tcpdump Packet capture

CONCEPTS

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

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

OUTPUT

`tcpdump -n`
No host name lookups

`tcpdump -nn`
No host or port name lookups

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

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

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

`dst port <n>`
Destination port only

FILTERS: PROTOCOLS AND LOGIC

`tcp`
TCP only (also udp, icmp)

`icmp`
ICMP, e.g. ping

`udp`
UDP only

`A and B`
Both must match

`A or B`
Either matches

`not A`
Negate (also !)

`'(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