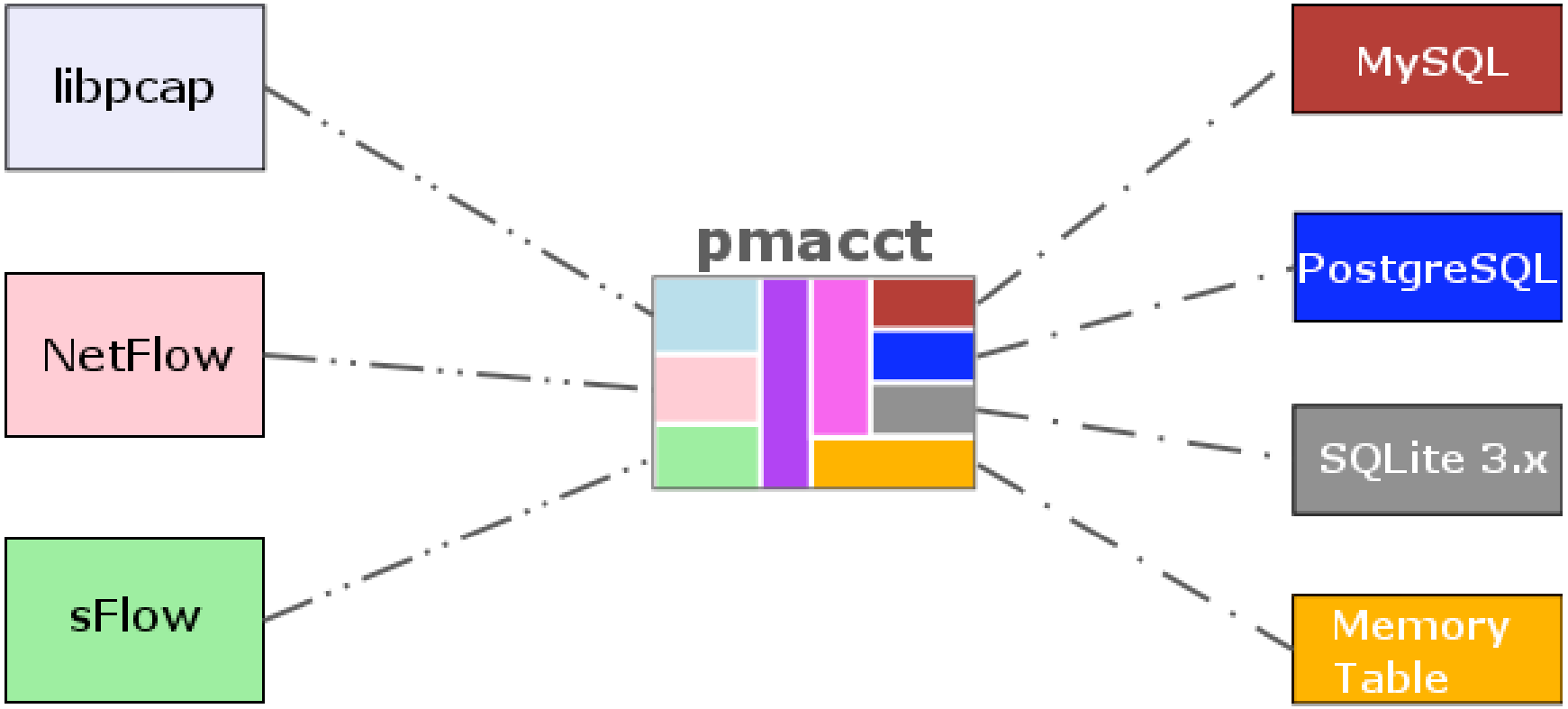
“pmacct, a new player in the network management arena”

http://www.ba.cnr.it/~paolo/pmacct/

Paolo LUCENTE, CNR-Italy

Mumbai, 24 Jan 2006

What is pmacct ?

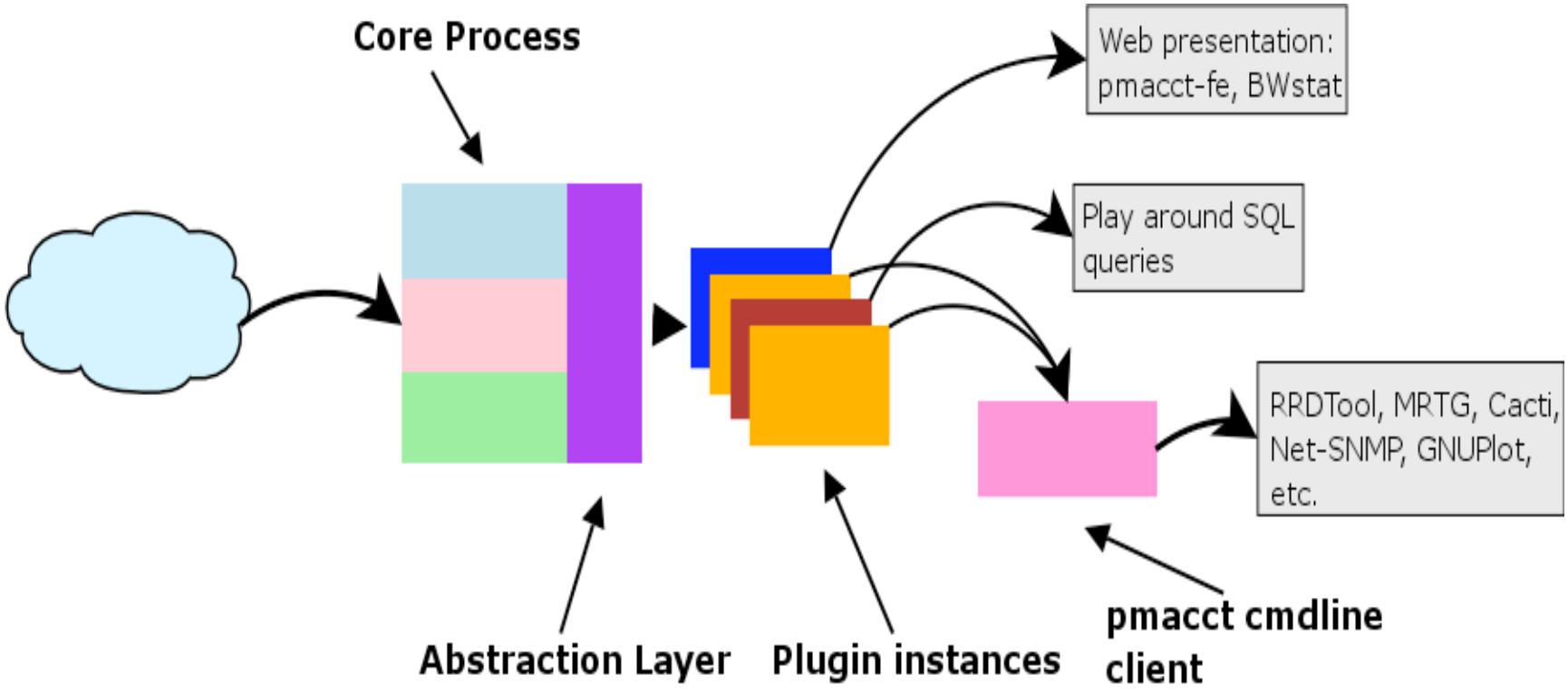


pmacct is a PASSIVE network monitoring tool

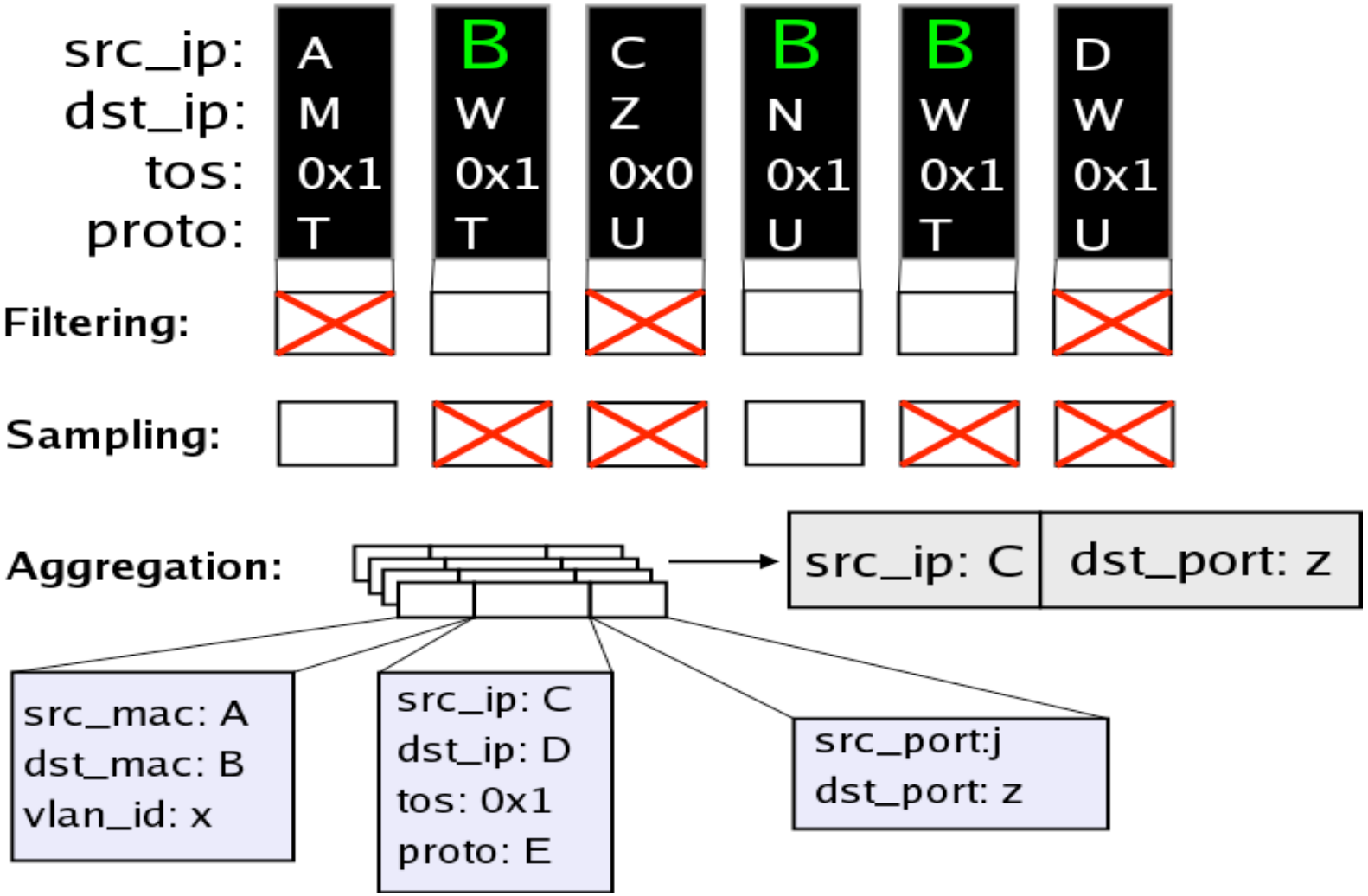
Passive network monitoring is basically an observation point; it enables us to understand:

- ✓ who is using the network.
- ✓ which applications/services are most used.
- ✓ how much bandwidth is in use over the time.
- ✓ are we generating DoS / target of a worm ?
- ✓ how our BGP peerings behave.
- ✓ what is that sudden hill in the last traffic graph ?

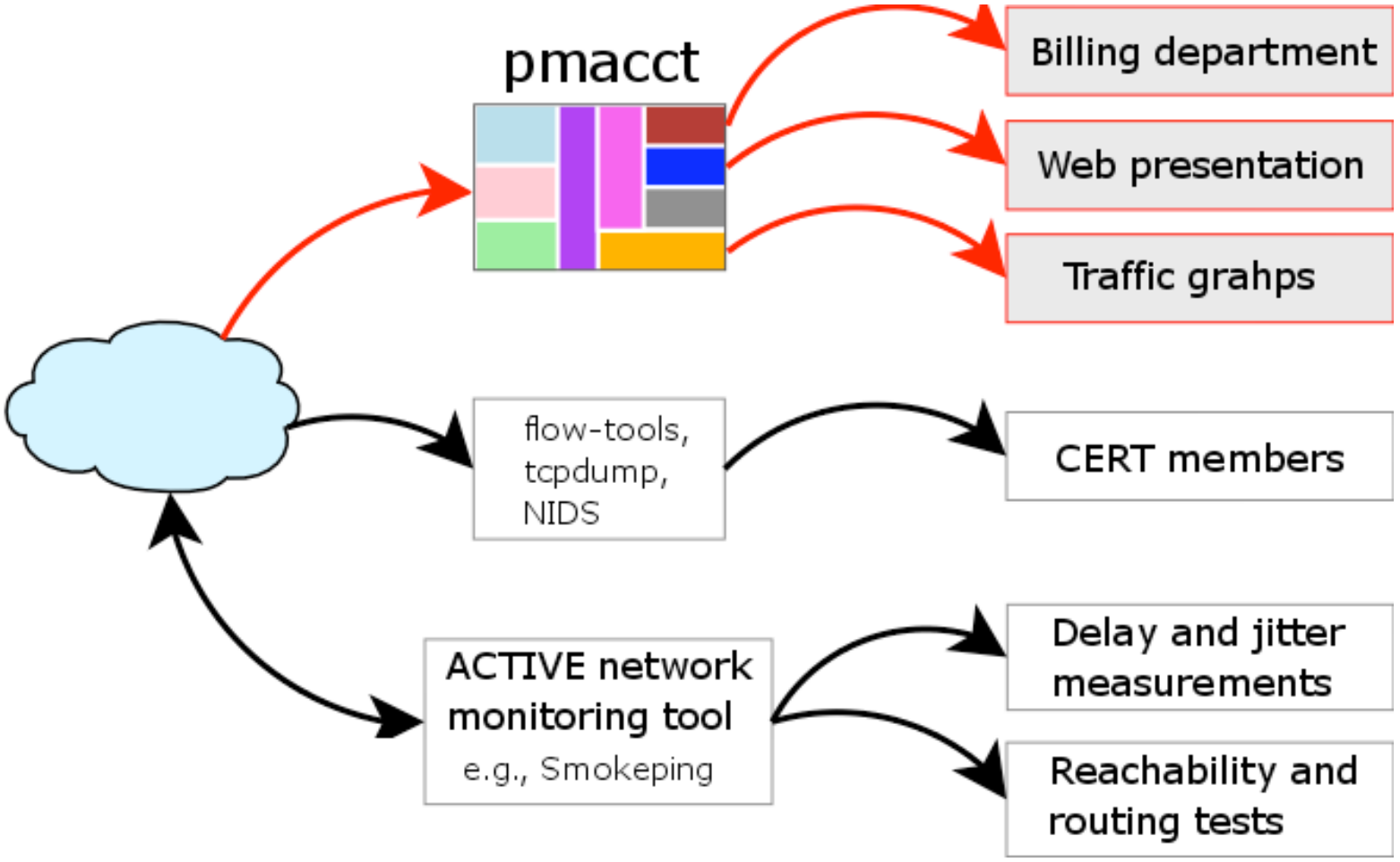
pmacct, the modular architecture: one collector, multiple services



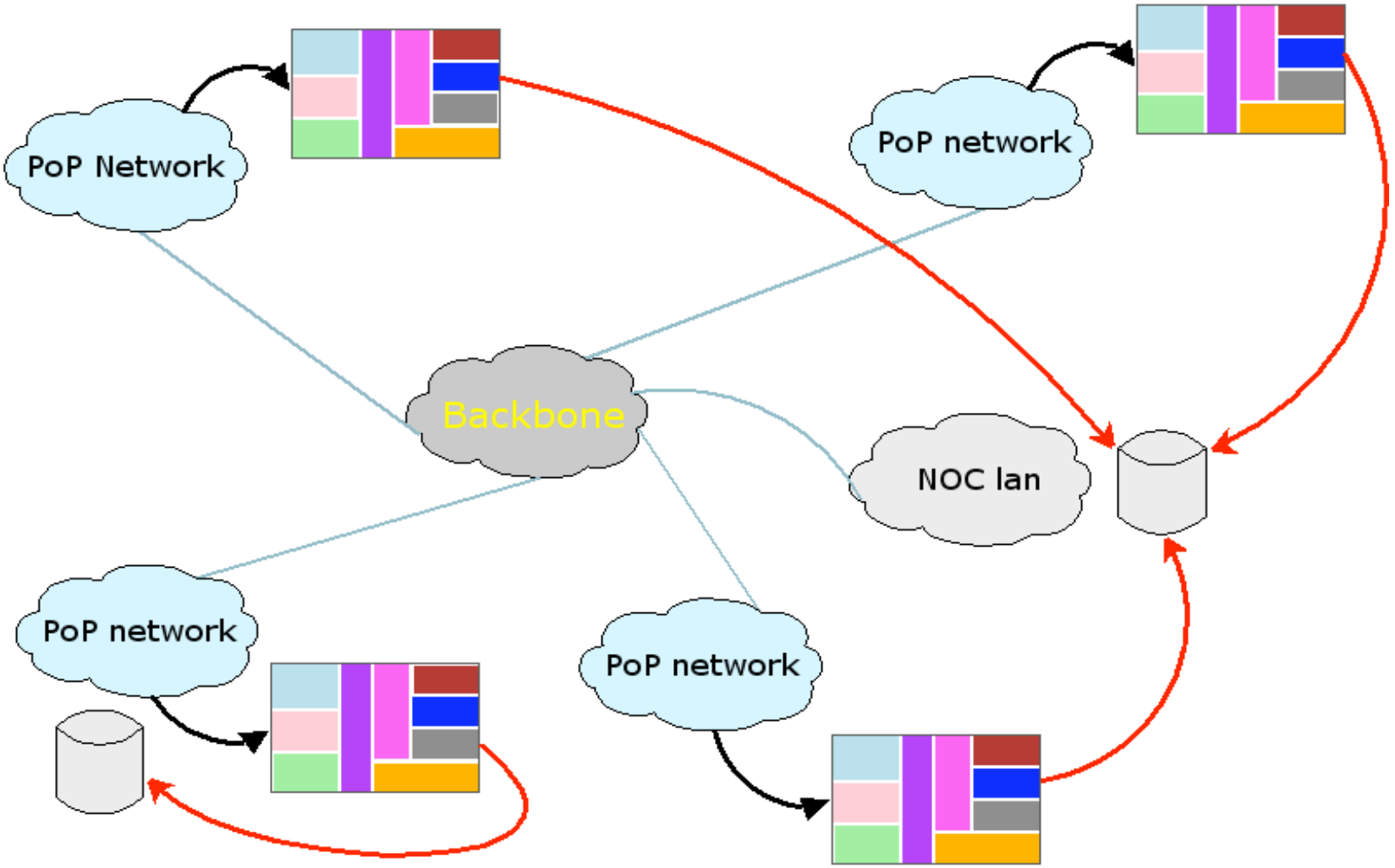
pmacct: reporting traffic data from broadband networks (I)



pmacct: reporting traffic data from broadband networks (II)



pmacct: a brief overview of the distributed architecture



“pmacct, a new player in the network management arena”

http://www.ba.cnr.it/~paolo/pmacct/

Part II

The examples

The newbie hat: In+Out (sum) traffic per host (I)

```
shell> cat pmacctd-imt.conf
!
! pmacctd configuration example
!
interface: eth0
plugins: memory
!
aggregate: sum_host, flows
networks_file: networks.lst
```

The newbie hat: In+Out (sum) traffic per host (II)

```
shell> ./pmacct -s
SRC IP          PACKETS     FLOWS       BYTES
150.145.84.4    2           2           152
150.145.82.19   7594        38          6584356
150.145.87.15   1           1           128
150.145.90.255  2           2           466
150.145.80.51   127224      8819        23678985
150.145.81.18   2           2           460
150.145.87.159  83          11          8758
150.145.80.0    22          1           1144
150.145.87.108  1           1           247
150.145.84.156  34          9           2856
150.145.81.255  33          7           6662
150.145.82.10   1423        30          1091800
150.145.87.6    16787       3361        929034
[ … continues … ]
```

The newbie hat: In+Out (sum) traffic per host (III)

a) The –M : getting a specific entry wrapped by a formatted output

shell> ./pmacct -c src_host -M 150.145.80.101

SRC IP	PACKETS	FLOWS	BYTES
150.145.80.101	287522	2616	273081046

b) The –N : getting the counters. Introducing the -r reset flag. The quick way to glue pmacct to external tools

shell> ./pmacct -c src_host -N 150.145.80.101 -r

334701089

shell> ./pmacct -c src_host -N 150.145.80.101

2790707

Building network traffic graphs (I)

```
interface: eth0
plugins: memory[out], memory[in]
!
aggregate[out]: src_net
aggregate_filter[out]: vlan and src net 150.145.80.0/20
imt_path[out]: /tmp/pmacct_out.pipe
!
aggregate[in]: dst_net
aggregate_filter[in]: vlan and dst net 150.145.80.0/20
imt_path[in]: /tmp/pmacct_in.pipe
```

Building network traffic graphs (II)

```
shell> cat mrtg-example.sh
#!/bin/sh

unset OUT
unset IN

OUT=`pmacct -c src_host –p /tmp/pmacct_out.pipe -N 150.145.80.0 -r`
IN=`pmacct -c dst_host –p /tmp/pmacct_in.pipe -N 150.145.80.0 -r`

echo $OUT
echo $IN
echo 0
echo 0
```

Building network traffic graphs (III)

```
shell> cat mrtg.conf
[ … ]
# Target specific definitions
Target[pp]: `/usr/local/pmacct/scripts/mrtg-example.sh`
SetEnv[pp]: MRTG_INT_IP="150.145.80.0" MRTG_INT_DESCR="Server LAN"
MaxBytes[pp]: 1250000
LegendI[pp]:
Title[pp]: Server LAN
PageTop[pp]: <H1>Server LAN</H1>
<TABLE>
   <TR><TD>System:</TD>  <TD>Server LAN</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>CNR-BA Staff</TD></TR>
   <TR><TD>Ip:</TD>  <TD>150.145.80.0</TD></TR>
</TABLE>
[ … ]
```

Network traffic data, the SQL way (I)

```
interface: eth0
plugins: pgsql[out], pgsql[in]
!
aggregate[out]: src_host
aggregate_filter[out]: vlan and src net 150.145.80.0/20
sql_table[out]: acct_out
!
aggregate[in]: dst_host
aggregate_filter[in]: vlan and dst net 150.145.80.0/20
sql_table[in]: acct_in
!
sql_refresh_time: 60
sql_history: 1h
sql_history_roundoff: h
sql_preprocess: minb=60000
```

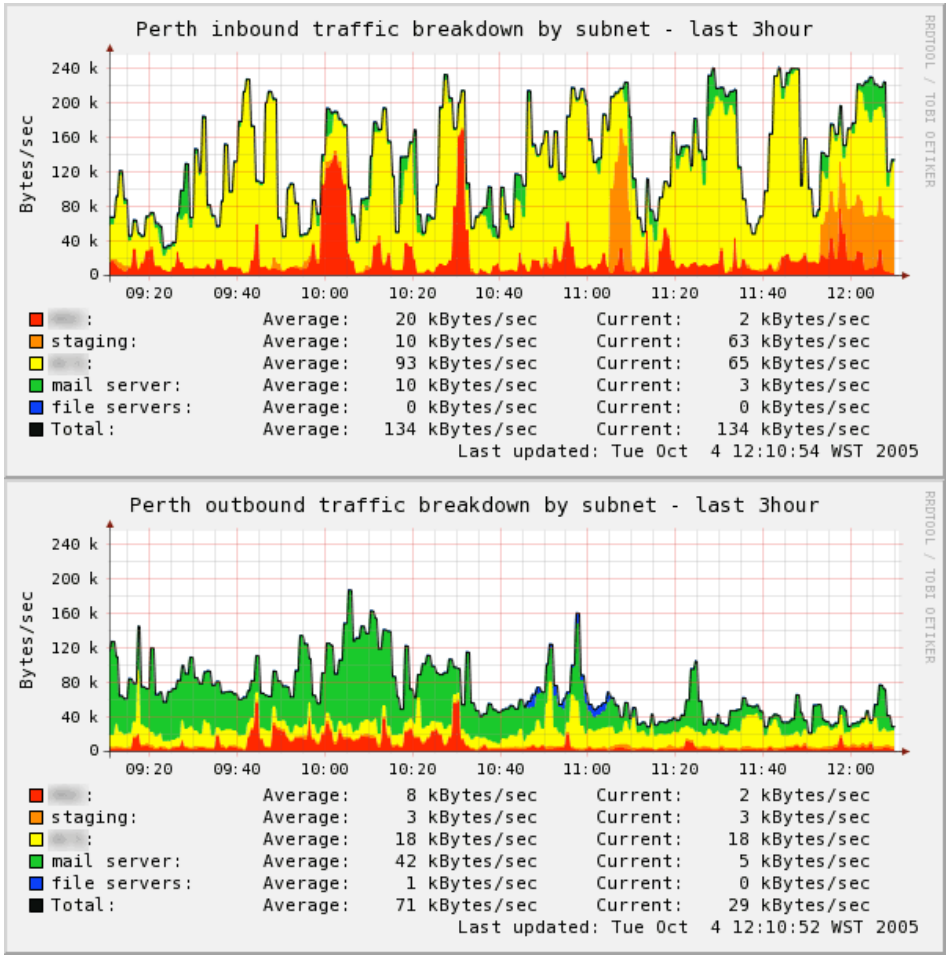
Network traffic data, the SQL way (II)

```
shell> psql -U pmacct -c "SELECT * FROM acct_out \
      WHERE ip_src = '150.145.80.101‘ \
      ORDER BY stamp_inserted DESC \
      LIMIT 10;"

     ip_src          |  packets |  bytes      |   stamp_inserted       |    stamp_updated
---------------------+----------+-------------+------------------------+-------------------------
 150.145.80.101 |  355394 | 29925806 | 2006-01-08 16:00:00 | 2006-01-08 16:48:02
 150.145.80.101 |  556245 | 46096570 | 2006-01-08 15:00:00 | 2006-01-08 16:00:02
 150.145.80.101 |   26364 | 12618610 | 2006-01-08 14:00:00 | 2006-01-08 15:00:02
 150.145.80.101 |  196319 | 16508068 | 2006-01-08 13:00:00 | 2006-01-08 14:00:01
 150.145.80.101 |  341143 | 40921593 | 2006-01-08 12:00:00 | 2006-01-08 13:00:02
 150.145.80.101 |  208050 | 30011464 | 2006-01-08 11:00:00 | 2006-01-08 12:00:01
 150.145.80.101 |  196337 | 15404272 | 2006-01-08 10:00:00 | 2006-01-08 11:01:02
 150.145.80.101 |  205970 | 16656939 | 2006-01-08 09:00:00 | 2006-01-08 10:00:03
 150.145.80.101 |  376094 | 22589504 | 2006-01-08 08:00:00 | 2006-01-08 09:00:02
 150.145.80.101 |   14779 |   6913855 | 2006-01-08 07:00:00 | 2006-01-08 08:01:01
(10 rows)
```

Network traffic data, the SQL way: what about “top N” ?

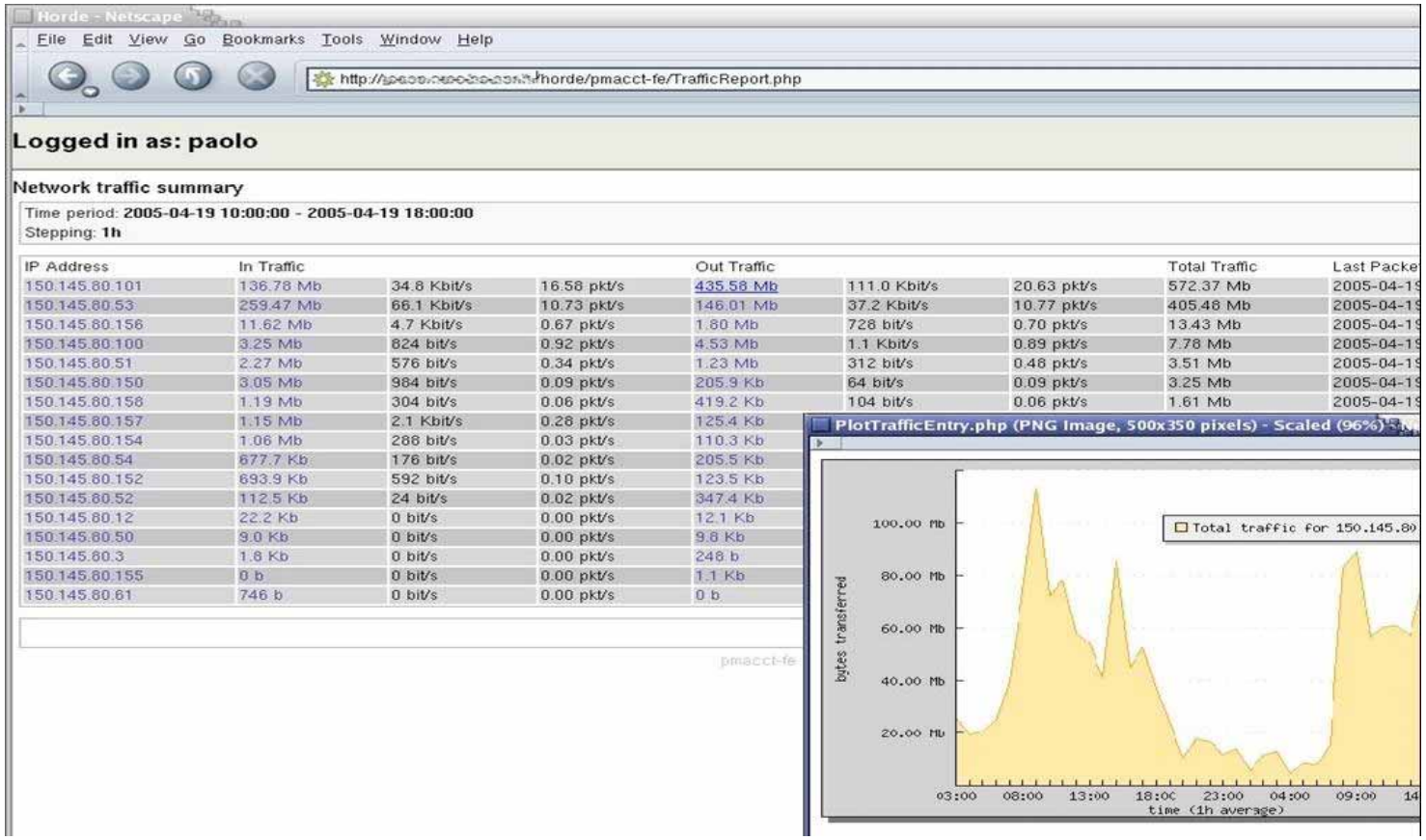
```
shell> psql –U pmacct –c “SELECT port_dst, ip_proto, packets, bytes \
    FROM dst_ports_db \
    WHERE dst_src = '150.145.80.101' AND \
    stamp_inserted = '2006-01-09 12:00:00‘ \
    ORDER BY bytes DESC
    LIMIT 10;”

 port_dst |  ip_proto |  packets |     bytes
----------+-----------+----------+----------------
      119 |         6 | 1084915 | 1594897858
       25 |         6 |   385883 |   374188510
       80 |         6 |    24632 |    26649410
      110 |         6 |    14595 |    15556361
       22 |         6 |    10775 |    13201890
      443 |         6 |     2943 |     1929708
      143 |         6 |      911 |     1111241
       53 |         1 |      607 |      879218
      995 |         6 |     9399 |      541329
       20 |         6 |      140 |      188855
(10 rows)
```

pmacct: results (I)
by Martin Pot, from RRDtool gallery

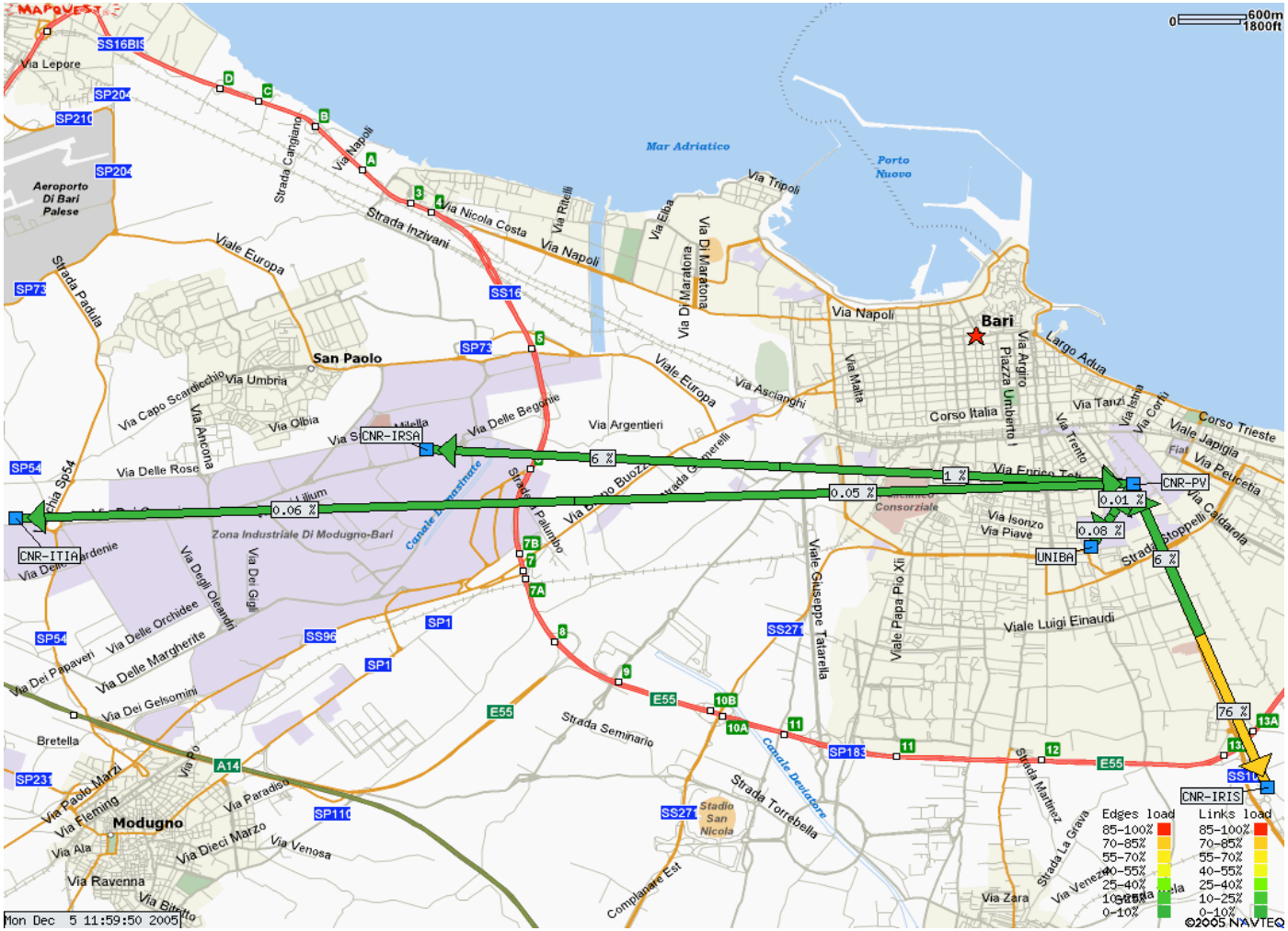


pmacct: results (II)
pmacct-fe screenshot (A)

pmacct: results (II)
pmacct-fe screenshot (B)



pmacct: results (III)
Network weather map



We are almost finished

Let’s take a moment to talk about future plans of pmacct

What’s going on ?

Thank you for your attention !

http://www.ba.cnr.it/~paolo/pmacct/

Paolo LUCENTE, paolo.lucente@ic.cnr.it