MYNTCD
Hálózati forgalom mérés a Georgikon Karon

Pintér Tamás

pinter@georgikon.hu, york@openproject.hu

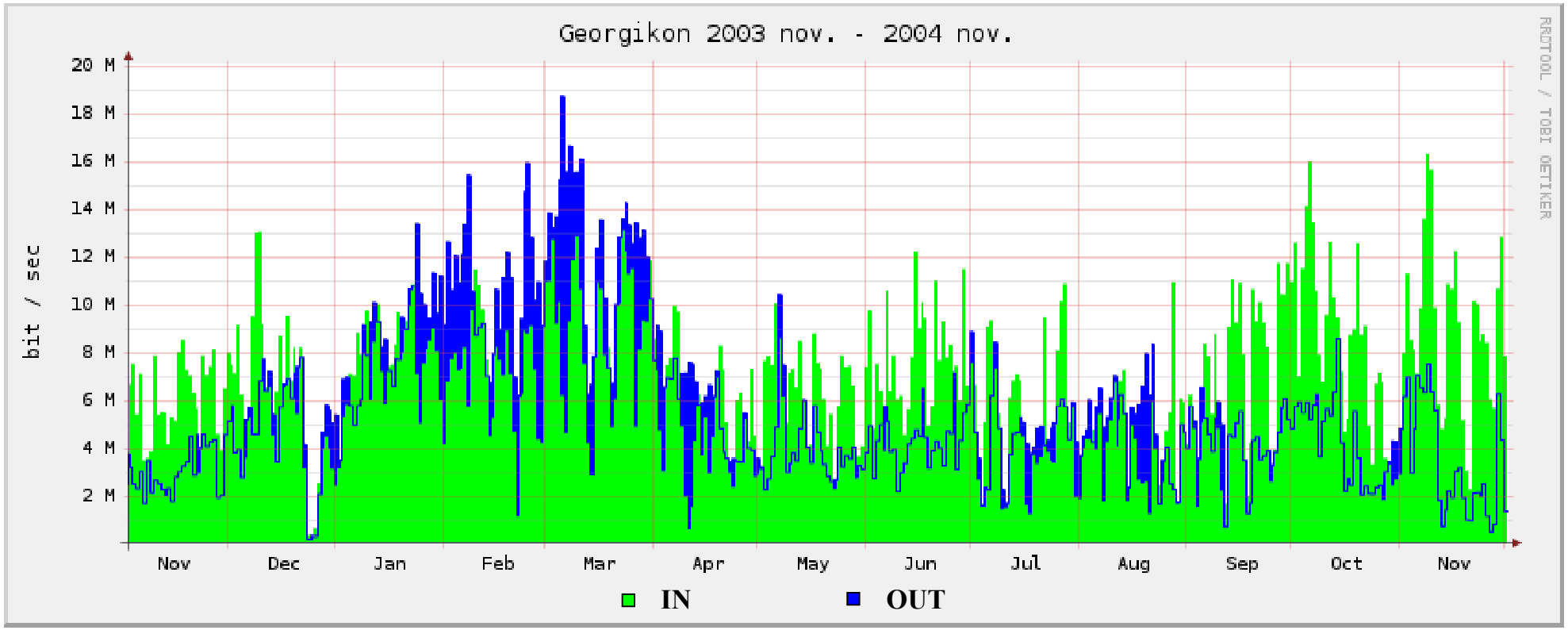
PE Georgikon Mezőgazdaságtudományi Kar

Keszthely

Tartalom:

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

PROBLÉMA


Georgikon 2003 nov. - 2004 nov.
bit / sec
20 M
18 M
16 M
14 M
12 M
10 M
8 M
6 M
4 M
2 M
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
IN
OUT
RRDTOOL / TOBI OETIKER

Forgalommérés:

- 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 felület (drupal modul)

Szoftveres környezet:

- Webszerver, PHP4, Pear DB, Drupal 4.7b4
- MySQL (PostgreSQL támogatás folyamatban)
- RRDtool

Myntcd daemon:

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

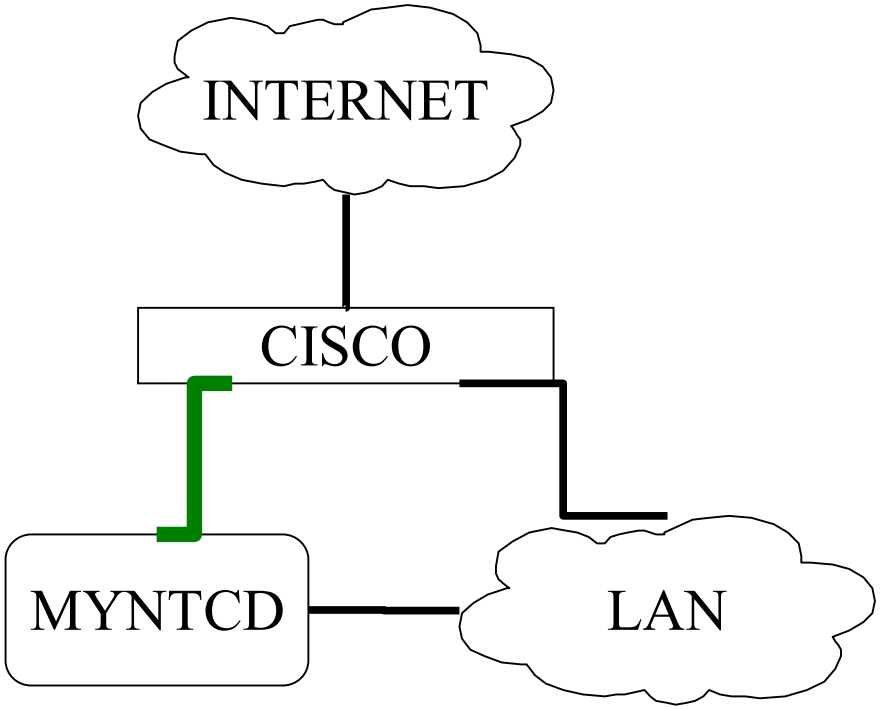
Időzített szkriptek (cron):

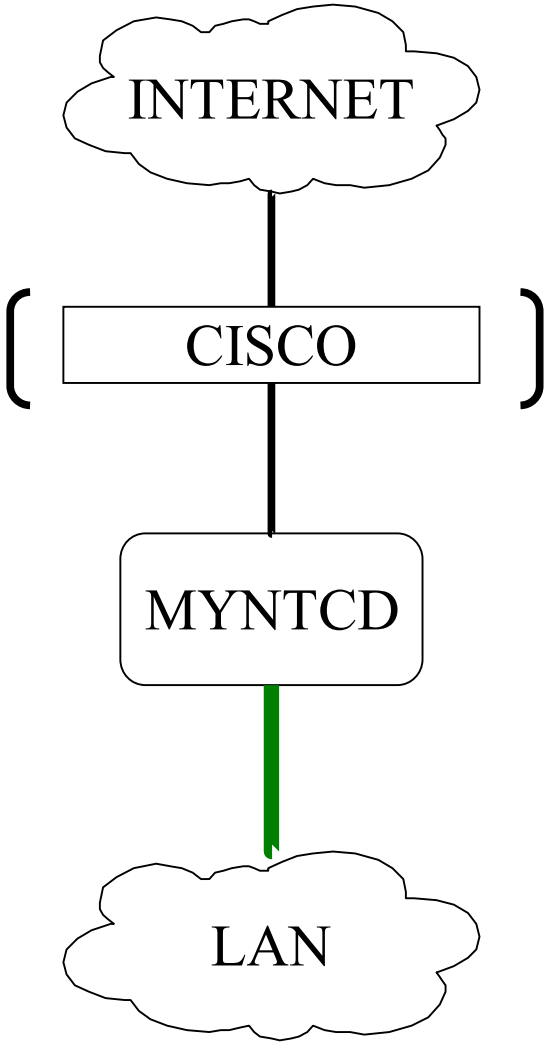
- PHP nyelven készültek
- myntc.php
  - adatbázisba tölti a daemon kimenetét
  - 24 óránként mozgatja az adatokat
- blacklist.php (jelenleg csak cisco-ra)
  - black/whitelist alapján generál és aktivál szűrőlistát

Web felület:

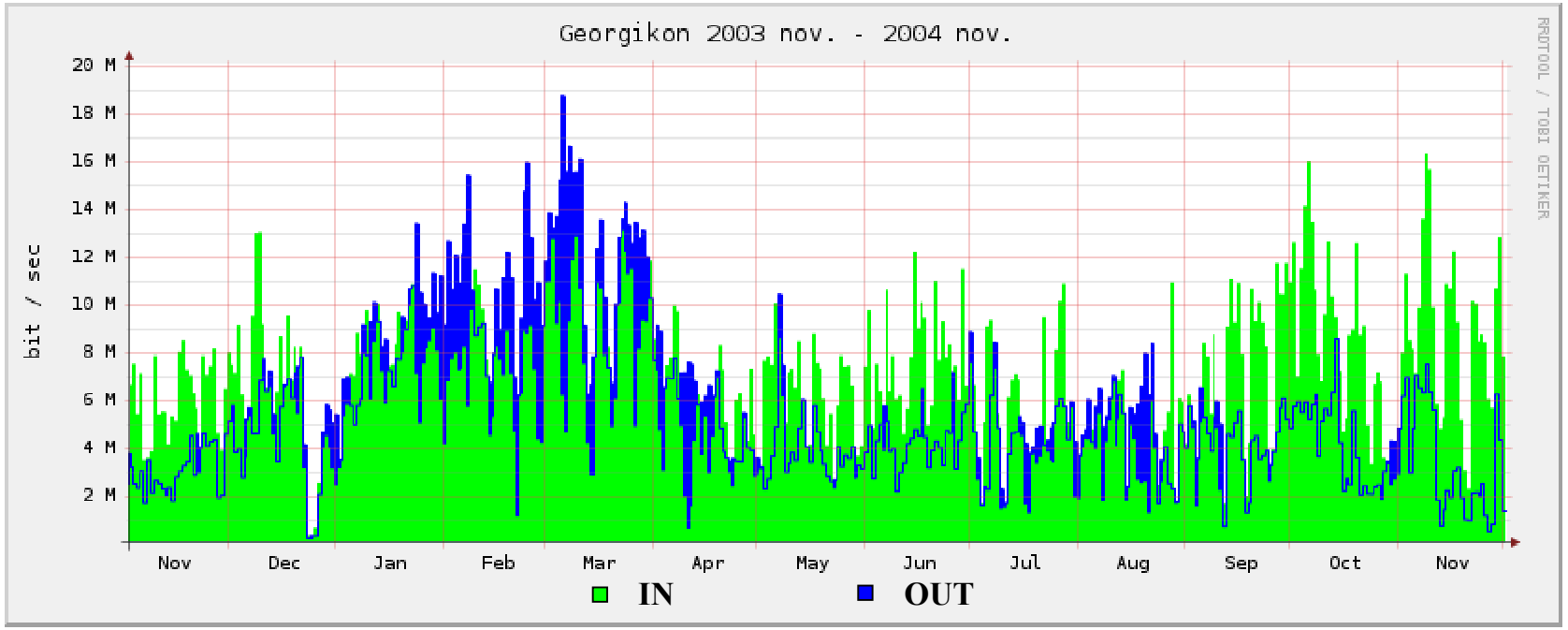
- PHP nyelven készült drupal modul
- Aktuális óra, nap, hónap forgalma látható
- 24-es maszk szerinti csoportosítás
- IP címenként forgalmi adatok (MB és csomag szám)
- IP címenként grafikonok (napi, heti, havi, évi)
- Top listák (ki-, bemenő és teljes forgalom szerint)
- Keresési lehetőség
- Saját adatok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

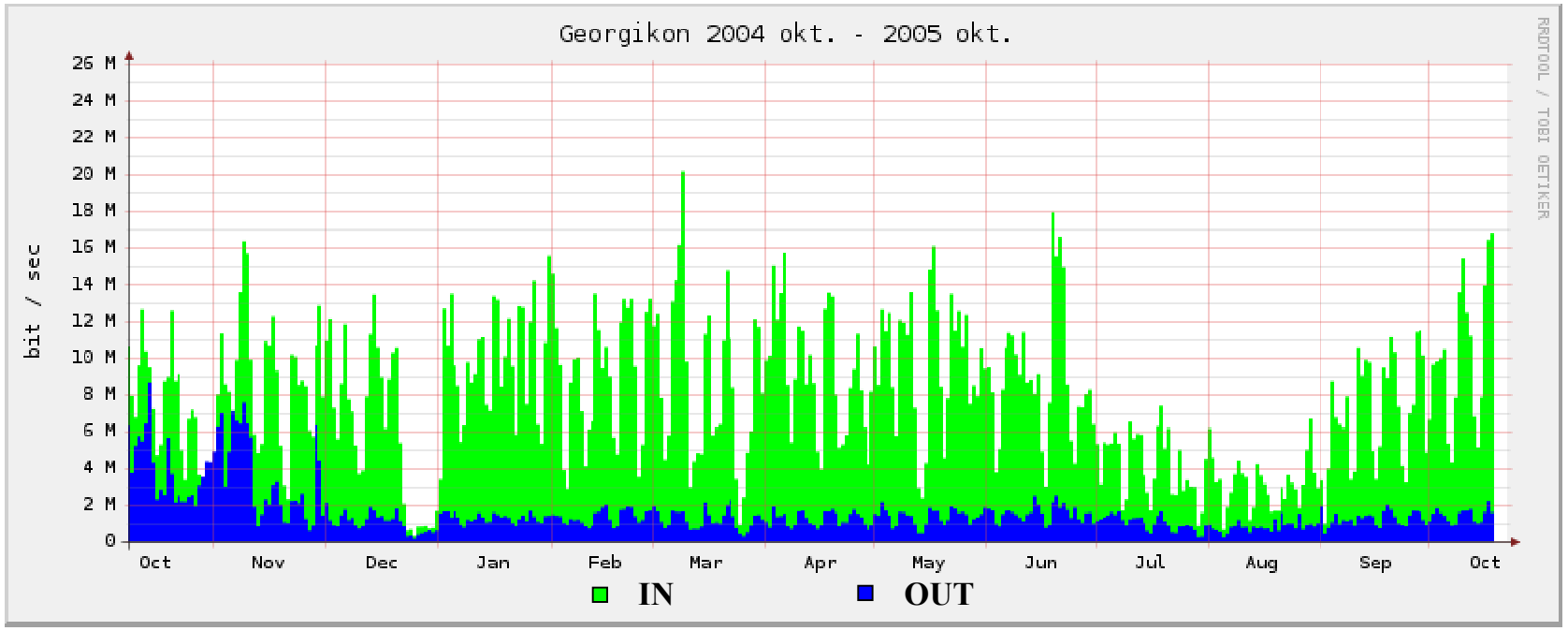
Mérés módja





Myntcd – Eredmények





Várható fejlesztések:

- IPV6 támogatás
- FreeBSD (NetBSD, OpenBSD), Solaris támogatás
- PostgreSQL támogatás
- Dokumentáció

Fejlesztők:

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

KÖSZÖNÖM A FIGYELMET

KÉRDÉSEK?

Pintér Tamás

pinter@georgikon.hu, york@openproject.hu

http://openproject.hu/myntcd