

Re: question concerning tcpdump

Re: question concerning tcpdump

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2007-05/msg00503.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Thu, 10 May 2007 14:40:22 -0500
-

On 10 May 2007, in the Usenet newsgroup comp.os.linux.misc, in article <1178788197.193157.170090@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, Bernd wrote:

I ran tcpdump for about 10 hours and wrote all traffic from this host to a file, using:
tcpdump -n -vv -w ~/tcpdump.txt -C 10 ip src host adress

OK

I have one line which i don't understand and i'm wondering about:

```
19:35:30.510098 IP xxxxxxxx.32786 > xxxxxxxx.smpdpd: S
555971953:555971953(0) win 5840 <mss
1460,sackOK,timestamp 15510435 0,nop,wscale 2>
```

Hello SuSE – "smpdpd" is SuSE Meta PPPD – one of their "improvements"

I deleted our ip's, hope that's o.k. for you.

Depends on what you are looking for

Can i find out if this packet used tcp or udp ?

man tcpdump, and look waaayyy down for "OUTPUT FORMAT"

Is the "win 5840" a sign for tcp ?

Yes, as is the "S" (SYN) flag. UDP doesn't use either one.

Re: question concerning tcpdump

Re: question concerning tcpdump

I don't know much about protocols, i just red a time ago that tcp uses "windows" for connection control.

0768 User Datagram Protocol. J. Postel. August 1980. (Format: TXT=5896 bytes) (Also STD0006) (Status: STANDARD)

0791 Internet Protocol. J. Postel. September 1981. (Format: TXT=97779 bytes) (Obsoletes RFC0760) (Updated by RFC1349) (Also STD0005) (Status: STANDARD)

0792 Internet Control Message Protocol. J. Postel. September 1981. (Format: TXT=30404 bytes) (Obsoletes RFC0777) (Updated by RFC0950) (Also STD0005) (Status: STANDARD)

0793 Transmission Control Protocol. J. Postel. September 1981. (Format: TXT=172710 bytes) (Updated by RFC3168) (Also STD0007) (Status: STANDARD)

Not really that big, but good for a quick answer.

The first "xed" ip is our host (the source), the second one (destination) is the router in our network.

/etc/services says: smpppd 3185/tcp # SuSE Meta PPPD
for smpppd. The machine we are talking about is a SuSE 9.2 box.
PPP is something with point-to-point protocol ?

Yes – SuSE Meta PPPD is something to do with "kinternet", and is required by SuSE for some reason for modem, ISDN, and DSL connections.

We don't have a modem or isdn-card on this box.

You can `_try_` using 'sbin/chkconfig' (see the man page) to prevent the service from starting.

What's the problem, or is this a continuation of the strange IPs question?

Old guy

.