

tcpdump more

Feb 2021

Here are some more great uses for tcpdump.

```
tcpdump -i eth0 -nn -Q in
```

Shows only the 'input' traffic on the specified interface

Can also use `-Q out` for just outgoing traffic

```
tcpdump -i eth0-nn igmp
```

Shows only IGMP traffic on the specified interface

Can be combined with `-Q in/out`

```
tcpdump -i eth0 -nn igmp -Q in
```

```
tcpdump -i eth0 -nn -w capfile.pcap
```

A simple tcpdump capture. `-w` is write.

Can be combined with `-Q in/out`

```
tcpdump -i eth0 -nn -Q out -w capfile.pcap
```

This captures only the output traffic on the interface eth0

```
tcpdump -i eth0 -nn port 5555
```

Shows only traffic using port 5555.

Can be combined with `-Q in/out`

```
tcpdump -i ens192 -nn -Q in port 5555
```

Shows only traffic on port 5555 coming in to eth0

From:

<http://cameraangle.co.uk/> - WalkerWiki - wiki.alanwalker.uk

Permanent link:

http://cameraangle.co.uk/doku.php?id=tcpdump_more&rev=1619098132

Last update: 2023/03/09 22:35

