Hardware Acceleration: An Essential Part of Cyber Security in High-Speed Networks

Jiří Novotný
novotny@ics.muni.cz

Pavel Čeleda
celeda@ics.muni.cz

Radek Krejčí
krejci@liberouter.org

DeepSec – In-Depth Security Conference 2010 – November 25, 2010, Vienna, Austria

Part I

Motivation

World Is Changing Quickly

World Is Changing Quickly

- Cyber security become to be **very important**.
- **Income** from cyber crime **is higher than from drugs**.

World Is Changing Quickly

- Cyber security become to be **very important**.
- **Income** from cyber crime **is higher than from drugs**.
- SPAM, phishing, social engineering, stealing of confidential information and many others.
- Botnet business (e.g. Chuck Norris botnet).

World Is Changing Quickly

- Cyber security become to be **very important**.
- **Income** from cyber crime **is higher than from drugs**.
- SPAM, phishing, social engineering, stealing of confidential information and many others.
- Botnet business (e.g. Chuck Norris botnet).
- DDoS attacks against Estonia and Georgia.

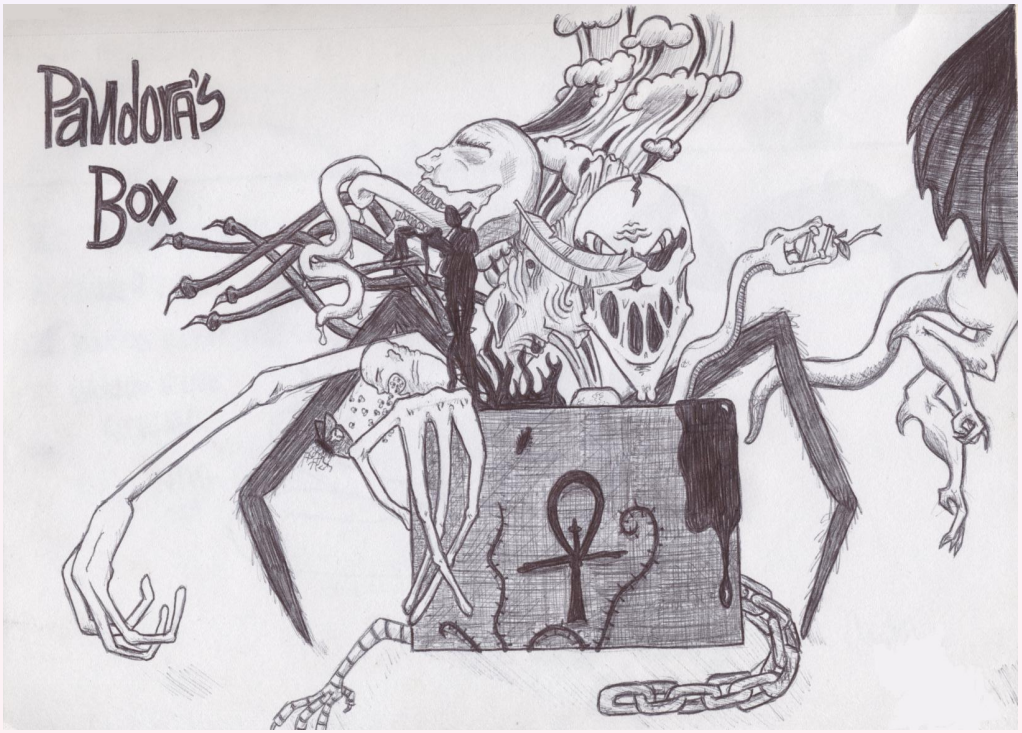
World Is Changing Quickly

- Cyber security become to be **very important**.
- **Income** from cyber crime **is higher than from drugs**.
- SPAM, phishing, social engineering, stealing of confidential information and many others.
- Botnet business (e.g. Chuck Norris botnet).
- DDoS attacks against Estonia and Georgia.

Internet is battlefield of today.

How Well Do You Know Your Network?

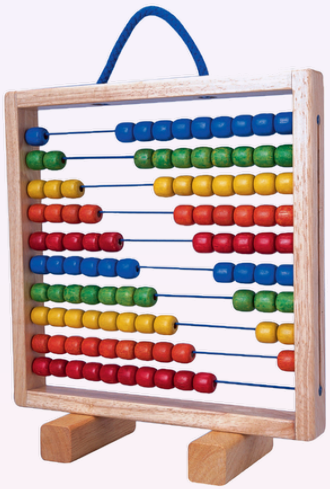
- Do you know **what is happening** on your network?
- Are you sure that your **network is secure**?
- Are you able to **detect** and **prove** network incidents?



Or does your network looks like Pandora's box?

Network Monitoring in Time

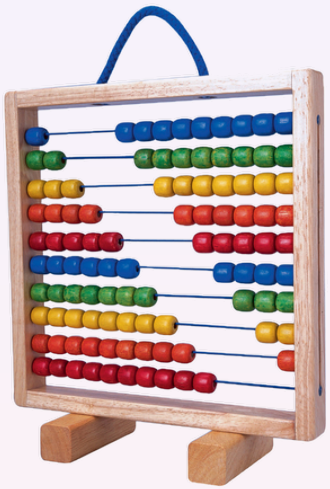
Originally



Basic functionality

Network Monitoring in Time

Originally



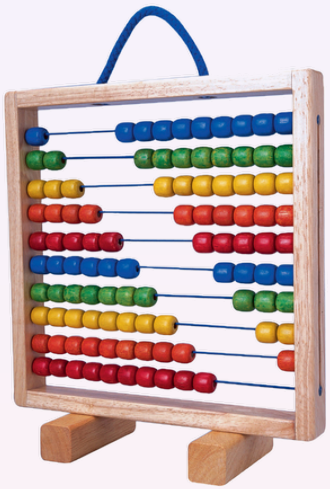
Basic functionality

Then

Incident handling
Network forensics

Network Monitoring in Time

Originally



Basic functionality

Then

Incident handling
Network forensics

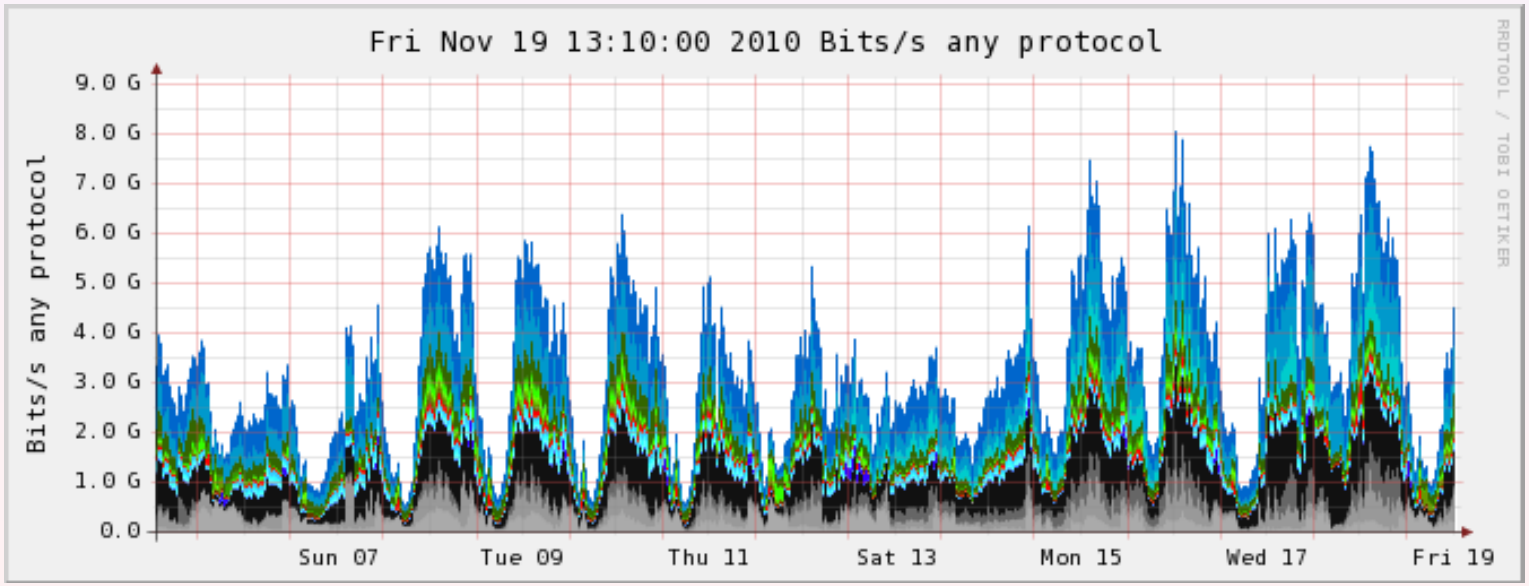
Now

Intrusion detection

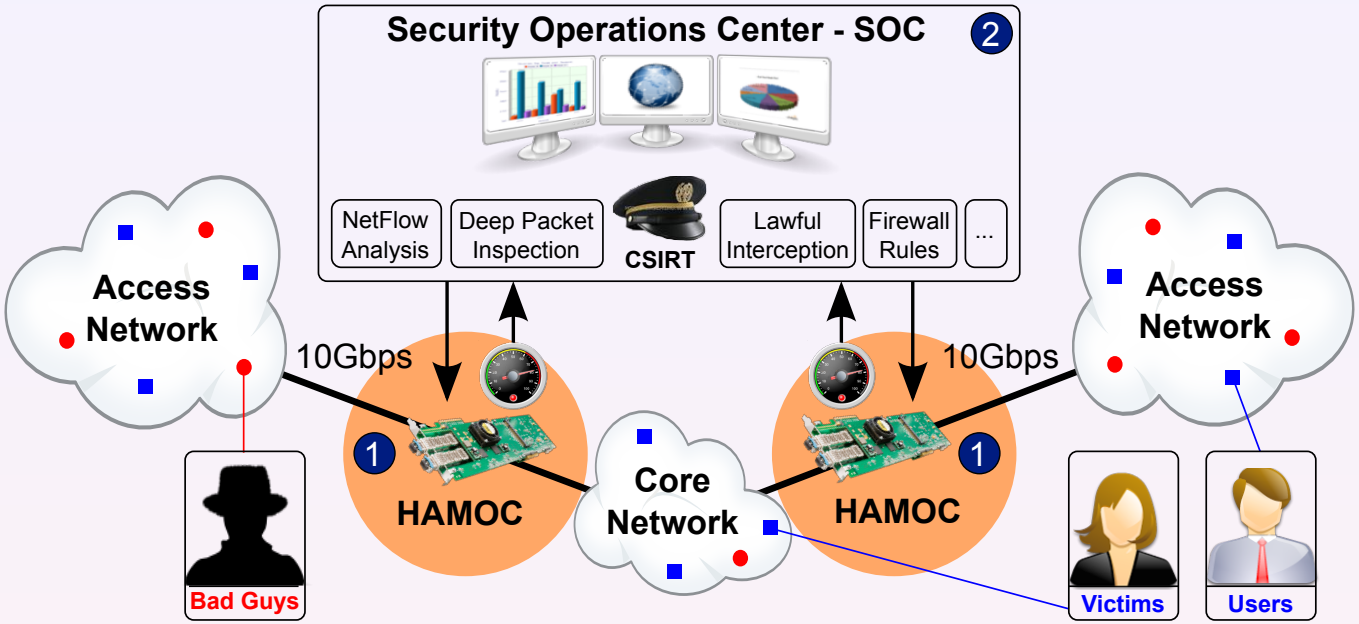
Present Computer Security

Main Issues

- **Huge amount of data** passing through network.
- Huge amount of monitoring data.
- Software-only monitoring solutions are not **fast enough**.
- Many of security tools are **too complex** for configuration.
- Hardware appliances are **not flexible enough**.
- Data from network devices have **no sufficient quality**.



Our Vision of the Network Security Monitoring System



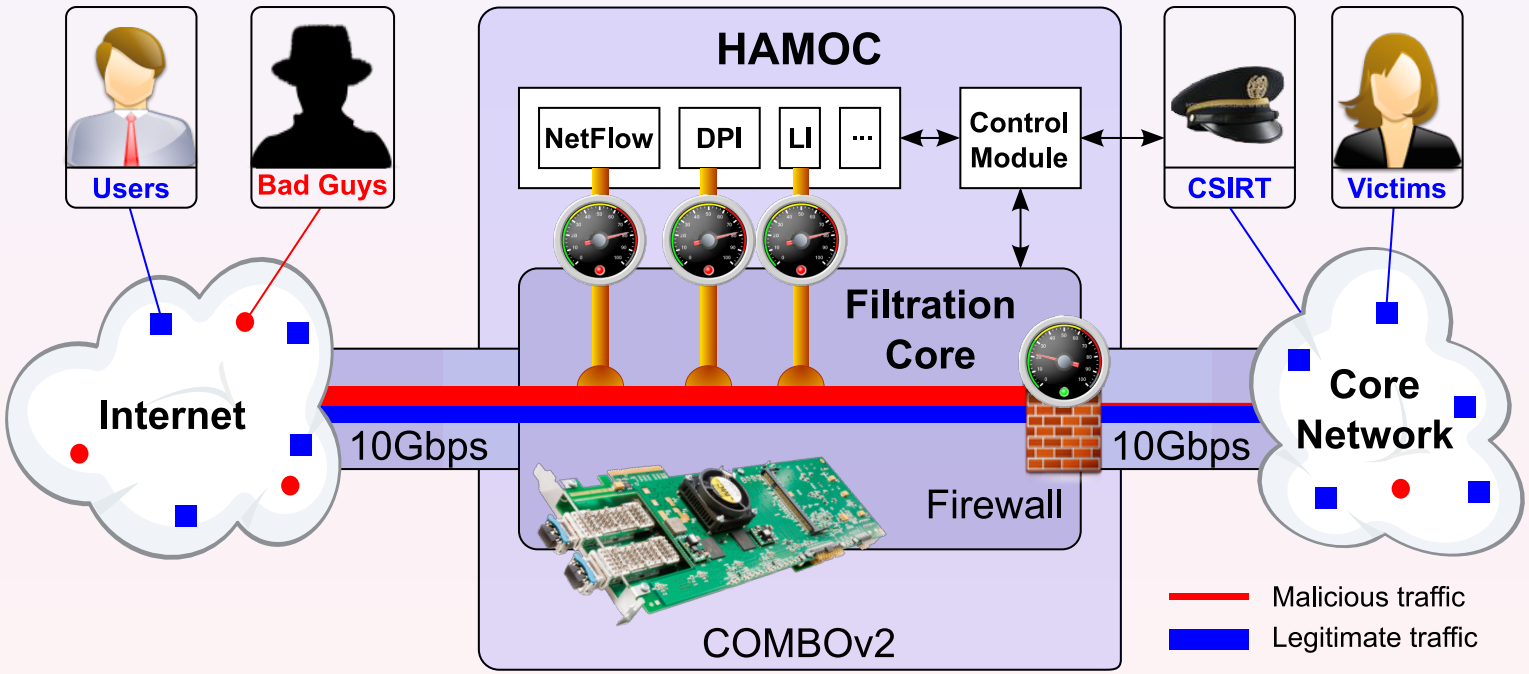
1. HAMOC
   - **High-speed acceleration** – COMBOv2 hardware accelerator.
   - **Flexibility** – Server PC box with monitoring software.
2. Security Operations Center.

Part II

Hardware Accelerated Monitoring Center (HAMOC)

HAMOC Goals

- Makes use of **hardware acceleration** more **user-friendly**.
- Set of third-party **tools tunned** to work with COMBOv2.
- **Use-cases** and **best practices** how to work with COMBOv2.



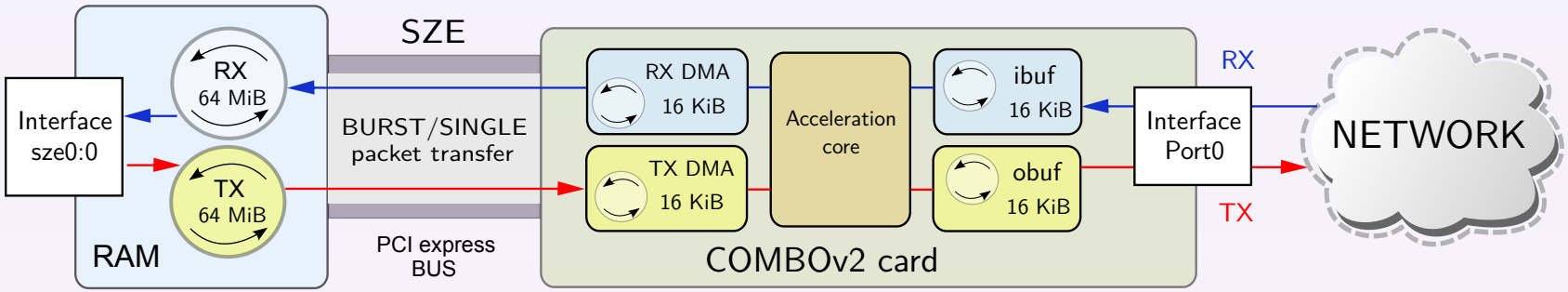
HAMOC Hardware – COMBOv2 Family

COMBOI-1G4 – 4x1 Gb/s

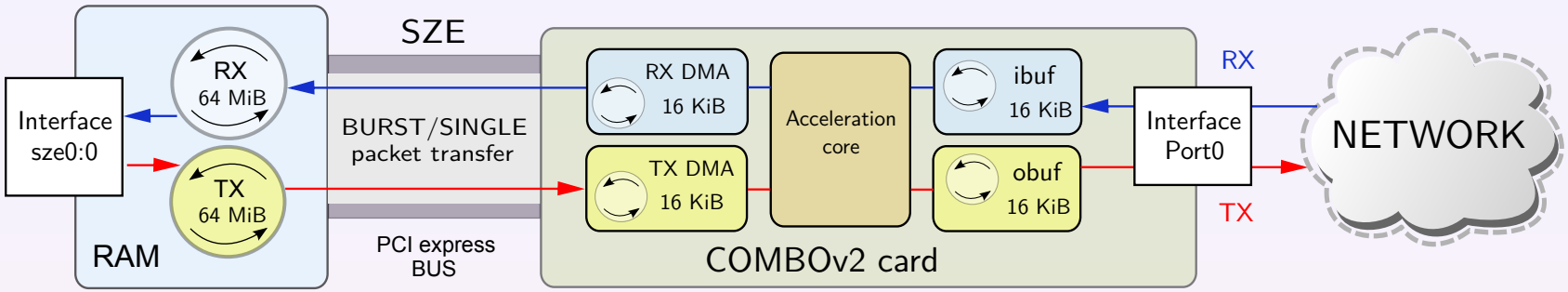
COMBOI-10G2 – 2x10 Gb/s

COMBOI-10G4TXT – 4x10 Gb/s

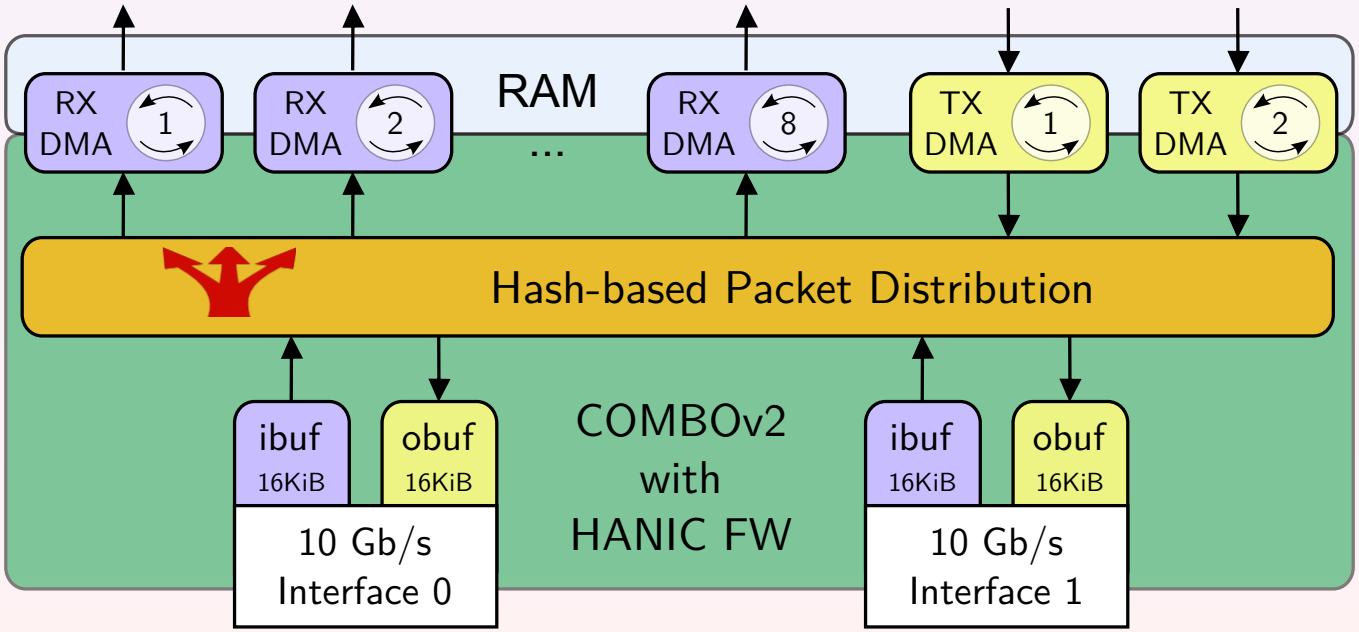
NetCOPE – SDK for the COMBO Hardware Accelerator



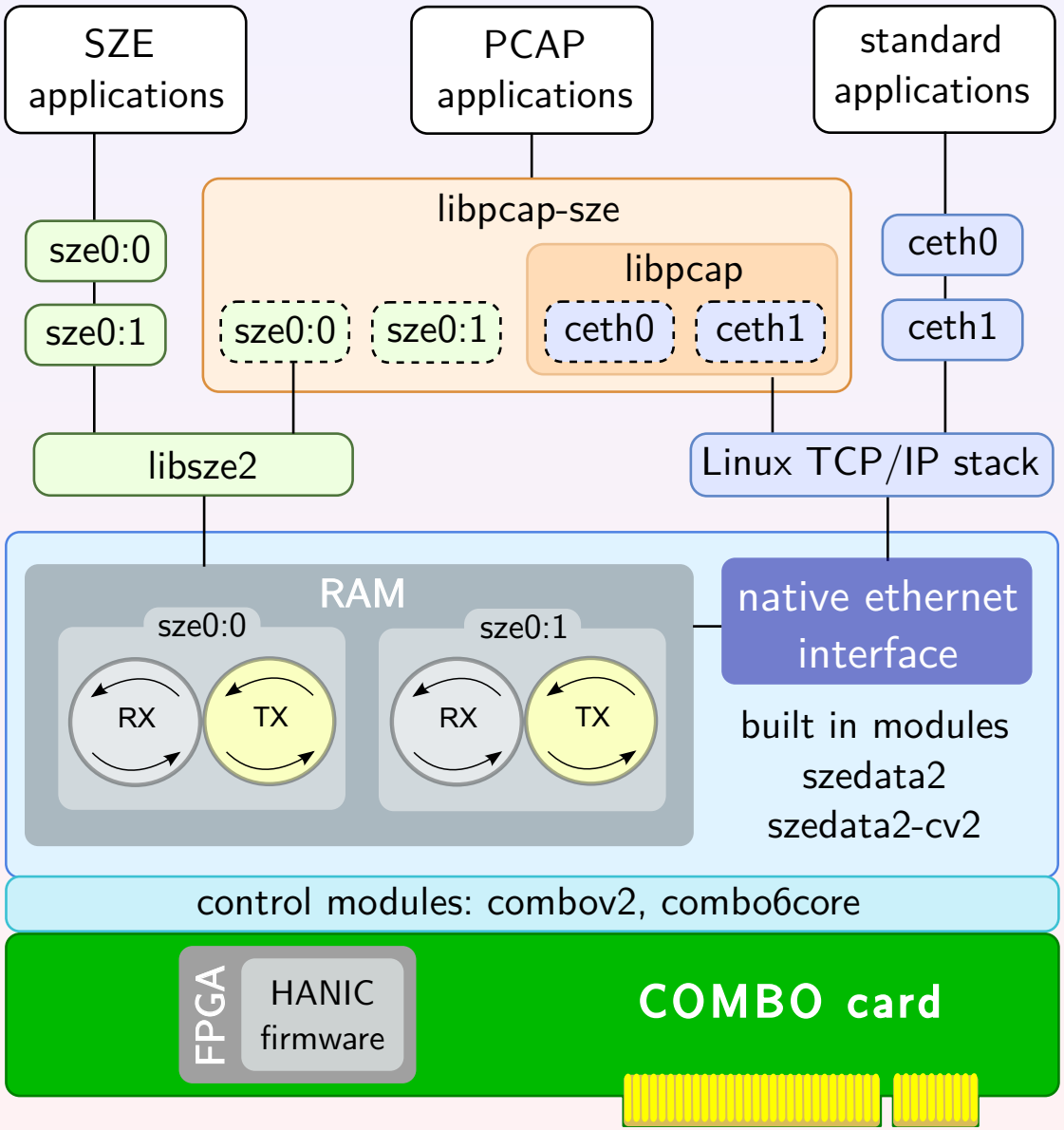
NetCOPE – SDK for the COMBO Hardware Accelerator



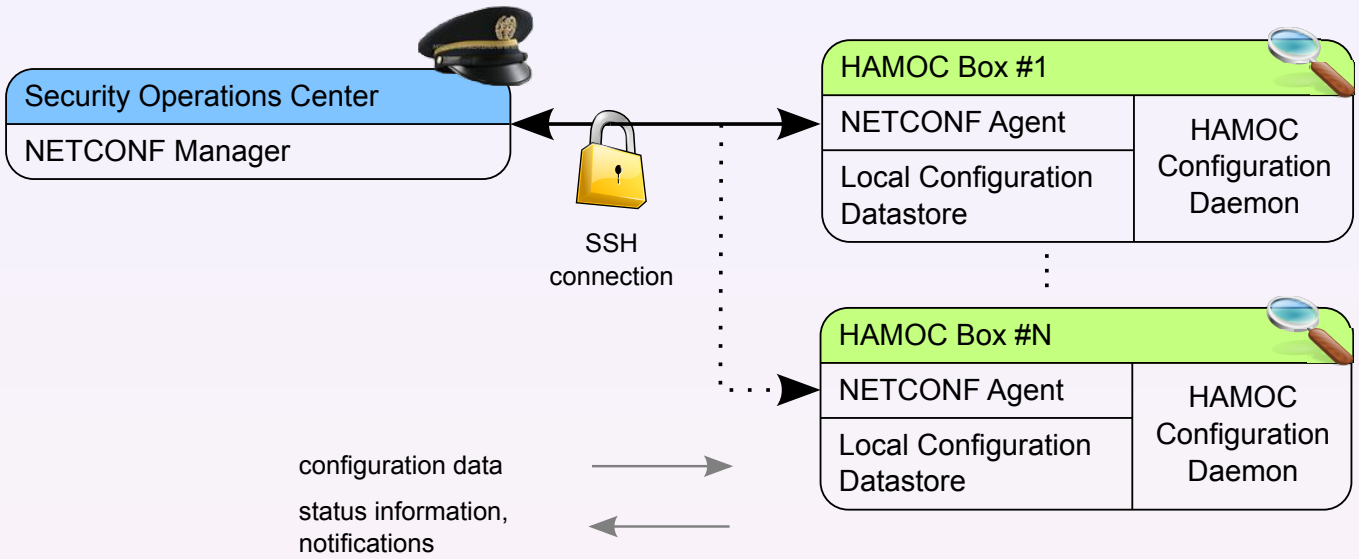
Hardware Accelerated NIC (HANIC) Firmware



Software Architecture



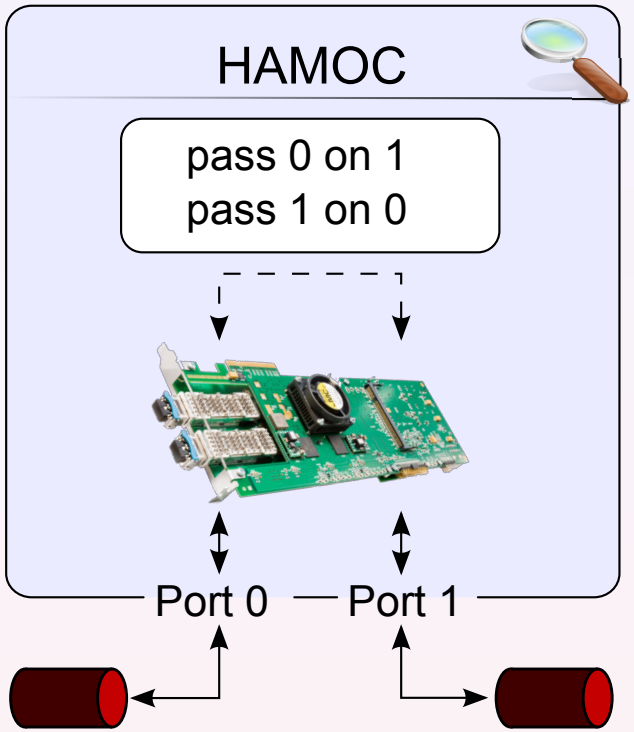
Remote Configuration



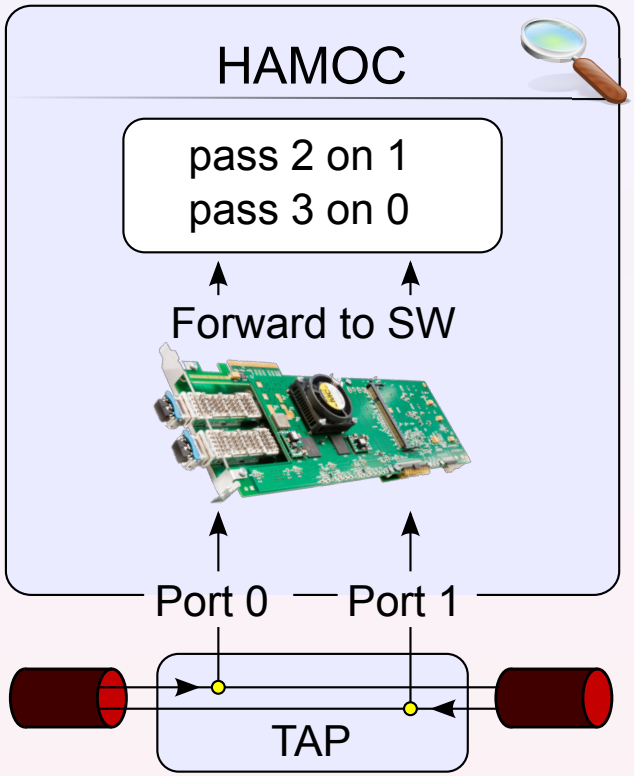
NETCONF Protocol

- **Secured** data **transport** over SSH (*Secure Shell*) version 2.
- **XML** data format.
- Event notifications capability.
- **Separated configuration** datastores:
  - startup, running, candidate.

Connection to Network

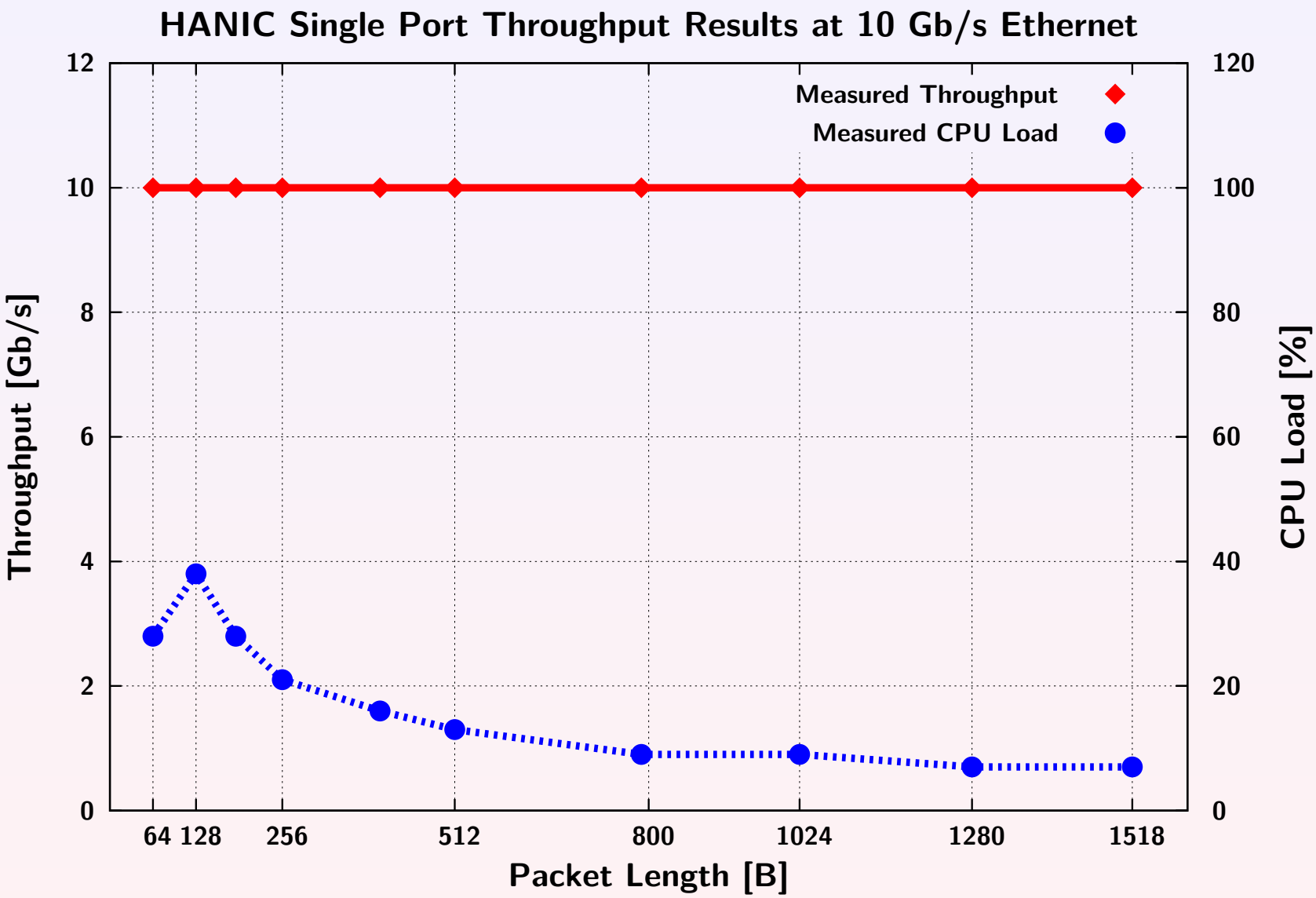


In-line Mode 10 Gb/s



TAP Mode 10 Gb/s

HAMOC – Test Results



HAMOC Summary

- Based on COMBOv2 **hardware accelerators**.
- Uses NetCOPE platform for **rapid firmware development**.
- Changing filtering rules **without packet loss**.
- Several API for applications (standard stack, **PCAP**, **SZE2**).
- Uses third party **well known applications** (e.g. Wireshark).
- Simple development of new applications.
- **Remote configuration** via NETCONF.

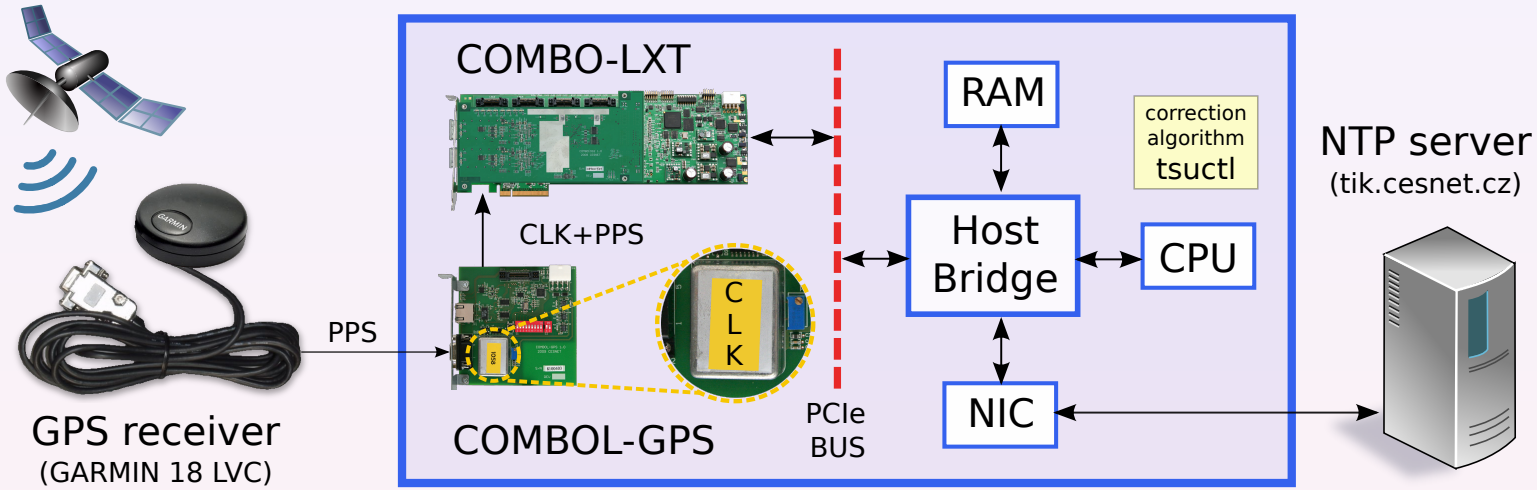
Part III

Use Cases – Deep Packet Inspection

Nanosecond Timestamps – I

Motivation

- COMBOv2 hardware supports **nanosecond timestamps**.



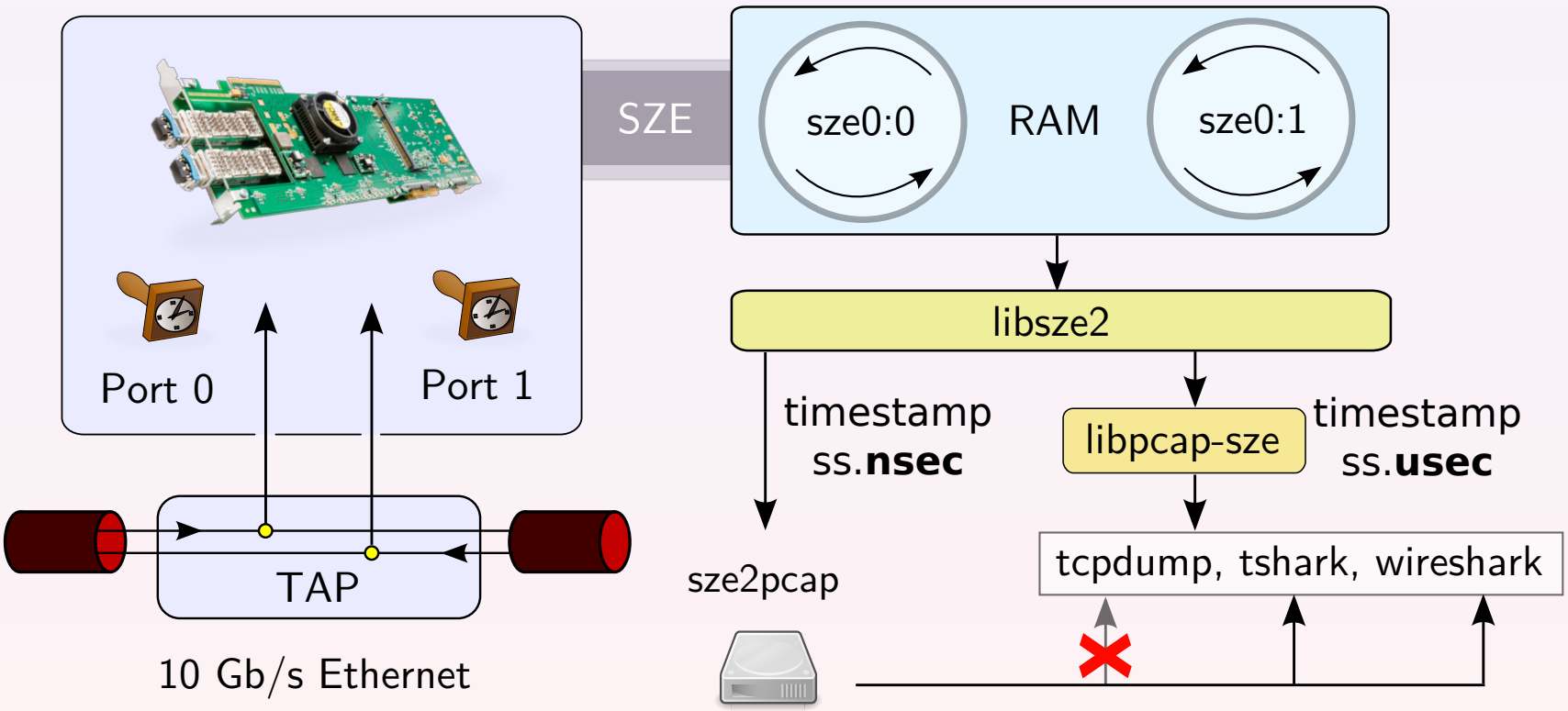
Problem

- libpcap library supports **microsecond** timestamps **only**.
- Wireshark supports **nanoseconds PCAP** file format.

Nanosecond Timestamps – II

Solution

- **sze2pcap** tool – writes network traffic to wireshark nanosecond PCAP format with **nanosecond precision**.



Nanosecond Timestamps – III

Usage

```
$ sze2pcap -c 1000 -i 0 -w /tmp/dump.pcap
$ wireshark /tmp/dump.pcap
```

No.	Time	Source	Destination
1	17:53:01.248256000	74.125.13.220	147.229.91.155
2	17:53:01.248258000	147.251.9.8	147.251.40.145
3	17:53:01.248263000	89.206.21.190	87.103.18.44
4	17:53:01.248263000	82.143.149.78	88.74.133.80
5	17:53:01.248263000	89.191.132.1	178.32.109.64
6	17:53:01.248265000	147.231.201.174	195.113.100.130
7	17:53:01.248269000	150.254.169.6	95.96.94.128
8	17:53:01.248270000	147.32.129.125	233.11.36.88

!! EQUAL

µs timestamps ←

Nanosecond Timestamps – III

Usage

```
$ sze2pcap -c 1000 -i 0 -w /tmp/dump.pcap
$ wireshark /tmp/dump.pcap
```

No.	Time	Source	Destination
1	17:53:01.248256000	74.125.13.220	147.229.91.155
2	17:53:01.248258000	147.251.9.8	147.251.40.145
3	17:53:01.248263000	89.206.21.190	87.103.18.44
4	17:53:01.248263000	82.143.149.78	88.74.133.80
5	17:53:01.248263000	89.191.132.1	178.32.109.64
6	17:53:01.248265000	147.231.201.174	195.113.100.130
7	17:53:01.248269000	150.254.169.6	95.96.94.128
8	17:53:01.248270000	147.32.129.125	233.11.36.88

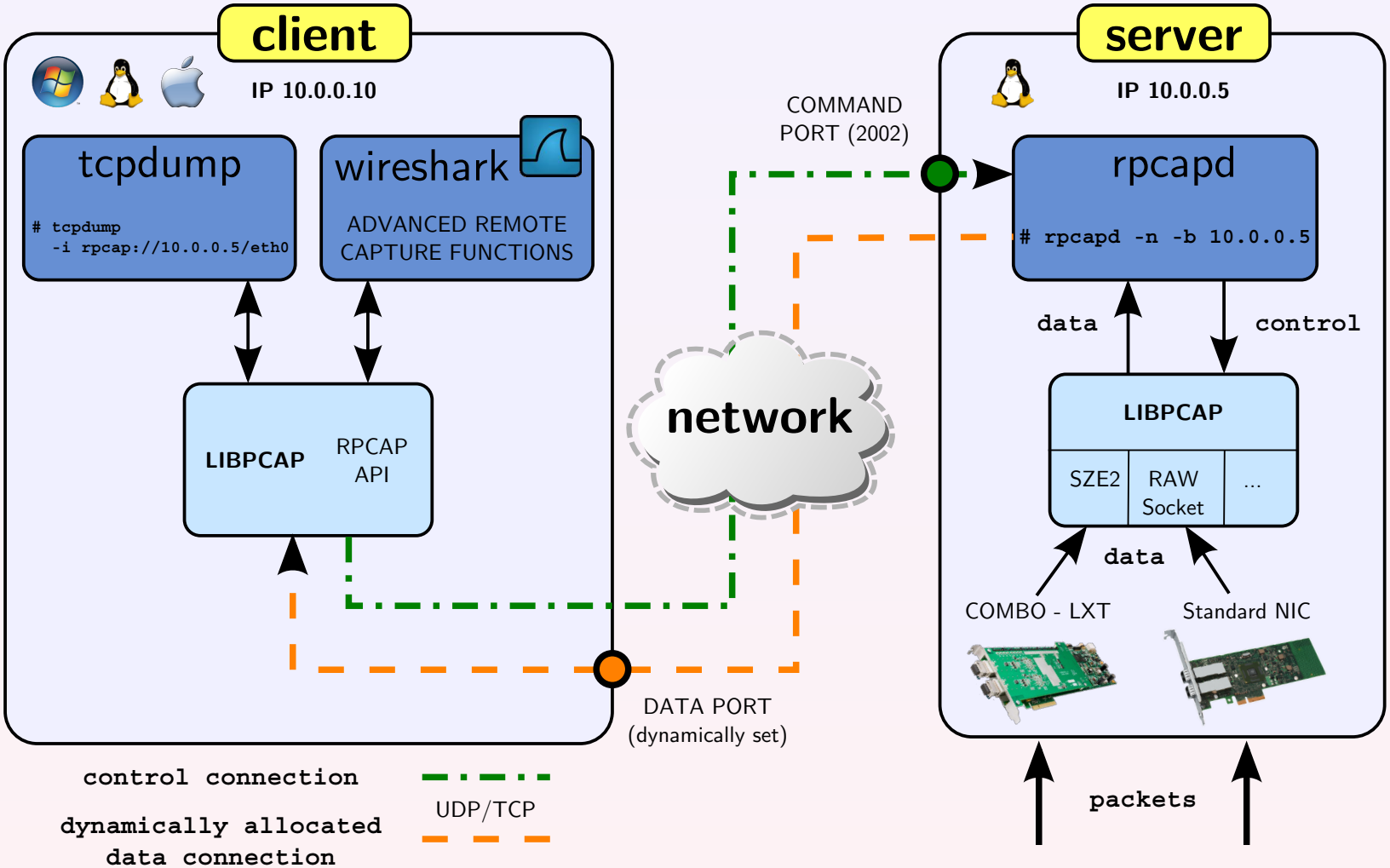
!! EQUAL

µs timestamps ←

No.	Time	Source	Destination
1	17:53:01.248256804	74.125.13.220	147.229.91.155
2	17:53:01.248258658	147.251.9.8	147.251.40.145
3	17:53:01.248263494	89.206.21.190	87.103.18.44
4	17:53:01.248263704	82.143.149.78	88.74.133.80
5	17:53:01.248263854	89.191.132.1	178.32.109.64
6	17:53:01.248265132	147.231.201.174	195.113.100.130
7	17:53:01.248269710	150.254.169.6	95.96.94.128
8	17:53:01.248270910	147.32.129.125	233.11.36.88

ns timestamps ←

Remote Packet Capture



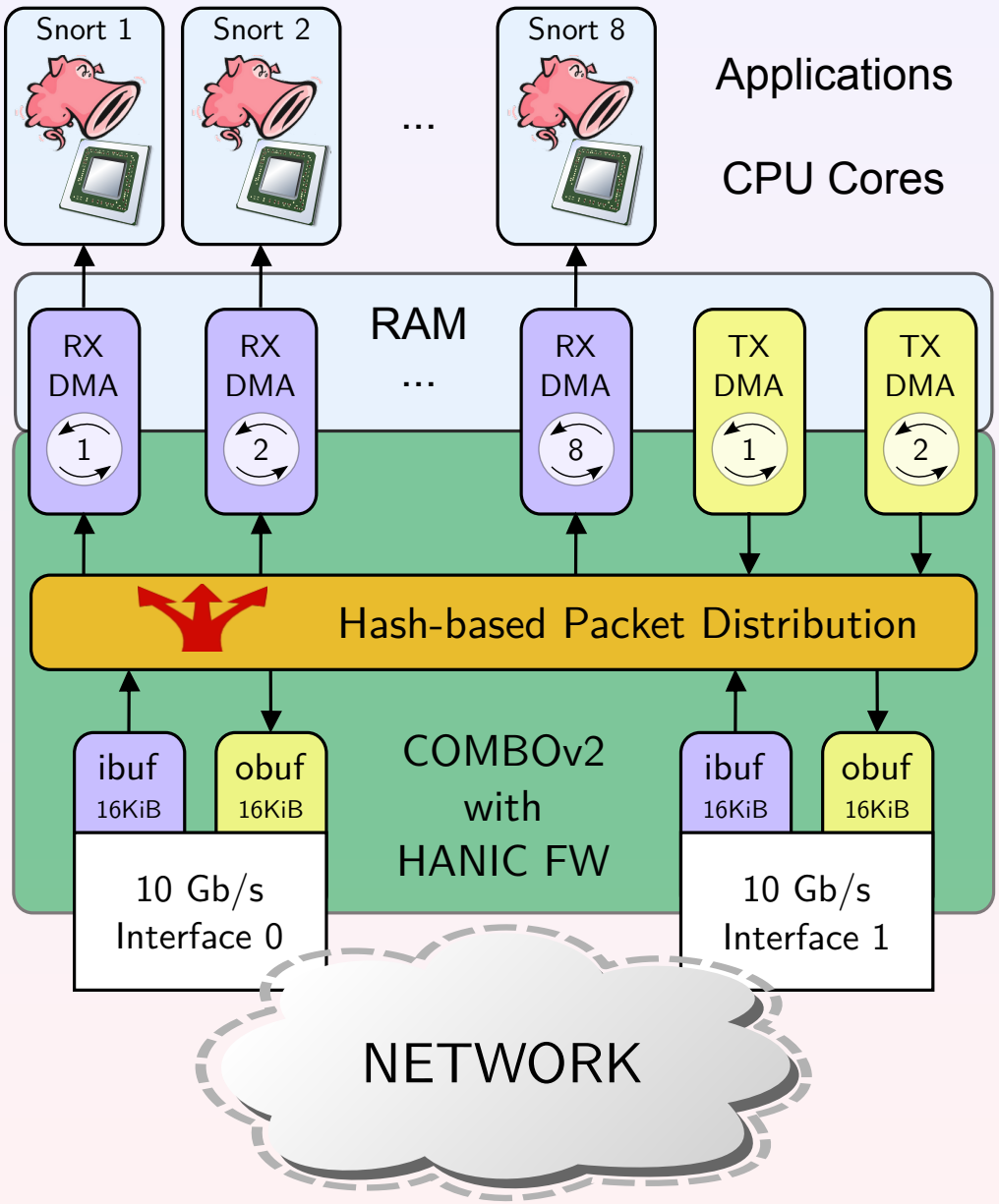
Use Case – VoIP Analyzer

- Captures control protocols (e.g. SIP, H.323 and H.248) and transport protocols (e.g. RTP, RTCP and SRTP).
- Uses Wireshark packet analyzer to **analyze VoIP traffic**.

10 Gb/s Ethernet Line | **HAMOC with SIP+RTP Filter** | **Wireshark**

Use Case – Snort over HAMOC

- **Sniffer** – displaying network traffic.
- **Packet Logger** – saving display traffic to file.
- **Network Intrusion** Detection System – IDS.
- **Inline Mode** – Intrusion Prevention System – IPS.
- 8 **parallel** instances of **Snort** → performace increase.

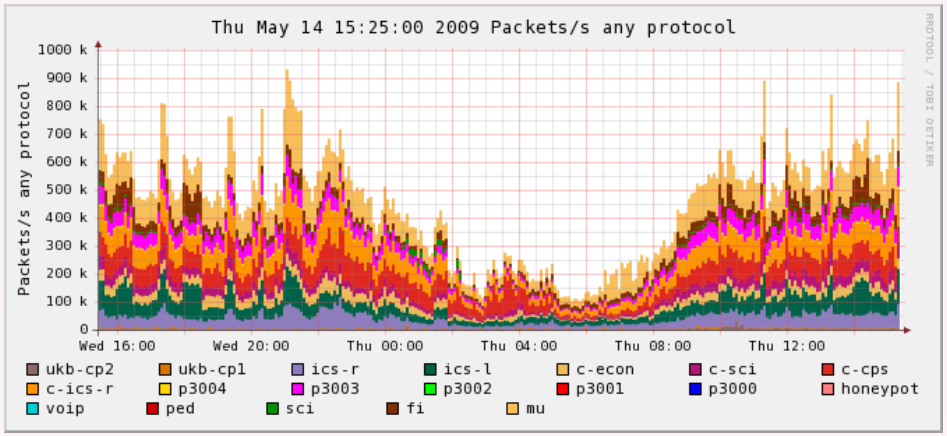


Part IV

Use Cases – Advanced Flow Analyses

Flow Based Monitoring

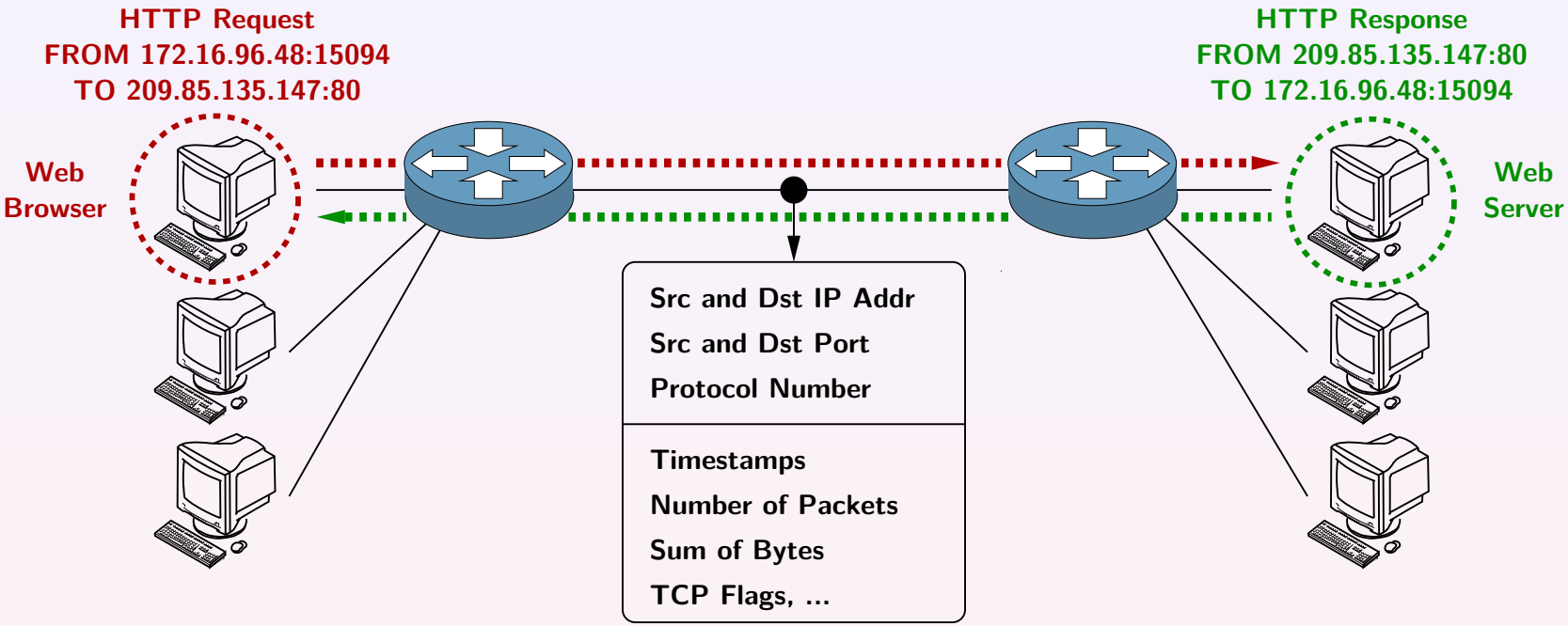
- Provides information about **who** communicates **with whom**, for **how long**, which **protocol**, **how much data** and so on.
- Based on CISCO **NetFlow v5/v9** technology and IETF **IPFIX**.
- Enables you to watch your network traffic **in real-time**.
- **GÉANT2 Security Toolset** = FlowMon probe + NfSen.



Detailed network view with NetFlow data.

Use Case – NetFlow Principles

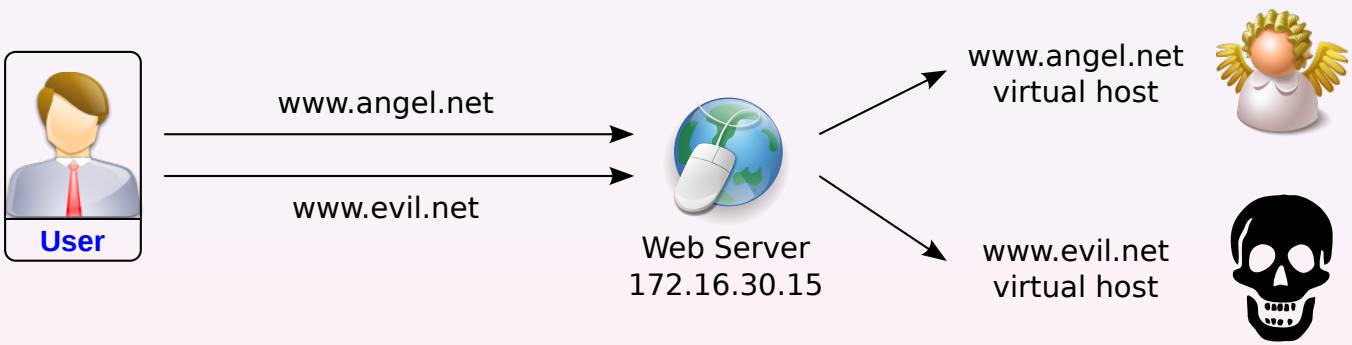
- Useing **FlowMon probe** to generate NetFlow or IPFIX data.



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

Use Case – Web Access Analyzer

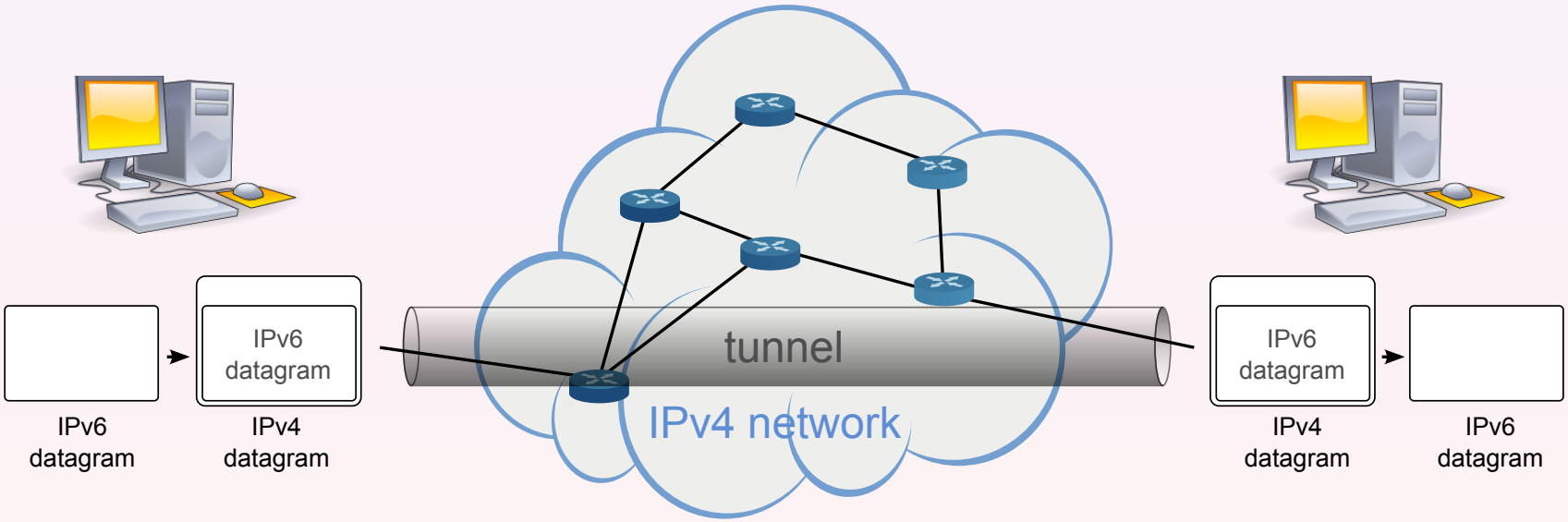
- Only **specific** part of **traffic** is analyzed.
- Uses **TAP or mirror port** to get traffic to analyze.
- Uses *httpry* utility to analyze HTTP traffic.




```
Timestamp            Source-IP     Dest-IP         Method  Host
2010-03-18 20:35:09  172.16.30.2   172.16.30.15    > GET   www.angel.net
2010-03-18 20:35:24  172.16.30.2   172.16.30.15    > GET   www.evil.net
```

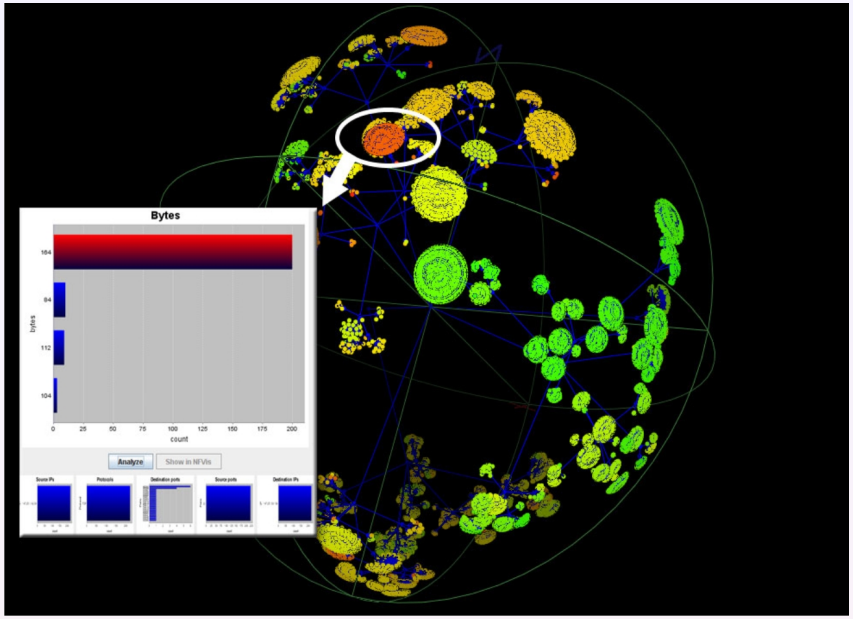
Use Case – Tunneled IPv6 Traffic Monitoring

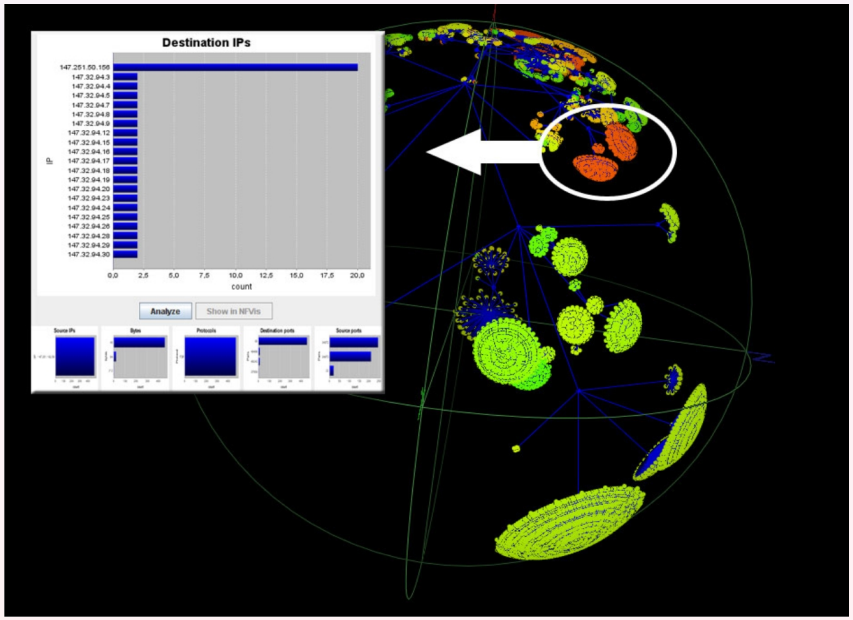
- **IPv6 is hidden** inside IPv4 tunnel – possible security risk.
- Support for common IPv6 transition mechanisms (Teredo, 6to4, ISATAP).
- Exporting statistics of envelope IPv4 as well as of tunneled IPv6 traffic using **modified NetFlow** protocol.



Network Behavioral Analysis

- Full **manual analysis** of flow data **is manually intensive**.
- Naive, high speed attacks are easy to detect.
- Automated solution needed to **detect sophisticated attacks**.
- Incident analysis and reporting.
- Available approaches:
  - thresholds,
  - trend analysis,
  - attack-specific patterns,
  - **anomaly detection**.





Part V

Use Cases – Network Defence

Network Defense

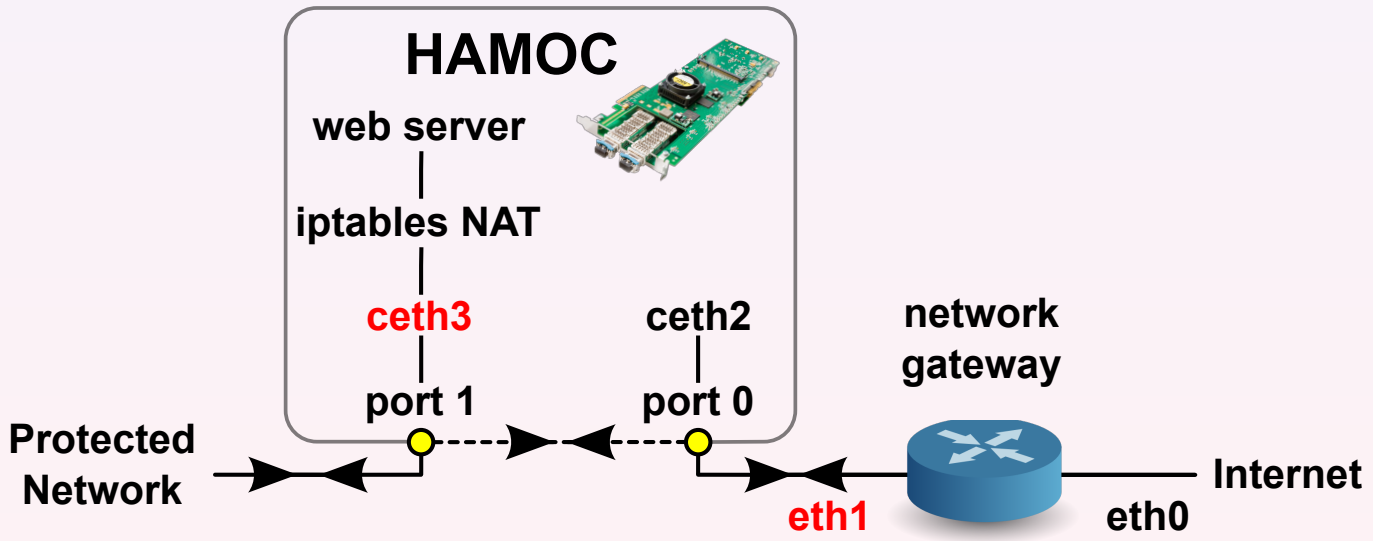
With acquired information you are able to do

- filtering and firewalling,
- network traffic splitting,
- packet sniffing,
- load balancing.

That all at **full linerate**
and **without packet loss**.

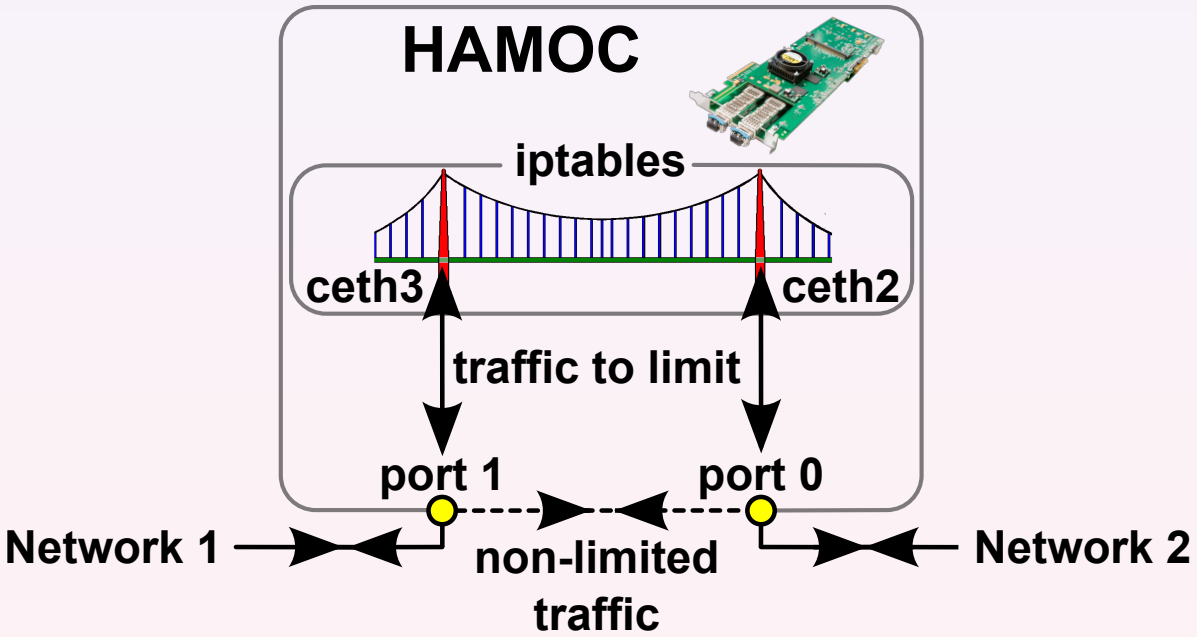
Use Case – Network Protector

- **Auto-disconnects** infected or enemy users **from network**.
- **Transparent for good guys**, leakproof for bad guys.
- Deployed as last device before network gateway.



Use Case – Traffic Limiter

- **Limits specific traffic** filtered by HAMOC firmware.
- Uses *iptables* traffic shaping features.



Part VI

Even Chuck Norris Can't Resist the Hardware Acceleration

Chuck Norris Botnet

- **Linux malware** – IRC bots with central C&C servers.
- Attacks **poorly-configured** Linux **MIPSEL** devices.
- Vulnerable devices – **ADSL modems** and **routers**.
- Uses **TELNET brute force** attack as infection vector.
- Users are **not aware** about the malicious activities.
- **Missing** anti-malware **solution** to detect it.
- Discovered by **hardware accelerated FlowMon probes** at **Masaryk University** on 2 December 2009.

The botnet got the Chuck Norris moniker from a comment in source code:

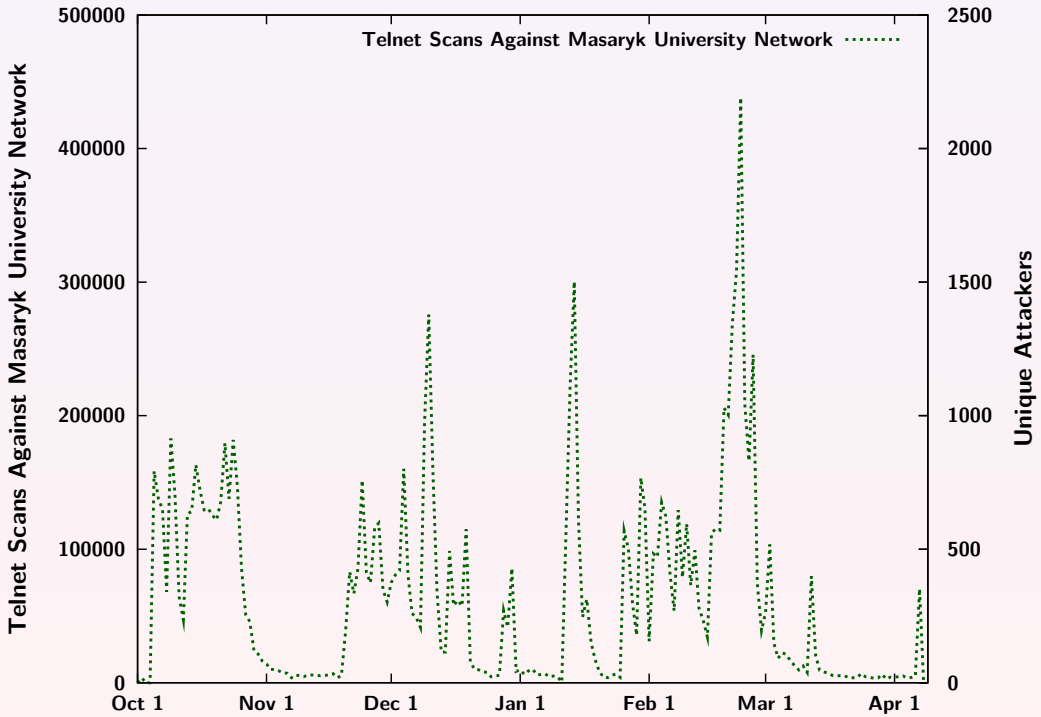
```
[R]anger Killato :  in nome di Chuck Norris !
```

Botnet Size and Evaluation

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.

Most Infected ISPs

Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network



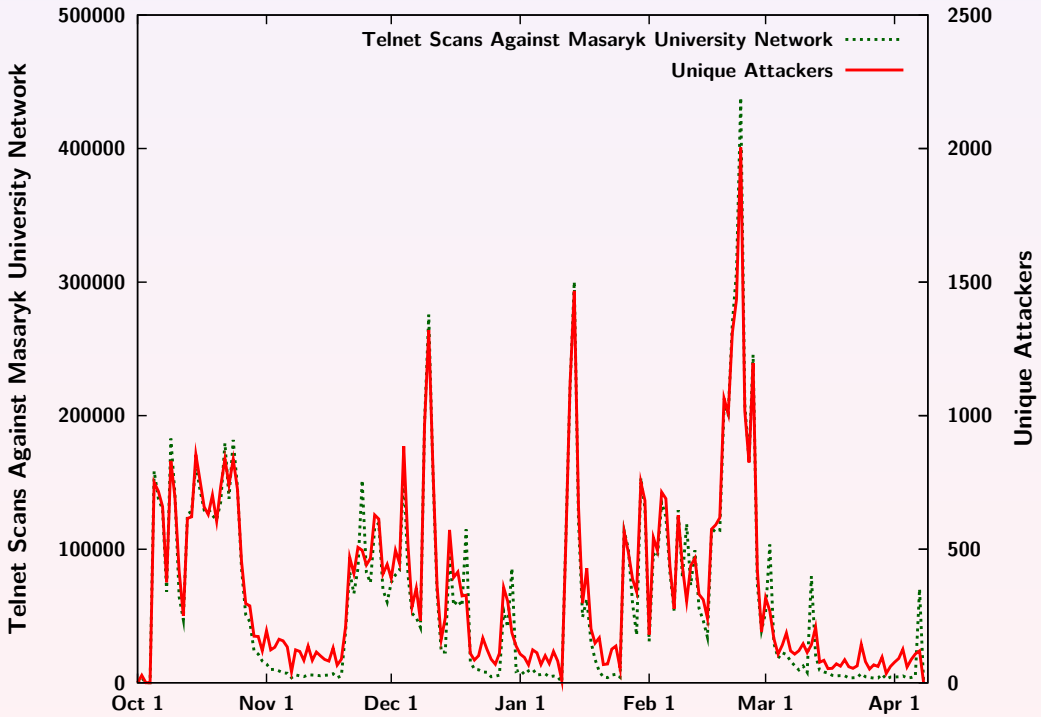
Unique attackers targeting the MU network

Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Botnet Size and Evaluation

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.



Most Infected ISPs

Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network

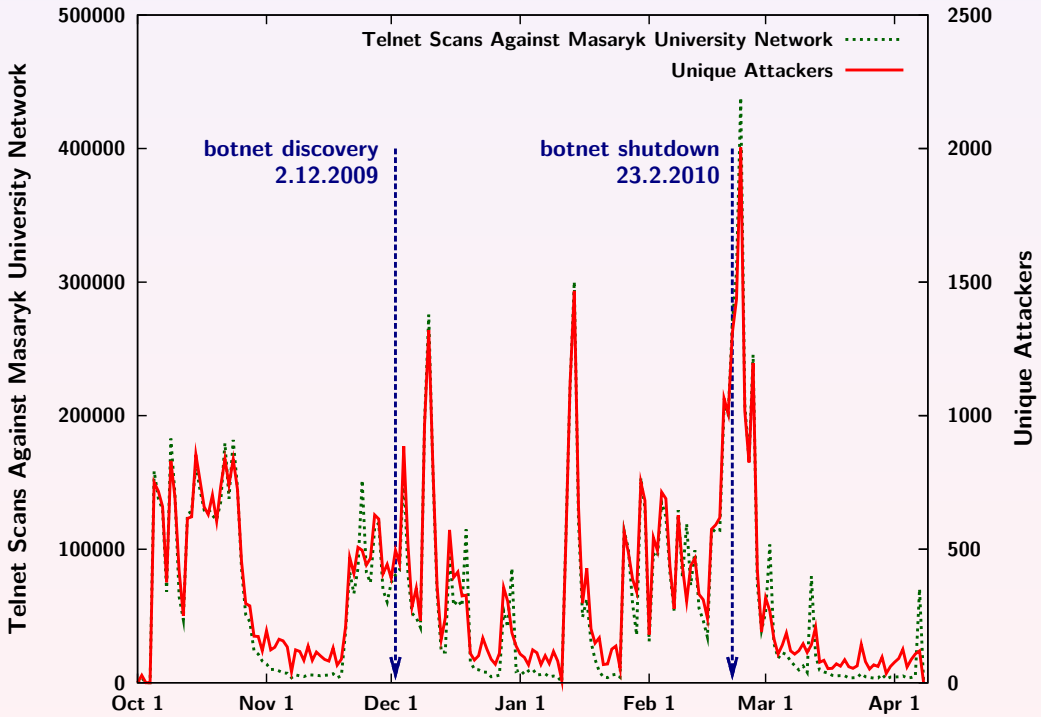
Unique attackers targeting the MU network

Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Botnet Size and Evaluation

- Size **estimation based on NetFlow** data from Masaryk University.
- **33000** unique **attackers** (infected devices) from **10/2009 – 02/2010**.



Most Infected ISPs

Telefonica del Peru
Global Village Telecom (Brazil)
Turk Telecom
Pakistan Telecommunication Company
China Unicom Hebei Province Network

Unique attackers targeting the MU network

Month	Min	Max	Avr	Mdn
October	0	854	502	621
November	41	628	241	136
December	69	1321	366	325
January	9	1467	312	137
February	180	2004	670	560
Total	0	2004	414	354

Botnet **stopped** activity on **23 February 2010**.

Part VII

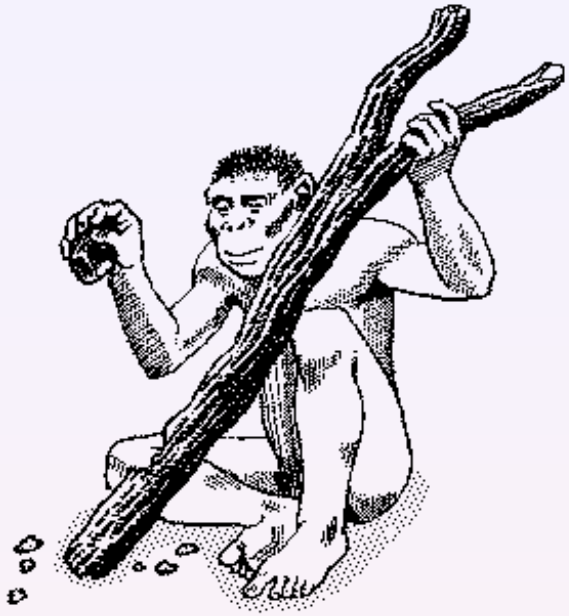
Conclusion

Conclusion

- **Hardware acceleration** enables reliable wirespeed traffic processing even in worst case scenarios – DoS/DDoS.
- **NetCOPE platform** allows rapid firmware development.
- Simple development of new applications due to **PCAP API**.
- Works even on **encrypted and tunneled traffic**.
- HAMOC is being **deployed at CESNET network**.
- The results of the research activities were transferred into **spin-off company**.

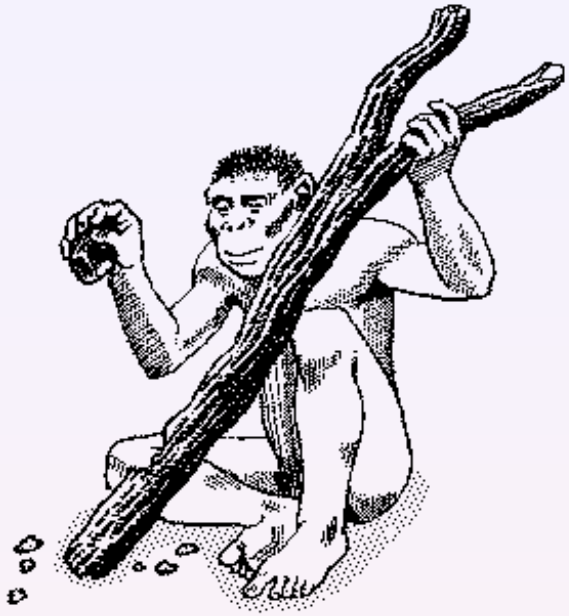
Future Work

- Extend portfolio of HAMOC applications.
- Adopt **40/100G Ethernet**.
- Deploy HAMOC to **more partners**.



Future Work

- Extend portfolio of HAMOC applications.
- Adopt **40/100G Ethernet**.
- Deploy HAMOC to **more partners**.



We are looking for new R&D partners.

Research and Development Background

R&D is held by CESNET (Czech NREN) in a frame of **Optical National Research Network and its New Applications** together with:

- Masaryk University
- Brno University of Technology

Team has about 60 members (most of them are students)

- Hardware
- Software
- Testing
- Support

Thank You For Your Attention

Hardware Acceleration: An Essential Part of Cyber Security in High-Speed Networks

Jiří Novotný
novotny@ics.muni.cz

Pavel Čeleda
celeda@ics.muni.cz

Radek Krejčí
krejci@liberouter.org

This material is based upon work supported by grants from the Czech Ministry of Education, EU Funds, European Research Office of the US Army, Ministry of Defece and Armed Forces of the Czech Republic.