Hardware Acceleration in Monitoring of Gigabit Networks: The SCAMPI project

Jiří Novotný
<novotny@ics.muni.cz>
Masaryk University

Arne Øslebø
<arneos@uninett.no>
Uninett

08.12.2004 Brugges
Scampi overview

• 2.5 year 5th Framework project

• Started April 2002, extended to May 2005

• 9 partners:

  CESNET, FORTH, FORTHNET
  IMEC, Leiden University, Masaryk University
  NETIKOS, TERENA, UNINETT
Main goals:

• Development of a high-performance intelligent monitoring adapter for 10 Gbps

• Development of an open and extensible architecture for network monitoring

• Development of monitoring and measurement tools

• Investigate strategies and methodologies for monitoring systems operating at 100 Gbps and beyond
Applications

- Intrusion detection - uses Snort signatures

- QoS application - packet loss, jitter, one way delay

- DOS attack detection - based on anomaly detection

- Flowrep - generic report generator with a web frontend for Netflow/IPFIX records
MAPI (Monitoring Application Programming Interface)

- Design goals:

  Make it quick and easy to implement new monitoring applications
  Support for multiple concurrent users and applications
  Global optimization - optimize processing of packets based on all applications from all users
  Transparent support for different hardware adapters
  Easy to extend - New drivers, function libraries
• Support for: SCAMPI adapter, DAG cards, NIC

• Network flow

  mapi_create_flow

  Initially all packets seen on the network

• Apply functions to a flow

  mapi_apply_functions

  BPF filter, string search, packet counter, byte counter, Netflow, jitter etc.
• Read results
  
  mapi_read_result
  mapi_get_next_pkt

• MAPIId Daemon that communicates with hardware devices and processes packets in software
Why Programmable Hardware

- Today's computers are not able to process traffic monitoring at wire speeds
  - PCI bus throughput
  - interrupt latency
  - slow disk access

  . . . . hardware acceleration
• ASICs are not flexible enough do not follow changing conditions of the Internet

• . . . . programmable hardware acceleration
Solution

SCAMPI adapters - based on COMBO family developed by CESNET and Masaryk University
COMBO6
COMBO6

Combination of programmable hardware and standard integrated circuits

- XILINX FPGA (VIRTEX II 3000-6000)
- CAM, 3xSRAM, DDRAM, EEPROM
- PLX, power supply
- Exchangeable interface cards

Status - fully operational, will be replaced with COMBO6X
COMBO6X

- 2xXILINX II PRO, 3xPower PC - processors inside FPGA can bring new ideas in network monitoring

- Using of FPGA and PCI core instead of PLX chip - speed of PCI bus goes up at least to 4Gb/s. With PCI-X core could go up 8Gb/s

- 3xSRAM, 1xCAM, 1xDRAM

- The COMBO6X with FPGA and PCI core is ready for redesign to Express PCI

Status - in manufacturing phase
COMBO-4MTX
COMBO-4MTX

Interface card with 4x1Gb/s copper ports

- 2xXILINX FPGA (VIRTEX II 1000-3000)
- 2xSRAM, EEPROM
- 4x1Gb ports

Status - fully operational
COMBO-4SFP
COMBO-4SFP

Interface card with 4x1Gb/s optical ports

- 2xXILINX FPGA (VIRTEX II 1000-3000)
- 2xSRAM, 3xEPPROM
- 4x1Gb ports in SFP cages (hot swap)
- hw supports four speeds - 1GbE, Infiniband, Fiber channel

Status - fully operational
COMBO-2XFP
COMBO-2XFP

Interface card with 2x10Gb/s optical ports

- 1xXILINX FPGA (VIRTEX II PRO XC2VP20), Power PC inside
- 1xSRAM, 1xCAM, 3xEEPROM
- 2x10Gb ports in XFP cages (hot swap)

Status - operational (but need to be redesigned, issues with phyters)
COMBO-2XFPRO, COMBO-4SFPRO

New generation of interface cards

- Based on XILINX VIRTEX II PRO and VIRTEX II PRO-X
- No phyters

- COMBO-4SFPRO - 4x1GbE (VIRTEX II PRO), 4xOC48 (VIRTEX II PRO-X)
- COMBO-2XFPRO - 2x10GbE or 2xOC192
- Status - in design phase
COMBO-PTM
COMBO-PTM

Precise Time Module

- XILINX FPGA (Spartan 3) - 90nm technology

- MCU - Texas Instruments MSP430FI49IPM

- Precise crystal

- Connector for GPS (PPM, data)

Status - fully operational
SCAMPI adapters

- SCAMPI-4MTX -> COMB06, COMBO-4MTX, COMBO-PTM

- SCAMPI-4SFP -> COMB06, COMBO-4SFP, COMBO-PTM, 4xSFP transceiver

- SCAMPI-2XFP -> COMB06X, COMBO-2XFP, COMBO-PTM, 2xXFP transceiver

- Any combination of COMBO6, COMBO6X with, COMBO-4MTX, COMBO-4SFP, COMBO-2XFP, COMBO-2XFPRO, COMBO-4SFPPro is available
SCAMPI Firmware

- Modular design
- VHDL-standard development approach with simulation
- Nanoprocessors instead of FSMs
- Prototyping firmware blocks in SW
- Hardware/software co-design
TSU  −  Time Stamp Unit
HFE  −  Header Field Extractor
LUP  −  Lookup Processor
STU  −  Statistic Unit
SAU  −  Sampling Unit
PCK  −  Payload Checker
DISP − Packet Dispatcher
HOST − Host Computer
VHDL blocks

Time Stamp Unit (TSU)

- 64 bits fixed point - 32 number of seconds (since 1.1.1970), 32 fraction of second

- resolution 10 ns (64 bytes at rate 10Gb/s ~ 50 ns)

- controlled by PPS input (e.g. GPS receiver), accuracy (with PPS) ~ 1 us, accuracy (with NTP) ~ 50 us
Packet classification

- Header Field Extractor (HFE) - extract information for classification from packet headers

- Look-up Processor (LUP) - packet classification

  CAM - matching up 272 bits

  processing unit - search tree
Sampling Unit (SAU)

- deterministic sampling - each n-th packet is passing through

- byte deterministic - each packet containing n-th byte is passing through

- probabilistic sampling - packet is passing with probability 1/n
STU (statistic unit)

- packets lengths statistic: number of packets, total length, sum of squares of lengths, min/max value
- statistics of intervals between packets: number of packets, total time, sum of squares of intervals, min/max

PCK (payload checker)

- CAM is used for payload checking
- checks payload for defined patterns (16 bytes)
SCAMPI SOFTWARE

- Linux driver
- Mapi for COMBO6
- Software simulator of COMBO6 on top of commodity card
- Comfort development environment for nanoprogams (nsim)
- Comboctl - loader and comfort debugging
More information can be found at

http://www.liberouter.org/