tcpdump

Jan 2017 (Updated MApr 2017)

---

tcpdump is a tool to capture IP Packets at a command line level, its similar to the PCAP used by Wireshark (Wireshark is just a GUI to control PCAP). I say just a GUI, its rather good and saying it is 'just' a GUI is a little harsh.

Originally, I was using tcpdump to capture IP traffic and write it to a file, and if this is what you wish to do, then go to the section on this page called File Capture. However if you just wish to view the tcpdump output on screen, then look at the section entitled Screen Capture.

Screen Caputre

To show the output of tcpdump on the screen, use the follwoing syntax.

```
tcpdump -i eth2 -nn
```

The -i eth2 specifies the interface you wish to monitor. the -nn tells tcpdump not to resolve port numbers to names (so won't display the word 'ftp' where it sees port 21 for example).

This results in the following style output.
<sxh [text][; options for SyntaxHighlighter]> 05:58:06.235597 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.235646 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.236112 IP 10.0.20.1.10000 > 239.0.200.1.10002: UDP, length 1316 05:58:06.236238 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.236422 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.236521 IP 10.0.20.100.1234 > 239.0.100.1.1234: UDP, length 1316 05:58:06.236595 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.236818 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.237060 IP 10.0.20.1.10000 > 239.0.200.1.10001: UDP, length 1316 05:58:06.237211 IP 10.0.20.1.10000 > 239.0.200.1.10003: UDP, length 1316 05:58:06.237402 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.237425 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.237524 IP 10.0.20.100.1234 > 239.0.100.1.1234: UDP, length 1316 05:58:06.237598 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.237985 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.238063 IP 10.0.20.1.10000 > 239.0.200.1.10001: UDP, length 1316 05:58:06.238213 IP 10.0.20.1.10000 > 239.0.200.1.10002: UDP, length 1316 05:58:06.238425 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.238572 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.238599 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.239174 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.239423 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.239521 IP 10.0.20.100.1234 > 239.0.100.1.1234: UDP, length 1316 05:58:06.239597 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.239741 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.240065 IP 10.0.20.1.10000 > 239.0.200.1.10001: UDP, length 1316 05:58:06.240215 IP 10.0.20.1.10000 > 239.0.200.1.10002: UDP, length 1316 05:58:06.240325 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.240423 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.240521 IP 10.0.20.100.1234 > 239.0.100.1.1234: UDP, length 1316 05:58:06.240597 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.240916 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.241166 IP 10.0.20.1.10000 > 239.0.200.1.10003: UDP, length 1316 05:58:06.241304 IP 10.0.20.1.10000 > 239.0.200.1.10004: UDP, length 1316 05:58:06.241423 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328 05:58:06.241507 IP 10.0.85.1.60817 > 239.0.85.1.1234: UDP, length 1316 05:58:06.241596 IP 10.0.20.1.1234 > 239.1.2.3.1234: UDP, length 1328

18909 packets captured 18913 packets received by filter 0 packets dropped by kernel </sxh>

File Capture

On Linux, we can use tcpdump to capture either the IP Input or the IP Output. There are many commands available for tcpdump, and I will list some later on this page, but first lets just look at a working example, because this might be all you need for now.

To capture an IP Output (ensure you have started your service) use the following example. The following example is for eth2, where a multicast exists on 239.0.12.1 port 1234.

```
The format for tcpdump is - tcpdump -i <interface> -s 65535 -w <some-file>
tcpdump -i eth2 -B 64000 dst host 239.0.12.1 and port 1234 and multicast -w /home/ts_capture_test.pcap
if the syntax is correct, the tcpdump will start:
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
```

running the previous command will start the capture, and it will capture until stopped (using CTRL-C)

Pressing CTRL-C stops the output, and you will see something like the following:

```
119658 packets captured
119663 packets received by filter
0 packets dropped by kernel
```

The capture is a pcap file, the same format that would have been captured if you were using Wireshark, to get the video from this you will have to extract it first.