HÁLÓZATFELÜGYELET SZABAD SZOFTVEREKKEL

Lajber Zoltán

lajber.zoltan@ih.szie.hu

Szent István Egyetem, Informatikai Hivatal

http://zeus.gau.hu/~lajbi

Bevezetés

Motto: mindenki másként csinálja

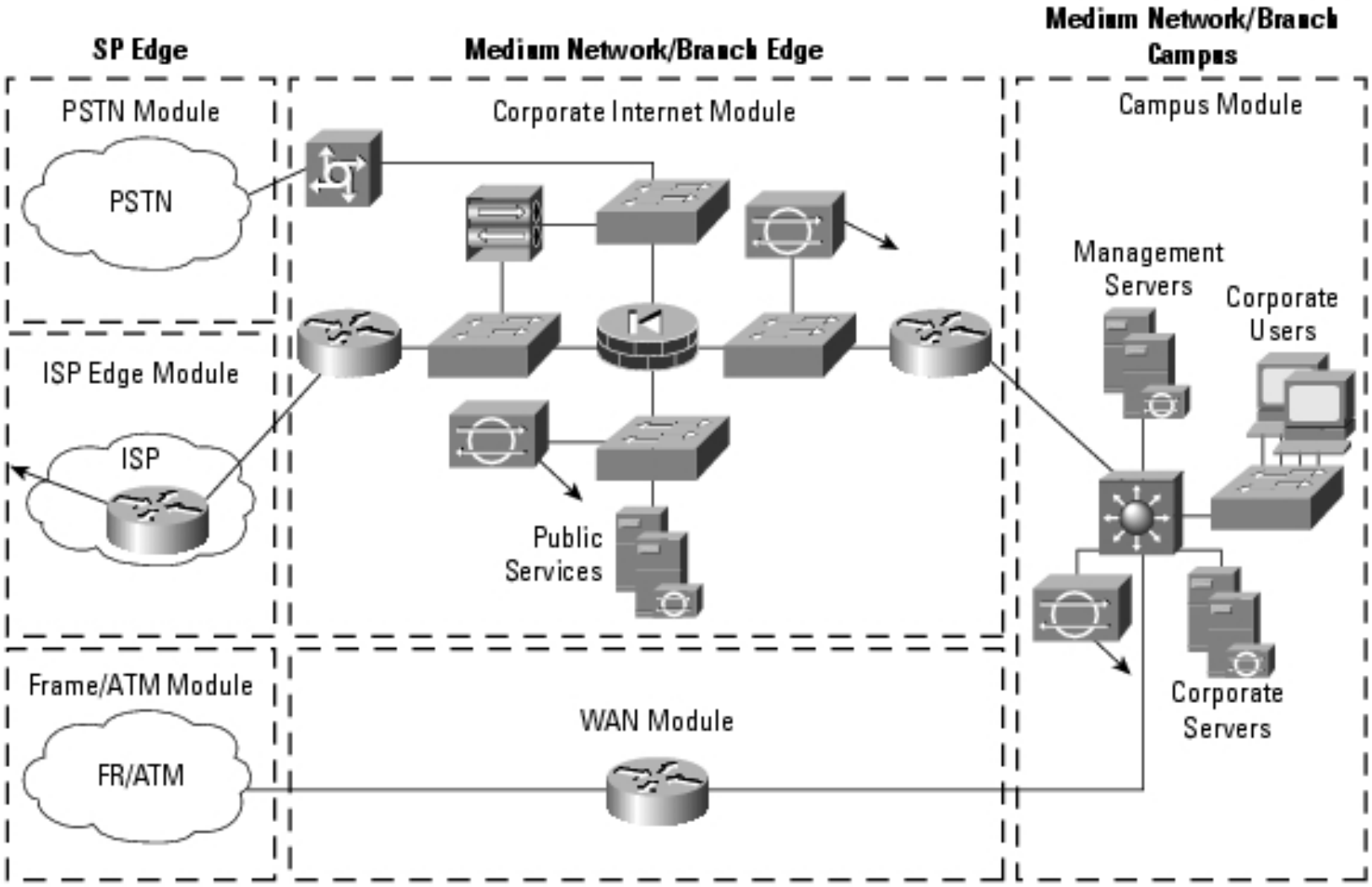
Előadás tematikája:

- tervezés
- esemény naplózás: syslog-ng
- forgalom naplózás: netacc-ng, flow-tools
- háttérszolgáltatások: NTP, DNS, TFTP, TACACS+, RADIUS
- mi történik a hálózatban? nagios
- mi történt, mi fog történni? munin, cricket
- nyilvántartások: netdisco, háztáji programok

TERVEZÉS

alap feltételezések

- hálózat managementre dedikált gép,
- noc (Network Operation Center) a szokásos elnevezés
- nagyobb hálózatokban management subnet
- noc kiemelt jogokkal rendelkezik
- védelme kritikus
- állatorvosi ló: `http://www.cisco.com/go/safe`


SP Edge
Medium Network/Branch Edge
Medium Network/Branch Campus
PSTN Module
PSTN
Corporate Internet Module
Campus Module
Management Servers
Corporate Users
ISP Edge Module
ISP
Public Services
Frame/ATM Module
FR/ATM
WAN Module
Corporate Servers

szétválasztás

- logikai és fizikai hálózati struktura eltér
- VLAN a szétválasztásra
- Cisco esetén az 1-es VLAN kitüntetett:
  - alapértelmezett vlan ⇒ez hiba, átt kell állítani
  - alapértelmezett managment VLAN ⇒állítható, de nem érdemes
  - mert a CDP, PAgP, nem PVSPT BPDU úgyis 1-es vlan-ban megy
- 1-es VLAN-ban csak infrastruktúra eszközök, csak a management gépről legyen elérhető
- route, DNS feloldás is csak 1-es és management gépekre

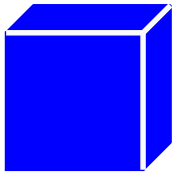
dokumentáció

Izlés szerint több program: Visio, dia, **tgif**

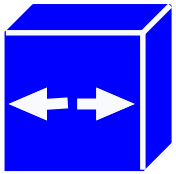
- saját szimbolumok
- sok formátum: png, eps, html imagemap

```
/etc/X11/app-defaults/Tgif:
Tgif.DefaultDomain: 0
Tgif.MaxDomains:        2
Tgif.DomainPath0:       NET:\ n \
                            /usr/local/lib/tgif/net:\ n \
Tgif.DomainPath1:       SERVER:\ n \
                            /usr/local/lib/tgif/server:\ n
```

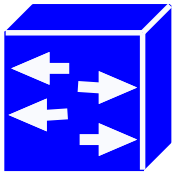
HUB
KTI



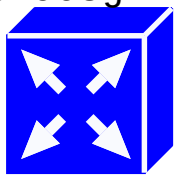
switch
KTI 624



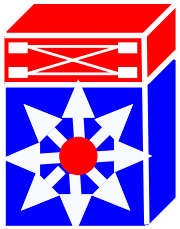
VLAN switch
c3548



L3 switch
c4908g-l3

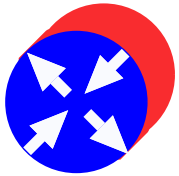


routerswitch
c6500



router
c7206vxr

pf router
c7206vxr



firewall
PIX

firewall
PIX

firewall
fwsm

firewall
fwsm

ESEMÉNY NAPLÓZÁS

- központi naplózás fontosabb eszköz az események kezelésében
- feltételezi, hogy a gépek órái jól járnak ⇒NTP
- túl részletes napló kezelhetetlen
- nagyforgalmú router vagy tűzfal belerokkanhat a naplózásba, DoS lehetősége
- log rotálás, archiválás, előírások...
- eredeti syslog nem elég jó a szétválogatásra több eszköz esetén
- `syslog-ng` szép, jó, kényelmes

`syslog-ng.conf` **részlet**

```
destination pix_err { file("/var/log/routers/pix_err.log" owner("root")
group("adm") perm(0640)); };
destination pix_crit { file("/var/log/routers/pix_crit.log" owner("root")
group("adm") perm(0640)); };
...
filter f_pix_crit       { host(192.188.242.246) and match("PIX-[12]");};
filter f_pix_err        { host(192.188.242.246) and match("PIX-[34567]");};
...
log { source(net); filter(f_pix_crit); destination(pix_crit); };
log { source(net); filter(f_pix_err); destination(pix_err); };
```

/etc/logrotate.d/routers **részlet**

```
/var/log/routers/*.log {
        daily
        olddir /var/log/routers/old/
        rotate 365
        compress
}
```

FORGALOM NAPLÓZÁS

netacc-ng: – linuxos routereken jó

- nem kell forgalommérés miatt tűzfal szabályokat beiktatni
- 100Mbps fölött mindenkép ratelimit kell a tűzfal logra
- adatbázisba is tud dolgozni

kis cisco dobozok: SPAN és pcap

nagy cisco dobozok: flow-export elkapása flow-tools-al

- jól darabolható logok
  - óránként új fájl, max 45G hely ⇒nálunk ez kb 1 hónap core router flow
- NAT előtt switched flow export a NAT-olt vlan-ról, de ez erősen növeli a méretet
- tovább küldhető pl. online elemzésre

HÁTTÉRSZOLÁLTATÁSOK

NTP :

- nagyon lényeges a gépek és routerek pontos órája
- core router szinkronizál kinti forrásokhoz
- mindenki más a core routerhez
- bootoláskor `ntpdate`, utána `ntpd`

DNS :

- nagyon sok szolgáltatás függ tőle (emergency PXE boot..)
- gyorsítja a helyreállítási munkálatokat
- rekurzív és authoratív funkciók szétválasztása
- redundancia, magas rendelkezésre állás
- logikus nevezéktan, aktiv eszközöknek külön subdomain

kábelek : `F2I-001`

switchek : `asw-f2i1.mtz.gau.hu`

ups : `ups-syma.mtz.gau.hu`

firewall context : `fwm-core-diak.mtz.gau.hu`

szerver ILOM : `sp-pityu1.mtz.gau.hu`

TACACS+ :

- hálózati eszközre beléptetés
- kiadott parancsok naplózása
- elvileg lehet emberek és parancsok külön engedélyezése

RADIUS :

- átmenő forgalomhoz jobb: behívó, vpn, wifi 802.1x
- többféle adatbázis lehet mögötte
- nálunk LDAP backend, de `users` fájl a kivételek kezelésére
- használat: 802.1x, VPN

TFTP :

- hálózati eszközök configja

  ```
  alias exec wrnet copy running-config tftp://192.188.242.5/asw-f2i1
  ```

- hálózati eszközök op. rendszere
- PXE boot rescue szervereknek, új gép telepítés gyorsítása
- verziókövető rendszerrel, webbel kombinálható ⇒HBONE
- speciális tűzfal szabályok: kérés UDP 69-re érkezik, de további csomagok UDP $>$ 1023
- nincs authentikáció, de az irandó fájlnak léteznie kell, és 666 jogunak kell lennie
- default hely helyett javasolt a `/var/lib/tftp`

MI TÖRTÉNIK A HÁLÓZATBAN: NAGIOS

Nagios működése

- `service check` -re készült, nem host pingetésre
- de szolgáltatás csak `host`on futhat...
- igyekszik elkerülni, hogy felesleges információkkal bombázzon: függőségek
- fontos elem: `state` nem két, hanem több állapotú

Függőségek

- amíg a service check lefut, nem csinál host check-et
- ha pl DNS megy, nem nézi meg a `switch1` és `switch2`-t
- ellenőrzés sorrendje:
  1. service
  2. host
  3. parent hosts
- nagios géppel egy szegmensen lévő gépeket definiálhatjuk parent nélkül (van még ilyen?)
- **döntés**: switch vagy router a szegmens határ? azaz L2 vagy L3 struktúra szerint épitkezzen-e a nagios
- ha pl L3, akkor nem tudhatja, hogy a távoli host a switch hibája miatt nem érhető el ⇒extra üzenetek

host check

- alapértelmezetten a `host check` csak akkor fut le, ha kell
- `check_interval` befolyásolja a viselkedést
- host check csak elérhetőséget vizsgál
- ping service hasznos host ellenőrzésre is, extra információk: ping time, packet loss
- lassú vonalak esetén alapértelmezett paraméterek átállítása szükséges

```
define service {
        use                             generic-service
        name                            ping-service
        service_description             PING
        check_command                   check_ping!200.0,20%!800.0,60%
        register                        0
        }

define service {
        use                             generic-service
        name                            ping-slow-service
        service_description             PING
        check_command                   check_ping!500.0,20%!1200.0,60%
        register                        0
        }
```

host és service state

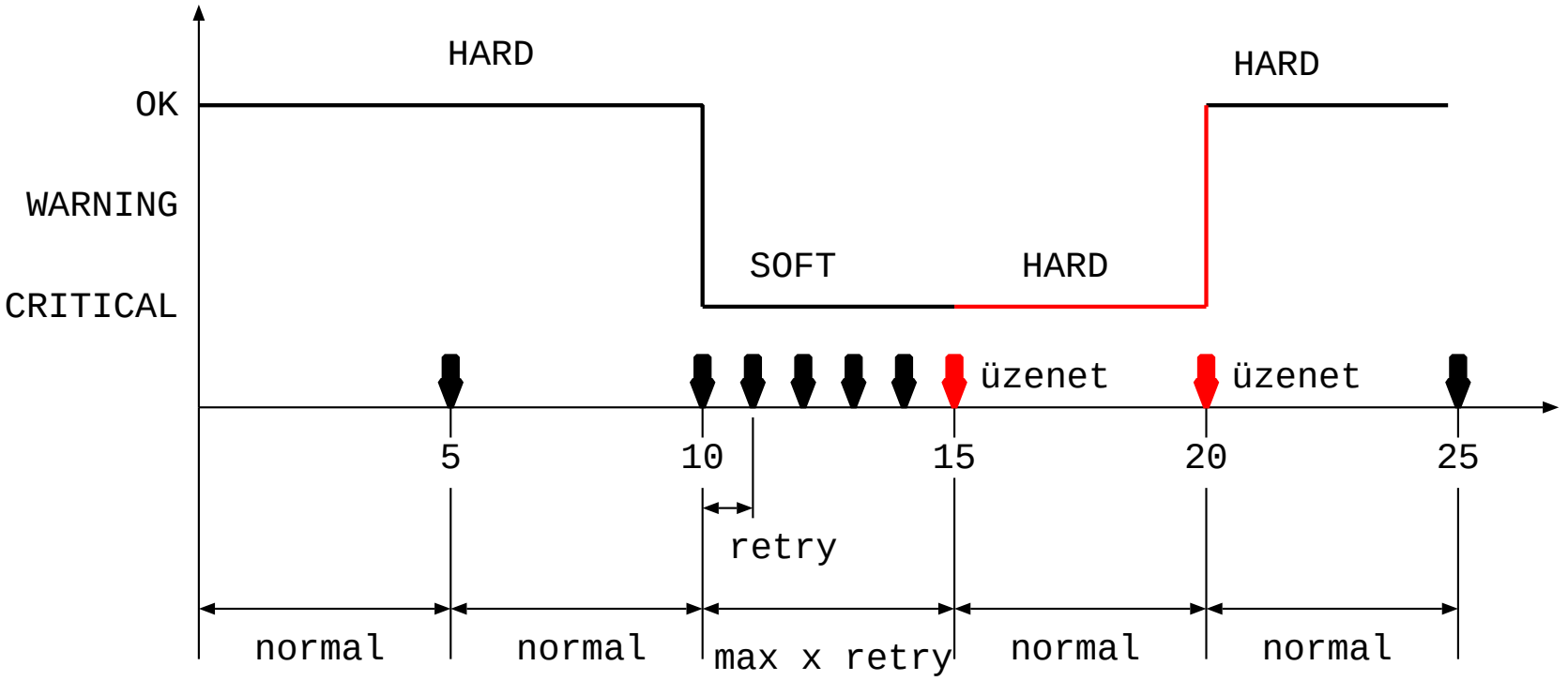
Host és service check lehetséges visszatérési értékei:

érték	jelentés	megjegyzés
0	OK	mindig HARD
1	WARNING	
2	CRITICAL	SOFT, majd HARD
3	UNKNOWN	plugin hiba

Vonatkozó config opciók:

opció	def.	megjegyzés
`normal_check_interval`	5	normál időköz
`retry_check_interval`	1	soft state időköz
`max_check_attempts`	5	soft state hossza

eseménysor


HARD
HARD
OK
WARNING
SOFT
HARD
CRITICAL
üzenet
üzenet
5
10
15
20
25
retry
normal
normal
max x retry
normal
normal

Konfigurálás

- lehet adatbázisban és fájlban
- több dolgot kell konzisztensen tartani
- nem tudok jó segédeszközt
- ellenőrzés: `nagios -v /etc/nagios/nagios.cfg`

hosts.cfg

```
define host{
        use             generic-host
        name            generic-dmz
        parents         edge
        register        0
}
define host{
        use             generic-dmz
        host_name       gate
        alias           gate.gau.hu
        address         192.188.242.65
}
```

services.cfg

```
define service{
        use                             generic-service
        name                            monguz-service
        service_description             monguz
        check_command                   check_tcp!8080
        register                        0
        }
define service{
        use                 monguz-service
        host_name           gaia
        contact_groups      server-admins
        }
```

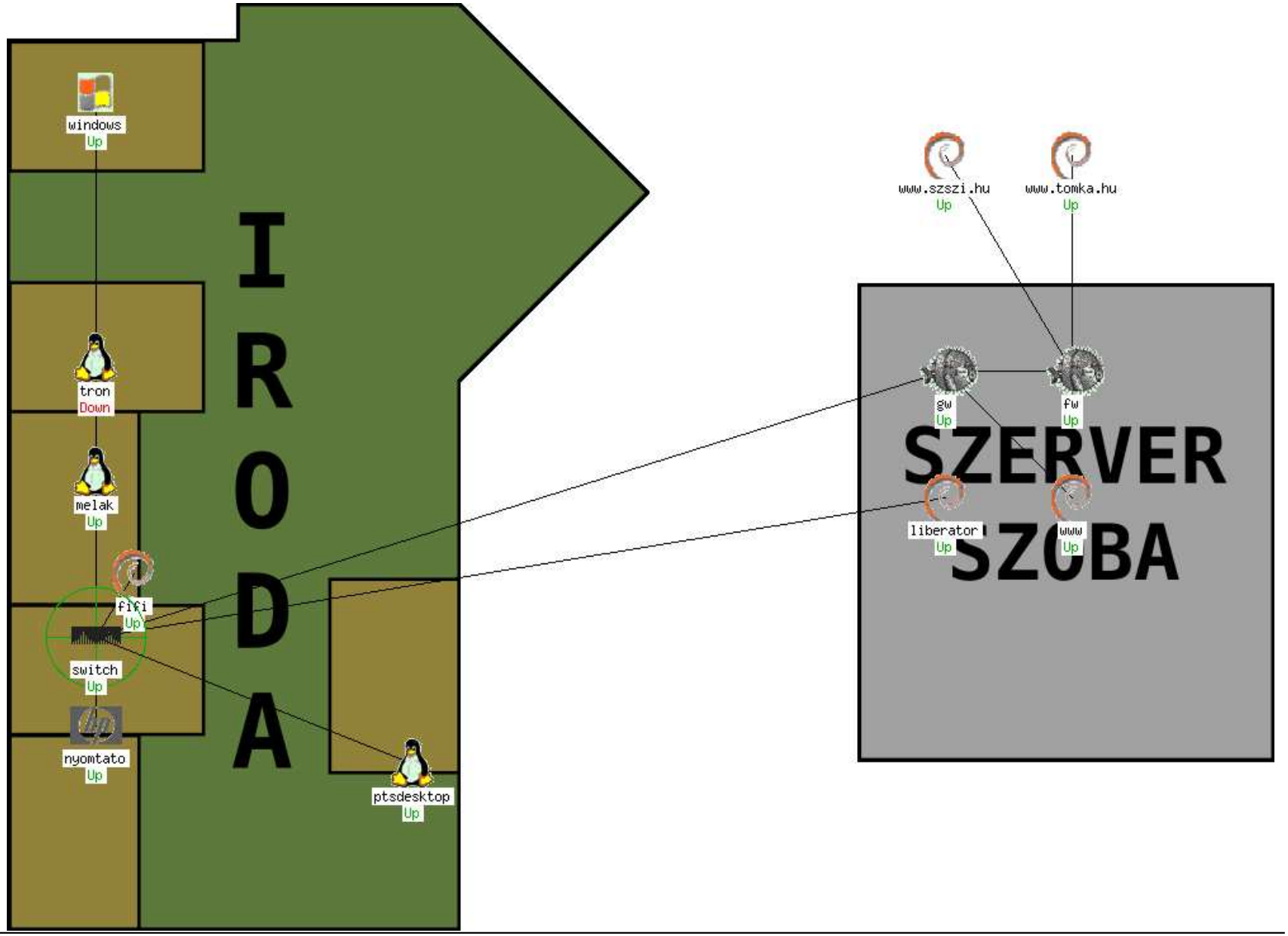
hostgroups.cfg

```
# neptun host group definition
define hostgroup{
        hostgroup_name  neptun
        alias           NEPTUN
        contact_groups  neptun-admins
        members         tsz1,web1,web3,web4,kom2,kom3,db3,db4,blade
}
```

hostextinfo.cfg

- cgi felület számára info
- 2D koordináták, alaprajz...
- 3D koordináták, VRML...

```
define hostextinfo{
        name                    switch
        icon_image              switch40.png
        statusmap_image         switch40.gd
        register                0
        }
define hostextinfo{
        use                     switch
        host_name               asw-apa1
        }
```


IRODA
SZERVER SZOBA
windows
Up
tron
Down
melak
Up
fifi
Up
switch
Up
nyomtato
Up
ptsdesktop
Up
www.szszi.hu
Up
www.tomka.hu
Up
gw
Up
fw
Up
liberator
Up
www
Up

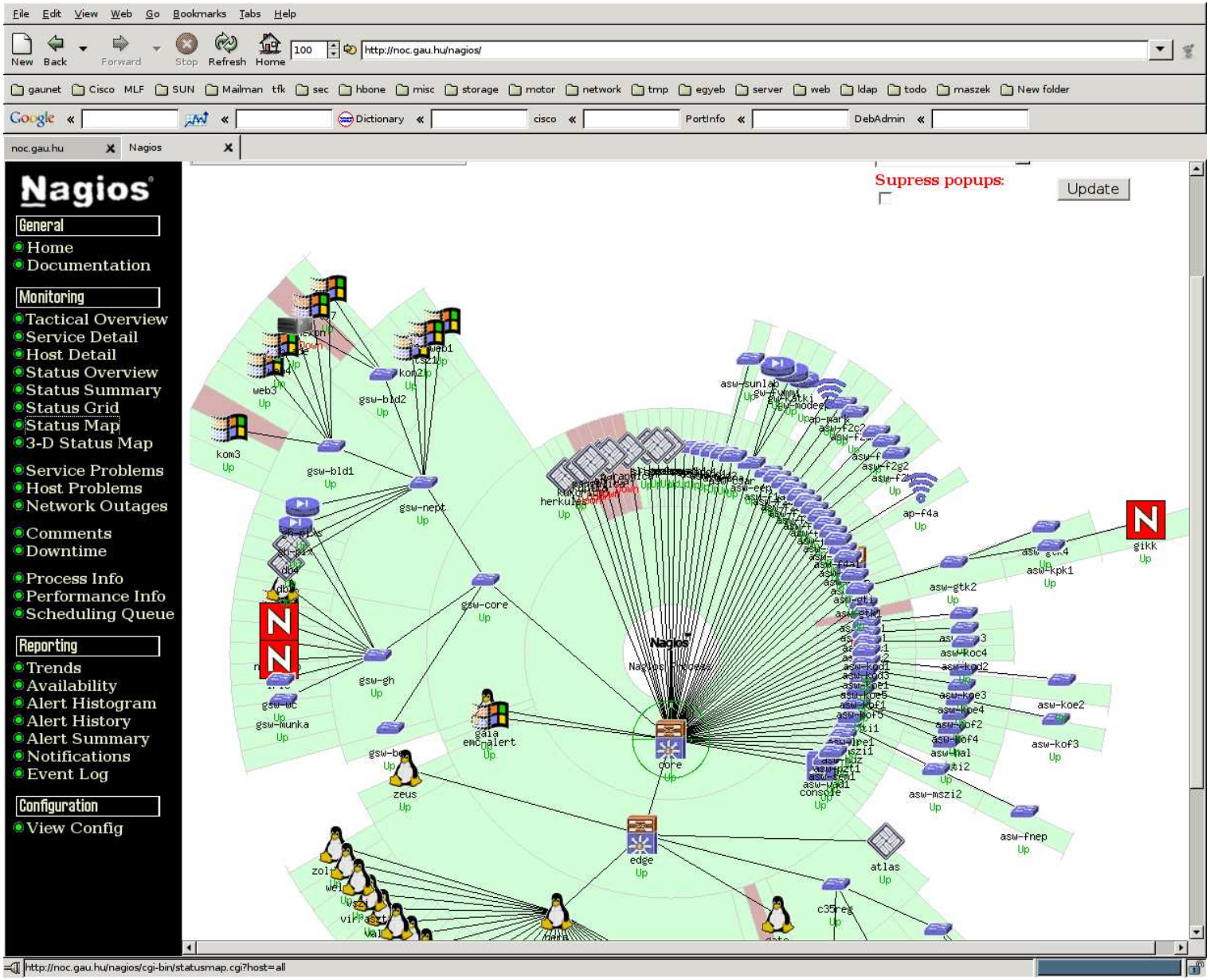
contacts.cfg

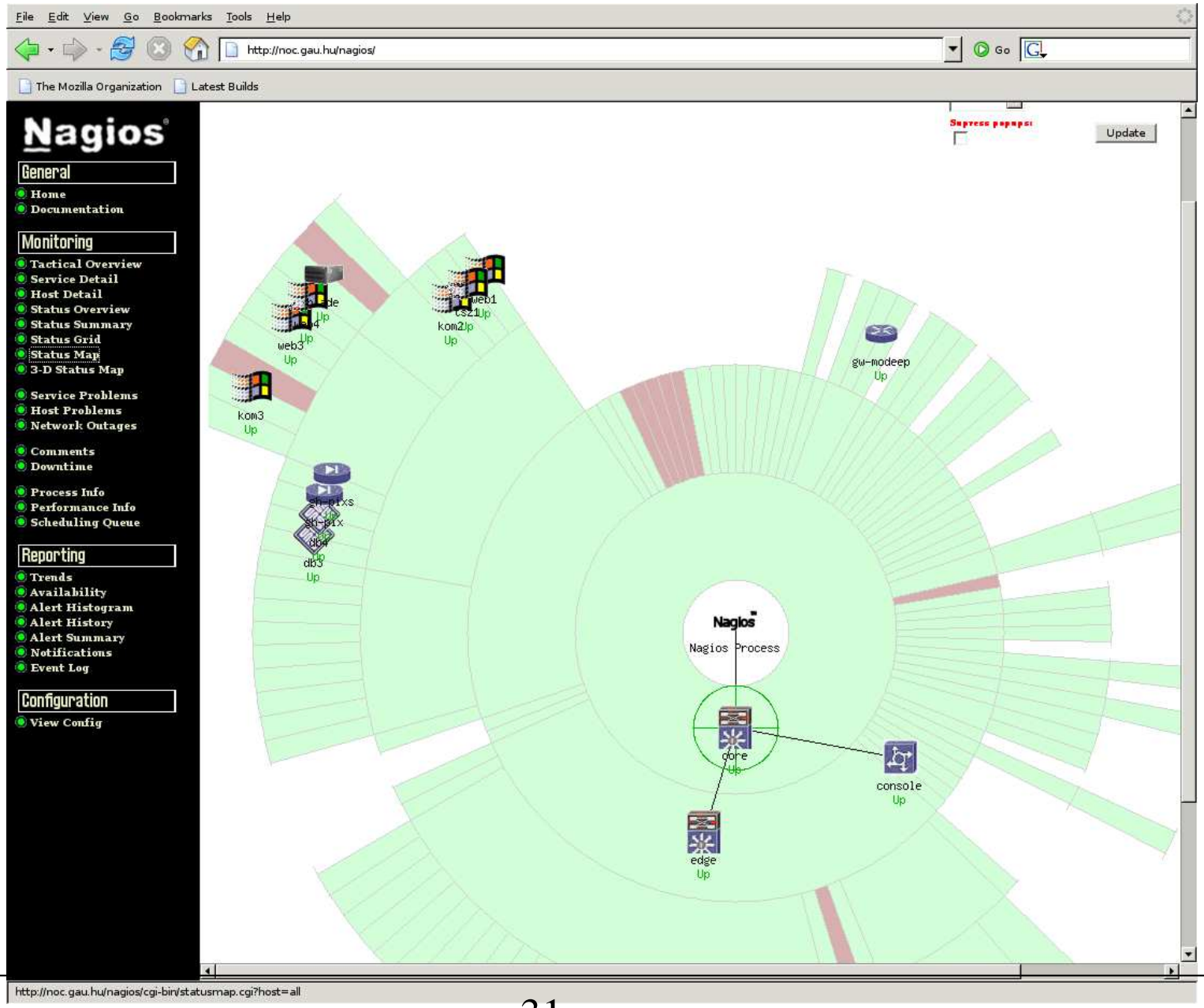
```
define contact{
        contact_name                    lajbi
        alias                           Lajber Zoltan
        use                             generic_contact
        email                           lajbi@zeus.gau.hu
        pager                           0555916580
}
```

contactgroups.cfg

- értesítések
- webes felületen mit lát

```
define contactgroup{
        contactgroup_name       net-admins
        alias                   network Administrators
        members                 fitori,lajbi,liszkai
        }
```


File Edit View Web Go Bookmarks Tabs Help
New Back Forward Stop Refresh Home
http://noc.gau.hu/nagios/
noc.gau.hu
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Supress popups:
Update
core
edge
gsw-core
gsw-nept
gsw-bld1
gsw-bld2
gsw-gh
gsw-wc
gsw-munka
zeus
gaia
emonalert
atlas
gikk
asw-gtk2
asw-kpk1
asw-koe2
asw-kof3
asw-mszi2
asw-fnep
http://noc.gau.hu/nagios/cgi-bin/statusmap.cgi?host=all


File Edit View Go Bookmarks Tools Help
http://noc.gau.hu/nagios/
The Mozilla Organization
Latest Builds
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Update
web3
Up
kom3
Up
kom2
Up
gw-modeep
Up
db3
Up
Nagios
Nagios Process
core
Up
console
Up
edge
Up
http://noc.gau.hu/nagios/cgi-bin/statusmap.cgi?host=all

tippek és trükkök

- saját iconok
  - status overview és hasonlók: icon png
  - status map: gd vagy gd2
  - indexed png konvertálható, `pngtogd` a `libgd-tools` csomagban
- `retain_nonstatus_information`
- `define service`-ben több host adható meg, sőt wildcard is
- `define service`-ben `hostgroup_name` is van

egy pager megoldás

- wavecom wmod2 adapter, usb-rs232 adapter
- gsm-tools programcsomag
- nagios config
- bővebb infó: `http://gatling.ikk.sztaki.hu/~kissg/gsm/`

```
#! /bin/sh
# gsmsmsd daemon for sending/receiving sm
#
# -=Lajbi=- 2003 07 02

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
DAEMON=/usr/bin/gsmsmsd
OPT="-b 9600 -d /dev/ttyUSB0 -c 1 -a \"mail lajbi@noc.gau.hu\" -s
/var/spool/sms/out sms no_stat"
NAME=gsmsmsd
DESC="sm daemon"
test -x $DAEMON || exit 0

set -e
```

```
case "$1" in
  start)
        echo -n "Starting $DESC: $NAME"
        start-stop-daemon --start --quiet -b --pidfile /var/run/$NAME.pid
        echo "."
        ;;
  stop)
        echo -n "Stopping $DESC: $NAME "
        start-stop-daemon --stop --quiet --pidfile /var/run/$NAME.pid
        echo "."
        ;;
  restart)
...
```

```
# /etc/nagios/misccommands.cfg
...
# 'notify-by-sms' command definition by Lajbi
define command{
        command_name    notify-by-sms
        command_line    /bin/echo -e "$CONTACTPAGER$\nService:
        $SERVICEDESC$\nHost: $HOSTNAME$\nAddress:$HOSTADDRESS$\n
State:$SERVICESTATE$\nInfo: $OUTPUT$\nDate: $DATETIME$"  >
        "/var/spool/sms/out/$CONTACTNAME$$HOSTNAME$$SERVICESTATE$"
        }
# 'host-notify-by-sms' command definition by Lajbi
define command{
        command_name    host-notify-by-sms
        command_line    /bin/echo -e "$CONTACTPAGER$\nHost '$HOSTALIAS$' is
        $HOSTSTATE$\nInfo: $OUTPUT$\nTime: $DATETIME$" >
        "/var/spool/sms/out/$CONTACTNAME$$HOSTALIAS$$HOSTSTATE$"
        }
```

```
# contacts.cfg
define contact{
        name                            generic_contact
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,u,r
        service_notification_commands   notify-by-email,notify-by-sms
        host_notification_commands      host-notify-by-email,host-notify-by-sms
        register                        0
        }
```

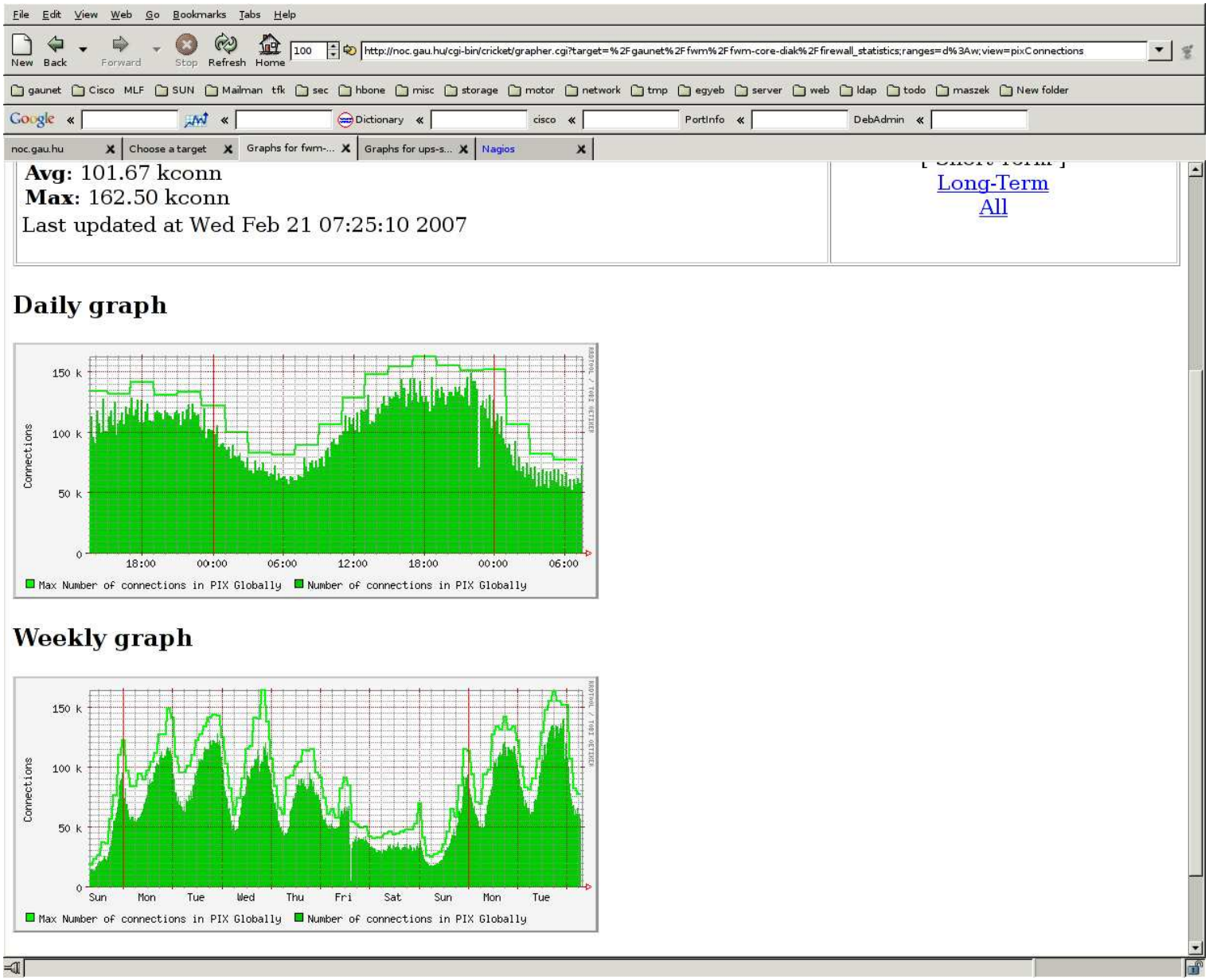
amiről nem beszéltünk még

- passziv szerviz ellenőrzés
- hierarchikus, elosztott nagios rendszer
- szolgáltatás függőség
- szolgáltatás és host eszkaláció
- ...

MI TÖRTÉNT, MI FOG TÖRTÉNNI

SNMP monitor - cricket

- fa szerkezet ⇒configdir
- sok hasonló eszköz kezelése egyszerű
- megfelelő SNMP mib-ek kibányászása
- `genRtrConfig`,`listInterfaces`
- `cricket-compile`
- rrdlib varázslók előnyben


File Edit View Web Go Bookmarks Tabs Help
New Back Forward Stop Refresh Home
http://noc.gau.hu/cgi-bin/cricket/grapher.cgi?target=%2Fgaunet%2Ffwm%2Ffwm-core-diak%2Firewall_statistics;ranges=d%3Aw;view=pixConnections
noc.gau.hu
Choose a target
Graphs for fwm-...
Graphs for ups-s...
Nagios
Avg: 101.67 kconn
Max: 162.50 kconn
Last updated at Wed Feb 21 07:25:10 2007
Long-Term
All
Daily graph
Connections
150 k
100 k
50 k
0
18:00
00:00
06:00
12:00
18:00
00:00
06:00
Max Number of connections in PIX Globally
Number of connections in PIX Globally
Weekly graph
Connections
150 k
100 k
50 k
0
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Mon
Tue
Max Number of connections in PIX Globally
Number of connections in PIX Globally

Defaults fájl:

```
OID     pixConnections  1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6

datasource pixConnections
   rrd-ds-type      =   GAUGE
   ds-source        =   snmp://%snmp%/pixConnections
   rrd-heartbeat    =   1800

targetType     Cisco-pix-stats
       ds = "pixConnections, aByteBlocksFree,bByteBlocksFree,
                  cByteBlocksFree,  dByteBlocksFree, pixcpu5sec, pixcpu5min"
       view = "pixConnections: pixConnections,freeBlocks: aByteBlocksFree
                 bByteBlocksFree cByteBlocksFree dByteBlocksFree,
                 cpu: pixcpu5sec pixcpu5min"
```

targets fájl:

```
target firewall_statistics
   inst                  = 0
   interface-name        = firewall_statistics
   long-desc             = "Number of connections currently in use by the
   entire firewall"
   short-desc            = "Number of connections currently in use by the
   entire firewall"
   target-type           = Cisco-pix-stats
```

host monitor - munin

- netSNMPd-hez rengeteg plugint kellett írni
- munin configja a hoston (is) történik
- plugin írás egyszerű
- munin: központi adatgyűjtés crontab-ból és webes felületen megjelenítés
- munin-node: monitorozandó gépen fut, egy TCP porton fülel

munin

- monitorozandó host ip-jét meg kell adni
- hostok csoportosítva, alapértelmezetten DNS szerint

```
[fkp;zfs.fkp.szie.hu]
    address 192.188.242.205
    use_node_name yes
[szolg;atlas.szie.hu]
    address 192.188.242.79
    use_node_name yes
[ih;sziszifusz.szie.hu]
    address 192.188.242.50
    use_node_name yes
```

munin-node

- ellentétben munin-nal, állandóan fut
- pluginon symlinkelve `/etc/munin/plugins/` vagy `/etc/opt/munin/plugins` -ba
- gyakori, hogy plugin neve határozza meg a figyelendő paramtétert, pl `/usr/share/munin/plugins/if_` ⇒`/etc/munin/plugins/if_eth0`
- plugin API egyszerű, jól dokumentált
- háztáji pluginok:
  - sun fire v20z, x4100 IPMI hőmérséklet és venti fordulat
  - solaris 9 `prtdiag -v` -ből hőmérséklet

munin pluginok

Három esetet kell kezelnie, paramétertől függően

autoconf : opcionális, adjon vissza ”yes”-t

```
# munin-run cpu autoconfig
yes
```

config : adja vissza a configot:

```
# munin-run cpu config
graph_title CPU usage
graph_order system user nice idle iowait irq softirq
graph_args --base 1000 -r --lower-limit 0 --upper-limit 400
graph_vlabel %
graph_scale no
graph_info This graph shows how CPU time is spent.
graph_category system
```

```
graph_category system
graph_period second
system.label system
system.draw AREA
system.max 5000
system.min 0
system.type DERIVE
system.warning 120
system.critical 200
system.info CPU time spent by the kernel in system activities
user.label user
...
```

paraméter nélkül: adja vissza a mért értékeket

```
# munin-run cpu
user.value 1498262
nice.value 1891378
system.value 1606920
idle.value 729010468
iowait.value 569093
irq.value 33221
softirq.value 217272
```

plugin futtatás : `munin-run plugin paramter`

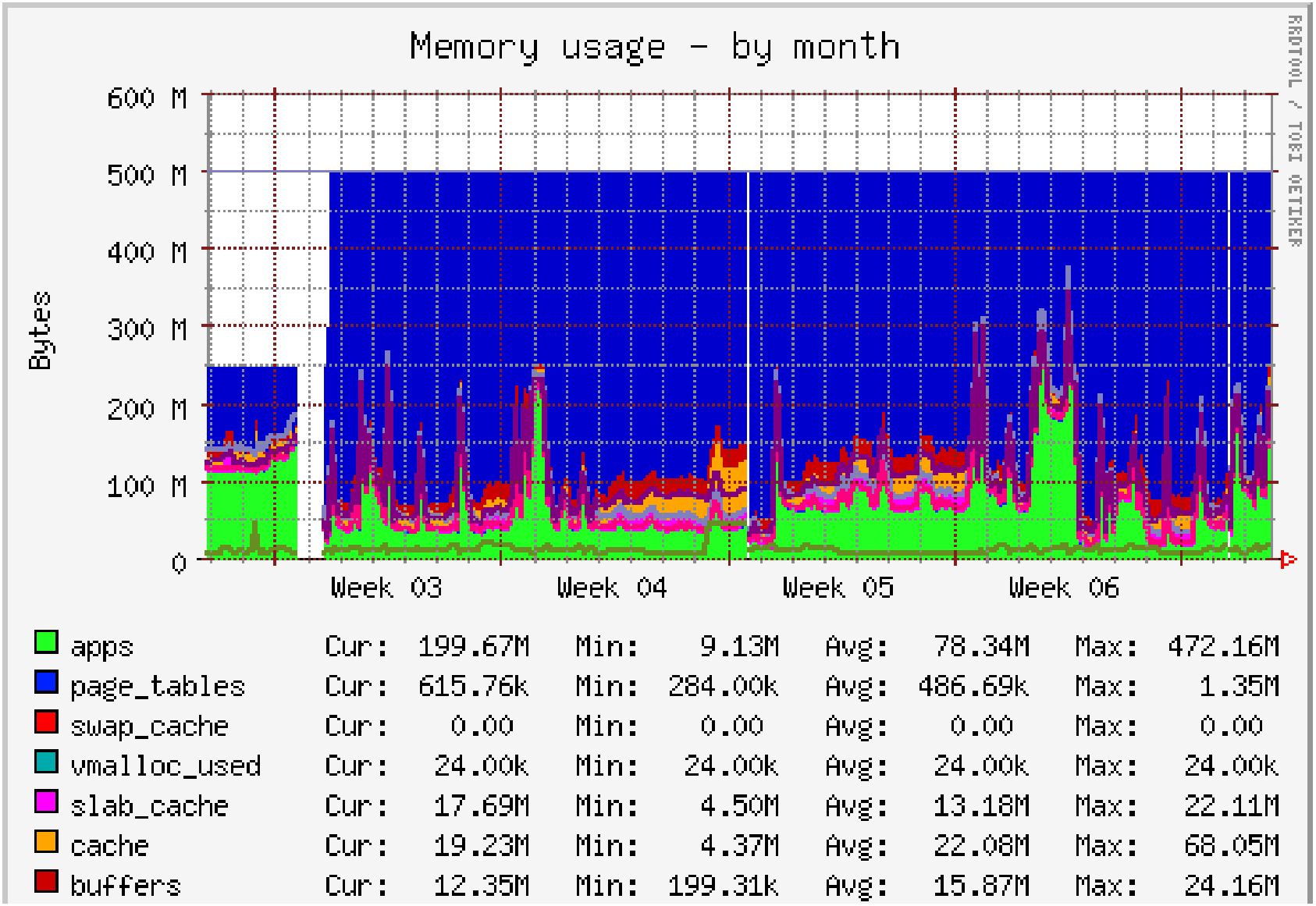
webes felület

- a definiált fa szerkezet, azon belül host, sorban a kategóriák
- `warning` szintű paraméter kategóriája sárga (pl. df 92%)
- `critical` szintű paraméter kategóriája piros (pl df 98%)

- **ih** :: [day week month year]
  - **mx1.gau.hu** :: [Other]
  - **nmc.gau.hu** :: [Disk Exim Mysql Network Other Postfix Processes System]
  - **noc.gau.hu** :: [Disk Network Other Postfix Processes System]
  - **pityu0.ih.szie.hu** :: [Disk Network Processes Sensors System]
  - **pityu1.ih.szie.hu** :: [Apache Disk Mysql Network Processes Sensors System]
  - **pityu5.ih.szie.hu** :: [Disk Network Processes Sensors System]
  - **pityu6.ih.szie.hu** :: [Disk Network Processes Sensors System Xen]
  - **rserver.gau.hu** :: [Disk Network Postfix Processes System]
  - **sziszifusz.szie.hu** :: [Apache Disk Network Processes System]

- **net** :: [day week month year]
  - **fw-kva.szie.hu** :: [Disk Network Processes System]
  - **fw-vti.szie.hu** :: [Disk Network Processes System]
  - **gate.gau.hu** :: [Disk Network Other Postfix Processes Sensors System]
  - **gw-diak.gau.hu** :: [Disk Network Processes System]

- **szolg** :: [day week month year]
  - **atlas.szie.hu** :: [Other]
  - **doktori.szie.hu** :: [Apache Disk Exim Network Postfix Processes System]


Memory usage - by month
RRDTOOL / TOBI OETIKER
Bytes
600 M
500 M
400 M
300 M
200 M
100 M
0
Week 03
Week 04
Week 05
Week 06
apps Cur: 199.67M Min: 9.13M Avg: 78.34M Max: 472.16M
page_tables Cur: 615.76k Min: 284.00k Avg: 486.69k Max: 1.35M
swap_cache Cur: 0.00 Min: 0.00 Avg: 0.00 Max: 0.00
vmalloc_used Cur: 24.00k Min: 24.00k Avg: 24.00k Max: 24.00k
slab_cache Cur: 17.69M Min: 4.50M Avg: 13.18M Max: 22.11M
cache Cur: 19.23M Min: 4.37M Avg: 22.08M Max: 68.05M
buffers Cur: 12.35M Min: 199.31k Avg: 15.87M Max: 24.16M

munin és nagios összekapcsolás

- ötlet: ha munin tud warning-ot, critical-t, üzenje is meg
- munin tud mail-t küldeni de üzengetni ott van a nagios
- kössük össze a kettőt
- megoldás: nagios nsca (Nagios Service Check Acceptor)
  `http://munin.projects.linpro.no/wiki/HowToContactNagios`

mi kell ehhez?

nagios :

- nagios.cfg:

```
command_file=/var/log/nagios/rw/nagios.cmd
log_passive_service_checks=0
accept_passive_service_checks=1
```

- checkcommands.cfg:

```
define command{
        command_name    check_dummy
        command_line    $USER1$/check_dummy $ARG1$
}
```

- services.cfg:

```
define service {
        use                             generic-service
        name                            passive-service
        active_checks_enabled           0
        passive_checks_enabled          1
        register                        0
        is_volatile                     1
        contact_groups                  server-admins
        notification_options            w,u,c,r
        check_command                   check_dummy!0
}
```

```
define service {
        use                             passive-service
        host_name                       gate
        service_description             disk
}
```

nsca szerver :

- /etc/nsca.cfg:

```
server_address=127.0.0.1
allowed_hosts=127.0.0.1
nsca_user=nagios
command_file=/var/log/nagios/rw/nagios.cmd
decryption_method=1
password=titok
```

- /etc/hosts.allow:

```
nsca:127.0.0.1
```

nsca kliens :

- `/etc/send_nsca.cfg`:

  ```
  encryption_method=1
  password=titok
  ```

- teszt: `echo -e "foo.example.com\ttest\t0\t0" | /usr/sbin/send_nsca -H localhost -c /etc/send_nsca.cfg`
- ellenőrzés 1: ha a `nagios.cmd` nem jó

  ```
  cat /var/run/nagios/nsca.dump:
  [1171915138] PROCESS_SERVICE_CHECK_RESULT;foo.example.com;test;0;0
  ```

- ellenőrzés 2: ha eddig minden OK:

  ```
  grep foo.example.com /var/log/nagios/nagios.log
  [1171915382] Warning:  Message queue contained results for service 'tes
  host 'foo.example.com'.  The service could not be found!
  ```

munin :

- munin-ban jeleneleg csak OK, WARNING, CRITICAL van, de nincs UNKNOW (lesz)
- `munin-limits` rendszeresen fut cron-ból
- sajnos a nagios service elnevezés kötött, ezért trükközni kell

- `/etc/munin/munin.conf` vonatkozó részlet:

```
contacts nagios
contact.nagios.command /usr/sbin/send_nsca -H localhost \
                                          -c /etc/send_nsca.cfg

[net;gate.gau.hu]
    contacts nagios
    address 192.188.242.65
    use_node_name yes
    notify_alias gate
# pre 1.3.3rc
    df.graph_title disk
# post 1.3.3rc
#    df.notify_alias disk
```

- még pár apróság:

```
# chgrp nagios /etc/send_nsca.cfg
# adduser  munin nagios
```

NYILVÁNTARTÁSOK

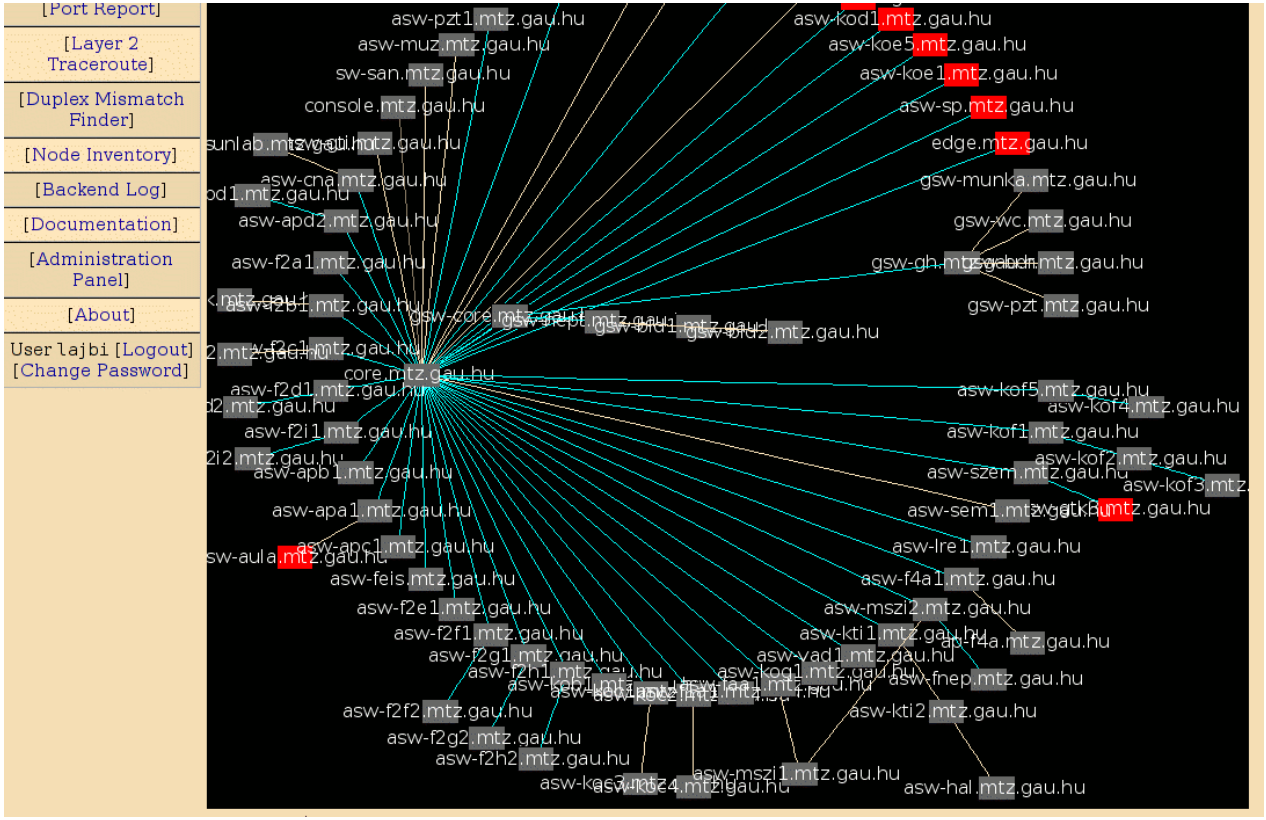
arpwatch

- kis hálózatokban mac cím és ip összeszedés
- változásokról emailben csacsog
- régebben csak promisc mód, most már SNMP lekérdezés is van

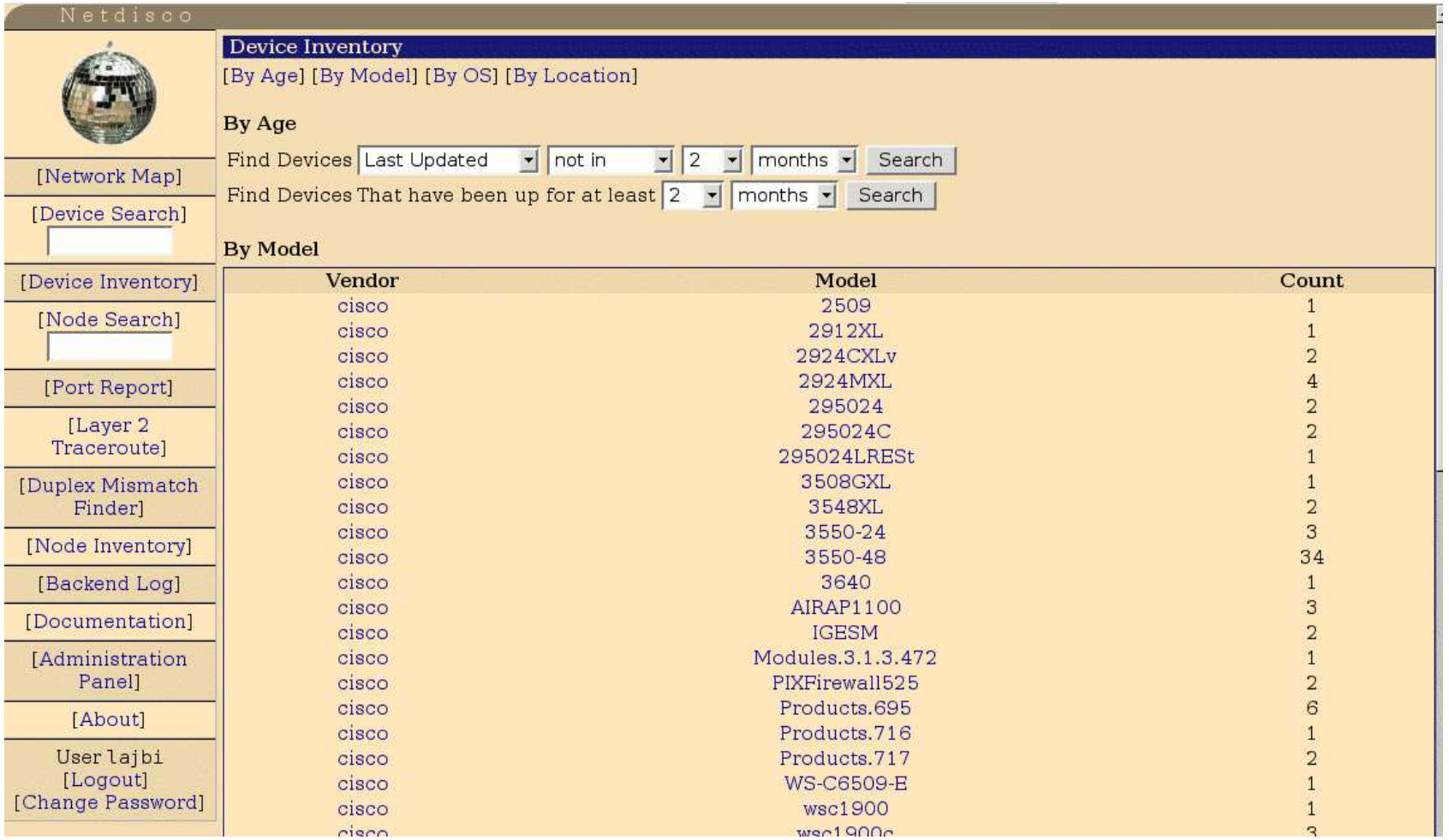
netdisco

– cron-ból futó feladatok, PostgreSQL adatbázis, webes felület

– SNMP és CDP segítségével térképezi fel a hálózatot. Ha nincs CDP, topologia kézzel megadható



– device, node inventory készül



Vendor	Model	Count
cisco	2509	1
cisco	2912XL	1
cisco	2924CXLv	2
cisco	2924MXL	4
cisco	295024	2
cisco	295024C	2
cisco	295024LRESt	1
cisco	3508GXL	1
cisco	3548XL	2
cisco	3550-24	3
cisco	3550-48	34
cisco	3640	1
cisco	AIRAP1100	3
cisco	IGESM	2
cisco	Modules.3.1.3.472	1
cisco	PIXFirewall525	2
cisco	Products.695	6
cisco	Products.716	1
cisco	Products.717	2
cisco	WS-C6509-E	1
cisco	wsc1900	1
cisco	wsc1900c	3

- archivált történelmi adatok (pl mac-hez ip cimek)
- néhány egyszerűbb ellenőrzés
- L2 traceroute mac, ip cím, hostnév vagy netbios név alapján


Netdisco
[Network Map]
[Device Search]
[Device Inventory]
[Node Search]
[Port Report]
[Layer 2 Traceroute]
[Duplex Mismatch Finder]
[Node Inventory]
[Backend Log]
[Documentation]
L2 Trace Route
Route
noc.gau.hu --> sun-lab.szie.hu
Port In
Device
Port Out
1. noc.gau.hu
2. [GigabitEthernet2/14] core.mtz.gau.hu [GigabitEthernet4/14]
3. [GigabitEthernet0/1] asw-cna.mtz.gau.hu [FastEthernet0/32]
4. sun-lab
From: noc.gau.hu
To: sun-lab.szie.hu
Trace Route
[Clear]
Hints
• L2 Traceroute only finds a Possible route through the network, using
path of packets may well be very different .
• Enter the MAC Address, IP Address or Hostname of a node or device
• For segments of the network missing topology info, no path may be f
Info in [Device Search].

Helyi fejlesztések

gödöllői HAT

- HAT - hálózati adattár
- kollégiumban havi befizetések, kábel id-k és switchlábak nyilvántartása
- főbb funkciók:
  - igény felvitel
  - befizetés - ip cim osztás
  - bekötendők listája
  - bekötés
  - lekérdezések
- feladtuk, nem fejlesztjük tovább

Psadmin

- Port Security Administrator, DUF-on Kiss András, később Gede Zoltán
- fő feladat a kollégiumi szobák aktív portjainak kiosztása, kezelése
- egyre bővülő feladatkör
  - https, mysql, Cisco, HP, LDAP
  - regisztrációs interface
  - nem a user adja meg az adatokat (pl mac cím)
  - fejlett jogosultság kezelés, pl kollégium épület felelős, oktató tanterem lekapcsolás
- bővebben:
  `http://makacs.duf.hu/~gzoli/vedes/gede_zoltan_dcz1ts_20070122.ppt`

AMIRŐL NEM VOLT SZÓ

cacti : `http://cacti.net/`

jffnms : `http://www.jffnms.org/`

zenoss : `http://www.zenoss.com/`

ÖSSZEFOGLALÁS

http://www.nagios.org/

http://cricket.sourceforge.net/

http://munin.projects.linpro.no/

http://netdisco.org/

http://www.splintered.net/sw/flow-tools/

http://www.freeradius.org/

http://packages.debian.org/stable/net/tac-plus

http://zeus.gau.hu/~lajbi/ipszilon_noc.pdf