tcpdump Packet capture

Interface -i, -Q → filter → **BPF filter** expression → -s, -c → **Capture** kernel buffer → -w / print → **Output** terminal or pcap

CONCEPTS

Options go first, then the filter. Quote the filter so the shell leaves parentheses alone.

The filter runs in the kernel, so a precise filter drops unwanted packets early and loses fewer of the ones you want.

CAPTURE

`tcpdump -D`
List capture interfaces

`tcpdump -i <iface>`
Capture on one interface

`tcpdump -i any`
Capture on all interfaces

`tcpdump -c <n>`
Stop after n packets

`tcpdump -s 0`
Capture full packets

`tcpdump -s <bytes>`
Limit bytes kept per packet

`tcpdump -Q in`
Only inbound packets (in, out, inout)

`tcpdump -p`
No promiscuous mode

`tcpdump -B <kib>`
Raise the capture buffer

OUTPUT

`tcpdump -n`
No host name lookups

`tcpdump -nn`
No host or port name lookups

`tcpdump -v`
More protocol detail (-vv, -vvv more)

`tcpdump -q`
Short, quiet lines

`tcpdump -A`
Payload as ASCII

`tcpdump -X`
Payload as hex and ASCII

`tcpdump -e`
Show link-level (MAC) header

`tcpdump -tttt`
Readable date and time

`tcpdump -l`
Line-buffer stdout for pipes

SAVE AND READ

`tcpdump -w <file>.pcap`
Write raw packets to a file

`tcpdump -r <file>.pcap`
Read a saved capture

`tcpdump -w <file>.pcap --print`
Save and also print

SAVE AND READ (cont.)

`tcpdump -U -w <file>.pcap`
Flush each packet to the file

`tcpdump -C <size> -w <file>`
Rotate by size (millions of bytes)

`tcpdump -W <n>`
Keep at most n files (ring buffer)

`tcpdump -G <sec> -w <file>-%FT%T.pcap`
Rotate by time

`tcpdump -Z <user>`
Drop root after opening device

FILTERS: HOSTS AND PORTS

`host <ip>`
Traffic to or from a host

`src host <ip>`
Only from this host

`dst host <ip>`
Only to this host

`net <cidr>`
A whole network, e.g. 10.0.0.0/8

`port <n>`
Source or destination port

FILTERS: HOSTS AND PORTS (cont.)

`src port <n>`
Source port only

`dst port <n>`
Destination port only

`portrange <a>-<b>`
A range of ports

`ether host <mac>`
A MAC address

FILTERS: PROTOCOLS AND LOGIC

`tcp`
TCP only (also udp, icmp)

`icmp`
ICMP, e.g. ping

`udp`
UDP only

`arp`
ARP requests and replies

`ip6`
IPv6 only

`A and B`
Both must match

`A or B`
Either matches

`not A`
Negate (also !)

FILTERS: PROTOCOLS AND LOGIC (cont.)

`'(A or B) and C'`
Group with quoted parentheses

TCP DETAILS

`'tcp[tcpflags] & tcp-syn != 0'`
Packets with SYN set

`'tcp[tcpflags] & tcp-rst != 0'`
Resets

Reading a line

Flags	Meaning
`[S]`	SYN, connection start
`[S.]`	SYN-ACK
`[.]`	ACK only
`[P.]`	data pushed
`[F.]`	FIN, closing
`[R]`	RST, refused or reset

RECIPES

Watch DNS

```
sudo tcpdump -i any -nn port 53
```

HTTP requests as text

```
sudo tcpdump -i <iface> -nn -A -s 0 'tcp dst port 80'
```

Capture to a ring of files

```
sudo tcpdump -i <iface> -nn -w cap -C 100 -W 10 -Z $USER
# keeps ten files of about 100 MB each
```