

FlowMon Probe Overview

- Linux PC with a flow-processing accelerator
- Accelerator – add-on PCI card
 - ▷ full-duplex Gigabit Ethernet repeater
 - ▷ full-duplex flow-processing engine
- Monitors IPv4 and IPv6 traffic
- Cache for 64K flows
- Sampling (optional!)
 - ▷ standard statistical sampling
 - ▷ sample-and-hold

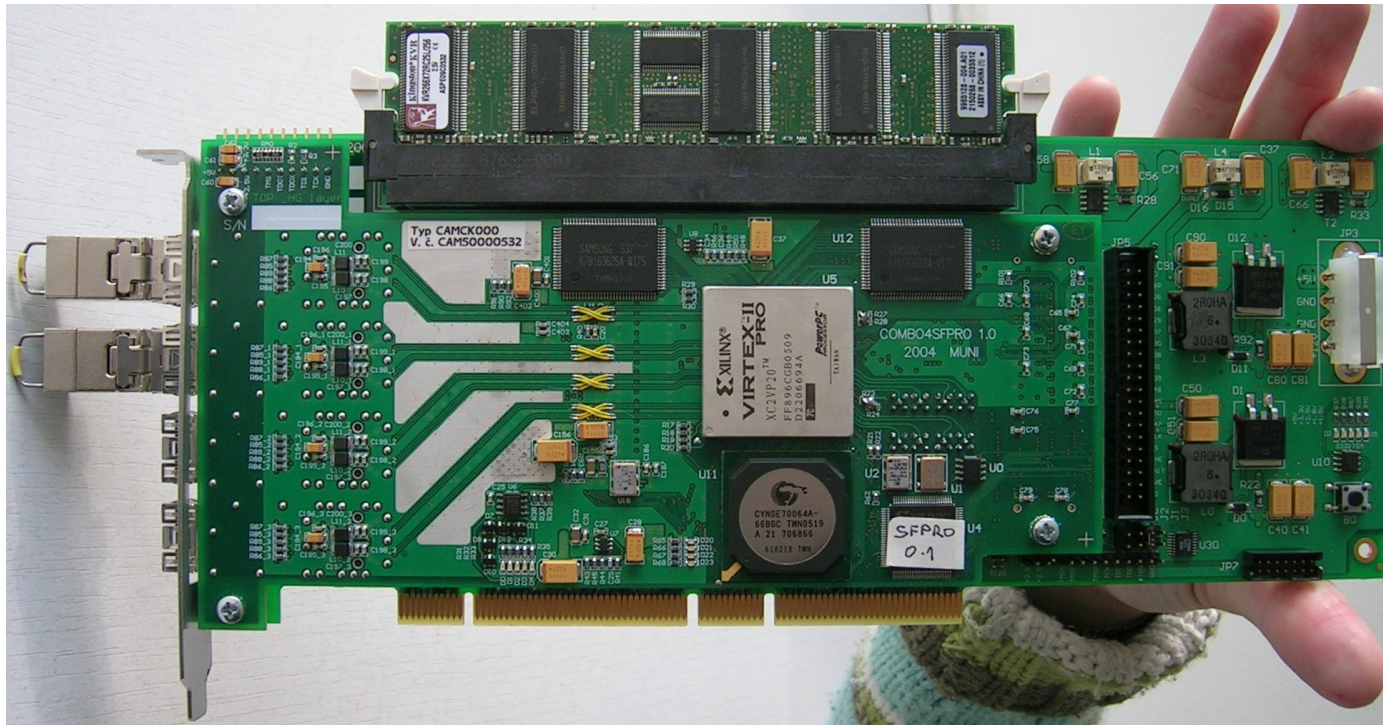
FlowMon Probe Overview (cont.)

- Export to multiple NetFlow v5 and v9 collectors
 - ▷ Per-collector record filtering (address ranges)
 - ▷ User-defined NetFlow v9 templates

- Make flow data available anywhere, anytime, in the most appropriate form
- Security – stealth device
- Performance – dedicated device
- Flexibility
 - ▷ adaptive sampling rate and/or inactive timeout
 - ▷ richer flow processing options
 - ▷ combination with other approaches (payload inspection)
- Platform for further research

- Sandwich of two FPGA-based cards
 - ▷ v1: COMBO6 & COMBO-4MTX/4SFP (32/33 PCI)
 - ▷ v2: COMBO6X & COMBO-4SFPRO (64/66 PCI, PCI-X)
- Porting to 10GE underway
 - ▷ :-(10GE interface card has to be redesigned

Hardware (cont.)



COMBO6X (bottom) and COMBO-4SFPRO (top)

- Device driver for Linux 2.4 and 2.6 kernels
- Flow exporter programs for NetFlow v5 and v9
- Configurable parameters:
 - ▷ active and inactive timeout
 - ▷ sampling rate (sample-and-hold option)
 - ▷ v9 template resend period
 - ▷ per-collector record filters

Filter Example

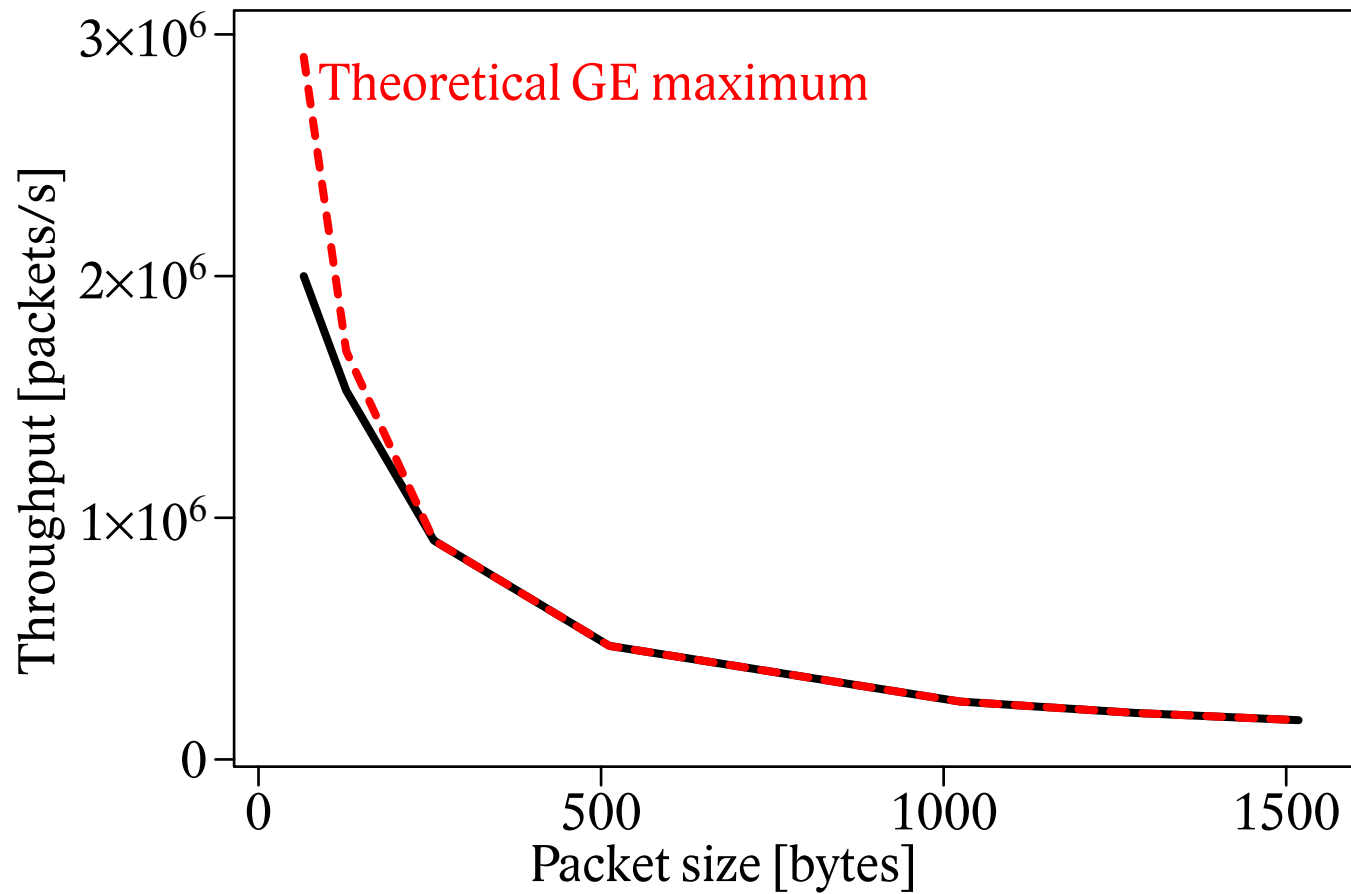
```
172.29.12.129 - 172.29.15.255 : src-dst
```

```
195.113.188.1 - 195.113.188.1 : dst
```

```
# All IPv6 flows are exported
```

```
:: - ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff : src-dst
```

Full-Duplex Performance



- Two probes deployed in CESNET backbone, more planned
- Additional tests by 4 JRA2 partners (SURFnet, SWITCH, GRNET, Bulgarian Acad. Sci.)
- Interoperable with NERD, NfSen, FTAS
 - ▷ IPv4 and IPv6 flows
 - ▷ NetFlow v5 and v9

Future Plans

- Commercial availability and support (summer 2006)
- Milestone – December 2006
 - ▷ GE line rate for all packet sizes
 - ▷ 10GE interface (throughput about 3.2 Gb/s)
 - ▷ Mirroring traffic to the remaining ports

Future Plans (cont.)

- Milestone – July 2007
 - ▷ cache for 500 Kflows
 - ▷ adaptive control of inactive timeout and sampling rate
 - ▷ configurable flow record
 - ▷ Anonymisation
 - ▷ IPFIX

Further Information

- GN2 deliverable DJ2.2.2

<http://www.geant2.net/server/show/nav.00d00b002>

- TNC 2006 paper (Monitoring&Measurement session)

- Home page

<http://www.flowmon.org/flowmon-probe>