Hardware acceleration of network traffic monitoring and analysis in 100Gbps networks

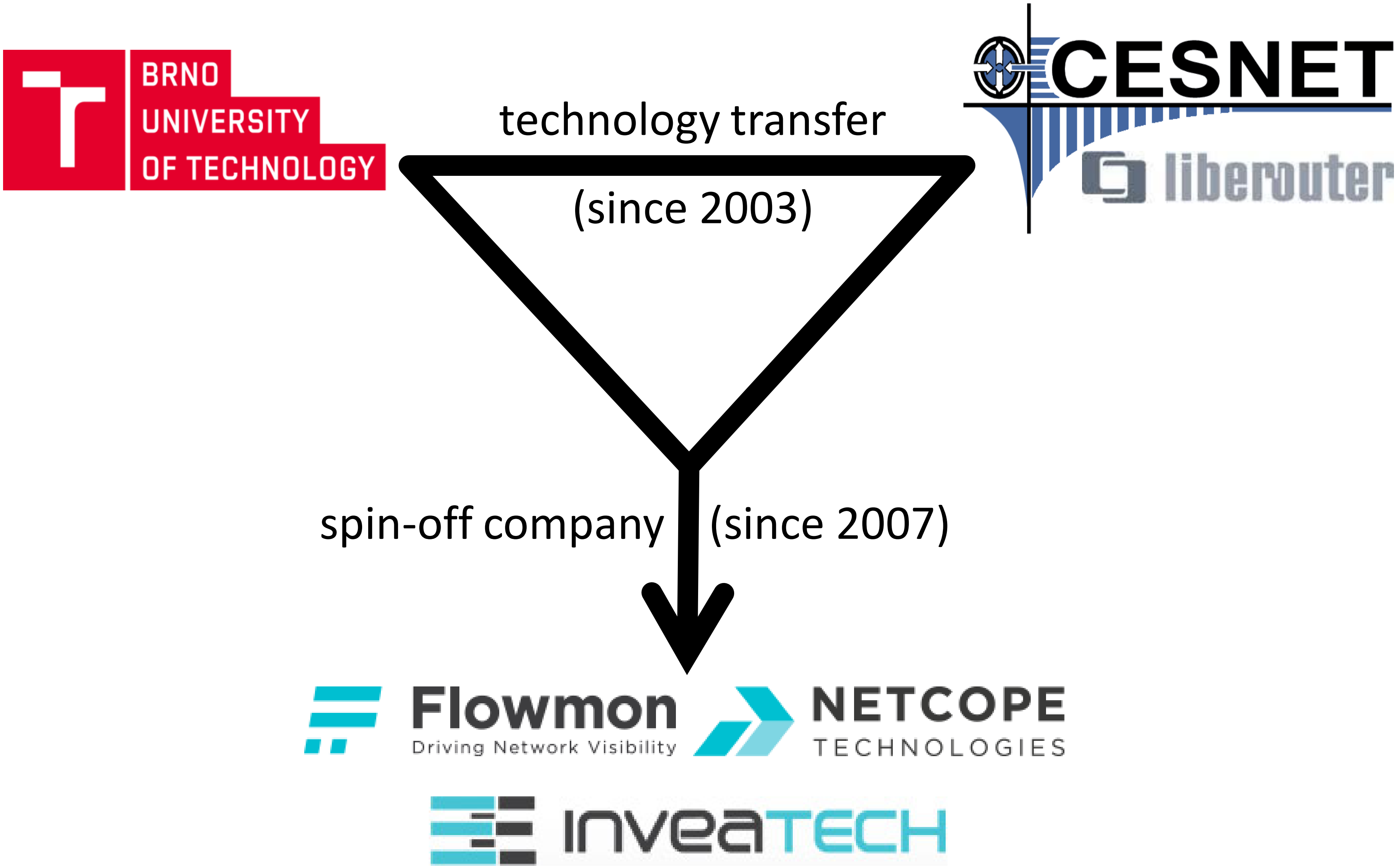
Lukáš Kekely

Brno University of Technology, Faculty of Information Technology
Božetěchova 1/2, 612 66 Brno - Královo Pole
ikekely@fit.vutbr.cz

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

HiPEAC, 21.02.2017

Cooperation



technology transfer

(since 2003)

spin-off company

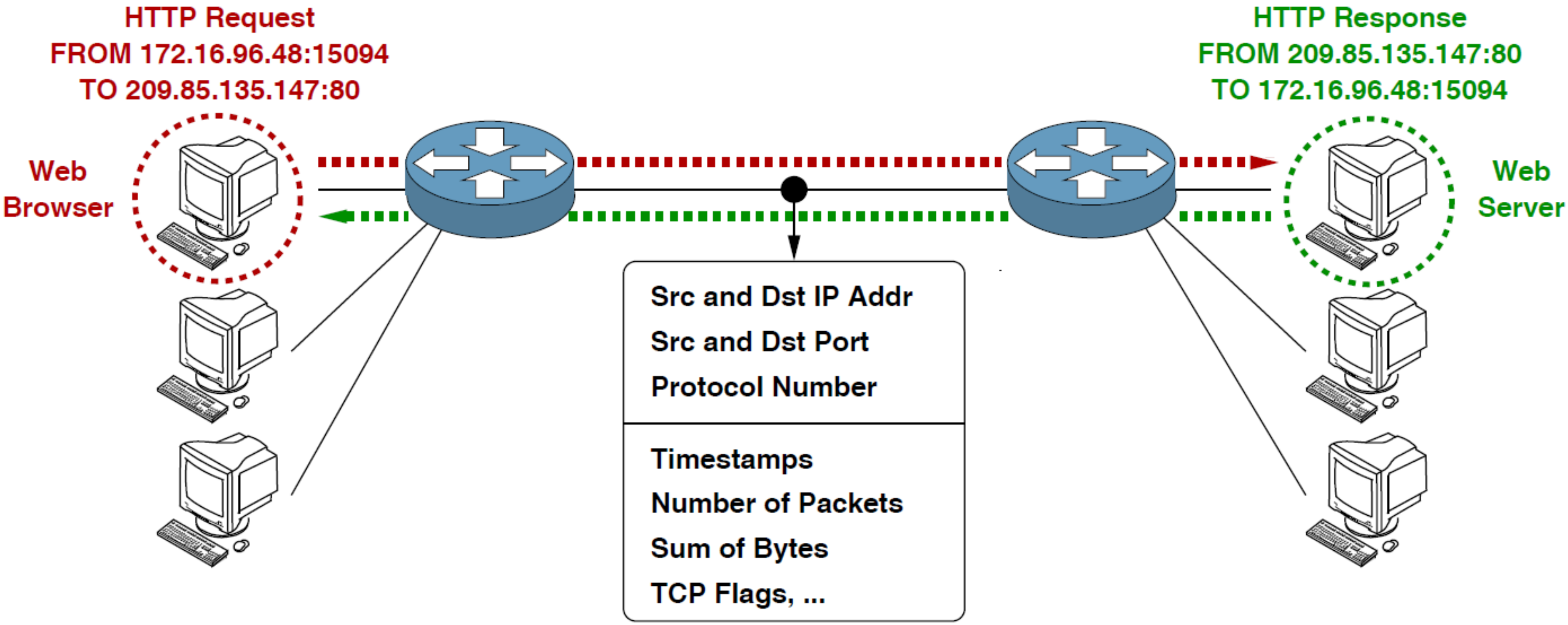
(since 2007)

Cooperation

- AFI's **Best Cooperation of the Year** national award, 2nd place
  - project TA03010561: *Distributed System for Complex Monitoring of High-Speed Networks*
- highest national research award **Czech Head**, in category **Industrie award** by Ministry of Industry and Trade
  - world's first 100 Gbps Ethernet interface card

Flow based monitoring

- communication **between who**, **when**, **how** and **how much**
  - can be enhanced by additional information (L7 layer)



HTTP Request
FROM 172.16.96.48:15094
TO 209.85.135.147:80

HTTP Response
FROM 209.85.135.147:80
TO 172.16.96.48:15094

Web Browser

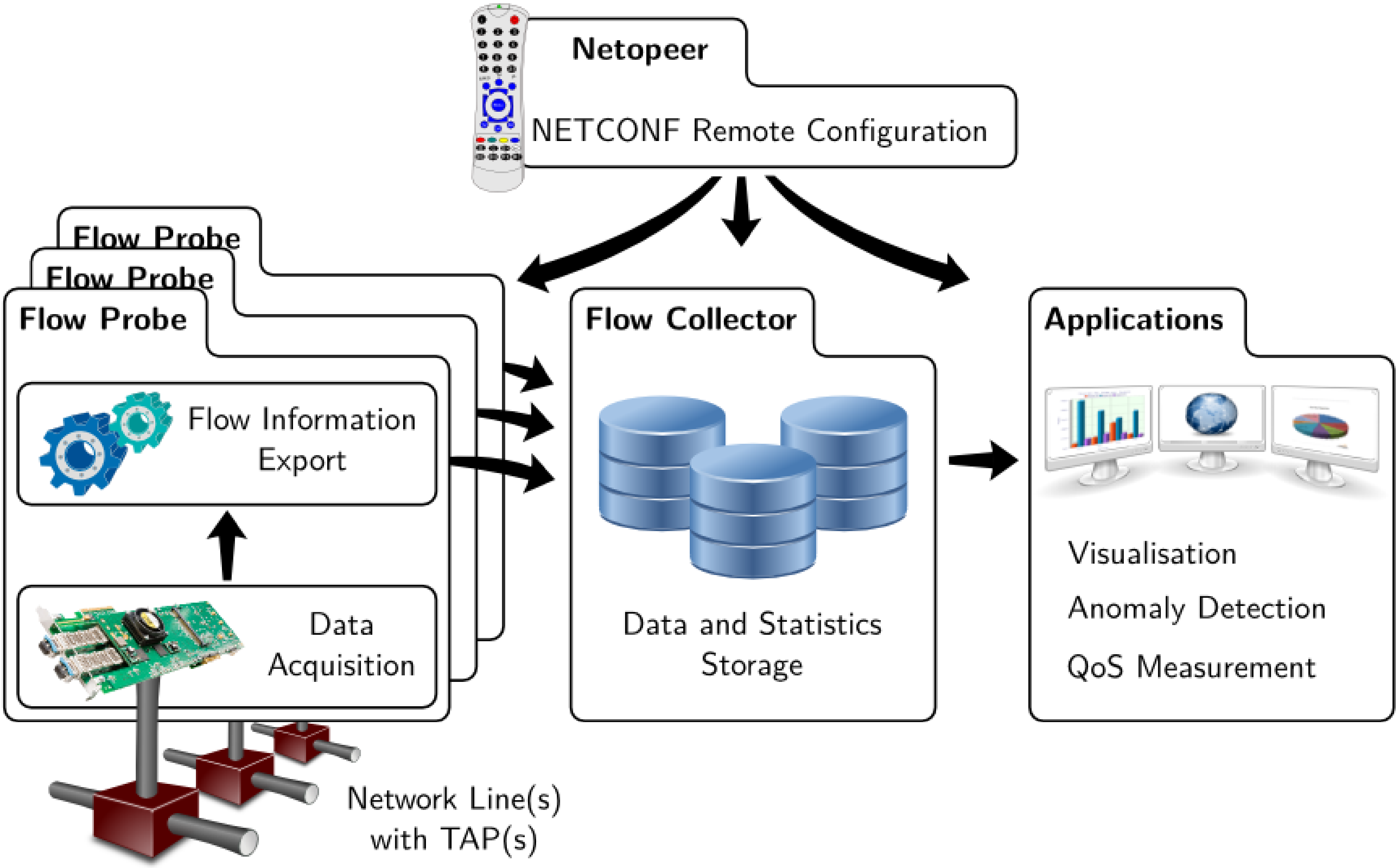
Web Server

Src and Dst IP Addr
Src and Dst Port
Protocol Number

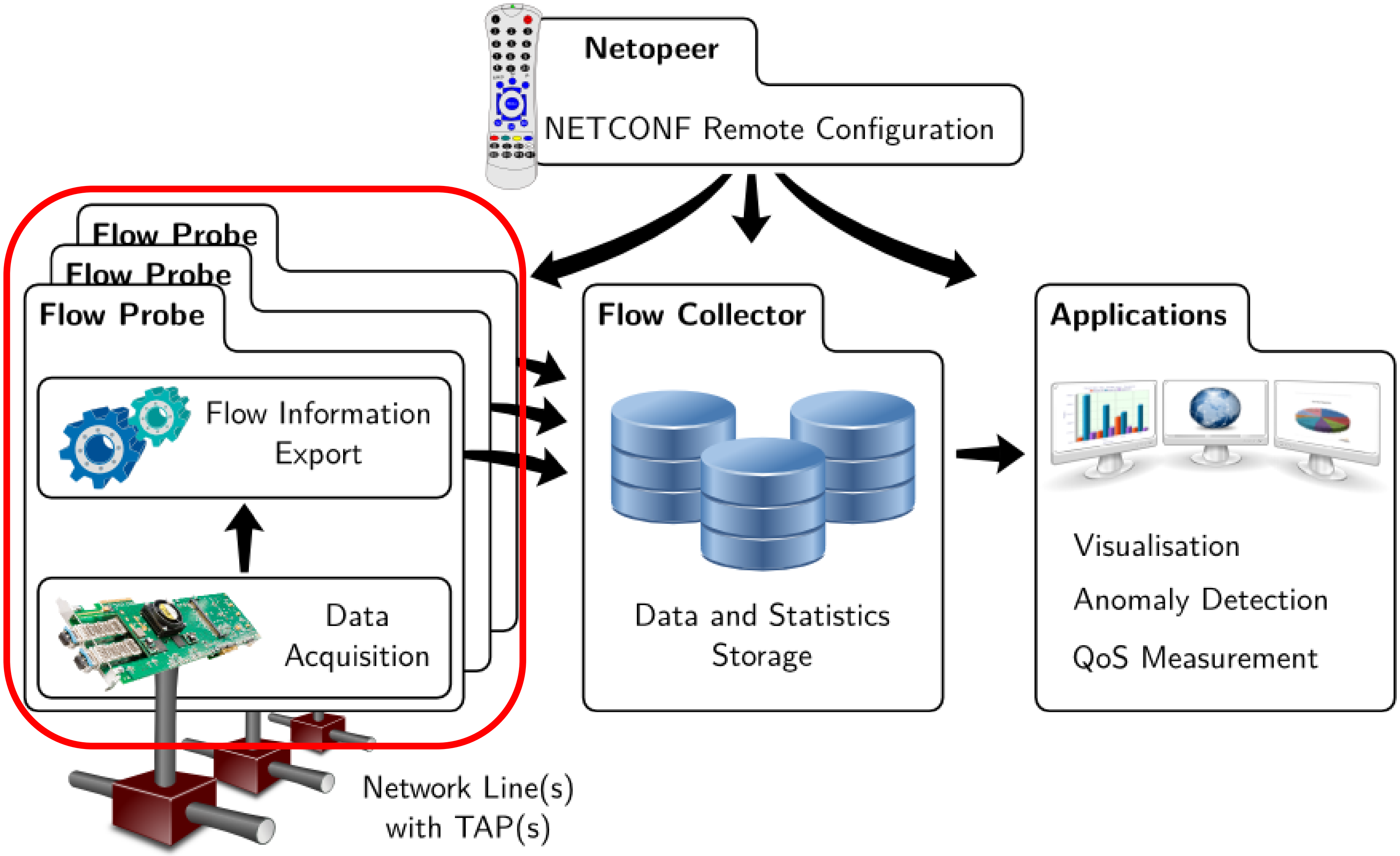
Timestamps
Number of Packets
Sum of Bytes
TCP Flags, ...

```
Flow start      Duration  Proto   Src IP Addr:Port            Dst IP Addr:Port      Flags   Packets   Bytes
09:41:21.763    0.101     TCP     172.16.96.48:15094    ->    209.85.135.147:80     .AP.SF        4     715
09:41:21.893    0.031     TCP     209.85.135.147:80     ->    172.16.96.48:15094    .AP.SF        4    1594
```

Research scope

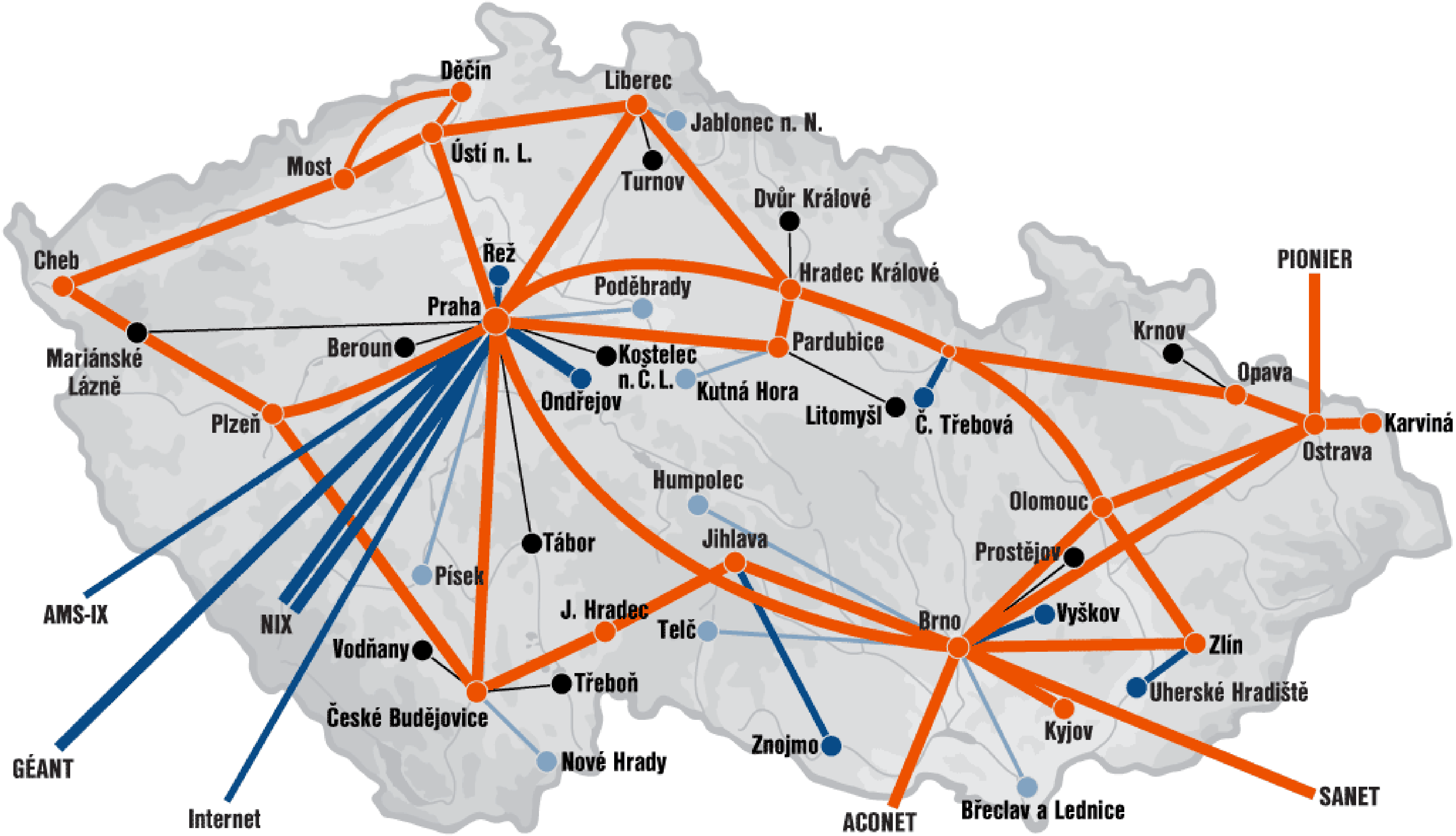


Research scope



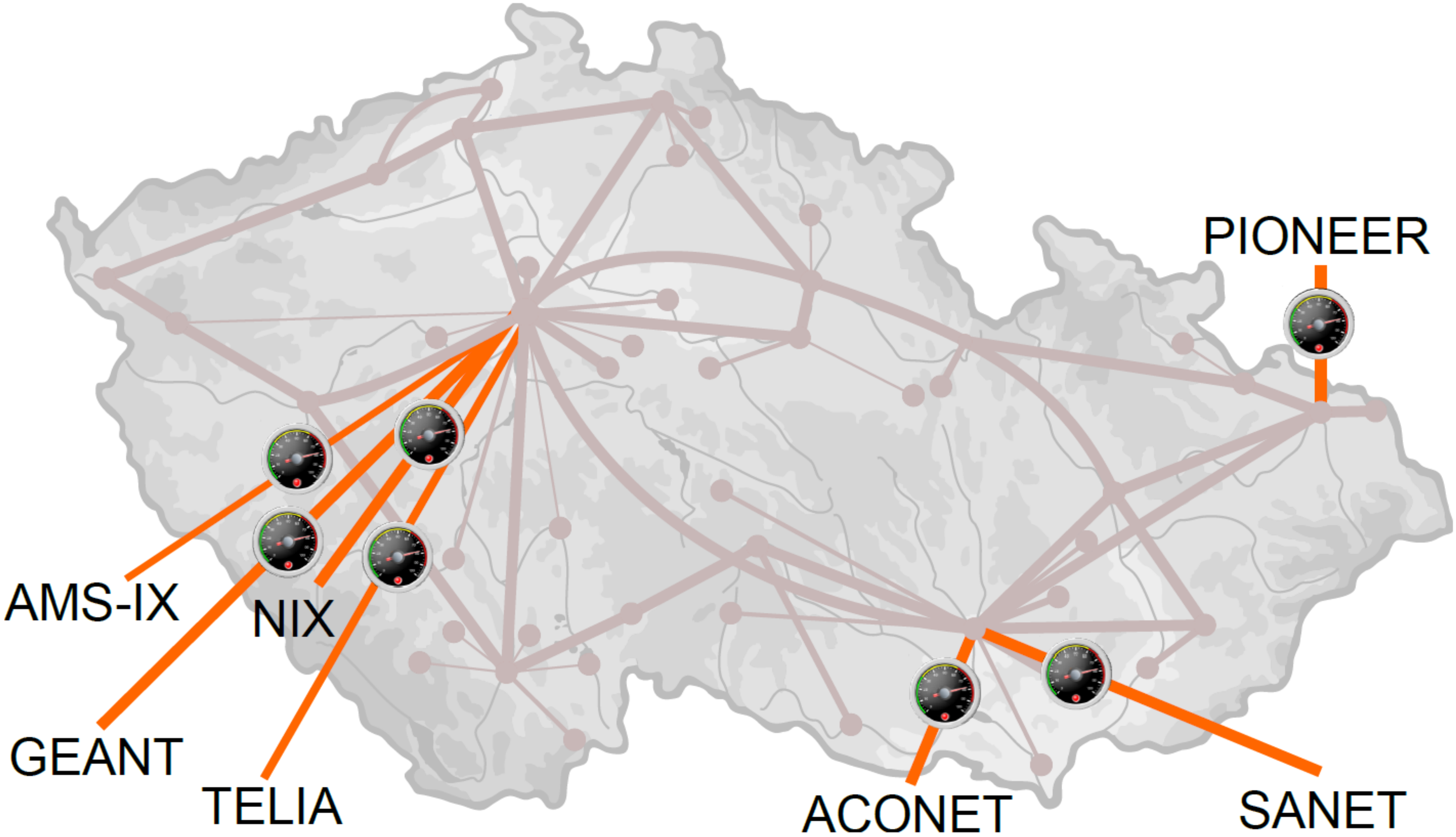
Monitoring testbed

- Czech NREN CESNET2 with over 400,000 connected users

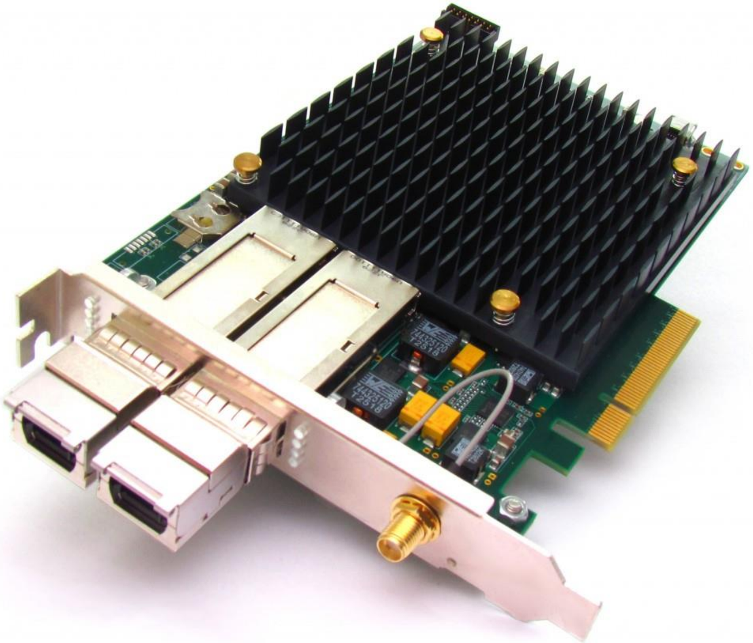


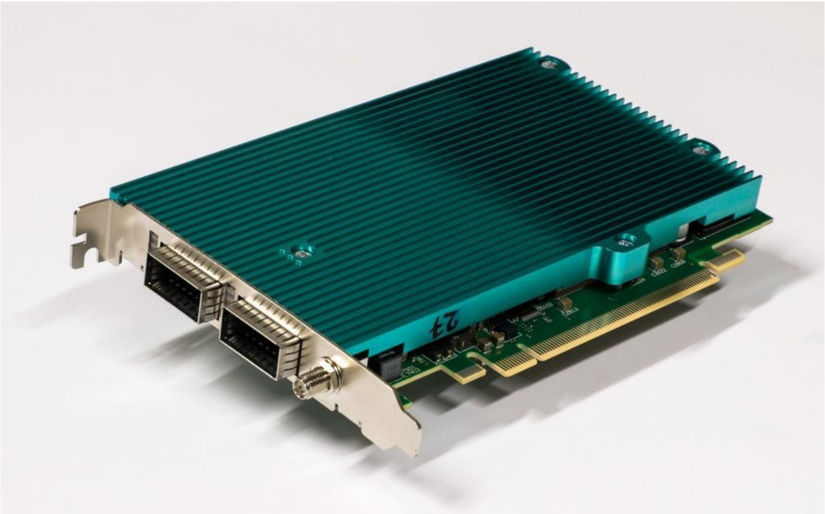
Monitoring testbed

- 7 metering points guarding the perimeter @ **40/100 Gbps**



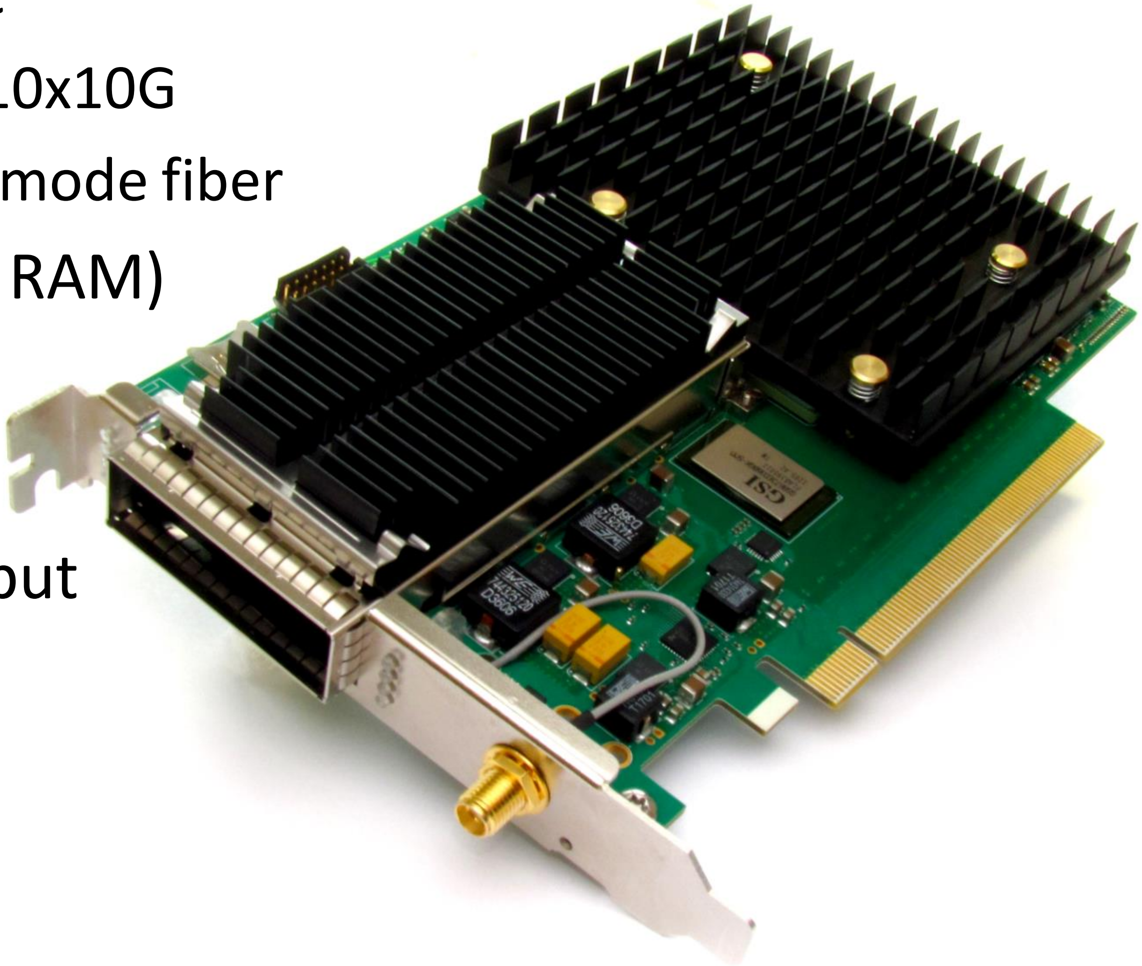
Acceleration cards





Acceleration cards

- ***Virtex7 H580T FPGA***
- CFP2 transciever cage
  - 100GE as 4x25G or 10x10G
  - singlemode or multimode fiber
- PCIe x16 (100Gbps to RAM)
- 3x QDRIIIe (3x72Mb)
- 8x DDR3 (8x4Gb)
- precise timestamp input
- Intel DPDK support



Monitoring probe approach

- Standard:
  - card operates as standard NIC (capturing packets)
  - software processing of the whole network traffic
- Accelerated:
  - card capable of accelerated traffic preprocessing
  - software performs only advanced/specific processing
  - unique concept of ***Software Defined Monitoring***

Software Defined Monitoring

- **What is it?**
  - our new approach to hardware acceleration of flow based high-speed network monitoring
  - brings hardware accelerated, application controlled and informed reduction of traffic load (processing offload)

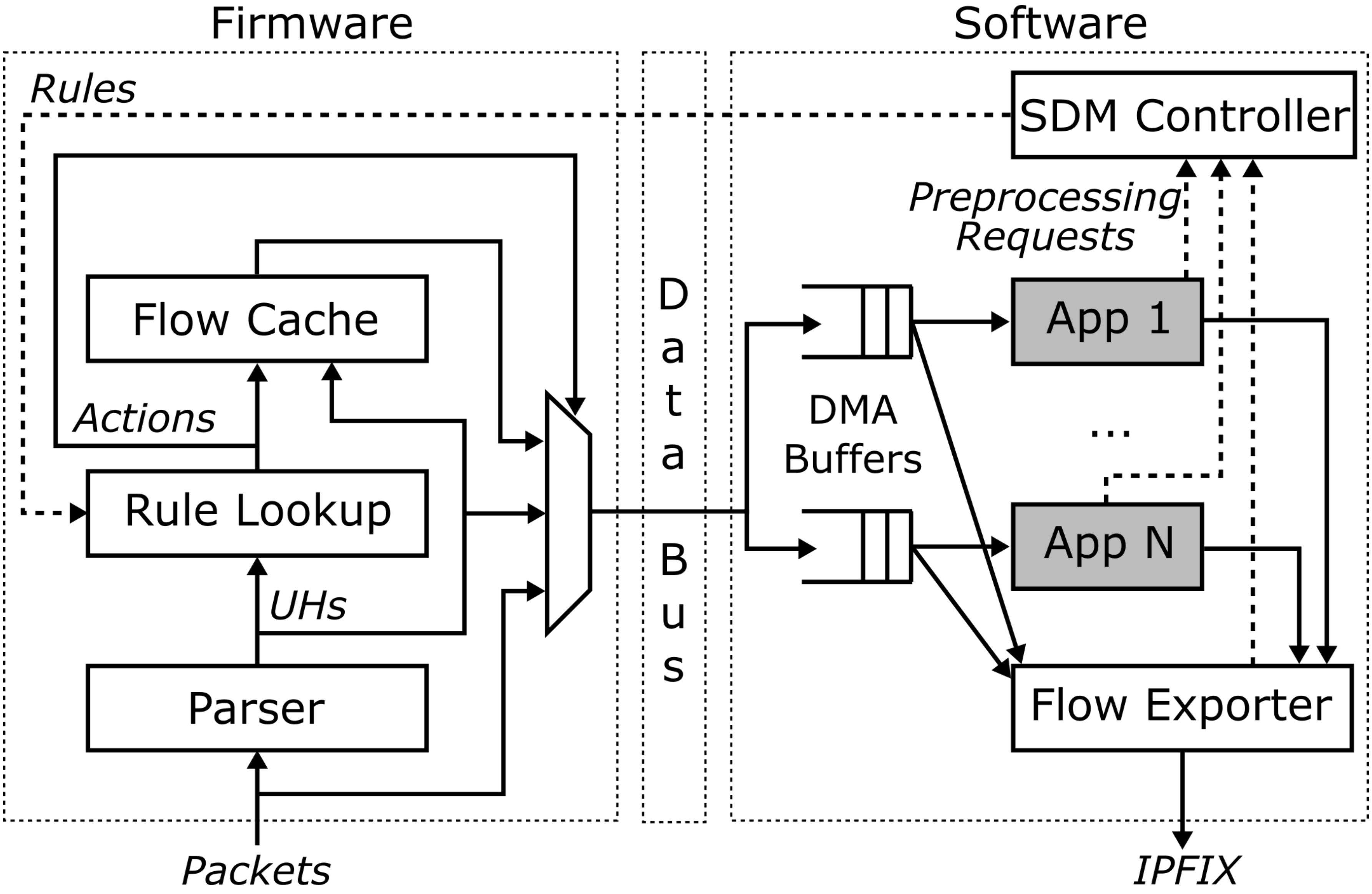
- **What does it do?**
  - **Hardware** provides various methods of packet preprocessing and aggregation – **The Muscles**
  - **Software** directly controls the actual usage of preprocessing on flow basis – **The Controller**
  - **User applications** request preprocessing acceleration and perform advanced monitoring tasks – **The Intelligence**

SDM preprocessing

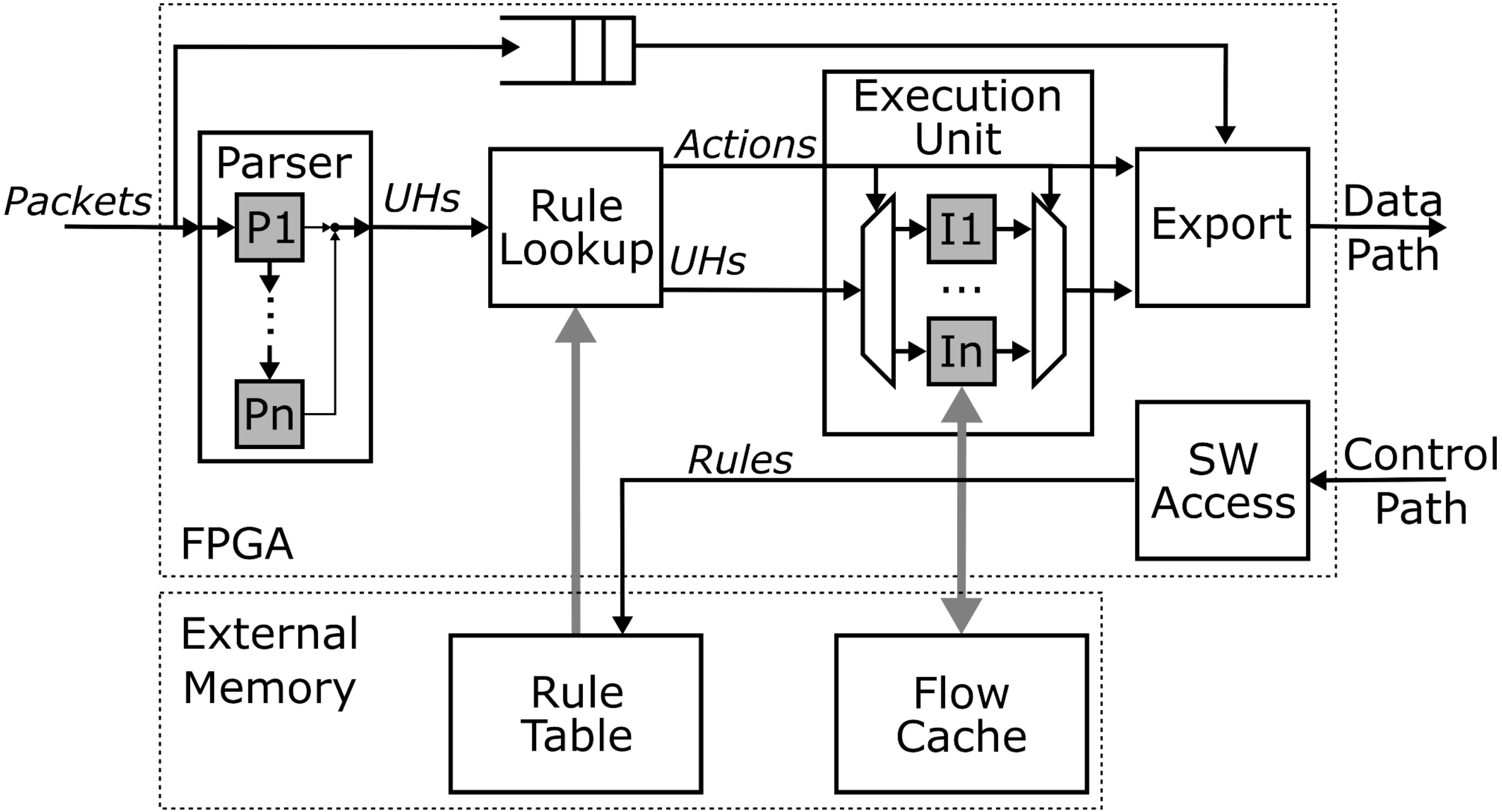
- controlled on the fly by rules from software applications

- four basic levels of packet preprocessing methods:
  - **Packet** – preserve the whole frame (with payload)
  - **Header** – preserve only important information about the frame
  - **Aggregate** – update a flow record in HW memory, send only aggregated information from multiple frames into SW
  - **Drop** – simply ignore the whole frame

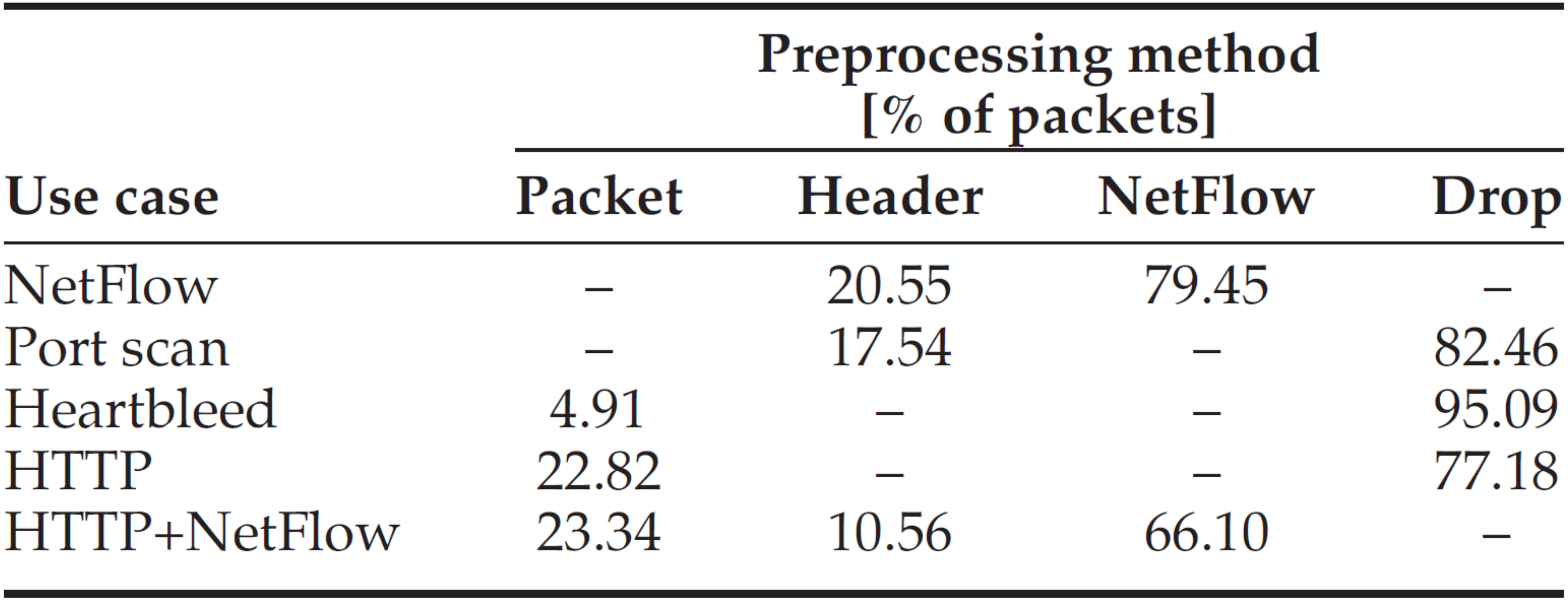
SDM conceptual architecture



SDM firmware architecture

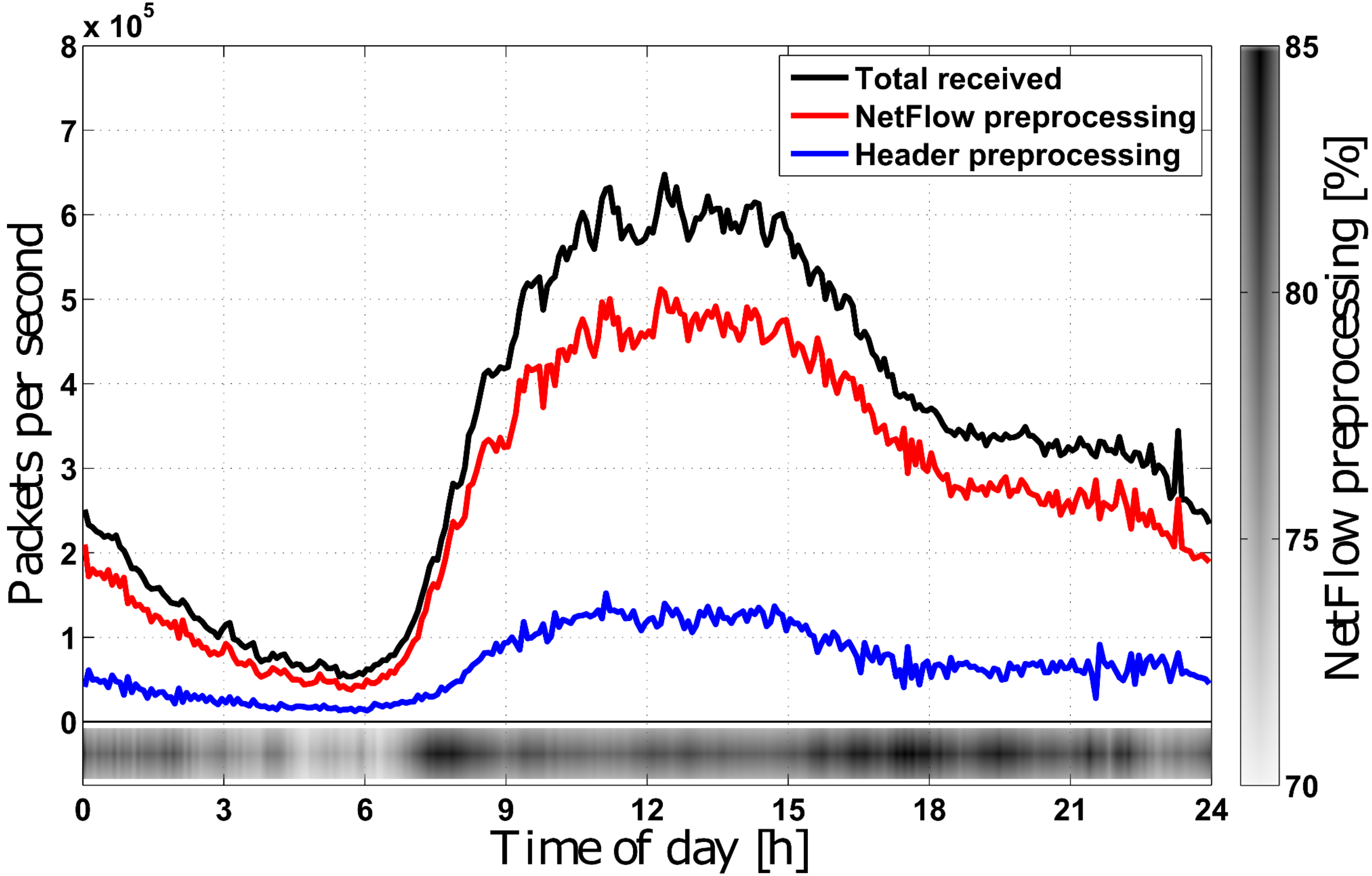


SDM results

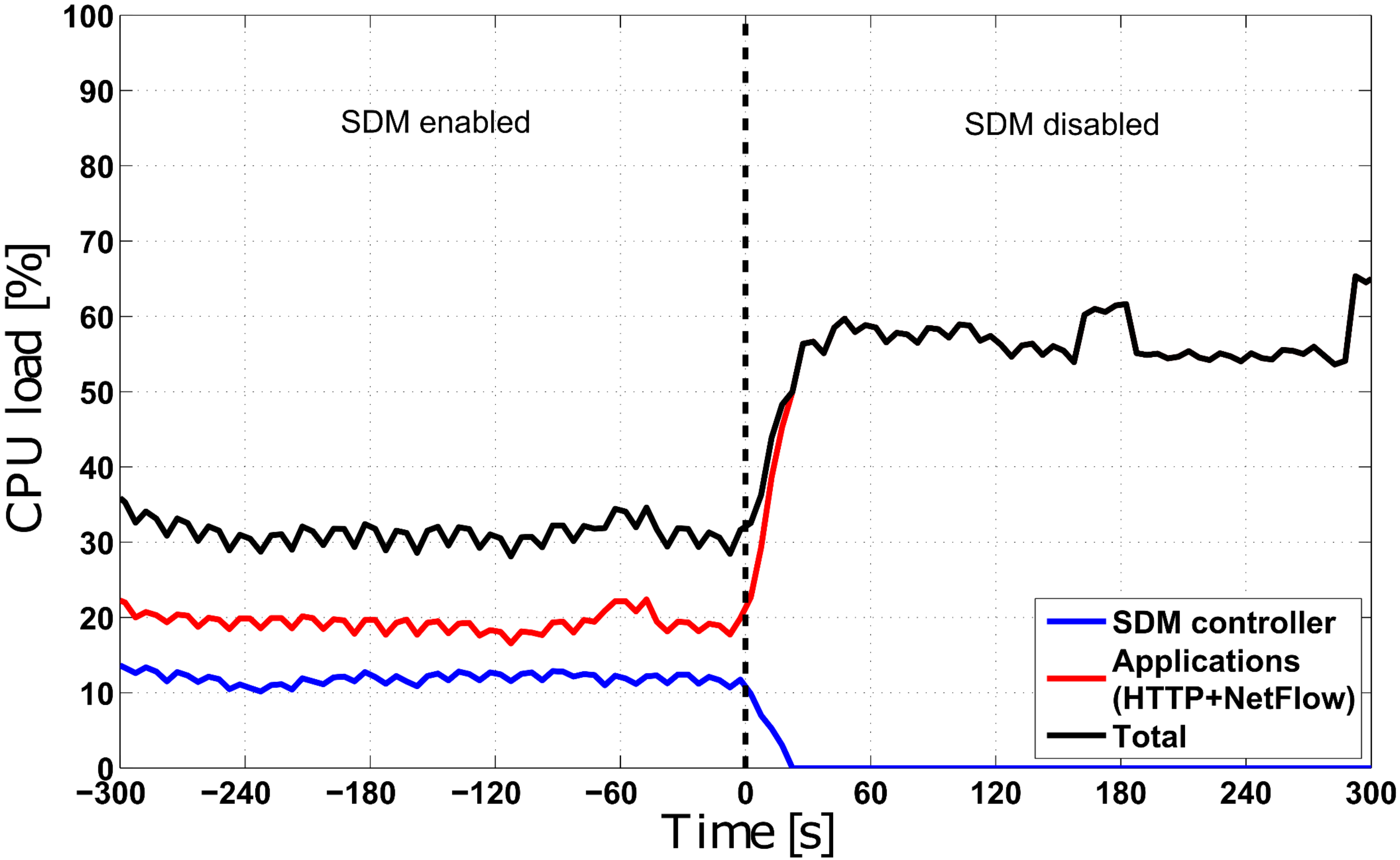


	Preprocessing method [% of packets]			
Use case	**Packet**	**Header**	**NetFlow**	**Drop**
NetFlow	–	20.55	79.45	–
Port scan	–	17.54	–	82.46
Heartbleed	4.91	–	–	95.09
HTTP	22.82	–	–	77.18
HTTP+NetFlow	23.34	10.56	66.10	–

SDM results – basic flows



SDM results – L7 processing



Summary

- powerful 3-sided research cooperation
  - research drive, real network deployment, industry feedback
- whole family of unique hardware accelerated Ethernet cards
  - 10 Gbps, 40 Gbps and various 100 Gbps ports
  - preparing for 400 Gbps Ethernet standard
- novel acceleration concept of SDM
  - noticeable reduction of traffic volume for applications (5-times)
  - can accelerate L7 processing and deep packet inspection
  - flexible usage thanks to intelligence in software applications

Thank you for your attention !

More info:

- *https://www.liberouter.org/*
- *ikekely@fit.vutbr.cz*
- *kekely@cesnet.cz*