

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

01 / Quick reference and concepts

Capture a bounded, targeted conversation and read a saved trace without unnecessary name lookups. tcpdump/libpcap on an authorized Unix-like host. Interface names, privileges, link-layer types and available options vary.



Confirm interface and filter before capture. Packet count is not a wall-clock timeout; stop the capture at the end of the approved test window.

Option / filter	Purpose	Watch for
-D	List capture interfaces	Names vary by host
-nn	Keep numeric addresses and ports	Avoid lookup side effects
-i eth0	Choose interface	Example name; replace it
-c 200	Stop after 200 matched packets	Can wait indefinitely on quiet flow
-s 128	Limit bytes kept per packet	May truncate useful headers
-w flow.pcap	Write raw capture	May include sensitive content
-r flow.pcap	Read saved capture	No new network capture
host / port / net	libpcap acquisition filter	Different from Wireshark syntax

What to understand first

- A capture filter runs during acquisition or reading; it can exclude packets permanently from the saved capture. Use parentheses and quote the expression to avoid shell interpretation.
- Choose a snap length sufficient for the question. Header-limited capture reduces exposure but can lose encapsulated headers; -s 0 keeps full packets and may collect payloads.
- Packet-count bounds do not stop a quiet capture on elapsed time. Plan an explicit operator stop or use an approved OS timeout mechanism with compatible syntax.
- Capture-drop counters describe the collection path, not necessarily loss on the network. VLAN tags, tunnels and offload can change what a capture point sees.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

Interface and filter preparation

Read-only listing / compile check

```
tcpdump -D  
tcpdump -i eth0 -d 'host 192.0.2.10 and tcp port 443'
```

Inspect: Listing and compiled-filter inspection do not save a trace. Confirm the chosen interface and intended match.

Targeted capture

Starts capture and writes a file

```
tcpdump -i eth0 -nn -s 128 -c 200 -w flow.pcap 'host 192.0.2.10 and tcp port 443'
```

Inspect: Use only authorized scope and required privileges. Stop when the test window ends; 128 bytes may be insufficient for encapsulated traffic.

Saved-file review

Reads existing file

```
tcpdump -nn -r flow.pcap 'tcp port 443'
```

Inspect: Read the saved flow numerically. Existing payload content remains in the file regardless of this display.

Capture filters versus display filters

Illustrative teaching example, not captured device output.

```
libpcap: host 192.0.2.10 and tcp port 443  
Wireshark: ip.addr == 192.0.2.10 && tcp.port == 443
```

- The two expressions target a similar IPv4 conversation but belong to different filter languages.
- Check matching packets against the capture link type; nested encapsulation can require additional filter treatment.

PACKET ANALYSIS | REV 2.0 | REVIEWED 2026-10-10

tcpdump & capture-filter quick reference

03 / Troubleshooting and acceptance

1. State the observation point, authorized endpoints, transport and time window.
2. Select the real interface and validate the filter syntax before collection.
3. Start the bounded capture, reproduce one attempt and stop deliberately.
4. Review both directions and collection-drop counters before inferring network loss.
5. Protect the trace and retain only the evidence needed for the troubleshooting question.

Common mistakes

- Using an unbounded full-payload capture as the default.
- Assuming -c provides a time limit or -nn hides captured data.
- Missing the flow because the chosen interface sees a translated or encapsulated tuple.

Acceptance checks

- Capture scope and duration match the approved test.
- Relevant headers and both directions are available.
- Trace storage and the escalation handoff preserve confidentiality.

Primary references

[tcpdump project manual source](#)

[libpcap filter manual source](#)

[Wireshark display-filter expressions](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

[Deployment and migration help](#) | [Network security review from Wolex](#)