Software Defined Monitoring: The New Norm for Network Monitoring

(IETF 87 – Berlin, Germany)

Lukáš Kekely, Viktor Puš
(kekely,pus@cesnet.cz)

CESNET

30. 6. 2013

Motivation

- advances in the network bandwidth (40 Gb/s and 100 Gb/s)
- monitoring and security cannot fall behind

⇒ **high throughtput** of traffic processing is imperative

- a lot different network protocols
- predicted end of network ossification

⇒ the solution must be very **flexible**

- insufficient support of application layer protocol processing
- HW processing is difficult vs. SW processing is slow

⇒ support **advanced (deeper) inspection** of traffic

Motivation

- advances in the network bandwidth (40 Gb/s and 100 Gb/s)
- monitoring and security cannot fall behind

⇒ **high throughtput** of traffic processing is imperative

- a lot different network protocols
- predicted end of network ossification

⇒ the solution must be very **flexible**

- insufficient support of application layer protocol processing
- HW processing is difficult vs. SW processing is slow

⇒ support **advanced (deeper) inspection** of traffic

Flexible application protocol analysis on high-speeds!

Software Defined Monitoring

> *What is it?*

Software Defined Monitoring

> *What is it?*

- New model (paradigm) of flow monitoring acceleration
- Takes advantage of hardware accelerated, application controlled reduction and distribution of network traffic
- Inspired by some ideas of Software Defined Networking

Software Defined Monitoring

> *What is it?*

- New model (paradigm) of flow monitoring acceleration
- Takes advantage of hardware accelerated, application controlled reduction and distribution of network traffic
- Inspired by some ideas of Software Defined Networking

> *What is it doing?*

Software Defined Monitoring

> *What is it?*

- New model (paradigm) of flow monitoring acceleration
- Takes advantage of hardware accelerated, application controlled reduction and distribution of network traffic
- Inspired by some ideas of Software Defined Networking

> *What is it doing?*

- **Hardware** provides various methods of packet preprocessing – **The Muscles**
- **Software** controls the usage of preprocessing on flow basis – **The Controller**
- **User applications** request the HW acceleration and perform advanced monitoring tasks – **The Intelligence**

Software Defined Monitoring

> *What is it?*

- New model (paradigm) of flow monitoring acceleration
- Takes advantage of hardware accelerated, application controlled reduction and distribution of network traffic
- Inspired by some ideas of Software Defined Networking

> *What is it doing?*

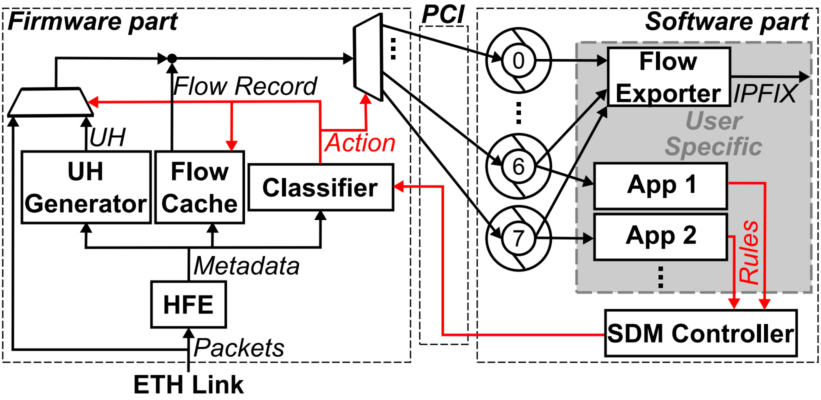
- **Hardware** provides various methods of packet preprocessing – **The Muscles**
- **Software** controls the usage of preprocessing on flow basis – **The Controller**
- **User applications** request the HW acceleration and perform advanced monitoring tasks – **The Intelligence**

Applications can adjust acceleration of traffic processing according to their actual needs!

SDM Functionality

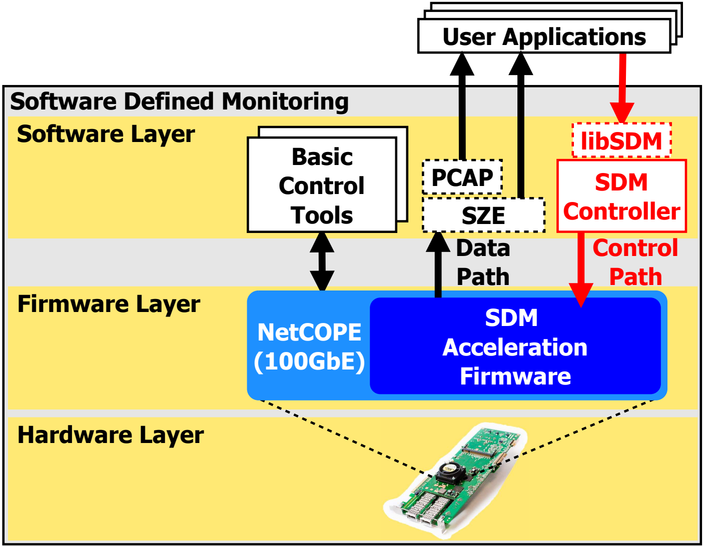
- Initial packets of unknown (new) flows are sent into SW
  - configurable implicit preprocessing method
- SW applications can change HW preprocessing of the following packets
  - **Interesting** – whole packets into SW
  - **Bulk** – header extraction, trimming or NetFlow in HW
  - **Uninteresting** – dropped directly in HW
- Configurable division of traffic into DMA channels
  - division preserves network flows
  - applications can select the channels to monitor

Logical Scheme of SDM

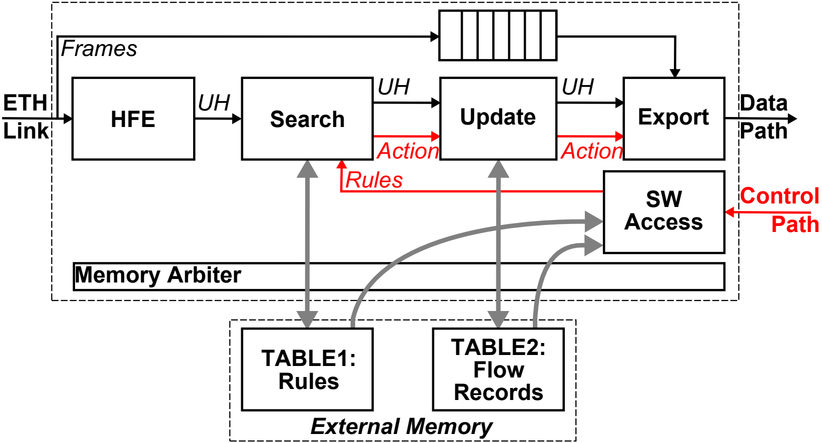


- visible software control feedback (red)
- firmware control realized using simple flow rules

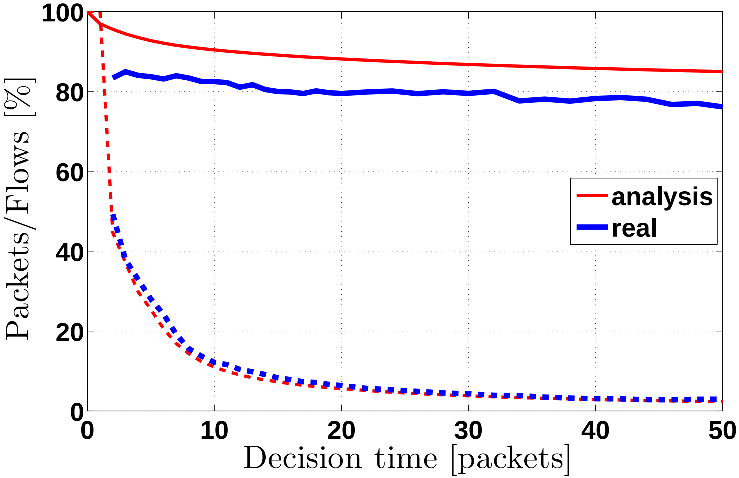
Layered Scheme of SDM



Firmware Implementation Scheme

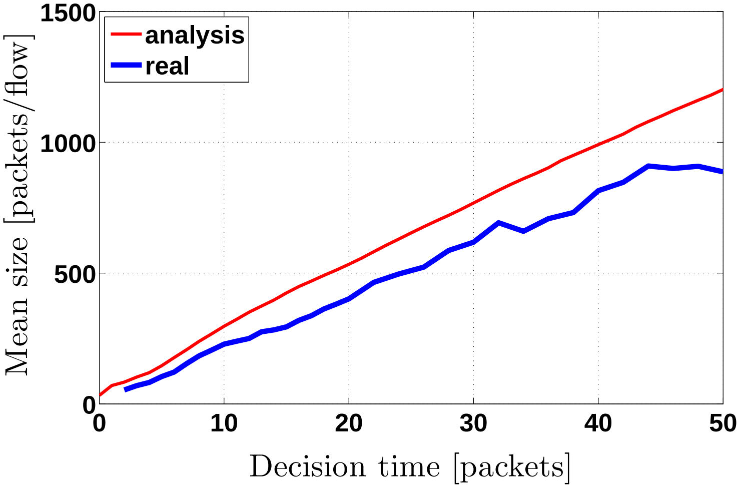


Offloadable Portion of Traffic (1)



- Portions of packets and flows offloadable into HW as function of the number of interesting initial packets

Offloadable Portion of Traffic (2)



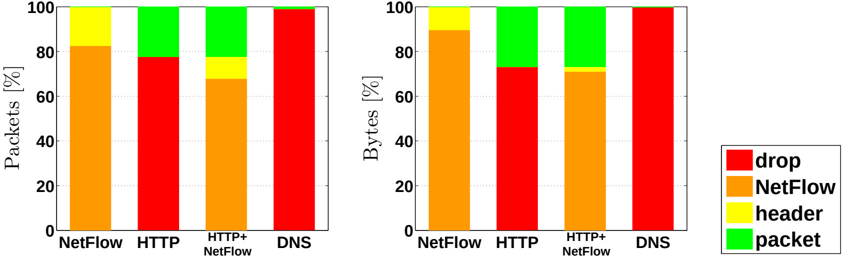
- Mean number of packets offloaded by one created rule as relation of the number of interesting initial packets

Realistic Use Cases (1)

We tested SDM performance on real network in 4 use cases:

- Standard **NetFlow** monitoring
- Analysis of application protocol **HTTP**
- Analysis of **HTTP** together with standard **NetFlow**
- Analysis of application protocol **DNS**

Realistic Use Cases (2)



- Portions of all incoming packets and bytes preprocessed in the hardware by particular method

Realistic Use Cases (3)

- **NetFlow**:
  - SW load is only $\frac{1}{5}$ **of packets** and $\frac{1}{100}$ **of bytes**
  - rules for $\frac{1}{10}$ **of flows** must be created
- **HTTP analysis**:
  - SW load is only $\frac{1}{4}$ **of packets** and $\frac{1}{4}$ **of bytes**
  - rules for $\frac{1}{20}$ **of flows** must be created
- **HTTP analysis and NetFlow**:
  - SW load is only $\frac{1}{3}$ **of packets** and $\frac{1}{4}$ **of bytes**
  - rules for $\frac{1}{12}$ **of flows** must be created
- **DNS analysis**:
  - SW load is only $\frac{1}{125}$ **of packets** and $\frac{1}{500}$ **of bytes**
  - rules for flows are not needed

Conclusion

New concept of flow based network monitoring acceleration – **Sofware Defined Monitoring**:

- fully software controlled hardware accelerator
- flow based measurements at speeds over 100 Gbps
- easy deployment of new tasks without HW modifications
- helps to accelerate application level processing

To Summarize

> *What is Software Defined Monitoring?*

To Summarize

> *What is Software Defined Monitoring?*

SDM is a new high-speed flexible acceleration platform which supports easy deployment of advanced monitoring and security applications in networks!

To Summarize

> *What is Software Defined Monitoring?*

SDM is a new high-speed flexible acceleration platform which supports easy deployment of advanced monitoring and security applications in networks!

> *Why should I use Software Defined Monitoring?*

To Summarize

> *What is Software Defined Monitoring?*

SDM is a new high-speed flexible acceleration platform which supports easy deployment of advanced monitoring and security applications in networks!

> *Why should I use Software Defined Monitoring?*

SDM enables high speed and high quality flow measurement of network traffic at the application layer!

Thank you for your attention.