

tcpdump

One-Liners: tcpdump

Helpful tcpdump commands.

Add -v to -vvvv to see from some to a lot of information.

General networking

Get CDP or LLDP information.

```
tcpdump -i enp132s0f0 -v -s 1500 -c 1 '(ether[12:2]=0x88cc or ether[20:2]=0x2000)'
```

Watch DHCP traffic

```
tcpdump -i enp1s0f0 port 67 or port 68 -e -n -vv
```

Show VLAN tags

```
tcpdump -i enp1s0f0 -e vlan -nn
```

Watch for 1 host

```
tcpdump -vvvv -n dst host 10.200.200.13 or src host 10.200.200.13
```

Revision #1

Created 20 January 2023 00:13:18 by Michael Cleary

Updated 20 January 2023 00:19:31 by Michael Cleary