

# Packet Capture Challenges

*“Why can’t I just use tcpdump”*

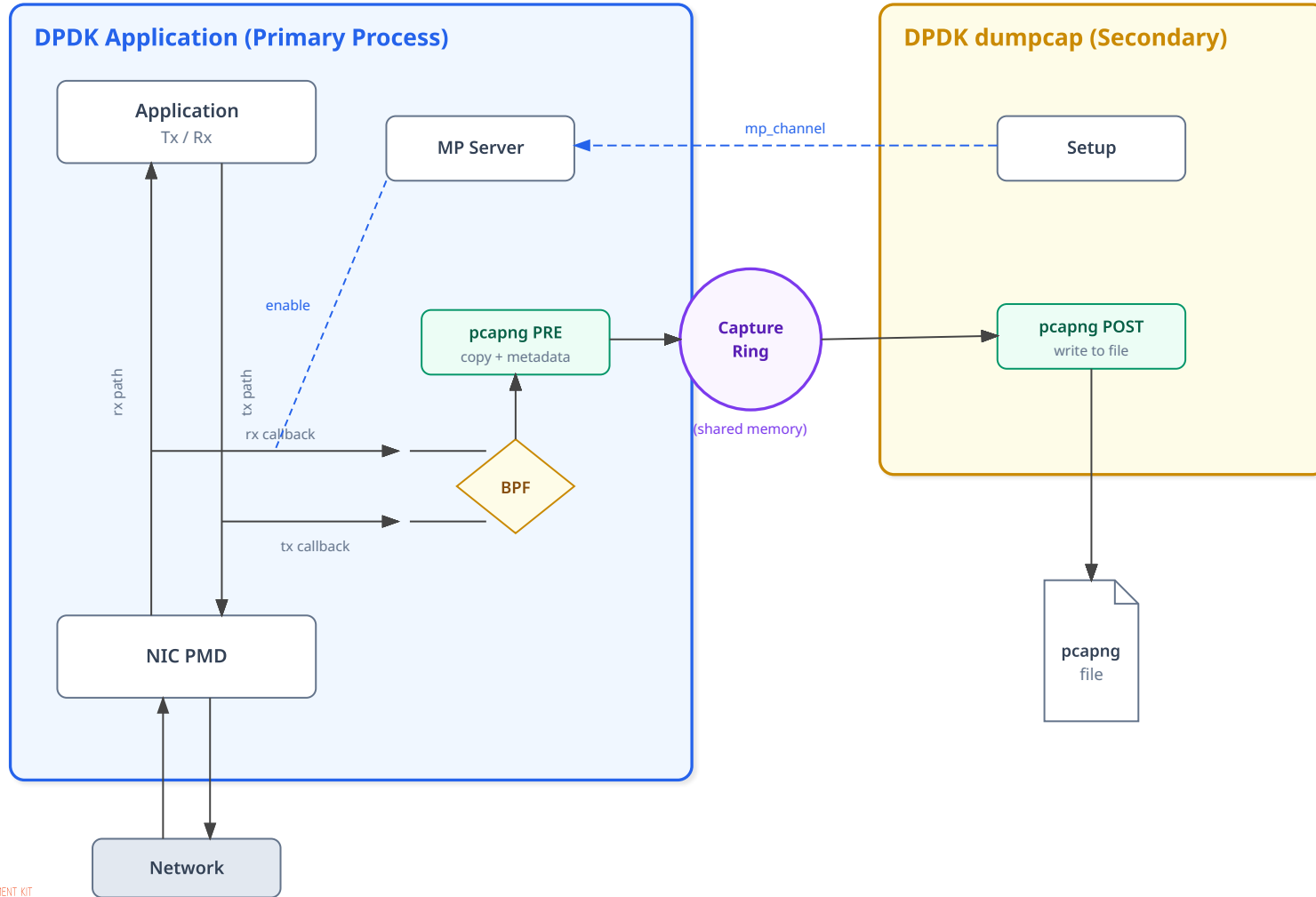


Stephen Hemminger

<[stephen@networkplumber.org](mailto:stephen@networkplumber.org)>

DPDK Summit, Stockholm Sweden

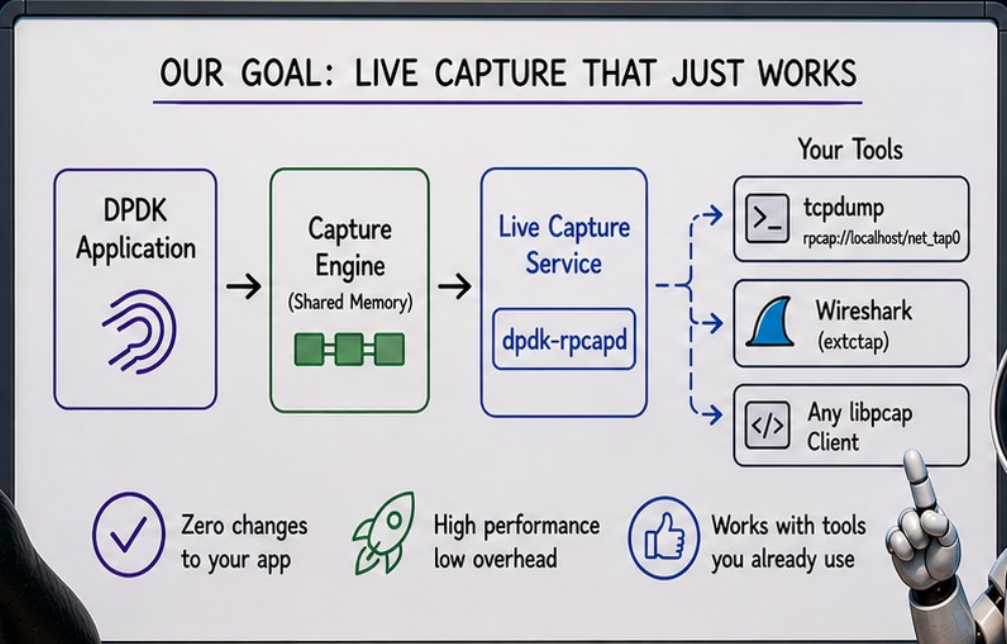
# Current : dpdk-dumpcap



# Packet Capture Ideas for **DPDK**

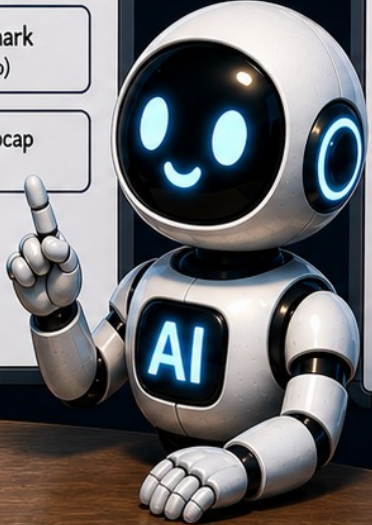


How do we get live packet capture out of DPDK easily?

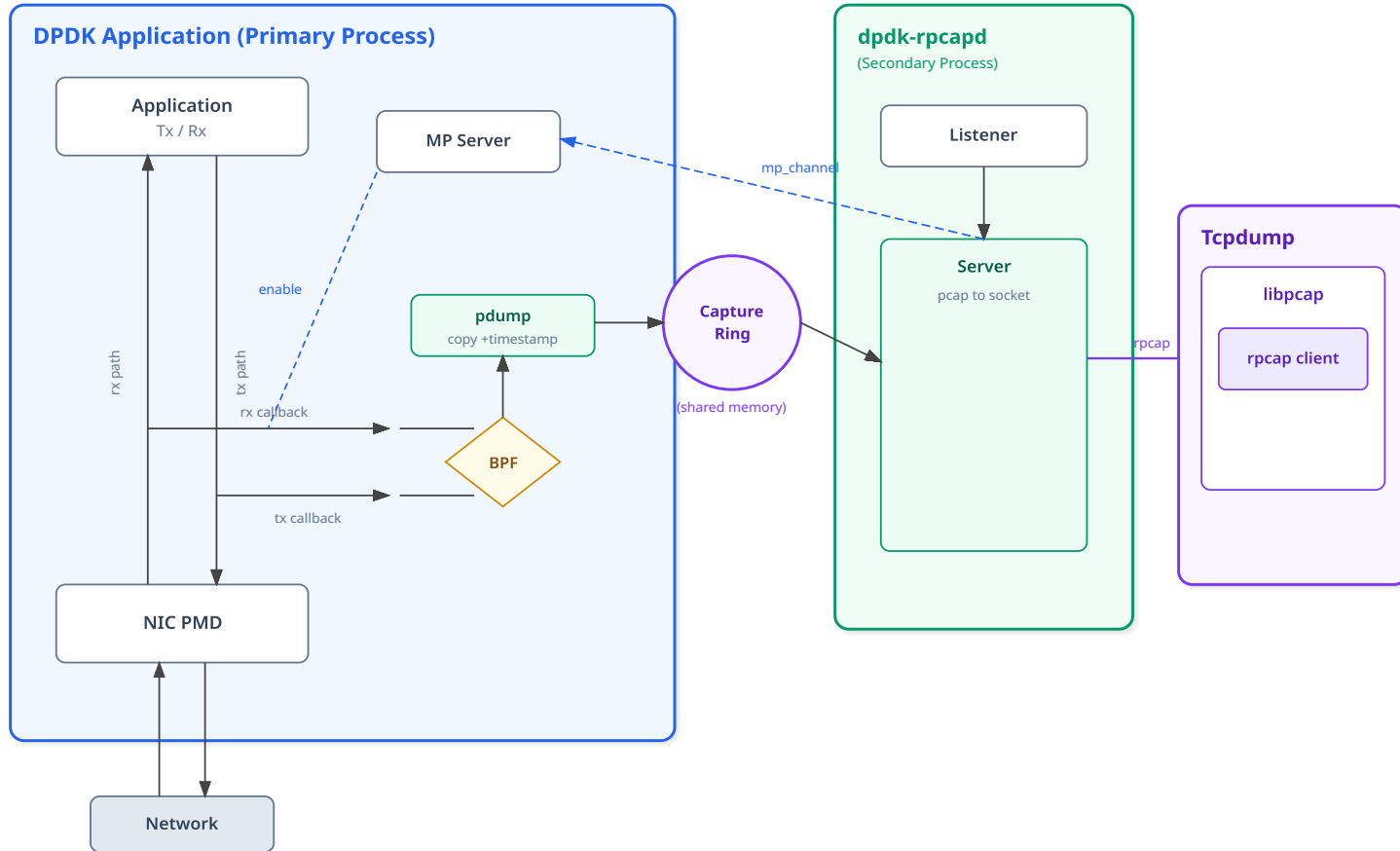


Let's make it live, simple, and familiar!

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)

```
— TCPDUMP (main focus) —
c.0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? phoenix.local. (151)
IP6 fe80::80c3:3fff:fede:28fd.5353 > ff02::fb.5353: 0 [9q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ftp._tcp.local. PTR (QM)? _webdav._tcp.local. PTR (QM)? _webdavs._tcp.local. PTR (QM)? _sftp-ssh._tcp.local. PTR (QM)? _smb._tcp.local. PTR (QM)? _afpovertcp._tcp.local. PTR (QM)? _nfs._tcp.local. PTR (QM)? _ipp._tcp.local. (141)
IP6 fe80::80c3:3fff:fede:28fd > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
IP6 fe80::80c3:3fff:fede:28fd.5353 > ff02::fb.5353: 0 [2q] [2n] ANY (QM)? d.f.8.2.e.d.e.f.f.f.f.3.3.c.0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. ANY (QM)? phoenix.local. (151)
10 packets captured
29 packets received by filter
0 packets dropped by kernel

— TESTPMD (traffic source) —
Configuring Port 0 (socket 0)
Port 0: 82:C3:3F:DE:28:FD
Checking link statuses...
Done
testpmd> start
rxonly packet forwarding - ports=1 - cores=1 - streams=1 - NUMA support enabled, MP allocation mode: native
Logical Core 17 (socket 0) forwards packets on 1 streams:
  RX P=0/Q=0 (socket 0) -> TX P=0/Q=0 (socket 0) peer=02:00:00:00:00:00

— RPCAPD (capture daemon) —
RPCAPD: client 127.0.0.1 connected
RPCAPD: awaiting connection
RPCAPD: capture started on net_tap0 (snaplen 2176, data port 33177)

[rpcap-dem0:sudo+ "TESTPMD (traffic sour" 15:13 01-May-26
```

# Key points

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

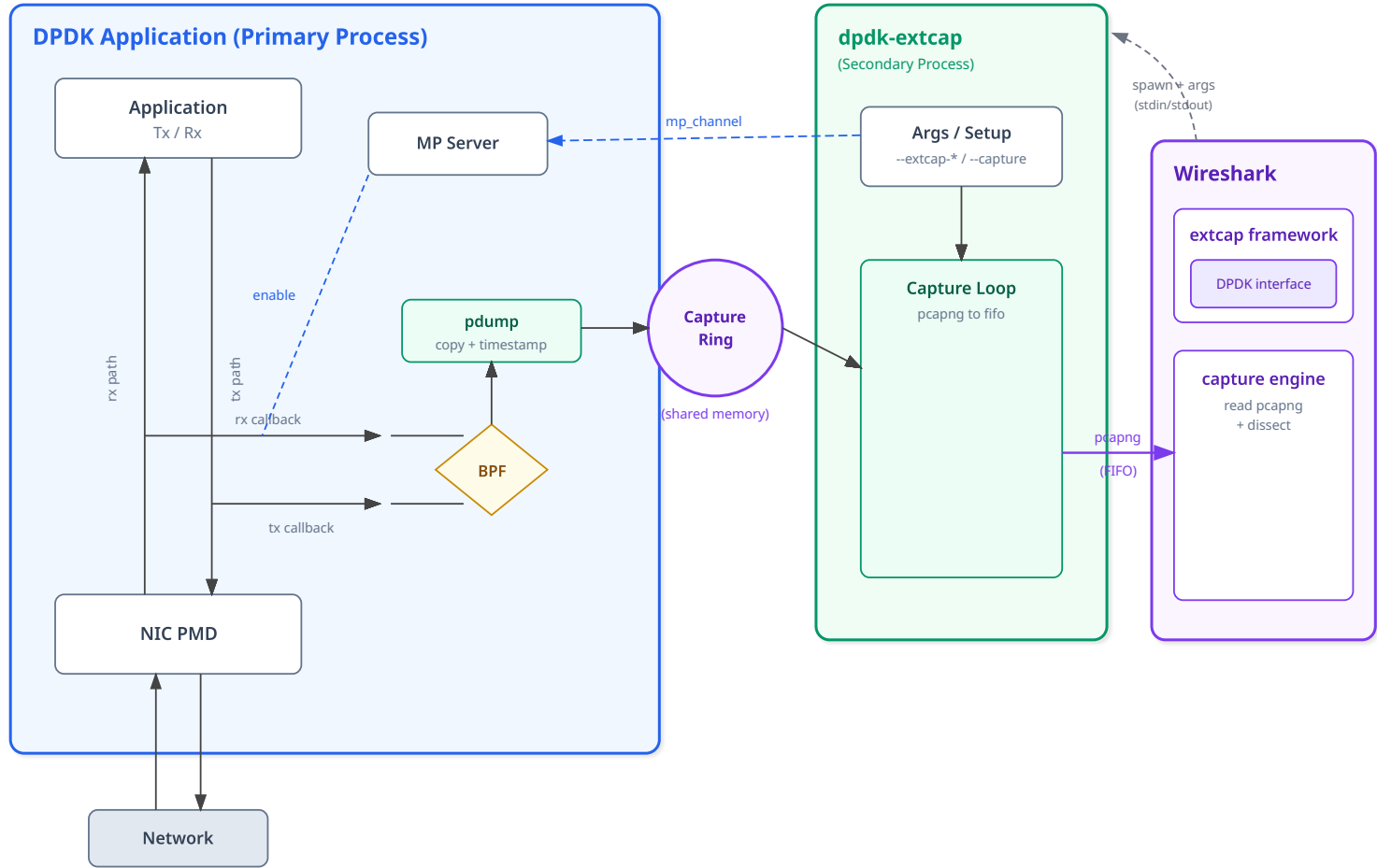


One more thing...

Can I use Wireshark instead?



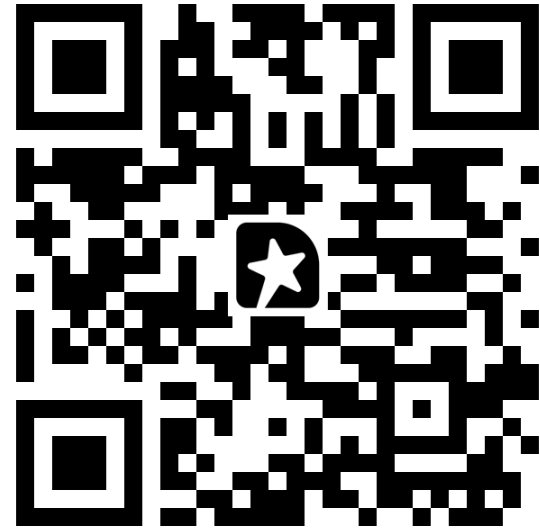
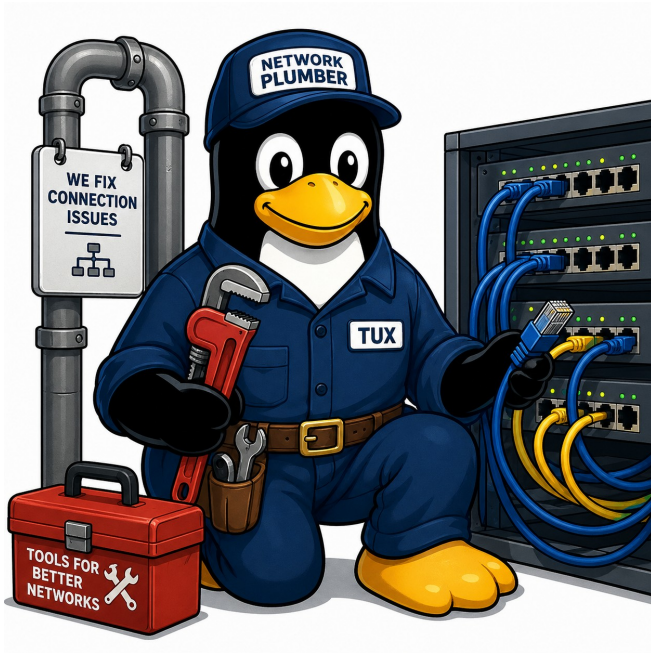
# Alternative: dpdk-extcap



## Capture Tools — Feature Comparison

Feature	dppdk-pdump	dppdk-dumpcap	dppdk-rpcapd	dppdk-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

