Služby sledování infrastruktury a IP provozu sítě pro uživatele e-infrastruktury CESNET

… monitorovací služby pro různé skupiny uživatelů …

Tomáš Košňar
CESNET z. s. p. o.
kosnar@cesnet.cz

*45. konference **EurOpen,** Kašperské Hory 5.-8. 10. 2014*

Obsah

- Co uživatelé chtějí a „potřebují“ ?
- Plošný souvislý monitoring
  - **Infrastruktury sítě**
  - **IP provozu na bázi toků**
    - Nástroje (SW) vyvíjené a používané v e-Infrastruktuře CESNET
    - Stručný popis, funkční komponenty, aktuální stav
    - Příklady použití, ukázky výstupů, ukázky funkcí detekce anomálií
    - Modely poskytování služby

Etická poznámka

- *Součástí prezentace jsou ukázky výstupů, které obsahují reálná provozní data nebo reálná schémata monitorovaných infrastruktur !!!*
  - *Z hlediska respektu k soukromí uživatelů byly proto vybrány (pokud to dávalo smysl) již morálně expirované ~ zastaralé výstupy*
  - *Anonymizace některých reálných provozních dat by zásadně degradovala vypovídací hodnotu výstupu*

Proto není možné prezentaci v původní podobě zveřejnit !!!

Co uživatelé chtějí a "potřebují" v oblasti monitorování ?

- Správci páteřních rozsáhlých sítí (alespoň naši) – chtějí pokud možno okamžitě vidět i ten **nejmenší detail v různých perspektivách** (časový rozsah apod.) *~ plnohodnotné interaktivní uživatelské rozhraní*
- Správci lokálních sítí/služeb – nechtějí se primárně zabývat monitorováním, sbírat a vyhodnocovat kvanta dat a atd..; jsou soustředěni no doručování „high-level" služeb koncovým uživatelům; ocení **pomoc při řešení problémů** *~ jednoduché intuitivní uživatelské rozhraní přehledového typu*
- Členové bezpečnostních týmů (CSIRT) – chtějí být **aktivně upozorněni** (je-li to možné) na **anomálie** a musí být schopni (v každém případě) analyzovat události v rámci „incident handling" procesu *~ uživatelské rozhraní se specifickými vlastnostmi (jednoduché v některých oblastech, komplexní v jiných)*
- Koncoví uživatelé – chtějí věci **používat**, **ne** je **analyzovat**; případně potřebují někoho, kdo vyřeší jejich problém – maximálně se zajímají o základní informace ohledně funkčnosti služeb (..co vyhodnotil operátorí..) *~ velmi jednoduché intuitivní uživatelské rozhraní*
- ..atd., atd. ...manažeři,...další skupiny – různé perspektivy, různé požadavky

Nástroje pro plošný monitoring vyvíjené a používané v e-Infrastruktuře CESNET

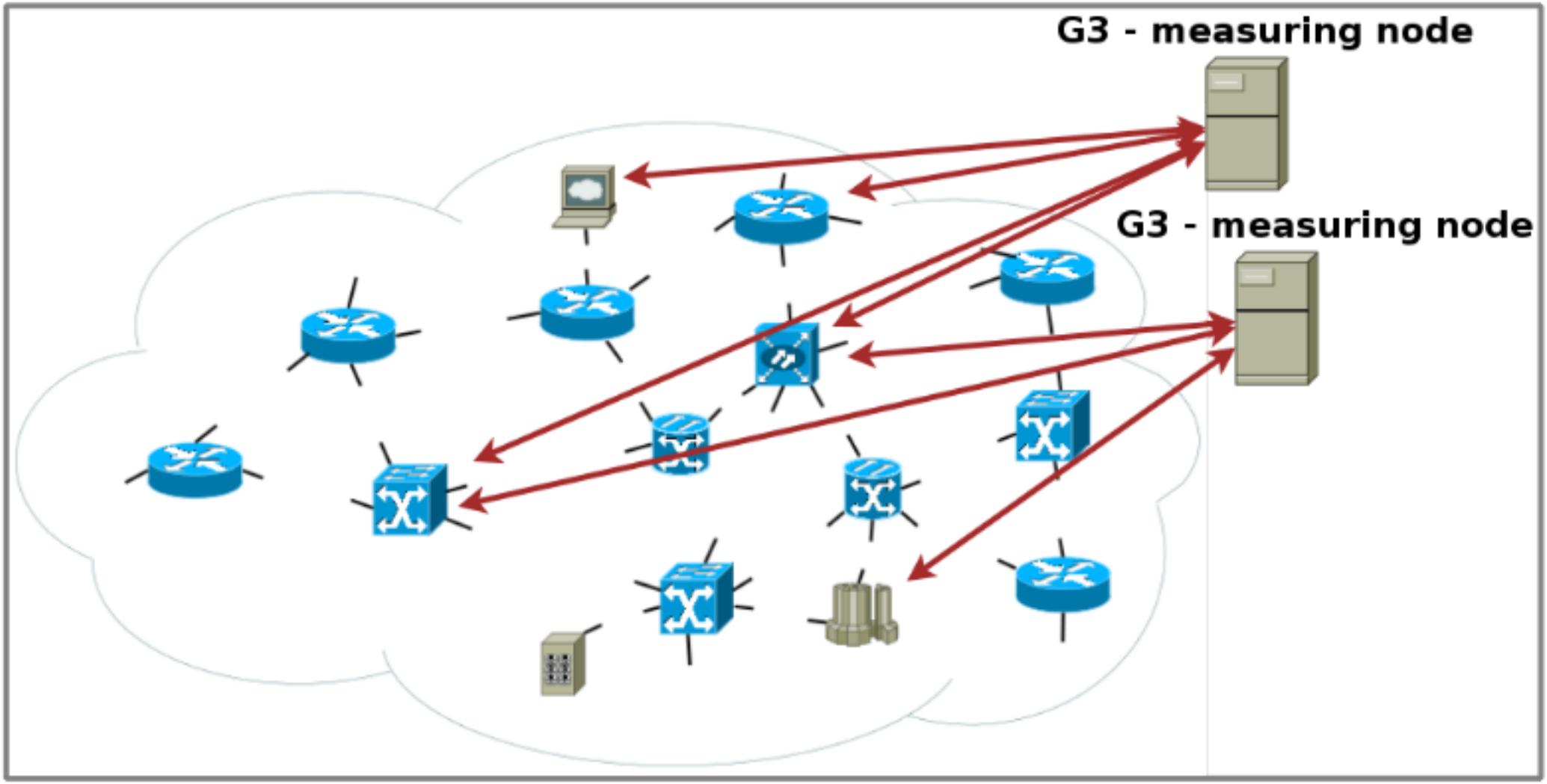
- Zaměřeno pouze na obecné SW nástroje (CESNET vyvíjí a užívá také další speciální [HW/HW-SW] nástroje)
- **Oblast sledování infrastruktury**
  - Informace o infrastruktuře, jejích komponentách a službách vytvářena z informacích sebraných ze zařízení a systémů, které infrastrukturu tvoří
    - **Systém G3**
- **Oblast sledování IP provozu na bázi toků (flow-based)**
  - Informace o IP provozu institucí, zařízení, přístrojů, linek, atd..., o incidentech a anomáliích - prostřednictvím zpracování informací o IP provozu na bázi toků (~ netflow) získaných z infrastruktury
    - **Systém FTAS**

Sledování infrastruktury – systém G3

- Původně vyvíjen jako systém pro plošné souvislé sledování páteře NREN, postupně rozšiřován o nové měřící schopnosti a nové komponenty
  - Použitelný v LAN, MAN, WAN, kampusových prostředích
  - Vývoj řízen převážně uživateli (správci páteřní sitě e-Infrastruktury CESNET, správci služeb, správci koncových sítí)
- Komponenty
  - **Měřící jádro**
  - Uživatelská rozhraní
    - **Interactivní UI**
    - **G3-reporter**
    - **Vizualizátor a notifikátor událostí a anomálií**

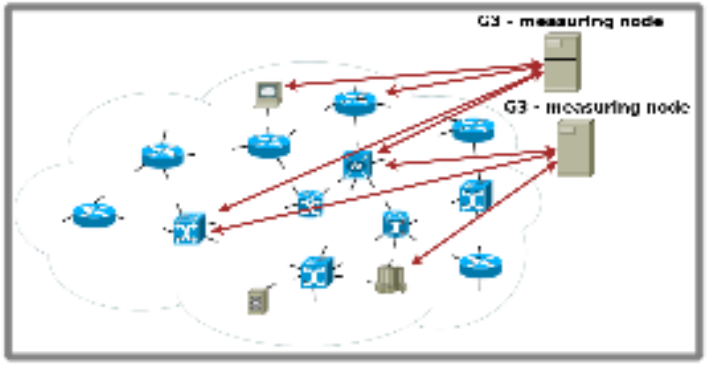
Systém G3 – měřící jádro

- Periodický sběr dat (v principu libovolnou metodou)
  - Zpravidla aktivní měřící uzel



Systém G3 – měřící jádro

- Zabudovaná podpora SNMP; RFC MIBs, proprietární (Cisco, Alcatel-Lucent, CESNET, ...) MIBs
- Automatické měření celého zařízení v každém kroku – *pro kompletní SNMP měření stačí nakonfigurovat IP adresu zařízení a autorizační údaje*
- Automatická konstrukce logické struktury zařizení – *nezávislá na technologických identifikátorech (SNMP indexes)*
- Konfigurovatelný (strategie) dynamický časový krok pro sběr dat – *nízká průměrná agresivita (zátěž zařízení) měření a zároveň možnost zachycení určité "dynamiky" dějů*
- Aktuálně je možno měřit > 700 údajů-položek (~ 550 SNMP OID)



Systém G3 – interaktivní UI

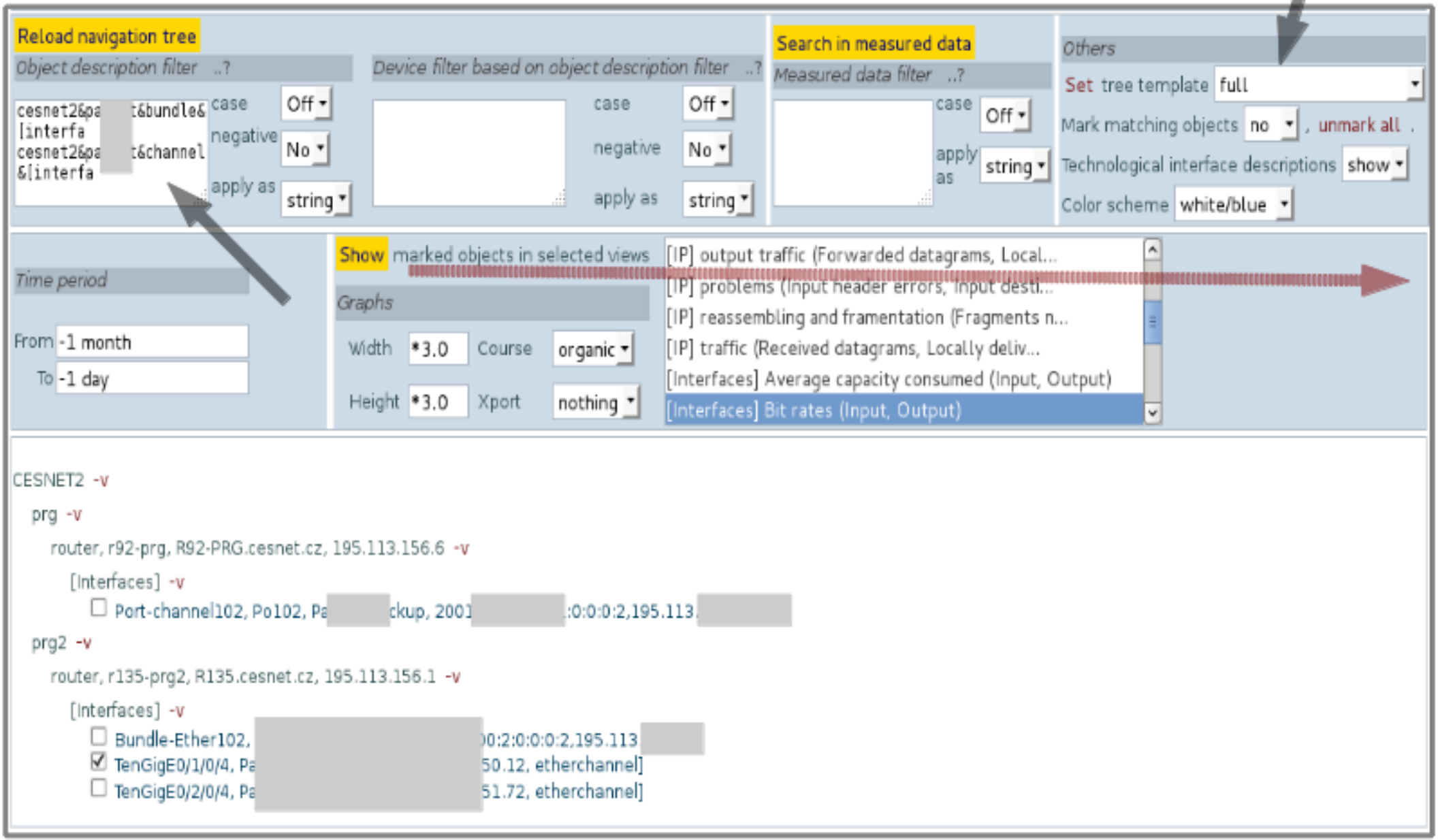
- Interaktivní „browser“ po struktuře zařízení a komponentách infrastruktury & vizualizátor vybraných údajů z vybraných objektů
  - Princip práce - 2 kroky
    - **a) Vyhledání & vybrání objektů zájmu**
      - Flexibilní vyhledávací aparát (několik možných způsobů, uložení podmínek pro další použití)
      - Speciální vyhledání objektů, na kterých byly v zadaném intervalu naměřeny „anomální“ hodnoty tj. přesahující interaktivně (v UI) zadané limity (např. rozhraní s chybovostí >= 1.2 pps, CPU s 1 minutovým využitím >= 75%)
      - Volitelné předlohy pro vizualizaci stromu objektů – lze interpretovat více objektů jako jeden agregovaný (např. všechna vyhledaná síťová rozhraní jako jadno anonymní)

Systém G3 – interaktivní UI

- Interaktivní „browser“ po struktuře zařízení a komponentách infrastruktury & vizualizátor vybraných údajů z vybraných objektů
  - Princip práce - 2 kroky
    - **b) Vizualizace vybraných objektů zvoleným způsobem**
      - Automatická agregace (grafické výstupy nad více objekty)
      - Vizualizace 1-n údajů-položek, předefinované systémové pohledy, možnost nakonfigurovat vlastní templaty

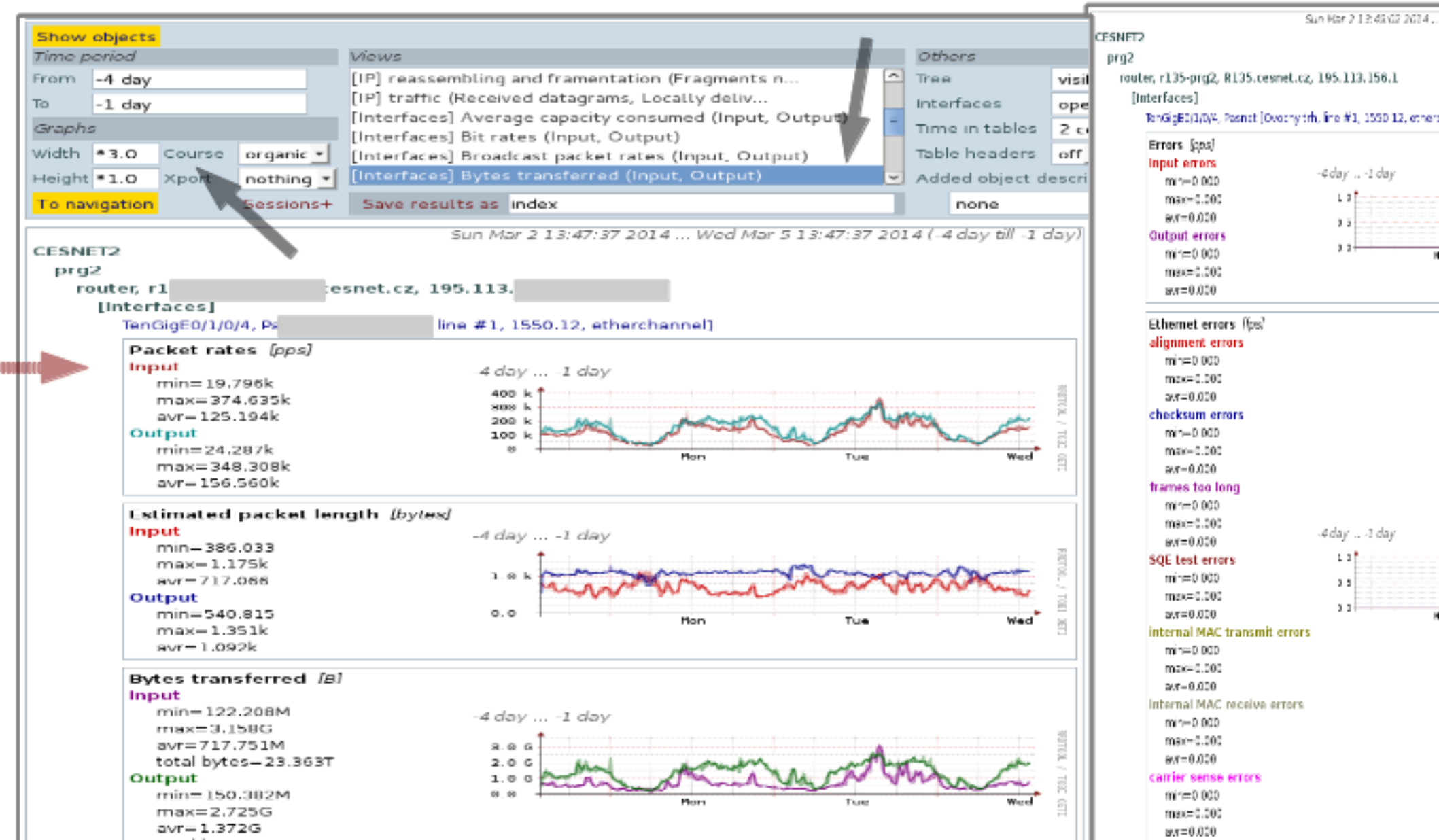
Systém G3 – interaktivní UI

- Krok 1: **vyhledání a výběr konkrétních objektů**



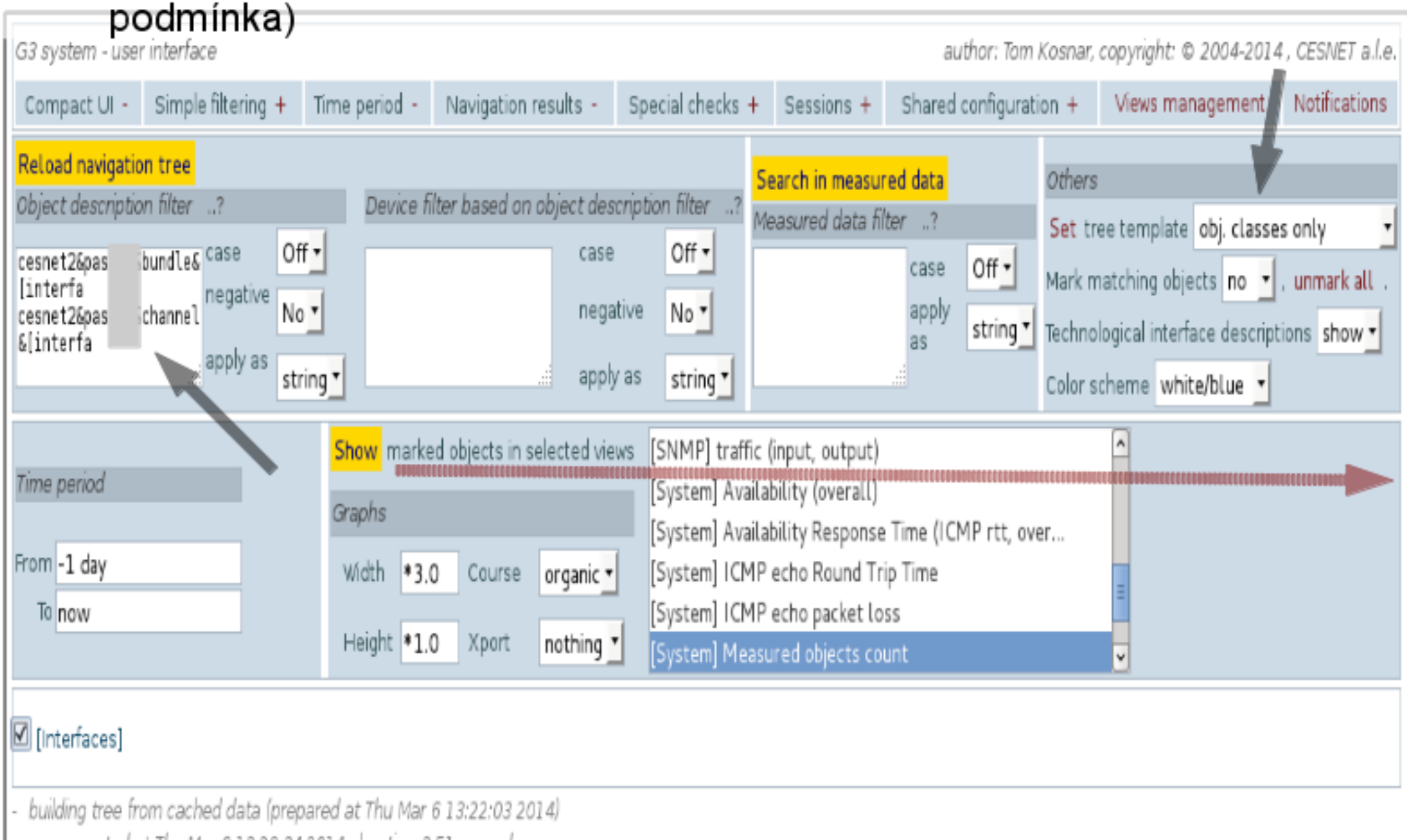
Systém G3 – interaktivní UI

- Krok 2: **vizualizace vybraných objektů zvoleným způsobem**



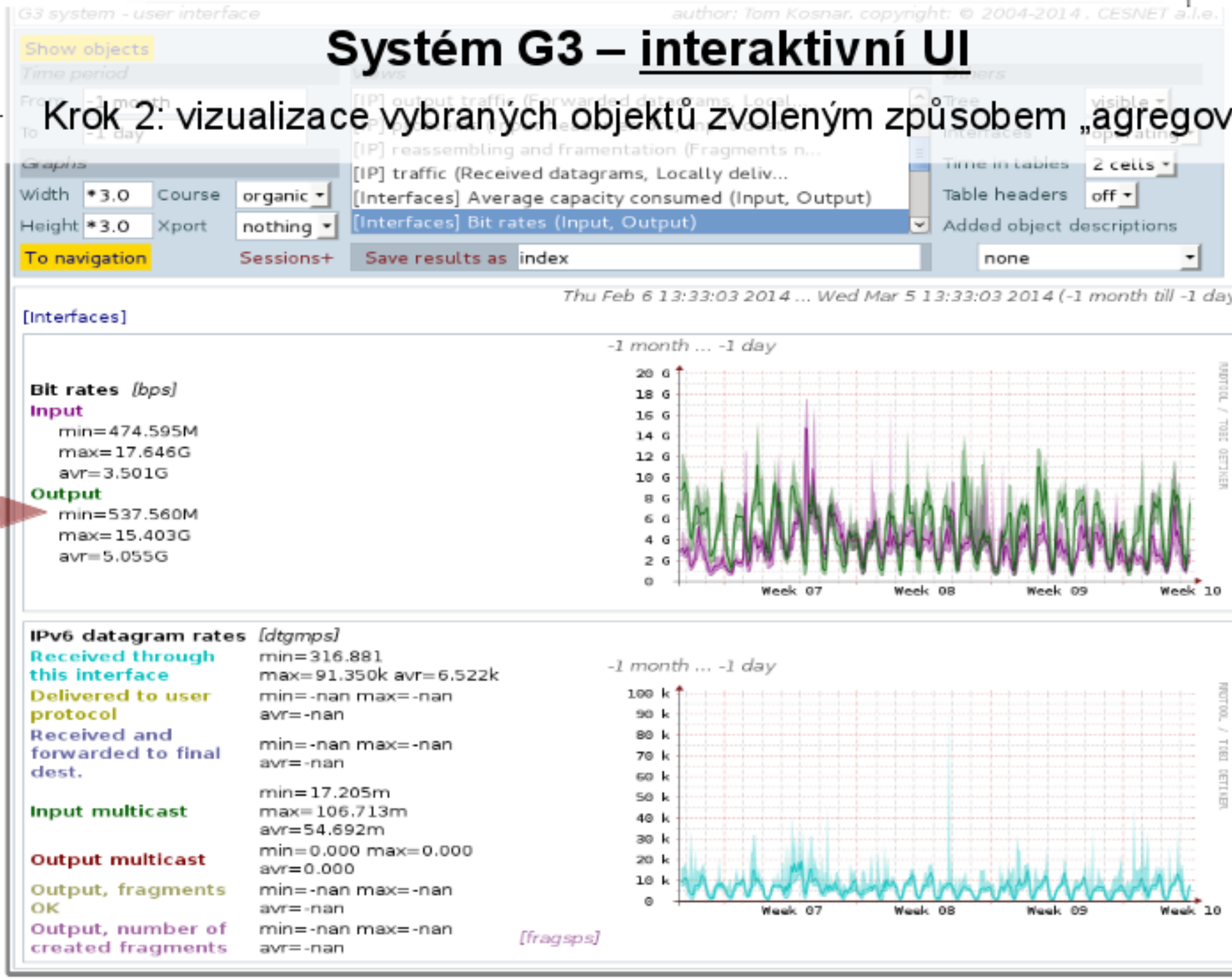
Systém G3 – interaktivní UI

- Krok 1: **vyhledání a výběr objektů „agregovaně“** (identická podmínka)



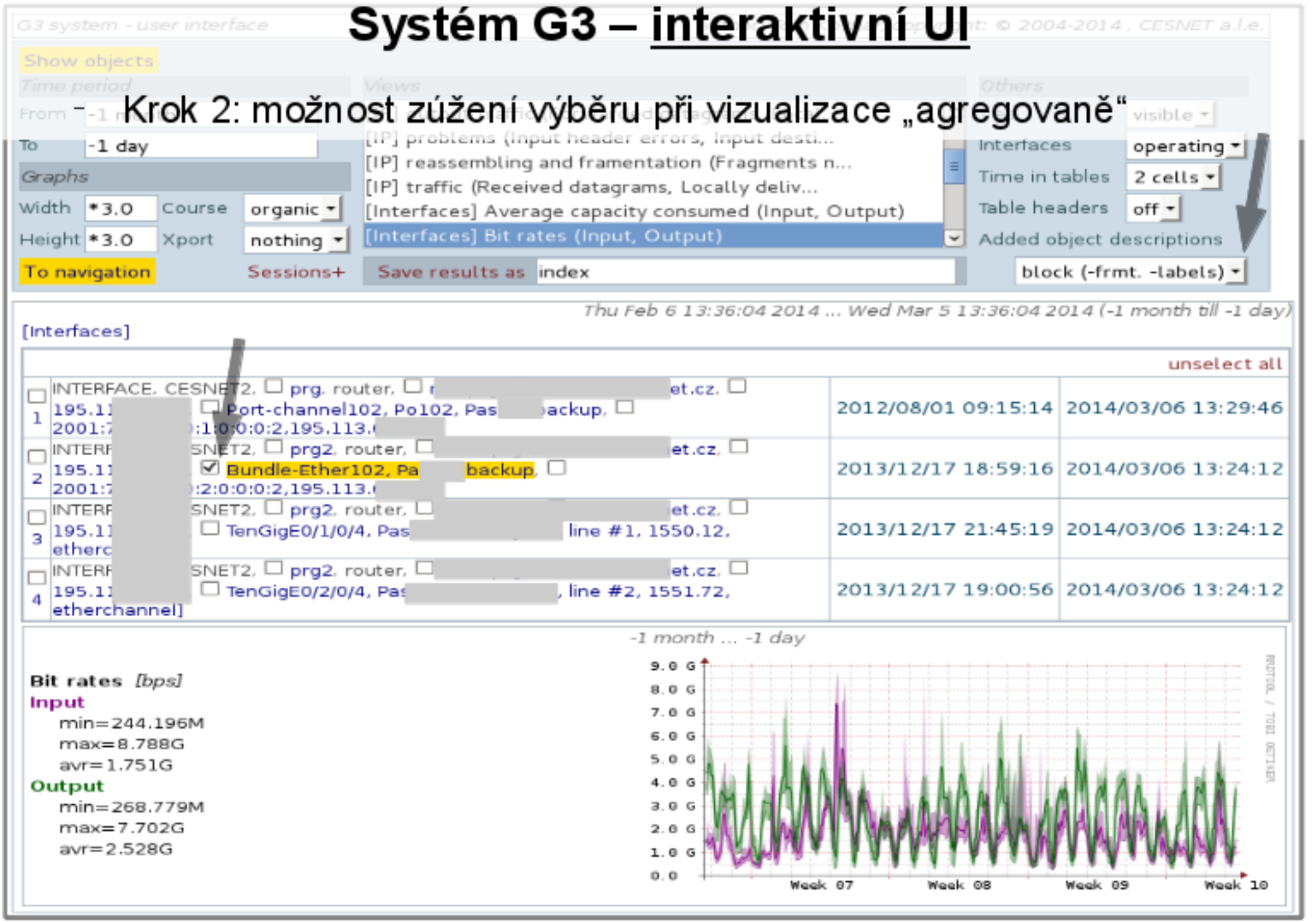
Systém G3 – interaktivní UI

- Krok 2: vizualizace vybraných objektů zvoleným způsobem „agregovaně“



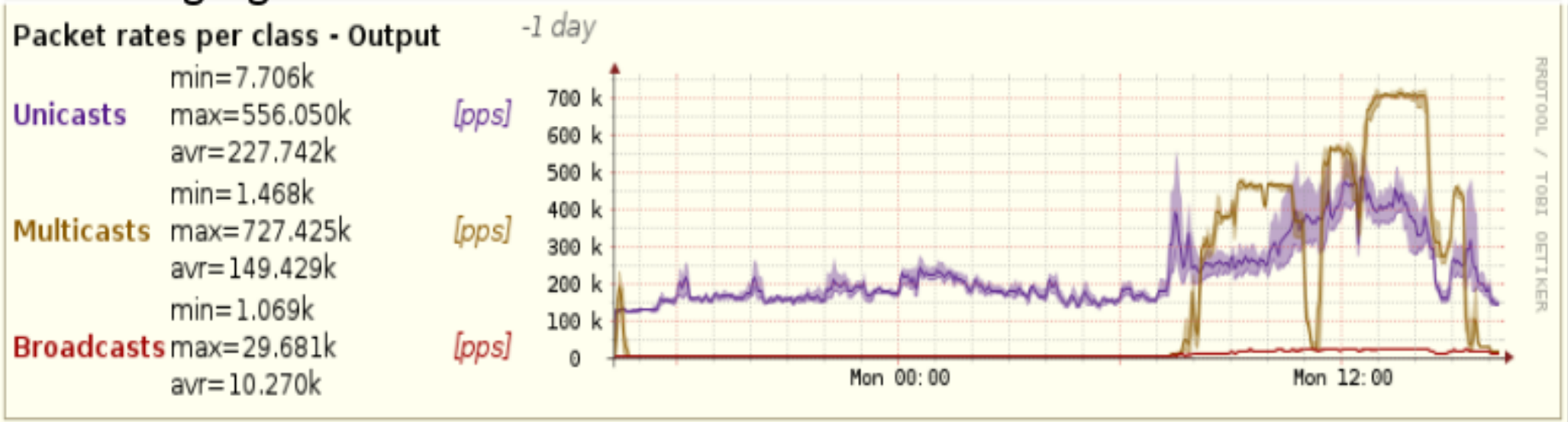
Systém G3 – interaktivní UI

– Krok 2: možnost zúžení výběru při vizualizace „agregovaně“

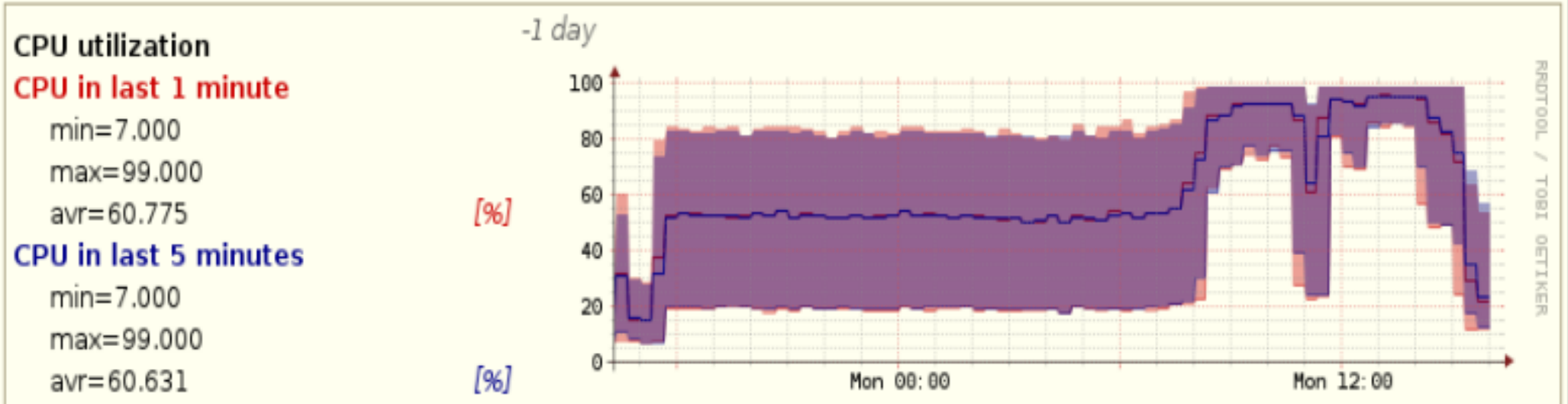


Systém G3 – interaktivní UI

- Ukázka efektivního využití agregačních vlastností (služba pro uživatelskou síť): pokus najít příčinu vysoké zátěže CPU pomocí agregované vizualizace všech CPU a rozhraní v síti...



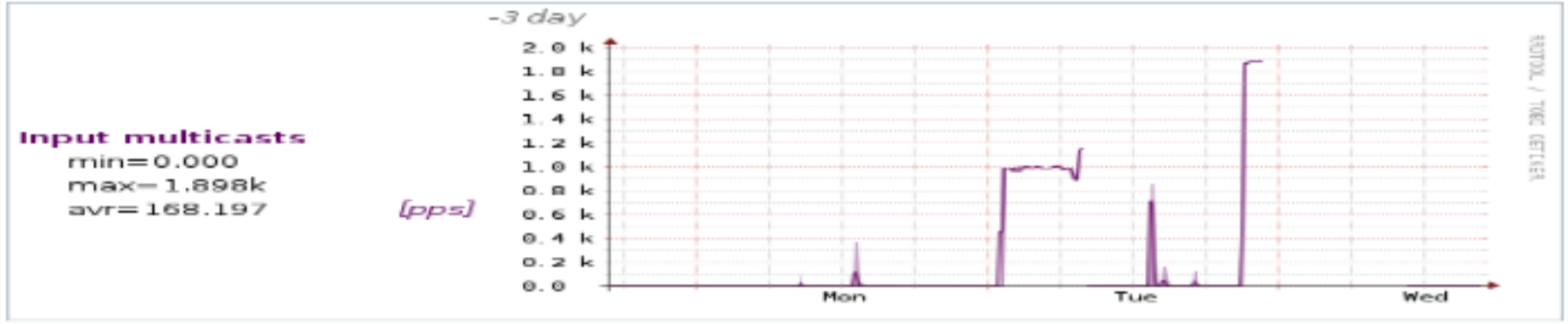
[HW]



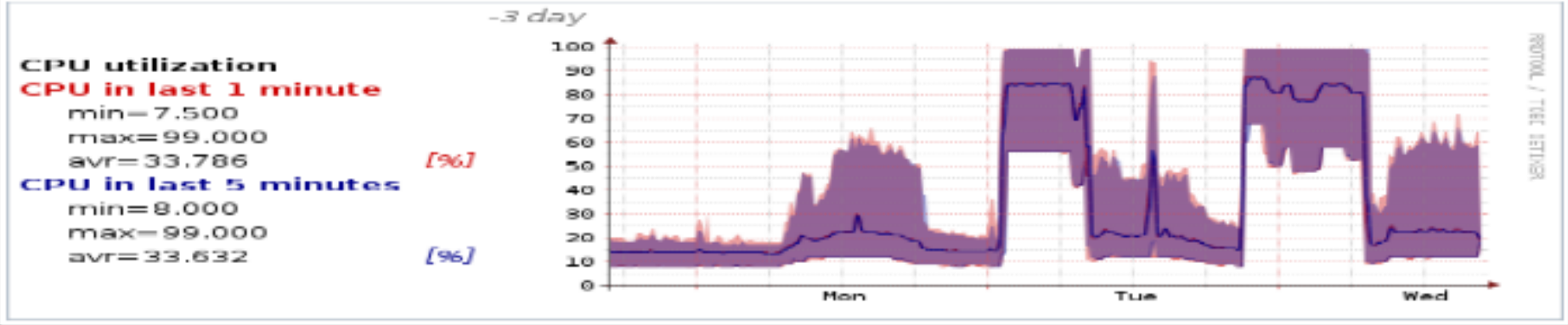
Systém G3 – interaktivní UI

- Ukázka (služba pro uživatelskou síť): hledání zdroje vysoké zátěže CPU – vyhledání konkrétního rozhraní (hluboko v infrastruktuře) s významným „příspěvkem“ multicast provozu – s průběhem analogickým zátěži CPU (CPU vizualizováno agregovaně)

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



[HW]



Systém G3 – interaktivní UI

- S **interaktivním UI** lze prakticky vše, ale...

*...je náročné – **a)** na technické znalosti uživatele, **b)** obecnost rozhraní jej činí složitým → OK pro síťové administrátory a specialisty, méně vhodné pro ostatní skupiny uživatelů...*

Je třeba i něco:

a) jednoduššího (ovládání, navigace) a srozumitelnějšího (interpretace dat) pro ostatní skupiny uživatelů

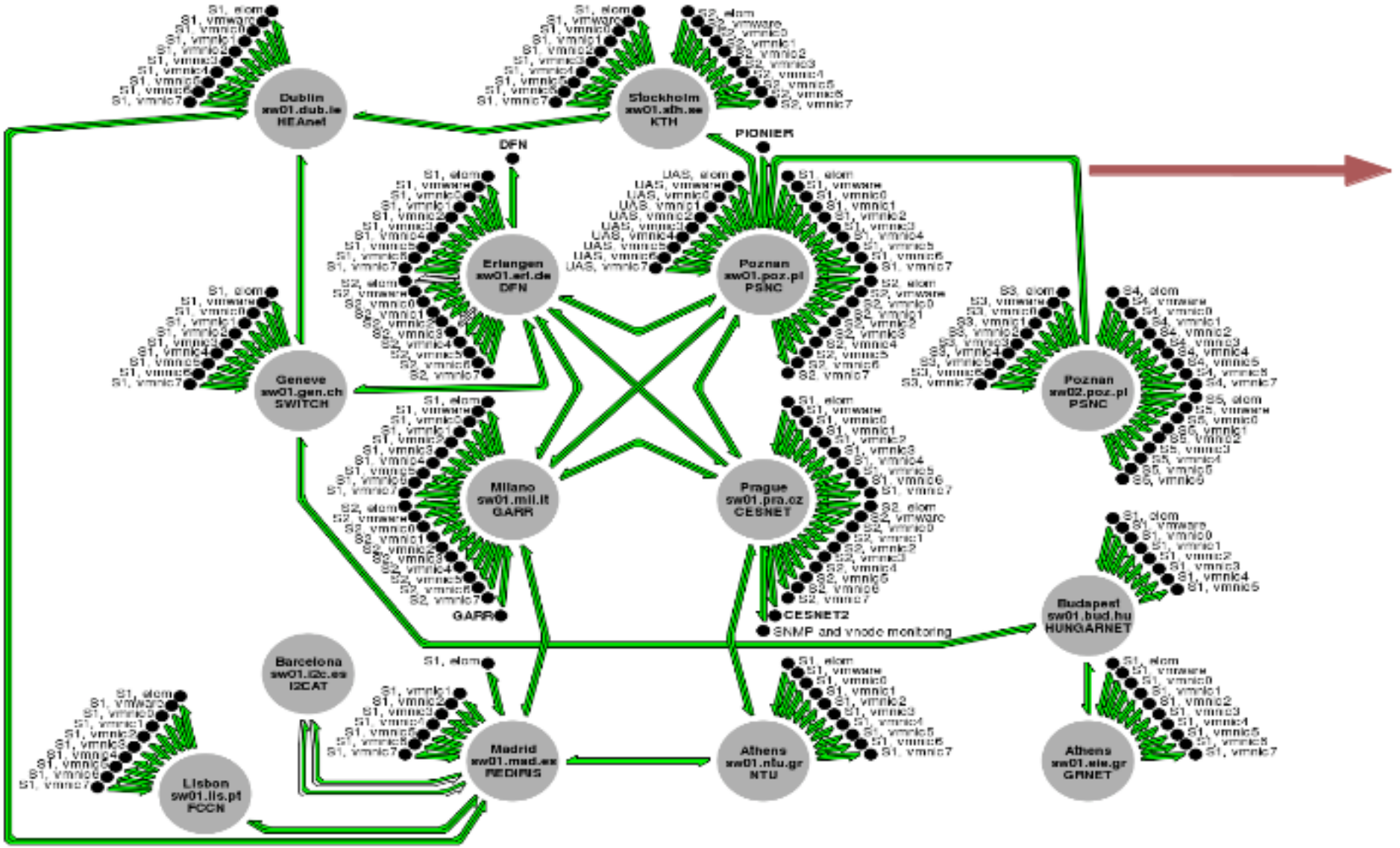
b) co by umělo automaticky detekovat a oznamovat anomálie

Systém G3 – reporter

- Struktury periodicky generovaných statických HTML stránek
  - Různé pohledy na sledovanou infrastrukturu a/nebo její část
  - Jednoduchá hierarchie (srozumitelnost navigace): **přehledová stránka** → **detailní výstupy** + příp. horizontální „prolinkování“
- Technicky řešeno ovládáním interaktivního UI přes STDIN/STDOUT (simulace chování skutečného uživatele)
- *Vhodné pro běžné uživatele – jednoduché & intuitivní, alespoň doufám ;-), vše na proklik*

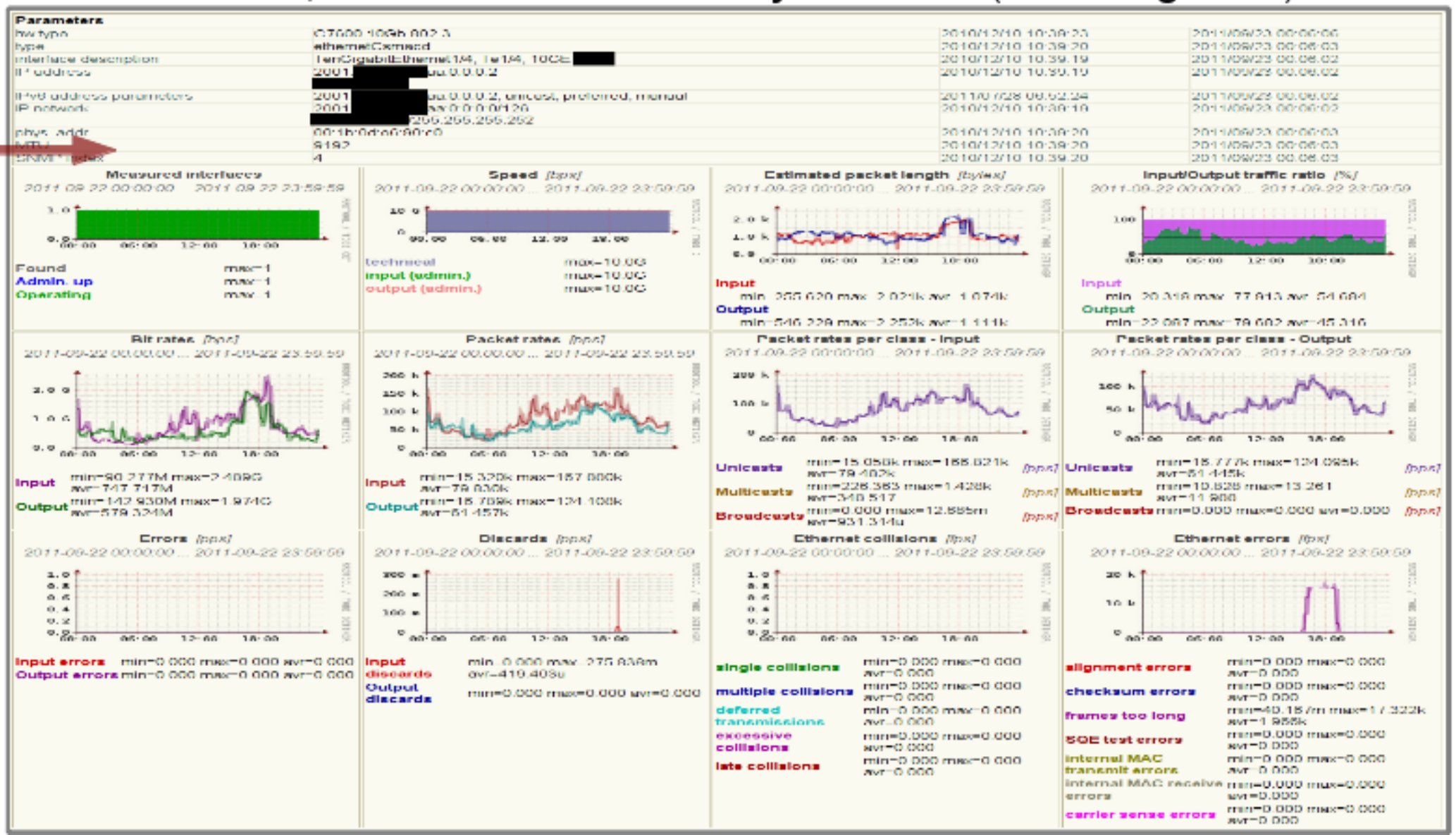
Systém G3 – reporter

- Ukázka monitorování infrastruktury projektu FEDERICA (FP7) – „zdraví sítě“, **úvodní přehledová stránka**



Systém G3 – reporter

- Ukázka detailního výstupu (proklik z mapy nebo z tabulky) – struktura, obsah i rozsah mohou být libovolné (dle konfigurace)



Systém G3 – reporter

- Ukázka monitorování využití streamovací platformy v e-Infrastruktuře CESNET

CESNET

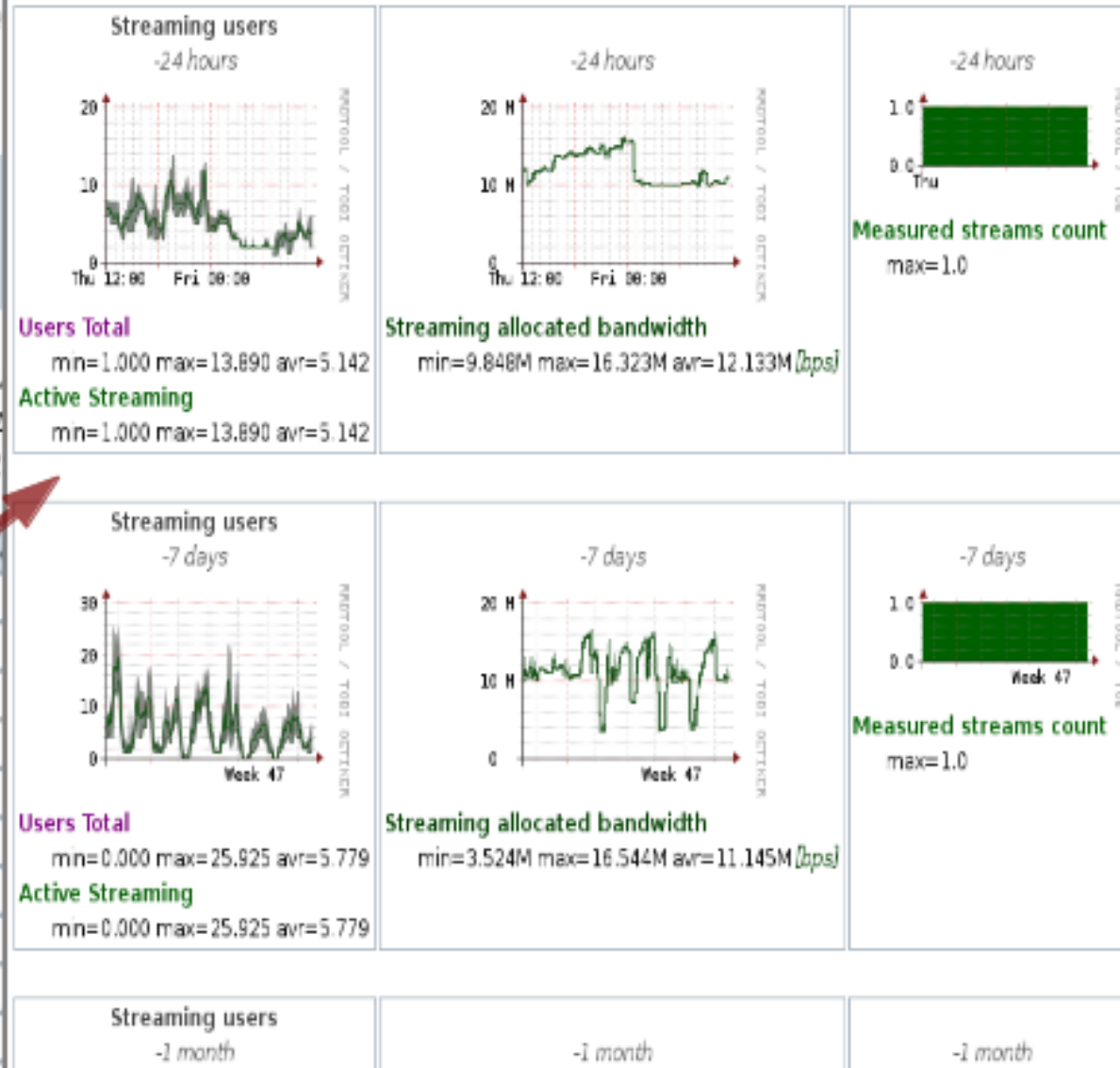
G3 system - reporte
author: Tom Kosnar,

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 (a
ser / sever14-vod	2.347	2.347
ser multisite	2.231	5.231
ser hdtv1	1.104	2.288
ser / zirafa1	0.000	0.000
ser / zirafa2	0.000	0.000
ser / zirafa3	0.000	0.000
ser / zoo1	0.000	0.000
ser / zoo2	0.000	0.000
ser / zoo3	0.000	0.000
ser / zoo6	0.000	0.000

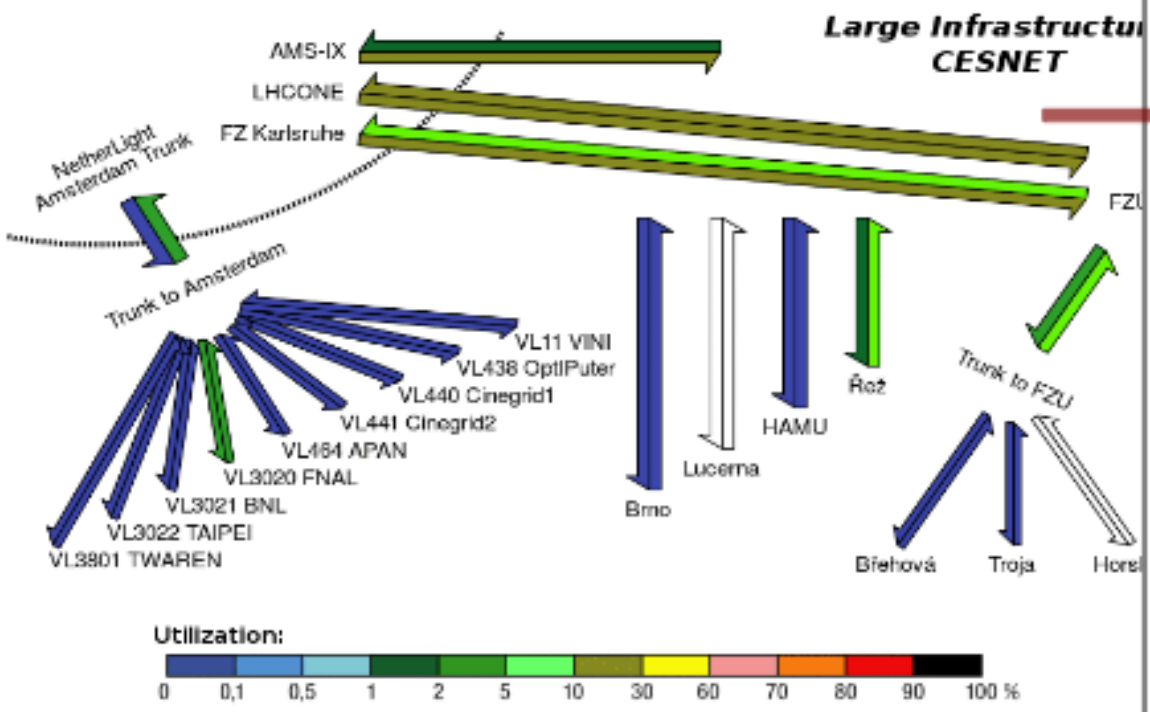


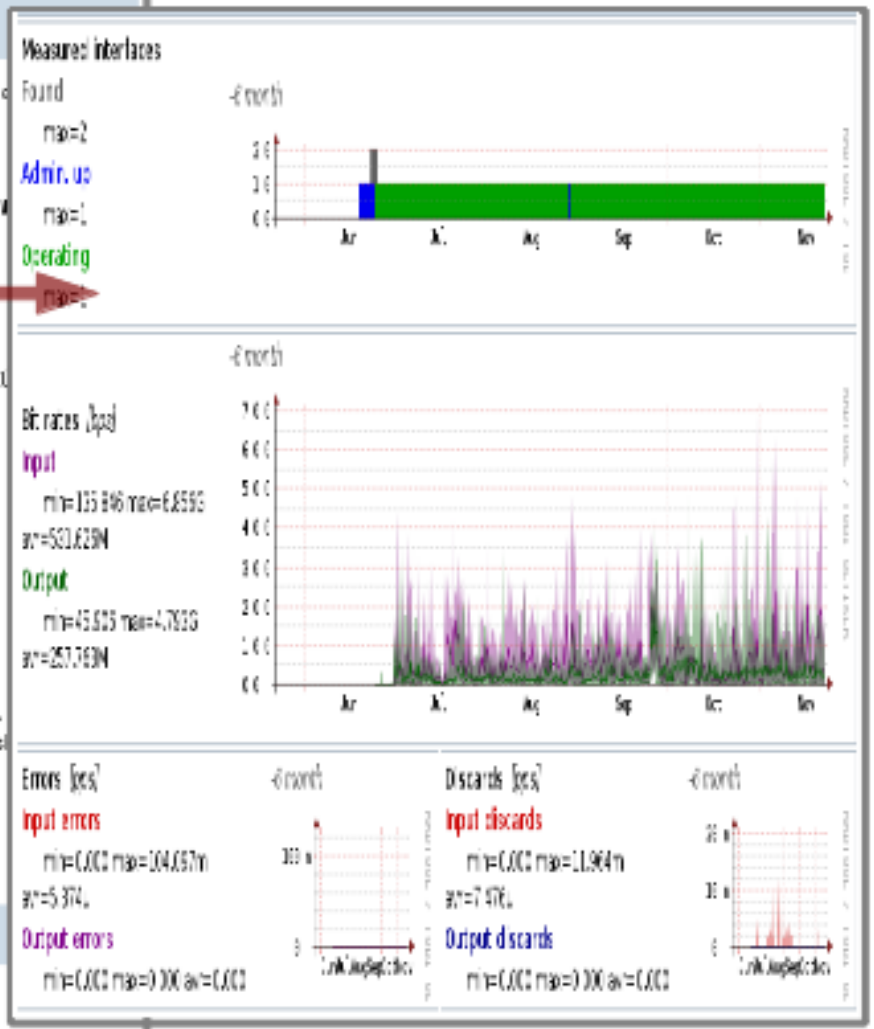
Systém G3 – reporter

- Ukázka monitorování vybraných E2E služeb v e-Infrastruktuře CESNET

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 presc
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.





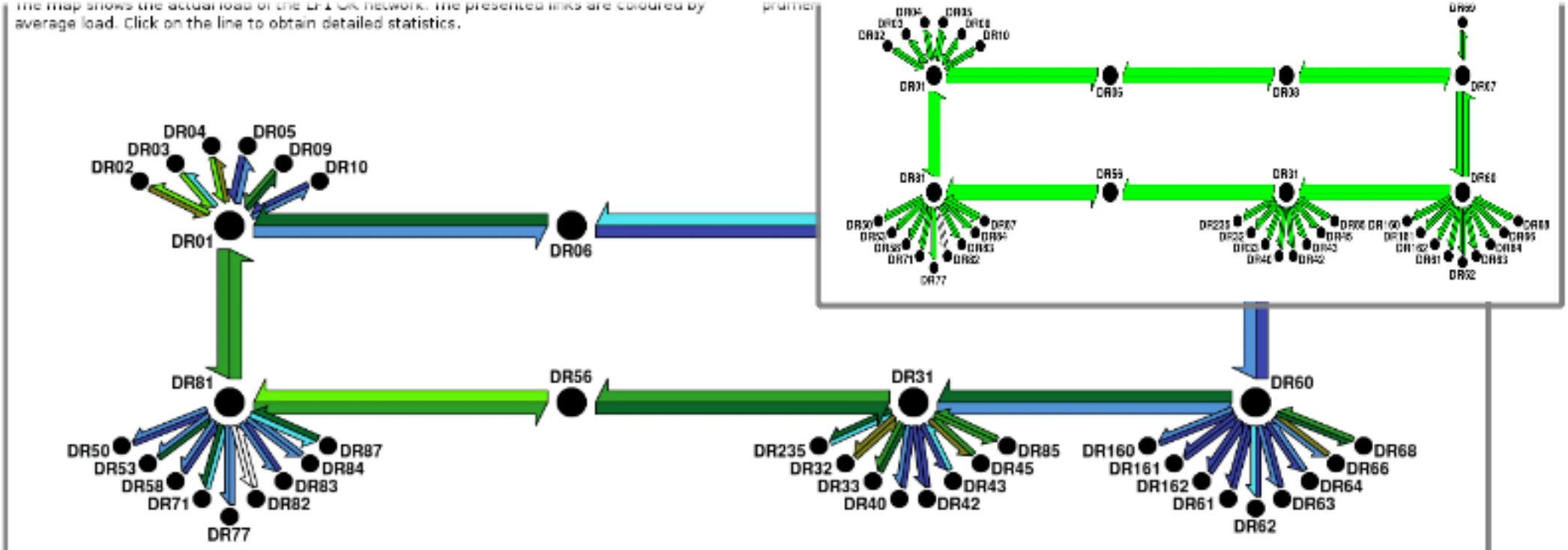
Other Information

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 %

Systém G3 – reporter

- Ukázka služby pro uživatele (úvodní stránky) – **využití & zdraví infrastruktury**



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

Systém G3 – reporter

- Ukázka služby pro uživatele – **přehledová stránka**

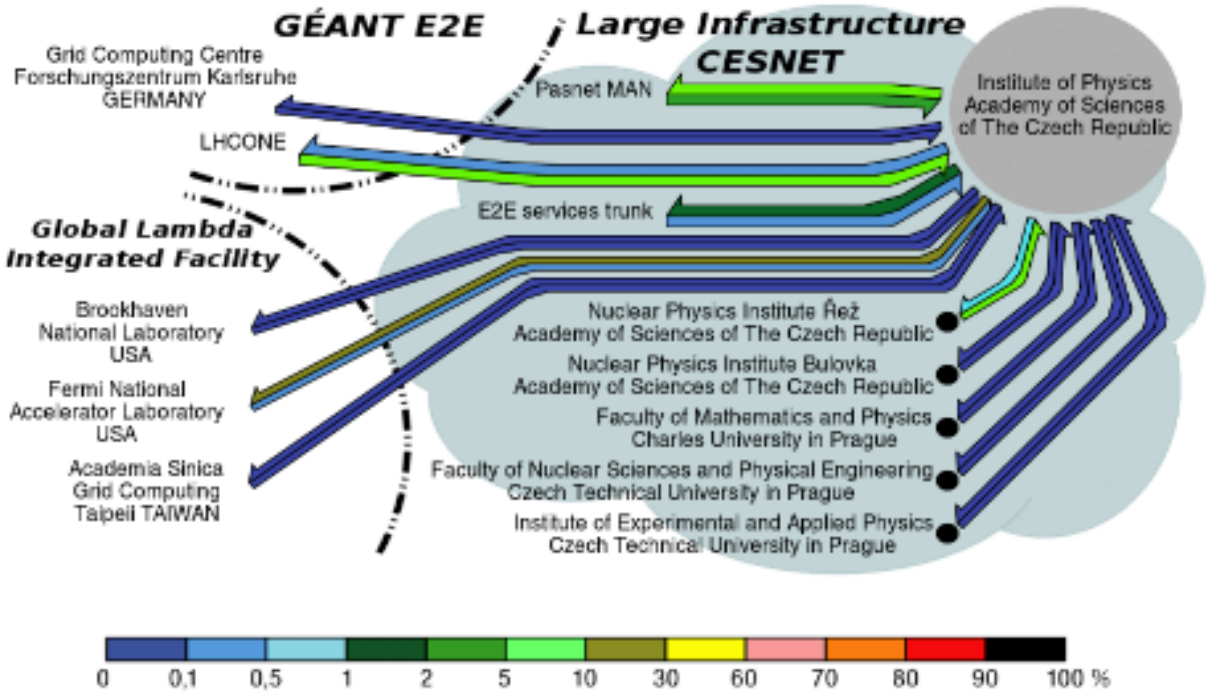
CESNET

G3 system - reporter
author: Tom Kosiar, copyright: © 2007-2013, CESNET z.s.p.o.

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.



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)
Institute of Physics ASCR Prague->Fermi National Accelerator Laboratory USA	18.732 %	1000.000 Mbps	187.320 Mbps	0.000 pps
LHCONE->Institute of Physics ASCR Prague	9.163 %	10.000 Gbps	916.321 Mbps	0.000 pps

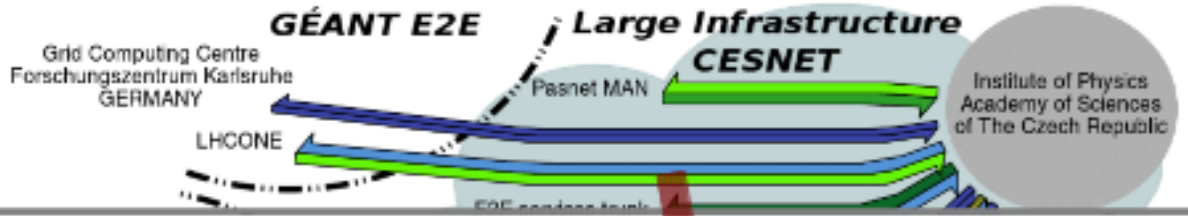
Systém G3 – reporter

– Ukázka služby pro uživatele – **detailní výstup**

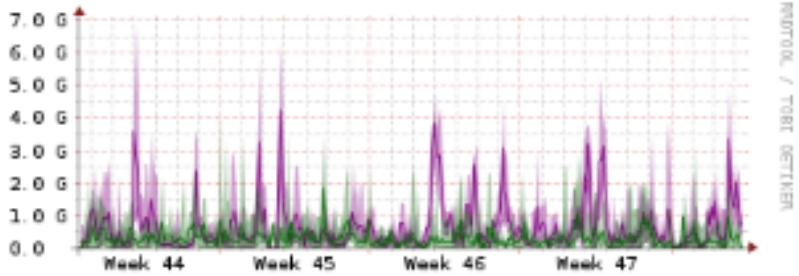
Large Infrastructure CESNET: Institute of Physics Academy of Sciences of The Czech Republic - network connections

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.

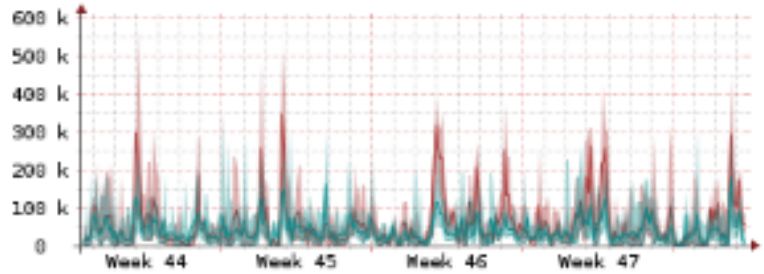


Bit rates *[bps]*
-1 month



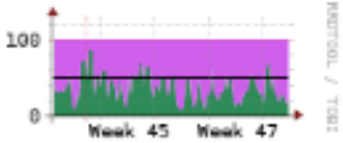
Input min=619.260k max=6.856G avr=691.786M
Output min=1.996M max=4.298G avr=311.151M

Packet rates *[pps]*
-1 month



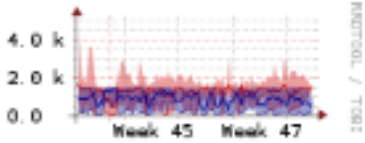
Input min=455.598 max=568.208k avr=60.428k
Output min=498.856 max=361.590k avr=43.240k

Input/Output traffic ratio *[%]*
-1 month



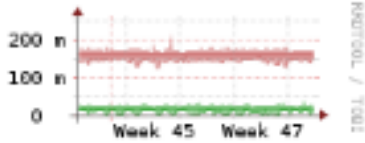
Input min=12.881 max=92.952 avr=62.446
Output min=7.048 max=87.119

Estimated packet length *[bytes]*
-1 month



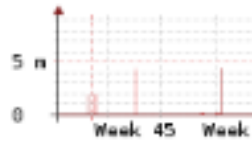
Input min=35.230 max=4.464k avr=1.311k
Output min=72.567 max=1.693k

Multicast packet rates *[pps]*
-1 month



Input min=127.187m max=216.519m avr=159.529m
Output min=0.000 max=40.567m

Broadcast packet rat
-1 month



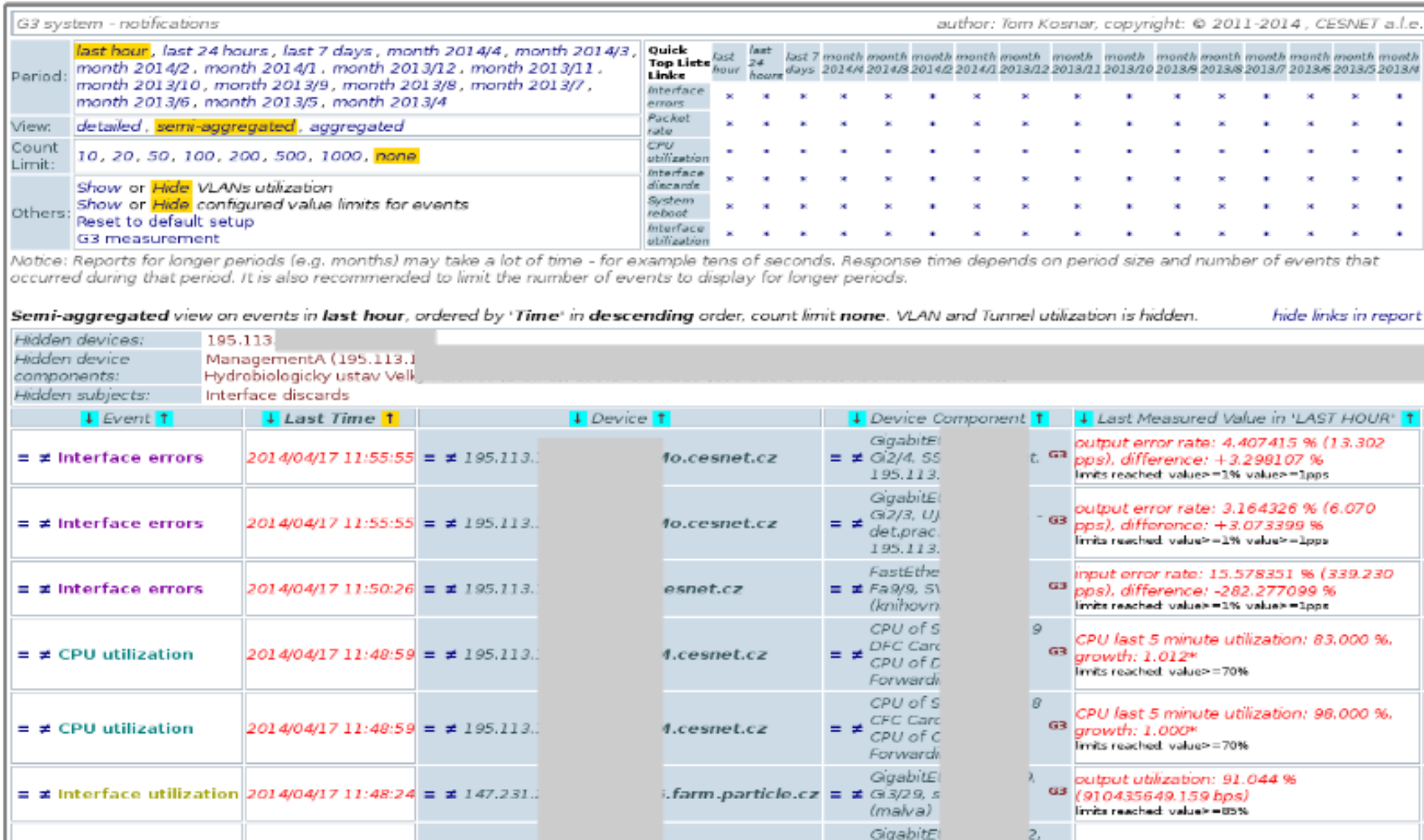
Input min=0.000 max=
avr=2.431u
Output min=0.000 max=

Systém G3 – vizualizace a notifikace událostí

- Založeno na on-fly porovnání aktuálně změřených (a/nebo zpracovaných) údajů (v měřícím jádru) vůči nakonfigurovaným limitů *(~ absolutní hodnoty, gradienty, změny,…)*
  - Limity konfigurované globálně nebo pro jednotlivá zařízení
  - Interaktivní „web-based“ (HTML) uživatelské rozhraní
  - Možný „plain-text“ výstup *(na základě konfigurace, vč. filtrů na konkrétní objekty atd..)* jako vstup pro Nagios, Icinga apod.
  - Možná specifická konfigurace pro různé skupiny uživatelů (filtrace ~ pouze konkrétní objekty ~ rozhraní, zařízení, typ událostí)

Systém G3 – vizualizace a notifikace událostí

- Ukázka HTML výstupu



G3 system - notifications — author: Tom Kosnar, copyright: © 2011-2014 , CESNET a.l.e.

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 Liste 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	month 2013/7	month 2013/6	month 2013/5	month 2013/4
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 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. hide links in report

Hidden devices:	195.113.
Hidden device components:	ManagementA (195.113.1 Hydrobiologicky ustav Velk
Hidden subjects:	Interface discards

Event	Last Time	Device	Device Component	Last Measured Value in 'LAST HOUR'
= ≠ Interface errors	2014/04/17 11:55:55	= ≠ 195.113. fo.cesnet.cz	= ≠ GigabitE Gi2/4, SS 195.113. t. G3	output error rate: 4.407415 % (13.302 pps), difference: +3.298107 % limits reached: value>=1% value>=1pps
= ≠ Interface errors	2014/04/17 11:55:55	= ≠ 195.113. fo.cesnet.cz	= ≠ GigabitE Gi2/3, UJ det.prac. 195.113. - G3	output error rate: 3.164326 % (6.070 pps), difference: +3.073399 % limits reached: value>=1% value>=1pps
= ≠ Interface errors	2014/04/17 11:50:26	= ≠ 195.113. esnet.cz	= ≠ FastEthe Fa9/9, S (knihovn G3	input error rate: 15.578351 % (339.230 pps), difference: -282.277099 % limits reached: value>=1% value>=1pps
= ≠ CPU utilization	2014/04/17 11:48:59	= ≠ 195.113. 1.cesnet.cz	= ≠ CPU of S DFC Card CPU of D Forwardi 9 G3	CPU last 5 minute utilization: 83.000 %, growth: 1.012* limits reached: value>=70%
= ≠ CPU utilization	2014/04/17 11:48:59	= ≠ 195.113. 1.cesnet.cz	= ≠ CPU of S CFC Card CPU of C Forwardi 8 G3	CPU last 5 minute utilization: 96.000 %, growth: 1.000* limits reached: value>=70%
= ≠ Interface utilization	2014/04/17 11:48:24	= ≠ 147.231. .farm.particle.cz	= ≠ GigabitE Gi3/29, s (malva)). G3	output utilization: 91.044 % (910435649.159 bps) limits reached: value>=85%
			GigabitE 2.	

Systém G3 – vizualizace a notifikace událostí

- Ukázka HTML výstupu - detail

Event	Last Time	Device	Device Component		Last Measured Value in 'LAST HOUR'	In 'LAST HOUR'	Total
= ≠ CPU utilization	2014/10/06 09:23:15	= ≠ 14	= ≠ CPU of Routing Processor 5, module	G3	CPU last 5 minute utilization: 83.000 %, growth: 1.012* limits reached: value>=70%	11 *	775 *
= ≠ CPU utilization	2014/10/06 09:23:13	= ≠ 14	= ≠ overall information	G3	CPU last 5 minute utilization: 83.000 %, growth: 1.012* limits reached: value>=70%	11 *	772 *
= ≠ Interface utilization	2014/10/06 09:23:07	= ≠ 19	= ≠ GigabitEthernet1/0/2, Gi1/0/2, Vysoka skola [redacted]	G3	output utilization: 90.966 % (90966333.056 bps) limits reached: value>=85%	4 *	676 *
= ≠ Broadcasts	2014/10/06 09:22:28	= ≠ 14	= ≠ Port-channel11, Po11, ha2	G3	output broadcast packet rate: 127257.493 pps -> 236034.899 pps, growth: 1.855* limits reached: value>=10000pps	10 *	278 *
= ≠ Multicasts	2014/10/06 09:22:28	= ≠ 14	= ≠ GigabitEthernet3/26, Gi3/26, swL041 (golias)	G3	output multicast packet rate: 71360.680 pps -> 156898.646 pps, growth: 2.199* limits reached: value>=100000pps	5 *	49 *
= ≠ Broadcasts	2014/10/06 09:22:28	= ≠ 14	= ≠ GigabitEthernet3/26, Gi3/26, swL041 [redacted]	G3	output broadcast packet rate: 55305.092 pps -> 78933.676 pps, growth: 1.427*	10 *	272 *

Systém G3 – vizualizace a notifikace událostí

- Ukázka plain-text výstupu s filtrací pro 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.          -BM.cesnet.cz;      CPU of Sub-Module 9
CPU utilization;       1397729682;    195.113.          -BM.cesnet.cz;      CPU of Sub-Module 8
Interface errors;      1397729616;    195.113.          1.cesnet.cz; FastEthernet9/9, Fa9/9, SVI
Interface errors;      1397729552;    195.113.          7-Mo.cesnet.cz;     GigabitEthernet2/4,
Interface errors;      1397729552;    195.113.          7-Mo.cesnet.cz;     GigabitEthernet2/3,
Interface utilization; 1397729079;    147.231.          506.far           cz;       GigabitEthe
Interface utilization; 1397728104;    147.231.          506.far           cz;       GigabitEthe
Interface utilization; 1397727490;    195.113.          106.cesnet.cz;      GigabitEthernet1/0/
ICMP echo loss; 1397726601;    195.113.          cesnet.cz;   ;      ICMP echo loss: 33.
# page created at Thu Apr 17 12:16:44 2014
```

Systém G3 – vizualizace a notifikace událostí

- Ukázka notifikací

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
```

Systém G3 – vizualizace a notifikace událostí

- Ukázka služby pro lokální síť – v závislosti na prostředí jsou podstatné i jiné údaje než v národní páteři – viz. STP

= ≠ Interface utilization	2014/04/17 10:25:34	= ≠ 10.1.56.101,	506A-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,	506A-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,	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,	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,	506A-DR56	G3	time since Stp topology changes: 00 hou minutes 30 seconds before time of measurement limits reached: value must grow
= ≠ Stp	2014/04/17 08:59:00	= ≠ 10.1.81.101,	4506A-DR81	G3	time since Stp topology changes: 00 hou minutes 32 seconds before time of measurement limits reached: value must grow
= ≠ CPU utilization	2014/04/17 08:49:51	= ≠ 10.1.8.101,	06A-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*

Systém G3 – vizualizace a notifikace událostí

- Ukázka detekovaného útoku na DNS CESNETu

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

Hidden devices: [redacted]
Hidden device components:

Event	Time	Device	Device Component	Measured Value
x ≠ Packet rate	2013/12/18 11:07:15	= ≠ 195.113. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	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. cesnet.cz	x ≠ Vlan4, Vl4, Cesne 2001:718:1:1:0:0 ne serv .113.14	G3 output unicast packet rate: 3120482.413 pps -> 2681636.330 pps, growth: 0.859*
			Vlan4, Vl4, Cesne ne serv	G3 output unicast packet rate: 2681636.330 pps ->

Systém G3 – vizualizace a notifikace událostí

- Ukázka detekovaného útoku na DNS CESNETu (grafy z perspektivy rozhrani smerovace k DNS serveru)

unrouted VLAN 4, VLAN-4, C _servers_l

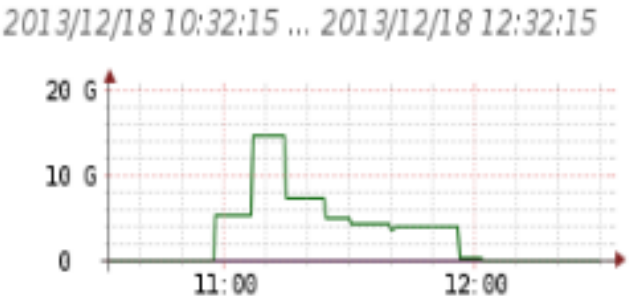
Bit rates *[bps]*

Input

min=1.358M
max=3.364M
avr=2.331M

Output

min=2.491M
max=14.657G
avr=3.154G



View (auto): 2. bit rates only

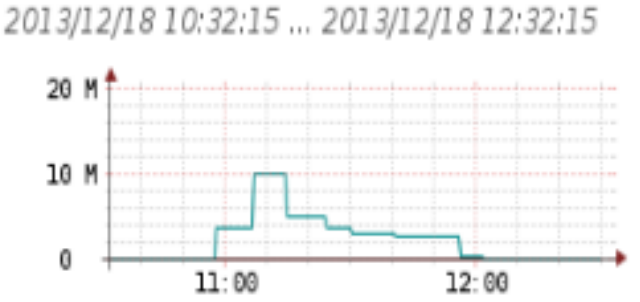
Packet rates *[pps]*

Input

min=1.348k
max=3.174k
avr=2.060k

Output

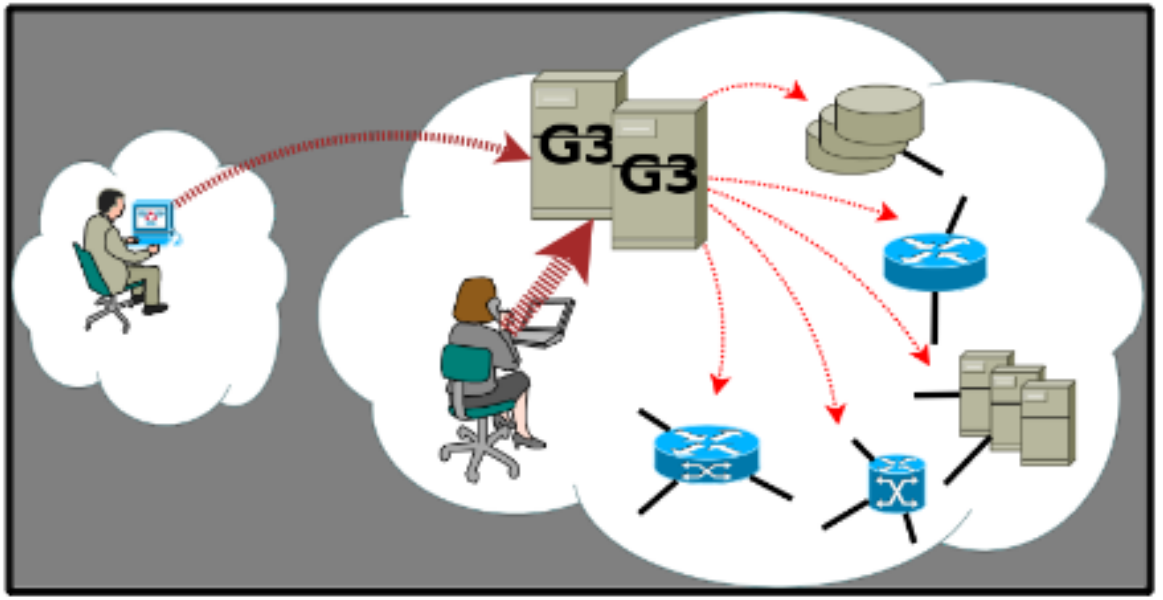
min=2.399k
max=10.005M
avr=2.203M



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

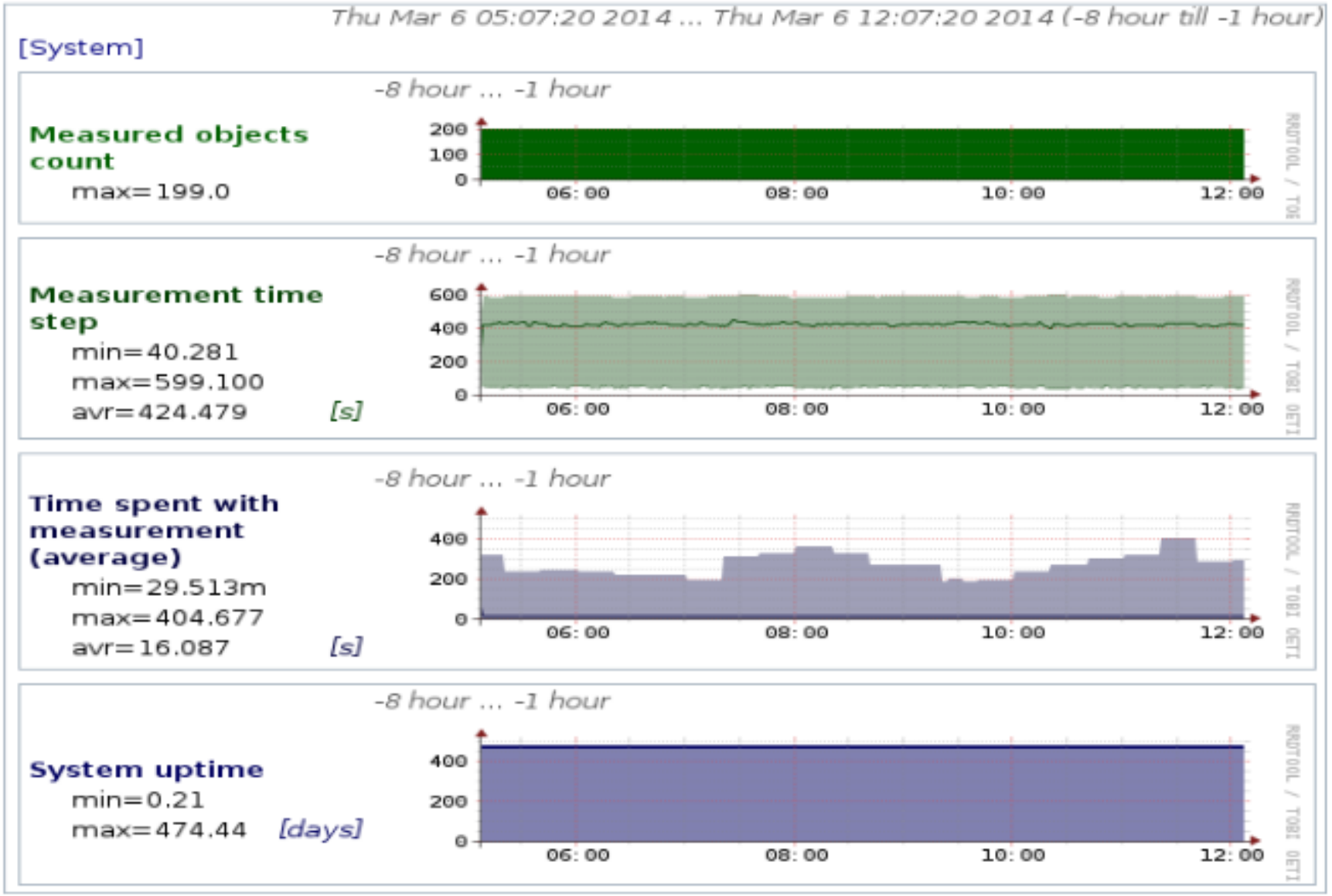
Systém G3 – typické způsoby poskytování služby

- Jako služba pro uživatelské skupiny v e-Infrastruktuře i pro sítě uživatelů
- **a) instalace v páteřní síti e-Infrastruktury CESNET**
  - Spravováno CESNETem, cílí na služby v e-Infrastruktuře
- **b) instalace v koncových sítí**
  - Sdílená správa OS
  - Správa a konfigurace aplikace - CESNET
  - Úspěšně provozováno i ve virtualizované infrastruktuře



Systém G3 – parametry systému v e-Infrastruktuře

- Ukázka sumárních parametrů primární instalace v páteřní síti e-Infrastruktury CESNET



Systém G3 – parametry systému v e-Infrastruktuře

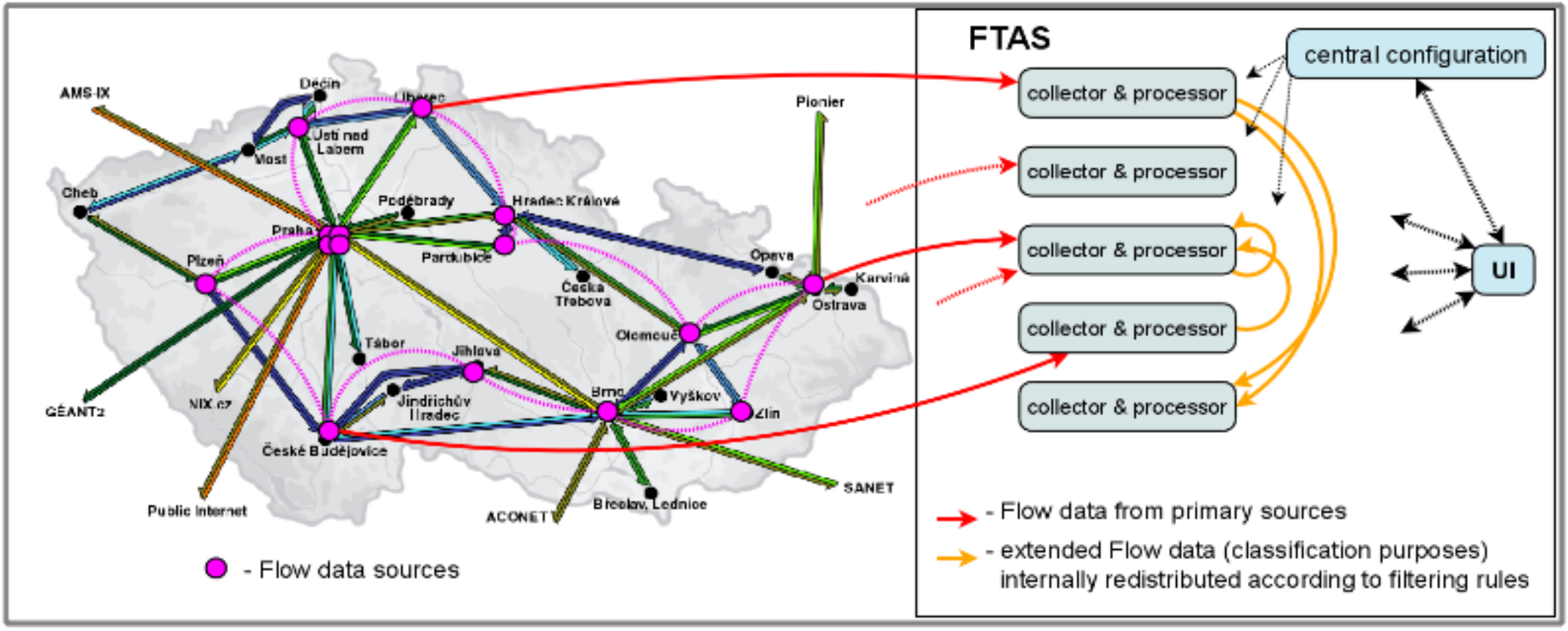
- 2 paralelní instalace ~ v každé měřeno ~ 200 zařízení, >700K údajů
- HW ~ 32 cores (E5-2690@2.9GHz), 192GB RAM, cca 1.5 TB v HW RAID 10 (SaS@15k) – většina dat je uložena v RRD ;-)
- Počet přístupů k interaktivnímu UI v roce 2014 ~ **3400** (pouze správci páteřní sítě)
- Počet přístupů k neveřejným výstupům modulu G3-reporter v roce 2014 ~ **320k** (členové týmů, institucí, správci služeb)
- Počet přístupů k veřejným výstupům modulu G3-reporter v roce 2014 ~ **330k**
- Počet přístupů k modulu vizualizace událostí v roce 2014 ~ **850k** (správci služeb, správci sítě, automaty)

Sledování IP provozu na bázi toků – systém FTAS

- Původně vyvíjen jako systém plošného sledování (~ traffic browser) IP provozu na bázi toků pro páteřní síť NREN *(ukázka před-před-předchozí generace prezentována EurOpen 2009)*, postupně rozšiřován od další moduly s novou funkcionalitou
- Použitelný v jakémkoli prostředí (LAN, MAN, WAN, kampus), jsou-li k dispozici zdroje informací o IP provozu (~netflow)
- Vývoj řízen uživateli (správci páteřní sítě a služeb e-Infrastruktury, CSIRTs, správci koncových sítí)
- Systémové komponenty
  - **Měřící jádro a základní zpracování "flow-based" dat**
  - Uživatelské rozhraní
    - **Interactivní UI**
    - **FTAS-reporter**
  - Specifické moduly (built-in)
    - **Následné statistické zpracování**
    - **Detekce anomálií**

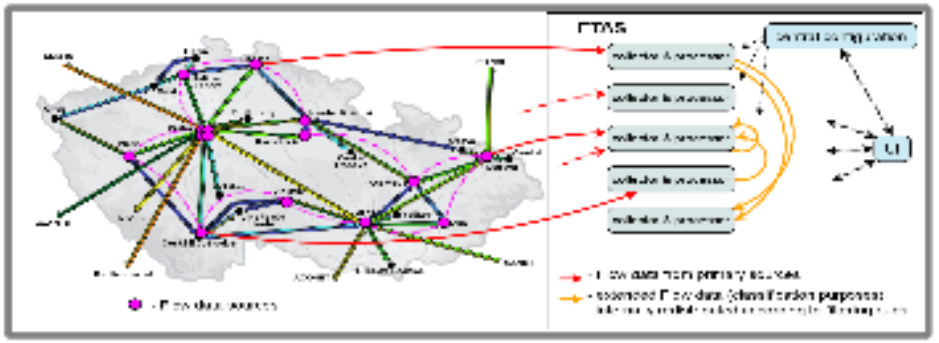
Systém FTAS – měřící jádro & zpracování dat

- **Zpracování provozu**: IPv4, IPv6
- **Exportní formáty a rozšíření**: v1,5,7,9,10, IPFIX, FlexibleNetflow, NetFlow Secure Event Logging
- **Architektura**: distribuovaná (centrální konfigurace, kolektory [DB může být vzdálená], UI, interní komunikace v4/v6), ale může běžet vše v jednom místě (úspěšně provozované ve virtuálech)



Systém FTAS – měřící jádro & zpracování dat

- **Řetěz primáního zpracování příchozích "flow-based" dat na kolektoru** (vše volitelné): replikace, multiplexing, parsing, klasifikace (~ významové, admistrativní, organizační začlenění), filtrace, on-fly detekce anomálií/možných útoků, on-fly procedura (redukce/modifikace záznamu – kód v konfiguraci), uložení
  - **Obvykle uložené datové entity** (libovolné konfigurace): podle zdrojů dat (směrovače, sondy), organizace a jejich části (univerzita → fakulty), zájmový provoz (na základě klasifikace a filtračních podmínek)
- **Následné statistické zpracování**: vyhledání z uložených dat (podle konfigurace), agregace podle skupin (~ fakulty v rámci univerzity), souhrnná agregace, uložení (v závislosti na konfiguraci dosahujeme průměrně cca 1:600 redukce objemu dat při zachování charakteristiky provozu)

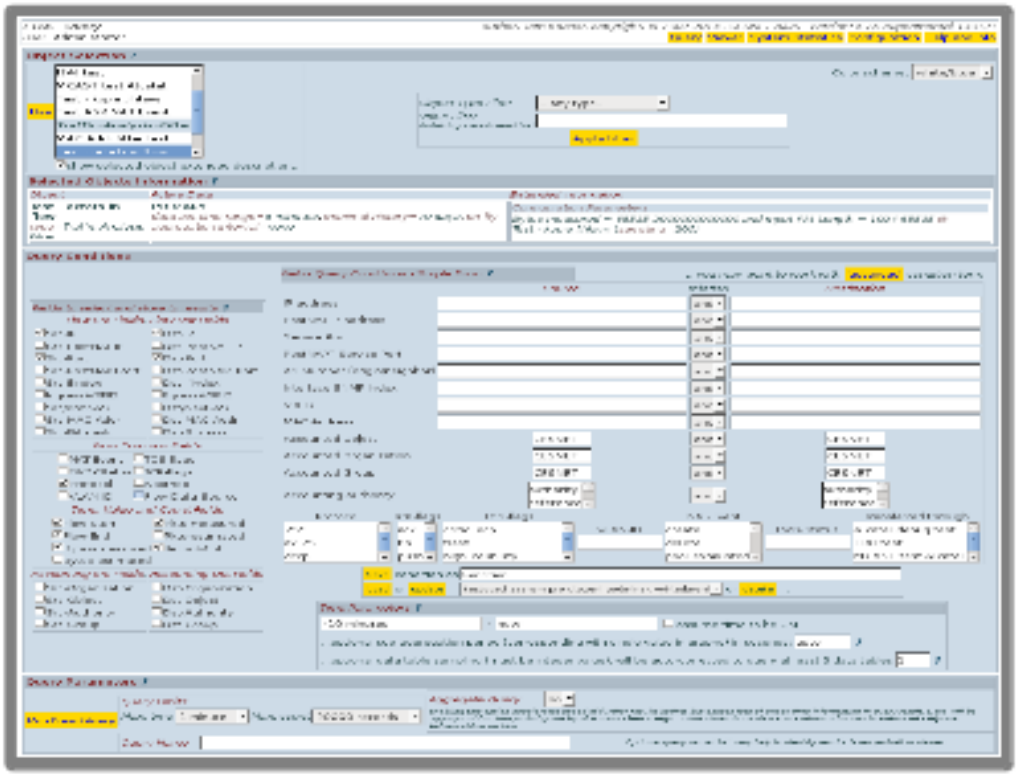


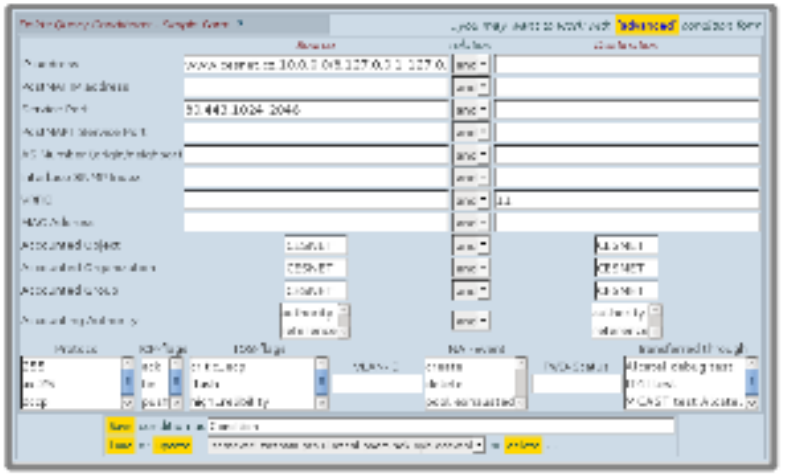
Systém FTAS – interaktivní UI

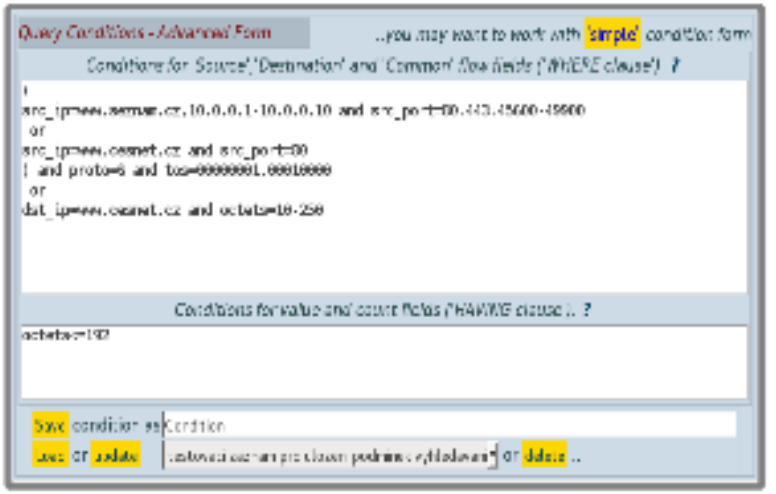
- Interaktivní "traffic-browser" pro IP provoz
- Umožňuje mj. vyhledat/analyzovat libovolný zájmový provoz v rámci historie dané dobou uchování dat
- Princip práce - 2 kroky
  - **a) Vyhledání dat**
    - Z libovolného množství uložených a/nebo statisticky zpracovaných datových sad *(např. ze zdrojových dat 3 směrovačů a 1 sondy)*
    - Komplexní vyhledávací aparát *(neomezená logická struktura podmínek pro vyhledávání)*
  - **b) Vizualizace vyhledaných dat**
    - Komplexní vyhledávací aparát
    - Flexibilita vizualizace - třídění, agregace, různé typy výstupu (tabulky, grafy, plain-text)
- *Komplexní, ale relativně složité, vhodné pro znalé uživatele*

Systém FTAS – interaktivní UI

- Ukázky formuláře pro vyhledávání
  - Plně adaptivní z hlediska vybraných zdrojů (dostupné informace + podmínky pro vyhledání)
  - Přepínatelný obecný a strukturovaný formulář pro zadání vyhledávacích podmínek







Object Selection

Use

- Prague: [redacted]
- Usti nad [redacted] 111
- Usti nad [redacted] SEAS internal
- Zlin: R1[redacted]
- ***Traffic-Analysis-Filter***
- 6to4 incoming traffic
- 6to4 outgoing traffic

☑ show selected object extended description...

Color scheme: white/blue

Object Type Filter ...any type...
Value Filter (regexp)
Apply filter

Selected Objects Information

Object	*Active Data*	*Extended information*
Prague[redacted] *type=Flo[redacted]Source, id=389*	**PRIMARY** *data set time range=10 minutes, maximal history=65 days, on-fly aggregation interval=none*	*Configuration Parameters* *input sampling=1, internal sampling=3, flow version=5,7,9*
Zlin: R1[redacted] *type=Flow-Data-Source, id=30*	**PRIMARY** *data set time range=15 minutes, maximal history=65 days, on-fly aggregation interval=none*	*Configuration Parameters* *input sampling=1, internal sampling=3, flow version=5,7,9*

Query Conditions

Flow Src. Fields, Flow Dst. Fields

☑ Src-IP	☑ Dst-IP
☑ Src-Port	☑ Dst-Port
☐ Src/Prev-AS	☐ Dst/Next-AS
☐ Src-ifIndex	☐ Dst-ifIndex
☐ Src-Bitmask	☐ Dst-Bitmask

Flow Common Fields

☑ Protocol ☐ Nexthop ☐ TOS-flags ☐ Flow-Data-Source ☐ TCP-flags

Time, Value and Count Fields

☐ Flow-Start	☑ Bytes-estimated
☐ Flow-End	☐ Pkts-measured
☐ Bytes-measured	☑ Pkts-estimated

Fields Query Conditions - Simple Form ...you may want to work with 'advanced' condition form

	Source	relation	Destination
IP address	www.debian.cz,ftp.sh.cvut.cz	and	195.113.150.0/25, ::-fff:fff:fff:fff:fff:fff:fff
Service Port	21,80	and	
AS Number (origin/neighbor)		and	
Interface SNMP Index		and	

Protocol: 255, ax.25, dccp
TCP-flags: ack, fin, push
TOS-flags: critic_ecp, flash, high_relibility

Time Parameters

-10 minute - now ☐ assume time to be GMT;

...optional sub-aggregation period (corresponding with single value in graphs) in seconds: auto

...optional data table sampling (must be integer value); will be auto-corrected to query at least 3 data tables: 1

Query Parameters

Run New Query

Query Limits

Max. query time 1 minute *Max. record count* 20000 records

☐ run in background ...after finishing notify to:

Aggregate Query no

*Enabling this option accelerates speed of further results listing, but causes loss of exact time information in query result. Data will be aggregated for time period given by '**data set time range**' value shown in **Active Data** information box in **Selected Objects Information** section.*

Fields Query Conditions - Simple Form ?

...you may want to work with 'advanced' condition form

	Source	relation	Destination
IP address	www.cesnet.cz,10.0.0.0/8,127.0.0.1-127.0.	and	
PostNAT IP address		and	
Service Port	80,443,1024-2048	and	
PostNAPT Service Port		and	
AS Number (origin/neighbor)		and	
Interface SNMP Index		and	
VRFID		and	11
MAC Address		and	
Accounted Object	CESNET	and	CESNET
Accounted Organization	CESNET	and	CESNET
Accounted Group	CESNET	and	CESNET
Accounting Authority	authority reference	and	authority reference

Protocol	TCP-flags	TOS-flags	VLAN-ID	NAT-Event	FWD-Status	Transferred through
255 ax.25 dccp	ack fin push	critic_ecp flash high_relibility		create delete pool exhausted		

Save condition as Condition

Load or update testovaci zaznam pro ulozeni podminek vyhledavani or delete ...

Query Conditions - Advanced Form

...you may want to work with 'simple' condition form

Conditions for 'Source','Destination' and 'Common' flow fields ('WHERE clause'). ?

```
(
src_ip=www.seznam.cz,10.0.0.1-10.0.0.10 and src_port=80,443,45600-49900
 or
src_ip=www.cesnet.cz and src_port=80
) and proto=6 and tos=00000001,00010000
 or
dst_ip=www.cesnet.cz and octets=10-250
```

Conditions for value and count fields ('HAVING clause'). ?

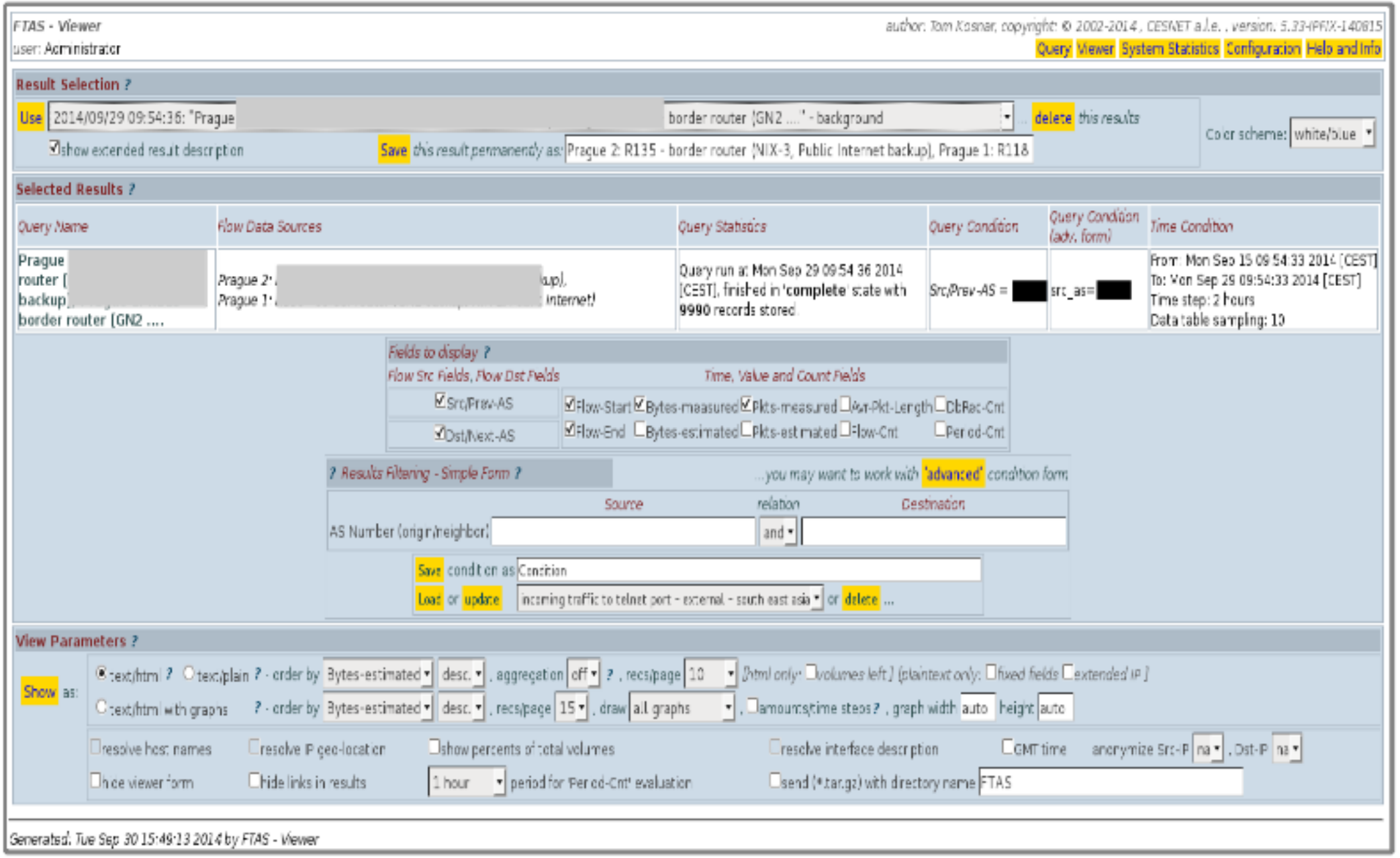
```
octets<=192
```

Save condition as Condition

Load or update testovaci zaznam pro ulozeni podminek vyhledavani or delete ...

Systém FTAS – interaktivní UI

- Formulář pro vizualizaci – analogický vyhledávacímu, adaptivní



Systém FTAS – interaktivní UI

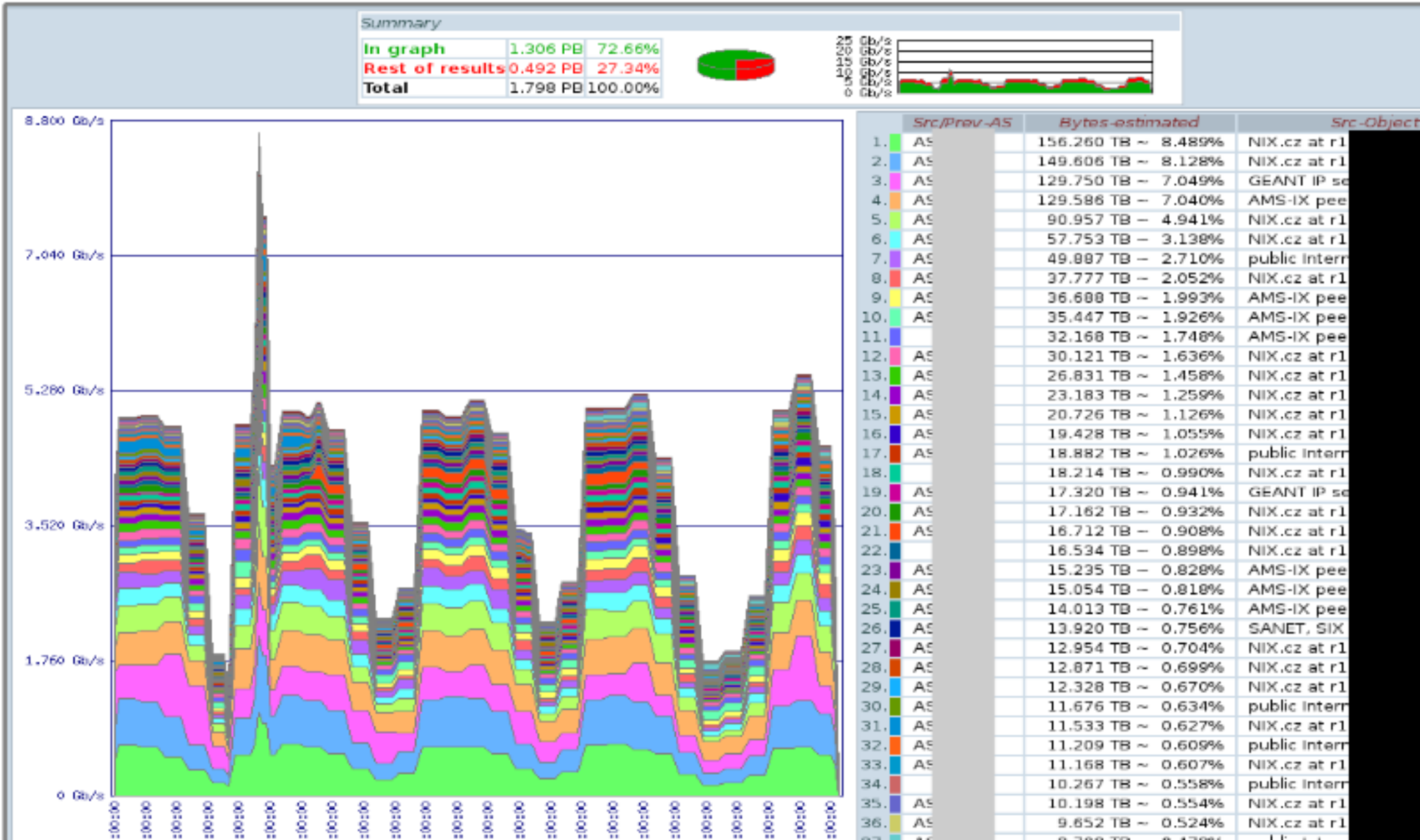
- Formulář pro vizualizaci, ukázky – tabulkový výstup, využití agregačních vlastností

	Src-IP	Dst-IP	Pkts-estimated	Bytes-estimated	Src-Port	Protocol	Avr-Pkt-Length	Dst-Port-Cnt
1.	2001:718:1:4:0:0:0:2	2001:4dd0:ff00:8ab:0:0:0:2	62.904 kp	76.566 MB	www (80)	tcp (6)	1276.32	2
2.	2001:718:2:0:0:0:0:222	2001:718:7:2:2963:36ca:6e55:bd4c	32.410 kp	44.440 MB	www (80)	tcp (6)	1437.80	87
3.	2001:718:2:0:0:0:0:222	2a00:1398:9:fb00:c985:7ff7:f0e8:3cb5	23.160 kp	30.572 MB	www (80)	tcp (6)	1384.18	76
4.	2001:718:1:4:0:0:0:2	2001:1528:136:dead:beef:0:0:1002	17.565 kp	25.107 MB	www (80)	tcp (6)	1498.79	1
5.	2001:718:2:0:0:0:0:222	2001:6f8:13e8:c0ff:1830:fb88:d44f:e9b4	18.316 kp	21.569 MB	www (80)	tcp (6)	1234.82	69
6.	2001:718:2:0:0:0:0:222	2002:e63:de03:0:0:0:e63:de03	9.328 kp	11.304 MB	www (80)	tcp (6)	1270.69	4
7.	2001:718:2:0:0:0:0:222	2001:470:1f06:a69:0:0:0:2	7.088 kp	9.702 MB	www (80)	tcp (6)	1435.22	25
8.	2001:718:2:0:0:0:0:222	2001:690:2180:80:6813:e525:daa3:193c	3.372 kp	4.700 MB	www (80)	tcp (6)	1461.59	9
9.	2001:718:1:4:0:0:0:2	2001:4de8:b0ba:deb0:215:c5ff:feff:2f	3.222 kp	4.558 MB	www (80)	tcp (6)	1483.32	2
10.	2001:718:2:0:0:0:0:222	2001:878:91e:2:0:1:0:0	3.406 kp	4.517 MB	www (80)	tcp (6)	1390.46	53
11.	2001:718:1:4:0:0:0:2	2a01:430:37:0:0:0:0:12	2.574 kp	3.640 MB	www (80)	tcp (6)	1482.81	2
12.	2001:718:2:0:0:0:0:222	2001:718:7:2:9d85:3e18:7f8e:3d35	1.910 kp	2.613 MB	www (80)	tcp (6)	1434.48	5
13.	2001:718:2:0:0:0:0:222	2001:718:801:168:1278:d2ff:fe70:62f5	1.426 kp	1.973 MB	www (80)	tcp (6)	1450.81	4
14.	2001:718:2:0:0:0:0:222	2a00:1a40:0:459:74f3:aa93:c120:45c0	0.834 kp	1.150 MB	www (80)	tcp (6)	1445.80	4
15.	2001:718:1:4:0:0:0:2	2001:1488:800:400:0:0:0:249	0.633 kp	0.887 MB	www (80)	tcp (6)	1470.05	1
16.	2001:718:1:4:0:0:0:2	2001:718:2:1611:0:1:0:d0	0.690 kp	0.833 MB	www (80)	tcp (6)	1266.12	2
17.	2001:718:1:4:0:0:0:2	2001:1528:1:e:250:56ff:fe88:4a61	0.558 kp	0.773 MB	www (80)	tcp (6)	1452.03	1

	Src-IP	Pkts-estimated	Bytes-estimated	Src-Port	Protocol	Avr-Pkt-Length	Record-Cnt	Dst-IP-Cnt	Dst-Port-Cnt
1.	2001:718:2:0:0:0:0:222	105.108 kp	135.869 MB	www (80)	tcp (6)	1355.46	479	87	473
2.	2001:718:1:4:0:0:0:2	93.999 kp	117.934 MB	www (80)	tcp (6)	1315.58	62	48	60
3.	2001:718:2:0:0:0:0:222	92.000 p	8.582 KB	ftp (21)	tcp (6)	95.52	3	3	3
4.	2001:718:1:4:0:0:0:2	90.000 p	7.119 KB	ftp (21)	tcp (6)	81	6	1	6

Systém FTAS – interaktivní UI

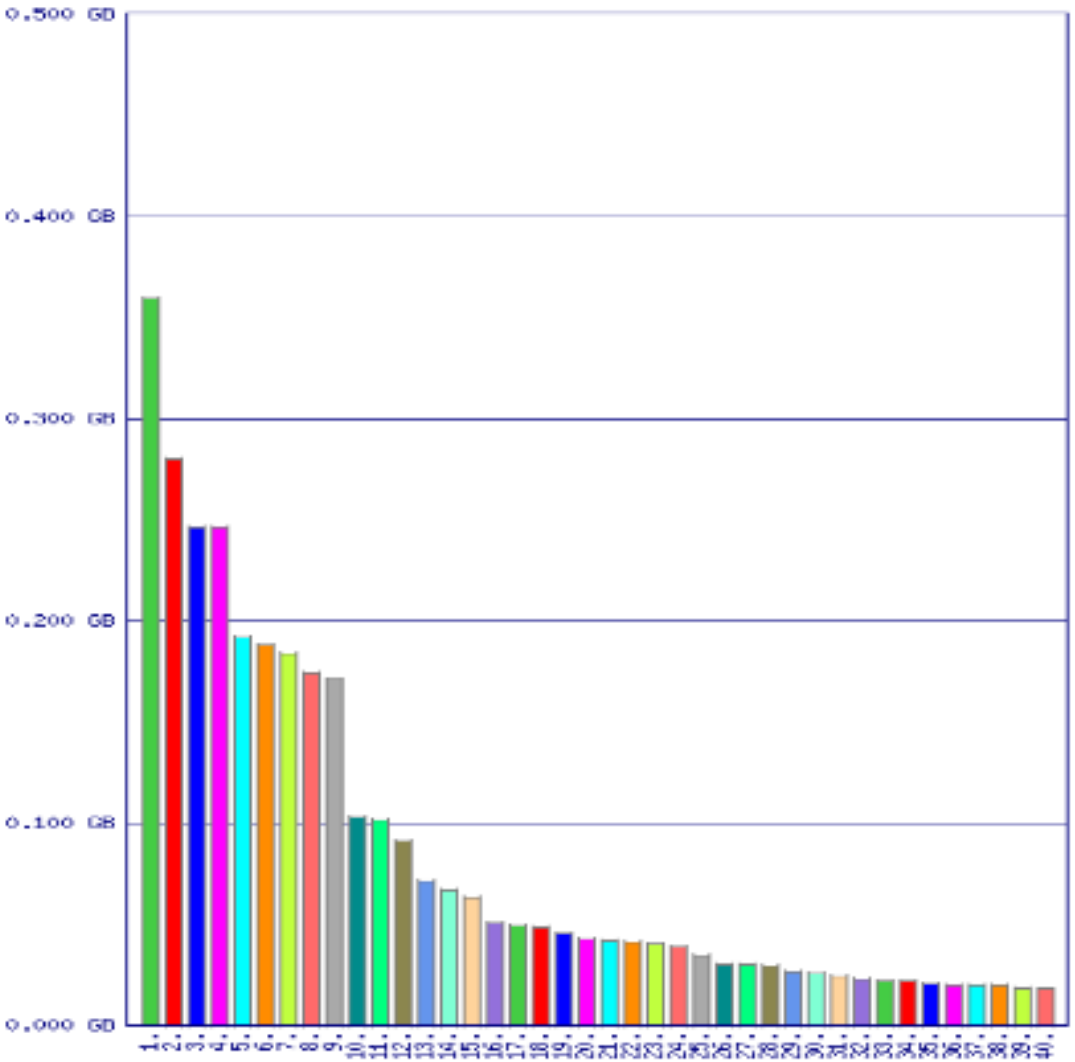
- Formulář pro vizualizaci, ukázky – grafický výstup, průběhové údaje, ze statisticky předzpracovaných dat



Systém FTAS – interaktivní UI

- Formulář pro vizualizaci, ukázky – grafický výstup, sumarizace

Summary		
In graph	3.322 GB	75.96%
Rest of results	1.051 GB	24.04%
Total	4.374 GB	100.00%



	Bytes-estimated	Src-Port	Dst-Port	Protocol
1	0.359 GB	www (80)	53460	tcp (6)
2	0.280 GB	www (80)	62544	tcp (6)
3	0.246 GB	www (80)	60868	tcp (6)
4	0.246 GB	www (80)	56632	tcp (6)
5	196.501 MB	www (80)	58780	tcp (6)
6	192.633 MB	www (80)	56665	tcp (6)
7	188.369 MB	www (80)	62816	tcp (6)
8	178.350 MB	www (80)	59388	tcp (6)
9	175.128 MB	www (80)	52069	tcp (6)
10	105.657 MB	www (80)	50131	tcp (6)
11	103.724 MB	www (80)	50772	tcp (6)
12	93.208 MB	1935	56069	tcp (6)
13	73.077 MB	www (80)	53355	tcp (6)
14	68.554 MB	www (80)	55634	tcp (6)
15	64.494 MB	1935	50189	tcp (6)
16	52.104 MB	www (80)	62842	tcp (6)
17	50.639 MB	www (80)	55678	tcp (6)
18	50.030 MB	www (80)	49652	tcp (6)
19	46.553 MB	www (80)	51932	tcp (6)
20	43.769 MB	www (80)	52401	tcp (6)
21	42.864 MB	www (80)	50963	tcp (6)
22	41.860 MB	www (80)	62610	tcp (6)
23	41.449 MB	www (80)	2177	tcp (6)
24	39.953 MB	www (80)	60456	tcp (6)
25	35.376 MB	www (80)	49363	tcp (6)
26	31.191 MB	www (80)	52518	tcp (6)
27	31.070 MB	www (80)	57824	tcp (6)
28	30.268 MB	www (80)	51892	tcp (6)
29	27.237 MB	www (80)	52043	tcp (6)
30	26.359 MB	www (80)	58246	tcp (6)
31	24.947 MB	www (80)	53847	tcp (6)
32	23.435 MB	www (80)	54173	tcp (6)
33	22.835 MB	www (80)	50246	tcp (6)
34	22.360 MB	www (80)	52868	tcp (6)
35	20.856 MB	rtsp (554)	49238	tcp (6)
36	20.586 MB	www (80)	53222	tcp (6)
37	20.387 MB	www (80)	57702	tcp (6)
38	19.942 MB	rtsp (554)	49709	tcp (6)
39	19.060 MB	www (80)	49758	tcp (6)

Systém FTAS – interaktivní UI

- Formulář pro vizualizaci, ukázky – "plain-text" výstup

```
# src_ip;src_ip_geo;dst_ip;dst_ip_geo;pkts;pkts_percent;octets;octets_percent;first;last;src_port;dst_port;tcp_flags;proto;tos;s
147.251.x.x;CZ;89.103.x.x;CZ;297792;14.4076357682795;446514085;19.0828909426944;11/10/20 16:49:37.915;11/10/20 16:50:44.091;www
147.231.x.x;CZ;147.251.x.x;CZ;250195;12.1048195755584;355276900;15.1836427223982;11/10/20 16:52:12.366;11/10/20 16:57:18.350;427
147.231.x.x;CZ;147.251.x.x;CZ;250124;12.1013844861687;355176080;15.1793339287241;11/10/20 16:47:06.458;11/10/20 16:52:12.506;427
147.251.x.x;CZ;89.103.x.x;CZ;207402;10.0344283043625;311103000;13.2957611425518;11/10/20 16:51:50.381;11/10/20 16:56:50.797;www
147.251.x.x;CZ;94.113.x.x;CZ;100403;4.85765183095103;150604500;6.43645821156799;11/10/20 16:47:32.604;11/10/20 16:52:39.164;www
147.251.x.x;CZ;94.113.x.x;CZ;90191;4.36357953731765;135286500;5.78180535003465;11/10/20 16:52:39.588;11/10/20 16:57:43.460;www (
147.251.x.x;CZ;90.183.x.x;CZ;87208;4.2192574014081;130800747;5.59009552906704;11/10/20 16:47:02.609;11/10/20 16:52:15.185;www (8
147.251.x.x;CZ;90.183.x.x;CZ;77538;3.75140790283438;116307000;4.97066917132515;11/10/20 16:47:46.004;11/10/20 16:52:51.220;www (
147.251.x.x;CZ;90.183.x.x;CZ;77507;3.74990807507267;116260500;4.96868187807138;11/10/20 16:48:45.029;11/10/20 16:53:52.229;www (
147.251.x.x;CZ;90.176.x.x;CZ;36147;1.74884755170051;53931324;2.3048893839197;11/10/20 16:46:37.229;11/10/20 16:51:38.413;www (80
147.251.x.x;CZ;89.102.x.x;CZ;28722;1.3896146119994;43082098;1.84122070352265;11/10/20 16:56:43.060;11/10/20 16:57:39.508;www (80
147.251.x.x;CZ;147.251.x.x;CZ;6040;0.292224505830943;8861324;0.378710739886023;11/10/20 16:52:09.176;11/10/20 16:52:43.864;763;n
147.251.x.x;CZ;147.251.x.x;CZ;4737;0.229183358298208;7093174;0.303144448129907;11/10/20 16:54:33.642;11/10/20 16:54:34.538;15051
147.251.x.x;CZ;147.231.x.x;CZ;127026;6.1457135890201;6729960;0.28762159368096;11/10/20 16:51:38.084;11/10/20 16:56:42.660;ssh (2
147.251.x.x;CZ;195.113.x.x;CZ;4401;0.212927160622845;6597710;0.281969560717271;11/10/20 16:48:09.070;11/10/20 16:48:09.262;15051
147.251.x.x;CZ;147.229.x.x;CZ;4309;0.2084760588784;6454472;0.275847928220841;11/10/20 16:52:31.813;11/10/20 16:52:32.261;15051;4
147.251.x.x;CZ;147.229.x.x;CZ;4297;0.207895480389994;6436511;0.275080320175013;11/10/20 16:52:09.074;11/10/20 16:52:09.394;15051
147.251.x.x;CZ;195.113.x.x;CZ;4185;0.202476747831539;6273939;0.268132401059906;11/10/20 16:56:22.193;11/10/20 16:56:22.321;15051
147.251.x.x;CZ;89.248.x.x;CZ;3558;0.172141521812334;5123520;0.218966381324149;11/10/20 16:46:26.892;11/10/20 16:51:38.316;8000;3
147.251.x.x;CZ;147.251.x.x;CZ;3217;0.155643416433468;4821939;0.206077566554983;11/10/20 16:56:09.703;11/10/20 16:56:09.895;15051
195.113.x.x;CZ;147.251.x.x;CZ;2145;0.103778404802545;3185876;0.136156341551796;11/10/20 16:54:35.692;11/10/20 16:55:30.668;883;n
195.113.x.x;CZ;147.251.x.x;CZ;2134;0.10324620785484;3180428;0.135923507709934;11/10/20 16:56:21.079;11/10/20 16:56:51.223;883;nf
90.183.x.x;CZ;147.251.x.x;CZ;41206;1.99360976610428;2239312;0.0957025727030915;11/10/20 16:49:31.334;11/10/20 16:54:33.734;61249
147.251.x.x;CZ;147.231.x.x;CZ;1669;0.0807487914291133;2100476;0.0897690706346855;11/10/20 16:55:52.101;11/10/20 16:56:09.637;nfs
147.251.x.x;CZ;88.212.x.x;SK;1434;0.0693791293644988;2031863;0.0868367232793919;11/10/20 16:51:37.511;11/10/20 16:51:38.343;http
(6);00000000;AS65080;AS2607;16;20
147.251.x.x;CZ;88.212.x.x;SK;1429;0.0691372216609964;2020261;0.0863408829282031;11/10/20 16:55:43.503;11/10/20 16:55:44.975;http
(6);00000000;AS65080;AS2607;16;20
147.251.x.x;CZ;88.212.x.x;SK;1414;0.0684114985504895;2000703;0.0855050231119171;11/10/20 16:51:36.492;11/10/20 16:51:37.580;https
(6);00000000;AS65080;AS2607;16;20
195.113.x.x;CZ;147.251.x.x;CZ;1080;0.0522520639565263;1601336;0.0684370802112782;11/10/20 16:56:18.873;11/10/20 16:56:45.049;745
195.113.x.x;CZ;147.251.x.x;CZ;1073;0.0519133931716229;1593432;0.068099283095626;11/10/20 16:51:20.495;11/10/20 16:51:49.167;883;
147.251.x.x;CZ;88.212.x.x;SK;1080;0.0522520639565263;1533228;0.0655263152880955;11/10/20 16:51:17.672;11/10/20 16:51:18.440;http
(6);00000000;AS65080;AS2607;16;20
```

Systém FTAS – reporter

- Struktury periodicky generovaných statických HTML stránek
  - Různé pohledy na provoz - zabudované strategie analýzy provozu
    - **Detekce anomálií** (např. vztah k bezpečnosti)
    - **Běžný statisticky orientovaný výstup**
  - Jednoduché schéma výstupů
    - **Přehledové stránky** (~ rozcestníky) → **detailní analytické výstupy** + horizontální prolinkování (dle konfigurace)
- Technicky ovládání interaktivního UI přes STDIN/STDOUT (simulace chování reálného uživatele)
- *Vhodné pro běžné uživatele – intuitivní, jdenoduché, vše na proklik*

Systém FTAS – reporter

- Příklad úvodního rozcestníku pro uživatele

FTAS - Reporter author: Tom Kosnar, copyright: © 2012-2013 , CESNET a.l.e. , version: 5.23beta-131021

Overview of available IP traffic reports for

Following table contains matrix of all IP traffic reports generated for You can access appropriate IP traffic report with the help of 'Enter' links. User access rights are distributed - you may not be allowed to access some reports.

Available Traffic Reports

	VFN
Traffic from · top sources	Enter
Traffic from · unwanted to ports 22, 135, 139, 445, 3389	Enter
Traffic to · sources of possible anomalies	Enter
Traffic to · top destinations	Enter
Traffic to · unwanted to ports 22, 135, 139, 445, 3389	Enter

Generated: Fri Nov 22 16:26:23 2013 by FTAS - Reporter

Systém FTAS – reporter

- Příklad souhrnné stránky se zachycenými anomáliemi

Period view: Traffic to [redacted] attacking destination port numbers 22, 135, 139, 445, 3389

The following table gives summary period based view on IP addresses that are possible sources of attacks on destination port numbers 22, 135, 139, 445, 3389. Primary limits are at least 10 flows within 10 seconds from single source IP address, secondary limits are - flow count>10 or source port count>10 or destination IP count>10 within 10 minutes.

Other reports: *Traffic to [redacted]* *destinations* *sources* *135, 139, 445, 3389* *possible anomalies*

Special links: *Available reports for [redacted]*

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

Results for Requested Period: hour

Period Start Time	Period End Time	Period Size	Events Found	Event Description
2013-11-22 02:00:00	*2013-11-22 15:59:59*	*14 hours*	*none*	
2013-11-22 01:00:00	2013-11-22 01:59:59	hour	1	37.59.29.37, peering -> tcp (6),ssh (22): 15 source ports, 15 dest. IPs, 18 flows, pktlen 58.87 B, measured at Prague 2: [redacted] backup)(398)
2013-11-22 00:00:00	2013-11-22 00:59:59	hour	1	218.7.37.194, unknown -> tcp (6),ssh (22): 1 source ports, 26 dest. IPs, 26 flows, pktlen 48 B, measured at Prague 2: R114 - border router (NIX-3, Public Internet backup)(398)
2013-11-21 23:00:00	*2013-11-21 23:59:59*	*1 hour*	*none*	
2013-11-21 22:00:00	2013-11-21 22:59:59	hour	1	222.186.129.89, unknown -> tcp (6),3389: 1 source ports, 12 dest. IPs, 12 flows, pktlen 46 B, measured at Prague 2: [redacted]
2013-11-21 20:00:00	*2013-11-21 21:59:59*	*2 hours*	*none*	
2013-11-21 19:00:00	2013-11-21 19:59:59	hour	2	183.129.249.106, unknown -> tcp (6),ssh (22): 1 source ports, 36 dest. IPs, 36 flows, pktlen 46 B, measured at Prague 2: R114 - border router (NIX-3, Public Internet backup)(398) 67.216.253.197, unknown -> tcp (6),3389: 1 source ports, 17 dest. IPs, 17 flows, pktlen 48 B, measured at Prague 2: [redacted]
2013-11-21 18:00:00	2013-11-21 18:59:59	hour	1	198.199.88.16, unknown -> tcp (6),ssh (22): 1 source ports, 24 dest. IPs, 24 flows, pktlen 48 B, measured at Pra[redacted] backup)(398)
2013-11-21 09:00:00	*2013-11-21 17:59:59*	*9 hours*	*none*	

Systém FTAS – reporter

- Příklad alternativní souhrnné stránky se zachycenými anomáliemi

TopList view: Traffic to attacking destination port numbers 22, 135, 139, 445, 3389

The following table gives summary top-list based view on IP addresses that are possible sources of attacks on destination port numbers 22, 135, 139, 445, 3389. C
flow count>10 or source port count>10 or destination IP count>10 within 10 minutes.

Other reports: *Traffic to* *destinations* *sources* *3389* *anomalies* *sources o*
Special links: *Available reports for*
Other views: *Periods* *Events* *TopList*

Order	Src-IP	Src-Group	Protocol	Dst-Port	Src-Port-Cnt	Dst-IP-Cnt	Record-Cnt	Bytes-measured	Pkts-measured	Event Count	First Occurance
1	207.244.68.106	unknown	tcp (6)	ssh (22)	4	119	119	5712	119	4	13/10/25 04:35:54.075
2	218.26.89.179	unknown									13/11/06
3	218.7.37.194	unknown									
4	95.131.98.218	peering									
5	125.211.197.158	unknown									
6	67.138.105.67	unknown									
7	162.13.124.76	peering									
8	61.142.106.34	unknown									
9	194.231.77.226	peering									

Src-IP=207.244.68.106 and Src-Group=unknown and Protocol=tcp (6) and Dst-Port=ssh on destination ports 22, 135, 139, 445, 3389

Src-IP=207.244.68.106 and Src-Group=unknown and Protocol=tcp (6) and Dst-Port=ssh (22) - attacks on destination ports 22, 135, 139, 445, 3389. There ar
analysis in the table below. Detailed analysis for each record is accessible through links in appropriate columns.

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

Src-IP	Src-Group	Protocol	Dst-Port	Src-Port-Cnt	Dst-IP-Cnt	Record-Cnt	Avr-Pkt-Length	Bytes-measured	Pkts-measured	Flow-Start
207.244.68.106	unknown	tcp (6)	ssh (22)	1	31	31	48	1488	31	13/10/28 07:59:17.766
207.244.68.106	unknown	tcp (6)	ssh (22)	1	31	31	48	1488	31	13/10/27 12:21:14.317
207.244.68.106	unknown	tcp (6)	ssh (22)	1	29	29	48	1392	29	13/10/25 06:41:01.763
207.244.68.106	unknown	tcp (6)	ssh (22)	1	28	28	48	1344	28	13/10/25 04:35:54.075

Systém FTAS – reporter

- Příklad detailní výstup zachycující provozní anomálii

Detailed analysis for 207.244.68.106, unknown-> tcp (6),ssh (22): 1 source ports, 31 dest. IPs, flows, pktlen 48 B, measured at Prague and period 2013-10-28 07:00:00 - 2013-10-28 07:59:59

Other views: Periods Events TopList Period 2013-10-28 07:00:00 - 2013-10-28 07:59:59 Plain text results

Results *(time values in CET)*

	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Flow-Start [CET]	Flow-End [CET]	Bytes-measured	Pkts-meas
1.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:17.766	13/10/28 07:59:17.766	48.000 B	1.0
2.	207.244.68.106 (USA)	195.113 (CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.684	13/10/28 07:59:18.684	48.000 B	1.0
3.	207.244.68.106 (USA)	195.113 (CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:17.874	13/10/28 07:59:17.874	48.000 B	1.0
4.	207.244.68.106 (USA)	195.113 (CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:17.827	13/10/28 07:59:17.827	48.000 B	1.0
5.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.700	13/10/28 07:59:18.700	48.000 B	1.0
6.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.744	13/10/28 07:59:18.744	48.000 B	1.0
7.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.744	13/10/28 07:59:18.744	48.000 B	1.0
8.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.697	13/10/28 07:59:18.697	48.000 B	1.0
9.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.697	13/10/28 07:59:18.697	48.000 B	1.0
10.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.742	13/10/28 07:59:18.742	48.000 B	1.0
11.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.740	13/10/28 07:59:18.740	48.000 B	1.0
12.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.684	13/10/28 07:59:18.684	48.000 B	1.0
13.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.732	13/10/28 07:59:18.732	48.000 B	1.0
14.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.683	13/10/28 07:59:18.683	48.000 B	1.0
15.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.683	13/10/28 07:59:18.683	48.000 B	1.0
16.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.731	13/10/28 07:59:18.731	48.000 B	1.0
17.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.656	13/10/28 07:59:18.656	48.000 B	1.0
18.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.731	13/10/28 07:59:18.731	48.000 B	1.0
19.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.680	13/10/28 07:59:18.680	48.000 B	1.0
20.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.731	13/10/28 07:59:18.731	48.000 B	1.0
21.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.731	13/10/28 07:59:18.731	48.000 B	1.0
22.	207.244.68.106 (USA)	195.113 CZE)	tcp (6)	26160	ssh (22)	13/10/28 07:59:18.680	13/10/28 07:59:18.680	48.000 B	1.0

Systém FTAS – reporter

- Příklad notifikace po detekci anomálie, vč. odkazu k „důkaznímu materiálu“

To:

Subject: Possible DoS warning - source IPs -> cvut.cz

Date: Fri, 22 Nov 2013 15:41:20 +0100 (CET)

```
Possible DoS warning - source IPs ->              .cz
 for period starting 2013-11-22 15:00:00 and finishing 2013-11-22 15:59:59.

 Src-IP           : 209.55.102.161
 Src-IP-Geo       : USA
 Src-Port-Cnt     : 1267
 Protocol         : tcp (6)
 Dst-IP           : 147.32.
 Dst-IP-Geo       : CZE
 Dst-Port         : ircd (6667)
 Record-Cnt       : 1297
 Avr-Pkt-Length   : 52
 Bytes-measured   : 68692
 Pkts-measured    : 1321
 Flow-Start       : 13/11/22 15:25:28.840
 Flow-End         : 13/11/22 15:39:09.680
 HTML-Report      :
https:/ cesnet.cz/                                  attacks 1/hour 2013112215/209.55.102.161 6 6667/index.html
 Plain  port :
https:/ cesnet.cz/                                  attacks 1/hour 2013112215/209.55.102.161 6 6667/results.txt


   This is auto-generated message - DON'T REPLY
```

Systém FTAS – reporter

- Příklad odkazovaného detailního výstupu

Detailed analysis for 209.55.102.161 USA -> [redacted]cvut.cz,tcp (6),ircd (6667): 1267 source ports, 1297 flows, pktlen 52 B and period 2013-11-22 15:00:00 - 2013-11-22 15:59:59

Other views: Periods Events TopList Period 2013-11-22 15:00:00 - 2013-11-22 15:59:59 Plain text results

Results *(time values in CET)*

	Src-IP	Dst-IP		Protocol	Src-Port	Dst-Port	Flow-Start [CET]	Flow-End [CET]	Bytes-measured	Pkts-me
1.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	65413	ircd (6667)	13/11/22 15:25:28.840	13/11/22 15:38:39.000	104.000 B	
2.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	65419	ircd (6667)	13/11/22 15:25:29.378	13/11/22 15:38:38.997	104.000 B	
3.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61988	ircd (6667)	13/11/22 15:25:33.083	13/11/22 15:25:33.083	52.000 B	
4.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61979	ircd (6667)	13/11/22 15:25:33.084	13/11/22 15:25:33.084	52.000 B	
5.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61740	ircd (6667)	13/11/22 15:25:33.098	13/11/22 15:25:33.098	52.000 B	
6.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61971	ircd (6667)	13/11/22 15:25:33.099	13/11/22 15:25:33.099	52.000 B	
7.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61724	ircd (6667)	13/11/22 15:25:33.099	13/11/22 15:25:33.099	52.000 B	
8.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61738	ircd (6667)	13/11/22 15:25:33.099	13/11/22 15:25:33.099	52.000 B	
9.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61970	ircd (6667)	13/11/22 15:25:33.100	13/11/22 15:25:33.100	52.000 B	
10.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61735	ircd (6667)	13/11/22 15:25:33.101	13/11/22 15:38:43.395	104.000 B	
11.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61734	ircd (6667)	13/11/22 15:25:33.101	13/11/22 15:38:43.396	104.000 B	
12.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61960	ircd (6667)	13/11/22 15:25:33.102	13/11/22 15:25:33.102	52.000 B	
13.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61948	ircd (6667)	13/11/22 15:25:33.104	13/11/22 15:25:33.104	52.000 B	
14.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61952	ircd (6667)	13/11/22 15:25:33.104	13/11/22 15:25:33.104	52.000 B	
15.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61944	ircd (6667)	13/11/22 15:25:33.106	13/11/22 15:25:33.106	52.000 B	
16.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61718	ircd (6667)	13/11/22 15:25:33.117	13/11/22 15:25:33.117	52.000 B	
17.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	62004	ircd (6667)	13/11/22 15:25:33.141	13/11/22 15:25:33.141	52.000 B	
18.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61997	ircd (6667)	13/11/22 15:25:33.143	13/11/22 15:25:33.143	52.000 B	
19.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61999	ircd (6667)	13/11/22 15:25:33.144	13/11/22 15:25:33.144	52.000 B	
20.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61986	ircd (6667)	13/11/22 15:25:33.439	13/11/22 15:25:33.439	52.000 B	
21.	209.55.102.161 (USA)	147.32.	(CZE)	tcp (6)	61983	ircd (6667)	13/11/22 15:25:33.441	13/11/22 15:25:33.441	52.000 B	

Systém FTAS – reporter

- Příklad reportingu pro více dílčích komponent (možné rozdělení přístupových práv)

FTAS - Reporter *author: Tom Kosnar, copyright: © 2012-2014 , CESNET a.l.e. , version: 5.33-IPFIX-140815*

Reports Generated for CESNET Storages

The table below gives all report types generated for CESNET Storages. Click on the 'Report' links to see specific report type results.

Available Reports

	Incoming traffic destinations top list	*Incoming traffic detailed top list*	*Incoming traffic sources top list*	*Outgoing traffic destinations top list*	*Outgoing traffic detailed top list*	*Outgoing traffic sources top list*
Storage 1, Plzeň *DU1-Plzen*	Enter	Enter	Enter	Enter	Enter	Enter
Storage 2, Jihlava *DU2-Jihlava*	Enter	Enter	Enter	Enter	Enter	Enter
Storage 3, Brno *DU3-Brno*	Enter	Enter	Enter	Enter	Enter	Enter

Generated: Tue Sep 30 16:40:32 2014 by FTAS - Reporter

Systém FTAS – reporter

- Příklad reportingu pro více dílčích komponent – běžný statistický výstup

FTAS - Reporter *author: Tom Kosnar, copyright: © 2012-2014 , CESNET a.l.e. , version: 5.33-IPFIX-140815*

Storage 1, Plzeň - outgoing traffic, sources top list

The following table gives top list of output traffic from Storage 1, Plzeň during appropriate periods.

Other reports: *Outgoing traffic, detailed top list* | *Outgoing traffic, sources top list* | *Outgoing traffic, destinations top list* | *Incoming traffic, detailed top list* | *Incoming traffic, sources top list* | *Incoming traffic, destinations top list*

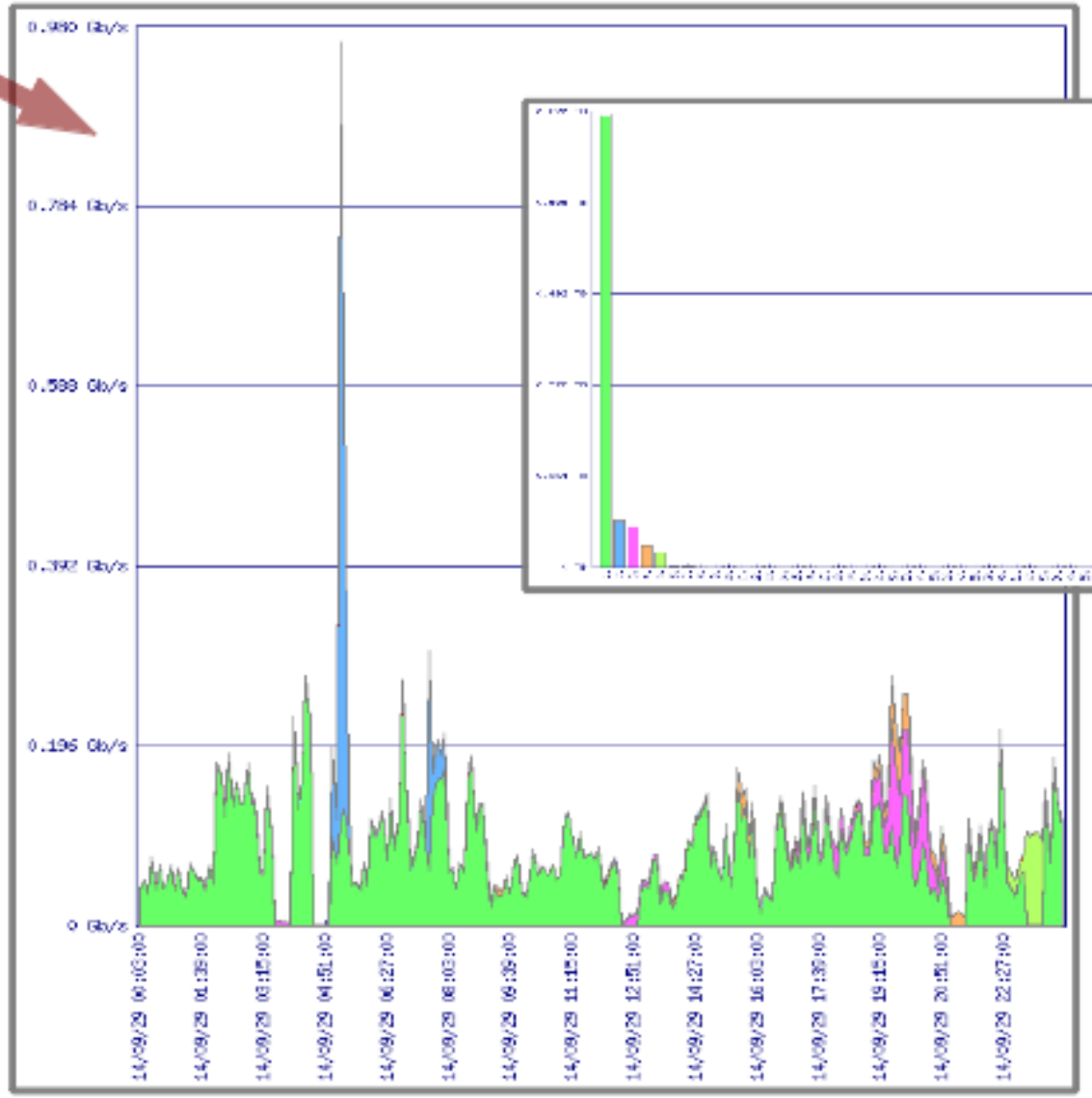
Special links: *Reports Generated for CESNET Storages*

Results for Requested Period: day

Report for	Period Start Time	Period End Time	Period Size
day 2014/9/30	2014-09-30 00:00:00	2014-09-30 16:27:12	16 hours, 27 minutes
day 2014/9/29	2014-09-29 00:00:00	2014-09-29 23:59:59	day
day 2014/9/28	2014-09-28 00:00:00	2014-09-28 23:59:59	day
day 2014/9/27	2014-09-27 00:00:00	2014-09-27 23:59:59	day
day 2014/9/26	2014-09-26 00:00:00	2014-09-26 23:59:59	day
day 2014/9/25	2014-09-25 00:00:00	2014-09-25 23:59:59	day
day 2014/9/24	2014-09-24 00:00:00	2014-09-24 23:59:59	day
day 2014/9/23	2014-09-23 00:00:00	2014-09-23 23:59:59	day
day 2014/9/22	2014-09-22 00:00:00	2014-09-22 23:59:59	day
day 2014/9/21	2014-09-21 00:00:00	2014-09-21 23:59:59	day
day 2014/9/20	2014-09-20 00:00:00	2014-09-20 23:59:59	day
day 2014/9/19	2014-09-19 00:00:00	2014-09-19 23:59:59	day
day 2014/9/18	2014-09-18 00:00:00	2014-09-18 23:59:59	day

Systém FTAS – reporter

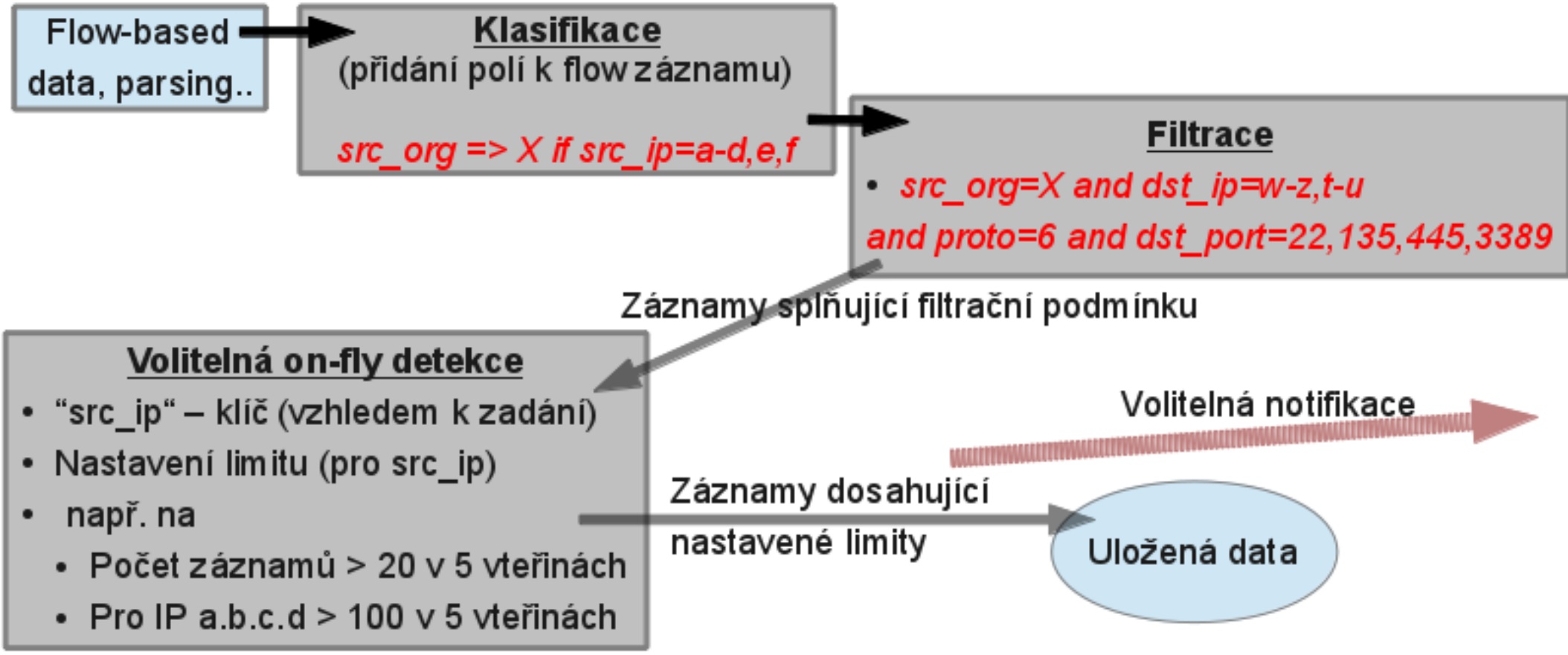
- Příklad reportingu pro více dílčích komponent – běžný statistický výstup



	Src-IP	Bytes-estimated
1.	[redacted]	0.812 TB ~ 78.521%
2.	[redacted]	85.293 GB ~ 8.055%
3.	[redacted]	72.901 GB ~ 6.884%
4.	[redacted]	39.156 GB ~ 3.698%
5.	[redacted]	26.152 GB ~ 2.470%
6.	[redacted]	1.634 GB ~ 0.154%
7.	[redacted]	1.495 GB ~ 0.141%
8.	[redacted]	137.632 MB ~ 0.013%
9.	[redacted]	96.486 MB ~ 0.009%
10.	[redacted]	84.197 MB ~ 0.008%
11.	[redacted]	78.716 MB ~ 0.007%
12.	[redacted]	70.153 MB ~ 0.006%
13.	[redacted]	66.128 MB ~ 0.006%
14.	[redacted]	57.741 MB ~ 0.005%
15.	[redacted]	22.070 MB ~ 0.002%
16.	[redacted]	19.266 MB ~ 0.002%
17.	[redacted]	18.623 MB ~ 0.002%
18.	[redacted]	17.533 MB ~ 0.002%
19.	[redacted]	16.665 MB ~ 0.002%
20.	[redacted]	16.582 MB ~ 0.002%
21.	[redacted]	14.978 MB ~ 0.001%
22.	[redacted]	14.594 MB ~ 0.001%
23.	[redacted]	12.547 MB ~ 0.001%

Systém FTAS – řešení detekce provozních anomálií

- Krok 1 – v "**měřícím jádru**"
- ***+ okamžitá indikace, - za cenu menší jistoty*** *(„krátká doba pozorování")*
- Příklad – detekce zdrojů ze sítě organizace X agresivně atakující služby (na základě čísel portů) ve specifikovaných IP segmentech



Systém FTAS – řešení detekce provozních anomálií

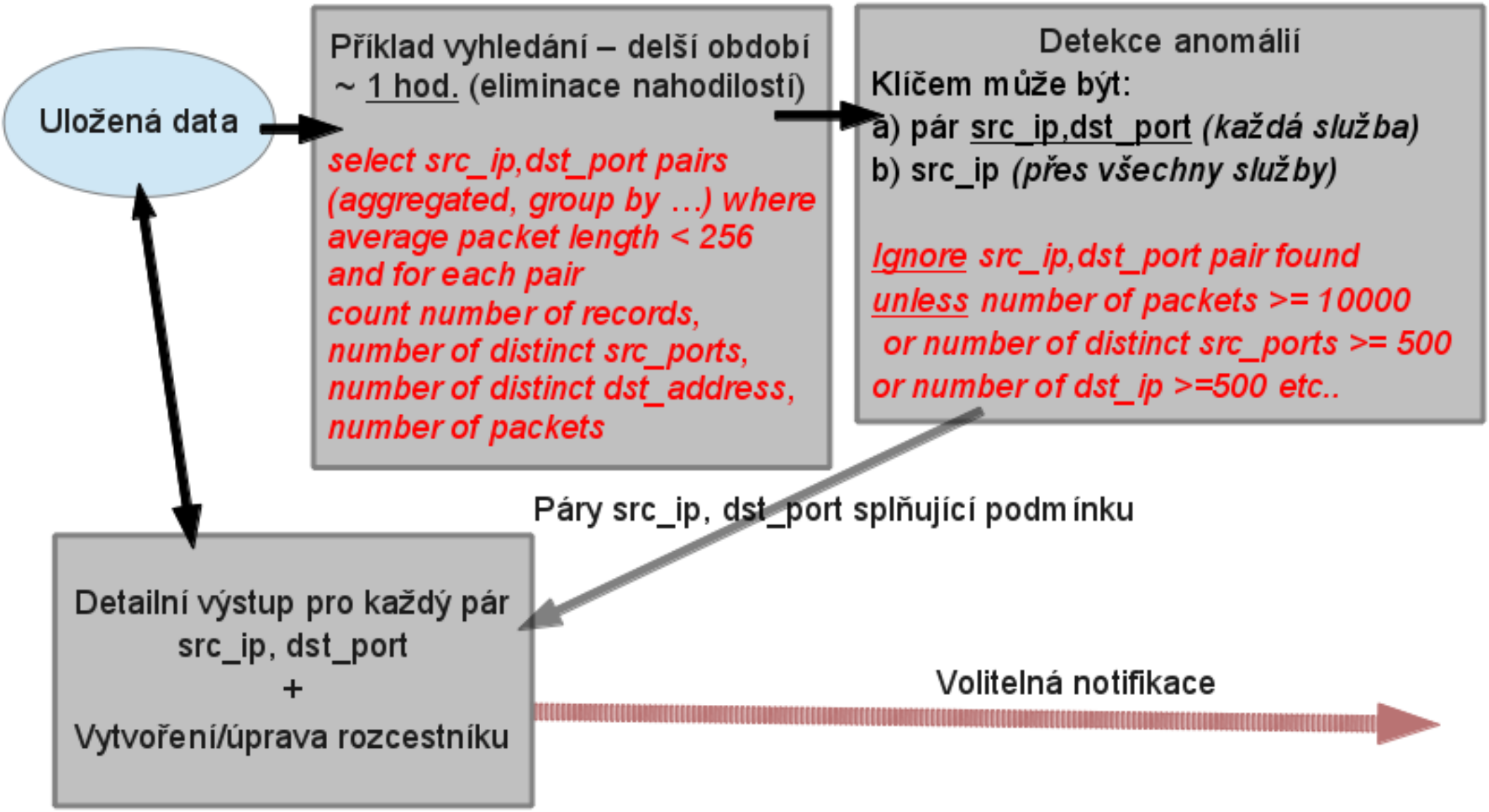
- Krok 1 – v "**měřícím jádru**"
- Volitelná notifikace
  - K dispozici okamžitě, ale vypovídací hodnota závislá na nastavených limitech
  - *Pozn.: ukázka notifikace přísluší jinému nastavení (detekce útoků na DNS)*

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     : [redacted]
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:
-----------------------------------------------------

195.1[redacted].7   udp/56267  -> 195.113.144.194 udp/domain:     69 B,    1 p, 69 Bpp, 13:07:14[GMT], 15:07:14[local]
195.1[redacted].104 udp/34870  -> 195.113.144.194 udp/domain:     83 B,    1 p, 83 Bpp, 13:06:43[GMT], 15:06:43[local]
147.3[redacted]93   udp/51417  -> 195.113.144.194 udp/domain:     56 B,    1 p, 56 Bpp, 13:07:06[GMT], 15:07:06[local]
147.3[redacted]183  udp/54316  -> 195.113.144.194 udp/domain:     69 B,    1 p, 69 Bpp, 13:06:58[GMT], 15:06:58[local]
195.1[redacted].7   udp/59703  -> 195.113.144.194 udp/domain:     74 B,    1 p, 74 Bpp, 13:06:45[GMT], 15:06:45[local]
195.1[redacted].120 udp/56776  -> 195.113.144.194 udp/domain:     83 B,    1 p, 83 Bpp, 13:06:44[GMT], 15:06:44[local]
147.3[redacted]137  udp/57687  -> 195.113.144.194 udp/domain:     73 B,    1 p, 73 Bpp, 13:06:56[GMT], 15:06:56[local]
195.1[redacted].79  udp/59918  -> 195.113.144.194 udp/domain:     83 B,    1 p, 83 Bpp, 13:07:23[GMT], 15:07:23[local]
147.3[redacted]137  udp/60575  -> 195.113.144.194 udp/domain:     72 B,    1 p, 72 Bpp, 13:06:56[GMT], 15:06:56[local]
195.1[redacted].109 udp/45692  -> 195.113.144.194 udp/domain:     73 B,    1 p, 73 Bpp, 13:07:00[GMT], 15:07:00[local]
195.1[redacted].4   udp/54446  -> 195.113.144.194 udp/domain:     94 B,    1 p, 94 Bpp, 13:07:20[GMT], 15:07:20[local]
195.1[redacted].111 udp/54195  -> 195.113.144.194 udp/domain:     73 B,    1 p, 73 Bpp, 13:07:07[GMT], 15:07:07[local]
```

Systém FTAS – řešení detekce provozních anomálií

- Krok 2 – ve "**FTAS-reporter**" - *se zpožděním, ale s vyšší jistotou*
  - Může použít data vytvořená v „kroku 1" jako vstupní *(což je mj. typická konfigurace)*



Systém FTAS – řešení detekce provozních anomálií

- Krok 2 – ve "**FTAS-reporter**" - volitelná notifikace
- *Pozn.: ukázka notifikace přísluší jinému nastavení*

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:/[redacted]/unwanted_outgoing_traffic_from[redacted]o_specif
 PlainTe
https:/[redacted]/unwanted_outgoing_traffic_from[redacted]o_specif
```

Systém FTAS – řešení detekce provozních anomálií

- Krok 2 – ve "**FTAS-reporter**" - ukázka detailního & "overview" výstupu

Detailed analysis for [redacted]4.58.76, [redacted]-> tcp (6),3389: 16376 source ports, 767192 dest. IPs, 91
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-me
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
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
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
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
5.	[redacted]4.58.76 (CZE)	2.190.110.211 (IRN)	tcp (6)						
6.	[redacted]4.58.76 (CZE)	2.190.110.212 (IRN)	tcp (6)						
7.	[redacted]4.58.76 (CZE)	2.190.110.219 (IRN)	tcp (6)						
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)						

FTAS - Reporter

Period view: IP addresses attacking destination port numbers 22, 1

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

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	[redacted]
2014-04-18 09:00:00	2014-04-18 09:59:59	hour	4	[redacted]

Systém FTAS – některé další novinky a rozšíření

- Od 2013: nová generace systému
  - **Variabilní interní datová struktura**
    - Přidána nová pole z rozšiřujících mechanismů
      - **N**etflow **S**ecurity **E**vent **L**ogging
      - **Flexible Netflow**
      - Systém připraven na další postupná rozšíření datové struktury
- **Od 2014: plná IPFIX podpora** (vč. polí s proměnnou délkou)
- Ve všech případech zachována kompatibilita s daty „uloženými“ předchozími verzemi (zajišťeno vlastnostmi UI)

Systém FTAS – některé další novinky a rozšíření

- Ukázka některých informací z NetFlow Security Event Logging exportu

	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNA
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)
	NAT-Event	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port	Dst-Port	Src-PostNAPTPort	Dst-PostNA

Systém FTAS – některé další novinky a rozšíření

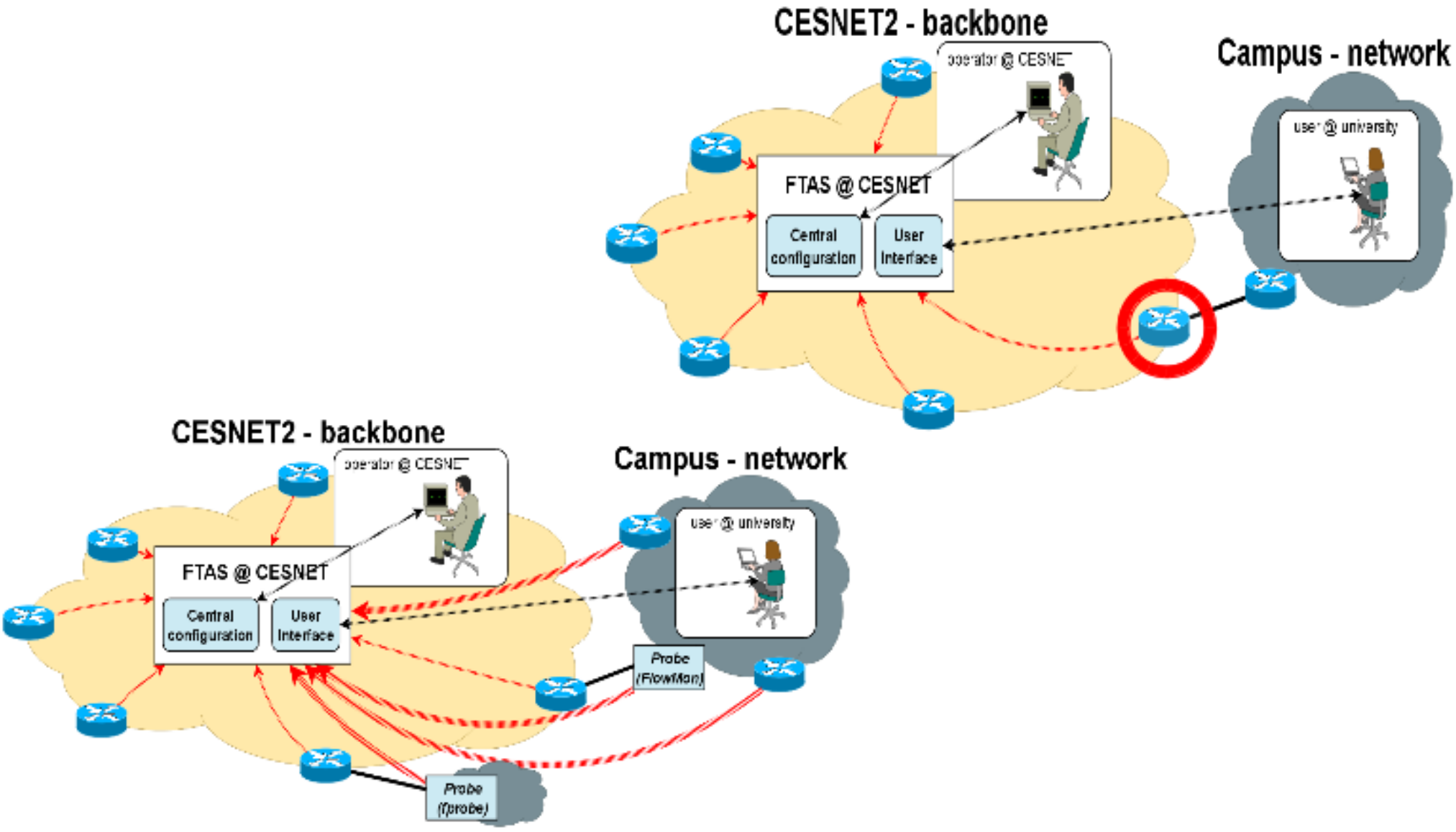
- Ukázka některých informací z Flexible NetFlow rozšíření
  - IP↔MAC addr.

o	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst
1.	Terminate For us	134.94	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0
2.	Terminate For us	10.31.2	10.31.2	icmp (1)	Echo Reply (0)	Echo Reply (0)	21	0
3.	Terminate For us	188.1.1	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	1	0
4.	Terminate For us	195.11	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0
5.	Terminate For us	195.11	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0
6.	Terminate For us	195.11	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0
7.	Terminate For us	195.11	195.11	icmp (1)	Echo Reply (0)	Echo Reply (0)	2	0
8.	Forwarded	134.94	195.11	icmp (1)	Echo Reply (0)	Echo (2048)	21	2

rt	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Src-MAC-Addr	Dst-MAC-Add
eply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:0
eply (0)	Echo Reply (0)	21	0	1	00:00:00:00:00:00	00:00:00:00:0
eply (0)	Echo Reply (0)	1	0	0	e0:2f:6d:2b:76:80	00:00:00:00:0
eply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:70	00:00:00:00:0
eply (0)	Echo Reply (0)	2	0	1	00:50:56:8d:0d:2d	00:00:00:00:0
eply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b8:ec	00:00:00:00:0
eply (0)	Echo Reply (0)	2	0	1	00:60:dd:44:b9:6d	00:00:00:00:0
eply (0)	Echo (2048)	21	2	1	00:00:00:00:00:00	00:50:56:8d:0
eply (0)	Echo Reply (0)	2	21	1	00:50:56:8d:0d:2d	00:00:00:00:0

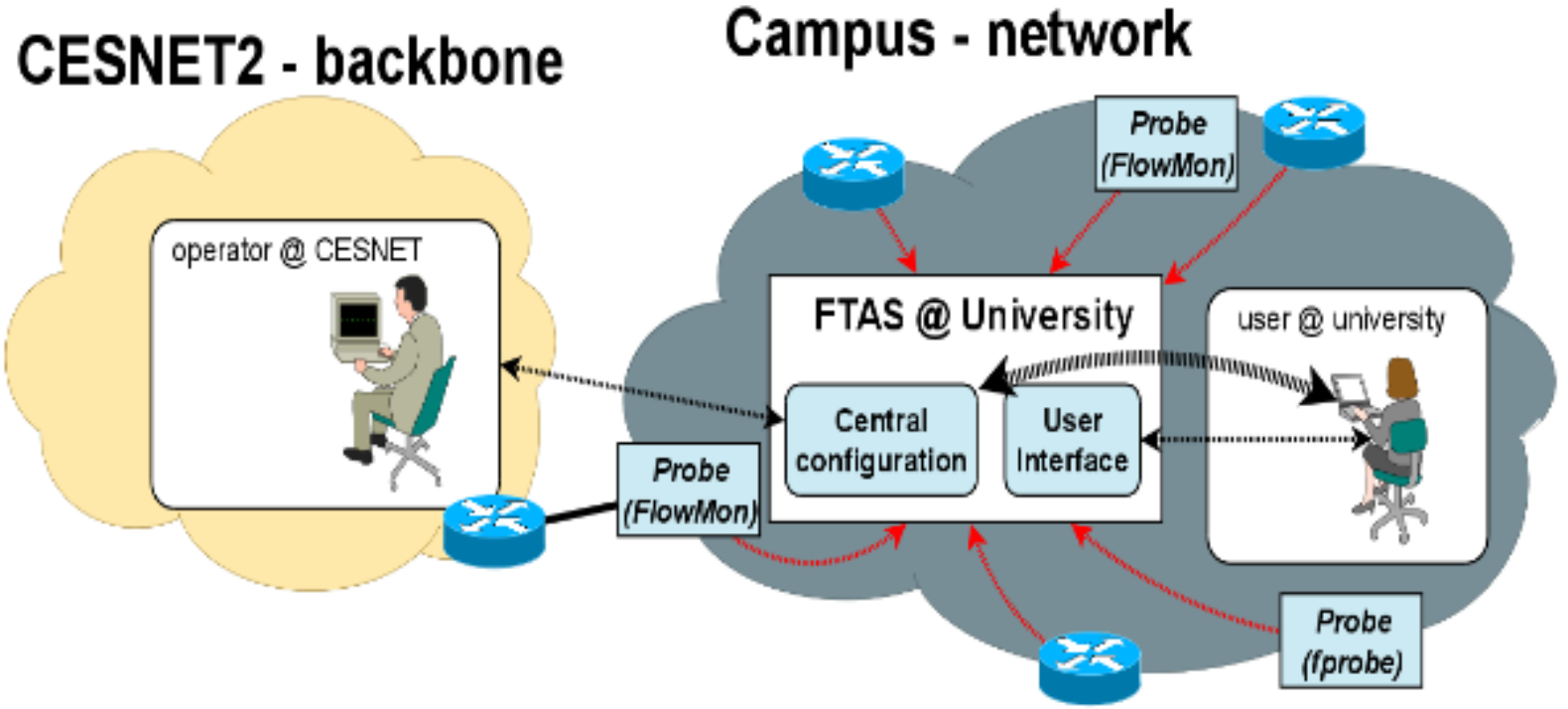
Systém FTAS – jako služba

- Primární instalace v páteřní síti e-Infrastruktury CESNET



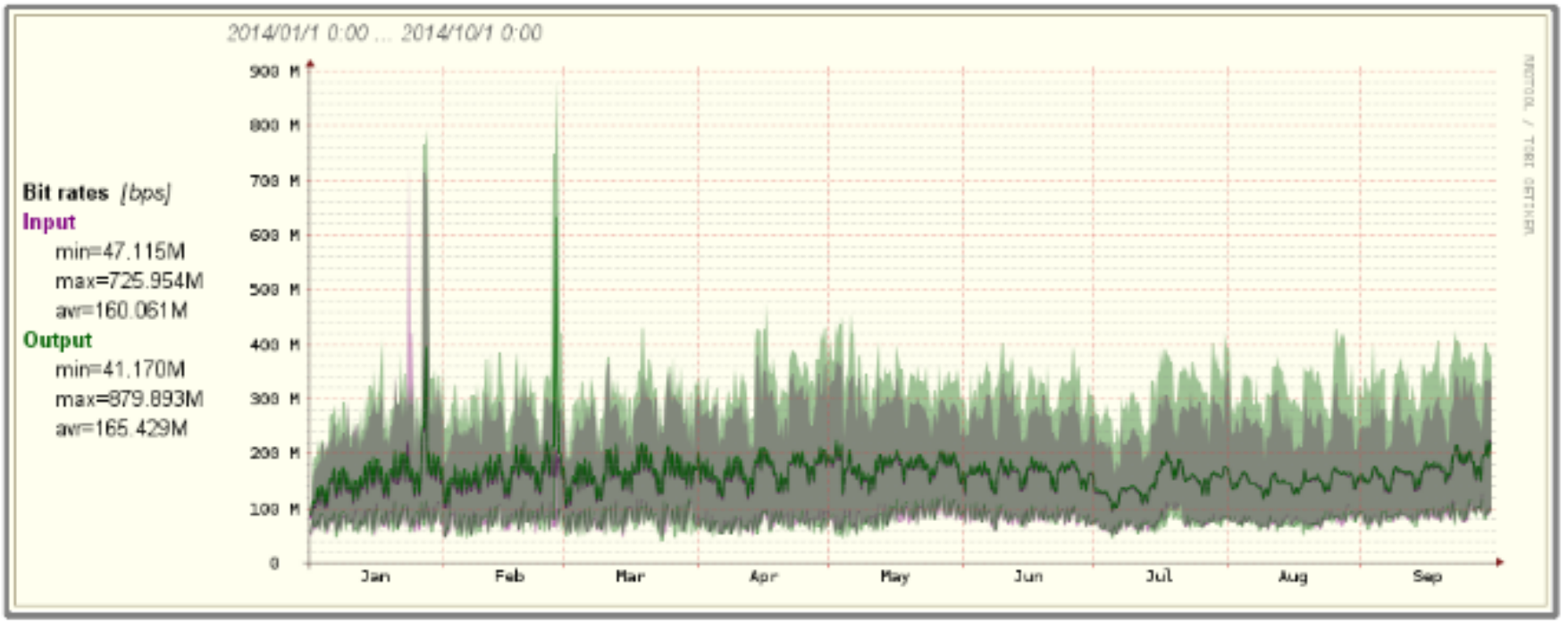
Systém FTAS – jako služba

- Instalace v sítích uživatelů
  - HW uživatele
  - Společná správa



Systém FTAS – v souhrnu

- **Primární instalace v e-Infrastruktuře CESNET**
  - 17 fyzických uzlů (340 jader, 160 TB storage)
  - Počet přístupů k interaktivnímu UI v roce 2014 ~ **10k**
  - Počet přístupů k výstupům FTAS-reporter modulu v roce 2014 > **180k**
  - Celkový objem zpracovávaných dat (vč. interní redistribuce) 2014



- **Další instalace FTAS**
  - **Samostané instalace v uživatelských sítích** (~ zpravidla 1 uzel)
  - Celkově 30+ institucí s dedikovanou konfigurací (v rámci primární instalace), reportingem nebo vlastní instalací

Díky za trpělivost a za pozornost ;-)

???