Hardware Acceleration of NetFlow Monitoring

Pavel Čeleda
celeda@liberouter.org

Jiří Novotný
novotny@ics.muni.cz

Joint EMANICS/IRTF-NMRG Workshop on Netflow/IPFIX
Usage in Network Management

Netflow Solutions

Routers – CISCO, Juniper, Enterasys, ...

- Busy with routing, flow monitoring addon feature.
- Flow monitoring is not implemented in all models.
- Fixed placement, possible target of attacks.
- Often mandatory sampling, no advanced features.

Flow Probes – nProbe, fprobe, softflowd, ...

- Based on commodity HW – PC and standard NICs.
- Low price.
- Solutions when flow monitoring required but not available.

But

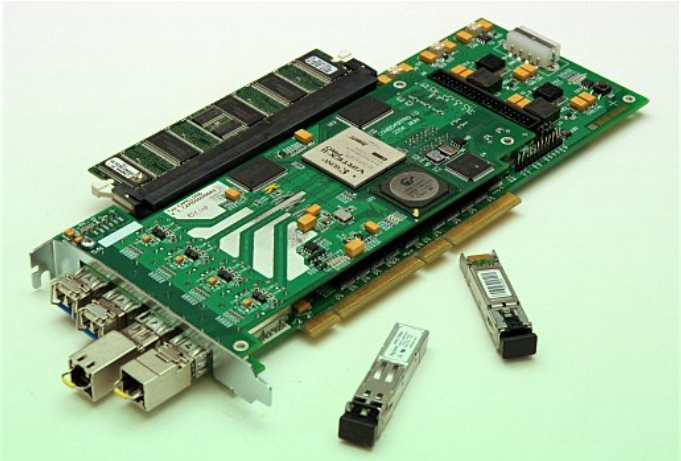
- Limited performance (PCAP, PCI-X) and stability problems.
- Packet drops.
- Time stamps issues.
- Requires extra system tuning and system/tools hacks.

Hardware Acceleration

Motivation

- PC is flexible but not fast enough to process gigabit links.
- Hardware is fast but not easy to use.

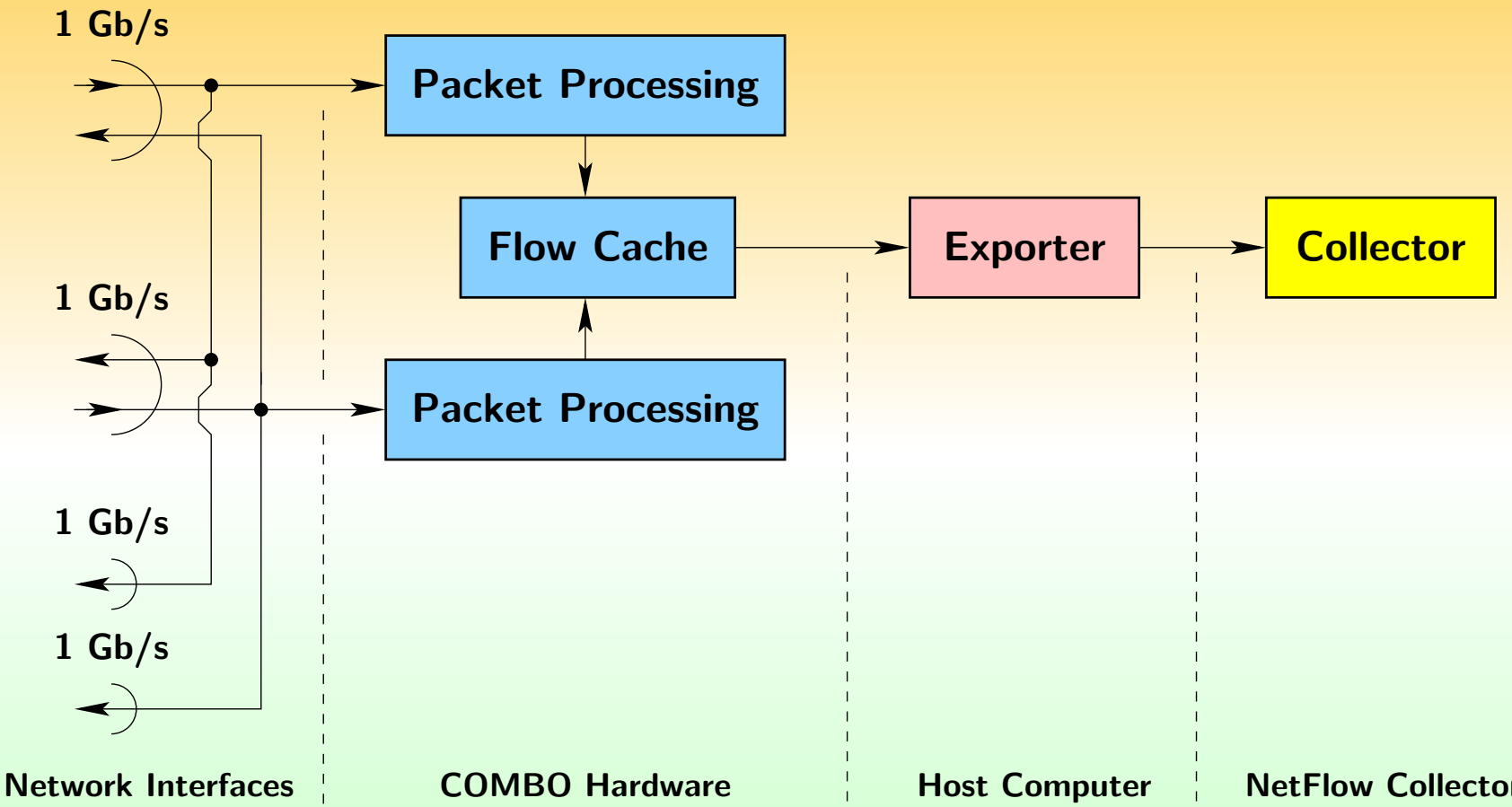
$\Rightarrow$ Combination of PC and programmable hardware (FPGA).



FlowMon Probe - Overview

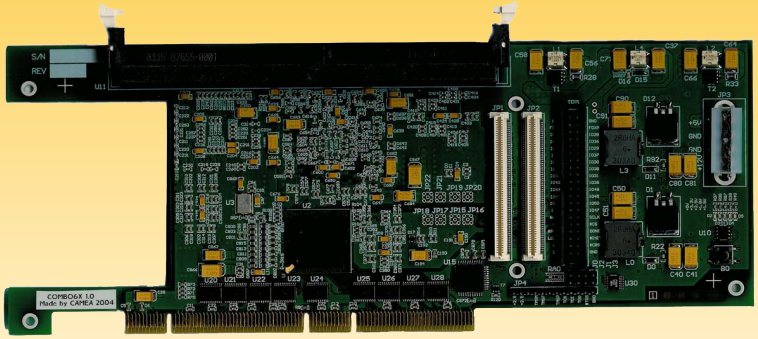
- Mobile network appliance, no fixed network position.
- Independent of network infrastructure used.
- Based on Linux $\rightarrow$ "unlimited" addon smart extensions.
- Low system load ($< 5\%$) for unsampled traffic.
- Observes whole network traffic under all conditions.
- Standard compliant - NetFlow v5/9 and IPFIX.
- User defined templates for NetFlow v9 and IPFIX.
- Simultaneous export to multiple collectors.
- Secure configuration via NETCONF web interface or SSH.
- Netflow monitoring solution from 10 Mb/s to 10 Gb/s.

FlowMon Probe Architecture

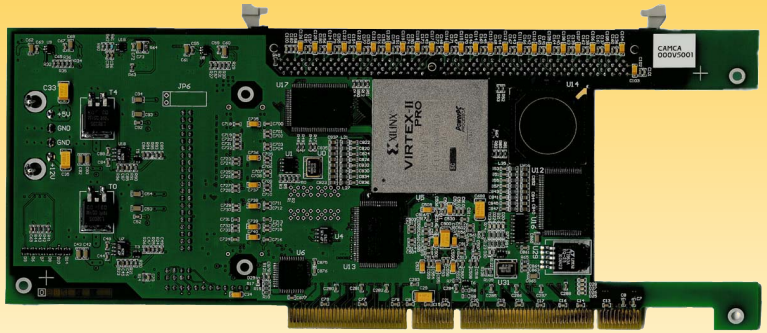


FlowMon probe block schema.

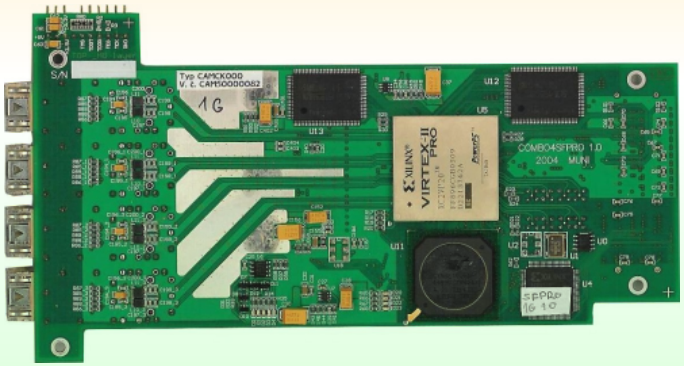
COMBO Card Family



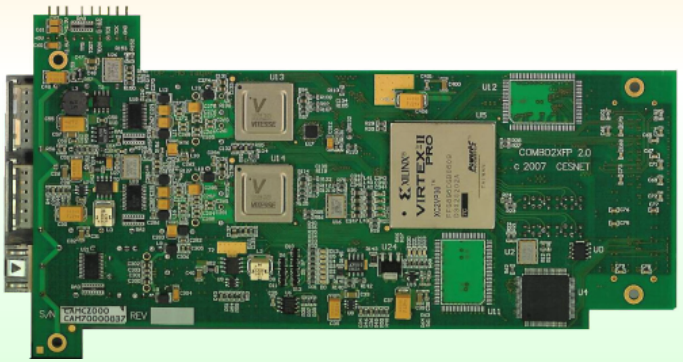
COMBO6X front side



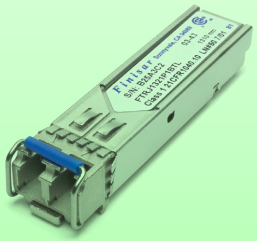
COMBO6X back side



COMBO-4SFPRO 4x1Gb/s

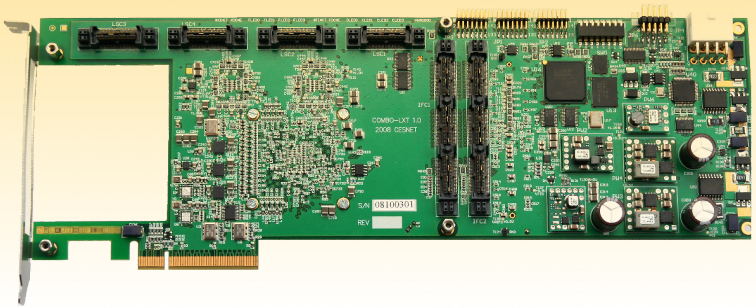


COMBO-2XFP2 2x10Gb/s

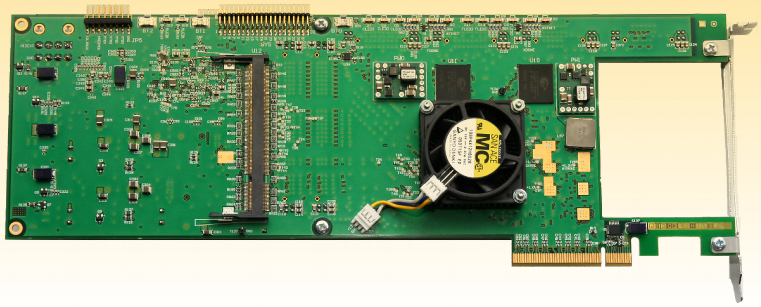


COMBOv2 Card Family

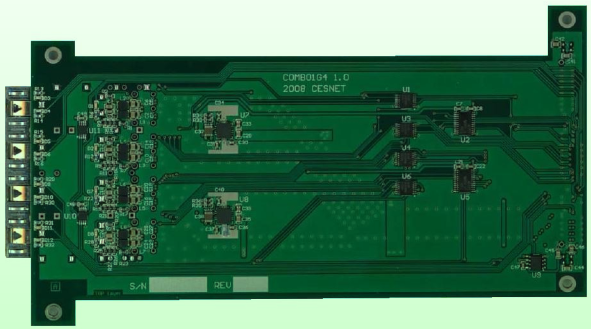
- Successor of COMBO6(X) card family.
- Designed for 10+ Gb/s speeds (up to 40-100 Gb/s).



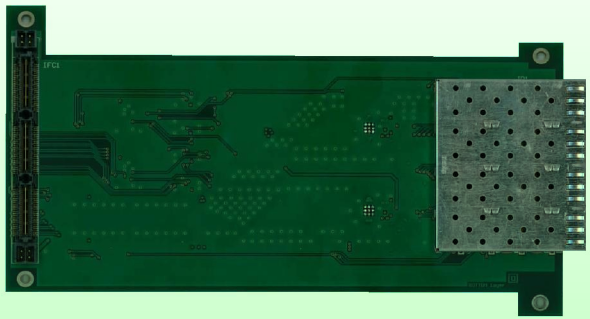
COMBO-LXT front side



COMBO-LXT back side

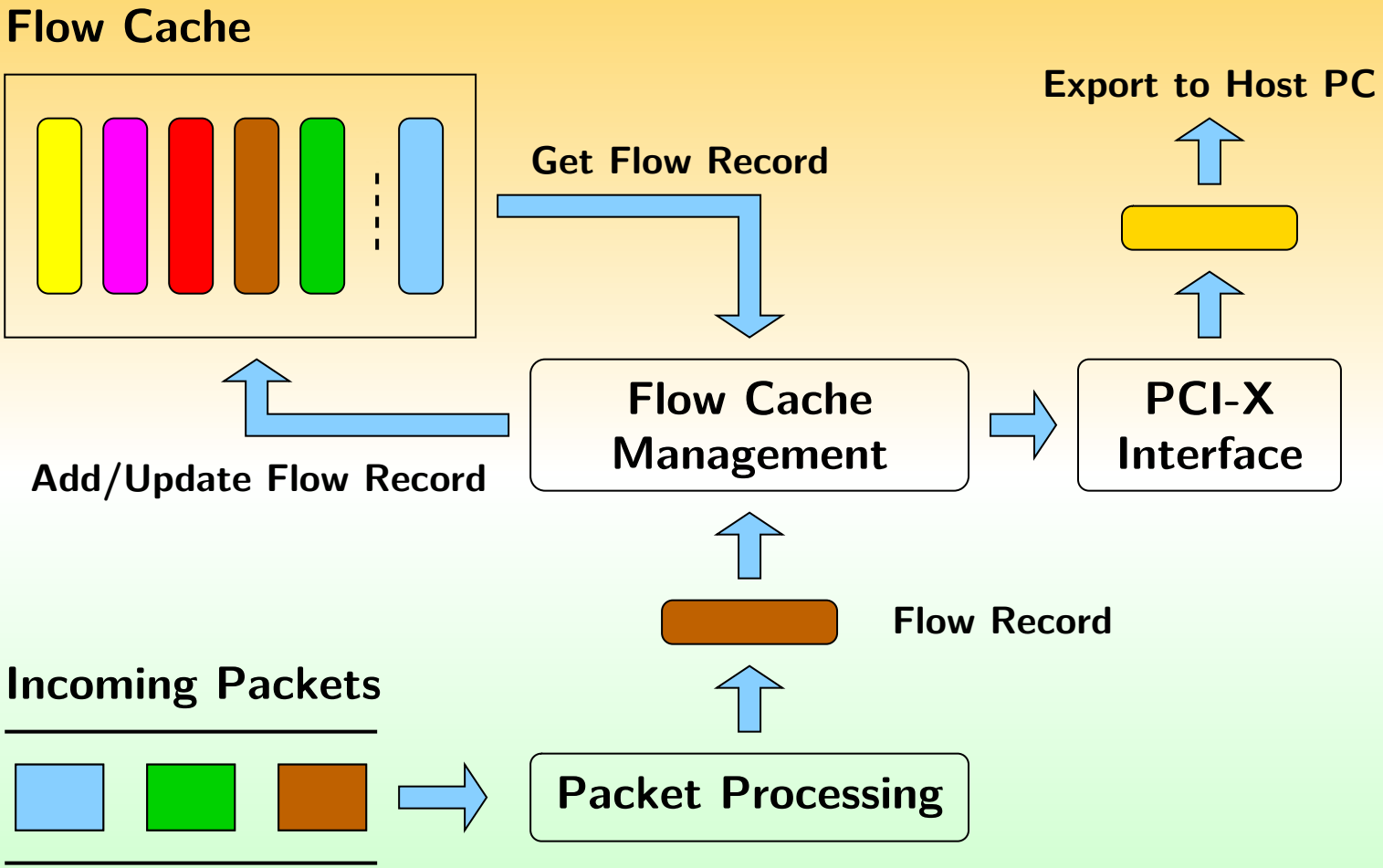


COMBOI-1G4 front side



COMBOI-1G4 back side

Packet Processing – Flow Cache – I



Metering process in FPGA.

Packet Processing – Flow Cache – II

Flow Cache Features

- Flow management unit uses bidirectional linked list implemented in hardware for LRU (Least Recently Used).
- Very accurate timeouts (5 μs interval).
- Statistic information in flow record is updated for each incoming packet.

Flow Cache Capacity

- Capacity depends on the COMBO card memory configuration.
- SSRAM memory – 128 k flow records.
- DDR SDRAM memory – 512 k flow records.
- Active and inactive timeouts are user configurable.

FlowMon Probe – Firmware Summary

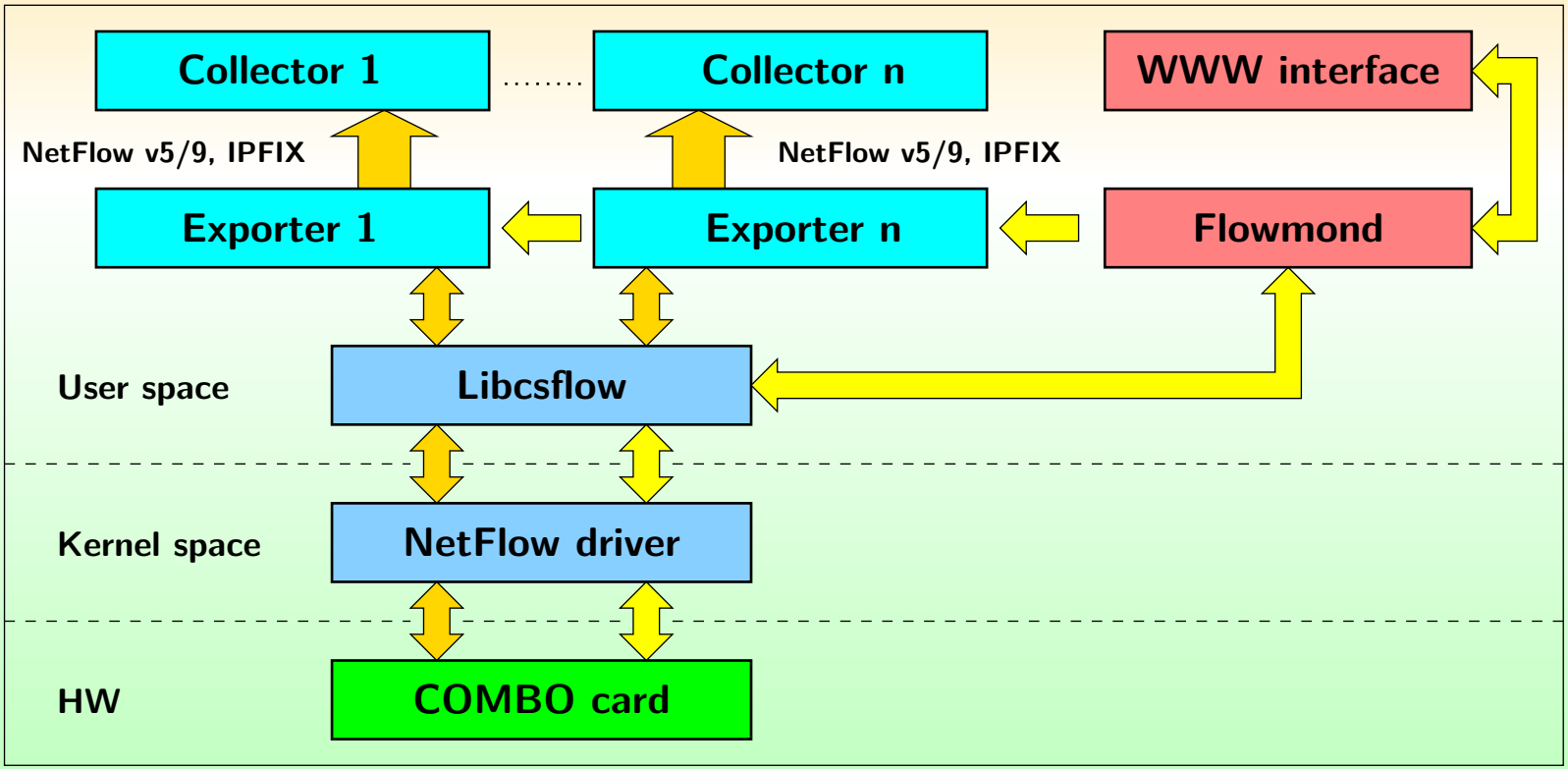
FPGA Firmware Features

- Support for 2×1 Gb/s or 1×10 Gb/s.
- IPv4, IPv6, VLAN, MPLS support.
- Flow cache 512 000 flow records.
- Static, random or adaptive sampling.
- Active and inactive timeouts.
- Repeater and splitter functionality.
- SFP and XFP transceivers (media convertor).

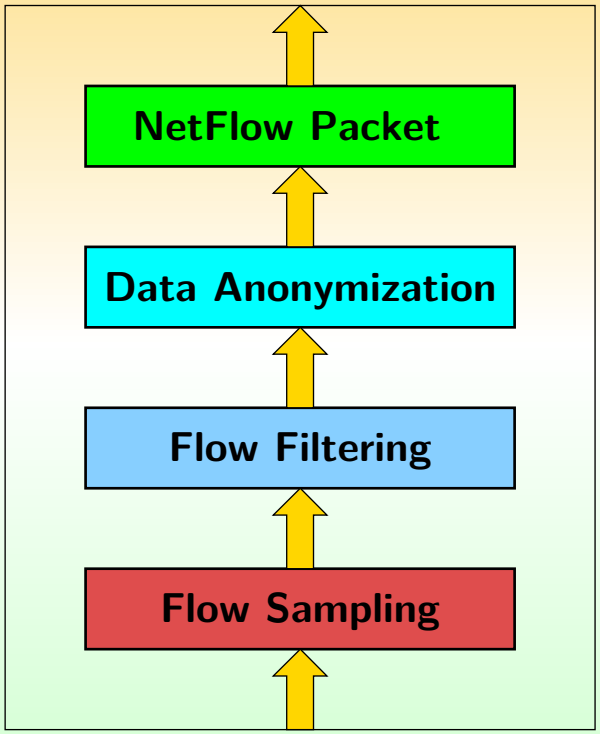
Reprogrammable FPGA chips.

FlowMon Probe – SW Architecture

- Linux 2.6 kernel drivers and user space libraries (libcsflow).
- Terminal and web configuration programs.
- NetFlow ver. 5/9 and IPFIX flow exporter program.



Flow Exporter Architecture

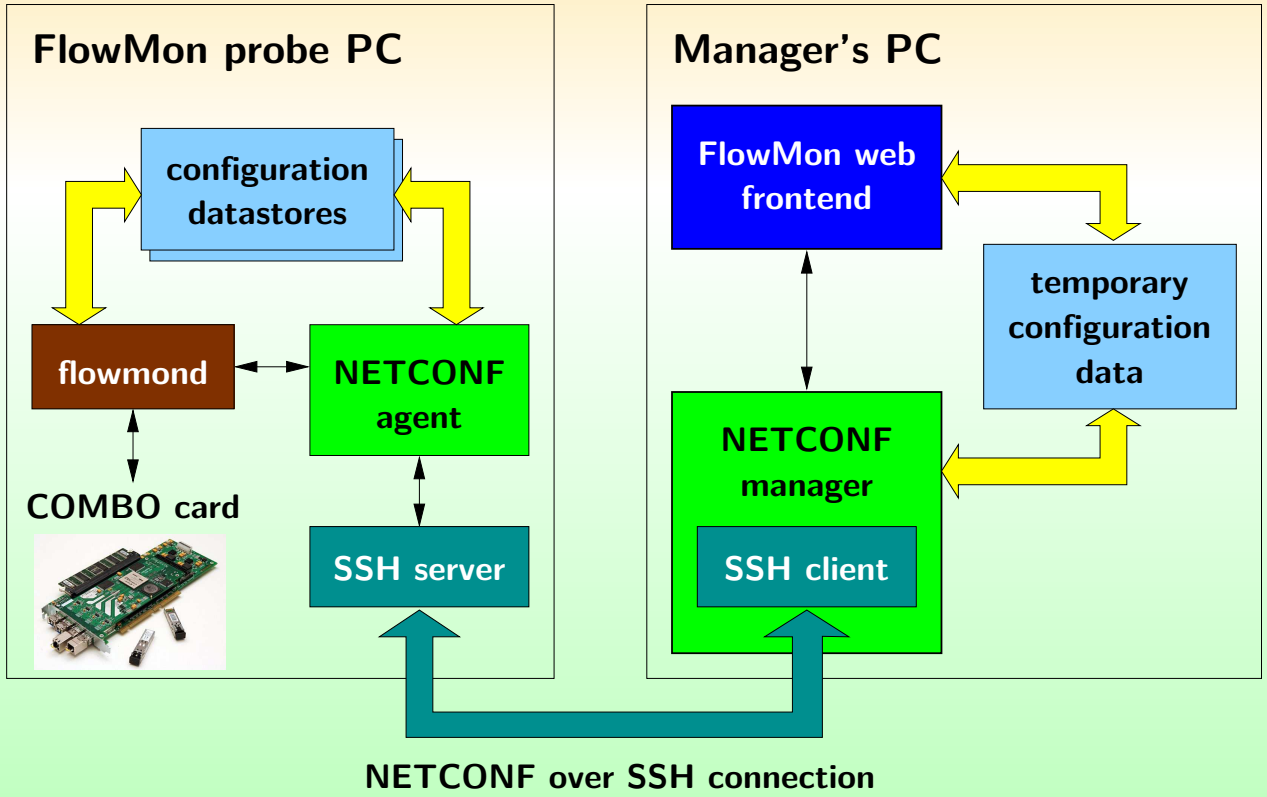


Exporter layers.

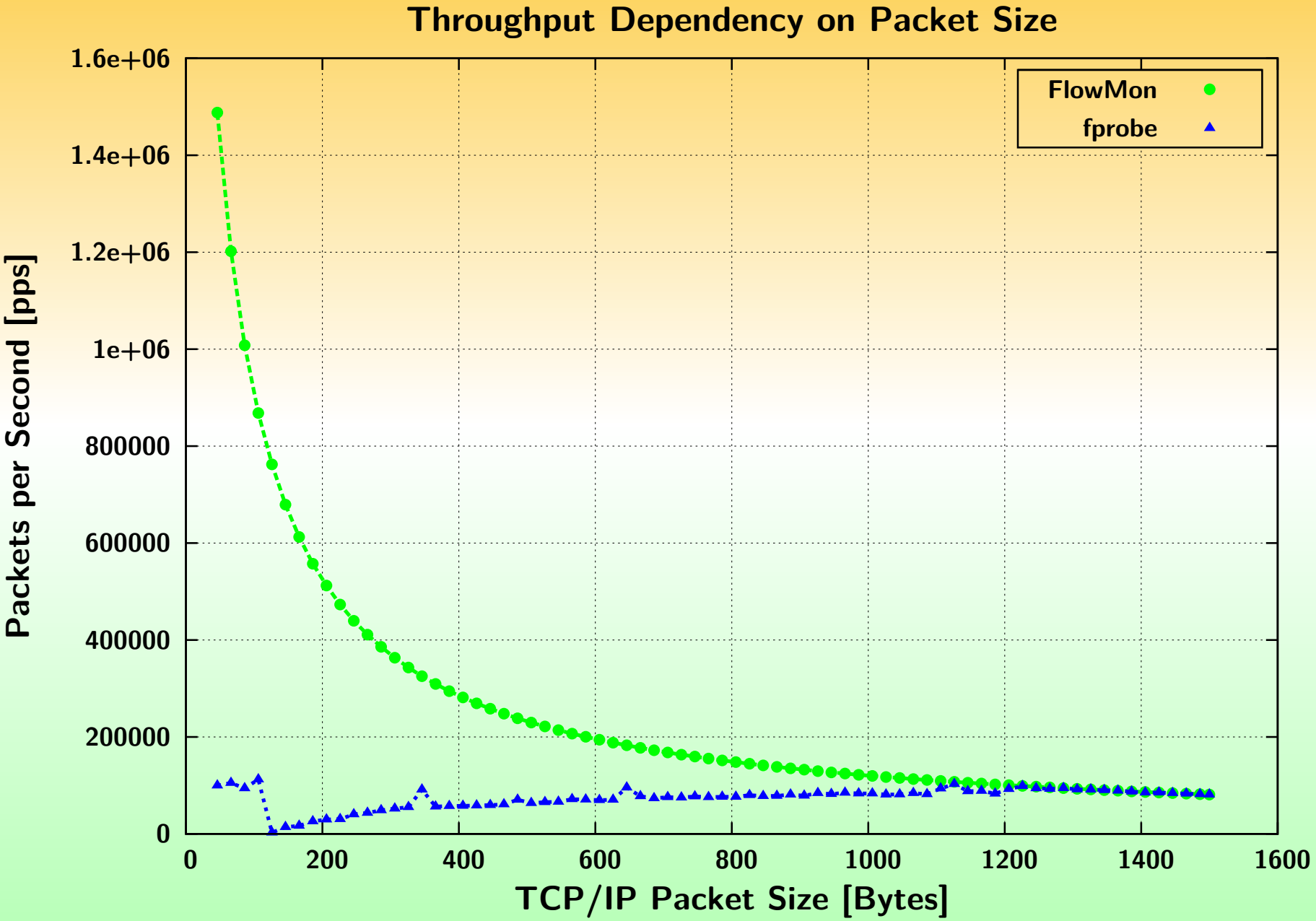
- Multiple concurrent exporters.
- Unique exporter identification.
- NetFlow v5/9 (RFC 3954) and IPFIX (RFC 3917) support.
- User defined templates for NetFlow v9 and IPFIX.
- Flow data anonymisation (AES or prefix substitution).
- Per-exporter flow filtering.
- Deterministic flow sampling.

NETCONF – Remote Probe Configuration

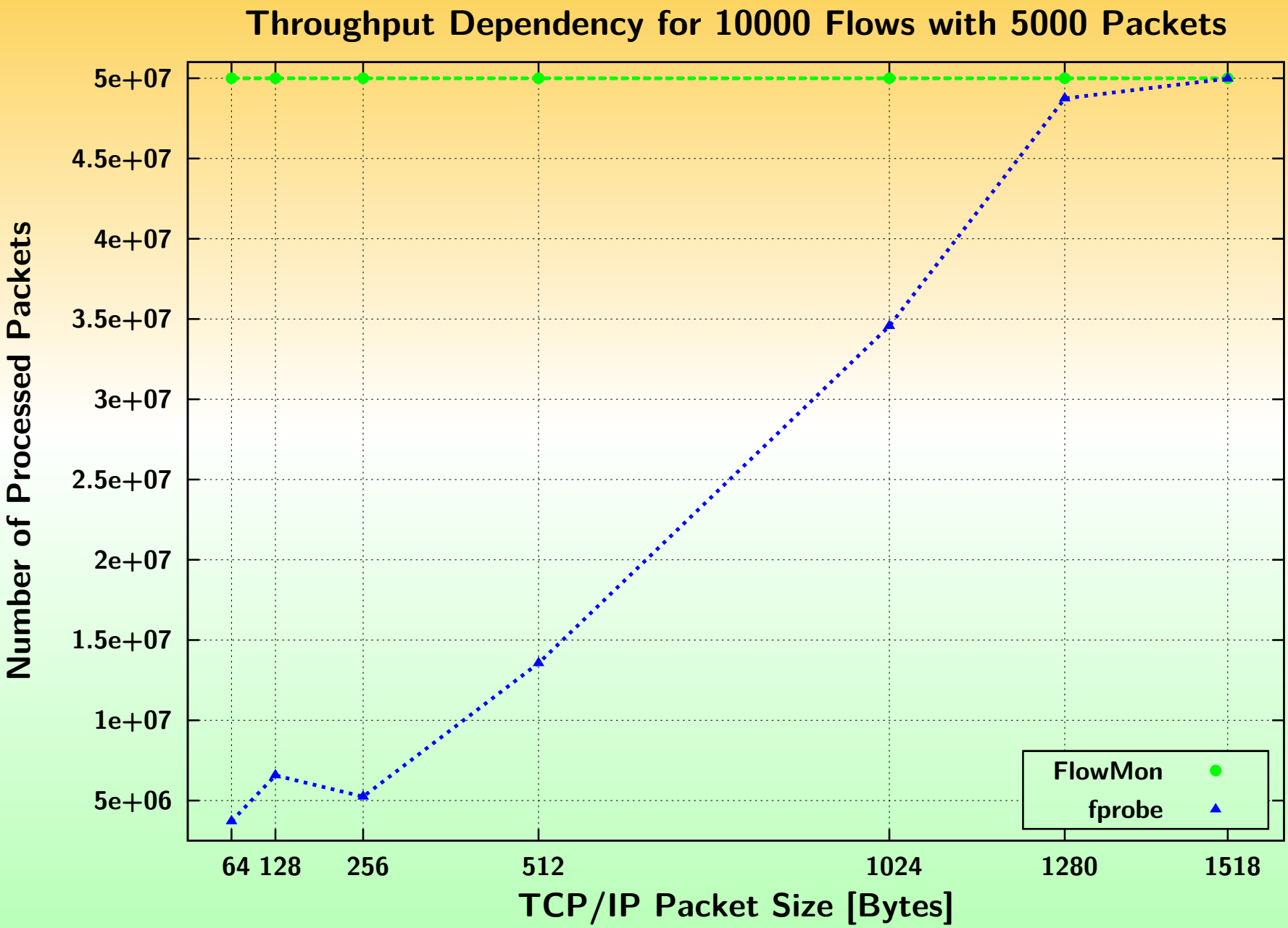
- NETCONF system – tool for changing configuration data.
- Web front end – performs critical administrative operations.
- Security by default – HTTPS and SSH.



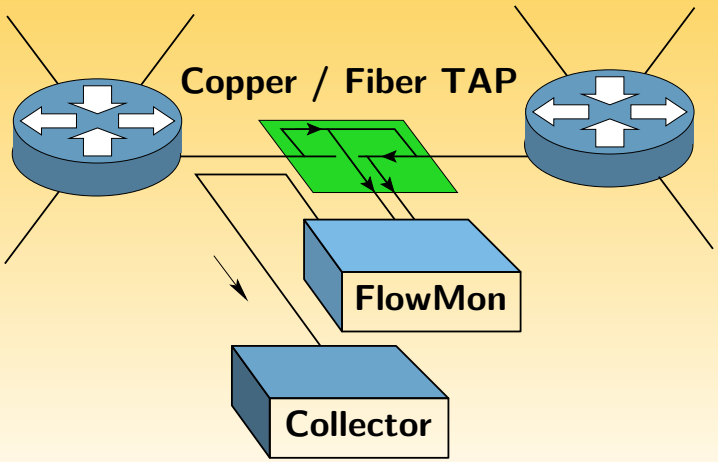
Throughput Test



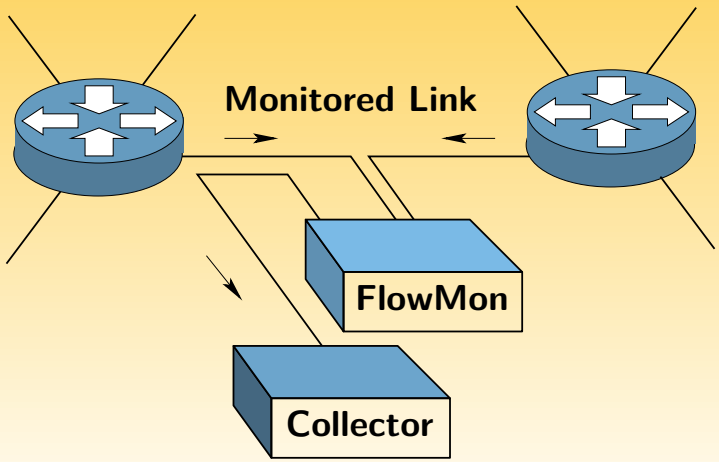
Flow Cache Test



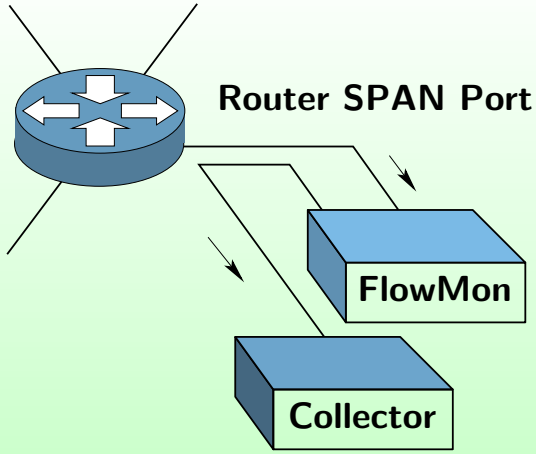
FlowMon Probe Network Connection



TAP Mode



In-line Mode



SPAN Mode

Tested NetFlow Collectors

FlowMon Probe has been tested with the following collectors:

Open Source

- NfSen – nfsen.sourceforge.net – **recommended**.
- FTAS – www.cesnet.cz.
- IBM AURORA – www.zurich.ibm.com/aurora.
- ntop – www.ntop.org.
- libipfix – ants.fokus.fraunhofer.de/libipfix – IPFIX.

Commercial

- Caligare Flow Inspector – www.caligare.com
- NetFlow Tracker – www.flukenetworks.com

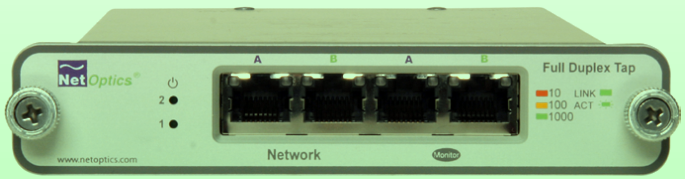
Lessons Learned From Practice - I

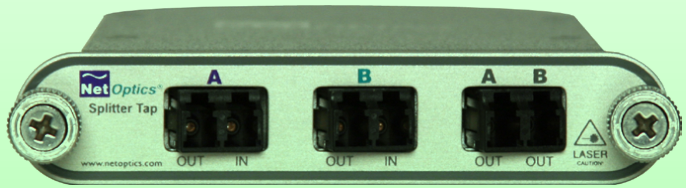
Our Testbed and Deployment Network

- HW testers for line-rate (worst-case) testing.
- NREN backbones, university campuses and ISP networks.
- Sustain live traffic 4-5 Gb/s, 700 kpkt/s, 30 kflows/s.
- Long-time NetFlow monitoring - probes and collectors.

Connection Must Have Features

- TAPS $\times$ SPAN - reliability of measured data.
- Network interfaces - SMF, MMF, Copper.
- Sensitive transceivers for low-signal inputs.





Lessons Learned From Practice - II

Probes Must Have Features

- Packet rate – number of packets/s to avoid packet drops.
- Flow cache capacity – affects number of generated flows.
- Timestamps – precise timestamps to identify traffic flows.
- Output reliability – we are interested in all packet sizes, all traffic mixes, bursts, (D)DoS traffic, ...

Collectors Must Have Features

- RFC compliant support for NetFlow v9.
- Store and process large volumes of (k)flows/s.

Conclusion

Who Is Using FlowMon

- Scientific research projects – flow monitoring (GÉANT2), network security (CSIRT), anomalies detection (CAMNEP).
- Recognized by GÉANT2 as part of security toolset + NfSen.
- Industry – Invea-Tech spin-off company uses FlowMon probes.

INVEA-TECH FlowMon

- Reasearch results (EU projects - SCAMPI, GÉANT2; CESNET MSM6383917201) transferred to universitie's spin-off company.
- FlowMon finished to fit market and customers needs.
- Standard and hardware-accelerated probe models.
- Complete monitoring solution from 10 Mb/s to 10 Gb/s.

Thank You For Your Attention

liberouter

Hardware – Accelerated Network Traffic Monitoring

Pavel Čeleda
celeda@liberouter.org

Jiří Novotný
novotny@ics.muni.cz

Liberouter Project
www.liberouter.org