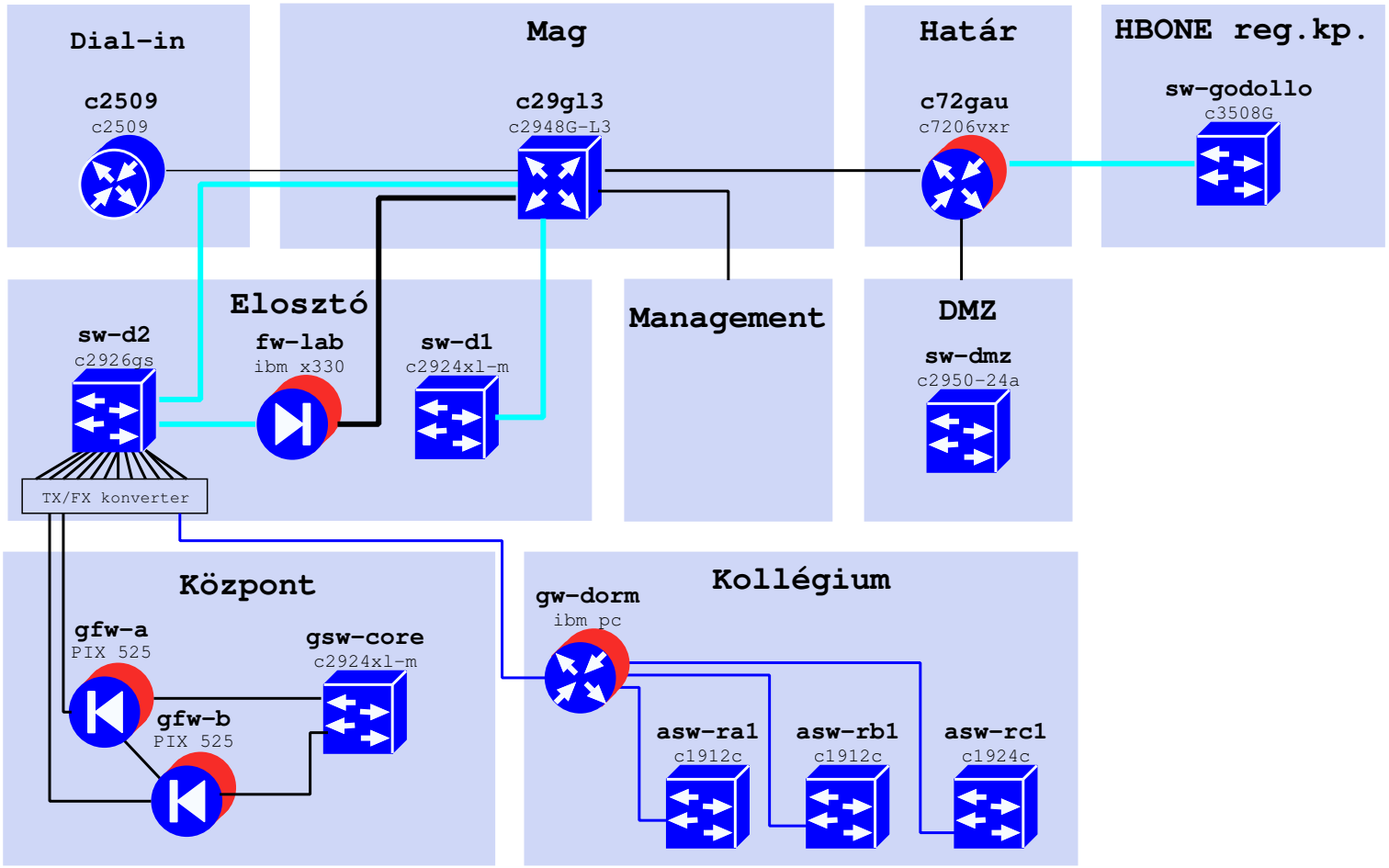
Egy közepes méretű egyetemi hálózat üzemeltetési tapasztalata

Lajber Zoltán
lajbi@zeus.gau.hu
Szent István Egyetem Informatikai Hivatal

- Gödöllői hálozat ismertetése
- Felügyeleti megoldások
- Üzemeltetési tapasztalatok
- Fejlesztési javaslatok

A gödöllői hálózat felépítése



40 $\Rightarrow$15 VLAN, eltérő fizikai és logikai architectura, kb 40 aktív elem

Felügyeleti megoldások

Management hálózat:

- Management gépeknet külön subnet, extra csomagszűrés, emelt szintű host biztonság
- Aktív elemek VLAN 1, 192.168.x.0/24, erős csomagszűrés
- VLAN 1 soha nincs access porton

AAA - TACACS+: aktív elemek eléréséhez központi TACACS+ szerveren authentikáció és parancs logolás

Syslog: routerek, fontosabb switchek központi syslog

Monitorozás: helyi NetSaint, regionális központ HP OpenView

Terhelés figyelés: mrtg/rrdtool

Forgalom mérés

Cisco Netflow: routerről heti 1GB.

Gyűjtés, alap feldolgozás: flow-tools, awk

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

Forgalmi statisztikák: postgres adatbázisban, gépenként napi bontásban

Naponta kétszer végrehajtandó feladatok:

- flow-print (4-12 milió sor), agreg.awk (40 - 150 ezer sor): 1 - 3 perc
- postgres copy ideiglenes táblába, feldolgozás: 5 - 10 másodperc
- forgalmi adatok maximális táblamérete: 12 db C osztályú cím, 365 nap $\Rightarrow$1 milió sor körül évente

Üzemeltetési tapasztalatok

Ethernet autonegotitation probléma

- újabb eszközök (2950, 2948G-L3) máskép viselkednek, mint a régiek (1924, 2924XL)
- mindkét fél auto duplex és speed esetén ”duplex mismatch”
- jellegzetes tünet: egyik irányban 5 - 8000 kbyte/sec, másik irányban 50-80 kbyte-sec
- ellenőrzés: egyik oldalon `late collisions`, másik oldalon `CRC errors`

TACACS+ probléma

- tünet: ha catalyst 19xx és a TACACS+ szerver között megszakad, majd helyreáll a kapcsolat, akkor a switch TACACS-a timeout-ol...
- megoldás: switch console, upgrade 9.xx -re

VLAN Domain probléma

- tünet: nagy leállás után VLAN-ok ”elvesznek”
- ok: c19xx, cat8xx: VTP server módban (mivel nincs client, csak transparent mód), a leszakadó és visszatérő részben a VTP domain ugyanaz, verziószám pedig nagyobb...
- megoldás: c19xx sw upgrade 9.xx-re (cat1900EN.9.00.04.bin), 2 elosztó régeg beli switch VTP server mód, többi switch VTP client mód.

DOS támadások

- előzmény: WAN csatlakozás sebessége 155Mbps-ről 1Gbps-re nőtt.
- hatás: icmp, majd SYN flood-ok $\Rightarrow$c7206vxr, NPE400 nem birta, heti 1-2 crash
- megoldás: router gondos beállítása

Router beállítások

A router: c7206vxr, NPE-400, GE+E I/O

Biztonság:

Csomagszűrés : RFC 1918, egyéb szokásos szűrések, 3 interface-en összesen kb 300 sor ACL alap + kivételek, ideiglenes szűrések

Router biztonság: felesleges szolgáltatások letiltása (http, small services), management interface ACL

spoof protection: `ip verify unicast reverse-path`

Tejesítmény:

Optmális switching: `ip cef`

TurboACL : `access-list compiled`

Hozzáférés biztosítása: `scheduler allocate 3000 1000`

BGP, IGP stabilizálás flood alatt: `spd enable`

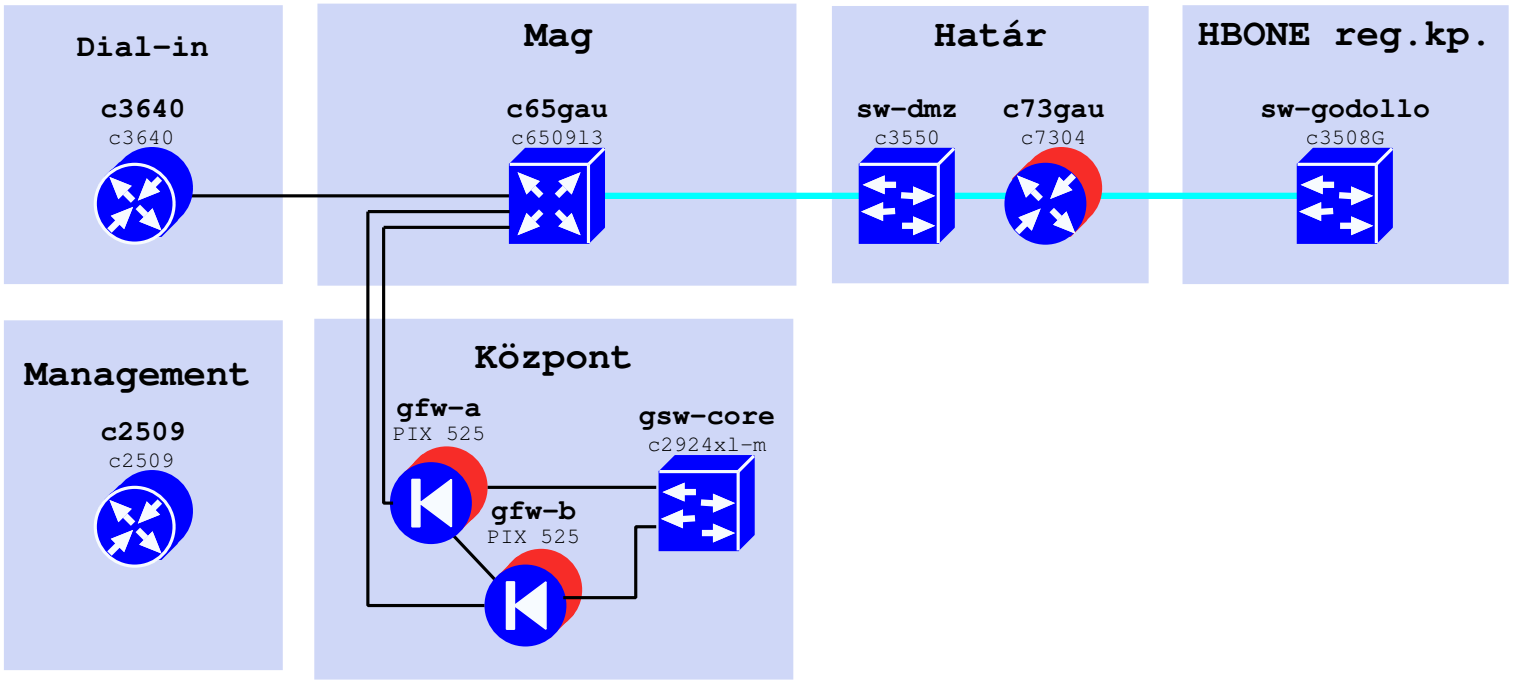
TCP SYN flood védelem:

```
ip tcp intercept list 102
ip tcp intercept max-incomplete low 5000
ip tcp intercept max-incomplete high 9000
ip tcp intercept one-minute low 2000
ip tcp intercept one-minute high 4000

access-list 102 permit tcp any 192.188.244.0 0.0.0.255
access-list 102 permit tcp any ...

c72gau#show tcp intercept statistics
Intercepting new connections using access-list 102
527 incomplete, 4210 established connections (total 4737)
1522 connection requests per minute
```

ICMP rate limit: CAR

```
access-list 101 permit icmp any any
interface gigabitEthernet 0/0
 rate-limit input access-group 101 800000 16000 24000
  conform-action transmit exceed-action drop

c72gau#show interfaces gigabitEthernet 0/0 rate-limit
GigabitEthernet0/0 OUTSIDE
  Input
    matches: access-group 101
      params:  800000 bps, 16000 limit, 24000 extended limit
      conformed 688227 packets, 61892416 bytes; action: transmit
      exceeded 502 packets, 66692 bytes; action: drop
      last packet: 332ms ago, current burst: 0 bytes
      last cleared 2d09h ago, conformed 2000 bps, exceeded 0 bps
```

Fejlesztési tervek



Gerinc: core, distribution, access ⇒core, access: teljesítmény, portsűrűség: c6509 L3, switch fabrick enabled

Határ router: teljesítmény: c2948G-L3, c4908G-L3, c7304, c75xx, ...

tulajdonságok: c7304, c75xx, ...

Az előadás letölthető:

http://zeus.gau.hu/~lajbi/nws2k2.pdf

http://zeus.gau.hu/~lajbi/nws2k2.tgz