2. Using the SNF interface for sniffing causes all traffic to be diverted from the normal Ethernet interface to the sniffing application. This will cause hosts to fail to respond on their 10G interfaces when packet sniffing is in progress.
3. Using snf0 versus eth0 when referencing the same MAC address with tcpdump. This issue is libpcap related. If you link to our distributed pcap, eth0 and snf0 will go through Sniffer10G. If you build your own and include Sniffer10G support, eth0 will go through the kernel and snf0 will go through Sniffer10G. Generally, we recommend the use of snfX simply because that always works with whatever pcap or when it does not, it indicates that you are not using the correct one. Refer to the Sniffer10G user guide documentation for verifying with the parameter SNF_DEBUG_MASK=0x3 flag that everything looks fine when opening the device.

4. The FreeBSD 10 port of the Sniffer10G v3 software currently does not support the FreeBSD-specific version of tcpdump included in **/usr/sbin/tcpdump**. As a temporary workaround, please instead use the unmodified tcpdump included in **/usr/ports/net/tcpdump** or obtain the tcpdump source code directly from: http://www.tcpdump.org/release/tcpdump-4.4.0.tar.gz.
5. Ubuntu 14.04 uses tcpdump-4.5.1 which includes libpcap-1.5.3. Sniffer10G v2 is not compatible with libpcap-1.5.3. Contact CSPI Technical Support (support@cspi.com) for the patch for libpcap-1.5.3 support. However, Sniffer10G v3 does include support for libpcap-1.5.3 and libpcap-1.6.2.

Revision	Date	Change
1	6/27/2016	Initial Draft
2	7/22/2016	Feedback