Customized anomaly detection and analysis tools as a service

Delivering monitoring services to different groups of users ...

Tom Kosnar
CESNET a. l. e.
kosnar@cesnet.cz

Workshop: Campus Monitoring and Security, Prague Apr. 24-25 2014

Content

- What do the users need ?
- Large scale SW monitoring tools we developed and use
  - **infrastructure monitoring**
  - **flow-based monitoring**
  - Overview, components, current state
  - Monitoring examples, output examples, anomaly detection examples

What do the users need ?

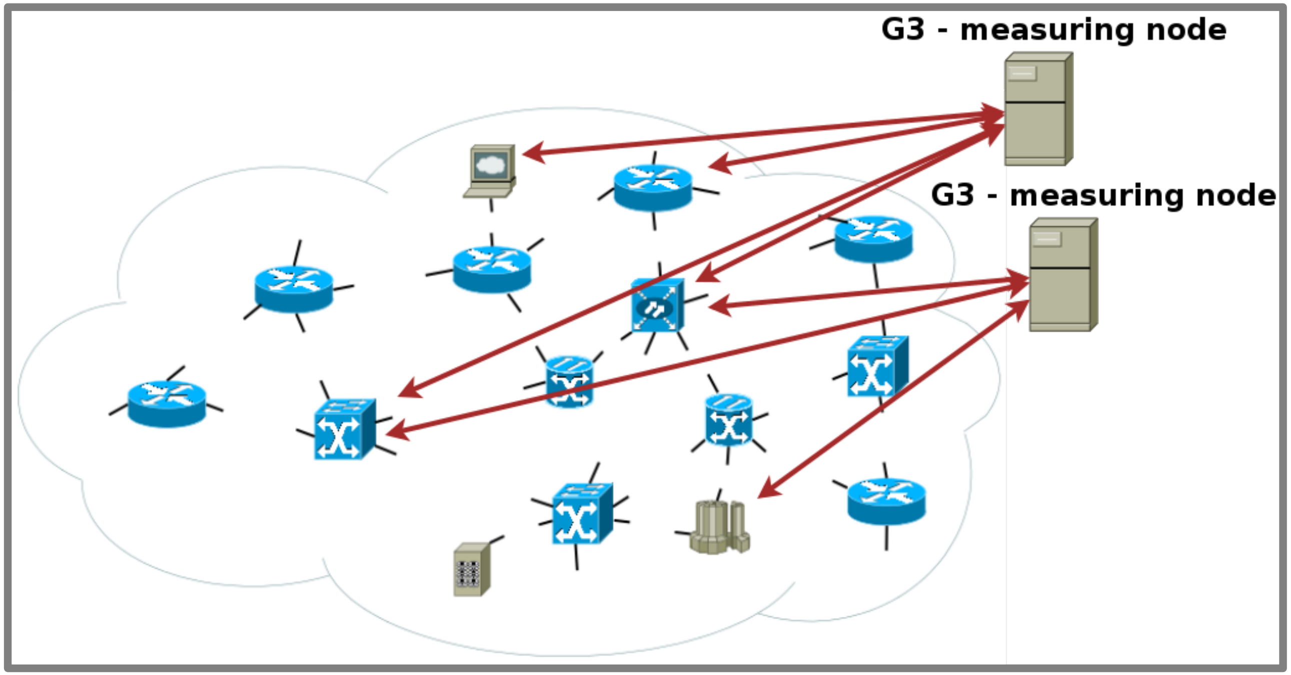
- Different groups of users who need support based on monitoring..
  - Backbone administrators (at least ours) – want to see immediately **everything** we can imagine (even very very detailed things); *interactive full-featured UI*
  - Local IT/service administrators – don't want to measure..or whatever (they focus on delivering high level services to end-users); they need **assistance to solve their problems**; *simple intuitive UI, overview style*
  - CSIRT people – require to be **notified** (if possible) in case of **anomalies** and must be able (in any case) to **analyze things** within the scope of incident handling process; *UI with specific features (simple in some areas, complex in others)*
  - End-users – want to use things and not to analyze them – they need someone who **solves their problems**, they may want to see basic state information about service only (“..*operator thinks, that service shall work ;-)”*); *very simple intuitive UI*
  - ….managers,...other groups – different perspective, different requirements

Large scale monitoring tools developed & used @ CESNET

- Focusing our common SW tools in this case (also have special HW based mentioned in other presentations)
- **Infrastructure monitoring area**
  - Information about infrastructure components and services generated from information measured on devices & systems that infrastructure consists of
    - **G3 system**
- **Flow-based monitoring area**
  - Information about IP traffic of institutions, facilities, devices, lines, etc..., information about incidents and anomalies processed from flow-based data measured in the infrastructure
    - **FTAS system**

G3 system – data measurement & processing core

- Periodical data gathering (in general any method)
- Built in SNMP support; RFC MIBs, proprietary (Cisco, CESNET)
- Automated device component discovery – *SNMP access & IP address to measure whole device (with SNMP)*
- Automated construction of logical structure of devices – *independent on technological identifiers (SNMP indexes)*
- Configurable dynamic timing of measurement (time-step strategy) – *low measurement aggressiveness while catching "some dynamic"*
- Currently can measure > 700 information items (~ 550 SNMP based on SNMP OID)

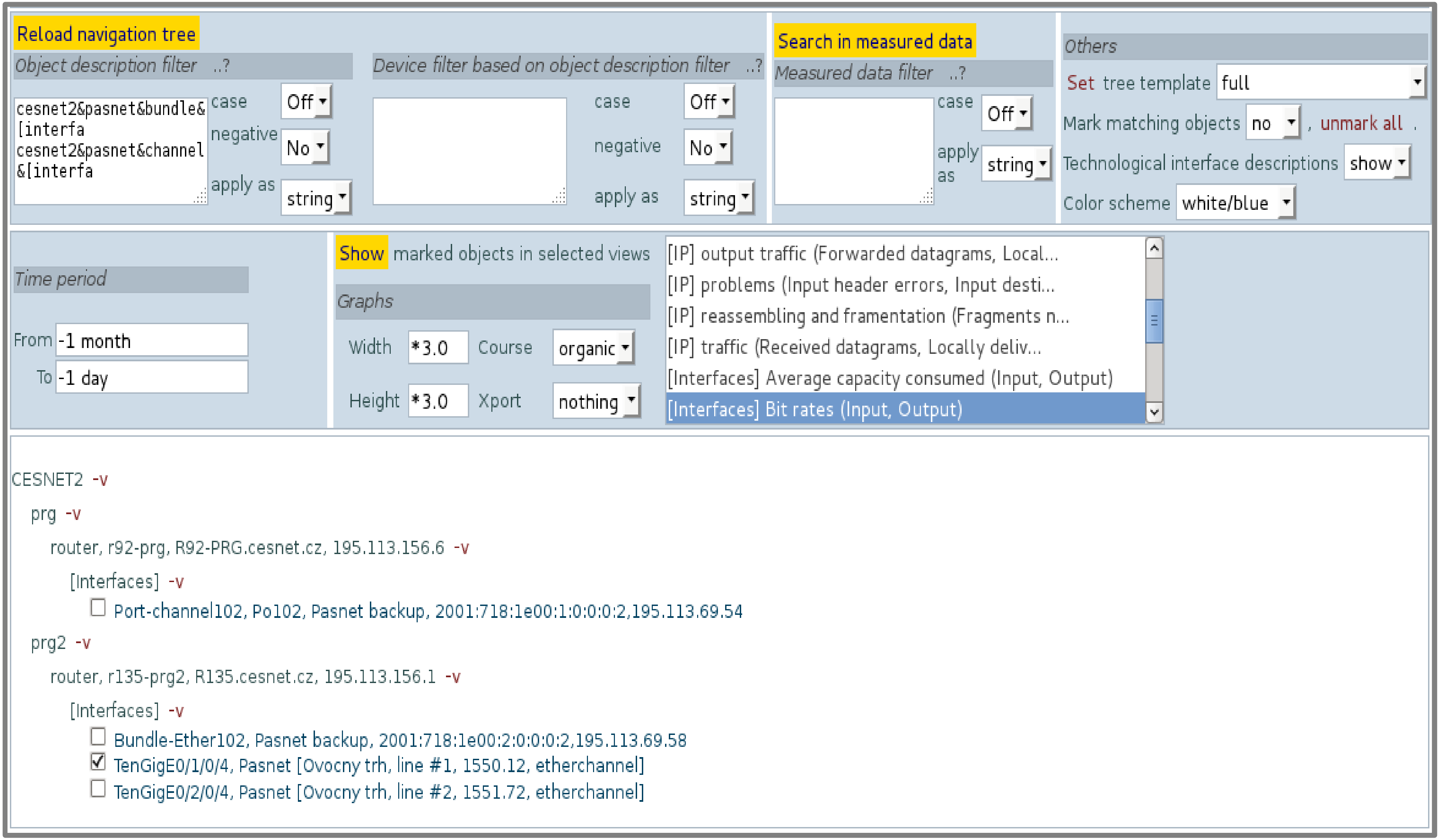


G3 data access – interactive UI

- **Infrastructure browser**
    - **To find objects** (device/service components) **of interest**
        - Several selection mechanisms or expand & collapse style
        - Special selections of objects with measured data above limits set in UI (~interfaces with error rates >= X pps, CPUs with load >= Y%, ...)
        - Flexibility in visualizing object tree - can interpret multiple instances of objects as single one (~all selected interfaces as one anonymous)
        - Can store current state (filtering conditions etc..) for further use
- **Visualizer of selected objects** as needed
    - Support for aggregated (graphical) outputs
    - Single items visualization, system and user defined configurable views,...

G3 data access – interactive UI

- Interactive UI example: first step - navigation ~ objects browser



Object description filter ..?

cesnet2&pasnet&bundle&[interfa
cesnet2&pasnet&channel&[interfa

case Off
negative No
apply as string

Device filter based on object description filter ..?

case Off
negative No
apply as string

Measured data filter ..?

case Off
apply as string

Set tree template full
Mark matching objects no , unmark all .
Technological interface descriptions show
Color scheme white/blue

Time period

From -1 month
To -1 day

Show marked objects in selected views

Graphs

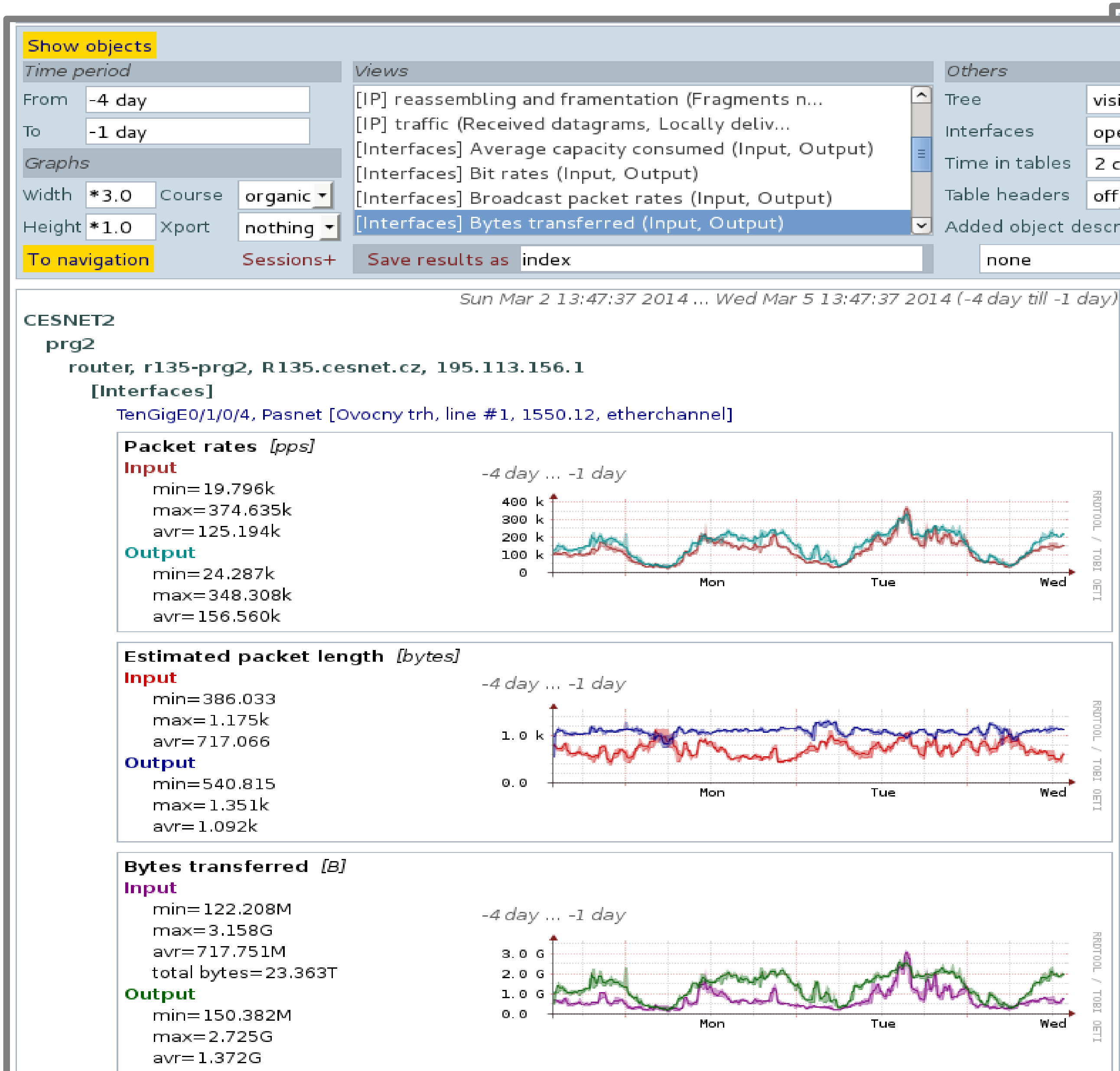
Width *3.0 Course organic
Height *3.0 Xport nothing

[IP] output traffic (Forwarded datagrams, Local...
[IP] problems (Input header errors, Input desti...
[IP] reassembling and framentation (Fragments n...
[IP] traffic (Received datagrams, Locally deliv...
[Interfaces] Average capacity consumed (Input, Output)
[Interfaces] Bit rates (Input, Output)

CESNET2 -v
prg -v
router, r92-prg, R92-PRG.cesnet.cz, 195.113.156.6 -v
[Interfaces] -v
☐ Port-channel102, Po102, Pasnet backup, 2001:718:1e00:1:0:0:0:2,195.113.69.54
prg2 -v
router, r135-prg2, R135.cesnet.cz, 195.113.156.1 -v
[Interfaces] -v
☐ Bundle-Ether102, Pasnet backup, 2001:718:1e00:2:0:0:0:2,195.113.69.58
☑ TenGigE0/1/0/4, Pasnet [Ovocny trh, line #1, 1550.12, etherchannel]
☐ TenGigE0/2/0/4, Pasnet [Ovocny trh, line #2, 1551.72, etherchannel]

G3 data access – interactive UI

- Interactive UI example: second step ~ selected objects visualizer



Show objects

Time period			
From	-4 day		
To	-1 day		

Graphs

Width	*3.0	Course	organic
Height	*1.0	Xport	nothing

Views

- [IP] reassembling and framentation (Fragments n...
- [IP] traffic (Received datagrams, Locally deliv...
- [Interfaces] Average capacity consumed (Input, Output)
- [Interfaces] Bit rates (Input, Output)
- [Interfaces] Broadcast packet rates (Input, Output)
- [Interfaces] Bytes transferred (Input, Output)

Others

Tree	visi
Interfaces	ope
Time in tables	2 c
Table headers	off
Added object descri	none

To navigation   Sessions+   Save results as index

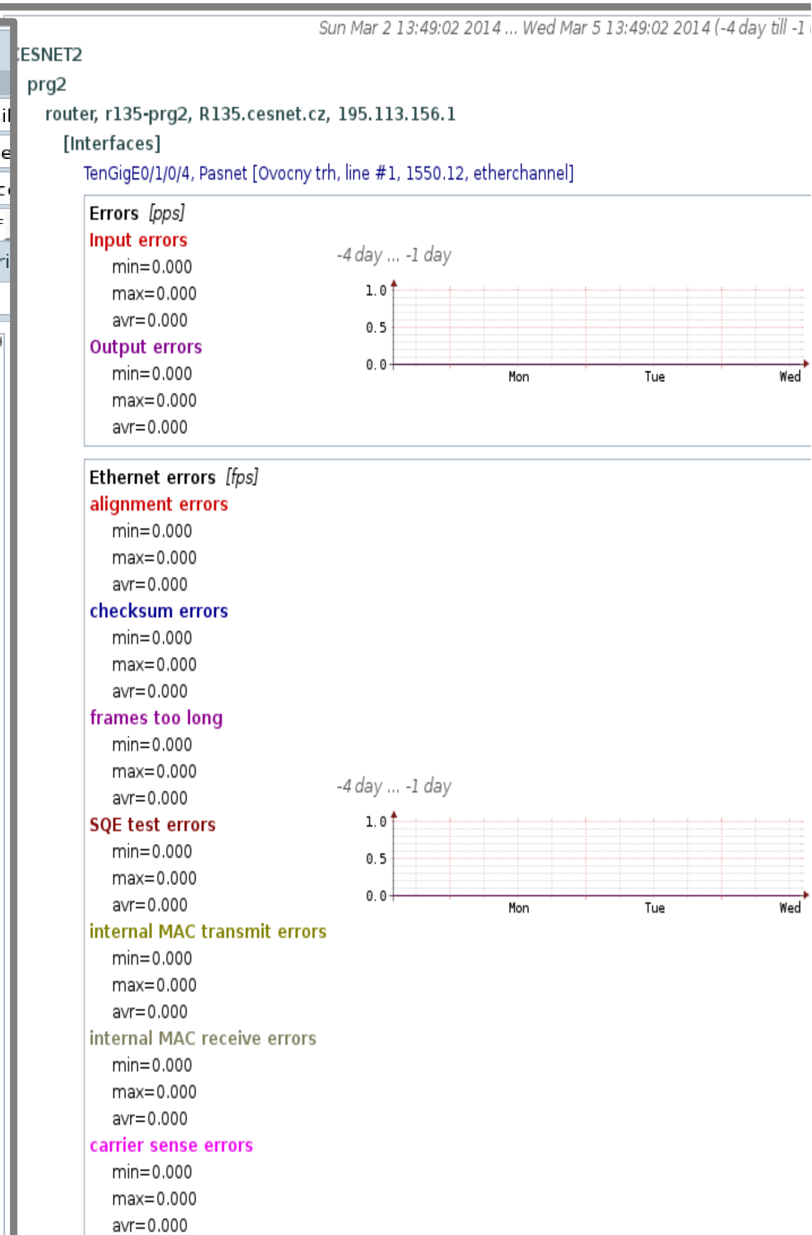
Sun Mar 2 13:47:37 2014 ... Wed Mar 5 13:47:37 2014 (-4 day till -1 day)

CESNET2
prg2
router, r135-prg2, R135.cesnet.cz, 195.113.156.1
[Interfaces]
TenGigE0/1/0/4, Pasnet [Ovocny trh, line #1, 1550.12, etherchannel]

Packet rates *[pps]*
Input
min=19.796k
max=374.635k
avr=125.194k
Output
min=24.287k
max=348.308k
avr=156.560k

Estimated packet length *[bytes]*
Input
min=386.033
max=1.175k
avr=717.066
Output
min=540.815
max=1.351k
avr=1.092k

Bytes transferred *[B]*
Input
min=122.208M
max=3.158G
avr=717.751M
total bytes=23.363T
Output
min=150.382M
max=2.725G
avr=1.372G



Sun Mar 2 13:49:02 2014 ... Wed Mar 5 13:49:02 2014 (-4 day till -1

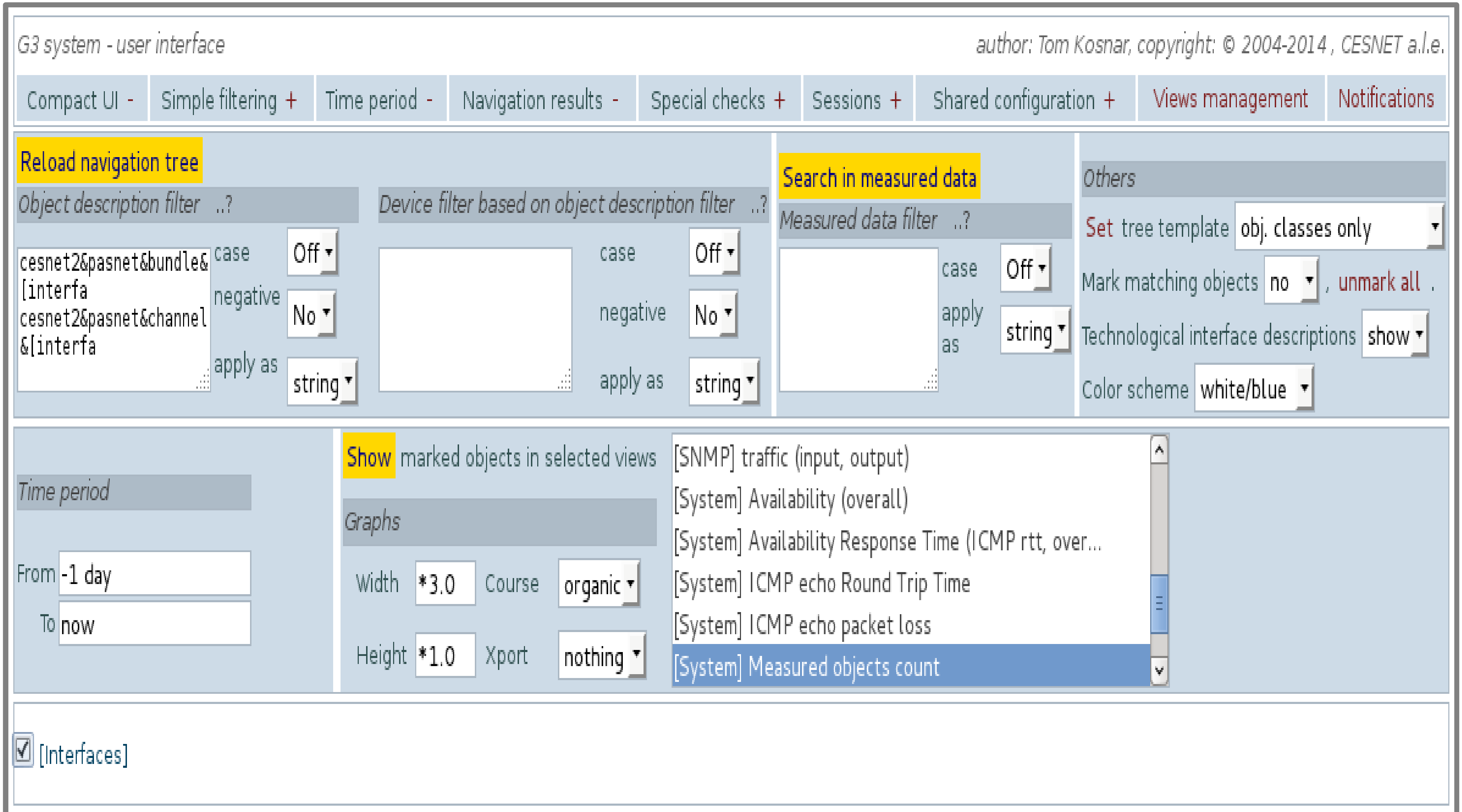
CESNET2
prg2
router, r135-prg2, R135.cesnet.cz, 195.113.156.1
[Interfaces]
TenGigE0/1/0/4, Pasnet [Ovocny trh, line #1, 1550.12, etherchannel]

Errors *[pps]*
Input errors
min=0.000
max=0.000
avr=0.000
Output errors
min=0.000
max=0.000
avr=0.000

Ethernet errors *[fps]*
alignment errors
min=0.000
max=0.000
avr=0.000
checksum errors
min=0.000
max=0.000
avr=0.000
frames too long
min=0.000
max=0.000
avr=0.000
SQE test errors
min=0.000
max=0.000
avr=0.000
internal MAC transmit errors
min=0.000
max=0.000
avr=0.000
internal MAC receive errors
min=0.000
max=0.000
avr=0.000
carrier sense errors
min=0.000
max=0.000
avr=0.000

G3 data access – interactive UI

- ..the same in aggregated form – all interfaces found are hidden behind “object class name” [Interfaces]



G3 system - user interface

author: Tom Kosnar, copyright: © 2004-2014 , CESNET a.l.e.

Object description filter ..?

```
cesnet2&pasnet&bundle&
[interfa
cesnet2&pasnet&channel
&[interfa
```

case Off

negative No

apply as string

Device filter based on object description filter ..?

case Off

negative No

apply as string

Measured data filter ..?

case Off

apply as string

Others

Set tree template obj. classes only

Mark matching objects no , unmark all .

Technological interface descriptions show

Color scheme white/blue

Time period

From -1 day

To now

Show marked objects in selected views

Graphs

Width *3.0 Course organic

Height *1.0 Xport nothing

[SNMP] traffic (input, output)

[System] Availability (overall)

[System] Availability Response Time (ICMP rtt, over...

[System] ICMP echo Round Trip Time

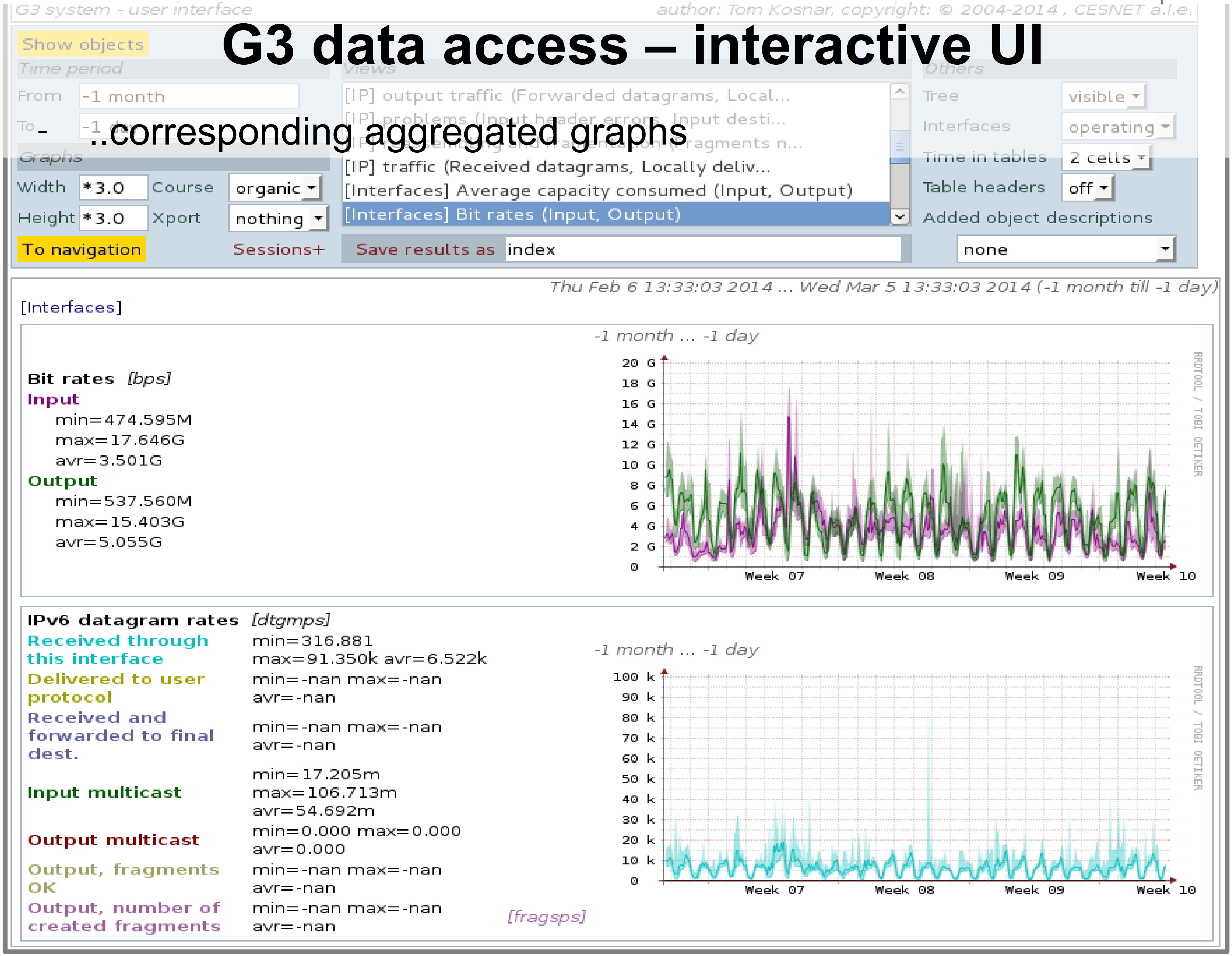
[System] ICMP echo packet loss

[System] Measured objects count

☑ [Interfaces]

G3 data access – interactive UI

..corresponding aggregated graphs



G3 system - user interface

author: Tom Kosnar, copyright: © 2004-2014 , CESNET a.l.e.

Show objects

Time period

From -1 month

To -1 day

Graphs

Width *3.0 Course organic

Height *3.0 Xport nothing

To navigation Sessions+

Views

[IP] output traffic (Forwarded datagrams, Local...
[IP] problems (Input header errors, Input desti...
[IP] reassembling and fragmentation (Fragments n...
[IP] traffic (Received datagrams, Locally deliv...
[Interfaces] Average capacity consumed (Input, Output)
[Interfaces] Bit rates (Input, Output)

Save results as index

Others

Tree visible

Interfaces operating

Time in tables 2 cells

Table headers off

Added object descriptions none

Thu Feb 6 13:33:03 2014 ... Wed Mar 5 13:33:03 2014 (-1 month till -1 day)

[Interfaces]

Bit rates *[bps]*

Input
min=474.595M
max=17.646G
avr=3.501G

Output
min=537.560M
max=15.403G
avr=5.055G

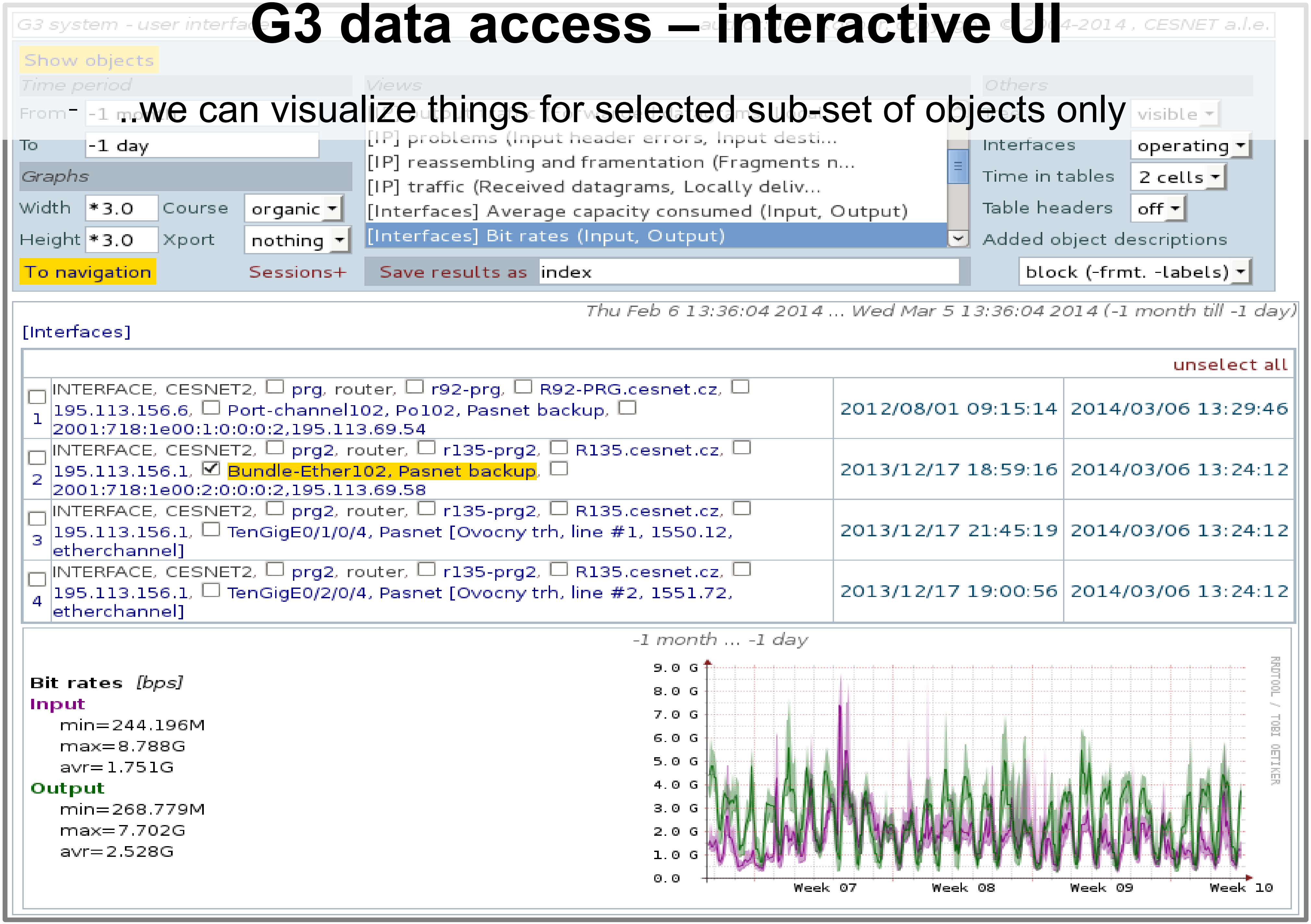
IPv6 datagram rates *[dtgmps]*

Received through this interface	min=316.881 max=91.350k avr=6.522k
Delivered to user protocol	min=-nan max=-nan avr=-nan
Received and forwarded to final dest.	min=-nan max=-nan avr=-nan
Input multicast	min=17.205m max=106.713m avr=54.692m
Output multicast	min=0.000 max=0.000 avr=0.000
Output, fragments OK	min=-nan max=-nan avr=-nan
Output, number of created fragments	min=-nan max=-nan avr=-nan

[fragsps]

G3 data access – interactive UI

..we can visualize things for selected sub-set of objects only



G3 system - user interfa… … 2…4-2014 , CESNET a.l.e.

Show objects

Time period				Views	Others	
From	-1 m…					visible
To	-1 day			[IP] problems (Input header errors, Input desti...	Interfaces	operating
Graphs				[IP] reassembling and framentation (Fragments n...	Time in tables	2 cells
Width	*3.0	Course	organic	[IP] traffic (Received datagrams, Locally deliv...	Table headers	off
Height	*3.0	Xport	nothing	[Interfaces] Average capacity consumed (Input, Output)	Added object descriptions	
				[Interfaces] Bit rates (Input, Output)		

To navigation Sessions+ Save results as index block (-frmt. -labels)

Thu Feb 6 13:36:04 2014 ... Wed Mar 5 13:36:04 2014 (-1 month till -1 day)

[Interfaces]

unselect all

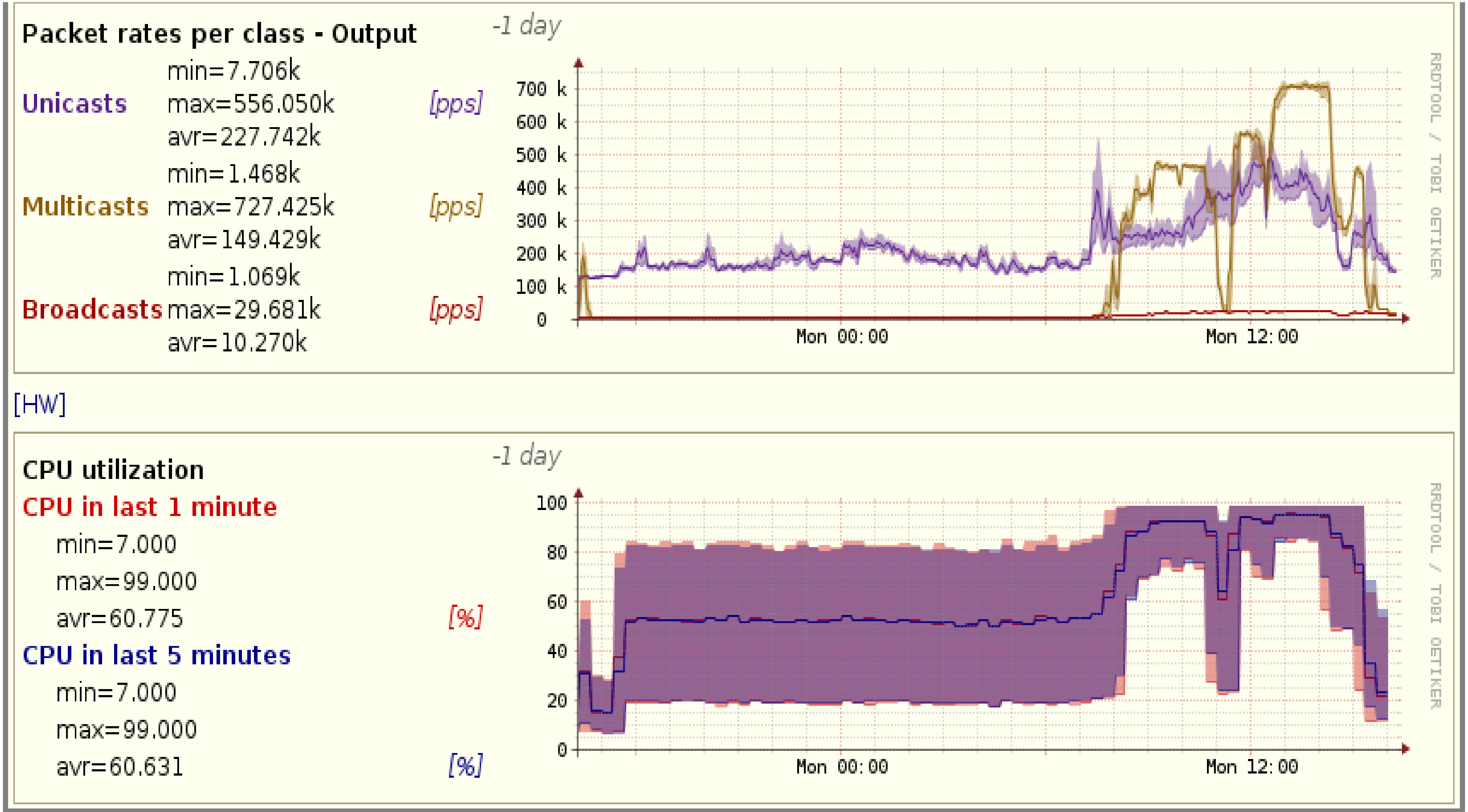
□ 1	INTERFACE, CESNET2, □ prg, router, □ r92-prg, □ R92-PRG.cesnet.cz, □ 195.113.156.6, □ Port-channel102, Po102, Pasnet backup, □ 2001:718:1e00:1:0:0:0:2,195.113.69.54	2012/08/01 09:15:14	2014/03/06 13:29:46
□ 2	INTERFACE, CESNET2, □ prg2, router, □ r135-prg2, □ R135.cesnet.cz, □ 195.113.156.1, ☑ Bundle-Ether102, Pasnet backup, □ 2001:718:1e00:2:0:0:0:2,195.113.69.58	2013/12/17 18:59:16	2014/03/06 13:24:12
□ 3	INTERFACE, CESNET2, □ prg2, router, □ r135-prg2, □ R135.cesnet.cz, □ 195.113.156.1, □ TenGigE0/1/0/4, Pasnet [Ovocny trh, line #1, 1550.12, etherchannel]	2013/12/17 21:45:19	2014/03/06 13:24:12
□ 4	INTERFACE, CESNET2, □ prg2, router, □ r135-prg2, □ R135.cesnet.cz, □ 195.113.156.1, □ TenGigE0/2/0/4, Pasnet [Ovocny trh, line #2, 1551.72, etherchannel]	2013/12/17 19:00:56	2014/03/06 13:24:12

-1 month ... -1 day

Bit rates *[bps]*
Input
min=244.196M
max=8.788G
avr=1.751G
Output
min=268.779M
max=7.702G
avr=2.528G

G3 data access – interactive UI

- ..service for users example (discovering reasons of network problems) – found relation between high CPU load and multicasts – aggregated output (all interfaces [800+] and CPUs)



Packet rates per class - Output

Unicasts	min=7.706k
	max=556.050k
	avr=227.742k
		[pps]

Multicasts	min=1.468k
	max=727.425k
	avr=149.429k
		[pps]

Broadcasts	min=1.069k
	max=29.681k
	avr=10.270k
		[pps]

[HW]

CPU utilization

CPU in last 1 minute		

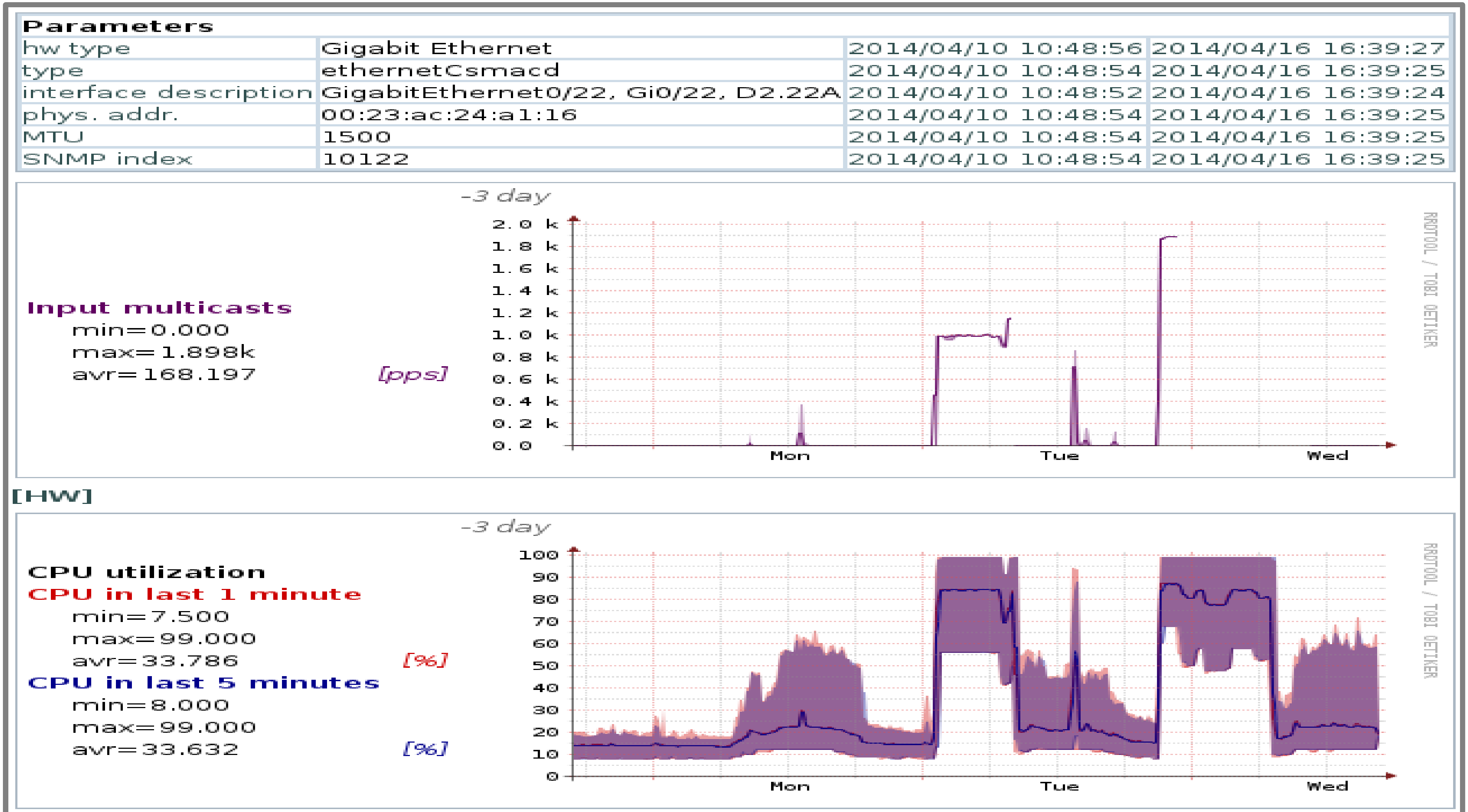
	min=7.000
	max=99.000
	avr=60.775
		[%]

CPU in last 5 minutes		

	min=7.000
	max=99.000
	avr=60.631
		[%]

G3 data access – interactive UI

- ..service for users example – finding end-user interface (deep in infrastructure) with significant incoming multicast – proven by course of aggregated CPU load (aggregated)



Parameters			
hw type	Gigabit Ethernet	2014/04/10 10:48:56	2014/04/16 16:39:27
type	ethernetCsmacd	2014/04/10 10:48:54	2014/04/16 16:39:25
interface description	GigabitEthernet0/22, Gi0/22, D2.22A	2014/04/10 10:48:52	2014/04/16 16:39:24
phys. addr.	00:23:ac:24:a1:16	2014/04/10 10:48:54	2014/04/16 16:39:25
MTU	1500	2014/04/10 10:48:54	2014/04/16 16:39:25
SNMP index	10122	2014/04/10 10:48:54	2014/04/16 16:39:25

Input multicasts
min=0.000
max=1.898k
avr=168.197 [pps]

[HW]

CPU utilization
CPU in last 1 minute
min=7.500
max=99.000
avr=33.786 [%]
CPU in last 5 minutes
min=8.000
max=99.000
avr=33.632 [%]

G3 data access

- **interactive UI** can do almost everything but...

...is demanding - user skills and knowledge (technical) → OK for network administrators, not suitable for other groups...

Have to offer:

a) **something easier to understand and handle**

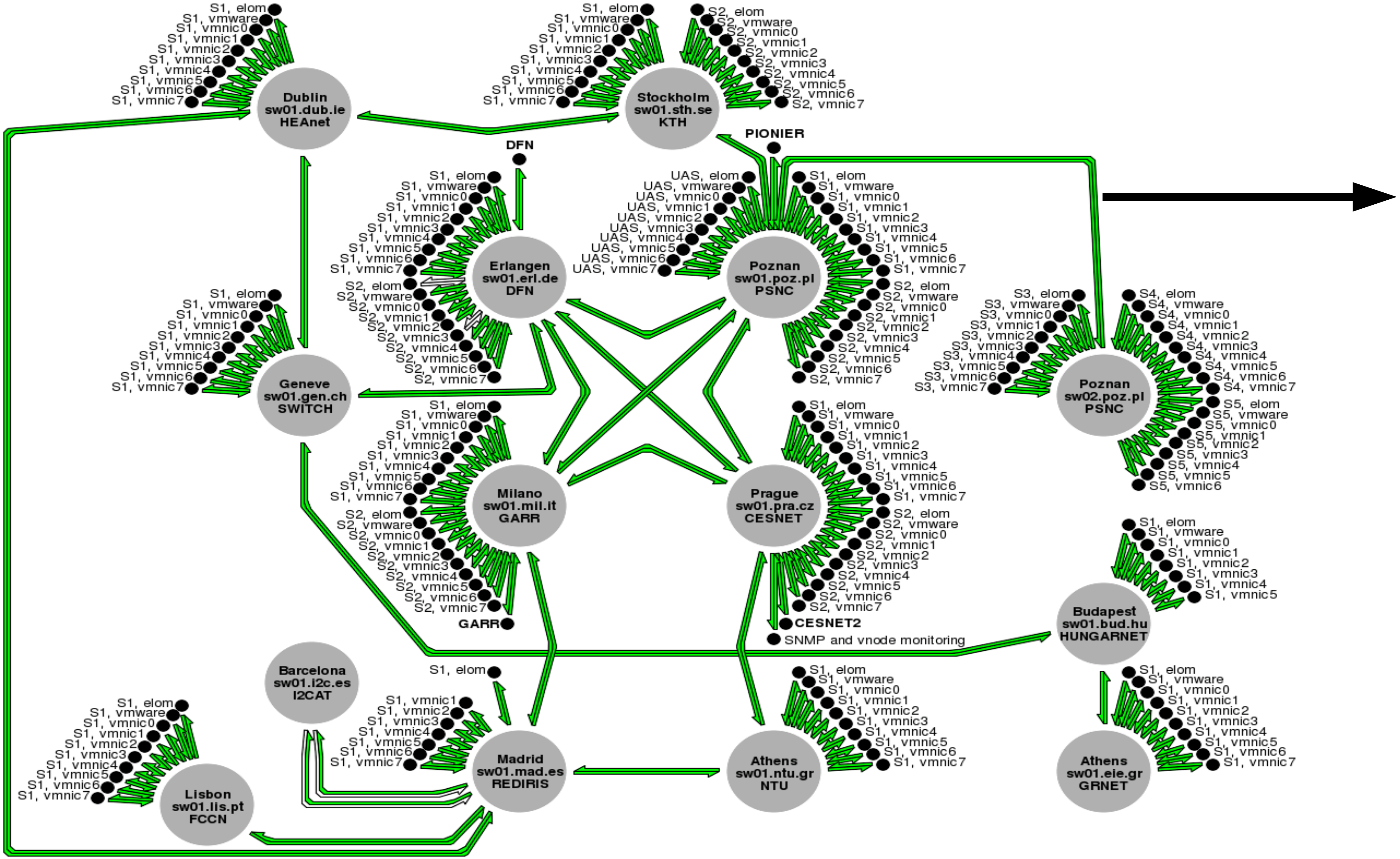
b) **something that detects anomalies**

G3 data access – Reporter

- *..something easier to understand and handle..*
- Structures of periodically generated static HTML pages
- Different views on infrastructure and its components
- Simple schema – overview page → detailed reports + configurable horizontal cross-links
- Implemented as STDIN/STDOUT control of interactive UI (real-user behavior simulation)
- *Suitable for ordinary users – intuitive, everything on-click*

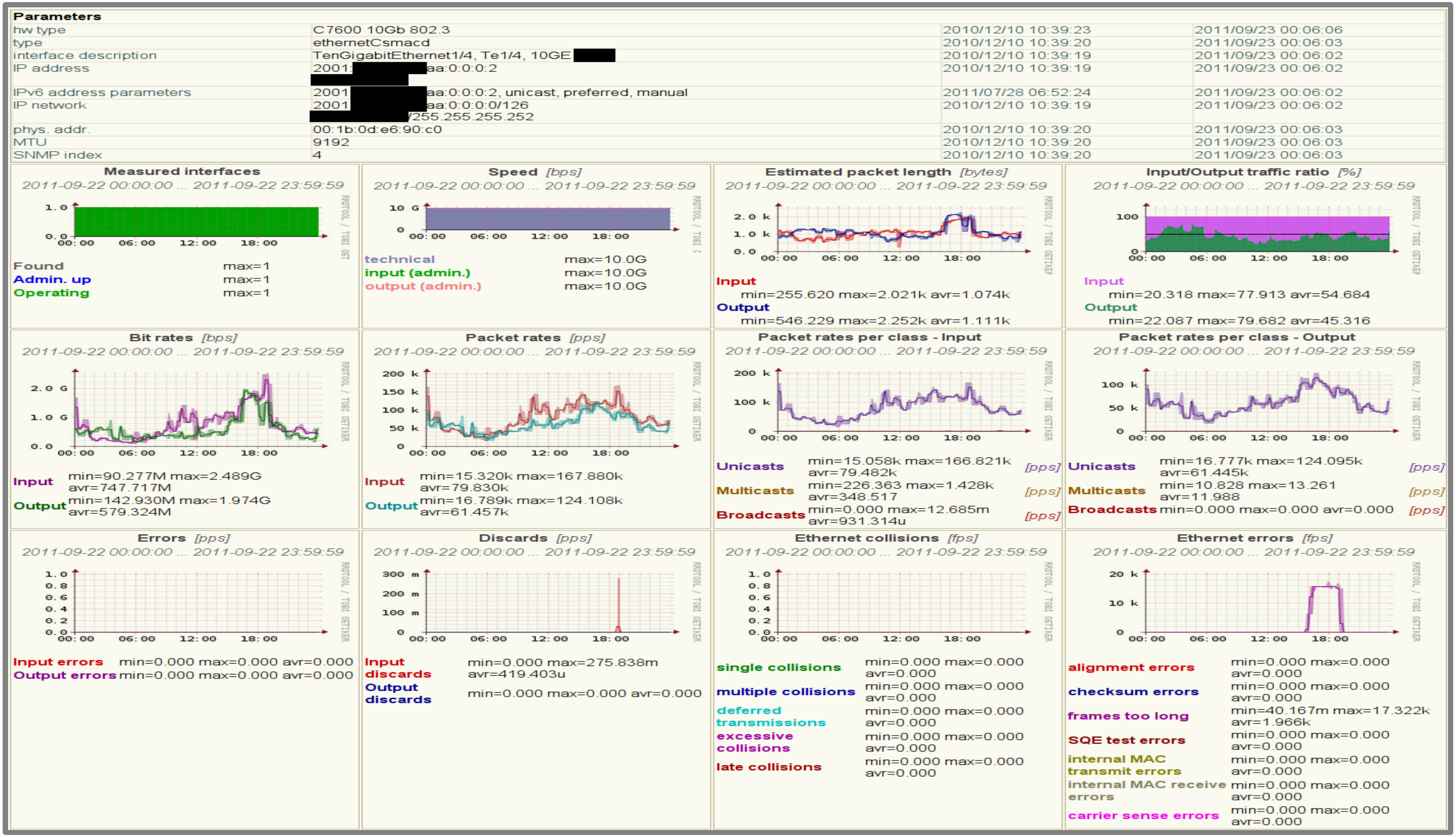
G3 data access – Reporter

- FEDERICA (FP7) monitoring example from the past ~ ”hedgehogs”



G3 data access – Reporter

- FEDERICA (FP7) monitoring example from the past



Parameters			
hw type	C7600 10Gb 802.3	2010/12/10 10:39:23	2011/09/23 00:06:06
type	ethernetCsmacd	2010/12/10 10:39:20	2011/09/23 00:06:03
interface description	TenGigabitEthernet1/4, Te1/4, 10GE [redacted]	2010/12/10 10:39:19	2011/09/23 00:06:02
IP address	2001:[redacted]aa:0:0:0:2	2010/12/10 10:39:19	2011/09/23 00:06:02
IPv6 address parameters	2001[redacted]aa:0:0:0:2, unicast, preferred, manual	2011/07/28 06:52:24	2011/09/23 00:06:02
IP network	2001[redacted]aa:0:0:0:0/126 [redacted]/255.255.255.252	2010/12/10 10:39:19	2011/09/23 00:06:02
phys. addr.	00:1b:0d:e6:90:c0	2010/12/10 10:39:20	2011/09/23 00:06:03
MTU	9192	2010/12/10 10:39:20	2011/09/23 00:06:03
SNMP index	4	2010/12/10 10:39:20	2011/09/23 00:06:03

Measured interfaces
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Found max=1
Admin. up max=1
Operating max=1

Speed *[bps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

technical max=10.0G
input (admin.) max=10.0G
output (admin.) max=10.0G

Estimated packet length *[bytes]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input
min=255.620 max=2.021k avr=1.074k
Output
min=546.229 max=2.252k avr=1.111k

Input/Output traffic ratio *[%]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input
min=20.318 max=77.913 avr=54.684
Output
min=22.087 max=79.682 avr=45.316

Bit rates *[bps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input min=90.277M max=2.489G avr=747.717M
Output min=142.930M max=1.974G avr=579.324M

Packet rates *[pps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input min=15.320k max=167.880k avr=79.830k
Output min=16.789k max=124.108k avr=61.457k

Packet rates per class - Input
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Unicasts min=15.058k max=166.821k avr=79.482k *[pps]*
Multicasts min=226.363 max=1.428k avr=348.517 *[pps]*
Broadcasts min=0.000 max=12.685m avr=931.314u *[pps]*

Packet rates per class - Output
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Unicasts min=16.777k max=124.095k avr=61.445k *[pps]*
Multicasts min=10.828 max=13.261 avr=11.988 *[pps]*
Broadcasts min=0.000 max=0.000 avr=0.000 *[pps]*

Errors *[pps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input errors min=0.000 max=0.000 avr=0.000
Output errors min=0.000 max=0.000 avr=0.000

Discards *[pps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

Input discards min=0.000 max=275.838m avr=419.403u
Output discards min=0.000 max=0.000 avr=0.000

Ethernet collisions *[fps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

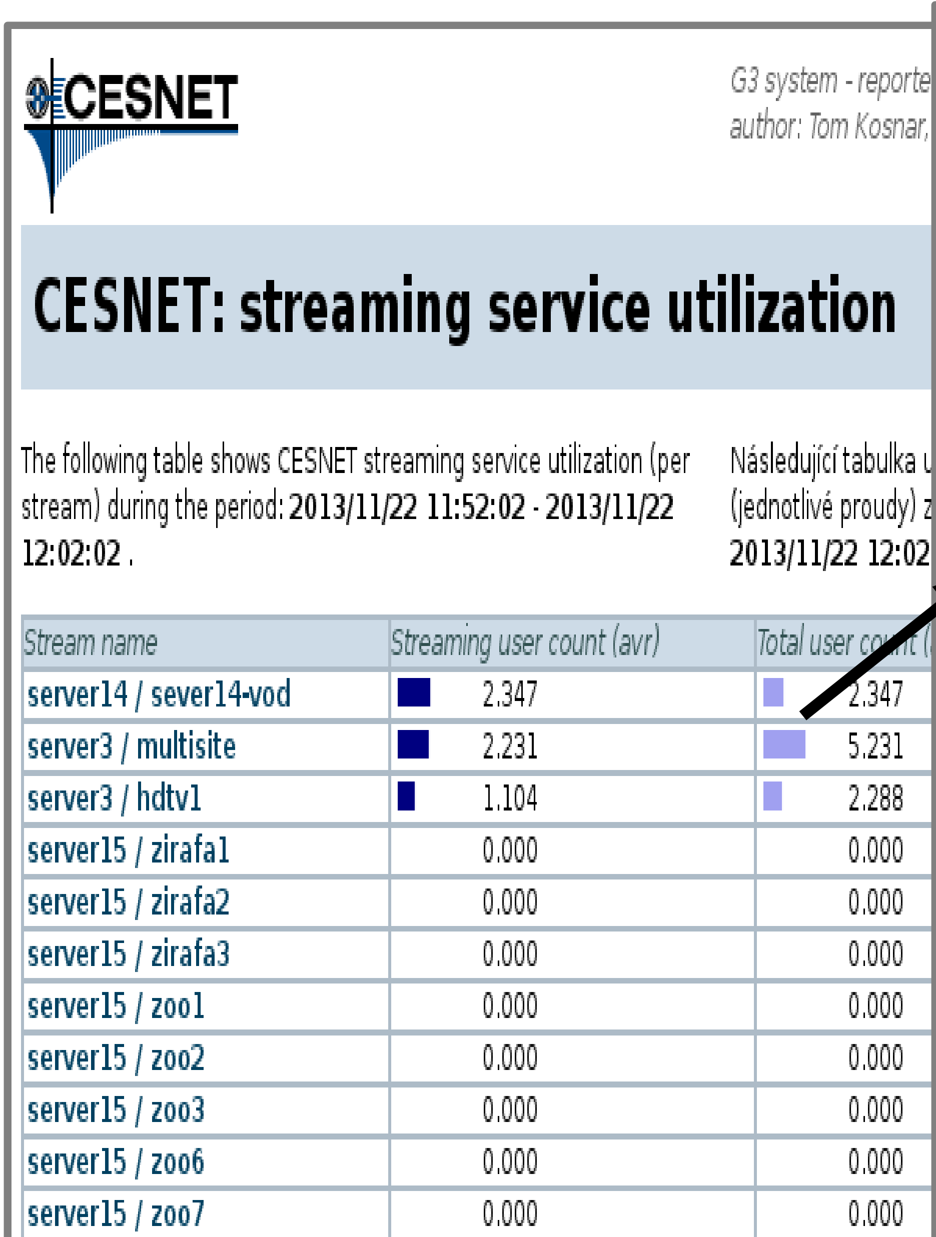
single collisions min=0.000 max=0.000 avr=0.000
multiple collisions min=0.000 max=0.000 avr=0.000
deferred transmissions min=0.000 max=0.000 avr=0.000
excessive collisions min=0.000 max=0.000 avr=0.000
late collisions min=0.000 max=0.000 avr=0.000

Ethernet errors *[fps]*
2011-09-22 00:00:00 ... 2011-09-22 23:59:59

alignment errors min=0.000 max=0.000 avr=0.000
checksum errors min=0.000 max=0.000 avr=0.000
frames too long min=40.167m max=17.322k avr=1.966k
SQE test errors min=0.000 max=0.000 avr=0.000
internal MAC transmit errors min=0.000 max=0.000 avr=0.000
internal MAC receive errors min=0.000 max=0.000 avr=0.000
carrier sense errors min=0.000 max=0.000 avr=0.000

G3 data access – Reporter

- CESNET streaming service utilization example (no SNMP)



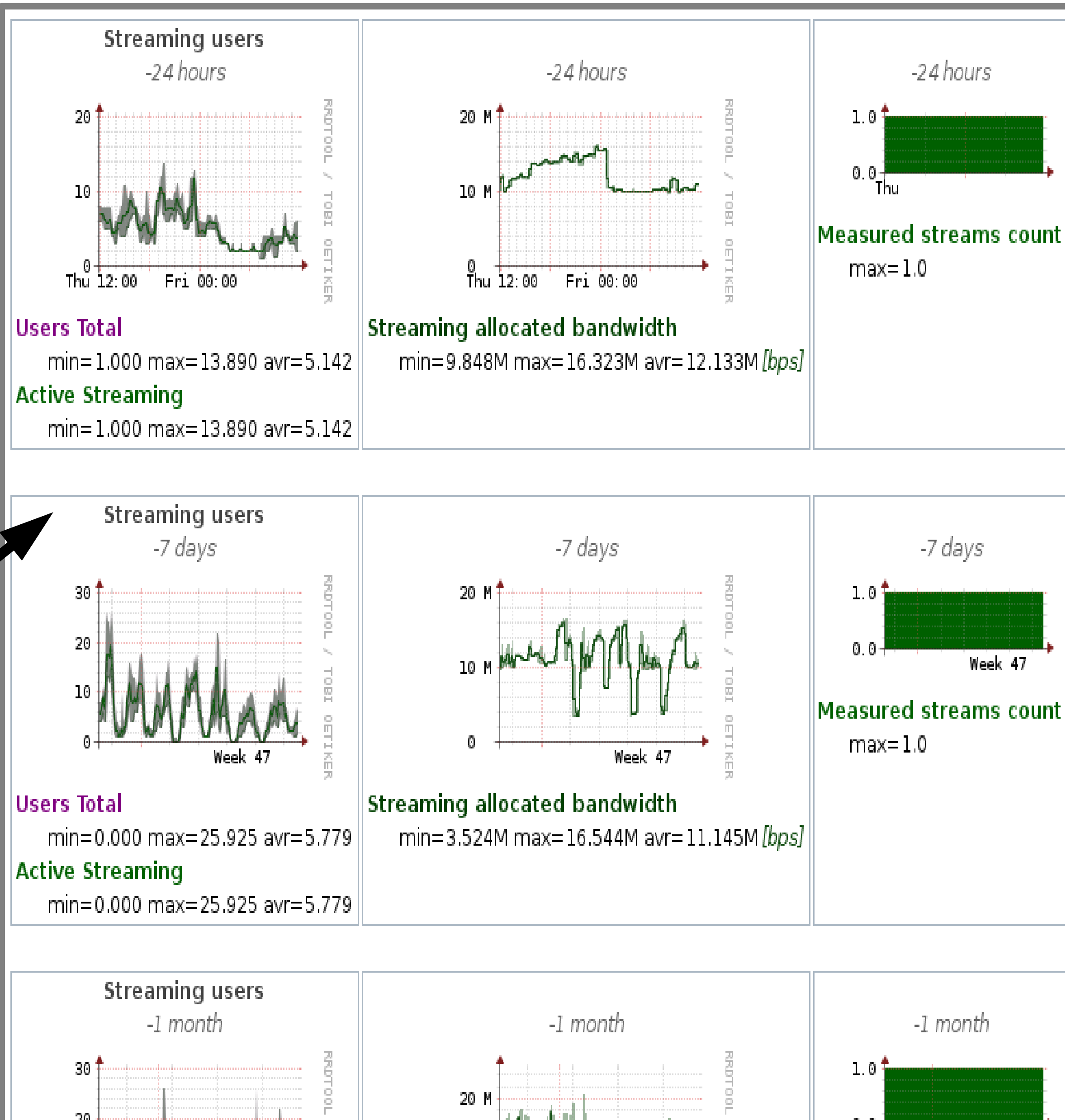
G3 system - reporte
author: Tom Kosnar,

CESNET: streaming service utilization

The following table shows CESNET streaming service utilization (per stream) during the period: **2013/11/22 11:52:02 - 2013/11/22 12:02:02** .

Následující tabulka u (jednotlivé proudy) z **2013/11/22 12:02**

Stream name	Streaming user count (avr)	Total user count (
server14 / sever14-vod	2.347	2.347
server3 / multisite	2.231	5.231
server3 / hdtv1	1.104	2.288
server15 / zirafa1	0.000	0.000
server15 / zirafa2	0.000	0.000
server15 / zirafa3	0.000	0.000
server15 / zoo1	0.000	0.000
server15 / zoo2	0.000	0.000
server15 / zoo3	0.000	0.000
server15 / zoo6	0.000	0.000
server15 / zoo7	0.000	0.000



Streaming users
-24 hours

Users Total
min=1.000 max=13.890 avr=5.142
Active Streaming
min=1.000 max=13.890 avr=5.142

-24 hours

Streaming allocated bandwidth
min=9.848M max=16.323M avr=12.133M *[bps]*

-24 hours

Measured streams count
max=1.0

Streaming users
-7 days

Users Total
min=0.000 max=25.925 avr=5.779
Active Streaming
min=0.000 max=25.925 avr=5.779

-7 days

Streaming allocated bandwidth
min=3.524M max=16.544M avr=11.145M *[bps]*

-7 days

Measured streams count
max=1.0

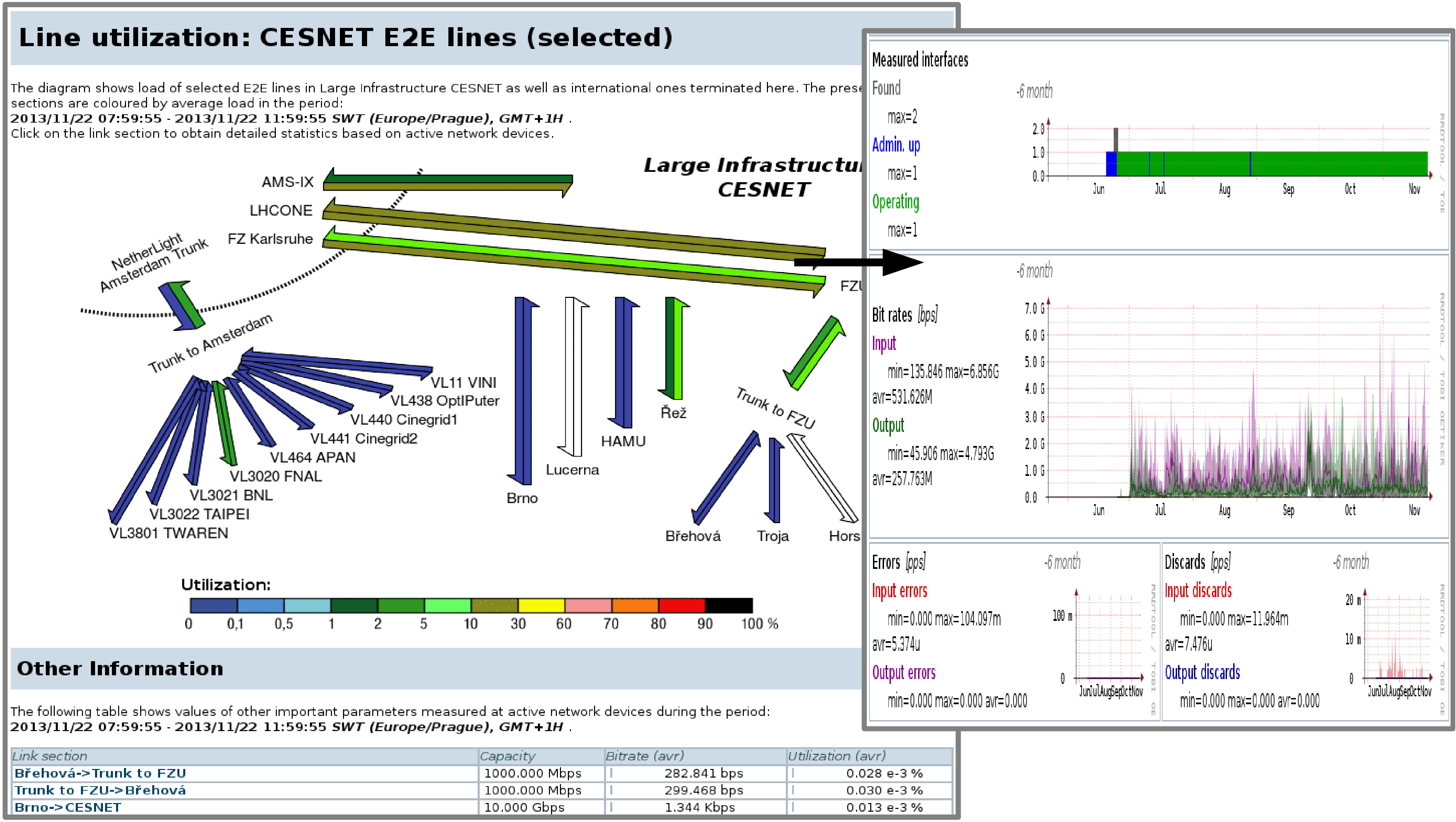
Streaming users
-1 month

-1 month

-1 month

G3 data access – Reporter

- Selected E2E services @ CESNET example



Line utilization: CESNET E2E lines (selected)

The diagram shows load of selected E2E lines in Large Infrastructure CESNET as well as international ones terminated here. The prese
sections are coloured by average load in the period:
2013/11/22 07:59:55 - 2013/11/22 11:59:55 ***SWT (Europe/Prague), GMT+1H*** .
Click on the link section to obtain detailed statistics based on active network devices.

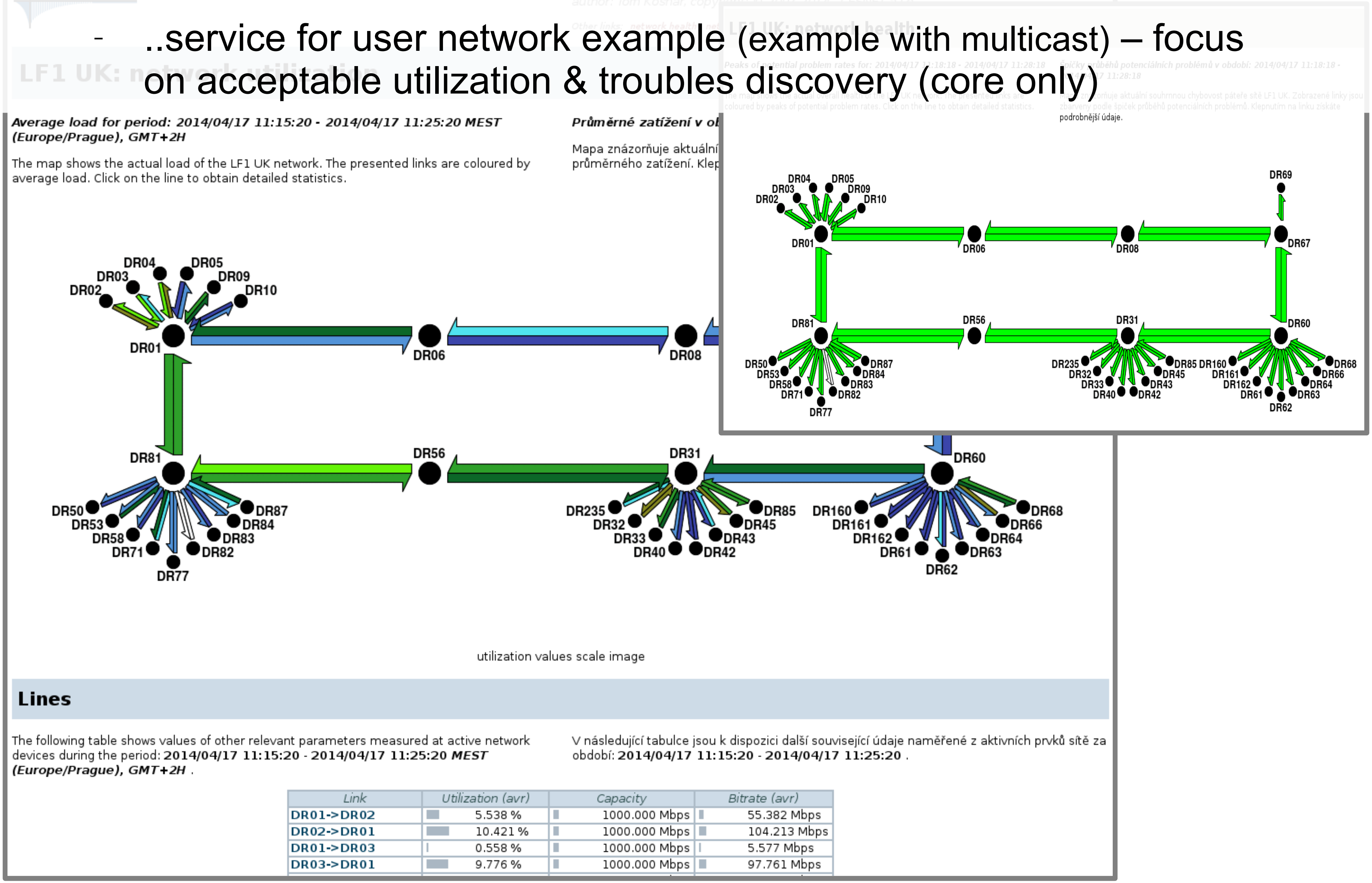
Other Information

The following table shows values of other important parameters measured at active network devices during the period:
2013/11/22 07:59:55 - 2013/11/22 11:59:55 ***SWT (Europe/Prague), GMT+1H*** .

Link section	*Capacity*	*Bitrate (avr)*	*Utilization (avr)*
Břehová->Trunk to FZU	1000.000 Mbps	282.841 bps	0.028 e-3 %
Trunk to FZU->Břehová	1000.000 Mbps	299.468 bps	0.030 e-3 %
Brno->CESNET	10.000 Gbps	1.344 Kbps	0.013 e-3 %

G3 data access – Reporter

- ..service for user network example (example with multicast) – focus on acceptable utilization & troubles discovery (core only)



G3 system - reporter
author: Tom Kosnar, copyright: © 2007-2014 , CESNET z.s.p.o.

Other links: network health ...

LF1 UK: network utilization

Average load for period: 2014/04/17 11:15:20 - 2014/04/17 11:25:20 MEST (Europe/Prague), GMT+2H

The map shows the actual load of the LF1 UK network. The presented links are coloured by average load. Click on the line to obtain detailed statistics.

Průměrné zatížení v ob

Mapa znázorňuje aktuální ... průměrného zatížení. Klep...

utilization values scale image

Lines

The following table shows values of other relevant parameters measured at active network devices during the period: **2014/04/17 11:15:20 - 2014/04/17 11:25:20** ***MEST (Europe/Prague), GMT+2H*** .

V následující tabulce jsou k dispozici další související údaje naměřené z aktivních prvků sítě za období: **2014/04/17 11:15:20 - 2014/04/17 11:25:20** .

Link	Utilization (avr)	Capacity	Bitrate (avr)
DR01->DR02	5.538 %	1000.000 Mbps	55.382 Mbps
DR02->DR01	10.421 %	1000.000 Mbps	104.213 Mbps
DR01->DR03	0.558 %	1000.000 Mbps	5.577 Mbps
DR03->DR01	9.776 %	1000.000 Mbps	97.761 Mbps

LF1 UK: network health

Peaks of potential problem rates for: 2014/04/17 11:18:18 - 2014/04/17 11:28:18

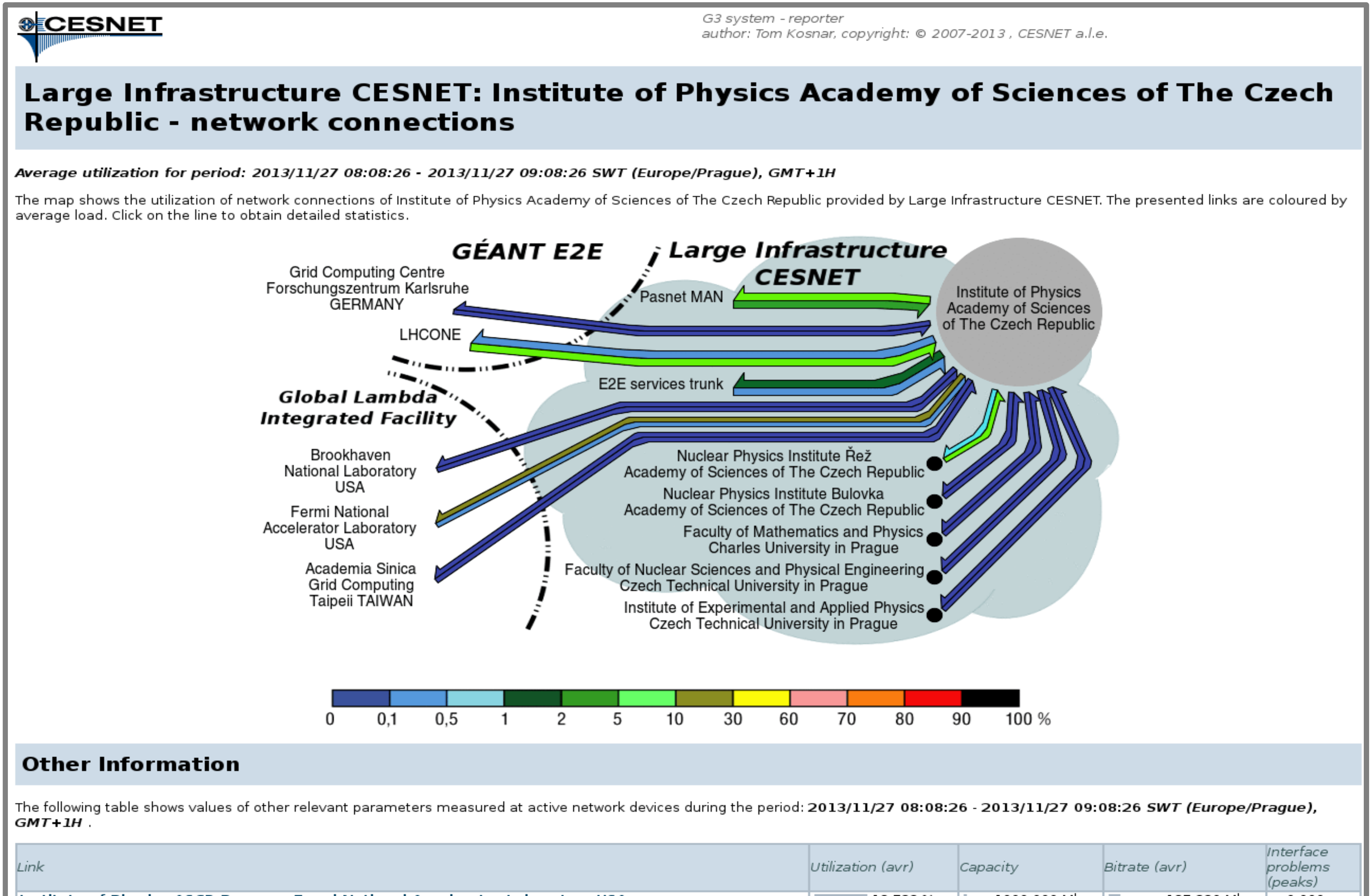
The map shows the actual overall health of the LF1 UK network. The presented links are coloured by peaks of potential problem rates. Click on the line to obtain detailed statistics.

Špičky průběhů potenciálních problémů v období: 2014/04/17 11:18:18 - 2014/04/17 11:28:18

Mapa znázorňuje aktuální souhrnnou chybovost páteře sítě LF1 UK. Zobrazené linky jsou zbarveny podle špiček průběhů potenciálních problémů. Klepnutím na linku získáte podrobnější údaje.

G3 data access – Reporter

- Service for user network example – utilization overview



G3 system - reporter
author: Tom Kosnar, copyright: © 2007-2013 , CESNET a.l.e.

Large Infrastructure CESNET: Institute of Physics Academy of Sciences of The Czech Republic - network connections

Average utilization for period: 2013/11/27 08:08:26 - 2013/11/27 09:08:26 SWT (Europe/Prague), GMT+1H

The map shows the utilization of network connections of Institute of Physics Academy of Sciences of The Czech Republic provided by Large Infrastructure CESNET. The presented links are coloured by average load. Click on the line to obtain detailed statistics.

GÉANT E2E
Large Infrastructure CESNET
Grid Computing Centre Forschungszentrum Karlsruhe GERMANY
LHCONE
Pasnet MAN
Institute of Physics Academy of Sciences of The Czech Republic
E2E services trunk
Global Lambda Integrated Facility
Brookhaven National Laboratory USA
Fermi National Accelerator Laboratory USA
Academia Sinica Grid Computing Taipeii TAIWAN
Nuclear Physics Institute Řež Academy of Sciences of The Czech Republic
Nuclear Physics Institute Bulovka Academy of Sciences of The Czech Republic
Faculty of Mathematics and Physics Charles University in Prague
Faculty of Nuclear Sciences and Physical Engineering Czech Technical University in Prague
Institute of Experimental and Applied Physics Czech Technical University in Prague
0
0,1
0,5
1
2
5
10
30
60
70
80
90
100 %

Other Information

The following table shows values of other relevant parameters measured at active network devices during the period: **2013/11/27 08:08:26 - 2013/11/27 09:08:26** ***SWT (Europe/Prague), GMT+1H*** .

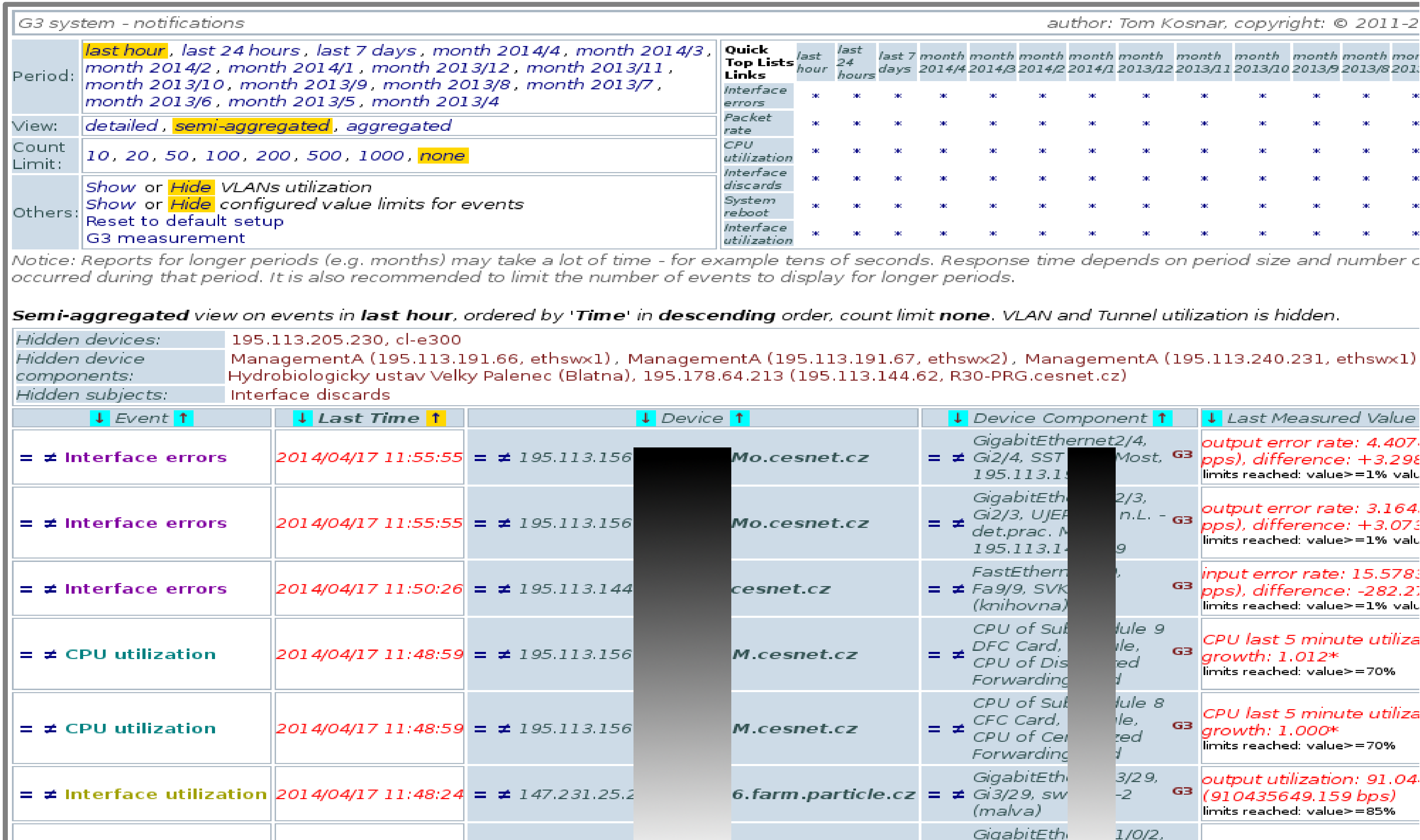
Link	*Utilization (avr)*	*Capacity*	*Bitrate (avr)*	*Interface problems (peaks)*

G3 data access – event visualizer & notifier

- *..something that detects anomalies..*
- Based on on-fly checking measured values (in measurement core) against configured limits *(absolute value, gradients, changes,...)*
  - Configured limits either global or device based
  - Web based interface (HTML output), interactive
  - Plain-text output *(with configured filters etc..)* as input for Nagios/Icinga/other probes and similar
  - Specific configuration options (filtering ~ selected interfaces, devices, event types) for specific users/user groups

G3 data access – event visualizer & notifier

- Typical output example



G3 system - notifications author: Tom Kosnar, copyright: © 2011-2

Period:	last hour, last 24 hours, last 7 days, month 2014/4, month 2014/3, month 2014/2, month 2014/1, month 2013/12, month 2013/11, month 2013/10, month 2013/9, month 2013/8, month 2013/7, month 2013/6, month 2013/5, month 2013/4
View:	detailed, semi-aggregated, aggregated
Count Limit:	10, 20, 50, 100, 200, 500, 1000, none
Others:	Show or Hide VLANs utilization Show or Hide configured value limits for events Reset to default setup G3 measurement

Quick Top Lists Links	last hour	last 24 hours	last 7 days	month 2014/4	month 2014/3	month 2014/2	month 2014/1	month 2013/12	month 2013/11	month 2013/10	month 2013/9	month 2013/8	mor 201
Interface errors	*	*	*	*	*	*	*	*	*	*	*	*	*
Packet rate	*	*	*	*	*	*	*	*	*	*	*	*	*
CPU utilization	*	*	*	*	*	*	*	*	*	*	*	*	*
Interface discards	*	*	*	*	*	*	*	*	*	*	*	*	*
System reboot	*	*	*	*	*	*	*	*	*	*	*	*	*
Interface utilization	*	*	*	*	*	*	*	*	*	*	*	*	*

Notice: Reports for longer periods (e.g. months) may take a lot of time - for example tens of seconds. Response time depends on period size and number c occurred during that period. It is also recommended to limit the number of events to display for longer periods.

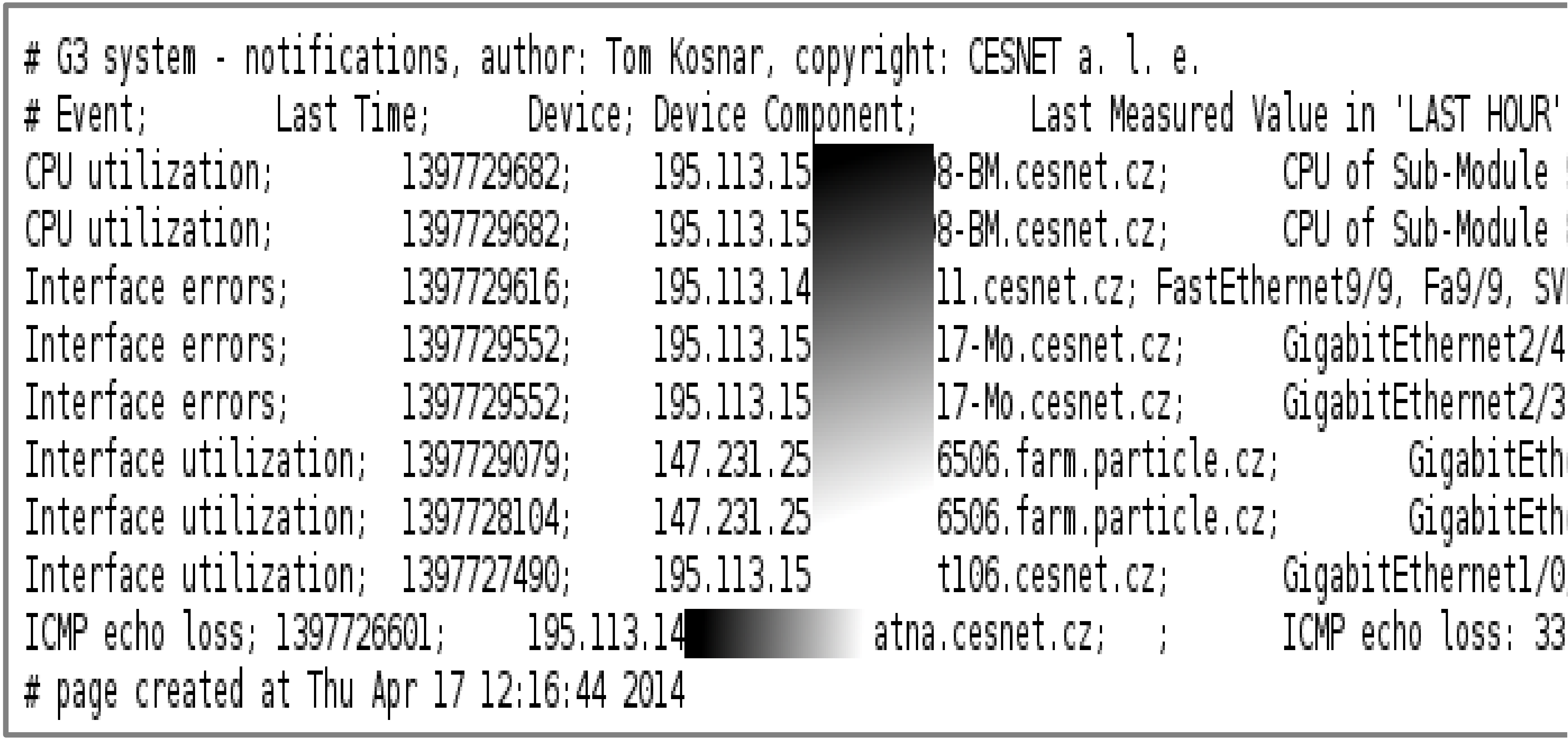
Semi-aggregated view on events in **last hour**, ordered by '**Time**' in **descending** order, count limit **none**. VLAN and Tunnel utilization is hidden.

Hidden devices:	195.113.205.230, cl-e300
Hidden device components:	ManagementA (195.113.191.66, ethswx1), ManagementA (195.113.191.67, ethswx2), ManagementA (195.113.240.231, ethswx1) Hydrobiologicky ustav Velky Palenec (Blatna), 195.178.64.213 (195.113.144.62, R30-PRG.cesnet.cz)
Hidden subjects:	Interface discards

↓ Event ↑	↓ Last Time ↑	↓ Device ↑	↓ Device Component ↑	↓ Last Measured Value
= ≠ Interface errors	2014/04/17 11:55:55	= ≠ 195.113.156 [redacted] Mo.cesnet.cz	= ≠ GigabitEthernet2/4, Gi2/4, SST [redacted] Most, 195.113.1 G3	output error rate: 4.407 pps), difference: +3.298 limits reached: value>=1% valu
= ≠ Interface errors	2014/04/17 11:55:55	= ≠ 195.113.156 [redacted] Mo.cesnet.cz	= ≠ GigabitEth [redacted] 2/3, Gi2/3, UJEP [redacted] n.L. - det.prac. N [redacted] 195.113.1 [redacted] 9 G3	output error rate: 3.164 pps), difference: +3.073 limits reached: value>=1% valu
= ≠ Interface errors	2014/04/17 11:50:26	= ≠ 195.113.144 [redacted] cesnet.cz	= ≠ FastEthern [redacted], Fa9/9, SVK [redacted] (knihovna) G3	input error rate: 15.578 pps), difference: -282.2 limits reached: value>=1% valu
= ≠ CPU utilization	2014/04/17 11:48:59	= ≠ 195.113.156 [redacted] M.cesnet.cz	= ≠ CPU of Sub [redacted] dule 9 DFC Card, [redacted] le, CPU of Dis [redacted] ted Forwarding [redacted] d G3	CPU last 5 minute utiliza growth: 1.012* limits reached: value>=70%
= ≠ CPU utilization	2014/04/17 11:48:59	= ≠ 195.113.156 [redacted] M.cesnet.cz	= ≠ CPU of Sub [redacted] dule 8 CFC Card, [redacted] le, CPU of Cen [redacted] zed Forwarding [redacted] d G3	CPU last 5 minute utiliza growth: 1.000* limits reached: value>=70%
= ≠ Interface utilization	2014/04/17 11:48:24	= ≠ 147.231.25.2 [redacted] 6.farm.particle.cz	= ≠ GigabitEth [redacted] 3/29, Gi3/29, sw [redacted] -2 (malva) G3	output utilization: 91.04 (910435649.159 bps) limits reached: value>=85%
		[redacted]	GigabitEth [redacted] 1/0/2,	

G3 data access – event visualizer & notifier

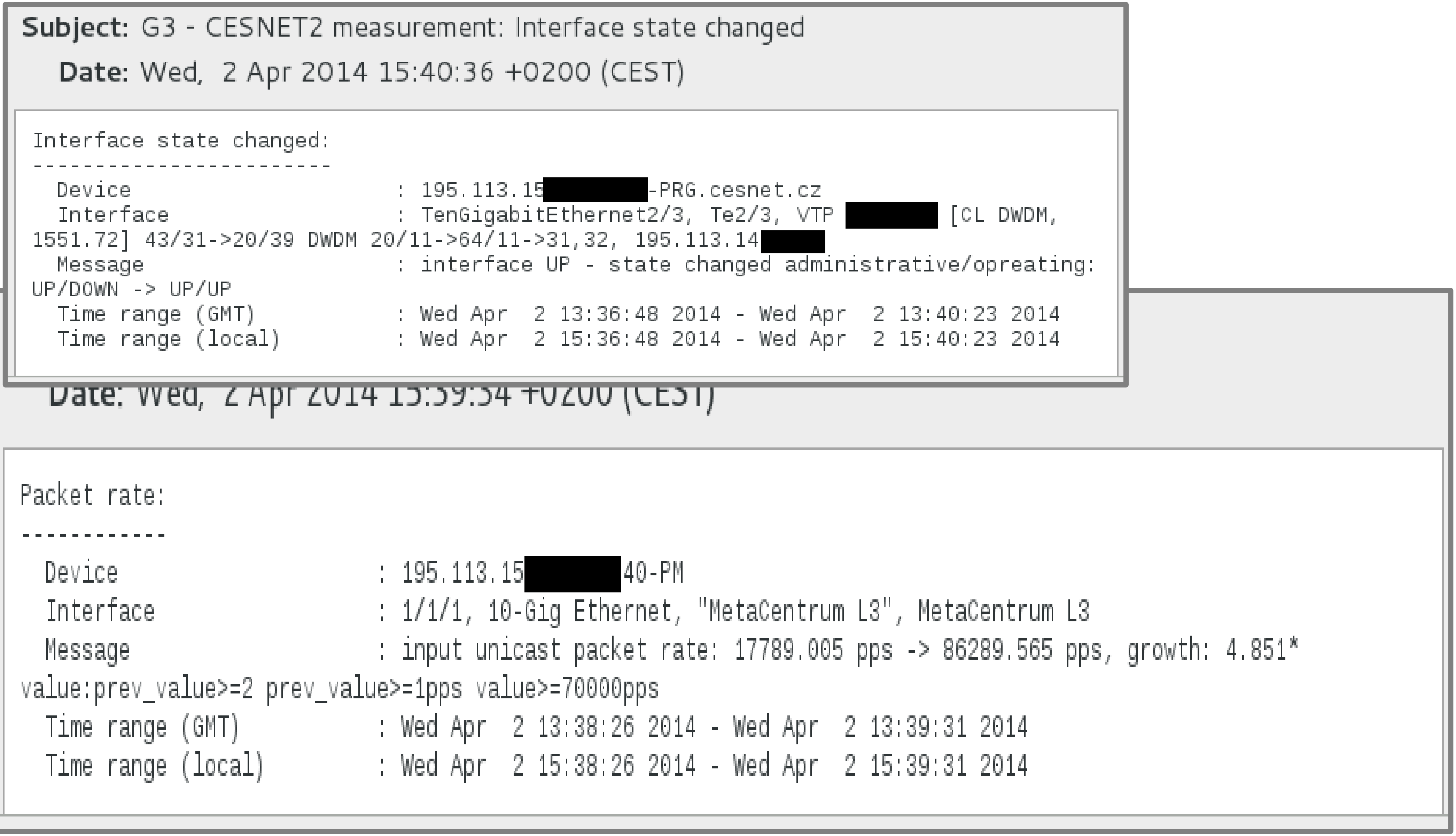
- Plain-text output example
  - Optional filtering available for further processing ~ Nagios/Icinga



```
# G3 system - notifications, author: Tom Kosnar, copyright: CESNET a. l. e.
# Event;          Last Time;      Device; Device Component;        Last Measured Value in 'LAST HOUR'
CPU utilization;          1397729682;     195.113.15[redacted]8-BM.cesnet.cz;        CPU of Sub-Module
CPU utilization;          1397729682;     195.113.15          8-BM.cesnet.cz;        CPU of Sub-Module
Interface errors;         1397729616;     195.113.14          11.cesnet.cz; FastEthernet9/9, Fa9/9, SV
Interface errors;         1397729552;     195.113.15          17-Mo.cesnet.cz;       GigabitEthernet2/4
Interface errors;         1397729552;     195.113.15          17-Mo.cesnet.cz;       GigabitEthernet2/3
Interface utilization;  1397729079;     147.231.25          6506.farm.particle.cz;         GigabitEth
Interface utilization;  1397728104;     147.231.25          6506.farm.particle.cz;         GigabitEth
Interface utilization;  1397727490;     195.113.15          t106.cesnet.cz;        GigabitEthernet1/0
ICMP echo loss; 1397726601;     195.113.14[redacted]atna.cesnet.cz;    ;        ICMP echo loss: 33
# page created at Thu Apr 17 12:16:44 2014
```

G3 data access – event visualizer & notifier

- Notification messages (optional)



Subject: G3 - CESNET2 measurement: Interface state changed

Date: Wed, 2 Apr 2014 15:40:36 +0200 (CEST)

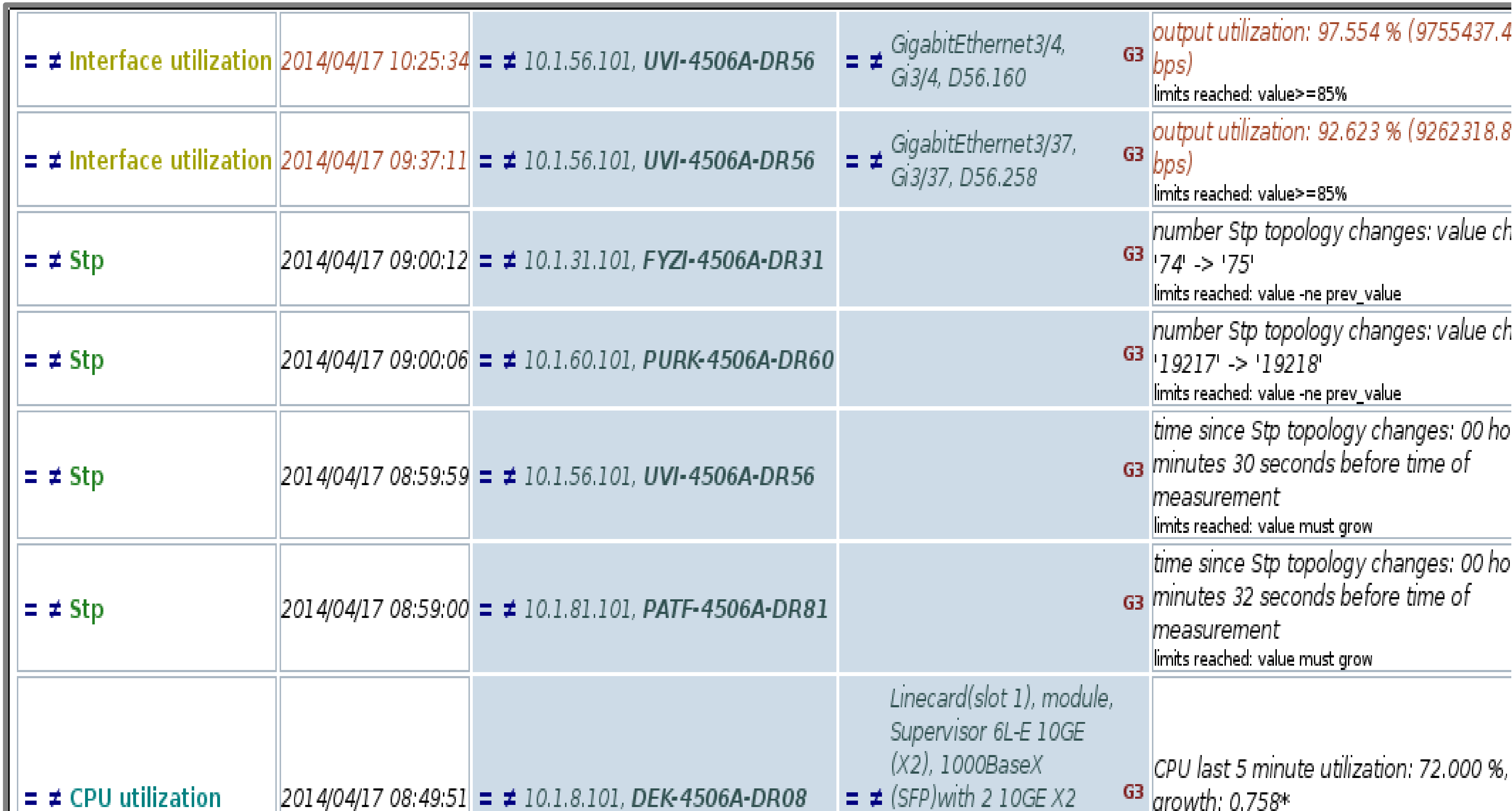
```
Interface state changed:
------------------------
  Device                      : 195.113.15[redacted]-PRG.cesnet.cz
  Interface                   : TenGigabitEthernet2/3, Te2/3, VTP [redacted] [CL DWDM,
1551.72] 43/31->20/39 DWDM 20/11->64/11->31,32, 195.113.14[redacted]
  Message                     : interface UP - state changed administrative/opreating:
UP/DOWN -> UP/UP
  Time range (GMT)            : Wed Apr  2 13:36:48 2014 - Wed Apr  2 13:40:23 2014
  Time range (local)          : Wed Apr  2 15:36:48 2014 - Wed Apr  2 15:40:23 2014
```

Date: Wed, 2 Apr 2014 15:39:34 +0200 (CEST)

```
Packet rate:
------------
  Device                      : 195.113.15[redacted]40-PM
  Interface                   : 1/1/1, 10-Gig Ethernet, "MetaCentrum L3", MetaCentrum L3
  Message                     : input unicast packet rate: 17789.005 pps -> 86289.565 pps, growth: 4.851*
value:prev_value>=2 prev_value>=1pps value>=70000pps
  Time range (GMT)            : Wed Apr  2 13:38:26 2014 - Wed Apr  2 13:39:31 2014
  Time range (local)          : Wed Apr  2 15:38:26 2014 - Wed Apr  2 15:39:31 2014
```

G3 data access – event visualizer & notifier

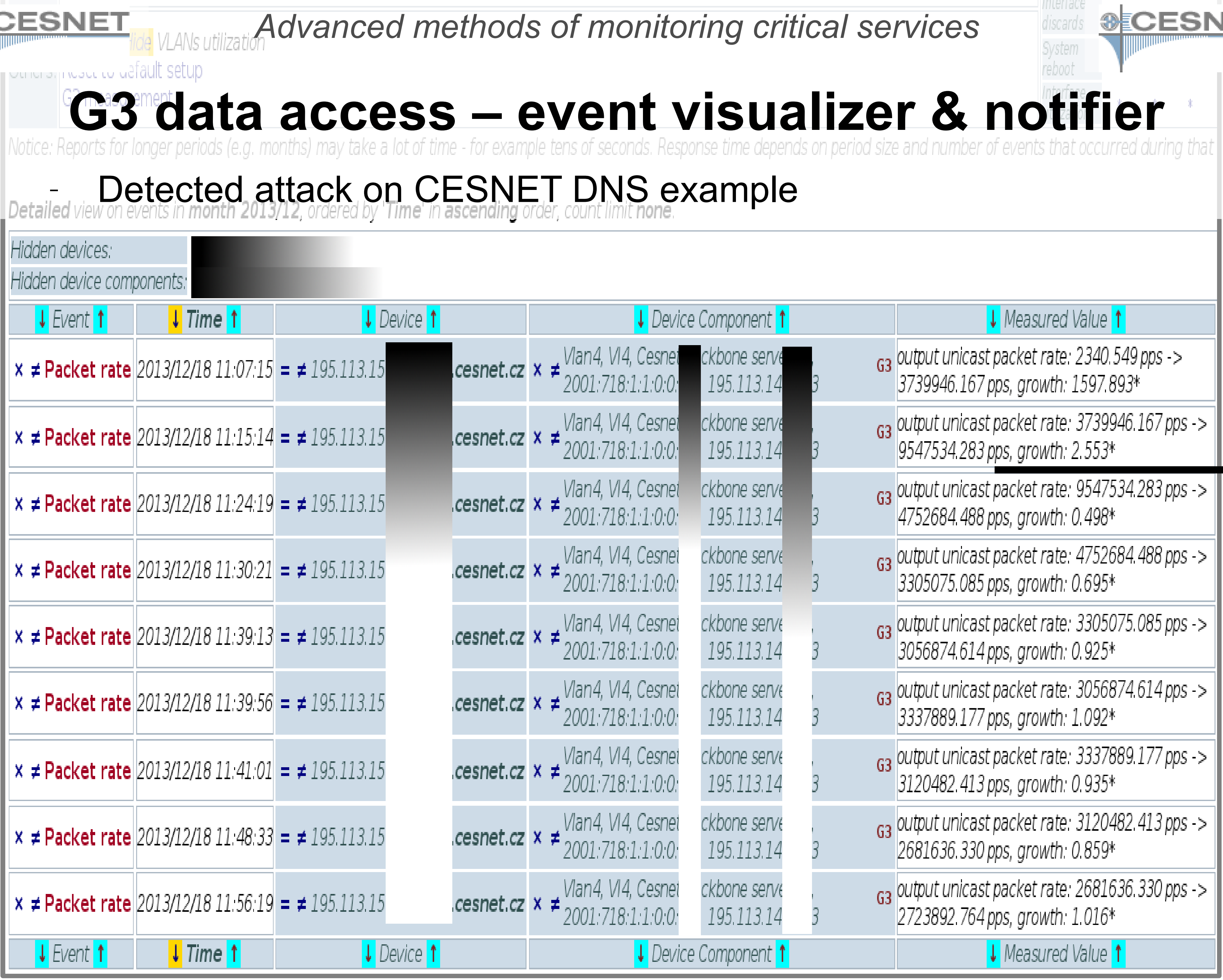
- ..service for user network – LAN example ..different things may become important ~ Stp



= ≠ Interface utilization	2014/04/17 10:25:34	= ≠ 10.1.56.101, UVI-4506A-DR56	= ≠ GigabitEthernet3/4, Gi3/4, D56.160	G3	output utilization: 97.554 % (9755437.4 bps) limits reached: value>=85%
= ≠ Interface utilization	2014/04/17 09:37:11	= ≠ 10.1.56.101, UVI-4506A-DR56	= ≠ GigabitEthernet3/37, Gi3/37, D56.258	G3	output utilization: 92.623 % (9262318.8 bps) limits reached: value>=85%
= ≠ Stp	2014/04/17 09:00:12	= ≠ 10.1.31.101, FYZI-4506A-DR31		G3	number Stp topology changes: value ch '74' -> '75' limits reached: value -ne prev_value
= ≠ Stp	2014/04/17 09:00:06	= ≠ 10.1.60.101, PURK-4506A-DR60		G3	number Stp topology changes: value ch '19217' -> '19218' limits reached: value -ne prev_value
= ≠ Stp	2014/04/17 08:59:59	= ≠ 10.1.56.101, UVI-4506A-DR56		G3	time since Stp topology changes: 00 ho minutes 30 seconds before time of measurement limits reached: value must grow
= ≠ Stp	2014/04/17 08:59:00	= ≠ 10.1.81.101, PATF-4506A-DR81		G3	time since Stp topology changes: 00 ho minutes 32 seconds before time of measurement limits reached: value must grow
= ≠ CPU utilization	2014/04/17 08:49:51	= ≠ 10.1.8.101, DEK-4506A-DR08	= ≠ Linecard(slot 1), module, Supervisor 6L-E 10GE (X2), 1000BaseX (SFP)with 2 10GE X2	G3	CPU last 5 minute utilization: 72.000 %, growth: 0.758*

G3 data access – event visualizer & notifier

- Detected attack on CESNET DNS example



Notice: Reports for longer periods (e.g. months) may take a lot of time - for example tens of seconds. Response time depends on period size and number of events that occurred during that

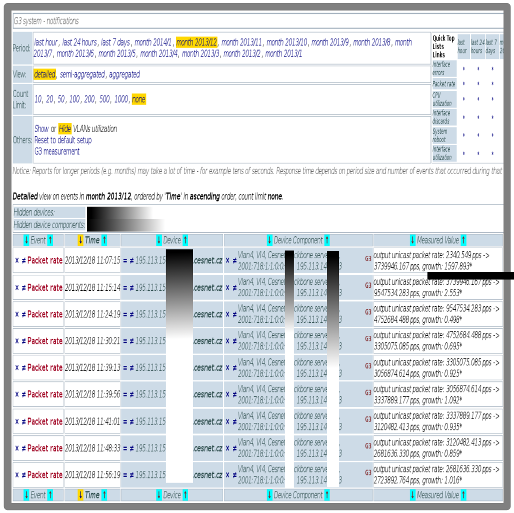
Detailed view on events in **month 2013/12**, ordered by **'Time'** in **ascending** order, count limit **none**.

Hidden devices:	[redacted]
Hidden device components:	[redacted]

↓ Event ↑	↓ Time ↑	↓ Device ↑	↓ Device Component ↑	↓ Measured Value ↑
x ≠ Packet rate	2013/12/18 11:07:15	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 2340.549 pps -> 3739946.167 pps, growth: 1597.893*
x ≠ Packet rate	2013/12/18 11:15:14	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3739946.167 pps -> 9547534.283 pps, growth: 2.553*
x ≠ Packet rate	2013/12/18 11:24:19	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 9547534.283 pps -> 4752684.488 pps, growth: 0.498*
x ≠ Packet rate	2013/12/18 11:30:21	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 4752684.488 pps -> 3305075.085 pps, growth: 0.695*
x ≠ Packet rate	2013/12/18 11:39:13	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3305075.085 pps -> 3056874.614 pps, growth: 0.925*
x ≠ Packet rate	2013/12/18 11:39:56	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3056874.614 pps -> 3337889.177 pps, growth: 1.092*
x ≠ Packet rate	2013/12/18 11:41:01	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3337889.177 pps -> 3120482.413 pps, growth: 0.935*
x ≠ Packet rate	2013/12/18 11:48:33	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3120482.413 pps -> 2681636.330 pps, growth: 0.859*
x ≠ Packet rate	2013/12/18 11:56:19	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted], 2001:718:1:1:0:0[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 2681636.330 pps -> 2723892.764 pps, growth: 1.016*
↓ Event ↑	↓ Time ↑	↓ Device ↑	↓ Device Component ↑	↓ Measured Value ↑

G3 data access – event visualizer & notifier

- Detected attack on CESNET DNS example



G3 system - notifications

Period:	last hour, last 24 hours, last 7 days, month 2014/1, month 2013/12, month 2013/11, month 2013/10, month 2013/9, month 2013/8, month 2013/7, month 2013/6, month 2013/5, month 2013/4, month 2013/3, month 2013/2, month 2013/1
View:	detailed, semi-aggregated, aggregated
Count Limit:	10, 20, 50, 100, 200, 500, 1000, none
Others:	Show or Hide VLANs utilization Reset to default setup G3 measurement

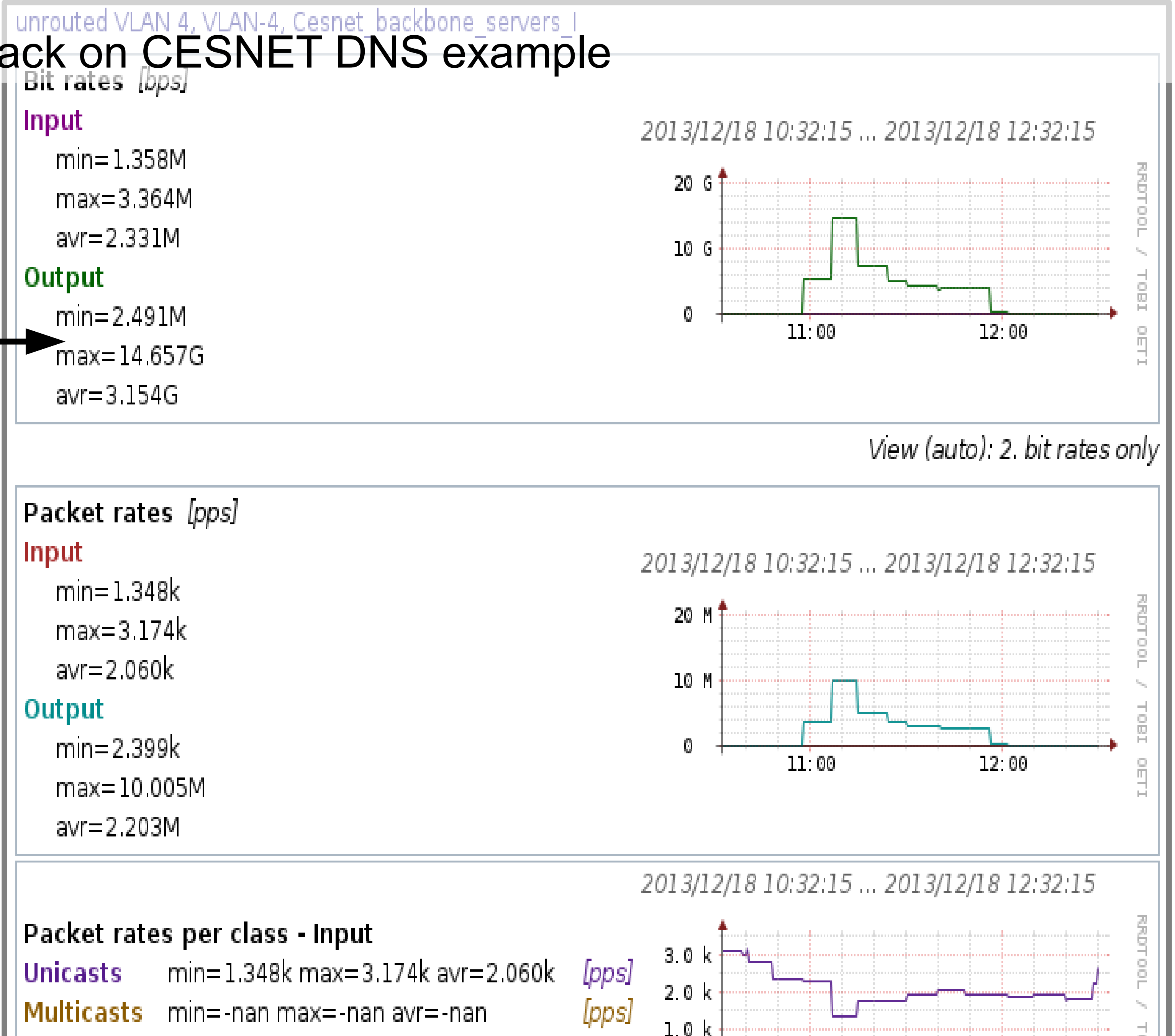
Quick Top Lists Links	last hour	last 24 hours	last 7 days	m 2
Interface errors	*	*	*	
Packet rate	*	*	*	
CPU utilization	*	*	*	
Interface discards	*	*	*	
System reboot	*	*	*	
Interface utilization	*	*	*	

Notice: Reports for longer periods (e.g. months) may take a lot of time - for example tens of seconds. Response time depends on period size and number of events that occurred during that

Detailed view on events in **month 2013/12**, ordered by '**Time**' in **ascending** order, count limit **none**.

Hidden devices:	[redacted]
Hidden device components:	[redacted]

↓ Event ↑	↓ Time ↑	↓ Device ↑	↓ Device Component ↑	↓ Measured Value ↑
x ≠ Packet rate	2013/12/18 11:07:15	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 2340.549 pps -> 3739946.167 pps, growth: 1597.893*
x ≠ Packet rate	2013/12/18 11:15:14	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3739946.167 pps -> 9547534.283 pps, growth: 2.553*
x ≠ Packet rate	2013/12/18 11:24:19	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 9547534.283 pps -> 4752684.488 pps, growth: 0.498*
x ≠ Packet rate	2013/12/18 11:30:21	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 4752684.488 pps -> 3305075.085 pps, growth: 0.695*
x ≠ Packet rate	2013/12/18 11:39:13	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3305075.085 pps -> 3056874.614 pps, growth: 0.925*
x ≠ Packet rate	2013/12/18 11:39:56	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3056874.614 pps -> 3337889.177 pps, growth: 1.092*
x ≠ Packet rate	2013/12/18 11:41:01	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3337889.177 pps -> 3120482.413 pps, growth: 0.935*
x ≠ Packet rate	2013/12/18 11:48:33	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 3120482.413 pps -> 2681636.330 pps, growth: 0.859*
x ≠ Packet rate	2013/12/18 11:56:19	= ≠ 195.113.15[redacted].cesnet.cz	x ≠ Vlan4, Vl4, Cesnet[redacted]ckbone serve[redacted] 2001:718:1:1:0:0:[redacted] 195.113.14[redacted]3 G3	output unicast packet rate: 2681636.330 pps -> 2723892.764 pps, growth: 1.016*
↓ Event ↑	↓ Time ↑	↓ Device ↑	↓ Device Component ↑	↓ Measured Value ↑



unrouted VLAN 4, VLAN-4, Cesnet_backbone_servers_I

Bit rates *[bps]*

Input

min=1.358M

max=3.364M

avr=2.331M

Output

min=2.491M

max=14.657G

avr=3.154G

2013/12/18 10:32:15 ... 2013/12/18 12:32:15

View (auto): 2. bit rates only

Packet rates *[pps]*

Input

min=1.348k

max=3.174k

avr=2.060k

Output

min=2.399k

max=10.005M

avr=2.203M

2013/12/18 10:32:15 ... 2013/12/18 12:32:15

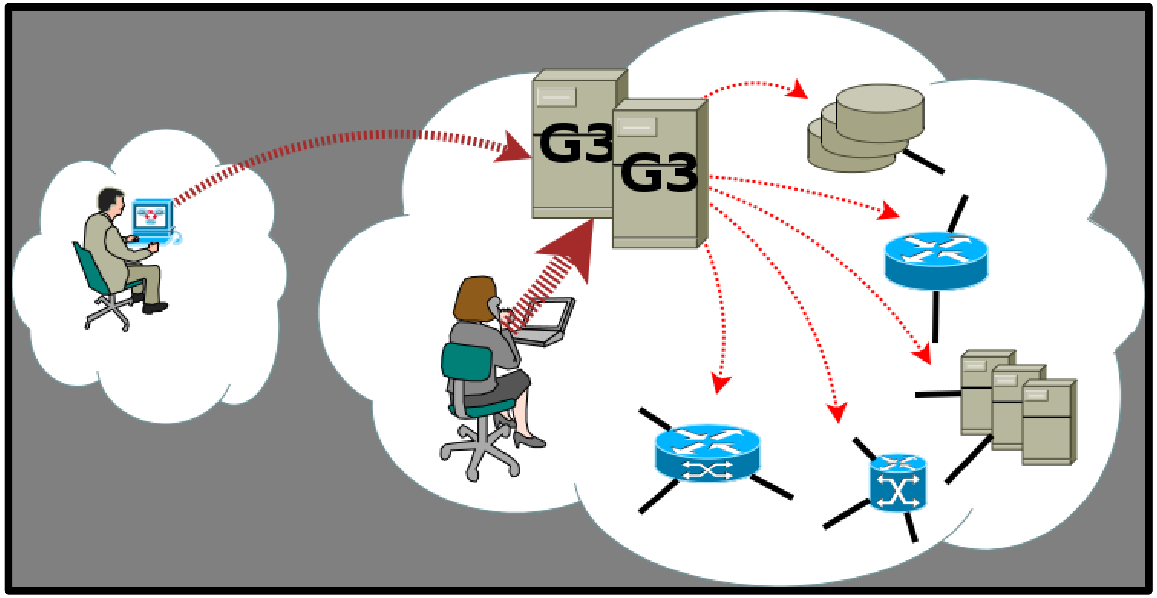
2013/12/18 10:32:15 ... 2013/12/18 12:32:15

Packet rates per class - Input

Unicasts	min=1.348k max=3.174k avr=2.060k	*[pps]*
Multicasts	min=-nan max=-nan avr=-nan	*[pps]*

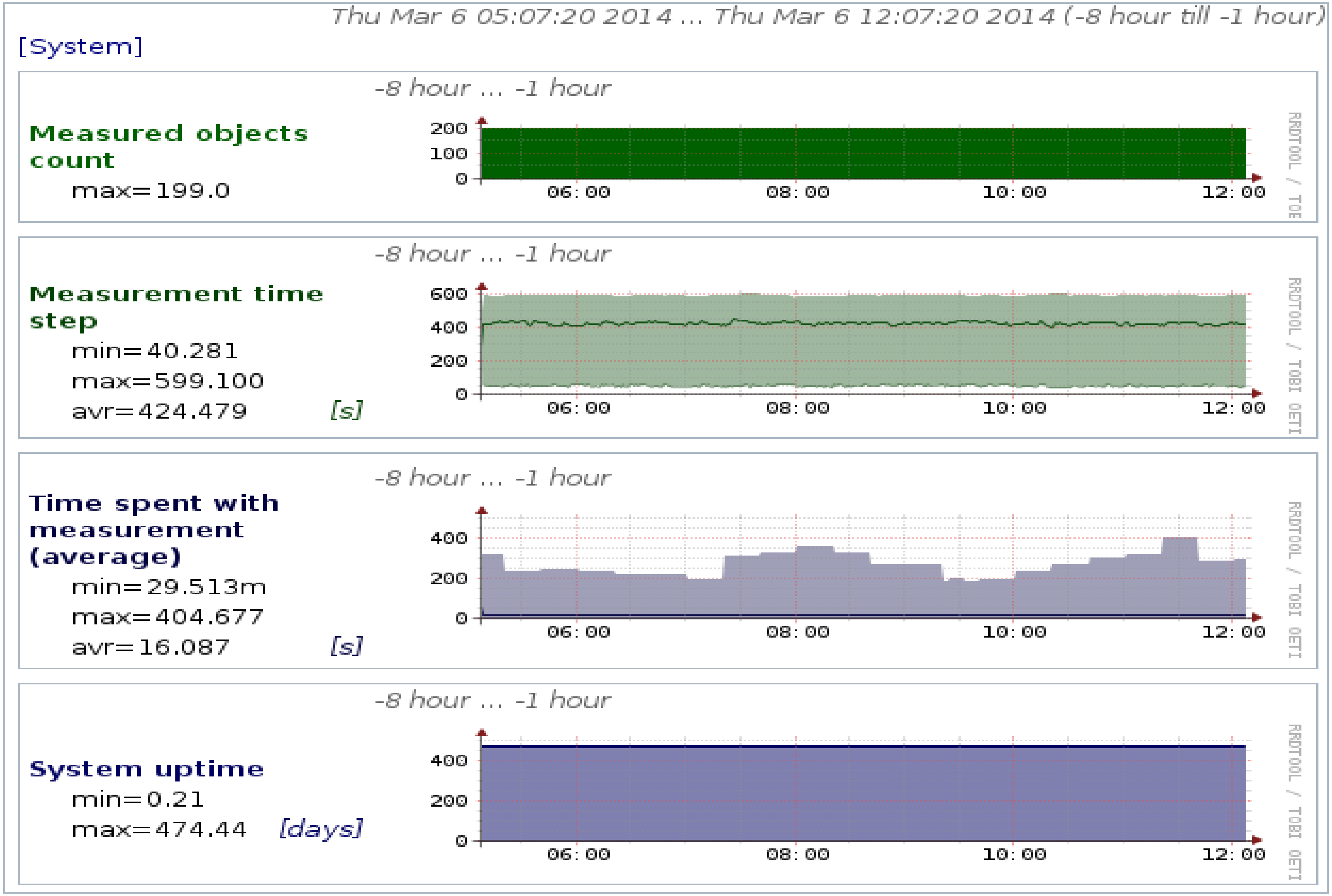
G3 system – summary

- Delivered as service to user groups in both NREN & user networks
- **a) installation in NREN backbone**
  - Operated by CESNET, focus - services in NREN backbone
  - Robust HW infrastructure (~ 200 devices, 700K items measured)
- **b) installation in user networks**
  - OS administration shared
  - Application administration & configuration CESNET
  - Successfully operating in virtual infrastructure



G3 system - summary

- Primary installation in NREN backbone summary (system measures itself...)



Thu Mar 6 05:07:20 2014 ... Thu Mar 6 12:07:20 2014 (-8 hour till -1 hour)

[System]

-8 hour ... -1 hour

Measured objects count
max=199.0

-8 hour ... -1 hour

Measurement time step
min=40.281
max=599.100
avr=424.479 [s]

-8 hour ... -1 hour

Time spent with measurement (average)
min=29.513m
max=404.677
avr=16.087 [s]

-8 hour ... -1 hour

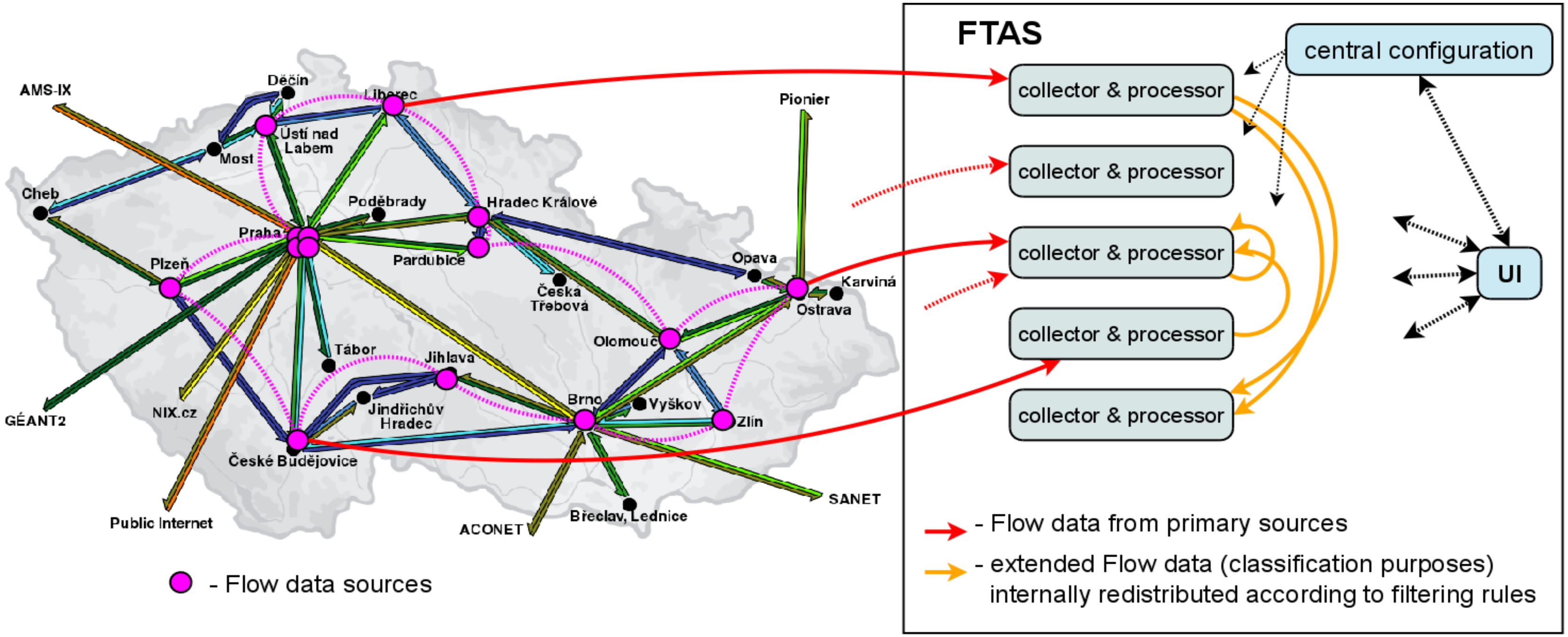
System uptime
min=0.21
max=474.44 [days]

Flow based measurements - FTAS system

- Developed as large scale flow-based measurement system for NREN backbone
- Usable in LAN, MAN, Campus environments
- Development driven by users (backbone administrators, NREN service administrators, CSIRTs, administrators of end-user networks)
- System components
  - **Data measurement & processing core**
  - Data access modules
    - **Interactive UI**
    - **Reporter**
- *System described during last “Campus network monitoring and security workshop” in CZ – Brno 2012*
  - ***Will focus on new features and anomaly detection...***

FTAS system – data measurement & processing core

- **Transport & data types**: IPv4, IPv6; export v1,5,7,9,10/IPFIX
- **Primary flow-data processing** (each optional): replication, multiplexing, classification, filtering, on-fly security checks, storage
  - **Typical stored data sets**: flow data sources, organizations, parts (university → faculties), traffic of interest (according to filtering rules)
- **Data set post-processing**: selection (rules given by configuration), per-group aggregation, overall aggregation, storage (reaching [based on configuration] ..1:600 data amount reduction)

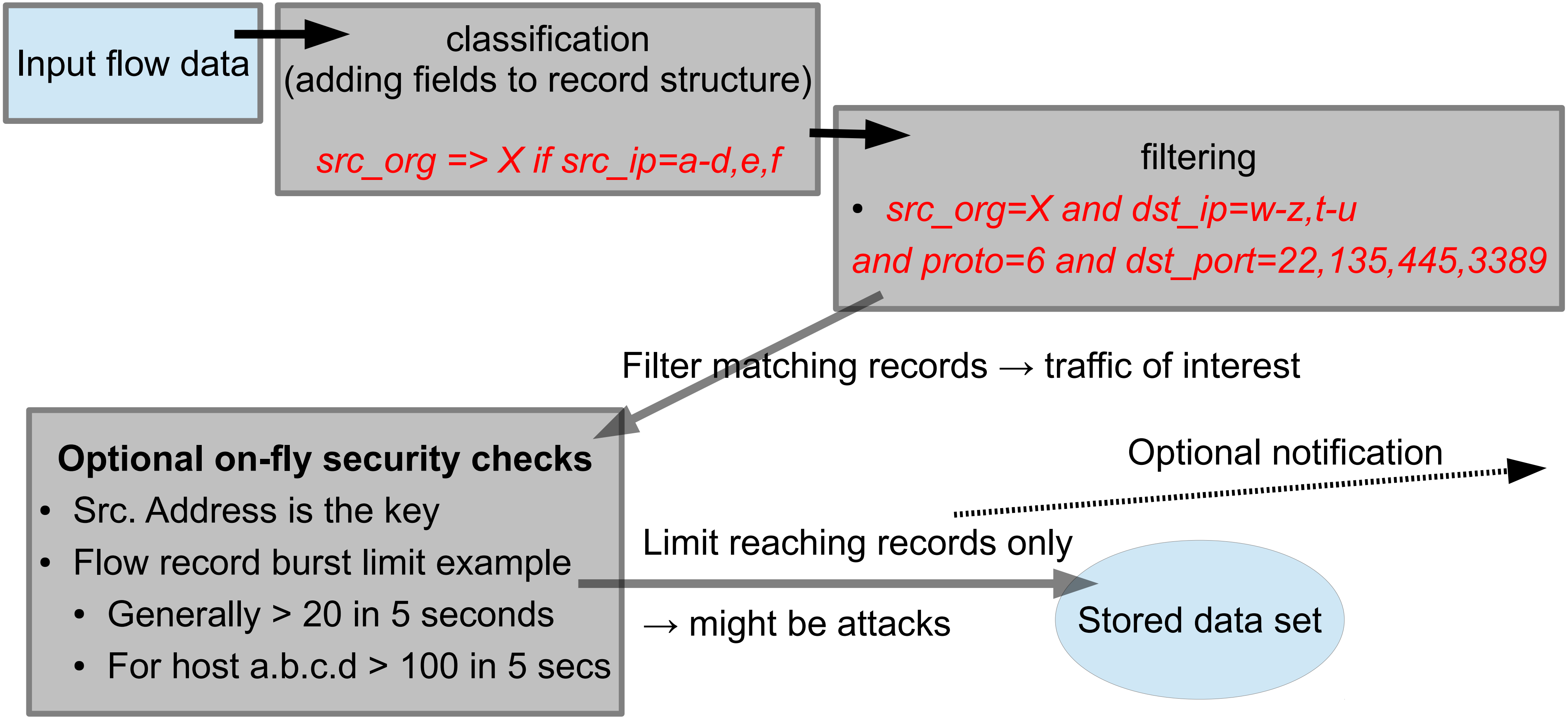


FTAS – data access

- **Interactive UI**
  - **Comprehensive IP traffic browser & visualizer**
  - Two phase work: single query + multiple visualizations
  - Full featured query methods, flexible visualization ~ ordering, aggregation, output types (tables, graphs, plain-text)
  - *Suitable for advanced users*
- **Reporter** *...similar to G3 reporter architecture...*
  - **Structures of periodically generated static HTML pages**
  - Different views on traffic ~ 2 built in processing strategies: security events detection, ordinary statistical output
  - Simple output schema – overview pages → detailed reports + configurable horizontal cross-links
  - Implemented as STDIN/STDOUT control of interactive UI (real-user behavior simulation)
  - *Suitable for ordinary users – intuitive, everything on-click*
- ***Anomalies ?*** *..no special module (as in G3)*

FTAS security anomaly detection processing chain example

- Option 1 – in "**data measurement & processing core**"
- *Real-time, results may be "less accurate", best as Option 2 prerequisite*
- Example – **detect hosts from organization X aggressively attacking services** (ports numbers) **in specified address ranges**



Input flow data

classification
(adding fields to record structure)

src_org => X if src_ip=a-d,e,f

filtering

- *src_org=X and dst_ip=w-z,t-u and proto=6 and dst_port=22,135,445,3389*

Filter matching records → traffic of interest

Optional on-fly security checks

- Src. Address is the key
- Flow record burst limit example
  - Generally > 20 in 5 seconds
  - For host a.b.c.d > 100 in 5 secs

Optional notification

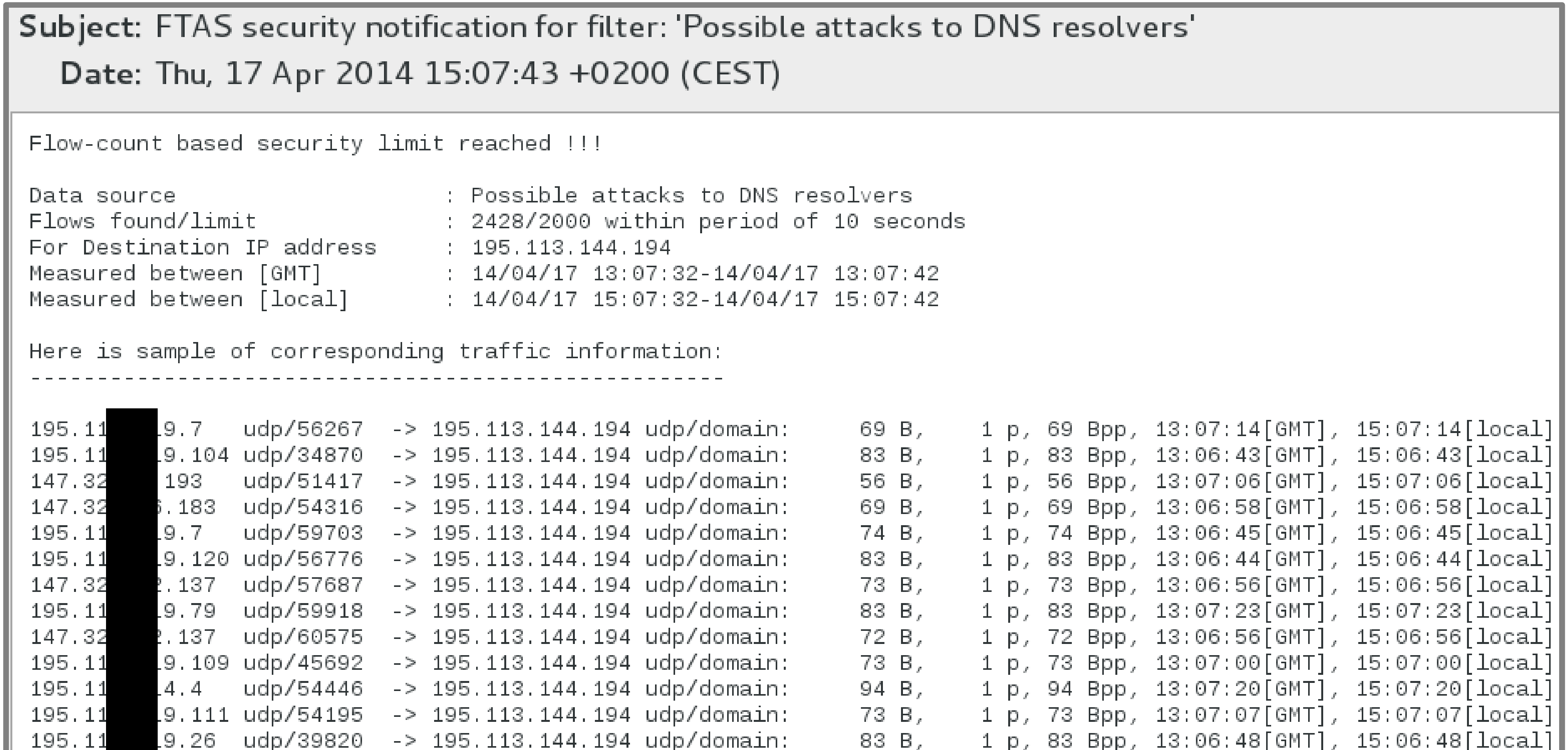
Limit reaching records only

→ might be attacks

Stored data set

FTAS security events detection processing chain example

- Option 1 – in “**data measurement & processing core**”
- Optional notification
  - Immediate, but cannot be always sure in case of soft limit
  - *Notice: notification belongs to different detector (DNS attacks)*

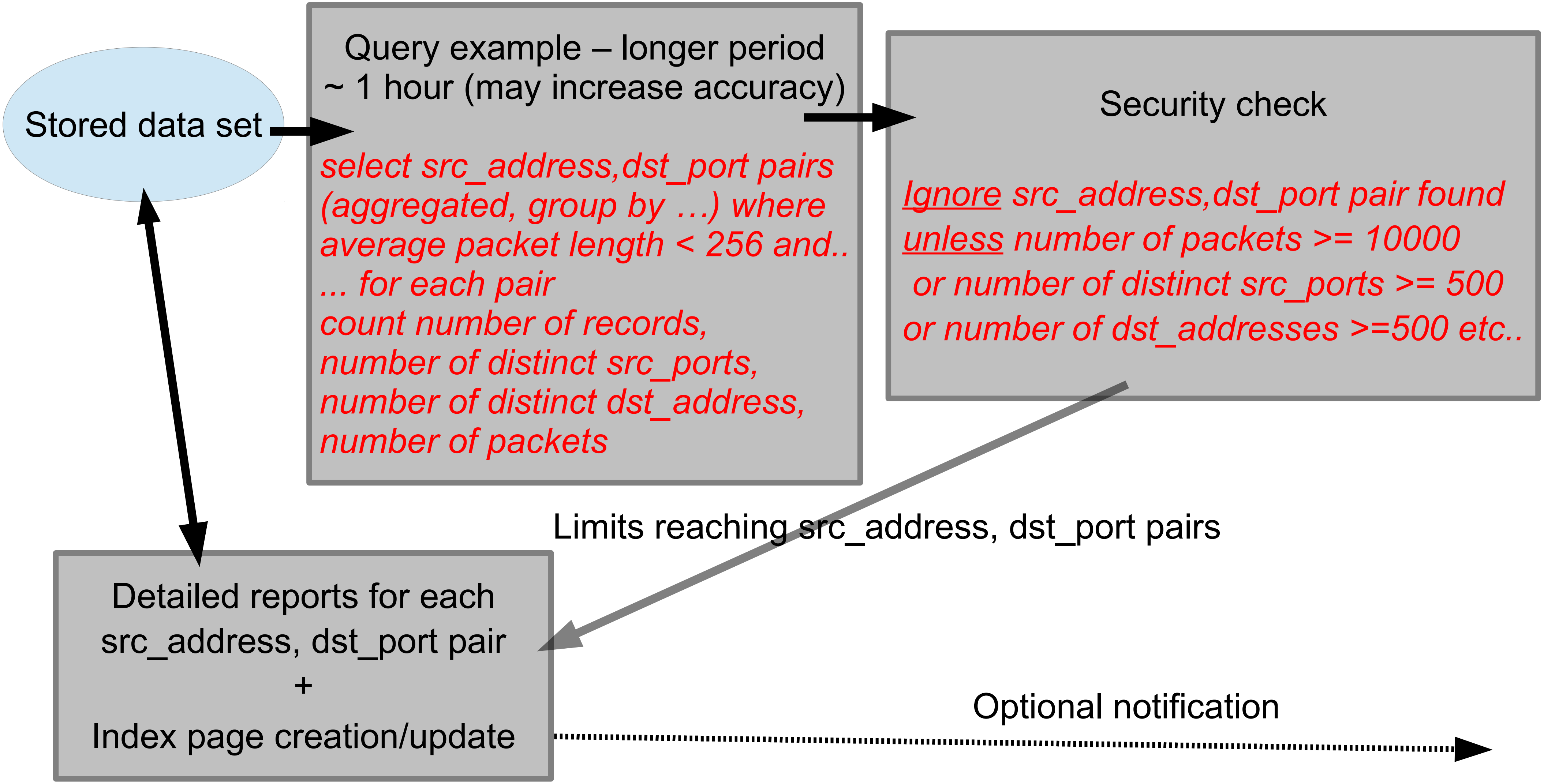


Subject: FTAS security notification for filter: 'Possible attacks to DNS resolvers'
Date: Thu, 17 Apr 2014 15:07:43 +0200 (CEST)

```
Flow-count based security limit reached !!!

Data source                    : Possible attacks to DNS resolvers
Flows found/limit              : 2428/2000 within period of 10 seconds
For Destination IP address     : 195.113.144.194
Measured between [GMT]         : 14/04/17 13:07:32-14/04/17 13:07:42
Measured between [local]       : 14/04/17 15:07:32-14/04/17 15:07:42

Here is sample of corresponding traffic information:
----------------------------------------------------

195.11[redacted]9.7   udp/56267  -> 195.113.144.194 udp/domain:     69 B,     1 p, 69 Bpp, 13:07:14[GMT], 15:07:14[local]
195.11[redacted]9.104 udp/34870  -> 195.113.144.194 udp/domain:     83 B,     1 p, 83 Bpp, 13:06:43[GMT], 15:06:43[local]
147.32[redacted]193   udp/51417  -> 195.113.144.194 udp/domain:     56 B,     1 p, 56 Bpp, 13:07:06[GMT], 15:07:06[local]
147.32[redacted].183  udp/54316  -> 195.113.144.194 udp/domain:     69 B,     1 p, 69 Bpp, 13:06:58[GMT], 15:06:58[local]
195.11[redacted]9.7   udp/59703  -> 195.113.144.194 udp/domain:     74 B,     1 p, 74 Bpp, 13:06:45[GMT], 15:06:45[local]
195.11[redacted]9.120 udp/56776  -> 195.113.144.194 udp/domain:     83 B,     1 p, 83 Bpp, 13:06:44[GMT], 15:06:44[local]
147.32[redacted].137  udp/57687  -> 195.113.144.194 udp/domain:     73 B,     1 p, 73 Bpp, 13:06:56[GMT], 15:06:56[local]
195.11[redacted]9.79  udp/59918  -> 195.113.144.194 udp/domain:     83 B,     1 p, 83 Bpp, 13:07:23[GMT], 15:07:23[local]
147.32[redacted].137  udp/60575  -> 195.113.144.194 udp/domain:     72 B,     1 p, 72 Bpp, 13:06:56[GMT], 15:06:56[local]
195.11[redacted]9.109 udp/45692  -> 195.113.144.194 udp/domain:     73 B,     1 p, 73 Bpp, 13:07:00[GMT], 15:07:00[local]
195.11[redacted]4.4   udp/54446  -> 195.113.144.194 udp/domain:     94 B,     1 p, 94 Bpp, 13:07:20[GMT], 15:07:20[local]
195.11[redacted]9.111 udp/54195  -> 195.113.144.194 udp/domain:     73 B,     1 p, 73 Bpp, 13:07:07[GMT], 15:07:07[local]
195.11[redacted]9.26  udp/39820  -> 195.113.144.194 udp/domain:     83 B,     1 p, 83 Bpp, 13:06:48[GMT], 15:06:48[local]
```

FTAS security events detection processing chain example

- Option 2 – in “**Reporter**” - *delayed, may be more accurate*
  - can use data stored as output of “Option 1” as input (typical cfg.)



Stored data set

Query example – longer period ~ 1 hour (may increase accuracy)

select src_address,dst_port pairs (aggregated, group by …) where average packet length < 256 and..
… for each pair
count number of records,
number of distinct src_ports,
number of distinct dst_address,
number of packets

Security check

Ignore src_address,dst_port pair found unless number of packets >= 10000
or number of distinct src_ports >= 500
or number of dst_addresses >=500 etc..

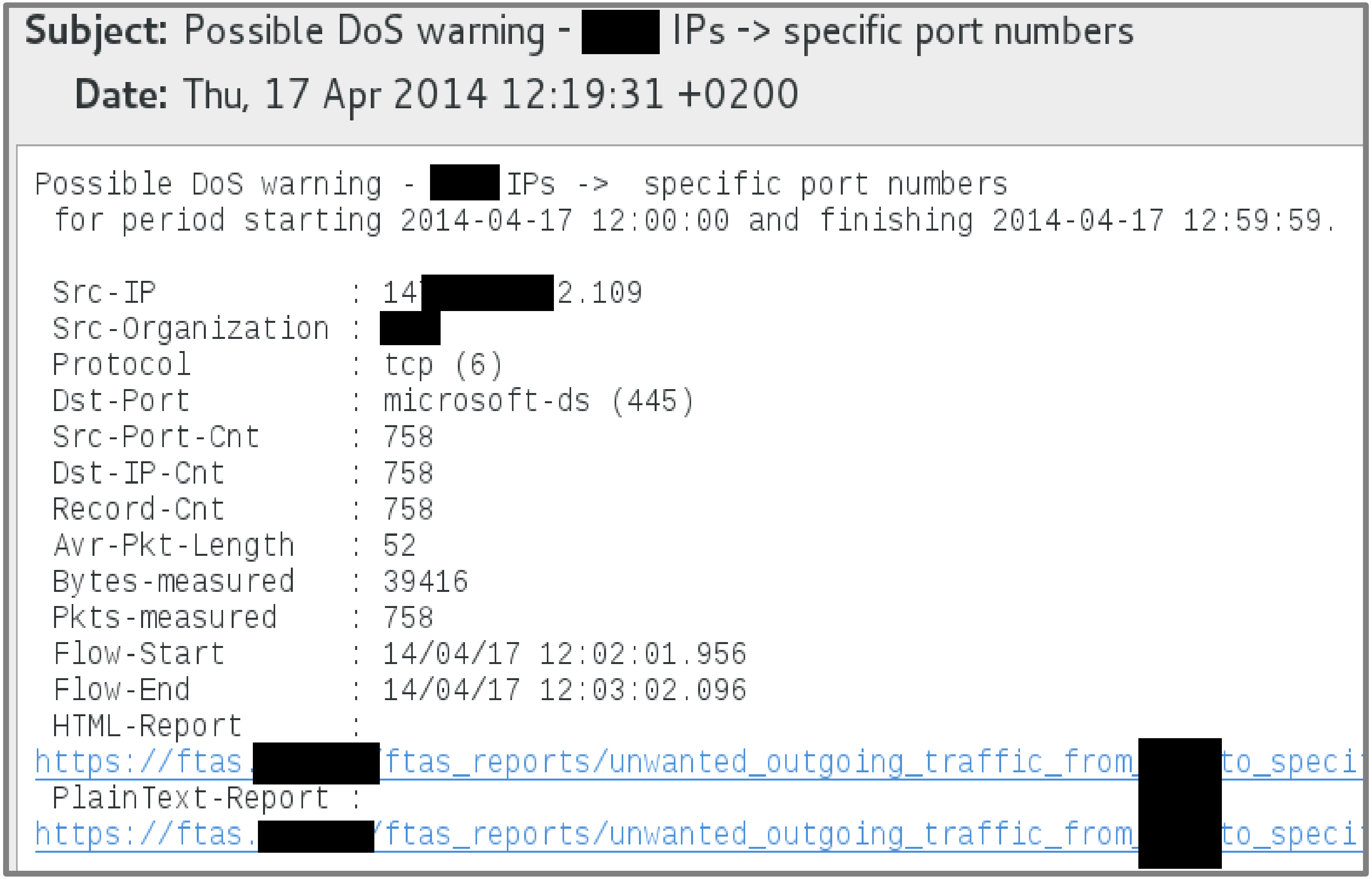
Limits reaching src_address, dst_port pairs

Detailed reports for each src_address, dst_port pair
+
Index page creation/update

Optional notification

FTAS security events detection processing chain example

- Option 2 – in "**Reporter**" - optional notification



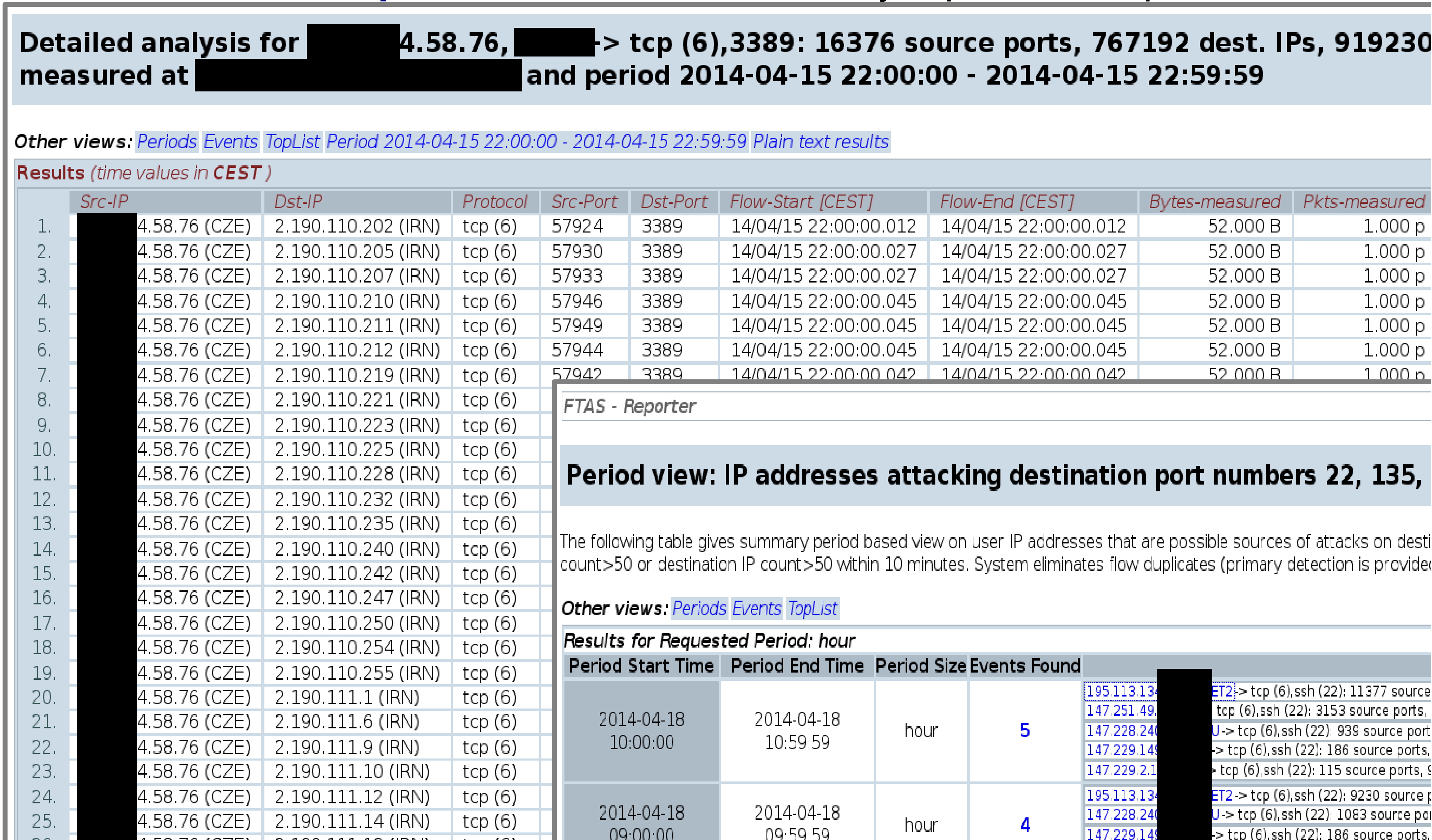
Subject: Possible DoS warning - [redacted] IPs -> specific port numbers

Date: Thu, 17 Apr 2014 12:19:31 +0200

```
Possible DoS warning - [redacted] IPs ->  specific port numbers
 for period starting 2014-04-17 12:00:00 and finishing 2014-04-17 12:59:59.

 Src-IP               : 14[redacted]2.109
 Src-Organization     : [redacted]
 Protocol             : tcp (6)
 Dst-Port             : microsoft-ds (445)
 Src-Port-Cnt         : 758
 Dst-IP-Cnt           : 758
 Record-Cnt           : 758
 Avr-Pkt-Length       : 52
 Bytes-measured       : 39416
 Pkts-measured        : 758
 Flow-Start           : 14/04/17 12:02:01.956
 Flow-End             : 14/04/17 12:03:02.096
 HTML-Report          :
https://ftas.[redacted]ftas_reports/unwanted_outgoing_traffic_from_[redacted]to_speci
 PlainText-Report :
https://ftas.[redacted]/ftas_reports/unwanted_outgoing_traffic_from_to_speci
```

FTAS security events detection processing chain example

- Phase 2 – in “**Reporter**” - detailed & summary reports example



Detailed analysis for [redacted]4.58.76, [redacted]-> tcp (6),3389: 16376 source ports, 767192 dest. IPs, 919230
measured at [redacted] and period 2014-04-15 22:00:00 - 2014-04-15 22:59:59

Other views: *Periods* *Events* *TopList* *Period 2014-04-15 22:00:00 - 2014-04-15 22:59:59* *Plain text results*

Results *(time values in* ***CEST*** *)*

	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured
1.	[redacted]4.58.76 (CZE)	2.190.110.202 (IRN)	tcp (6)	57924	3389	14/04/15 22:00:00.012	14/04/15 22:00:00.012	52.000 B	1.000 p
2.	[redacted]4.58.76 (CZE)	2.190.110.205 (IRN)	tcp (6)	57930	3389	14/04/15 22:00:00.027	14/04/15 22:00:00.027	52.000 B	1.000 p
3.	[redacted]4.58.76 (CZE)	2.190.110.207 (IRN)	tcp (6)	57933	3389	14/04/15 22:00:00.027	14/04/15 22:00:00.027	52.000 B	1.000 p
4.	[redacted]4.58.76 (CZE)	2.190.110.210 (IRN)	tcp (6)	57946	3389	14/04/15 22:00:00.045	14/04/15 22:00:00.045	52.000 B	1.000 p
5.	[redacted]4.58.76 (CZE)	2.190.110.211 (IRN)	tcp (6)	57949	3389	14/04/15 22:00:00.045	14/04/15 22:00:00.045	52.000 B	1.000 p
6.	[redacted]4.58.76 (CZE)	2.190.110.212 (IRN)	tcp (6)	57944	3389	14/04/15 22:00:00.045	14/04/15 22:00:00.045	52.000 B	1.000 p
7.	[redacted]4.58.76 (CZE)	2.190.110.219 (IRN)	tcp (6)	57942	3389	14/04/15 22:00:00.042	14/04/15 22:00:00.042	52.000 B	1.000 p
8.	[redacted]4.58.76 (CZE)	2.190.110.221 (IRN)	tcp (6)						
9.	[redacted]4.58.76 (CZE)	2.190.110.223 (IRN)	tcp (6)						
10.	[redacted]4.58.76 (CZE)	2.190.110.225 (IRN)	tcp (6)						
11.	[redacted]4.58.76 (CZE)	2.190.110.228 (IRN)	tcp (6)						
12.	[redacted]4.58.76 (CZE)	2.190.110.232 (IRN)	tcp (6)						
13.	[redacted]4.58.76 (CZE)	2.190.110.235 (IRN)	tcp (6)						
14.	[redacted]4.58.76 (CZE)	2.190.110.240 (IRN)	tcp (6)						
15.	[redacted]4.58.76 (CZE)	2.190.110.242 (IRN)	tcp (6)						
16.	[redacted]4.58.76 (CZE)	2.190.110.247 (IRN)	tcp (6)						
17.	[redacted]4.58.76 (CZE)	2.190.110.250 (IRN)	tcp (6)						
18.	[redacted]4.58.76 (CZE)	2.190.110.254 (IRN)	tcp (6)						
19.	[redacted]4.58.76 (CZE)	2.190.110.255 (IRN)	tcp (6)						
20.	[redacted]4.58.76 (CZE)	2.190.111.1 (IRN)	tcp (6)						
21.	[redacted]4.58.76 (CZE)	2.190.111.6 (IRN)	tcp (6)						
22.	[redacted]4.58.76 (CZE)	2.190.111.9 (IRN)	tcp (6)						
23.	[redacted]4.58.76 (CZE)	2.190.111.10 (IRN)	tcp (6)						
24.	[redacted]4.58.76 (CZE)	2.190.111.12 (IRN)	tcp (6)						
25.	[redacted]4.58.76 (CZE)	2.190.111.14 (IRN)	tcp (6)						

FTAS - Reporter

Period view: IP addresses attacking destination port numbers 22, 135,

The following table gives summary period based view on user IP addresses that are possible sources of attacks on desti
count>50 or destination IP count>50 within 10 minutes. System eliminates flow duplicates (primary detection is provide

Other views: *Periods* *Events* *TopList*

Results for Requested Period: hour

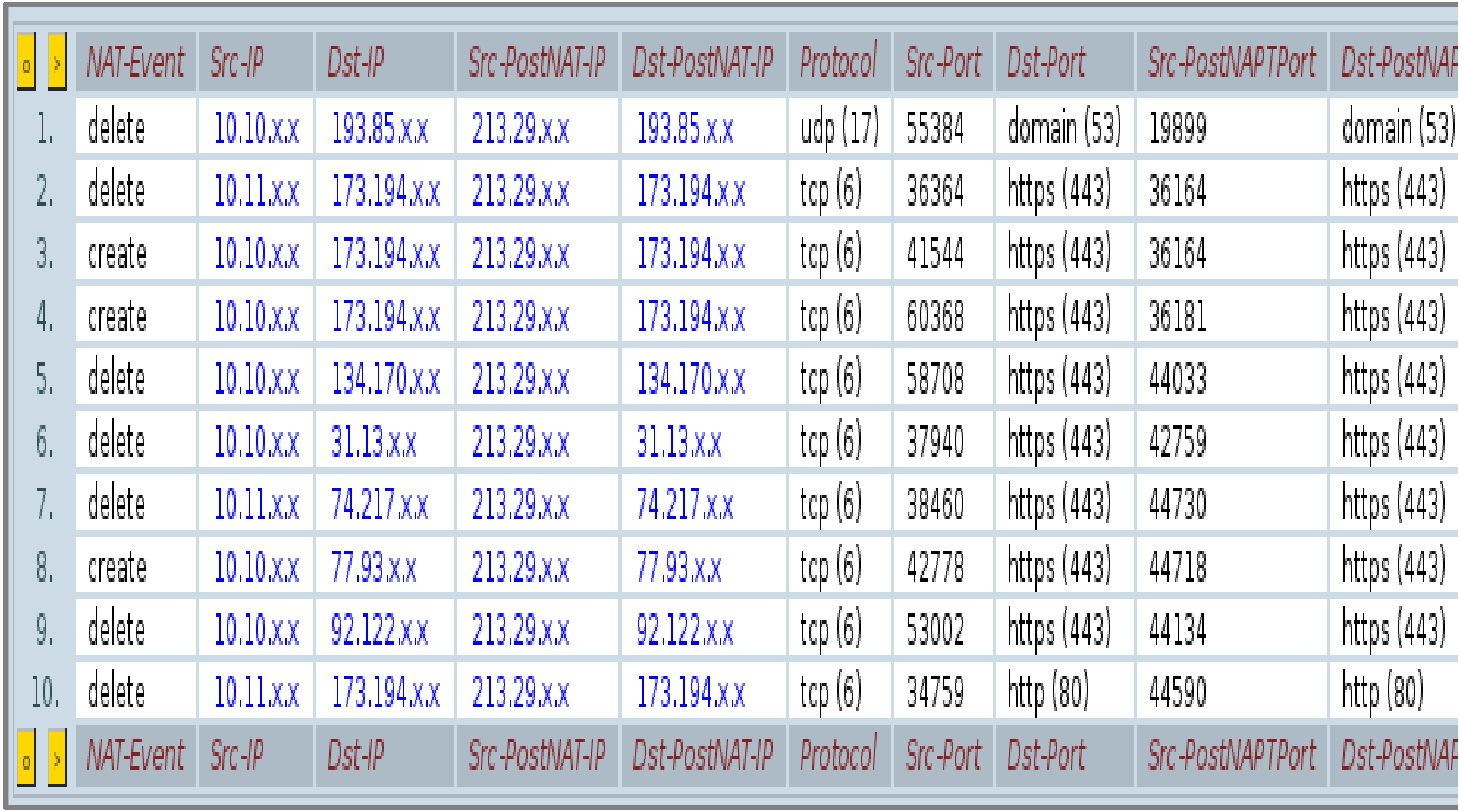
Period Start Time	Period End Time	Period Size	Events Found	
2014-04-18 10:00:00	2014-04-18 10:59:59	hour	5	195.113.134[redacted]ET2 -> tcp (6),ssh (22): 11377 source 147.251.49.[redacted] tcp (6),ssh (22): 3153 source ports, 147.228.240[redacted]U -> tcp (6),ssh (22): 939 source port 147.229.149[redacted]-> tcp (6),ssh (22): 186 source ports, 147.229.2.1[redacted]> tcp (6),ssh (22): 115 source ports,
2014-04-18 09:00:00	2014-04-18 09:59:59	hour	4	195.113.134[redacted]ET2 -> tcp (6),ssh (22): 9230 source 147.228.240[redacted]U -> tcp (6),ssh (22): 1083 source po 147.229.149[redacted]-> tcp (6),ssh (22): 186 source ports,

FTAS news & extensions

- Users require..new options for different network environments → to be incorporated into FTAS
  - **2013: new FTAS generation**
    - **Variable internal data structure**
      - Added suitable sub-set of available fields
        - **N**etflow **S**ecure **E**vent **L**ogging
        - **Flexible Netflow**
      - Since that time (..I broke fixed internal data structure..) adding new field[s] takes ~ 1 hour of programming...
  - **2014: IPFIX support** (including variable length fields)
- Backward compatibility with results created by old generation/versions (UI takes care)

FTAS news & extensions

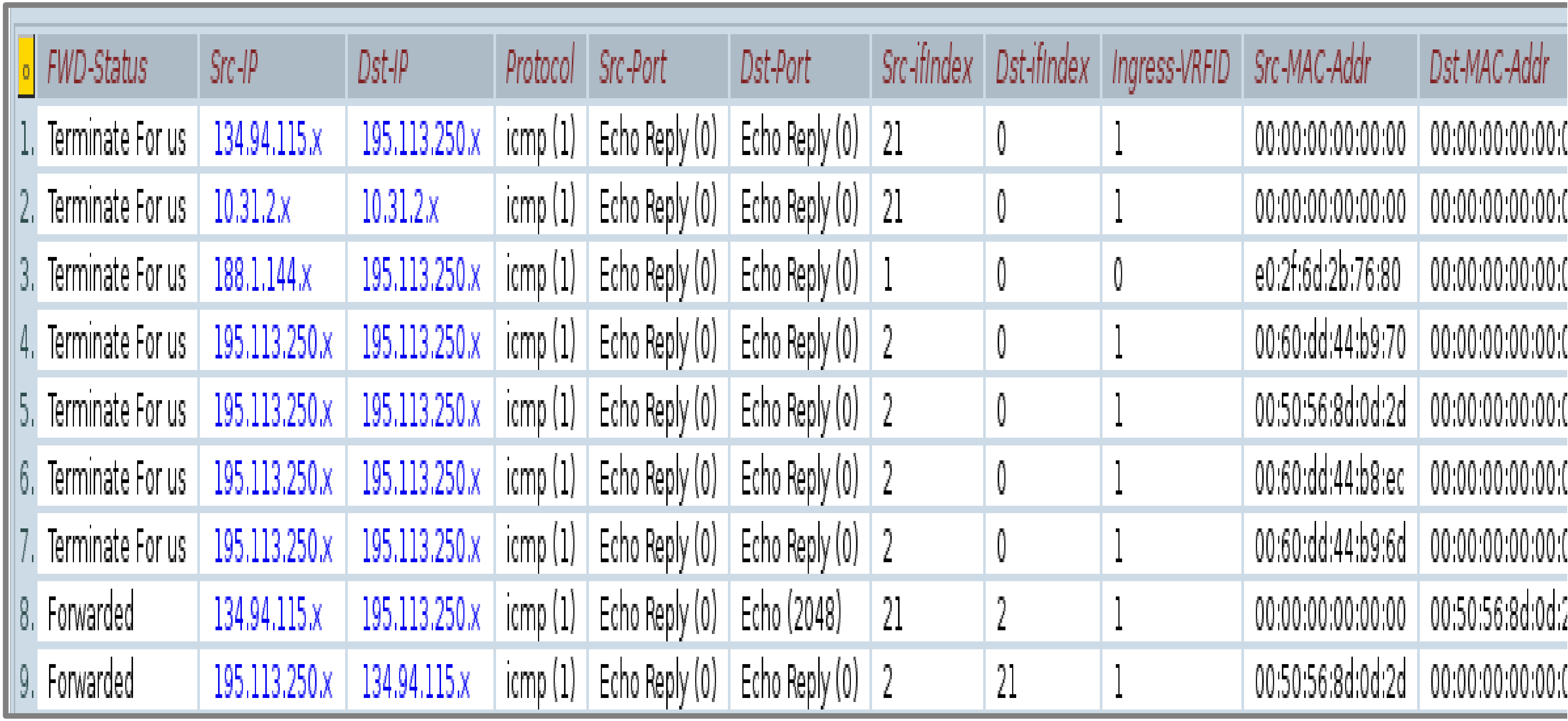
- NSEL output example



o >	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAP
1.	delete	10.10.x.x	193.85.x.x	213.29.x.x	193.85.x.x	udp (17)	55384	domain (53)	19899	domain (53)
2.	delete	10.11.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	36364	https (443)	36164	https (443)
3.	create	10.10.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	41544	https (443)	36164	https (443)
4.	create	10.10.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	60368	https (443)	36181	https (443)
5.	delete	10.10.x.x	134.170.x.x	213.29.x.x	134.170.x.x	tcp (6)	58708	https (443)	44033	https (443)
6.	delete	10.10.x.x	31.13.x.x	213.29.x.x	31.13.x.x	tcp (6)	37940	https (443)	42759	https (443)
7.	delete	10.11.x.x	74.217.x.x	213.29.x.x	74.217.x.x	tcp (6)	38460	https (443)	44730	https (443)
8.	create	10.10.x.x	77.93.x.x	213.29.x.x	77.93.x.x	tcp (6)	42778	https (443)	44718	https (443)
9.	delete	10.10.x.x	92.122.x.x	213.29.x.x	92.122.x.x	tcp (6)	53002	https (443)	44134	https (443)
10.	delete	10.11.x.x	173.194.x.x	213.29.x.x	173.194.x.x	tcp (6)	34759	http (80)	44590	http (80)
o >	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNAP

FTAS news & extensions

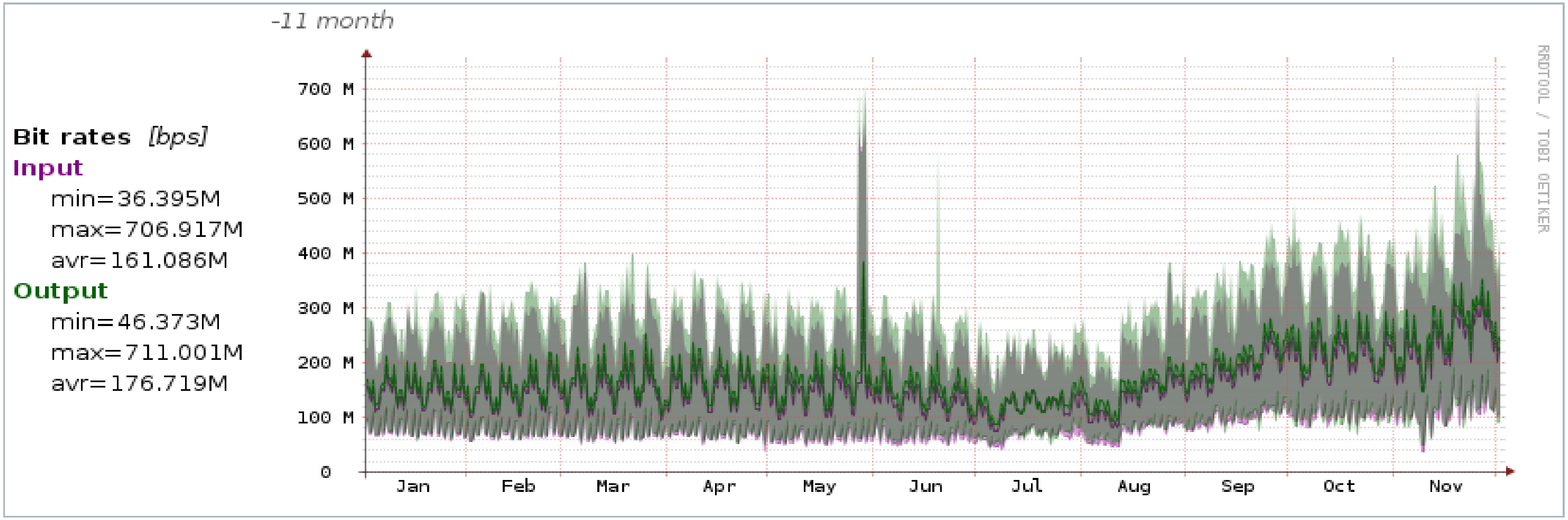
- Flexible Netflow extension fields examples
  - Especially MACs may help to find real source of traffic...when available on large L2 domains sites... real IP↔MAC pairs



	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Src-MAC-Addr	Dst-MAC-Addr
1.	Terminate For us	134.94.115.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:00:0
2.	Terminate For us	10.31.2.x	10.31.2.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:00:0
3.	Terminate For us	188.1.144.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	1	0	0	e0:2f:6d:2b:76:80	00:00:00:00:00:0
4.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:70	00:00:00:00:00:0
5.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:50:56:8d:0d:2d	00:00:00:00:00:0
6.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b8:ec	00:00:00:00:00:0
7.	Terminate For us	195.113.250.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:6d	00:00:00:00:00:0
8.	Forwarded	134.94.115.x	195.113.250.x	icmp (1)	Echo Reply (0)	Echo (2048)	21	2	1	00:00:00:00:00:00	00:50:56:8d:0d:2
9.	Forwarded	195.113.250.x	134.94.115.x	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	21	1	00:50:56:8d:0d:2d	00:00:00:00:00:0

FTAS service summary

- **Primary installation, in CESNET NREN core**
  - 15 physical nodes, 40 netflow sources, data ttl ~ 65-90 days
  - Interactive UI access count in 2013 > **15k**
  - Reporter outputs access count in 2013 > **120k**
  - Total volume of flow data processed (incl. Int. redistribution)

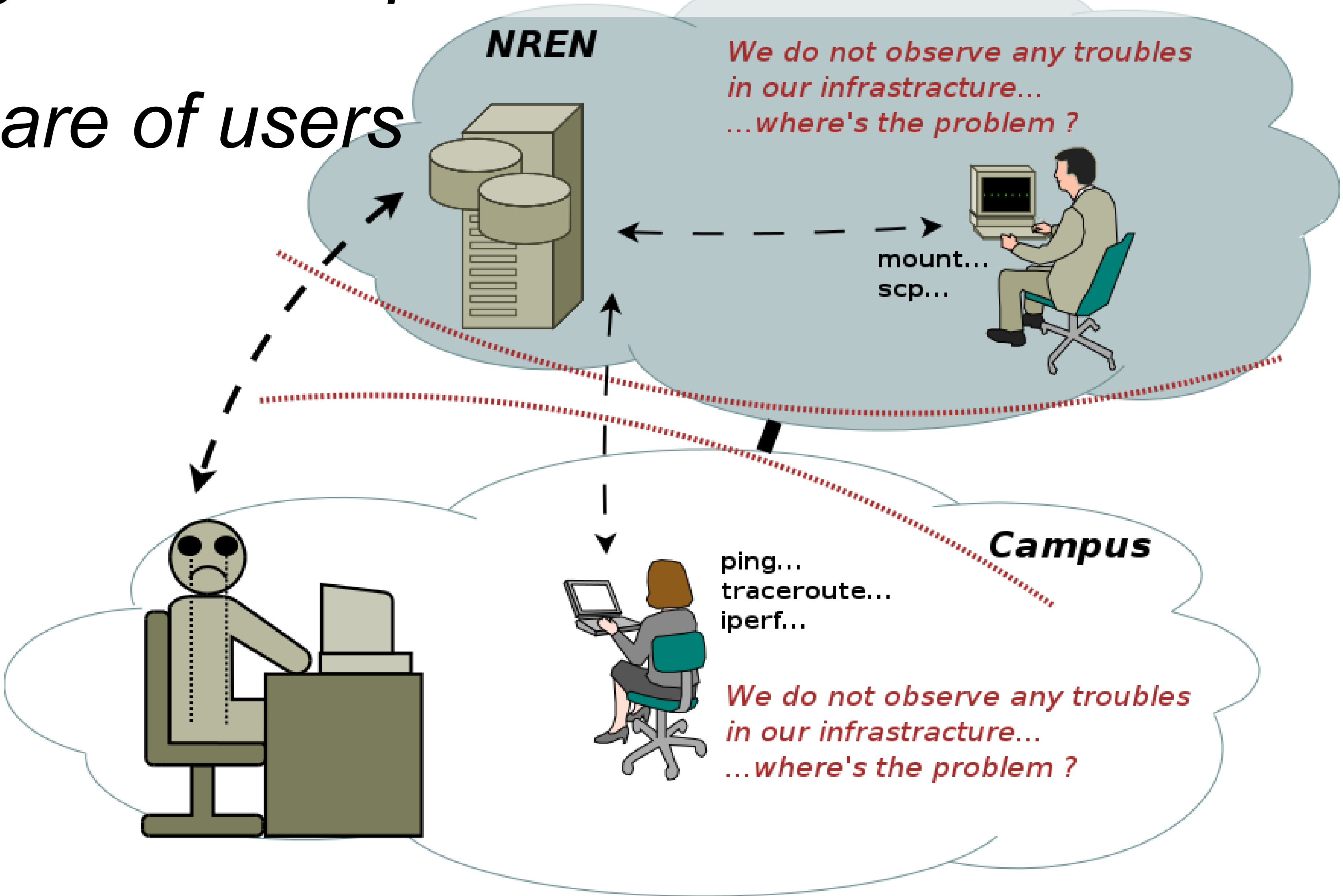


- **Other FTAS installations**
  - **standalone in user networks** (~ 1 node/inst.)
- Overall 30+ institutions with dedicated configurations, reporting or with standalone installations, hundred+ specific traffic filters

Thank you for your patience...

Message ?? ..let's provide real service

..take care of users



NREN
We do not observe any troubles
in our infrastructure...
...where's the problem ?
mount...
scp...
Campus
ping...
traceroute...
iperf...
We do not observe any troubles
in our infrastructure...
...where's the problem ?