Zabbix in Campus

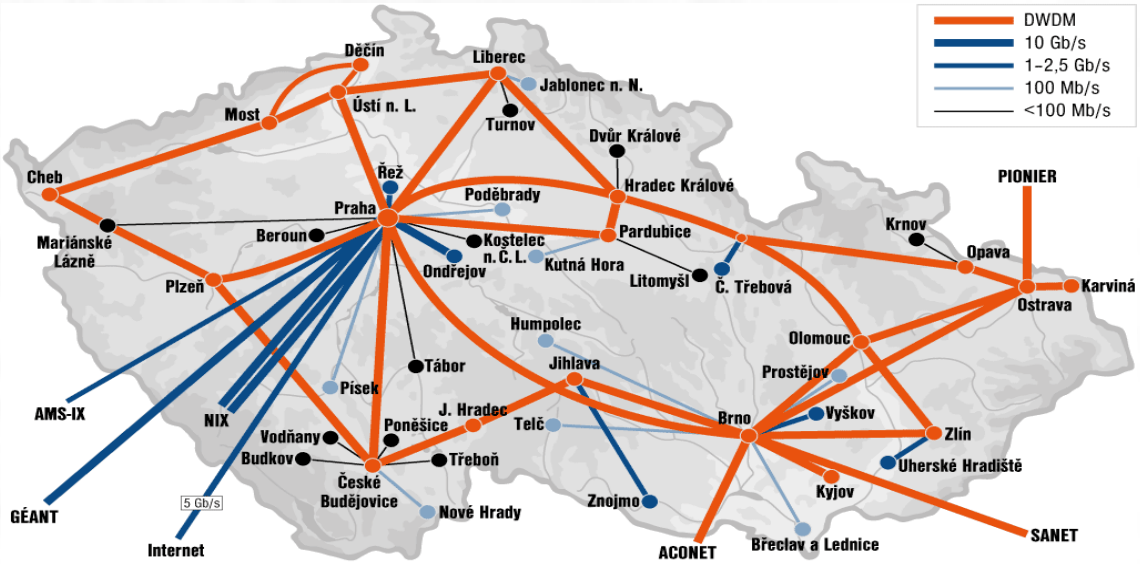
Lukas Macura
CESNET
Silesian University in Opava
Lukas.macura@cesnet.cz

Contents

- CESNET
- Silesian University (SLU)
- History of zabbix on SLU
- Current state of Zabbix at SLU
- Current state of Zabbix at CESNET
- What we are missing?
- Conclusions

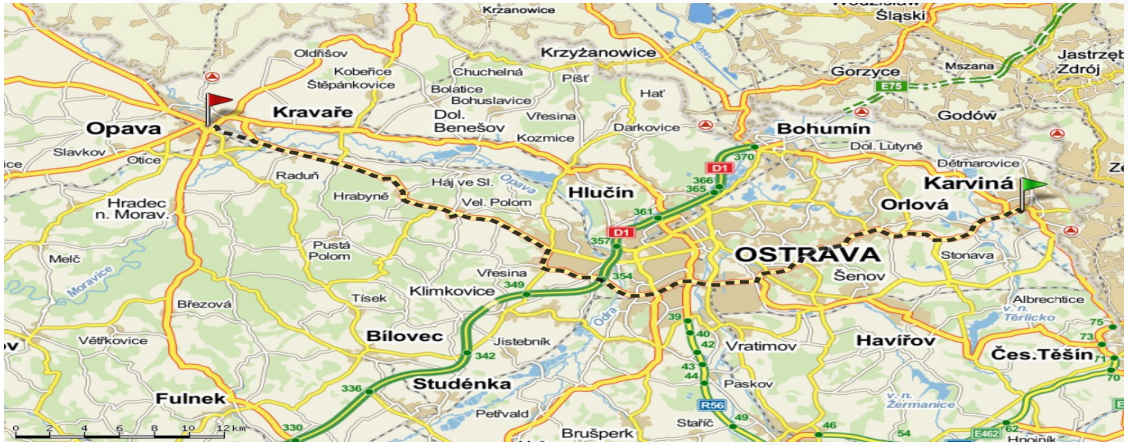
CESNET

- Czech academical network for research
- Includes all public Czech Universities



Silesian University in Opava

- Divided into Karvina and Opava
  - Faculty of Philosophy and Science in Opava
  - *School of Business Administration in Karvina*
  - Faculty of Public Policies in Opava
  - Institute of Mathematics in Opava



Monitoring theory

- We need monitoring to know about crashes
- We need crashes to test monitoring
- We need crashes of monitoring to be happy that everything works
- But worsest scenario if users acts as monitoring (they are ugly from it)
- We have to:
  - Either monitor and predict crashes
  - Or do not have any user

History of monitoring on SLU

- We experienced before zabbix
- We used many kind of monitoring software
- Each had some problems
- It was only basic monitoring of main services
- Used mainly to overview during troubleshooting
- **„Dark time“ - crashes were unknown**

History of zabbix on SLU
First stage (2004)

- Searched for monitoring solution
- Found Zabbix as great project (alpha stage)
- Configured very basic monitoring
- Not suitable for complex setup
- Basic availability of servers
- Problems with „false positives“
- **„Happy time“ - crashes were known and we were happy from it**

History of Zabbix at SLU
First stage

- „One man show“ :)
- Hardly configured
- We needed to upgrade often because of new features
- No clean upgrade procedure from alpha versions
- Moving to second stage
- **„Fuzzy time“ - crashes were sometimes known and we were happy when Zabbix reported it**

History of Zabbix at SLU
First stage

- „One man show“ :)
- Hardly configured
- We needed to upgrade often because of new features
- No clean upgrade procedure from alpha versions
- Moving to second stage
- **„Fuzzy time“ - crashes were sometimes known and we were happy when Zabbix reported it**

History of Zabbix at SLU
Second stage

- Problem with upgrade „solved“ by big boom
- We started to configure from scratch
- There were not so many hosts/items
- We „migrated“ to 1.4
- **„Hectic time“ - More crash specific than monitoring specific becouse of „one man show“ in monitoring**

History of Zabbix at SLU
Third stage

- We needed to interconnect two servers
- One in Opava, second in Karvina
- Problems with multi-node setup
- In fact, we found that it is not needed
- Spliting multinode into two nodes
- From this point, Zabbix is used even for inventory
- **„Light time“ - crashes are localised, monitored, reported and everybody is happy..**

History of Zabbix at SLU
Fourth stage

- Inventory data inside..
- Why not use them for other purposes?
- Import/export script for Cisco devices
- All network devices inside
- Created graphs and maps
  - Servers
  - Networks
  - Wireless networks
  - Network devices

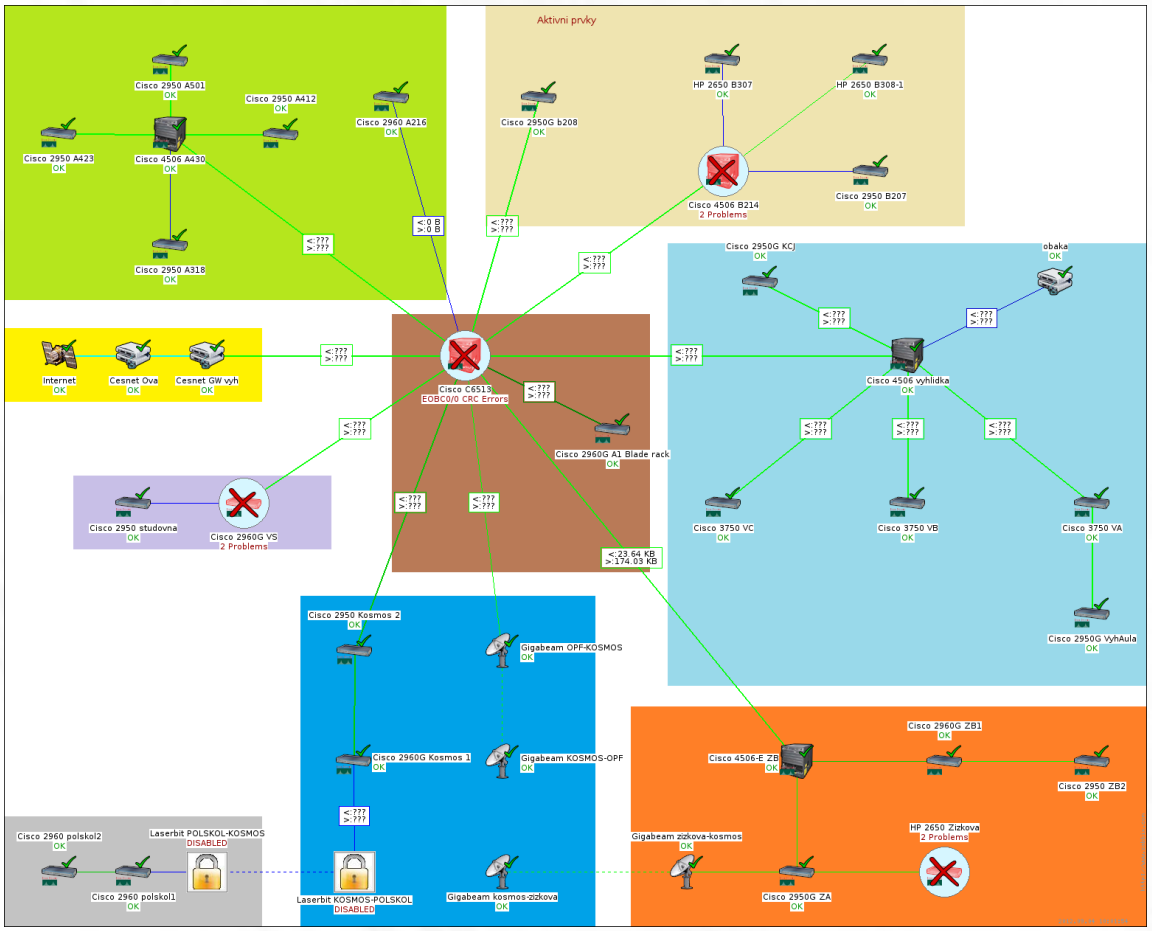
History of Zabbix at SLU
Fourth stage

- Informations about server:
  - Inventory
  - Data from agent
  - Data from agentless monitoring
  - Pending updates (debian)
  - Status of backup (daily, weekly)
  - Throughput of connection (from switch)

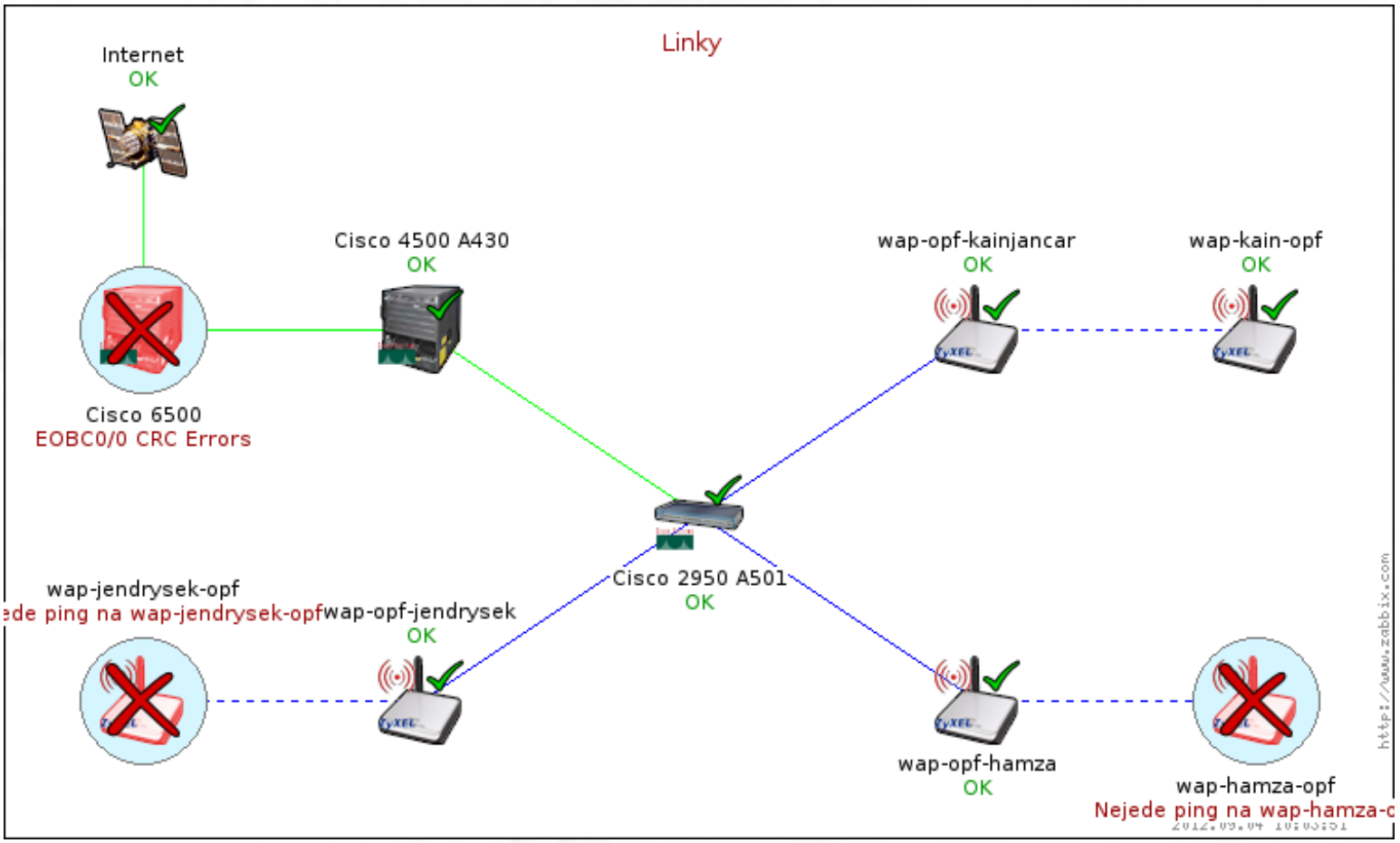
Zabbix on SLU today

- Version 2.0.2
- Migration took some time ;)
- Everything works great
- We changed template system to new, autodiscovery for SNMP devices
- All inventory informations inside
- Especially virtual infrastructure is documented

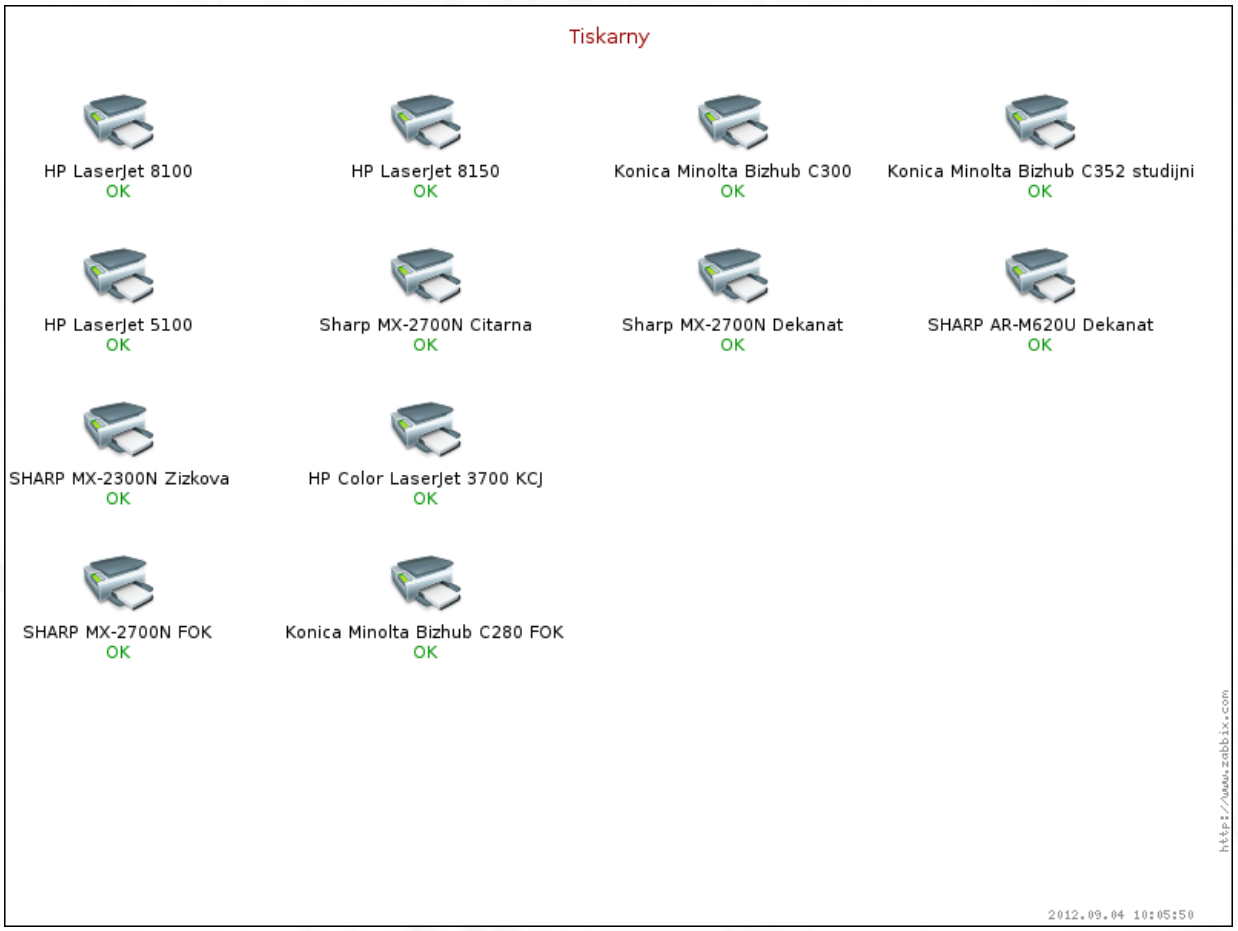
Network map


Aktivni prvky
Cisco 2950 A501
OK
Cisco 2950 A412
OK
Cisco 2960 A216
OK
Cisco 2950 A423
OK
Cisco 4506 A430
OK
Cisco 2950 A318
OK
Cisco 2950G b208
OK
HP 2650 B307
OK
HP 2650 B308-1
OK
Cisco 4506 B214
2 Problems
Cisco 2950 B207
OK
Cisco 2950G KCJ
OK
obaka
OK
Cisco 4506 vyhlidka
OK
Cisco 3750 VC
OK
Cisco 3750 VB
OK
Cisco 3750 VA
OK
Cisco 2950G VyhAula
OK
Internet
OK
Cesnet Ova
OK
Cesnet GW vyh
OK
Cisco C6513
EOBC0/0 CRC Errors
Cisco 2960G A1 Blade rack
OK
Cisco 2950 studovna
OK
Cisco 2960G VS
2 Problems
Cisco 2950 Kosmos 2
OK
Gigabeam OPF-KOSMOS
OK
Cisco 2960G Kosmos 1
OK
Gigabeam KOSMOS-OPF
OK
Laserbit KOSMOS-POLSKOL
DISABLED
Gigabeam kosmos-zizkova
OK
Cisco 2960 polskol2
OK
Laserbit POLSKOL-KOSMOS
DISABLED
Cisco 2960 polskol1
OK
Cisco 4506-E ZB
OK
Cisco 2960G ZB1
OK
Cisco 2950 ZB2
OK
Gigabeam zizkova-kosmos
OK
HP 2650 Zizkova
2 Problems
Cisco 2950G ZA
OK

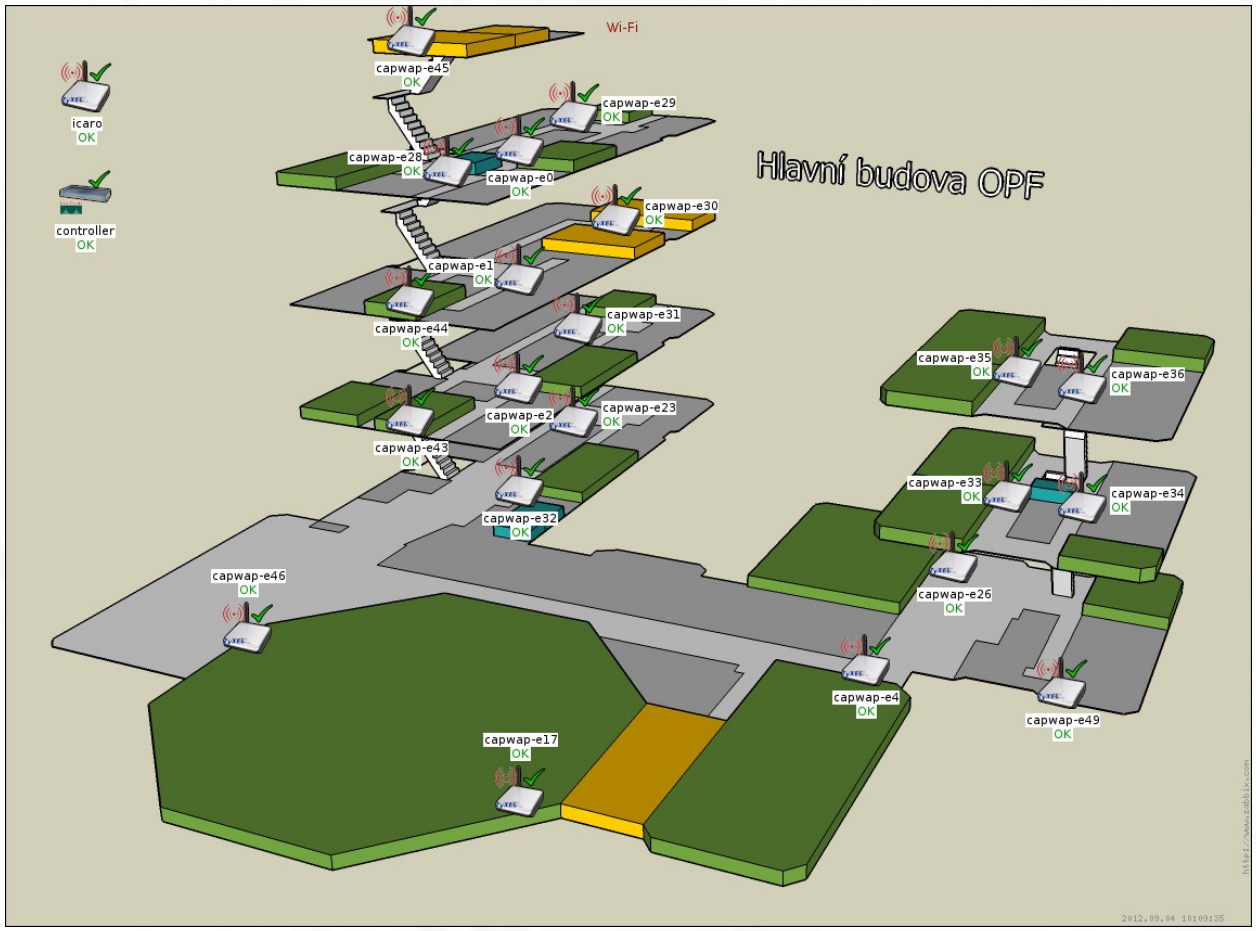
Network links map



Printers map



Wifi map


Wi-Fi
Hlavní budova OPF
capwap-e45
OK
icaro
OK
controller
OK
capwap-e29
OK
capwap-e28
OK
capwap-e0
OK
capwap-e30
OK
capwap-e1
OK
capwap-e31
OK
capwap-e44
OK
capwap-e2
OK
capwap-e23
OK
capwap-e43
OK
capwap-e32
OK
capwap-e46
OK
capwap-e17
OK
capwap-e35
OK
capwap-e36
OK
capwap-e33
OK
capwap-e34
OK
capwap-e26
OK
capwap-e4
OK
capwap-e49
OK

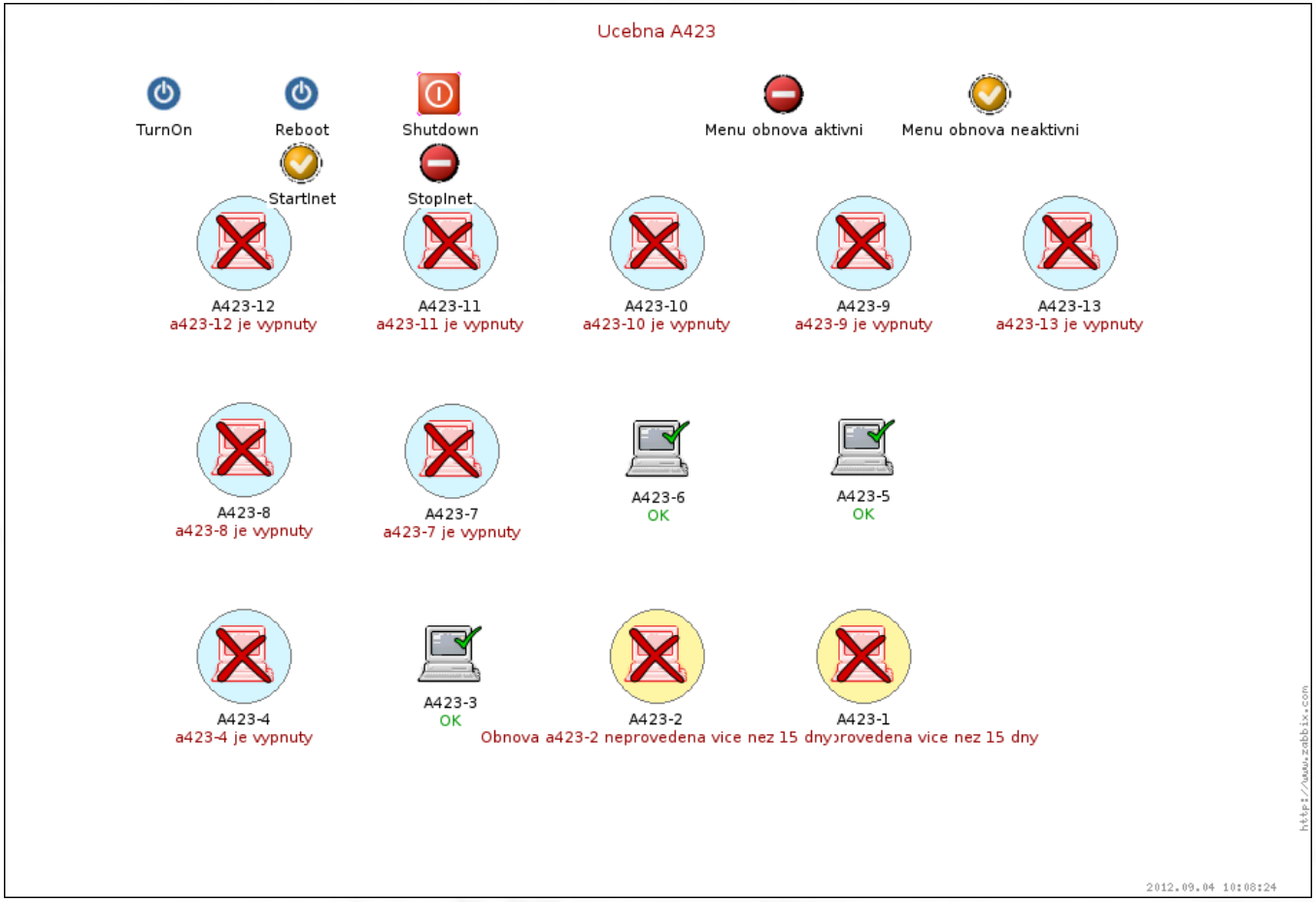
ObnovaNG at SLU

- System for refreshing PC labs
- Users has admin privileges on lab PCs
- They can erase/modify everything
- If they want to know IT, they has to know how to destroy PC ;)
- ObnovaNG uses Zabbix and Rsync to „refresh“ PC into predefined state
- Used before tests by lectors too

Today's usage for labs

- Informations about Lab PC:
  - Inventory (Mac address, ..)
  - Data from agentless monitoring
  - Status of refresh (obnovang)
  - Ping (PC is on/off)
  - Last logged user

Lab map


Ucebna A423
TurnOn
Reboot
Shutdown
Menu obnova aktivni
Menu obnova neaktivni
StartInet
StopInet
A423-12
a423-12 je vypnuty
A423-11
a423-11 je vypnuty
A423-10
a423-10 je vypnuty
A423-9
a423-9 je vypnuty
A423-13
a423-13 je vypnuty
A423-8
a423-8 je vypnuty
A423-7
a423-7 je vypnuty
A423-6
OK
A423-5
OK
A423-4
a423-4 je vypnuty
A423-3
OK
A423-2
A423-1
Obnova a423-2 neprovedena vice nez 15 dnyprovedena vice nez 15 dny
2012.09.04 10:08:24

Today's usage for servers

- Informations about server:
  - All informations from agent
  - Disk, CPU, throughput, running services
  - Status of central backup
  - Status of debian updates
  - Local scripts to check some specialities

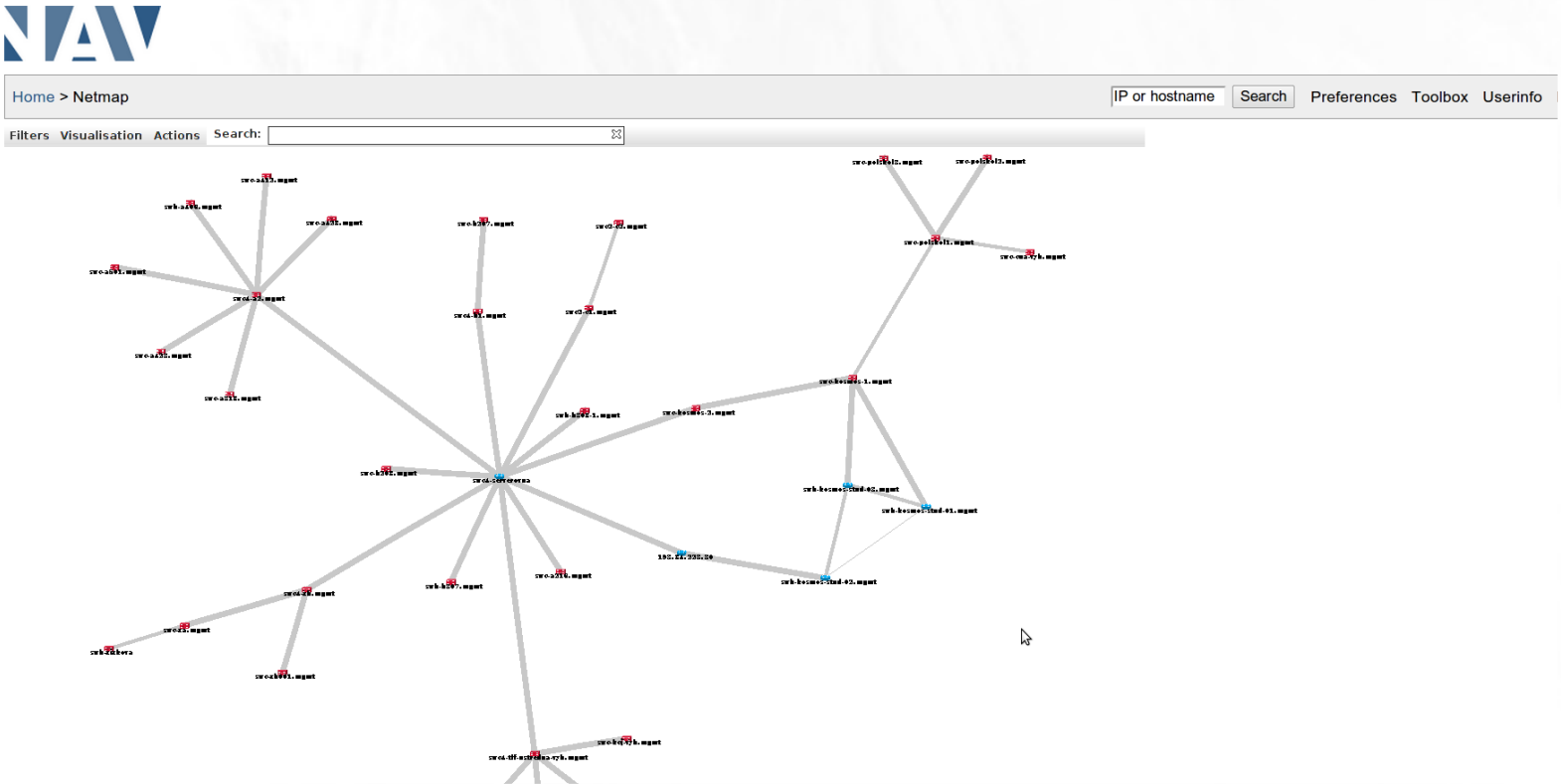
Current state of Zabbix at SLU

- Two Zabbix Servers, not connected
- LDAP central authentication
- Some monitoring even in NAV
- Huge amount of data
- Still on mysql

Other tools
NAV

- Nav (http://nav.uninett.no/)
- Great tool to troubleshoot L2 and L3 problems
- To glue MAC, IP and switch port
- To search MAC or IP and find directly switch port
- To track stateless IPv6 addresses
- Together with Zabbix, it is ultimate tool
- Maybe better interconnection with Zabbix in future?

Nav automatic map



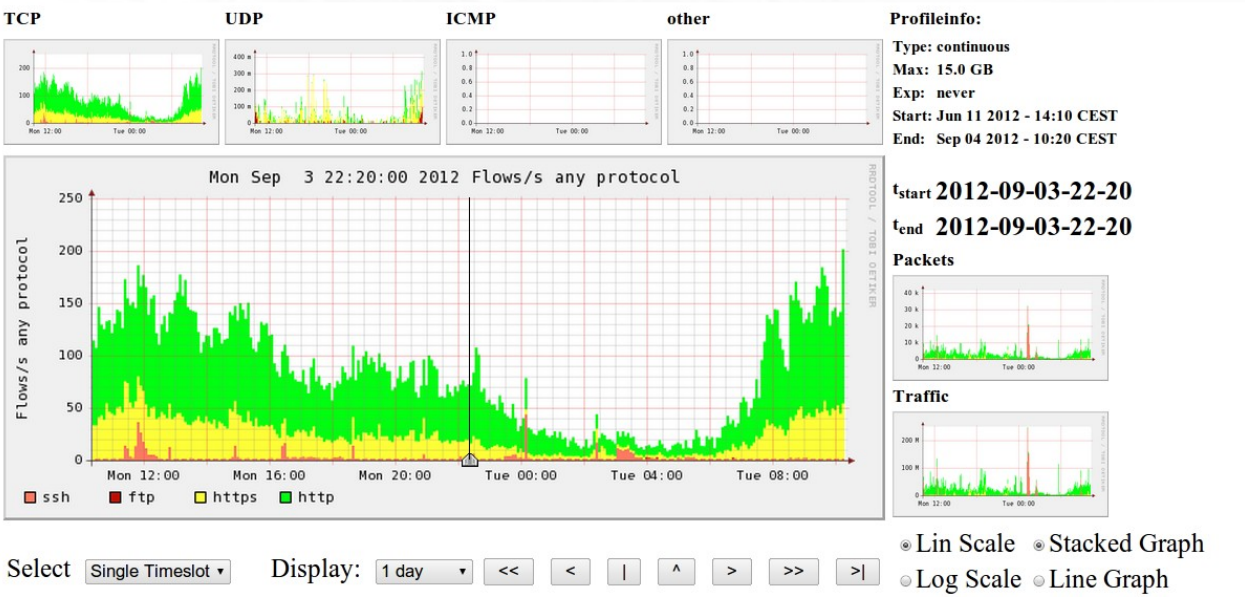
Other tools

Flowmon probe

- Flowmon probe from Invea Tech
- Used for
  - Troubleshooting internal network problems
  - Track security incidents
- Can be preconfigured with its own Zabbix server
- Maybe it is good to interconnect with Zabbix?

Other tools

Flowmon



Statistics timeslot Sep 03 2012 - 22:20

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ http	52.6 /s	52.6 /s	0 /s	0 /s	0 /s	2.6 k/s	2.6 k/s	0 /s	0 /s	0 /s	22.1 Mb/s	22.1 Mb/s	0 b/s	0 b/s	0 b/s
☑ https	17.9 /s	17.8 /s	0.0 /s	0 /s	0 /s	751.1 /s	751.0 /s	0.0 /s	0 /s	0 /s	6.3 Mb/s	6.3 Mb/s	10.7 b/s	0 b/s	0 b/s
☑ ftp	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	0.2 /s	0.2 /s	0 /s	0 /s	0 /s	92.5 b/s	92.5 b/s	0 b/s	0 b/s	0 b/s
☑ ssh	1.6 /s	1.6 /s	0 /s	0 /s	0 /s	12.2 /s	12.2 /s	0 /s	0 /s	0 /s	16.7 kb/s	16.7 kb/s	0 b/s	0 b/s	0 b/s

All
None

Display: ○ Sum ◉ Rate

Other tools

PAWOUK

- Software for students on dormitory
- Register, activate, deactivate and manage Internet connection for students
- Connected with freeradius server
- Used with Cisco as 802.1x
- Used with webauth where 802.1x is not possible

Other tools

Central rsyslog server

- Central point of logging
- Some important information in Zabbix too
- Glue for searching incidents and problems (IP/Mac, Radius, EduID, Eduroam,...)
- Splunk used for data mining

Current implementation
Results

- More software solutions together
- Core is Zabbix (monitoring, inventory, simple management)
- NAV mainly for detecting and searching L2 and L3 nodes on network
- Flowmon for security incidents and data monitoring
- PAWOUK for managing, searching and (dis)connecting students
- Central Rsyslog server
- We need 100% guarantee that we can find any network flow from/to our network and glue right person to it for security incident handling.

Current state of Zabbix at CESNET

- Bad, but I am doing best to change it :)
- Nagios is widely used and goodly configured
- Nobody want's to change becouse of
  - „Never touch running system“ formula

What we are missing?

- Working CLI for backups/exports/imports for automatized backups and imports
- Quicker recovery (delayed?)
- Migration tool from mysql into pgsql
- Interconnection with NAV?
- Better management of SNMP devices (partialy solved in 2.0 SNMP autodiscovery)
- Possibility to analyze and glue history data by some module (statistics, AI, playground for students)

What we are missing?

- Modularity? Yes, it is possible to use API for any external software. But for analysing huge amount of data?
- IPv6 services support in GUI (not possible to create IPv6 service template based?)
- Timeline – possibility to see what happened in past time and ability to „switch“ frontend to some time back (maybe to future? :))
- SVG graphs for better granularity and export
- SVG maps
- Scripting (lua?) for more complex scenarios or module support (eg. For functionality like NAV)

What we are missing?

- Wizard for adding and discovering new devices (simple, agent, SNMP)
- Automatic creation of map from host group or via wizard
- „Click until death“ problem

Other zabbix projects

- Meteo4u.cz
  - Combination of Drupal and Zabbix
  - Using Zabbix API
  - Using Zabbix graphs
  - Using entire power of Zabbix

Other zabbix projects

- BESIP (SIP server based on OpenWRT)
  - Should use Zabbix as default
  - Either only agent or server too
  - Embedded design (sqlite)
  - Needed to upgrade Zabbix in OpenWrt
  - Besip info available at http://homeproj.cesnet.cz/projects/besip/wiki
  - Repository for OpenWRT available, zabbix2 inside!

Conclusions

- Great software, stay on!
-
- Lukas Macura
- CESNET
- Silesian University in Opava
- Lukas.macura@cesnet.cz