Software Defined Monitoring: The New Norm for Network Monitoring
(IETF 87 – Berlin, Germany)

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

30. 6. 2013
Motivation

- advances in the network bandwidth (40 Gb/s and 100 Gb/s)
- monitoring and security cannot fall behind
  ⇒ high throughput 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 throughput 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!
> 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!
> **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?**

- 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*
> **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!
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
visible software control feedback (red)
firmware control realized using simple flow rules
Firmware Implementation Scheme

Frames

HFE

Search

Update

Export

Data Path

Control Path

ETH Link

UH

UH

UH

Memory Arbiter

External Memory

TABLE1: Rules

TABLE2: Flow Records

SW Access

L. Kekely

Software Defined Monitoring

30. 6. 2013 7 / 15
Portions of packets and flows offloadable into HW as function of the number of interesting initial packets
Mean number of packets offloaded by one created rule as relation of the number of interesting initial packets.
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**
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
New concept of flow based network monitoring acceleration – **Software 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
> What is Software Defined Monitoring?
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!
> 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?
> 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.