

tcpdump

Dealing with Ethernet headers and VLANs

```
# include ethernet header
tcpdump -n -e

# show only non-vlan traffic
tcpdump -n -e not vlan

# show only vlan traffic
tcpdump -n -e vlan

# show only vlan 1000 traffic
tcpdump -n -e '(vlan and (ether[14:2] & 0xfff == 1000))'

# show only vlan 1000 and 1001 traffic - needs testing
tcpdump -n -e '(vlan and (ether[14:2] & 0xfff == 1000 or ether[14:2] & 0xfff == 1001))'
```

#end

Revision #2

Created 21 May 2024 20:05:04 by bluecrow76

Updated 21 May 2024 20:50:42 by bluecrow76