#### "pmacct, a new player in the network management arena"

http://www.pmacct.net

#### Paolo LUCENTE, CNR-Italy

Istanbul, 25 April 2006

# What is pmacct?



### pmacct: why, when and how .. (I)

- The project came out of operational needs, 3 years ago (beginnings of 2003)
- At the time it was easy to get data either:
  - "static", ie. fixed view of your network traffic data. Full stop.
  - logged on the disk in a range of proprietary format; then APIs to get in touch with them.
  - nicely arranged on the console screen or web browser of choice.

### pmacct: why, when and how .. (II)

Though, we were still missing:

- A way to get data from our network, being also able to choose how to report them and supporting multiple collection methods.
- A straight way to feed network data to external applications in order to build figures, graphs, plots, sums, etc.
- A straight way to powerfulness and flexibility offered by the SQL data language.

## pmacct is a PASSIVE network monitoring tool

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

- $\checkmark$  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 ?

### **ACTIVE** network monitoring tools

- .. by contrast, they are probes injected in the network; and they enable us to understand different things:
- How many packets get lost ?
- ✓ Do all the probes have the same trip ?
- ✓ How much it takes to deliver the probe ?
- Hey, let's check that our premium IP offering works as expected under heavy traffic loads

#### pmacct, the modular architecture: one collector, multiple views



### pmacct: reporting traffic data from broadband networks (I)



### pmacct: reporting traffic data from broadband networks (II)



# pmacct: an outlook of the distributed architecture



#### pmacct: about classification



# pmacct: classification, RE

An example of Regular Expressions applied to classification (this is from the L7-filter project repository):

http/(0\.9|1\.0|1\.1) [1-5][0-9][0-9] [\x09-\x0d -~]\*(connection:|content-type:|contentlength:|date:)|post [\x09-\x0d -~]\* http/[01]\.[019]

# pmacct: classification, SO

u\_int32\_t classifier(struct pkt\_classifier\_data \*data, int caplen, void \*\*context, void \*\*rev\_context, void \*\*extra)

```
struct rtp context *ctx = NULL;
rtp hdr t *hdr = (rtp_hdr_t *) data->payload_ptr;
u int16 t init;
u int8 t version, pt;
init = ntohs(hdr->init);
version = init >> 14;
pt = init \& 0x7f;
if (version == 2 && (pt < 35 || pt >= 96)) { /* Possibly, we are facing a RTP stream */
         if (!(*context)) { /* We don't have enough data about the stream */
                       ctx = malloc(sizeof(struct rtp_context));
                       if (ctx) {
                                     ctx->seq = ntohs(hdr->seq);
                                     *context = ctx:
                       return 0;
         }
         else {
                       ctx = (struct rtp context *) *context;
                       if (ntohs(hdr->seq) == ctx->seq+1) return 1;
         }
return 0;
```

{

}

#### pmacct: classification, RE vs. SO

- Regular Expressions (RE) classifiers are proficient against the packet payload, easy to develop and suitable for text-based protocols.
- Shared Object (SO) classifiers are powerful (ie. because of contexts), not limited to just catch patterns (ie. Machine Learning tecniques) and deal smoothly with binary-encoded protocols. BUT require extensive and careful development.

## "pmacct, a new player in the network management arena"

http://www.pmacct.net

#### Part II

Examples and results

```
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)

PACKETS	FLOWS	BYTES
2	2	152
7594	38	6584356
1	1	128
2	2	466
127224	8819	23678985
2	2	460
83	11	8758
22	1	1144
1	1	247
34	9	2856
33	7	6662
1423	30	1091800
16787	3361	929034
]		
	PACKETS 2 7594 1 2 127224 2 83 22 1 34 33 1423 16787	PACKETSFLOWS227594381122127224881922831122111349337142330167873361

# 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
ļ
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
Legendl[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>lp:</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   150.145.80.101   150.145.80.101   150.145.80.101   150.145.80.101   150.145.80.101   150.145.80.101   150.145.80.101	355394   2992580 556245   4609657 26364   1261861 196319   1650806 341143   4092159 208050   3001146 196337   1540427	6   2006-01-08 16:00:00 0   2006-01-08 15:00:00 0   2006-01-08 14:00:00 8   2006-01-08 13:00:00 3   2006-01-08 12:00:00 4   2006-01-08 11:00:00 2   2006-01-08 10:00:00	
150.145.80.101   150.145.80.101   150.145.80.101   (10 rows)	205970   1665693 376094   2258950 14779   691385	9   2006-01-08 09:00:00 4   2006-01-08 08:00:00 5   2006-01-08 07:00:00	2006-01-08 10:00:03   2006-01-08 09:00:02   2006-01-08 08:01:01

# 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	+ ا 6	1084915	1594897858
25	6	385883	374188510
80 j	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)			

# Network traffic data, the SQL way: classification and "top N" !

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

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



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

Horde - Netscape		
<u>_ File Edit View 9</u>	<u>ao B</u> ookmarks <u>T</u> ools <u>W</u> indow <u>H</u> elp	
0,00	Kittp://pecse.com/com/com/com/com/com/com/com/com/com/	
4	Logged in as: paolo	
		Observation Point gw.ba.cnr.it Select Observation Point
		Report Traffic report <u>–</u> Select Report Type
	Network Object	Time period S 2005-04-19 10:00:00 ▼ E 2005-04-19 17:00:00 ▼ Create report

Reload page

pmacct-fe 0.1 - Visit the pmacct homepage

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

Network traffic summary           Time period: 2005-04-19 10:00:00 - 2005-04-19 18:00:00           Stepping: 1h           Total Traffic	
Time period: 2005-04-19 10:00:00 - 2005-04-19 18:00:00           Stepring: 1h         Out Traffic         Total Traf           150.145:80.101         136.78 Mb         34.8 Kbit/s         16.58 pkt/s         435.58 Mb         111.0 Kbit/s         20.63 pkt/s         572.37 M           150.145:80.156         11.62 Mb         4.7 Kbit/s         0.67 pkt/s         180.045         0.70 pkt/s         134.3 Mb           150.145:80.156         11.62 Mb         4.7 Kbit/s         0.67 pkt/s         1.80 Mb         728 bit/s         0.70 pkt/s         134.3 Mb           150.145:80.150         3.25 Mb         824 bit/s         0.32 pkt/s         1.22 Mb         3.13 Kb         3.13 Kb         0.67 pkt/s         1.23 Mb         312 bit/s         0.49 pkt/s         3.78 Mb           150.145:80.150         3.05 Mb         984 bit/s         0.92 pkt/s         205.9 Kb         64 bit/s         0.09 pkt/s         3.25 Mb           150.145:80.156         1.19 Mb         304 bit/s         0.06 pkt/s         419.2 Kb         104 bit/s         0.06 pkt/s         1.61 Mb           150.145:80.156         1.16 Mb         2.1 Kbit/s         0.02 pkt/s         205.5 Kb         104 bit/s         0.06 pkt/s         1.61 Mb           150.145:80.152         693.9 Kb<	
IP Address         In Traffic         Out Traffic         Total Traffic           150.145.80.101         136.78 Mb         34.8 Kbit/s         16.58 pkt/s         435.58 Mb         111.0 Kbit/s         20.63 pkt/s         572.37 M           150.145.80.156         11.62 Mb         425.58 Mb         111.0 Kbit/s         20.63 pkt/s         572.37 M           150.145.80.156         11.62 Mb         47. Kbit/s         0.67 pkt/s         146.01 Mb         37.2 Kbit/s         10.77 pkt/s         405.48 M           150.145.80.156         11.62 Mb         47. Kbit/s         0.67 pkt/s         1.80 Mb         726 bit/s         0.70 pkt/s         13.43 Mb           150.145.80.150         3.25 Mb         824 bit/s         0.92 pkt/s         1.23 Mb         312 bit/s         0.48 pkt/s         3.51 Mb           150.145.80.513         2.27 Mb         576 bit/s         0.34 pkt/s         1.23 Mb         312 bit/s         0.48 pkt/s         3.51 Mb           150.145.80.150         3.05 Mb         984 bit/s         0.09 pkt/s         205.9 Kb         64 bit/s         0.09 pkt/s         3.25 Mb           150.145.80.157         1.15 Mb         2.1 Kbit/s         0.28 pkt/s         125.4 Kb         104 bit/s         0.06 pkt/s         1.61 Mb           150.145.80.52	
150.145.80.101       136.78 Mb       34.8 Kbit/s       16.56 pkt/s       435.58 Mb       111.0 Kbit/s       20.63 pkt/s       572.37 M         150.145.80.53       259.47 Mb       66.1 Kbit/s       10.73 pkt/s       146.01 Mb       37.2 Kbit/s       10.77 pkt/s       405.48 M         150.145.80.56       11.62 Mb       4.7 Kbit/s       0.67 pkt/s       1.80 Mb       37.2 Kbit/s       0.70 pkt/s       13.43 Mb         150.145.80.100       3.25 Mb       824 bit/s       0.92 pkt/s       4.53 Mb       1.1 Kbit/s       0.89 pkt/s       7.78 Mb         150.145.80.150       3.05 Mb       984 bit/s       0.09 pkt/s       205.9 Kb       64 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.150       1.19 Mb       304 bit/s       0.09 pkt/s       205.9 Kb       64 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb       105.145.80.52       150.145.80.52       125.5 Kb       120.00 pkt/s       121.1 Kb       100.00 mb       100.00 mb<	c Last Pack
150.145.80.53       259.47 Mb       66.1 Kbit/s       10.73 pkt/s       146.01 Mb       37.2 Kbit/s       10.77 pkt/s       405.48 M         150.145.80.156       11.62 Mb       4.7 Kbit/s       0.67 pkt/s       1.80 Mb       728 bit/s       0.70 pkt/s       13.43 Mb         150.145.80.156       11.62 Mb       8.47 Kbit/s       0.92 pkt/s       4.53 Mb       1.1 Kbit/s       0.89 pkt/s       7.78 Mb         150.145.80.51       2.27 Mb       576 bit/s       0.34 pkt/s       1.23 Mb       312 bit/s       0.48 pkt/s       3.51 Mb         150.145.80.150       3.05 Mb       984 bit/s       0.09 pkt/s       205.9 Kb       64 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.156       1.19 Mb       304 bit/s       0.06 pkt/s       419.2 Kb       104 bit/s       0.06 pkt/s       3.25 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.154       1.06 Mb       286 bit/s       0.03 pkt/s       123.5 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.152       19.3 Pkb       52 bit/s       0.10 pkt/s       347.4 Kb       100.00 mb       100.00 mb       100.00 mb       100.00 mb       100.00	2005-04-1
150.145.80.156       11.62 Mb       4.7 Kbit/s       0.67 pkt/s       1.80 Mb       726 bit/s       0.70 pkt/s       13.43 Mb         150.145.80.100       3.25 Mb       824 bit/s       0.92 pkt/s       4.53 Mb       1.1 Kbit/s       0.89 pkt/s       7.78 Mb         150.145.80.110       3.25 Mb       576 bit/s       0.34 pkt/s       1.23 Mb       312 bit/s       0.48 pkt/s       3.51 Mb         150.145.80.150       3.05 Mb       94 bit/s       0.09 pkt/s       205.9 Kb       64 bit/s       0.99 pkt/s       3.25 Mb         150.145.80.156       1.19 Mb       304 bit/s       0.06 pkt/s       419.2 Kb       104 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.154       1.06 Mb       266 bit/s       0.02 pkt/s       225.5 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       323.5 Kb       100.00 mb	2005-04-1
150.145.80.100       3.25 Mb       824 bit/s       0.92 pkt/s       4.53 Mb       1.1 Kbit/s       0.69 pkt/s       7.76 Mb         150.145.80.51       2.27 Mb       576 bit/s       0.34 pkt/s       1.23 Mb       312 bit/s       0.48 pkt/s       3.51 Mb         150.145.80.150       3.05 Mb       944 bit/s       0.09 pkt/s       2.05 9 Kb       64 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.158       1.19 Mb       304 bit/s       0.06 pkt/s       419.2 Kb       104 bit/s       0.06 pkt/s       3.25 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.154       1.06 Mb       268 bit/s       0.03 pkt/s       110.3 Kb       150.145.80.54       67.7 Kb       176 bit/s       0.02 pkt/s       205.5 Kb       150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb       100.00 mb       100.	2005-04-1
150.145.80.51       2.27 Mb       576 bit/s       0.34 pt/s       1.23 Mb       312 bit/s       0.48 pt/s       3.51 Mb         150.145.80.150       3.05 Mb       984 bit/s       0.09 pt/s       205.9 Kb       64 bit/s       0.09 pt/s       3.25 Mb         150.145.80.150       3.05 Mb       304 bit/s       0.06 pt/s       419.2 Kb       104 bit/s       0.06 pt/s       1.61 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.26 pt/s       125.4 Kb       PlotTrafficEntry.php (PNG Image, S00x350 pixel         150.145.80.54       677.7 Kb       176 bit/s       0.02 pt/s       205.5 Kb       150.145.80.52       112.5 Kb       24 bit/s       0.02 pt/s       347.4 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.00 pt/s       32.5 Kb       100.00 mb       100.0	2005-04-1
150.145.80.150       3.05 Mb       984 bit/s       0.09 pkt/s       205.9 Kb       64 bit/s       0.09 pkt/s       3.25 Mb         150.145.80.156       1.19 Mb       304 bit/s       0.06 pkt/s       419.2 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.26 pkt/s       1254 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.154       1.06 Mb       286 bit/s       0.03 pkt/s       110.3 Kb       155.145.80.54       67.7 Kb       176 bit/s       0.02 pkt/s       205.5 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb       105.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb         150.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb       150.145.80.12       22.2 Kb       0 bit/s       0.00 pkt/s       121.1 Kb       100.00 mb       100.00 mb <td< td=""><td>2005-04-1</td></td<>	2005-04-1
150.145.80.158       1.19 Mb       304 bit/s       0.06 pkt/s       419.2 Kb       104 bit/s       0.06 pkt/s       1.61 Mb         150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       PlotTrafficEntry.php (PNG Image, 500x350 pixel         150.145.80.154       1.06 Mb       268 bit/s       0.03 pkt/s       110.3 kb       PlotTrafficEntry.php (PNG Image, 500x350 pixel         150.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb       150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.00 pkt/s       12.1 Kb       100.00 mb       100.00 mb <td< td=""><td>2005-04-1</td></td<>	2005-04-1
150.145.80.157       1.15 Mb       2.1 Kbit/s       0.28 pkt/s       125.4 Kb       PlotTrafficEntry.php (PNG Image, 500x350 pixel         150.145.80.154       1.06 Mb       286 bit/s       0.03 pkt/s       110.3 Kb       110.3 Kb         150.145.80.154       67.7 Kb       176 bit/s       0.02 pkt/s       205.5 Kb       150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb         150.145.80.12       22.2 Kb       0 bit/s       0.00 pkt/s       12.1 Kb       100.00 mb       100.00 mb         150.145.80.3       1.8 Kb       0 bit/s       0.00 pkt/s       12.1 Kb       100.00 mb       100.00 mb         150.145.80.3       1.8 Kb       0 bit/s       0.00 pkt/s       248 b       100.00 mb       - <t< td=""><td>2005-04-1</td></t<>	2005-04-1
150.145.80.154       1.06 Mb       286 bit/s       0.03 ptt/s       110.3 Kb         150.145.80.54       677.7 Kb       176 bit/s       0.02 ptt/s       205.5 Kb         150.145.80.152       693.9 Kb       592 bit/s       0.10 ptt/s       123.5 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.02 ptt/s       347.4 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.00 ptt/s       12.1 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.00 ptt/s       12.1 Kb         150.145.80.50       9.0 Kb       0 bit/s       0.00 ptt/s       9.8 Kb         150.145.80.3       1.8 Kb       0 bit/s       0.00 ptt/s       2.48 b         150.145.80.155       0 b       0 bit/s       0.00 ptt/s       1.1 Kb         150.145.80.61       746 b       0 bit/s       0.00 ptt/s       0 b         150.145.80.61       746 b       0 bit/s       0.00 ptt/s       0 b	s) - Scaled (96%) -
150.145.80.54       677.7 Kb       176 bit/s       0.02 pkt/s       205 Kb         150.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb         150.145.80.52       112.5 Kb       0 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.50       9.0 Kb       0 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.3       1.8 Kb       0 bit/s       0.00 pkt/s       248 b         150.145.80.155       0 b       0 bit/s       0.00 pkt/s       1.1 Kb         150.145.80.61       746 b       0 bit/s       0.00 pkt/s       0 b         60.00 Mb       -       -       -	
150.145.80.152       693.9 Kb       592 bit/s       0.10 pkt/s       123.5 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb         150.145.80.52       112.5 Kb       24 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.50       9.0 Kb       0 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.31       1.8 Kb       0 bit/s       0.00 pkt/s       248 b         150.145.80.155       0 b       0 bit/s       0.00 pkt/s       1.1 Kb         150.145.80.61       746 b       0 bit/s       0.00 pkt/s       0 b         60.00 Mb       -       -       -	
150.145.80.52       112.5 Kb       24 bit/s       0.02 pkt/s       347.4 Kb         150.145.80.12       22.2 Kb       0 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.50       9.0 Kb       0 bit/s       0.00 pkt/s       9.8 Kb         150.145.80.3       1.8 Kb       0 bit/s       0.00 pkt/s       248 b         150.145.80.155       0.b       0 bit/s       0.00 pkt/s       1.1 Kb         150.145.80.61       746 b       0 bit/s       0.00 pkt/s       0.b         60.00 Mb       -       -       -	
150.145.80.12       22.2 Kb       0 bit/s       0.00 pkt/s       12.1 Kb         150.145.80.50       9.0 Kb       0 bit/s       0.00 pkt/s       9.8 Kb         150.145.80.30       1.8 Kb       0 bit/s       0.00 pkt/s       248 b         150.145.80.155       0 b       0 bit/s       0.00 pkt/s       1.1 Kb         150.145.80.61       746 b       0 bit/s       0.00 pkt/s       0 b         60.00 Mb       -       -       -	
150.145.80.50         9.0 kb         0 bit/s         0.00 pkt/s         9.8 Kb           150.145.80.3         1.8 Kb         0 bit/s         0.00 pkt/s         248 b           150.145.80.155         0 b         0 bit/s         0.00 pkt/s         1.1 Kb           150.145.80.61         746 b         0 bit/s         0.00 pkt/s         0 b           50.145.80.61         746 b         0 bit/s         0.00 pkt/s         0 b	naffic for 150 145 5
150.145.80.3         1.8 Kb         0 bit/s         0.00 pkt/s         248 b           150.145.80.155         0 b         0 bit/s         0.00 pkt/s         1.1 Kb           150.145.80.61         746 b         0 bit/s         0.00 pkt/s         0 b           60.00 Mb         -         -         -	Tarrit For 150.145.0
150.145.80.155 0 b 0 bit/s 0.00 pkt/s 1.1 Kb 150.145.80.61 746 b 0 bit/s 0.00 pkt/s 0 b 5 60.00 Mb - 5 60.00	A
150.145.80.61 746 b 0 bit/s 0.00 pkt/s 0 b	
50.00 Mb	
13 60.00 Mb	
	and the second second
pmacchie 8	
prinautries 3	
- 40.00 mb	
20.00 Hu	
	2

#### pmacct: results (III) network weather maps with GWEN



# A preview of FloX, the flow explorer by Sven Anderson

8					Fle	X - Mozilla Firef	ox					_ = ×
Datei Bearbeiten	<u>A</u> nsicht	<u>G</u> ehe <u>I</u>	<u>L</u> esezeic	hen E <u>x</u> t	tras <u>H</u> ilfe							$\langle \rangle$
🗇 • 🔿 • 🛃 🔕 1	😚 🗋 http	://		/flox/inde	ex.php?table=acc	t_v5_2&start=2	2006-04-21	%2010%3A17	7%3A55	&end=200 💌	O Go C.	
SPIEGEL ONLINE	🔂 heise o	nline 🔯 k	aputten	dorf 🗋 S	Studentenwerk G	öt 🗋 NDR Inf	o 🗀 Origina	al Toolbar 🗋 L	Link Die	s		
FloX												
Tables												
acct_v5 ac	ct_v5_2											
Flow Keys												
agent_id cl	ass_id m	nac_src	mac_ds	st vlan	ip_src ip_ds	t port_src: 80	port_dst	ip_proto: 6	tos	stamp_inserte	d stamp_updated	
(click on key to calcula	ite the summ	ation rankir	ng for thai	t key)								
Settings												
update Summation Ra	⊥ anking bytes	packets	flows									
16.85	82118306	63829	1076 5	select								
6.248	7798215	6742	370	select								
7.202	5170396	3533	16 5	select								
6.235	4489851	3750	105 5	select								
6.227	3612289	2946	113 5	select								
6.231	1587445	1487	112 5	select								
6.239	1466193	2399	297 5	select								
0.138	1145785	8/1	22 5	select								
2.100	860171	845	57 0	elect								
0.234	000171	045	57 5	select								
FloX v0.1b1 • © 2006	Sven Anders	on <sven(a< td=""><td>t)anderso</td><td>on.de&gt;</td><td></td><td></td><td></td><td></td><th></th><td></td><th></th><td></td></sven(a<>	t)anderso	on.de>								
Suchen:			⊖ Ab <u>w</u> ä		n @Aufwarts su	uchen <u>H</u> ervor	heben 🗆 <u>G</u>	roß-/Kleinschr	reibung	beachten		
Fertig						Taipei:	Sa 04:01	🎱 15° C 🍊	)   18°	C 🇞 20° C	💫 22° C 🗞 2	5° C 🕗

# Thank you for your attention !

#### http://www.pmacct.net

#### Paolo LUCENTE, paolo@pmacct.net