

# MYNTCD

## Hálózati forgalom mérés a Georgikon Karon

Pintér Tamás

[pinter@georgikon.hu](mailto:pinter@georgikon.hu), [york@openproject.hu](mailto:york@openproject.hu)

VE Georgikon Mezőgazdaságtudományi Kar

Keszthely

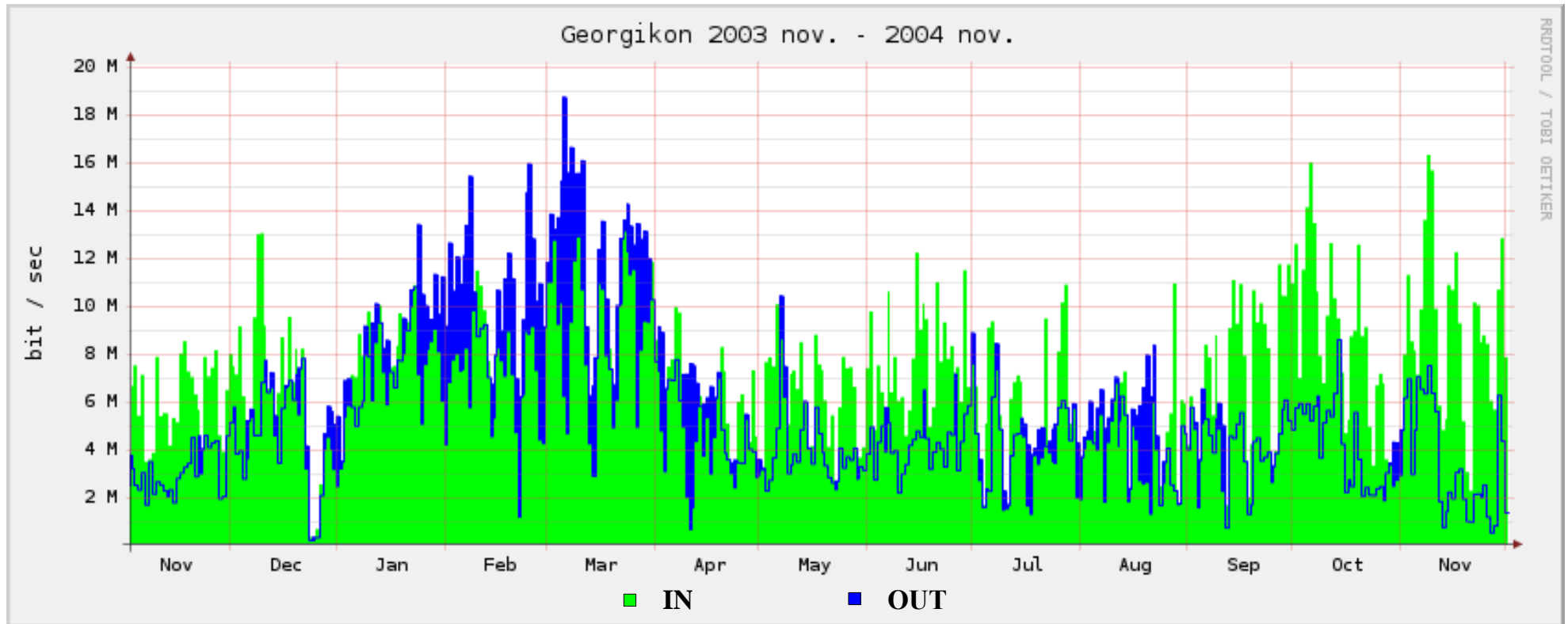


## Tartalom:

- Bevezetés
  - ◆ Probléma
  - ◆ Megoldás, lehetséges alternatívák
  - ◆ Miért saját fejlesztés
- Myntcd bemutatása
- Elért eredmények
- Myntcd jövője



# PROBLÉMA





## Forgalmérés:

- Pécsi NWS - Nagy Elemér Károly előadása
- Cisco netflow
- Net-Acct (<http://exorsus.net/project/net-acct>)
- Netacct-mysql (<http://netacct-mysql.gabrovo.com/>)

**Saját fejlesztés Myntcd**



## **Myntcd felépítése:**

- Myntcd daemon
- Időzített szkriptek (cron)
- Web oldalak
- Segéd szkriptek

## **Szoftveres környezet:**

- PHP4, Pear DB
- MySQL (PostgreSQL támogatás folyamatban)
- RRDtool



## Myntcd daemon:

- C nyelven készült
- Hálózati kártyát promiscuous módban olvassa
- Libpcap (v0.7, v0.8)
- Megadhatók IP cím(ek)/tartomány(ok)
- Megkülönböztetett forgalom: TCP/UDP/ICMP/Egyéb
- Időzített mentés
- Támogatott rendszerek: Linux, FreeBSD (NetBSD, OpenBSD)



## Időzített szkriptek (cron):

- PHP nyelven készültek
- myntc.php
  - ◆ adatbázisba tölti a daemon kimenetét
  - ◆ 1 és 24 óránként mozgatja az adatokat
  - ◆ Statikus HTML oldalak és képek generálása
- blacklist.php (jelenleg csak cisco-ra)
  - ◆ black/whitelist alapján generál és aktivál szűrőlistát



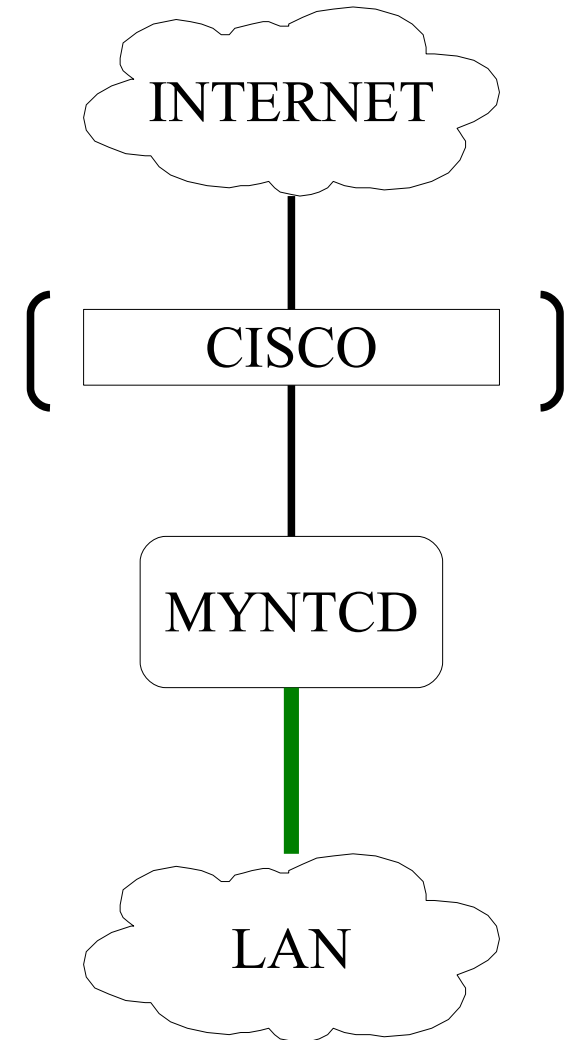
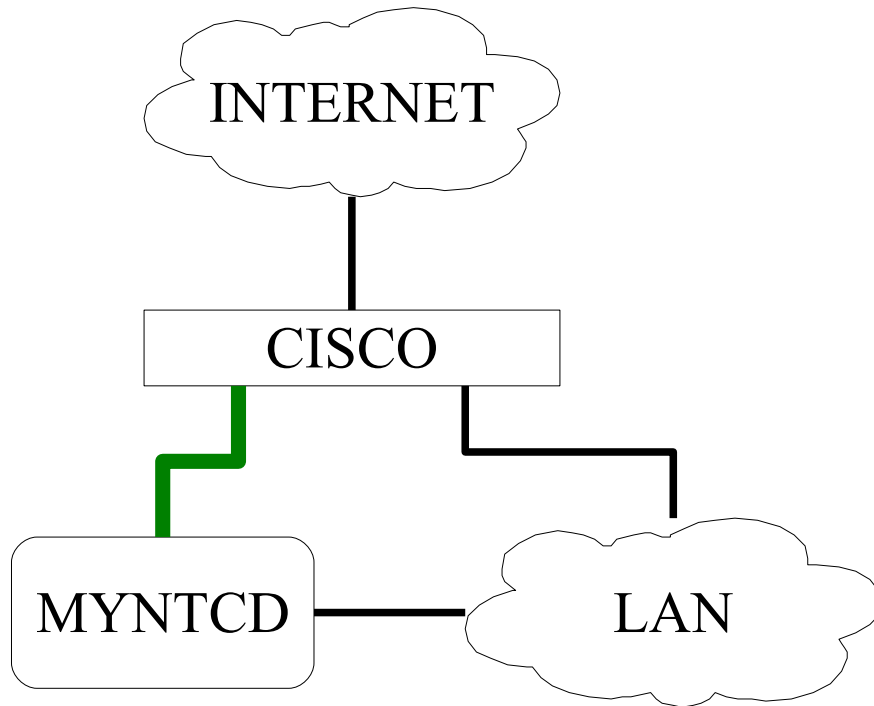
## Web oldalak:

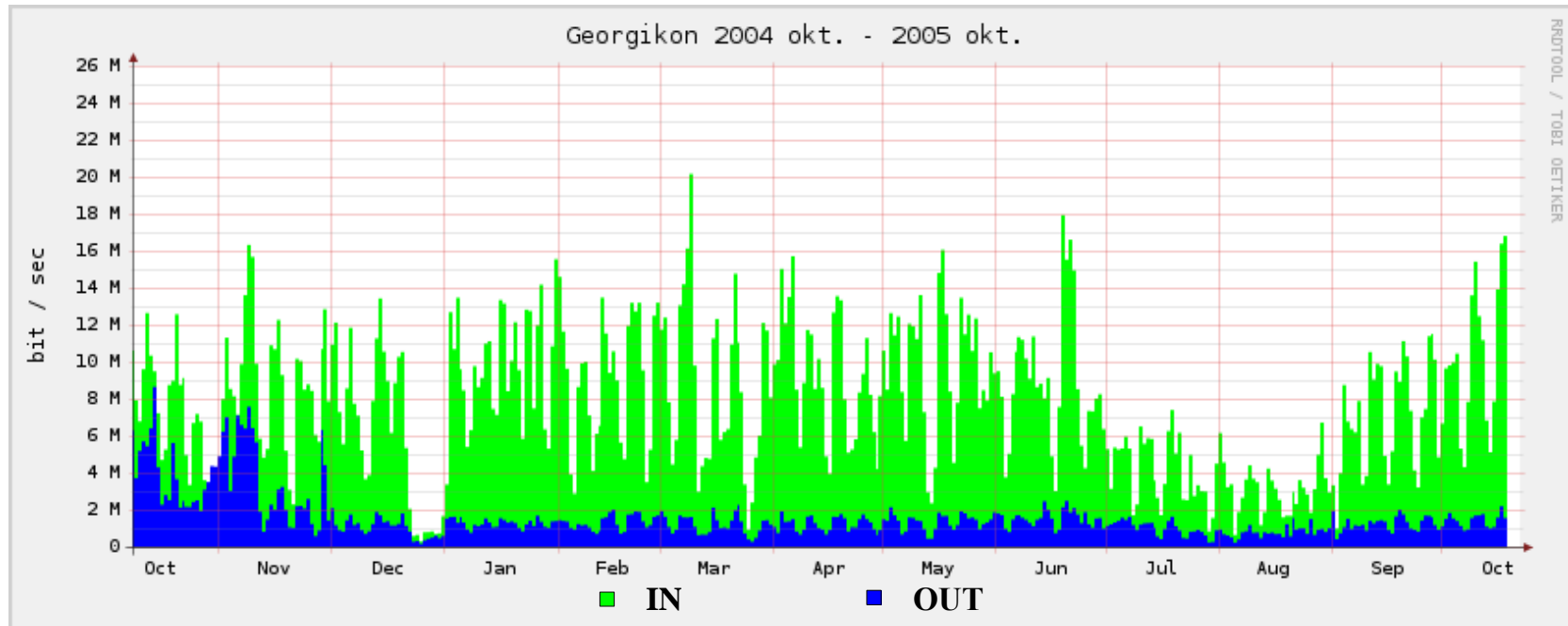
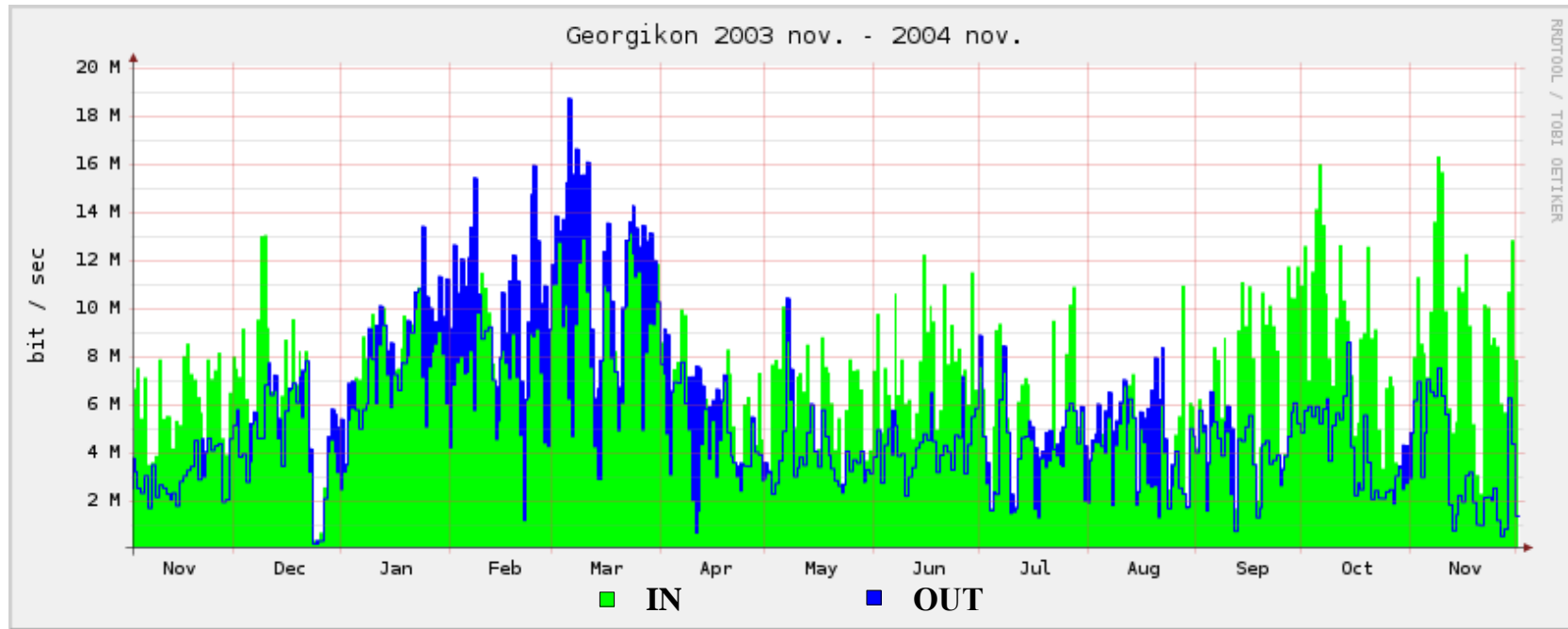
- PHP nyelven készültek
- Aktuális óra, nap, hónap forgalma látható
- 24-es maszk szerinti csoportosítás
- IP címenként forgalmi adatok (MB és csomag szám)
- IP címenként grafikonok (napi, heti, havi, évi)
- Top listák (ki-, bemenő és teljes forgalom szerint)
- Keresési lehetőség





## Mérés módja







## Várható fejlesztések:

- IPV6 támogatás
- Több nyelv támogatása
- Áttekinthetőbb és információ gazdagabb webes felület
- PostgreSQL támogatás
- Dokumentáció



## Fejlesztők:

- Bognár Péter ([stx@gentoo.hu](mailto:stx@gentoo.hu))
- Pécsi Sándor ([xea@gentoo.hu](mailto:xea@gentoo.hu))
- Pintér Tamás ([york@openproject.hu](mailto:york@openproject.hu))



# KÖSZÖNÖM A FIGYELMET KÉRDÉSEK?

Pintér Tamás

[pinter@georgikon.hu](mailto:pinter@georgikon.hu), [york@openproject.hu](mailto:york@openproject.hu)

<http://openproject.hu/myntcd>