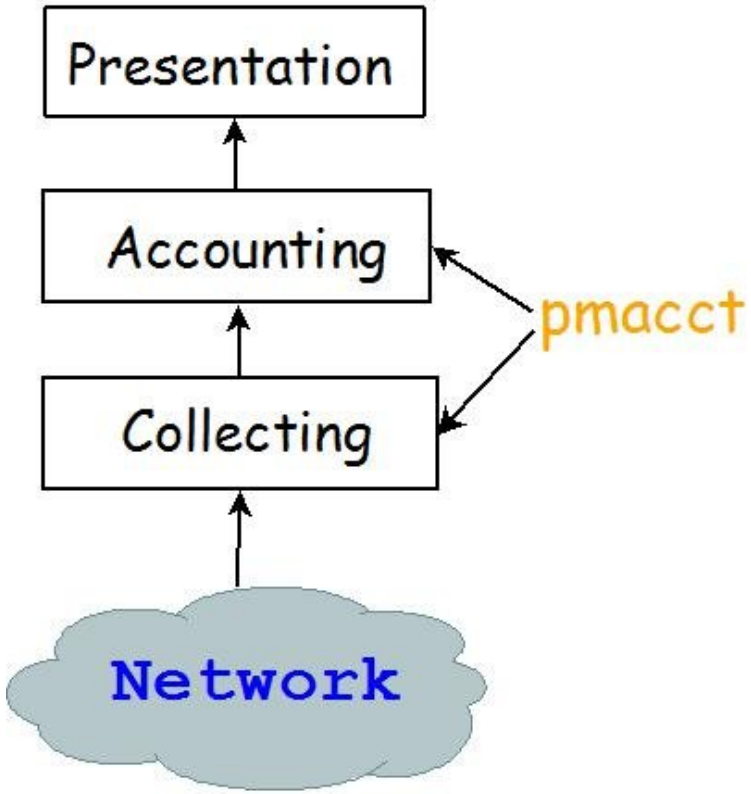
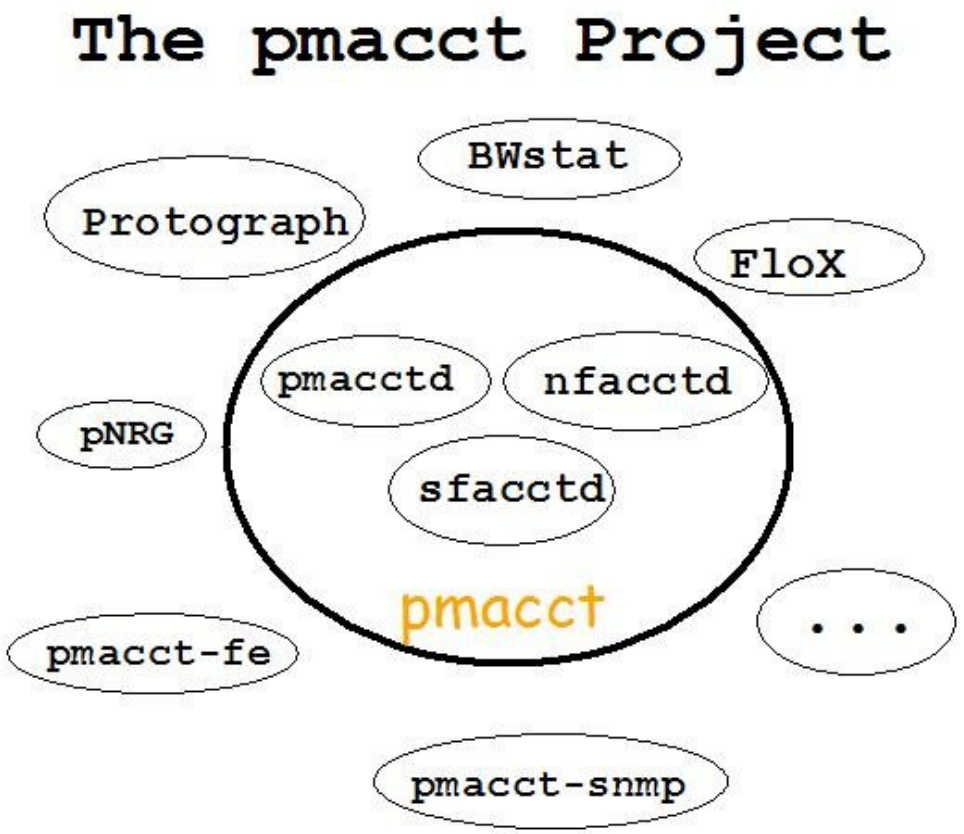
“IP accounting reloaded, the pmacct project: NetFlow, sFlow, SQL, RRD, stream classification and much more …”

Paolo Lucente *<paolo at pmacct dot net>*

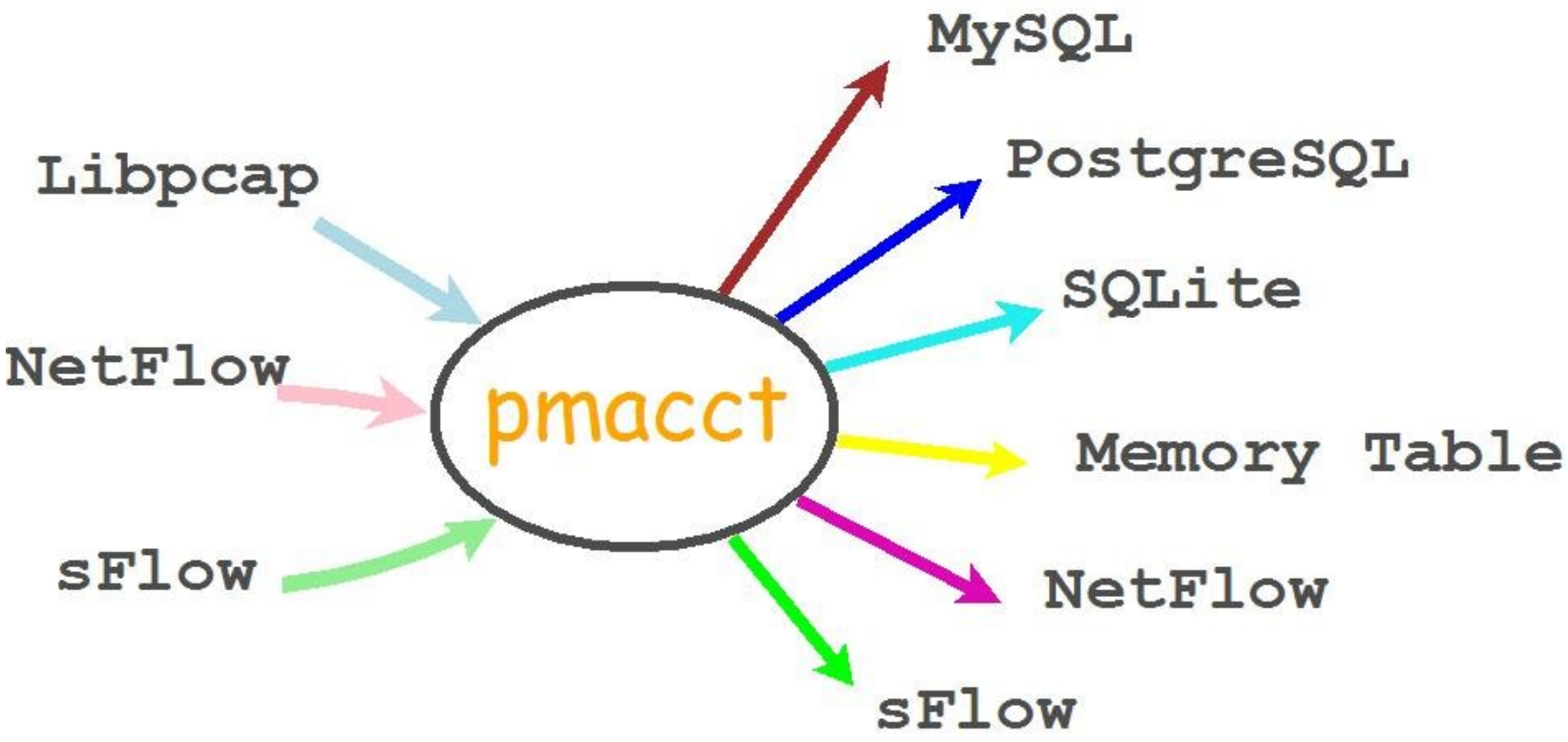
INEX members meeting, Dublin, 3rd May 2007

pmacct, what is this?





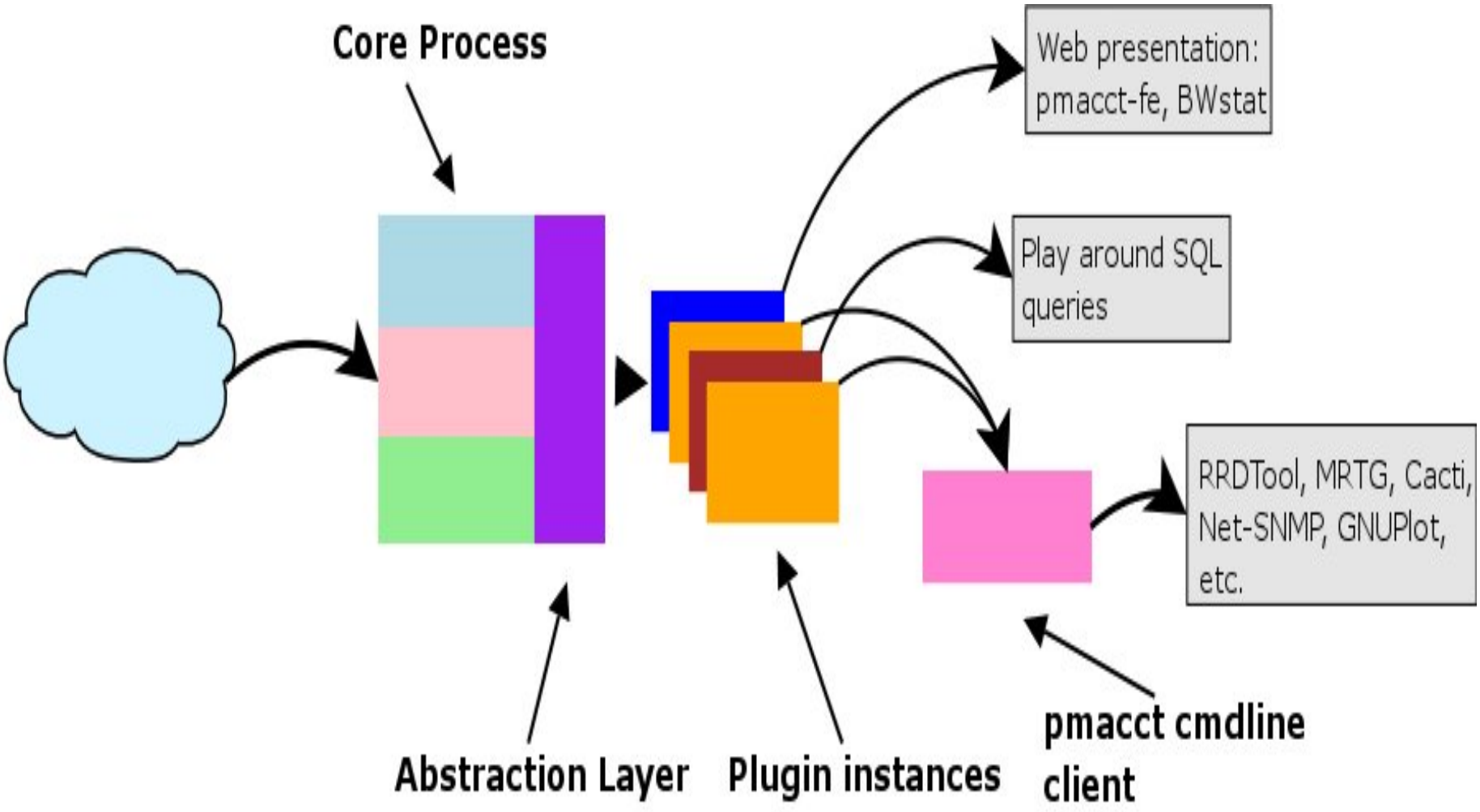
pmacct, what is this?(cont.d)



pmacct, what is this?(cont.d)

- ✓ Collects and accounts traffic data
- ✓ Stores data on either RDBMS or memory tables
- ✓ Aggregates data spatially and temporally
- ✓ Exports data to remote collectors through NetFlow and sFlow
- ✓ Can also convert data between the two protocols
- ▪ Doesn't store data in either proprietary format flat-files or RRDs (there is no motivation in duplicating others' work)
- ▪ Is not focused on offering captivating web presentation interfaces (projects topped over pmacct do)
- ▪ Is not intended to log singular packets/micro-flows/samples (tcpdump, flow-tools and sflowtool care)

A **modular** architecture: **single** collector, **multiple** views



pmacct, sample configuration

```
daemonize: true
nfacctd_ip: 83.147.xxx.yyy
nfacctd_port: 2100
plugins: memory[a], memory[b], pgsql[c]
!
! networks_file: /usr/local/etc/pmacct/AS-list.txt
! pre_tag_map: /usr/local/etc/pmacct/pretag.map
!
! “aggregate” supports: src_mac,dst_mac,vlan,src_host,dst_host,
! src_net,dst_net,src_as,dst_as,src_port,dst_port,tos,proto,
! sum_mac,sum_host,sum_net,sum_as,sum_port,tag,class,tcpflags
!
aggregate[a]: flows, dst_as
imt_path[a]: /tmp/a.pipe
!
aggregate[b]: flows, src_as
imt_path[b]: /tmp/b.pipe
!
aggregate[c]: sum_as
sql_table_version[c]: 6
sql_refresh_time[c]: 60
sql_history[c]: 10m
```

Let’s query the memory plugins

a) The –s : getting the full table

```
shell> pmacct –s –T bytes –p /tmp/a.pipe
DST_AS  PACKETS                 FLOWS                   BYTES
6461    830599267               71559981                273719551839
3257    157827450               12267805                55976570326
30834   29819152                2346227                 8620549465
5466    15741561                903261                  5776330161
6830    6236988                 175447                  4093125030
5462    9622433                 557196                  3896168294
22773   8206029                 755407                  3337029358
15169   14653753                957462                  2712205806
[ … continues … ]
```

b) The –M : getting a specific entry in a formatted way

```
shell> pmacct -c dst_as -M 5466 –p /tmp/b.pipe
SRC_AS  PACKETS                 FLOWS                   BYTES
5466    18282495                849972                  7601706332
```

c) The –N : getting the counters to inject traffic data into 3rd party tools.

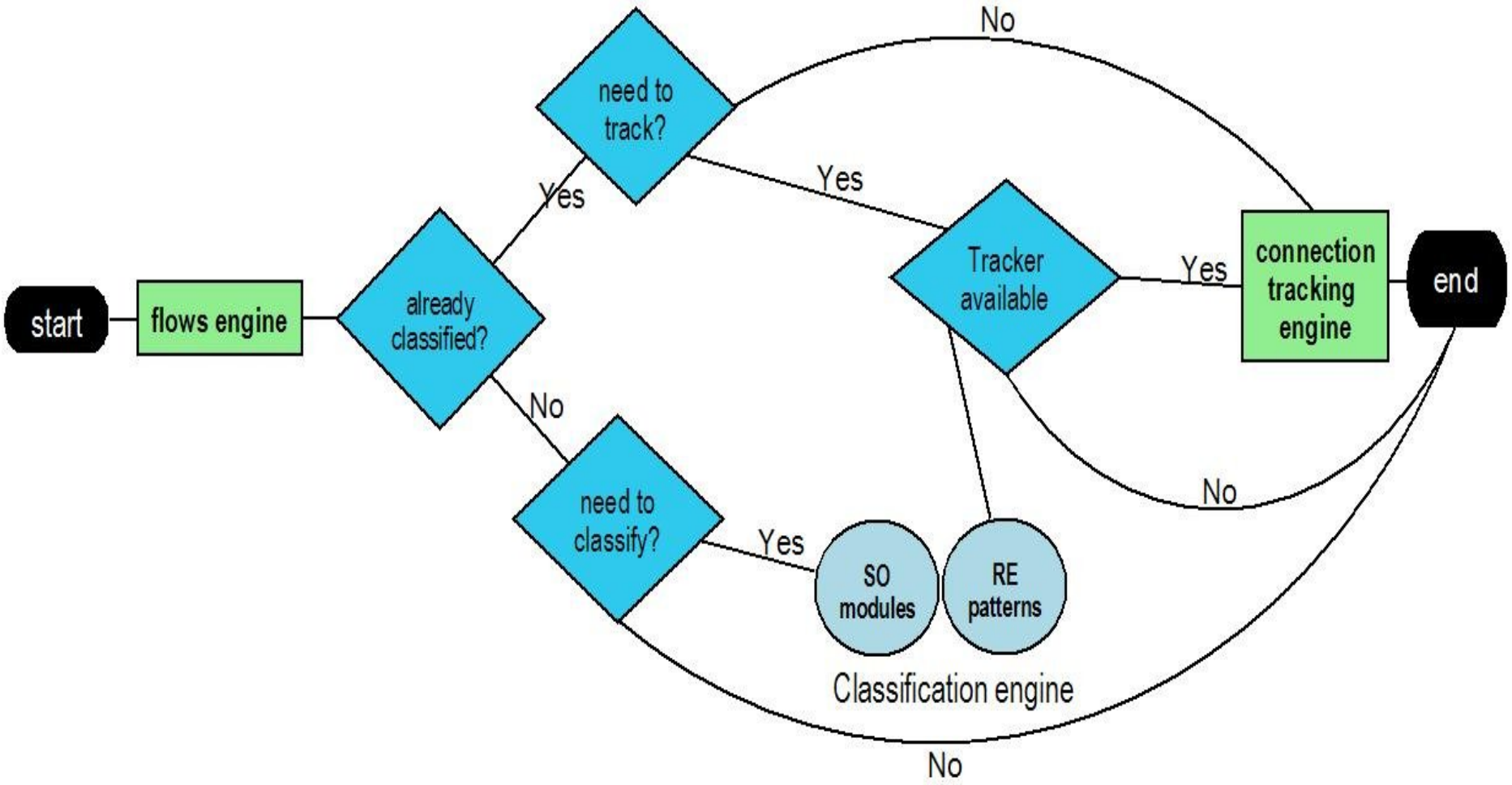
```
shell> pmacct -c dst_as -N 5466 –r –p /tmp/b.pipe
7601706332
```

And now, let’s query the SQL plugin

```
shell> psql -U pmacct -c "SELECT * FROM acct_v6 \
    WHERE as_src = 5466 \
    ORDER BY stamp_inserted DESC \
    LIMIT 10;"
```

```
 as_src | packets |  bytes   |   stamp_inserted    |    stamp_updated
--------+---------+----------+---------------------+---------------------
   5466 |   87720 | 36748765 | 2007-04-28 15:20:00 | 2007-04-28 15:31:01
   5466 |  196890 | 54533602 | 2007-04-28 15:10:00 | 2007-04-28 15:21:01
   5466 |   79842 | 33719090 | 2007-04-28 15:00:00 | 2007-04-28 15:11:01
   5466 |  112490 | 38097275 | 2007-04-28 14:50:00 | 2007-04-28 15:01:01
   5466 |   82304 | 29833249 | 2007-04-28 14:40:00 | 2007-04-28 14:51:01
   5466 |  107652 | 30395903 | 2007-04-28 14:30:00 | 2007-04-28 14:41:01
   5466 |   58509 | 17846999 | 2007-04-28 14:20:00 | 2007-04-28 14:31:02
   5466 |   72979 | 30813448 | 2007-04-28 14:10:00 | 2007-04-28 14:21:01
   5466 |  107350 | 35594580 | 2007-04-28 14:00:00 | 2007-04-28 14:11:01
   5466 |  126019 | 41857901 | 2007-04-28 13:50:00 | 2007-04-28 14:01:01
(10 rows)
```

pmacct, stream classification



Stream classification, RE vs SO

- ✓ **Regular Expression (RE) classifiers are easy to develop and suitable for text-based protocols.**

- ✓ **Shared Object (SO) classifiers are contextual, not limited to pattern catching and work just fine against binary payloads. BUT require careful development.**

Stream classification: results

```
shell> psql -U pmacct -c "SELECT class_id, packets, bytes, flows \
   FROM acct_v5 \
   ORDER BY bytes DESC \
   LIMIT 10;"

    class_id     |  packets  |    bytes     |  flows
-----------------+-----------+--------------+--------------
  nntp           | 533424546 | 534913922183 |       13480
  http           | 567179034 | 409970727835 |    22581928
  smtp           | 336913736 | 116445824169 |    17286471
  ssh            | 139908289 | 108291107166 |     1110903
  edonkey        | 167213900 | 107343376842 |     4501937
  ftp            | 197626712 |  97059417721 |      139749
  pop3           |  86367951 |  60221933775 |     1462006
  ssl            |  62489714 |  34784217799 |     2602435
  bittorrent     |  52031296 |  31068910458 |      414216
  rtsp           |  20099589 |   9595494054 |        3959
(10 rows)
```

pmacct: typical tasks

Generic:

- ✓ Graphing historical traffic trends
- ✓ Accounting, billing and security
- ✓ Triggering alerts/events for specific traffic-patterns
- ✓ Presentation of traffic data

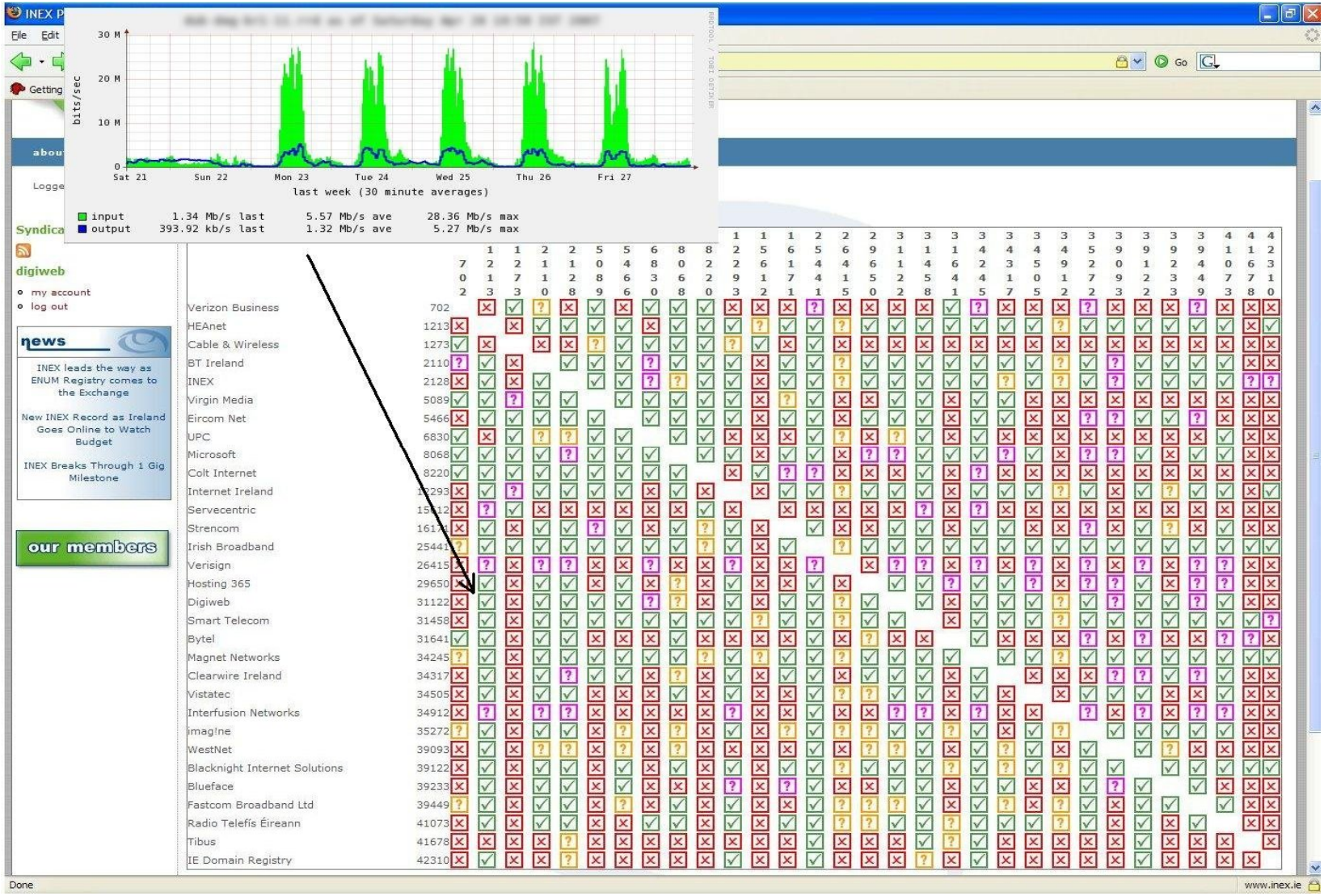
IXPs:

- ✓ Quantitative BGP peering matrices

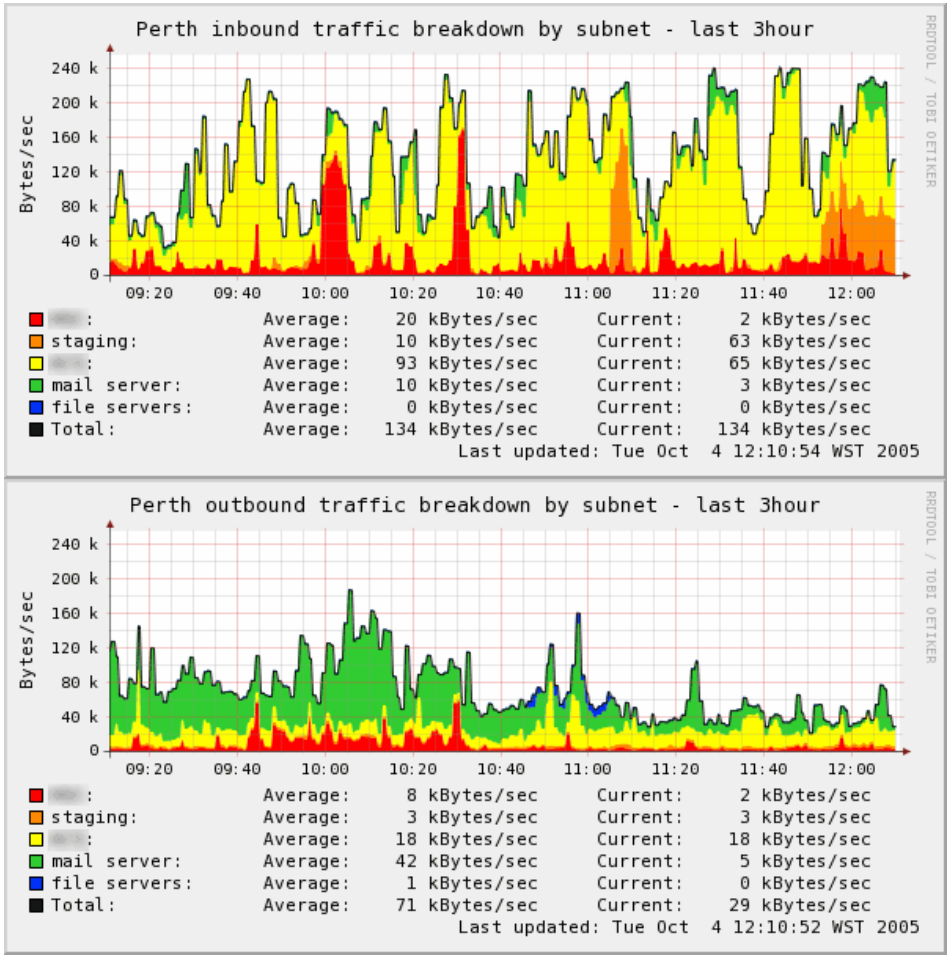
ISPs:

- ✓ Analysis of traffic trends for BGP peers
- ✓ Managing traffic quotas for residential customers

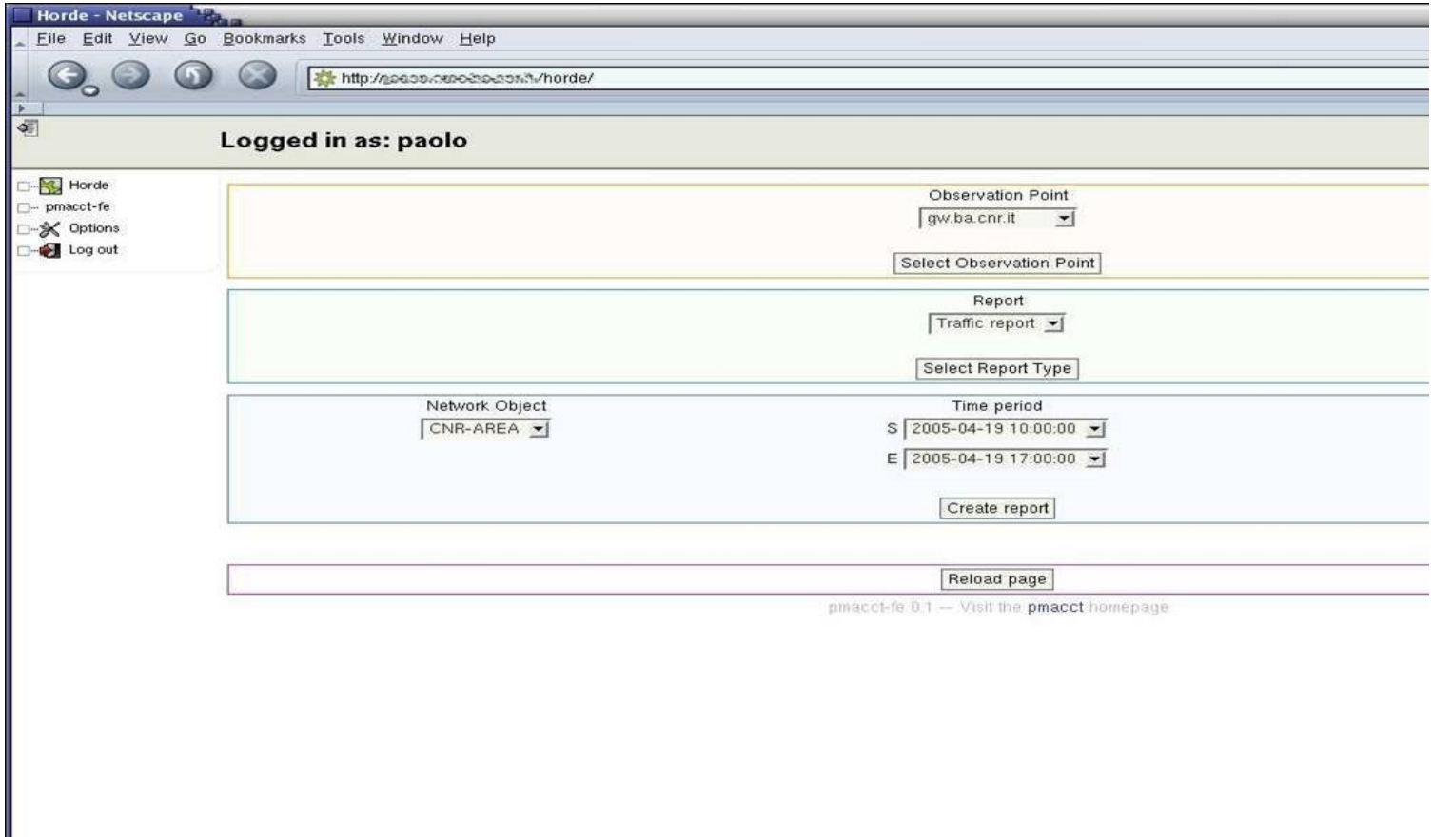
For example …


30 M
20 M
10 M
0
bits/sec
Sat 21
Sun 22
Mon 23
Tue 24
Wed 25
Thu 26
Fri 27
last week (30 minute averages)
input 1.34 Mb/s last 5.57 Mb/s ave 28.36 Mb/s max
output 393.92 kb/s last 1.32 Mb/s ave 5.27 Mb/s max
digiweb
my account
log out
news
INEX leads the way as ENUM Registry comes to the Exchange
New INEX Record as Ireland Goes Online to Watch Budget
INEX Breaks Through 1 Gig Milestone
our members
Verizon Business 702
HEAnet 1213
Cable & Wireless 1273
BT Ireland 2110
INEX 2128
Virgin Media 5089
Eircom Net 5466
UPC 6830
Microsoft 8068
Colt Internet 8220
Internet Ireland 13293
Servecentric 15512
Strencom 16174
Irish Broadband 25441
Verisign 26415
Hosting 365 29650
Digiweb 31122
Smart Telecom 31458
Bytel 31641
Magnet Networks 34245
Clearwire Ireland 34317
Vistatec 34505
Interfusion Networks 34912
imagine 35272
WestNet 39093
Blacknight Internet Solutions 39122
Blueface 39233
Fastcom Broadband Ltd 39449
Radio Telefís Éireann 41073
Tibus 41678
IE Domain Registry 42310
Done
www.inex.ie

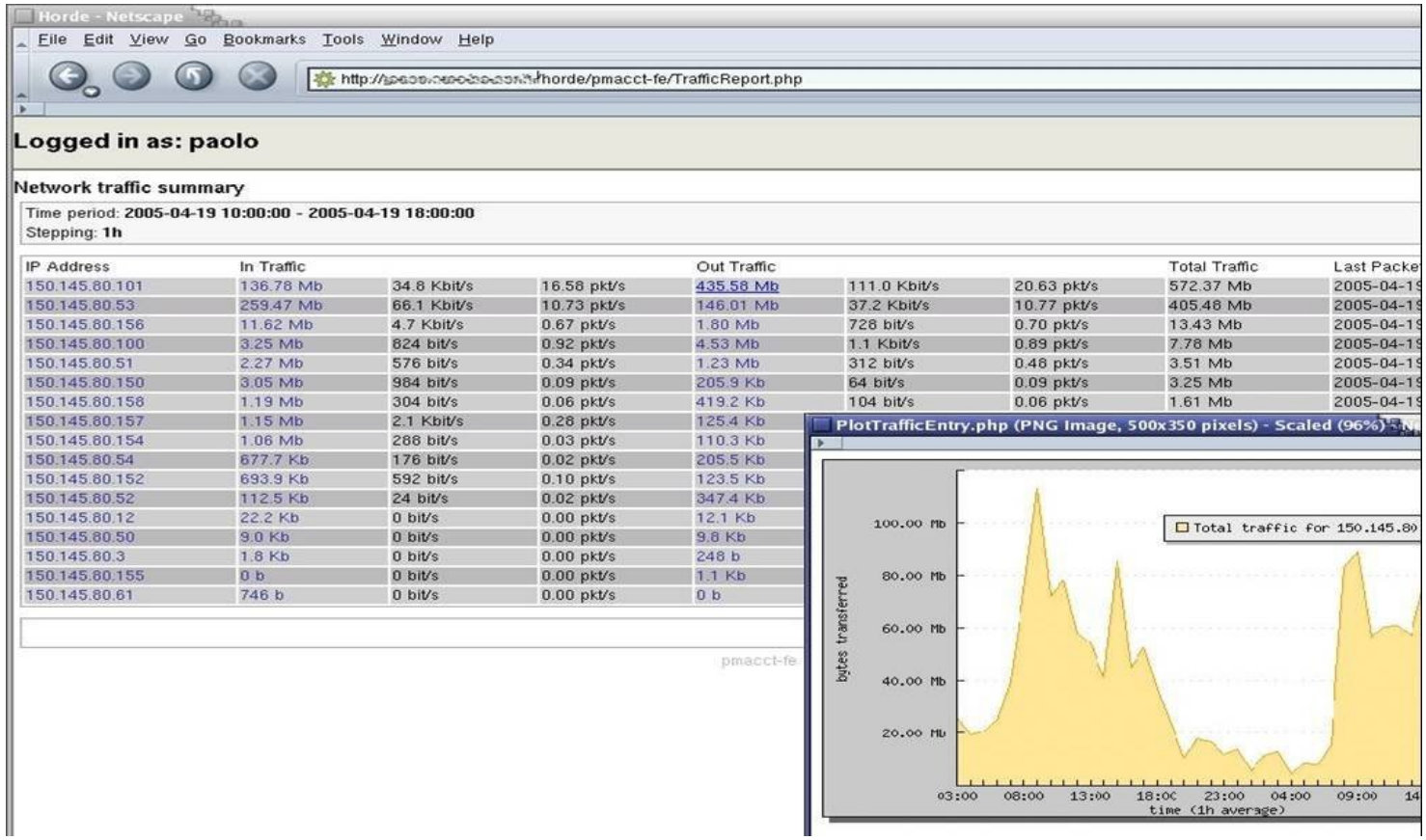
Feeding into RRDtool. Martin Pot, from RRDtool gallery



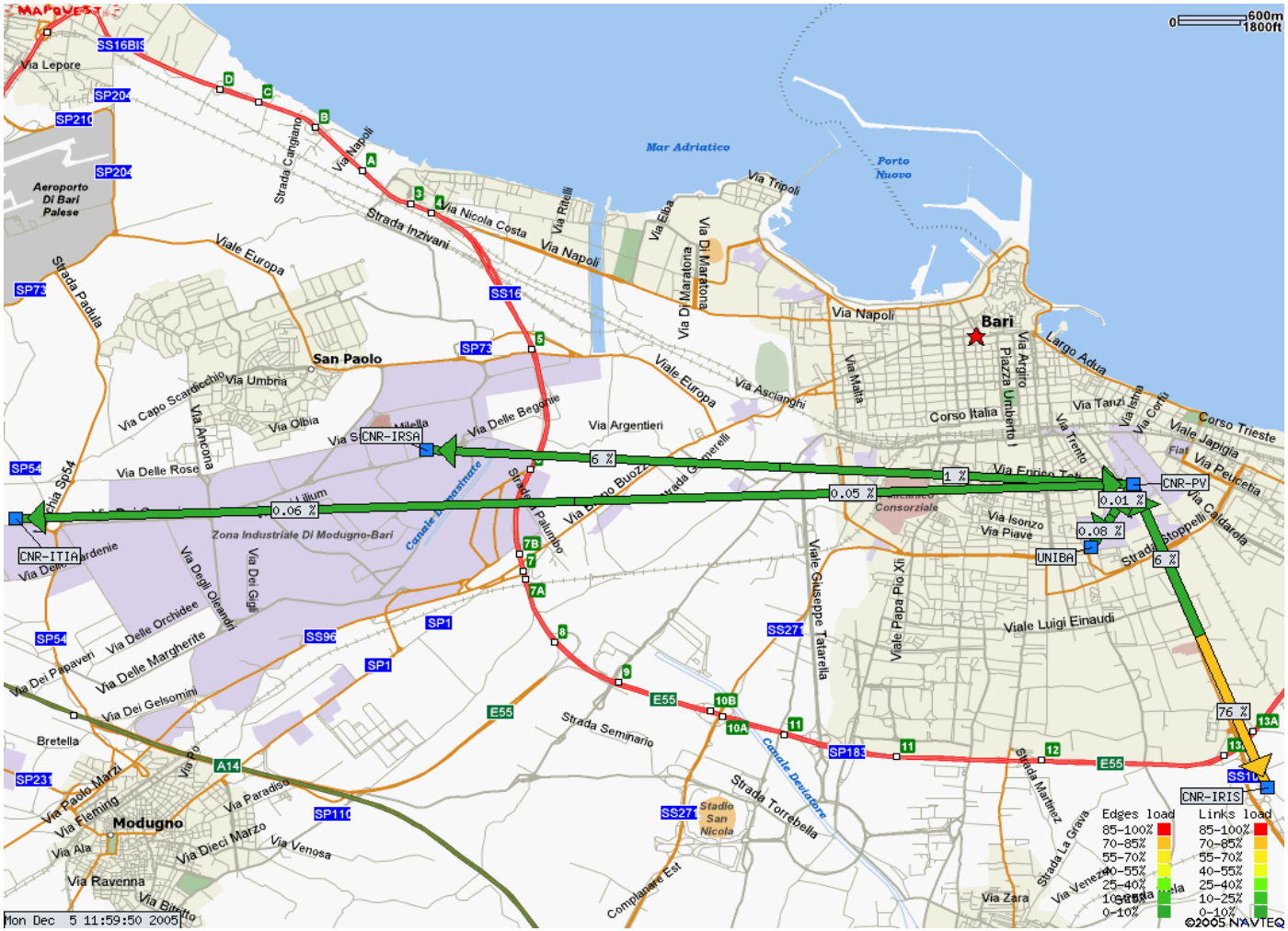
pmacct-fe: intro



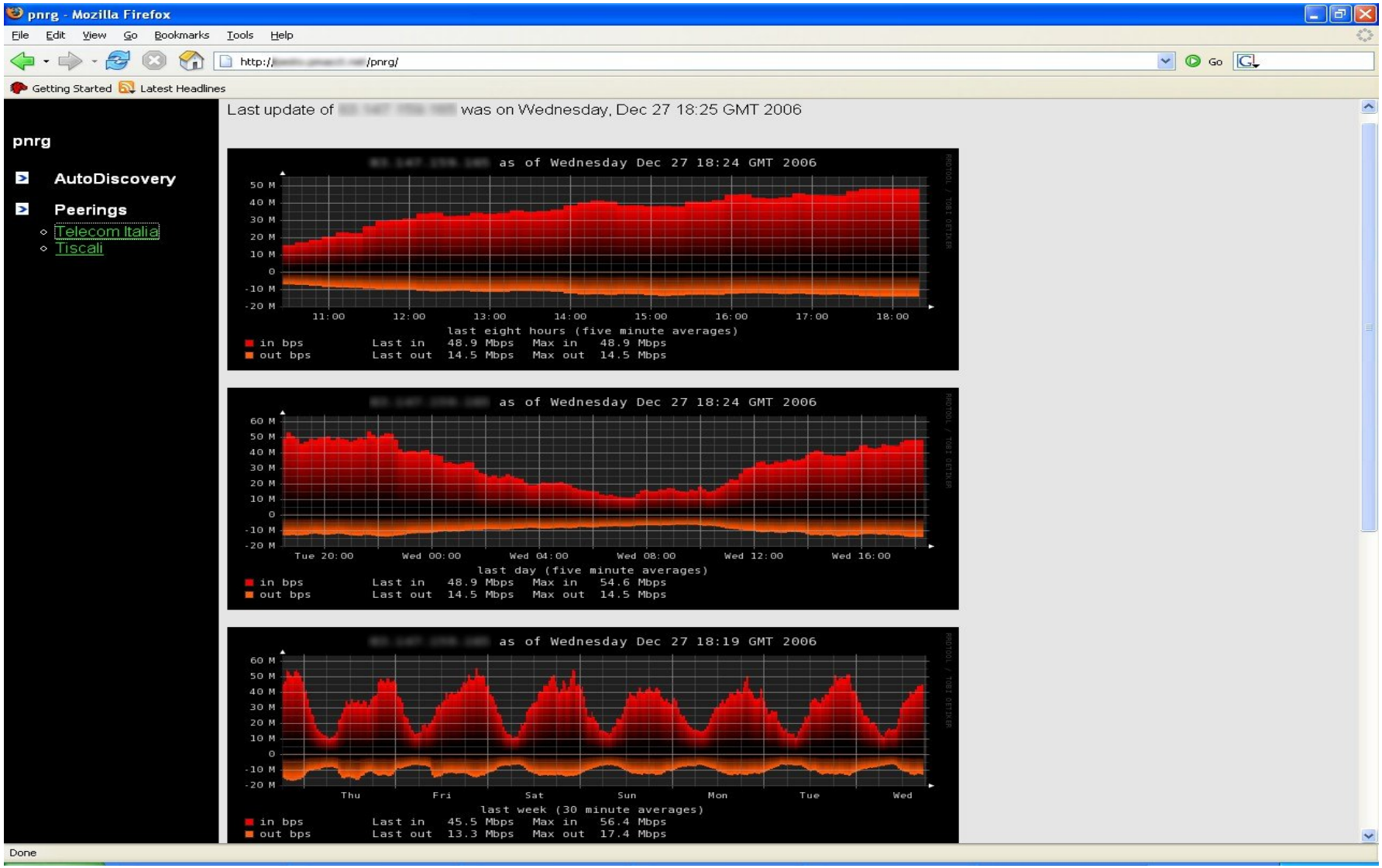
pmacct-fe: selection



GWEN: network weather maps



PNRG: RRD graphs applying SNMP auto-discovery concepts



Thanks for your attention !

http://www.pmacct.net/

Paolo LUCENTE, <*paolo at pmacct dot net*>