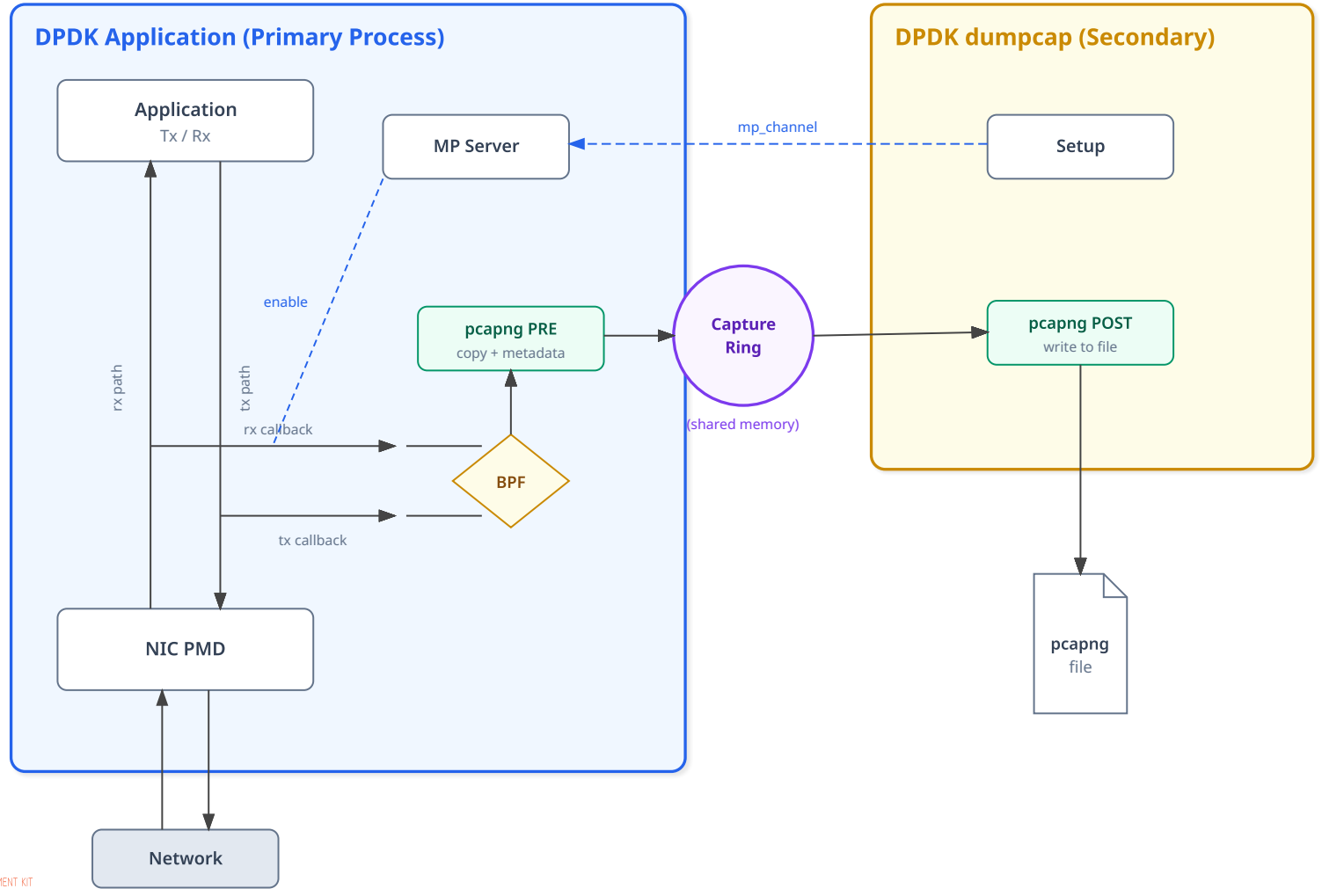
Packet Capture Challenges

“Why can’t I just use tcpdump”

Stephen Hemminger
<stephen@networkplumber.org>

DPDK Summit, Stockholm Sweden

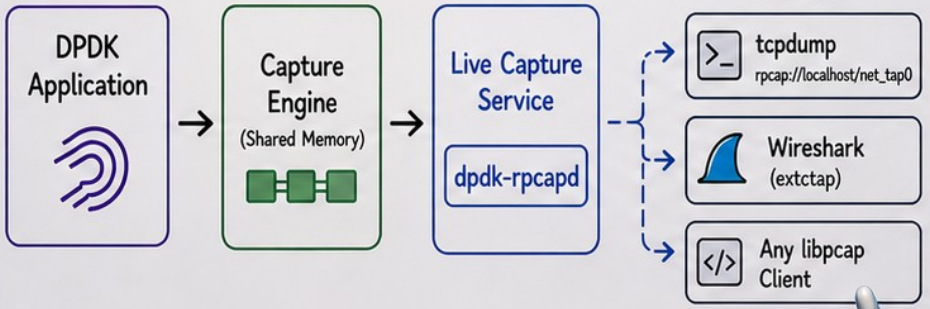
Current : dpdk-dumpcap



Packet Capture Ideas for DPDK

How do we get live packet capture out of DPDK easily?

OUR GOAL: LIVE CAPTURE THAT JUST WORKS



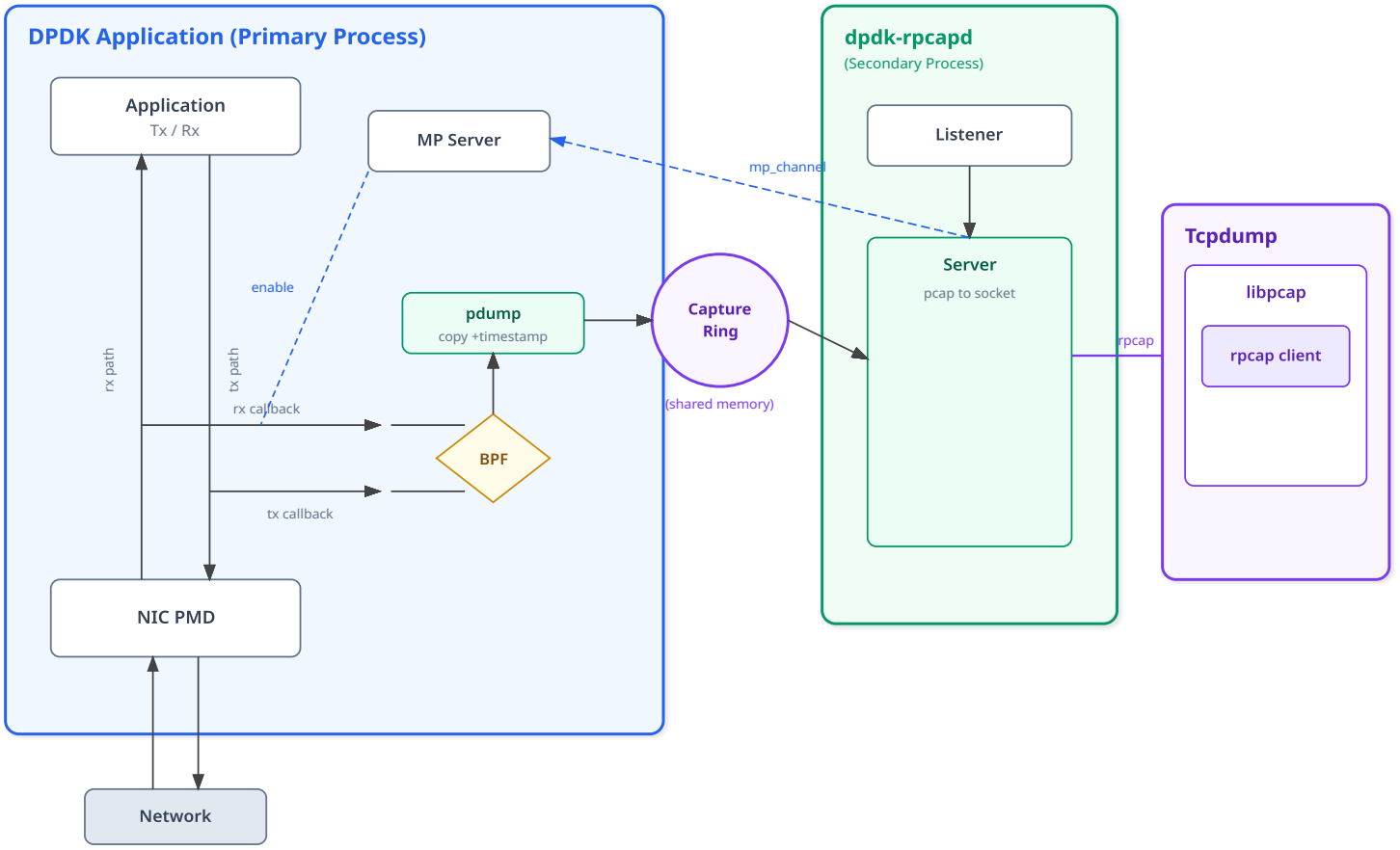
- Zero changes to your app
- High performance low overhead
- Works with tools you already use

Let's make it live, simple, and familiar!

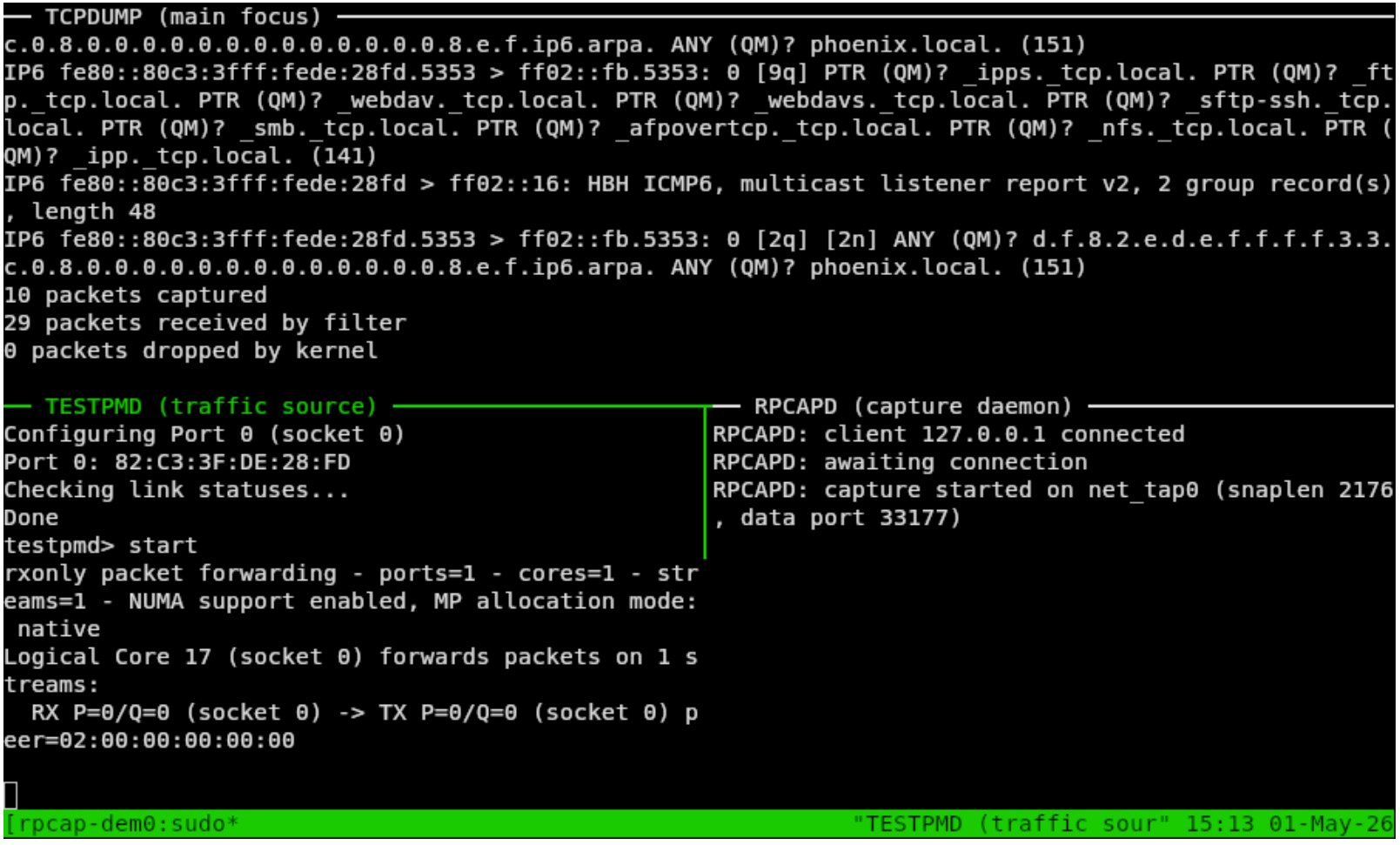
OTHER ATTEMPTS THAT DON'T FIT:

dpdkcap	Not maintained
DPDK2disk	Writes to disk
FlowScope	Not live capture
PcapPlusPlus	Library, not tool
Suricata	Heavy, not ideal
Snort 3 DAQ	No live pcap
VPP pcap trace	Different stack
TRex	Generator, not capture
n2disk	Writes to disk
Napatech	Vendor specific

Proposed: dpdk-rpcapd



Tcpdump (live demo)



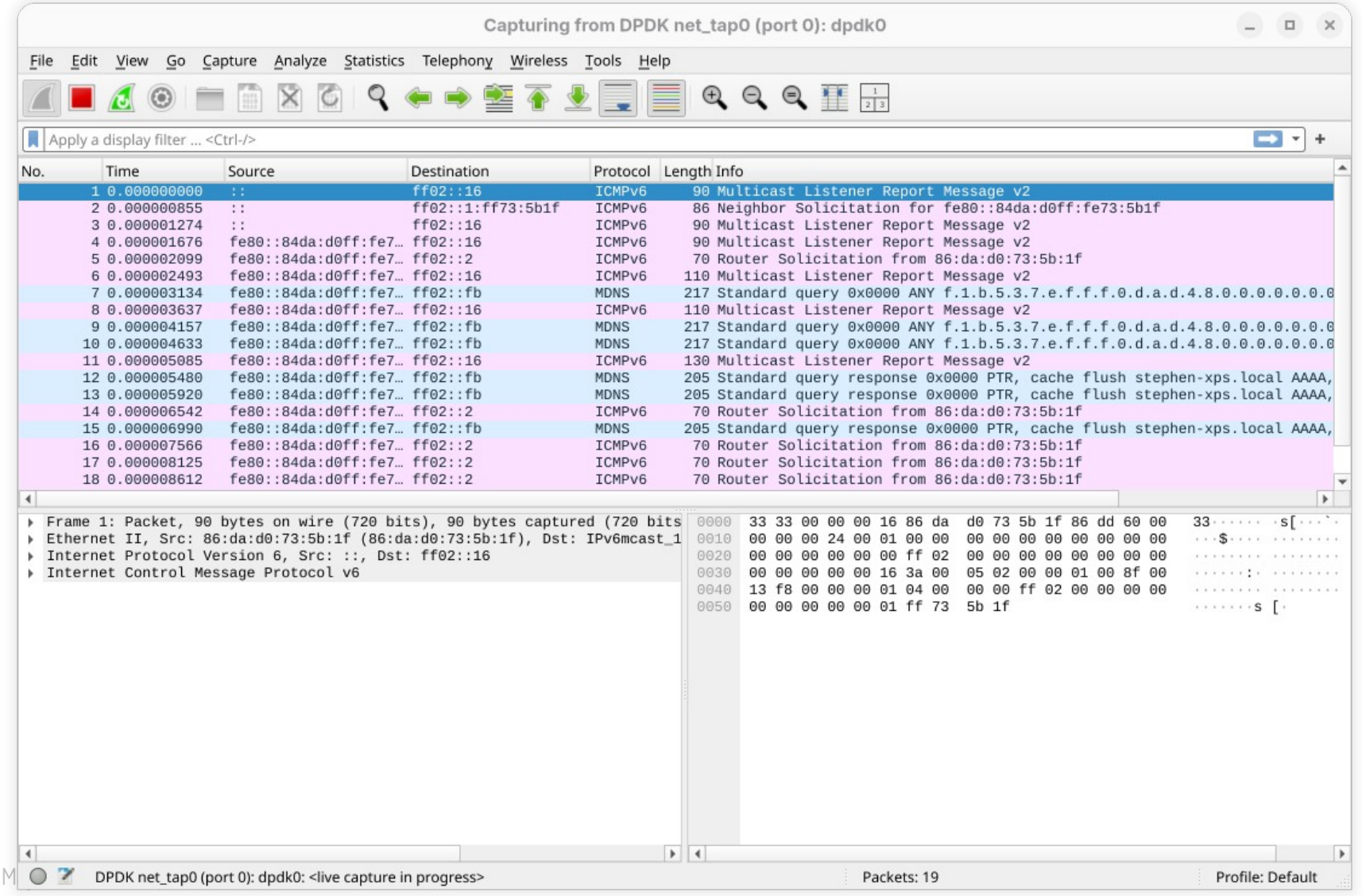
Key points

- Uses existing libpcap remote API
- New DPDK application dpdk-rpcapd
- Reuses existing DPDK pdump library
- Coexists with previous DPDK dumpcap/pdump

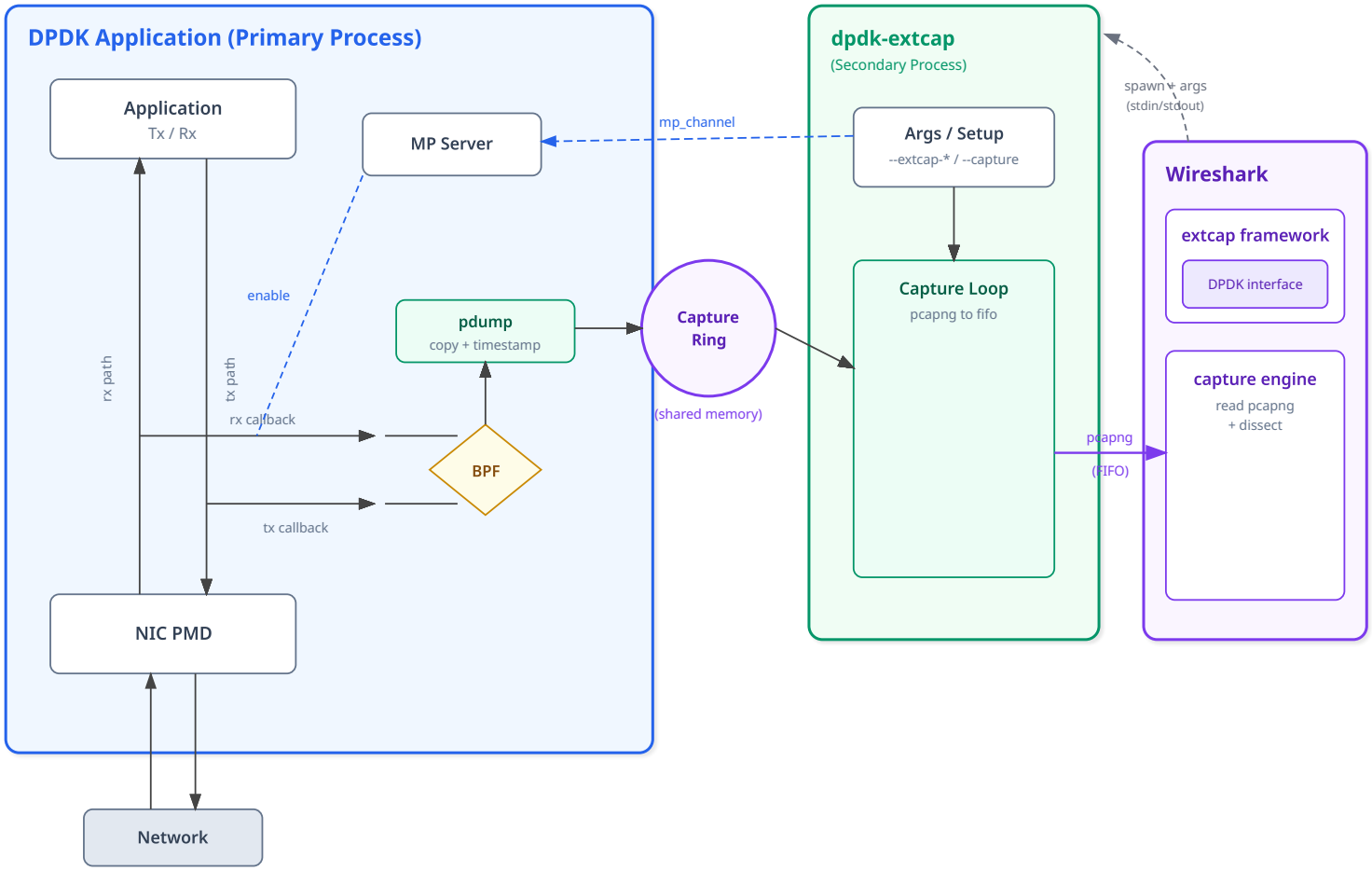
One more thing…

Can I use Wireshark instead?

Wireshark demo



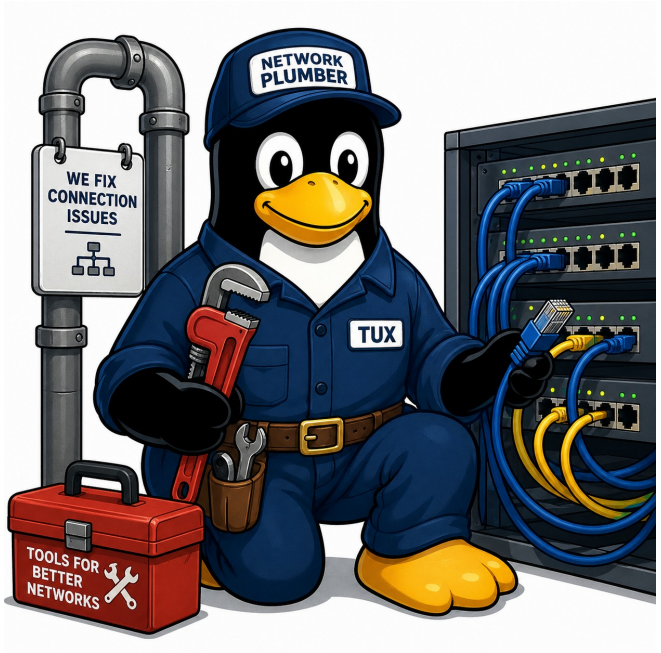
Alternative: dpdk-extcap



Capture Tools — Feature Comparison

Feature	dpdk-pdump	dpdk-dumpcap	dpdk-rpcapd	dpdk-extcap
File format	pcap	pcapng	pcap	pcapng
Timestamp resolution	ns	ns	µs	ns
Target	file	file	live (rpcap)	live (FIFO)
BPF filter	✗	✓	✗	✓
Per-packet metadata	✗	✓	✗	✓
Wireshark integration	open file	open file	live (libpcap rebuild)	live (extcap dir)
tcpdump integration	open file	open file	live (libpcap rebuild)	✗
Authentication	file perms	file perms	none	local user
Introduction	DPDK 16.07	DPDK 21.11	DPDK 26.07?	DPDK 26.07?
Use Case	deprecate?	performance	tcpdump users	least friction

Followup



Packet capture challenges