tcpdump cheat sheet

Packet structure

The TCP flags are in `tcp[13]`: ACK = 0×10, RST = 0×04, SYN = 0×02, FIN = 0×01.

The ICMP type is in `icmp[0]`. Useful types are 0 (echo response), 3 (destination unreachable), 8 (echo request) and 11 (time exceeded).

Since tcpdump does not fully decode IPv6, we must do it ourselves. The transport layer protocol number is in the `ip6[6]` ("next header") field: ICMP = 0×01, TCP = 0×06, UDP = 0×11. The IPv6 header is 40 bytes, assuming no extension headers, so `tcp[13]` maps to `ip6[53]` and `icmp[0]` maps to `ip6[40]`.

Recipes

Rejected traffic

Capture RST and ICMP Destination Unreachable packets, useful when debugging a firewall to see what it rejects:

```
((tcp[13] & 4 == 4) || (ip6[6] == 6 && ip6[53] & 4 == 4) || (icmp[0] == 3) || (icmp6 && ip6[40] == 1))
```

Successful TCP handshakes

Capture SYN+ACK packets to monitor successful TCP handshakes:

```
((tcp[13] & 0x12 == 0x12) || (ip6[6] == 6 && ip6[53] & 0x12 == 0x12))
```

TCP termination

Capture FIN+ACK packets to monitor TCP session terminations:

```
((tcp[13] & 0x11 == 0x11) || (ip6[6] == 6 && ip6[53] & 0x11 == 0x11))
```

Note: it is technically possible for only one end to send FIN (without ACK) and for the other to keep transmitting, or for either end to send FIN and ACK separately. In practice, a TCP connection nearly always ends with FIN, FIN+ACK, ACK.

IPv6 neighbor and router discovery

Capture ICMP6 neighbor solicitation / advertisement packets (135, 136) and ICMP6 router solicitation / advertisement / redirect packets (133, 134, 137):

```
(icmp6 && (ip6[40] >= 133 && ip6[40] <= 137))
```


Leave a Reply Cancel reply

Your email address will not be published. Required fields are marked

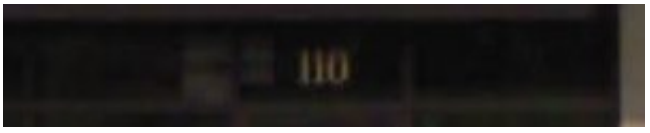
Name

Email

Website

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`



1. javascript:void(0)
2. http://www.google.com/intl/en/policies/