Flow measurements from the packet-switched NREN PIONIER: technology and experience

Wiktor Procyk, Szymon Trocha
{wiktor.procyk, szymon.trocha} @man.poznan.pl

Introduction

Changes in the computer networks during recent years:

- increased bandwidth and popularity
- new services – grids, videoconferencing, VoIP requiring bandwidth and quality
- growing meaning of quality assurance and SLA

Need of network monitoring and engineering

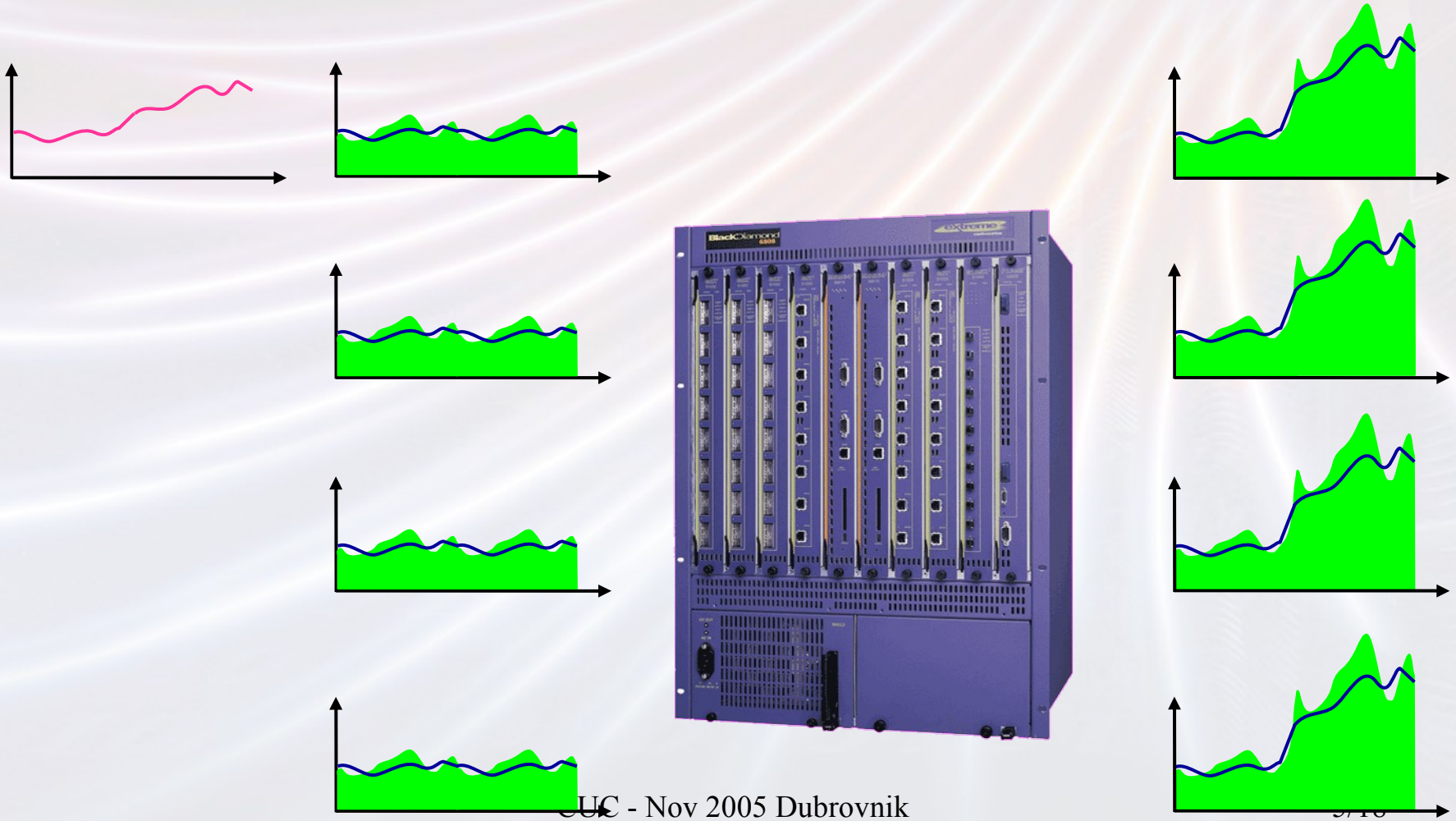
Overview

- need of monitoring on the Layer 2 in case of services like “Digital channels”
- for monitoring Layer 2 sFlow multivendor sampling technology can be used
- GPL based tools are used in many NRENs for monitoring purposes because of their low price and flexibility
- sFlow is poorly supported by nearly all GPL tools

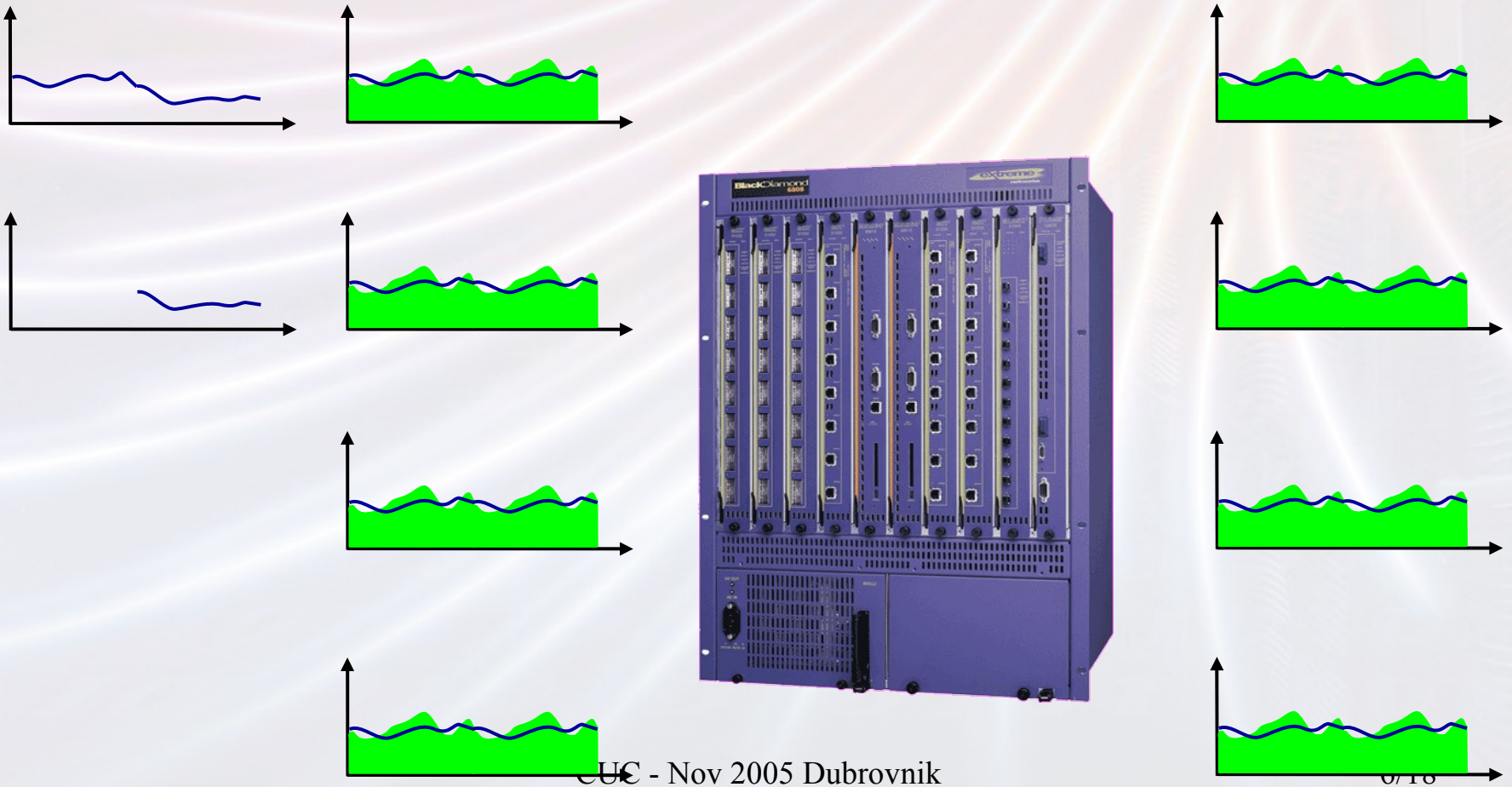
What Is The Problem?

- Network device: Extreme Networks BlackDiamond 6800 switch; sFlow enabled per interface; sampling rate set per whole device
- Conditions: 8 interfaces with equal network traffic volume; sFlow enabled on 1st interface
- Problem description: number of sFlow samples is independent from network volume traffic

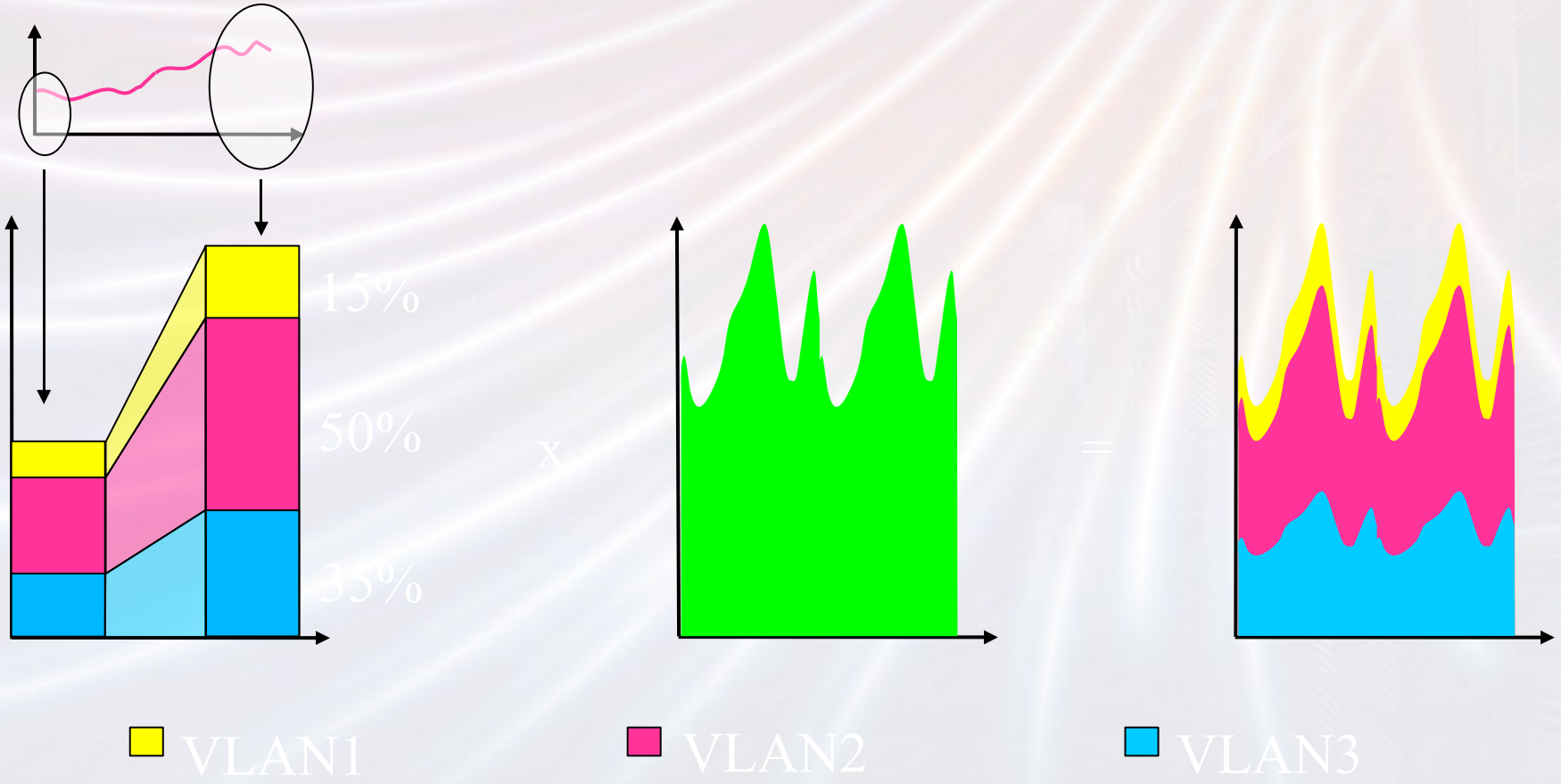
Problem – case 1



Problem – case 2



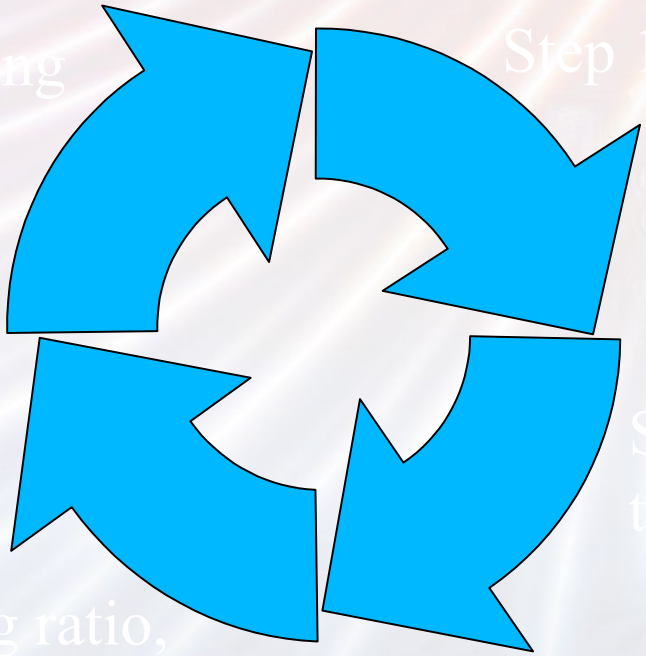
Proposed solution



Algorithm

Step 4 – data processing

Step 1 – acquiring data



Step 2 – dividing time into periods

Step 3 – calculating ratio, updating files

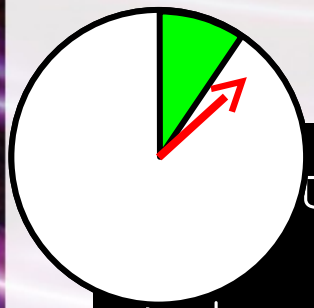
Step 1 – Acquiring Data

```
startDatagram ================
datagramSourceIP 150.254.234.11
...
agent 150.254.234.11
packetSequenceNo 10866390
...
...
inputPort 8001
outputPort 0
flowBlock_tag 0:1
...
```

Keywords

- agent
- inputPort
- outputPort
- sampledPacketSize
- decodedVLAN

Step 2 – Dividing Time into Periods



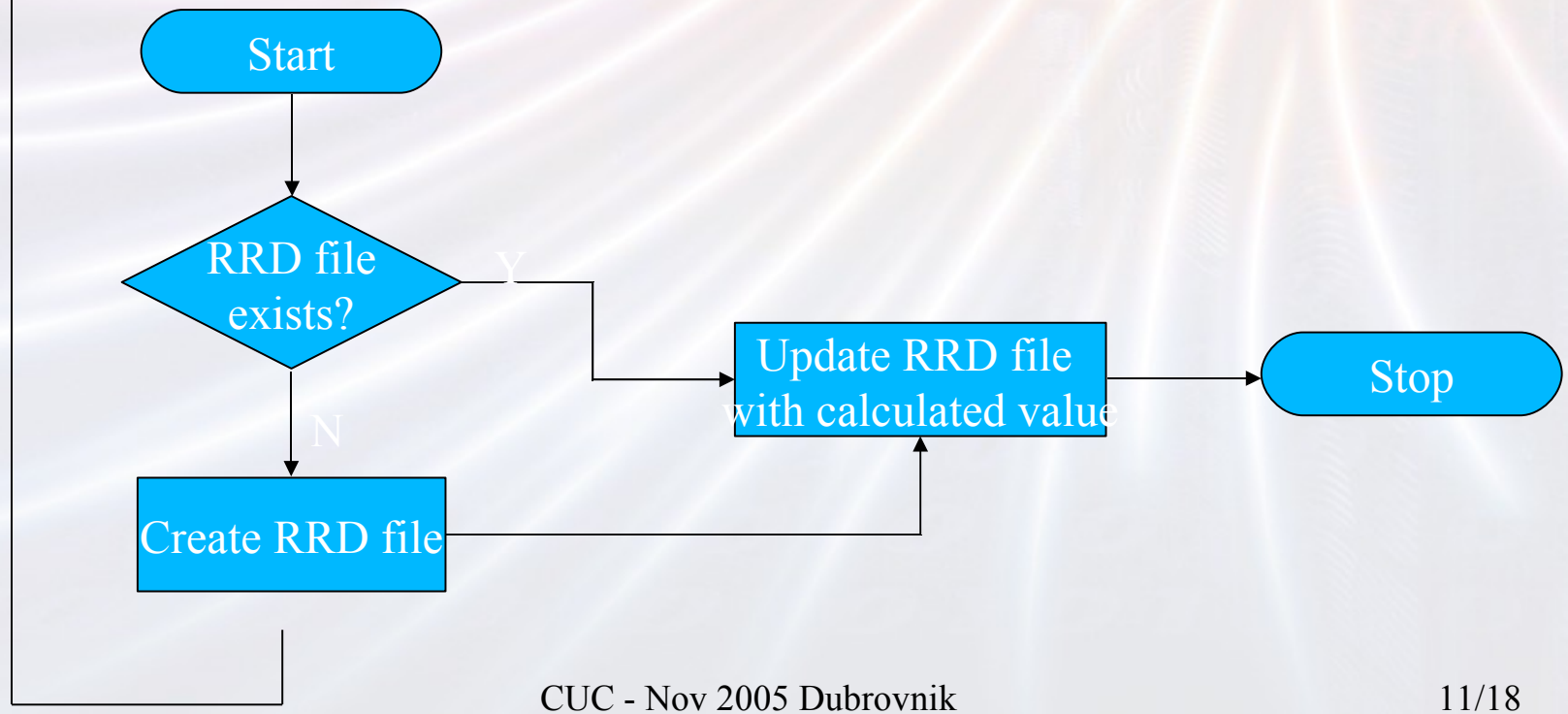
```
tDatagram ============

datagramSourceIP 150.254.234.11

...

packetSequenceNo 10866390

...

decodedVLAN 365
```

Time to update files

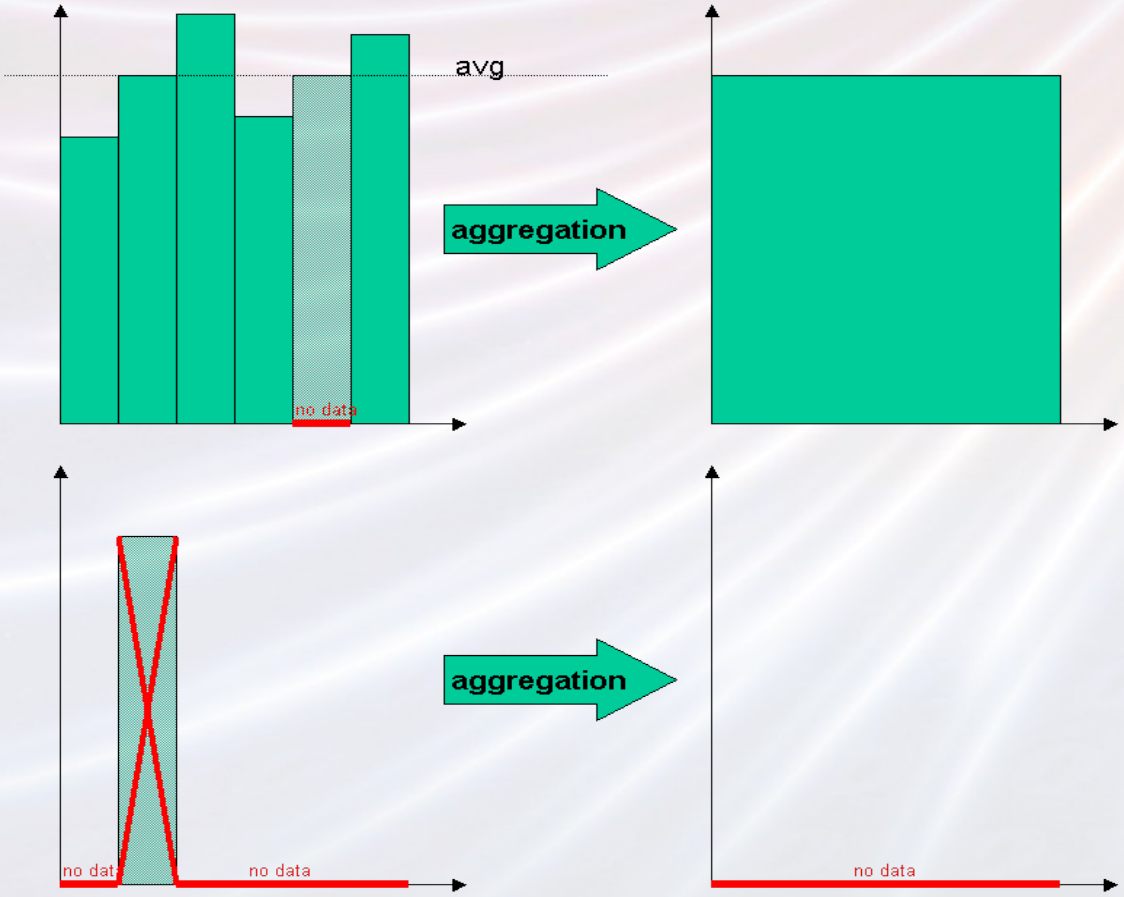
Step 3 – Updating Files

$$s = \frac{v}{T}$$

T the total traffic on the interface;
v the traffic on a particular VLAN on that interface;
s VLAN's share on that interface



The Rules for RRD Aggregation



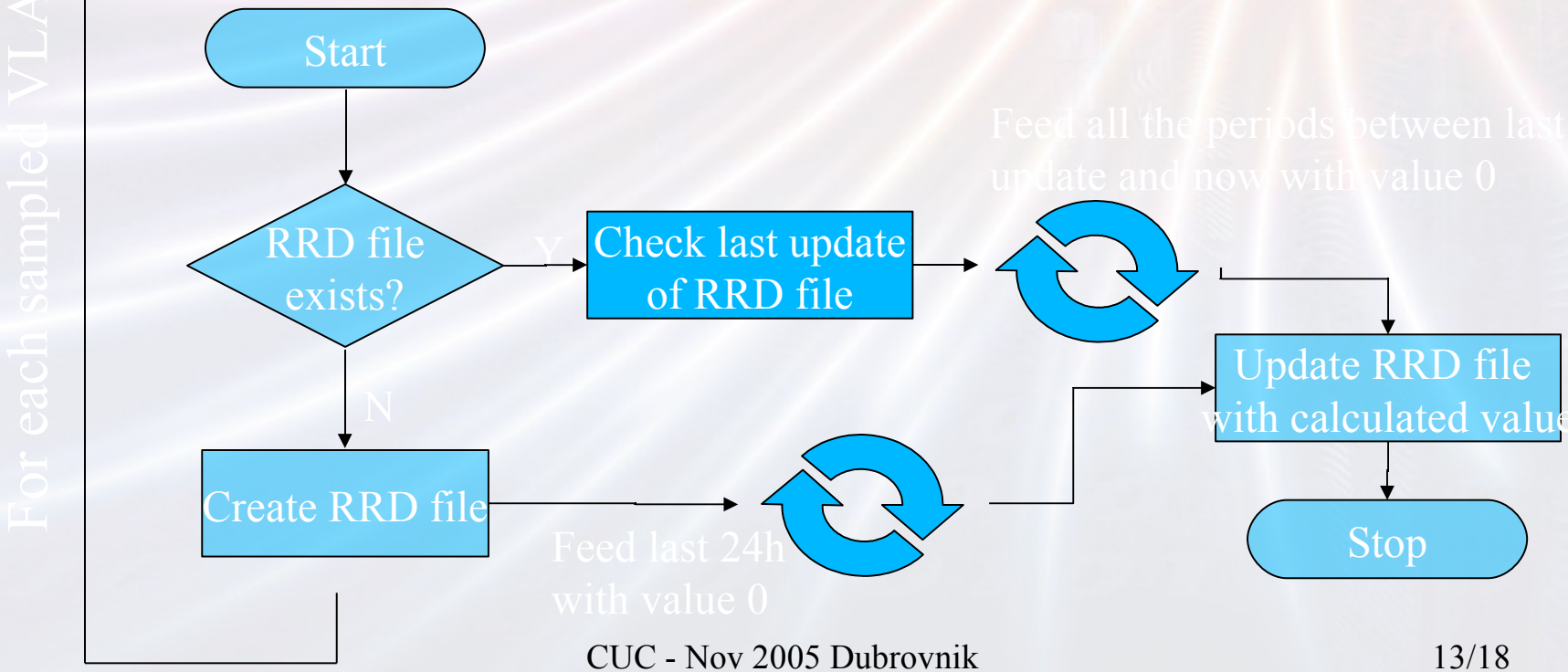
Sum of all shares on the interface exceeds 100%

Sum of all shares on the interface does not achieve 100%

Step 3 – Updating Files (Modified)

$$s = \frac{v}{T}$$

T the total traffic on the interface;
v the traffic on a particular VLAN on that interface;
s VLAN's share on that interface



Step 4 – Data Processing

<agentIP>-<interface>	in	out
150.254.234.11-1	153	154
150.254.234.11-2	153	154
150.254.234.11-3	153	154
…		
150.254.234.11-8	153	154

<agentIP>-<interface>-<VLAN>	in	out
150.254.234.11-1-1	45	53
150.254.234.11-1-2	32	37
150.254.234.11-1-3	76	64
150.254.234.11-2-1	45	53
150.254.234.11-2-2	32	37
…		
150.254.234.11-8-3	76	64

Implementation

Network

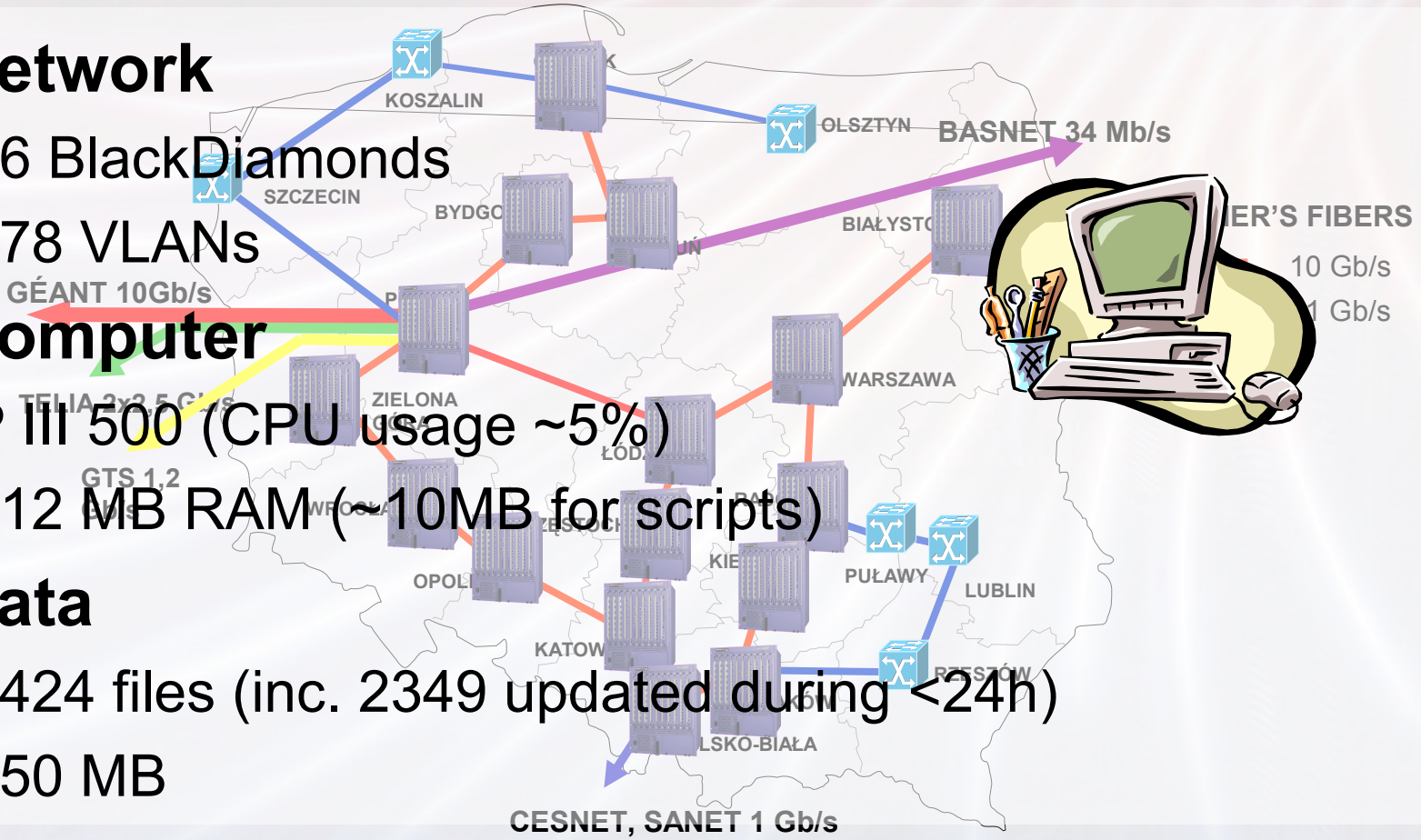
- 16 BlackDiamonds
- 278 VLANs

Computer

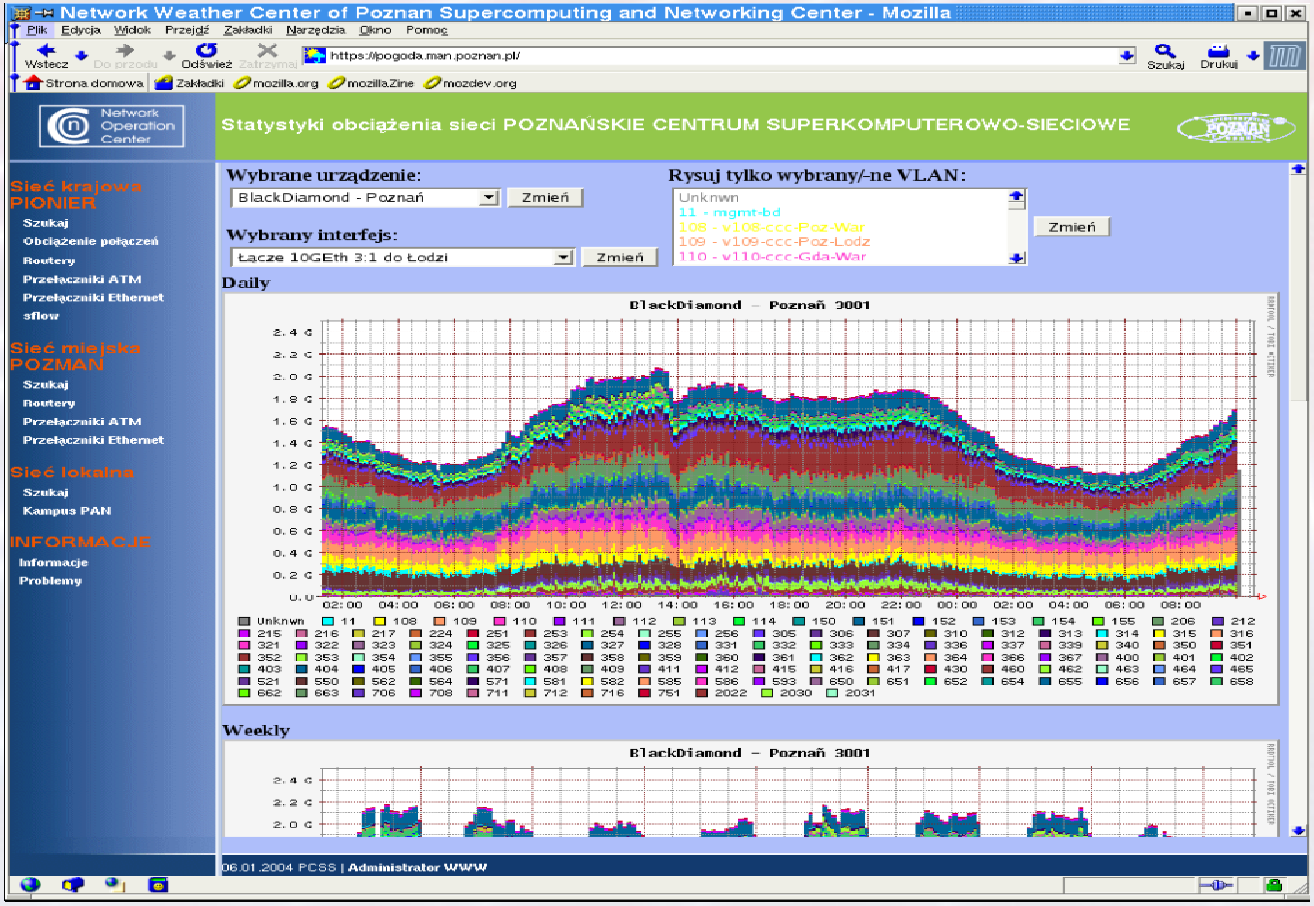
- P III 500 (CPU usage ~5%)
- 512 MB RAM (~10MB for scripts)

Data

- 5424 files (inc. 2349 updated during <24h)
- 350 MB



Access to the Data – as Easy as Possible



Website Frontend

- written entirely in PHP
- visualisation of all or only selected VLANs on particular port
- relations between RRD files stored in the database
- used mostly by PIONIER NOC

Q&A

{wiktor.procyk, szymon.trocha} @man.poznan.pl