

Fun with tcpdump

Bill Totman

NYCBUG
August 3rd, 2011

tcpdump History

Written in 1987 by Van Jacobson, Craig Leres, and Steven McCanne.

Ubiquitous across Unix and Unix-like Oses.

BSD Licensed.

Wireshark can handle its output.

Common Syntax

```
tcpdump [options] [expression]
```

```
tcpdump -i int host name
```

int is the name *ifconfig* outputs for you and *host* can be followed by a resolvable *name* or *IP address*.

```
tcpdump -i int port 80 and host IP
```

More Common Syntax

```
tcpdump -i int -w file.cap port 80 and host01
```

```
tcpdump -r file.cap
```

```
tcpdump -i int protocol and host01
```

```
tcpdump -i em0 icmp and host 192.168.10.3
```

Uncommon Syntax

```
tcpdump -i em1 -w testing.cap port 80 \  
    and \( dst 192.168.10.3 and src 192.168.10.2 \)
```

The parenthesis server to separate logical associations and must be escaped.

```
tcpdump -i em1 port 22 and not host 192.168.10.2
```

If you SSH from 192.168.10.2 that SSH traffic can clutter your capture: exclude it.

Logic Syntax

tcpdump can handle the following logic operators on tcpdump's "primitives":

Negation (`!` or `not`)

Concatenation (`&&` or `and`)

Alternation (`|` or `or`)

Differences in Syntax?

```
tcpdump -i em1 icmp and host 192.168.10.3
```

```
22:31:37.108064 IP 192.168.10.2 > pfsense-vm02.local: \
```

```
    ICMP echo request, id 26946, seq 391, length 64
```

```
22:31:37.108151 IP pfsense-vm02.local > 192.168.10.2: \
```

```
    ICMP echo reply, id 26946, seq 391, length 64
```

Differences in Syntax?

```
tcpdump -vi em1 icmp and host 192.168.10.3
```

```
22:33:27.199580 IP \
```

```
(tos 0x0, ttl 64, id 30258, offset 0, \  
flags [none], proto ICMP (1), length 84) \
```

```
192.168.10.2 > pfsense-vm02.local: \
```

```
ICMP echo request, id 26946, seq 500, length 64
```

```
22:33:27.199640 IP \
```

```
(tos 0x0, ttl 64, id 26198, offset 0, \  
flags [none], proto ICMP (1), length 84) \
```

```
pfsense-vm02.local > 192.168.10.2: \
```

```
ICMP echo reply, id 26946, seq 500, length 64
```

Differences in Syntax?

```
tcpdump -vvi em1 icmp and host 192.168.10.3
```

```
22:45:54.630259 IP \
```

```
(tos 0x0, ttl 64, id 47647, offset 0, \  
flags [none], proto ICMP (1), length 84) \
```

```
192.168.10.2 > pfsense-vm02.local: \
```

```
ICMP echo request, id 26946, seq 1240, length 64
```

```
22:45:54.630345 IP \
```

```
(tos 0x0, ttl 64, id 36459, offset 0, \  
flags [none], proto ICMP (1), length 84) \
```

```
pfsense-vm02.local > 192.168.10.2: \
```

```
ICMP echo reply, id 26946, seq 1240, length 64
```

Troubleshooting Shortcuts

If you wanted to confirm whether a firewall was NATting a particular host:

```
DST=4.2.2.2
```

```
SRC=192.168.3.3
```

```
tcpdump -i em0 $DST and not $SRC
```

Troubleshooting Shortcuts

When it can really make a difference:

```
HOST1=4.2.2.2
```

```
HOST2=192.168.3.3
```

```
HOST3=207.33.44.9
```

```
tcpdump -i em0 \(\(src $HOST1 and dst $HOST2\) \
    or \(src $HOST1 and dst $HOST3\) \
    or \(host $HOST2 and host $HOST3\) \)
```

References

- <http://tcpdump.org>
- Tcpdump. (2011, July 28). In Wikipedia, The Free Encyclopedia. Retrieved 20:45, August 3, 2011, from <http://en.wikipedia.org/w/index.php?title=Tcpdump&oldid=441838709>
- <http://www.freebsd.org/cgi/man.cgi>
- <http://billtotman.com>

Bonus

- `cd /tmp`
- `mkdir test`
- `cd test`
- `ls > content.txt`
- `cat content.txt`

What is the output of the `cat` command?