Monitoreo y Diagnóstico

Cristián Rojas
crrojas@nic.cl

Monitoreo

- ¿Por qué? ¿Para qué?
  - Errores de software
  - Errores de hardware
  - Errores humanos (usuarios, administradores)
  - Ataques
  - Etc

Monitoreo

- Bueno, ya entendí por qué debo monitorear, pero.... ¿qué monitorear?
  - Nodos
  - Servicios
  - Redes

Nodo

- Estado de un servidor local
  - Carga (cpu)
  - Memoria
  - Discos
    - Espacio
    - I/O
  - Otros
    - Uptime
    - Procesos
    - Usuarios
    - Puertos
    - File descriptors (inodos)

Nodo

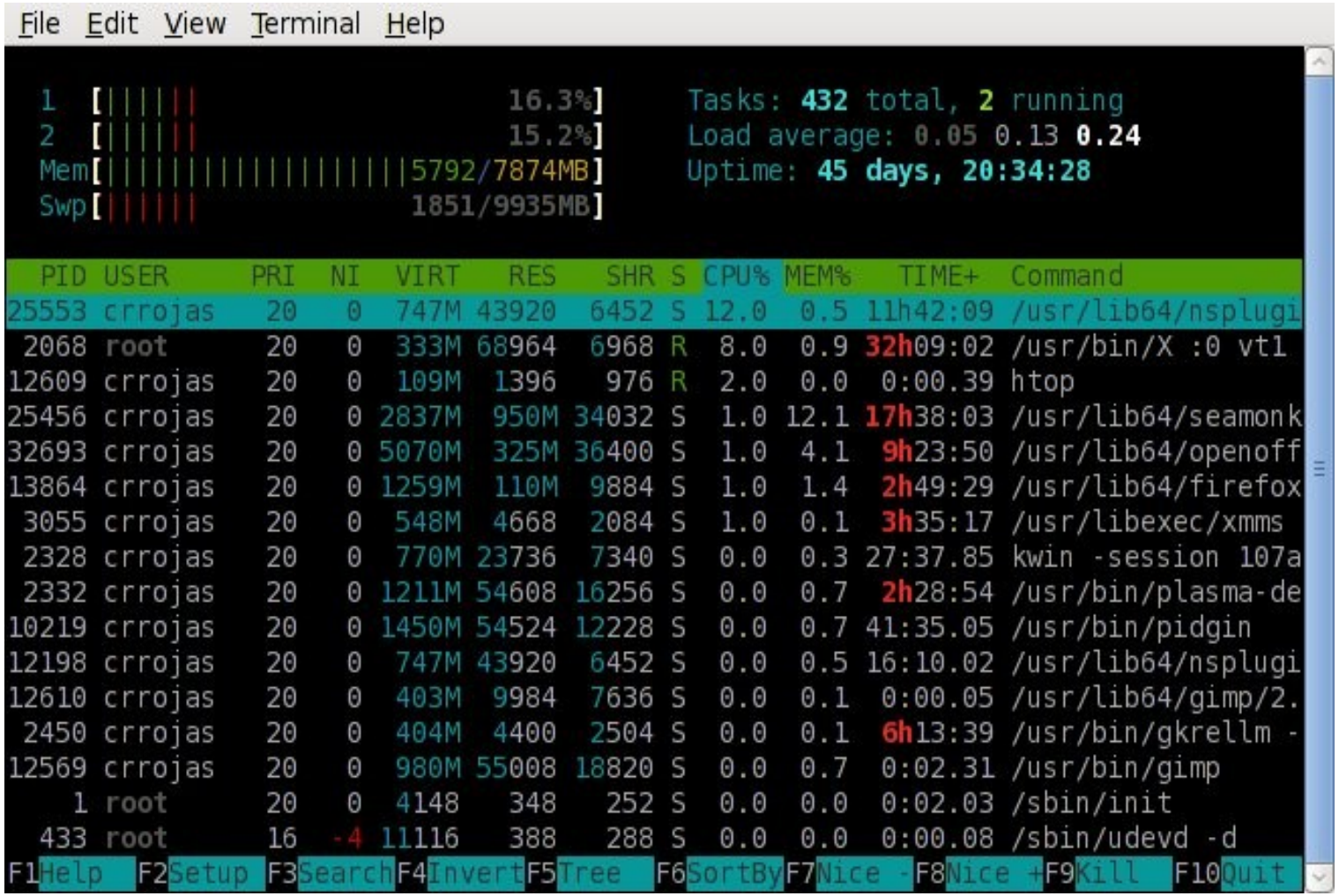
- Herramientas (*) Generalmente son de distribución
  - top (*)
    - muestra puntos de carga, % uso cpu, memoria disponible
  - htop
    - idem
  - df (*)
    - muestra espacio disponible en las particiones del sistema. Puede mostrar los inodos disponibles
  - du
    - Permite ver el tamaño de los directorios
  - discus
    - similar a df, pero más intuitivo

top

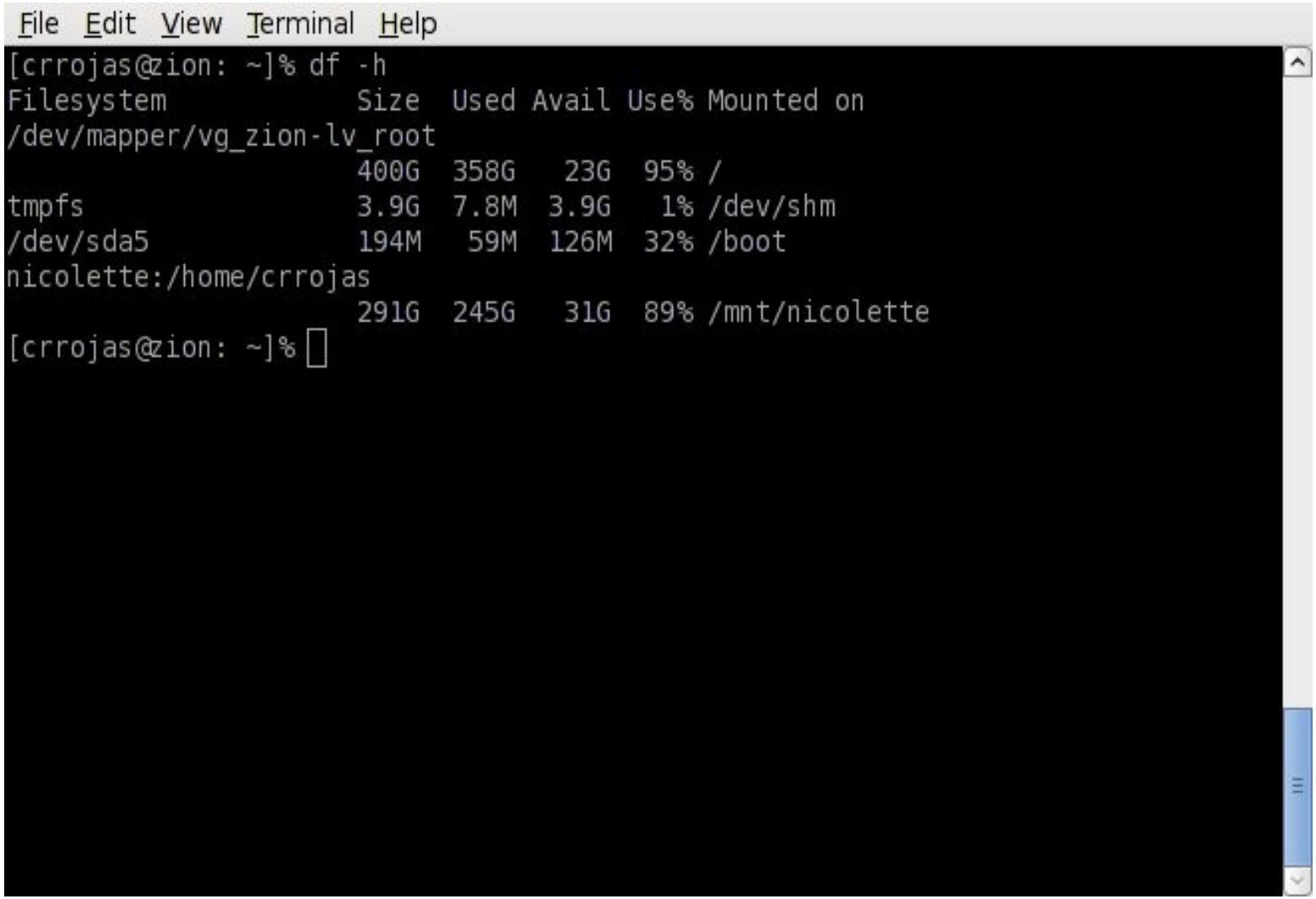
File Edit View Terminal Help

```
top - 11:53:51 up 45 days, 20:33, 61 users,  load average: 0.14, 0.16, 0.26
Tasks: 317 total,   3 running, 313 sleeping,   0 stopped,   1 zombie
Cpu(s): 11.3%us,  4.9%sy,  0.0%ni, 83.4%id,  0.3%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   8063316k total,  7538904k used,   524412k free,   198056k buffers
Swap: 10174456k total,  1896356k used,  8278100k free,  1415948k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
25553 crrojas   20   0  747m  43m 6452 R 13.6  0.5 788:48.67 npviewer.bin
 2068 root      20   0  334m  67m 6936 R 10.3  0.9   1928:56 X
25456 crrojas   20   0 2837m 950m  33m S  1.7 12.1   1098:54 seamonkey-bin
32693 crrojas   20   0 5070m 325m  35m S  1.7  4.1 578:17.74 scalc.bin
 2328 crrojas   20   0  770m  23m 7340 S  1.0  0.3  27:37.48 kwin
10219 crrojas   20   0 1450m  53m  11m S  1.0  0.7  41:53.76 pidgin
13864 crrojas   20   0 1259m 110m 9884 S  1.0  1.4 178:52.84 firefox
 2332 crrojas   20   0 1211m  53m  15m S  0.7  0.7 197:48.86 plasma-desktop
 2450 crrojas   20   0  404m 4400 2504 S  0.7  0.1 373:39.19 gkrellm
 4018 crrojas    9 -11  505m 9192 7996 S  0.7  0.1 445:34.59 pulseaudio
12561 crrojas   20   0 15060 1332  864 R  0.7  0.0   0:00.12 top
 2442 crrojas   20   0  651m  88m 6760 S  0.3  1.1  66:00.69 konsole
 3055 crrojas   20   0  548m 4668 2084 S  0.3  0.1 224:29.13 xmms
12522 crrojas   20   0  430m  12m 9136 S  0.3  0.2   0:00.27 gnome-terminal
12573 crrojas   20   0  401m 9976 7636 S  0.3  0.1   0:00.06 screenshot
15979 crrojas   20   0  231m 3360  832 S  0.3  0.0   7:37.08 synergys
25468 crrojas   20   0 15060  904  476 S  0.3  0.0  61:37.12 top
```

htop


File Edit View Terminal Help
1 [|||||| 16.3%]
2 [|||||| 15.2%]
Mem[||||||||||||||||||5792/7874MB]
Swp[|||||| 1851/9935MB]
Tasks: 432 total, 2 running
Load average: 0.05 0.13 0.24
Uptime: 45 days, 20:34:28
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
25553 crrojas 20 0 747M 43920 6452 S 12.0 0.5 11h42:09 /usr/lib64/nsplugi
2068 root 20 0 333M 68964 6968 R 8.0 0.9 32h09:02 /usr/bin/X :0 vt1
12609 crrojas 20 0 109M 1396 976 R 2.0 0.0 0:00.39 htop
25456 crrojas 20 0 2837M 950M 34032 S 1.0 12.1 17h38:03 /usr/lib64/seamonk
32693 crrojas 20 0 5070M 325M 36400 S 1.0 4.1 9h23:50 /usr/lib64/openoff
13864 crrojas 20 0 1259M 110M 9884 S 1.0 1.4 2h49:29 /usr/lib64/firefox
3055 crrojas 20 0 548M 4668 2084 S 1.0 0.1 3h35:17 /usr/libexec/xmms
2328 crrojas 20 0 770M 23736 7340 S 0.0 0.3 27:37.85 kwin -session 107a
2332 crrojas 20 0 1211M 54608 16256 S 0.0 0.7 2h28:54 /usr/bin/plasma-de
10219 crrojas 20 0 1450M 54524 12228 S 0.0 0.7 41:35.05 /usr/bin/pidgin
12198 crrojas 20 0 747M 43920 6452 S 0.0 0.5 16:10.02 /usr/lib64/nsplugi
12610 crrojas 20 0 403M 9984 7636 S 0.0 0.1 0:00.05 /usr/lib64/gimp/2.
2450 crrojas 20 0 404M 4400 2504 S 0.0 0.1 6h13:39 /usr/bin/gkrellm -
12569 crrojas 20 0 980M 55008 18820 S 0.0 0.7 0:02.31 /usr/bin/gimp
1 root 20 0 4148 348 252 S 0.0 0.0 0:02.03 /sbin/init
433 root 16 -4 11116 388 288 S 0.0 0.0 0:00.08 /sbin/udevd -d
F1Help F2Setup F3Search F4Invert F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit

df


File Edit View Terminal Help
[crrojas@zion: ~]% df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg_zion-lv_root
400G 358G 23G 95% /
tmpfs 3.9G 7.8M 3.9G 1% /dev/shm
/dev/sda5 194M 59M 126M 32% /boot
nicolette:/home/crrojas
291G 245G 31G 89% /mnt/nicolette
[crrojas@zion: ~]%

du

File Edit View Terminal Help

```
[crrojas@zion: /tmp]% du -h -s *
632K    01.jpg
4.0K    1
4.0K    11
8.0K    1294683610.26287_0.mail.nic.cl:2,S
0       1PKbAIns.zip.part
4.0K    2
4.0K    22NDRV.tmp
16K     31518
12K     31518.2
12K     31518.dec
16K     36426
12K     36426.2
12K     36426.dec
16K     37453
12K     37453.dec
16K     38374
12K     38374.dec
0       4d8a7703af49c
0       4d8a77057701d
0       4d8a77160b200
0       4d9dd71d2dfa3
0       4d9dd71d47233
0       4d9dd71d482a1
```

Nodo

- Herramientas
  - gkrell
    - Monitor gráfico de cpu, memoria, disco, etc.
  - iostat (sysstat)
    - Muestra estadísticas sobre el I/O del sistema
  - iotop
    - Similar, pero continuo
  - nmap (*)
    - Herramienta para ver puertos abiertos en un servidor

gkrellm


zion
Ion 23 Ma
11:58 31
18%
CPU0
27%
CPU1
512 procs
61 users
Proc
0
sda
0
sdb
eth0
0:00
Mem
Swap
-/-
45d 20:38

iostat

File Edit View Terminal Help

```
[crrojas@morpheus ~]$ iostat
Linux 2.6.32.26-175.fc12.x86_64 (morpheus)      05/23/2011      _x86_64_      (
2 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           2.30    0.00    3.79    9.13    0.00   84.78

Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sda              28.75      1431.56       130.81     544510      49754
dm-0              0.90         6.97         0.21       2650         80
dm-1             11.89        79.38        22.15      30194       8424
dm-2             54.97      1225.41       108.40     466098      41232
dm-3              0.66         5.28         0.00       2008          0

[crrojas@morpheus ~]$
```

iotop

File Edit View Terminal Help

```
Total DISK READ:  0.00 B/s | Total DISK WRITE:  31.00 K/s
  TID  PRIO  USER     DISK READ  DISK WRITE  SWAPIN     IO>    COMMAND
  403 be/3 root        0.00 B/s   15.50 K/s  0.00 %  7.14 % [jbd2/dm-2-8]
  382 be/4 root        0.00 B/s    0.00 B/s  0.00 %  7.07 % [kdmflush]
    1 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % init
    2 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kthreadd]
    3 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/0]
    4 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/0]
    5 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/0]
    6 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [migration/1]
    7 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [ksoftirqd/1]
    8 rt/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [watchdog/1]
    9 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [events/0]
   10 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [events/1]
   11 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [cpuset]
   12 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [khelper]
   13 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [netns]
   14 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [async/mgr]
   15 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [pm]
   16 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [sync_supers]
   17 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [bdi-default]
   18 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kintegrityd/0]
   19 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kintegrityd/1]
   20 be/4 root        0.00 B/s    0.00 B/s  0.00 %  0.00 % [kblockd/0]
```

File Edit View Terminal Tabs Help

Terminal

```
[root@zion curso-sysadmin]# nmap -sS -A www.cero32.cl

Starting Nmap 5.21 ( http://nmap.org ) at 2011-05-23 16:55 CLT
Nmap scan report for www.cero32.cl (200.1.122.29)
Host is up (0.00063s latency).
rDNS record for 200.1.122.29: cero32.cl
Not shown: 993 closed ports
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 69:36:4e:26:d4:8f:5c:50:1f:c6:5c:09:0c:86:63:d3 (DSA)
|_2048 ee:0f:58:3d:1d:d1:01:a6:84:cf:85:e3:06:ce:85:6a (RSA)
53/tcp   open     domain
80/tcp   open     http         Apache httpd 2.2.3 ((CentOS))
|_html-title: cero32 . cl
139/tcp  filtered netbios-ssn
179/tcp  filtered bgp
445/tcp  filtered microsoft-ds
3306/tcp open     mysql        MySQL 5.0.77
| mysql-info: Protocol: 10
| Version: 5.0.77
| Thread ID: 1147
| Some Capabilities: Connect with DB, Compress, Transactions, Secure Connection
| Status: Autocommit
|_Salt: BFwG<7=l*).Mv/$bFvA}
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.28
Network Distance: 3 hops

TRACEROUTE (using port 135/tcp)
HOP RTT     ADDRESS
1   0.25 ms cisco.intra.nic.cl (172.30.10.1)
2   0.47 ms ciscoa1.intra.nic.cl (172.30.177.3)
3   0.79 ms cero32.cl (200.1.122.29)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.17 seconds
[root@zion curso-sysadmin]#
```

Servicios

- Si el servidor (SO) funciona bien, pasamos a los servicios:
  - Web
  - Correo
  - BD
  - DNS
  - Servicios propios
  - otros

Monitoreo Web

- La mayoría de los monitores se basa en los logs
  - Importante loggear todo lo posible
  - Lo típico es tener un log de acceso y un log de errores.
  - Eventualmente 2 más para accesos seguros (https)

Monitoreo Web

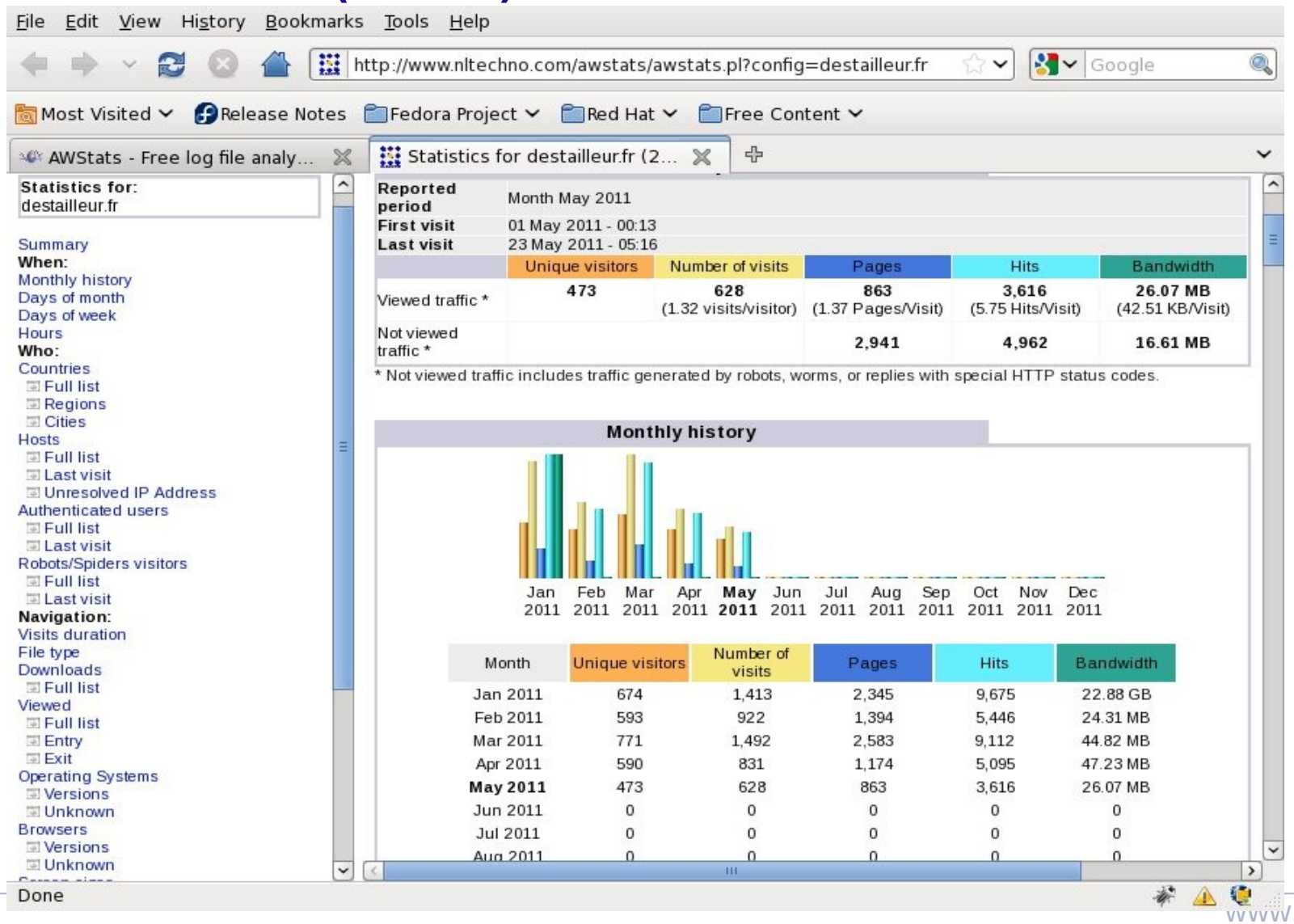
- Herramientas
  - apachetop
    - similar a top, pero muestra los request a un servidor web
  - awstats
    - Análisis de logs
  - less/grep/tail etc
  - aplicaciones pagadas

apachetop

File Edit View Terminal Help

```
last hit: 16:11:44          atop runtime:  0 days, 00:01:37              16:12:01
All:           10 reqs (   0.1/sec)         95.4K ( 1205.5B/sec)    9764.3B/req
2xx:        5 (50.0%) 3xx:        4 (40.0%) 4xx:      1 (10.0%) 5xx:      0 ( 0.0%)
R ( 30s):       6 reqs (   0.2/sec)         37.3K ( 1274.7B/sec)    6373.7B/req
2xx:        2 (33.3%) 3xx:        4 (66.7%) 4xx:      0 ( 0.0%) 5xx:      0 ( 0.0%)

 REQS REQ/S    KB KB/S URL
    1  0.06  31.3  1.7*/
    1  0.06   0.0  0.0 /templates/pilot_3_theme/css/default.css,niftycorners.css,index_left.c
    1  0.06   0.0  0.0 /templates/pilot_3_theme/js/location.js,iepngfix_tilebg.js,jquery-1.4.
    1  0.06   0.0  0.0 /uploades/icons/thumb_28_568300fa.jpg
    1  0.06   0.0  0.0 /uploades/icons/thumb_27_ce877b89.jpg
    1  0.06   6.1  0.4 /uploades/icons/big_thumb_11_e32bc902.jpg
```

awstats (web)


File Edit View History Bookmarks Tools Help
http://www.nltechno.com/awstats/awstats.pl?config=destailleur.fr
Google
Most Visited
Release Notes
Fedora Project
Red Hat
Free Content
AWStats - Free log file analy...
Statistics for destailleur.fr (2...
Statistics for:
destailleur.fr
Summary
When:
Monthly history
Days of month
Days of week
Hours
Who:
Countries
Full list
Regions
Cities
Hosts
Full list
Last visit
Unresolved IP Address
Authenticated users
Full list
Last visit
Robots/Spiders visitors
Full list
Last visit
Navigation:
Visits duration
File type
Downloads
Full list
Viewed
Full list
Entry
Exit
Operating Systems
Versions
Unknown
Browsers
Versions
Unknown
Reported period Month May 2011
First visit 01 May 2011 - 00:13
Last visit 23 May 2011 - 05:16
Unique visitors | Number of visits | Pages | Hits | Bandwidth
Viewed traffic * 473 | 628 (1.32 visits/visitor) | 863 (1.37 Pages/Visit) | 3,616 (5.75 Hits/Visit) | 26.07 MB (42.51 KB/Visit)
Not viewed traffic * | | 2,941 | 4,962 | 16.61 MB
* Not viewed traffic includes traffic generated by robots, worms, or replies with special HTTP status codes.
Monthly history
Jan 2011 Feb 2011 Mar 2011 Apr 2011 May 2011 Jun 2011 Jul 2011 Aug 2011 Sep 2011 Oct 2011 Nov 2011 Dec 2011
Month | Unique visitors | Number of visits | Pages | Hits | Bandwidth
Jan 2011 | 674 | 1,413 | 2,345 | 9,675 | 22.88 GB
Feb 2011 | 593 | 922 | 1,394 | 5,446 | 24.31 MB
Mar 2011 | 771 | 1,492 | 2,583 | 9,112 | 44.82 MB
Apr 2011 | 590 | 831 | 1,174 | 5,095 | 47.23 MB
May 2011 | 473 | 628 | 863 | 3,616 | 26.07 MB
Jun 2011 | 0 | 0 | 0 | 0 | 0
Jul 2011 | 0 | 0 | 0 | 0 | 0
Aug 2011 | 0 | 0 | 0 | 0 | 0
Done

Monitoreo del Correo

- Los logs son la principal fuente de información.
- mailq
  - Analiza la cola de correos.
- qshape
  - idem
- awstats
  - graficos de logs
- mailgraph
  - idem

mailq

File Edit View Terminal Help

```
[root@morpheus ~]# mailq
/var/spool/mqueue is empty
                Total requests: 0
[root@morpheus ~]# mailq -Ac
/var/spool/clientmqueue is empty
                Total requests: 0
[root@morpheus ~]#
```

Monitoreo BD

- Las BD = datos. Si fallan puede ser la muerte de una empresa
- consistencia
- espacio en disco
- carga
- queries

Monitoreo BD

- mytop
  - clone de top
- inntop
  - idem
- query profiler
  - Revisión de queries
- check_prostgres
  - tamaños de tablas, transacciones, locks, etc
- pgFouine
  - analizar logs

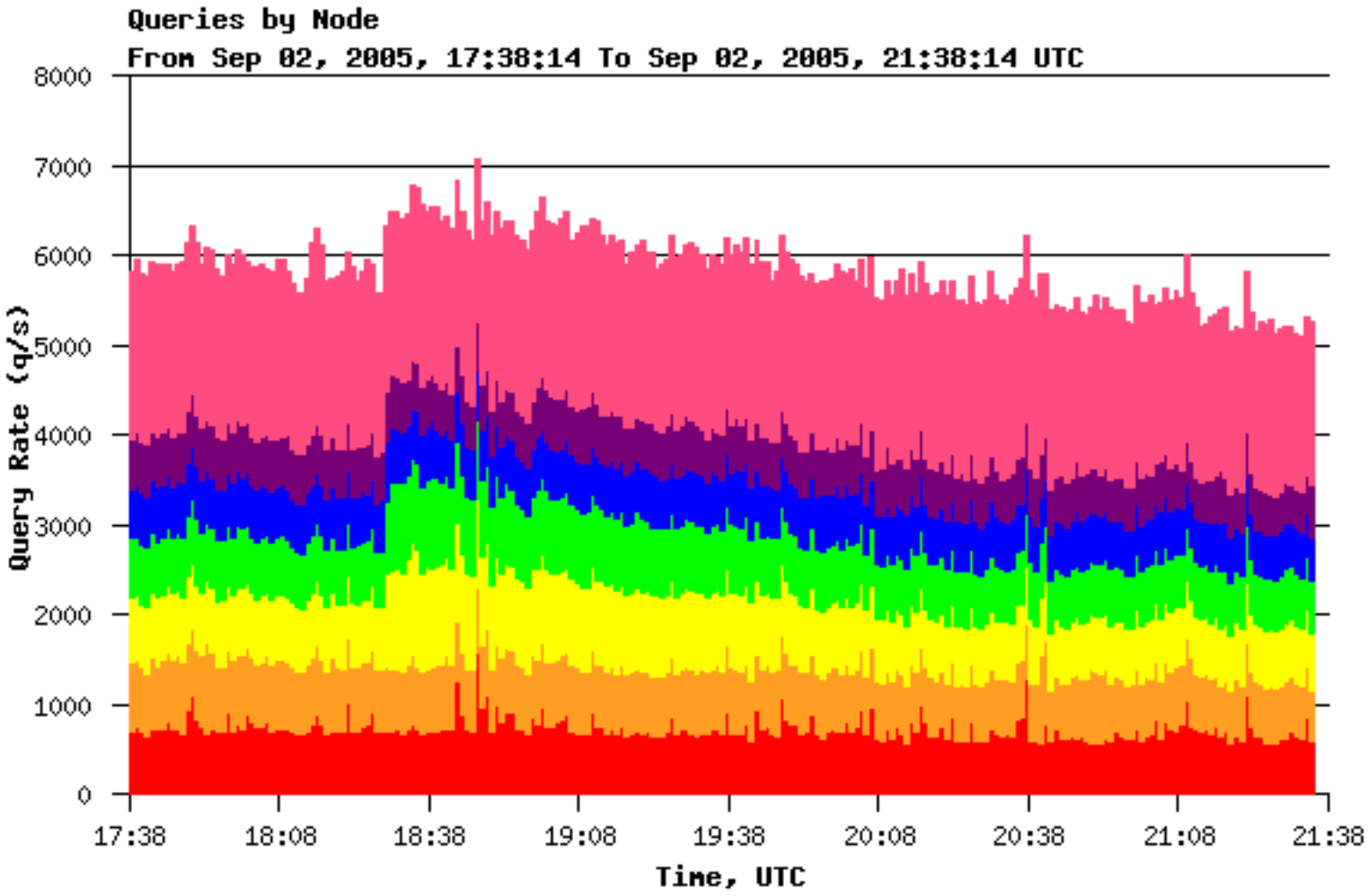
mytop


File Edit View Terminal Help
MySQL on localhost (5.1.47-log) up 0+00:17:44 [12:18:33]
Queries: 571.0 qps: 1 Slow: 0.0 Se/In/Up/De(%): 43/06/11/03
qps now: 11 Slow qps: 0.0 Threads: 1 (1/ 0) 04/00/00/00
Key Efficiency: 85.2% Bps in/out: 52.2/334.1 Now in/out: 462.1/ 9.1k
Id User Host/IP DB Time Cmd Query or State
18 root localhost test 0 Query show full processlist

Monitoreo DNS

- DNS es una pieza vital, pero poca gente le da la importancia que merece
  - dnstop
    - Otra herramienta tipo top
  - dsc
    - graficos en tiempo real sobre cantidas y tipo de consulta

dsc


Queries by Node
From Sep 02, 2005, 17:38:14 To Sep 02, 2005, 21:38:14 UTC
Query Rate (q/s)
8000
7000
6000
5000
4000
3000
2000
1000
0
17:38
18:08
18:38
19:08
19:38
20:08
20:38
21:08
21:38
Time, UTC

Monitoreo otros Servicios

- Depende del servicio.
- Monitoreos a la medida
- Tratar de no reinventar la rueda

Monitoreo Red

- El correcto funcionamiento de la red es vital y transversal a todas las aplicaciones
  - Visibilidad
    - Monitoreo nodo – mundo
    - Monitoreo mundo – nodo
  - Cantidad de tráfico
  - Ancho de banda
  - Ruteo

Monitoreo Red

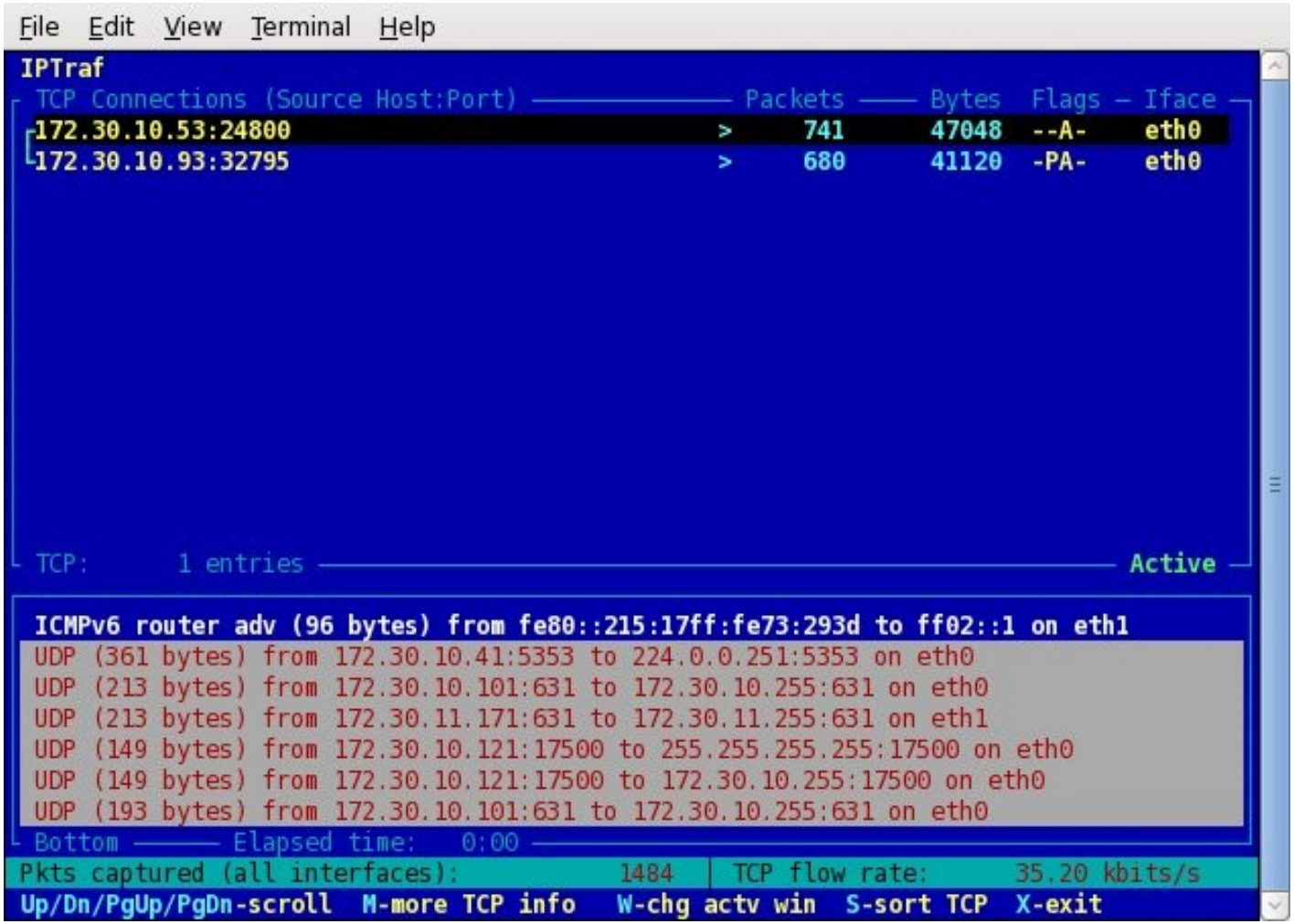
- ping/ping6
  - tiempo de respuesta
- traceroute/traceroute6
  - Muestra la ruta que sigue un paquete para llegar a destino
- iptraf
  - muestra varios datos sobre el trafico de las interfaces de red
- iperf
  - permite realizar mediones de ancho de banda entre 2 nodos.

pig / traceroute

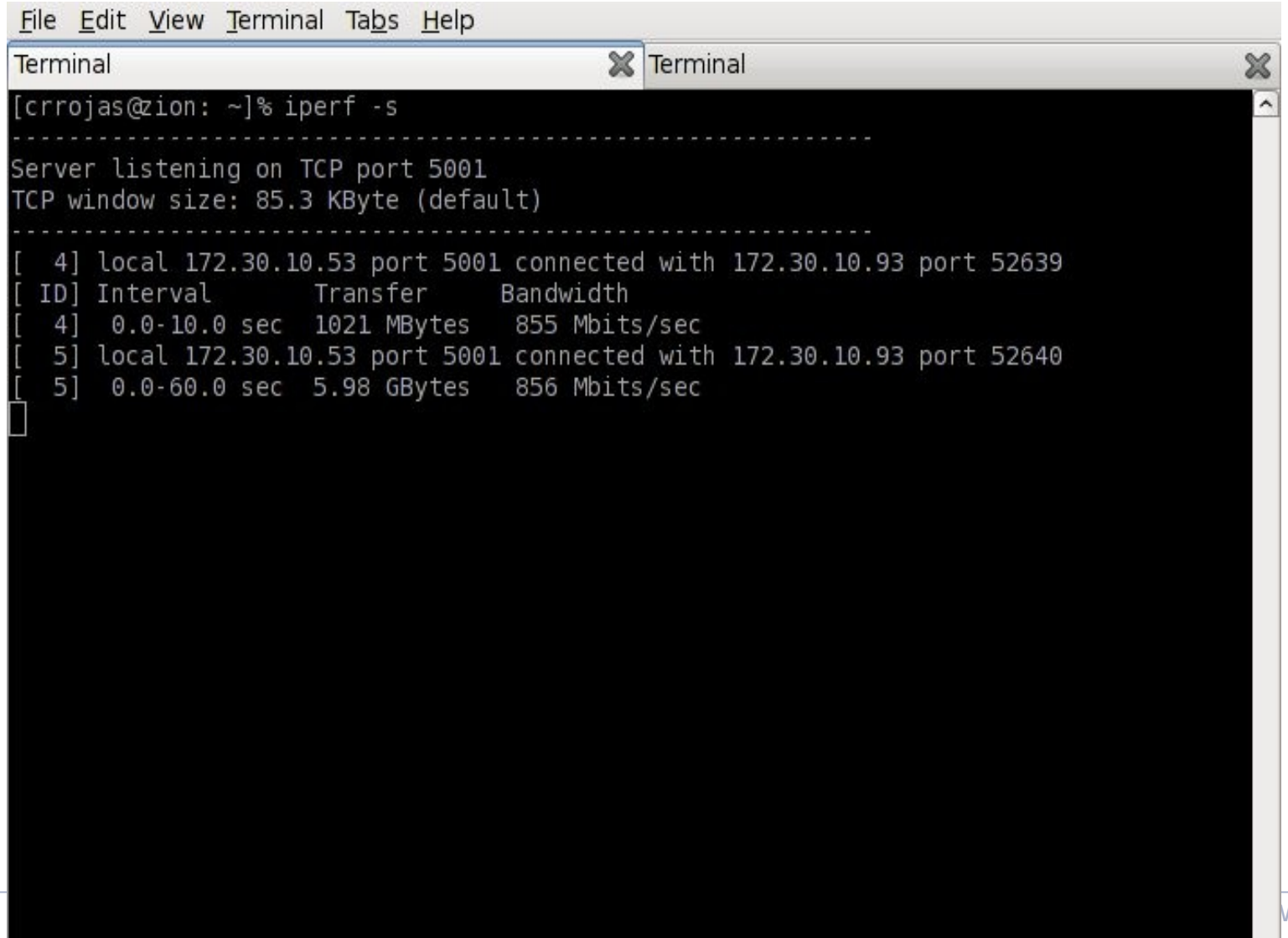
File Edit View Terminal Help

```
[crrojas@zion: ~]% traceroute www.latercera.com
traceroute to www.latercera.com (200.91.29.45), 30 hops max, 60 byte packets
 1  cisco.intra.nic.cl (172.30.10.1)  0.160 ms  0.145 ms  0.173 ms
 2  190.208.0.233 (190.208.0.233)  0.758 ms  0.754 ms  0.748 ms
 3  190.208.5.65 (190.208.5.65)  0.835 ms  0.830 ms  0.912 ms
 4  Ge0-0-2.pit-c12410.Santiago.ip.telmexchile.cl (200.27.103.82)  1.018 ms  1.010 m
s  1.007 ms
 5  gw-napmundo.mundo.movistar.cl (200.91.13.1)  1.352 ms  1.393 ms  1.438 ms
 6  gw2-copesa.cust.movistar.cl (200.91.13.102)  1.832 ms  1.528 ms  1.711 ms
 7  * * *
 8  200.91.29.45 (200.91.29.45)  1.690 ms  1.494 ms  1.770 ms
[crrojas@zion: ~]% ping www.latercera.com
PING vs01f5.latercera.com (200.91.29.77) 56(84) bytes of data.
64 bytes from 200.91.29.77: icmp_seq=1 ttl=248 time=1.83 ms
64 bytes from 200.91.29.77: icmp_seq=2 ttl=248 time=1.44 ms
64 bytes from 200.91.29.77: icmp_seq=3 ttl=248 time=1.95 ms
^C
--- vs01f5.latercera.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2238ms
rtt min/avg/max/mdev = 1.441/1.741/1.953/0.223 ms
[crrojas@zion: ~]% ping6 www6.nic.cl
PING www6.nic.cl(2001:1398:1::6003) 56 data bytes
64 bytes from 2001:1398:1::6003: icmp_seq=1 ttl=62 time=2.32 ms
64 bytes from 2001:1398:1::6003: icmp_seq=2 ttl=62 time=0.587 ms
^C
--- www6.nic.cl ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1100ms
rtt min/avg/max/mdev = 0.587/1.455/2.324/0.869 ms
[crrojas@zion: ~]%
```

iptraf


File Edit View Terminal Help
IPTraf
TCP Connections (Source Host:Port) Packets Bytes Flags Iface
172.30.10.53:24800 > 741 47048 --A- eth0
172.30.10.93:32795 > 680 41120 -PA- eth0
TCP: 1 entries Active
ICMPv6 router adv (96 bytes) from fe80::215:17ff:fe73:293d to ff02::1 on eth1
UDP (361 bytes) from 172.30.10.41:5353 to 224.0.0.251:5353 on eth0
UDP (213 bytes) from 172.30.10.101:631 to 172.30.10.255:631 on eth0
UDP (213 bytes) from 172.30.11.171:631 to 172.30.11.255:631 on eth1
UDP (149 bytes) from 172.30.10.121:17500 to 255.255.255.255:17500 on eth0
UDP (149 bytes) from 172.30.10.121:17500 to 172.30.10.255:17500 on eth0
UDP (193 bytes) from 172.30.10.101:631 to 172.30.10.255:631 on eth0
Bottom Elapsed time: 0:00
Pkts captured (all interfaces): 1484 TCP flow rate: 35.20 kbits/s
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit

iperf (servidor)



iperf (cliente)

File Edit View Terminal Help

```
[root@morpheus ~]# iperf -c 172.30.10.53
------------------------------------------------------------
Client connecting to 172.30.10.53, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 172.30.10.93 port 52639 connected with 172.30.10.53 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1021 MBytes   857 Mbits/sec
[root@morpheus ~]# iperf -c 172.30.10.53 -t 60
------------------------------------------------------------
Client connecting to 172.30.10.53, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 172.30.10.93 port 52640 connected with 172.30.10.53 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-60.0 sec  5.98 GBytes   857 Mbits/sec
[root@morpheus ~]#
```

Monitoreo

- Es infactible monitorear todo “a mano”
- Hay herramientas que agrupan múltiples monitoreos:
  - Nagios
    - Puede revisar múltiples aplicaciones en diversos servidores. Multiples plugins. Configurable
  - Cacti
    - Es la versión mejorada de nagios.
  - Hyperic HQ
    - Similar a los anteriores
- Otras aplicaciones pagadas que tienen objetivos similares

nagios

Service Status

All services

Host Status Summary

Up	Down	Unreachable	Pending
17	13	1	1
Unhandled	**Problems**		**All**
13	14		32

Last Updated: 2011-04-09 11:17:54

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
74	4	8	56	1
Unhandled	**Problems**			**All**
46	68			143

Last Updated: 2011-04-09 11:17:55

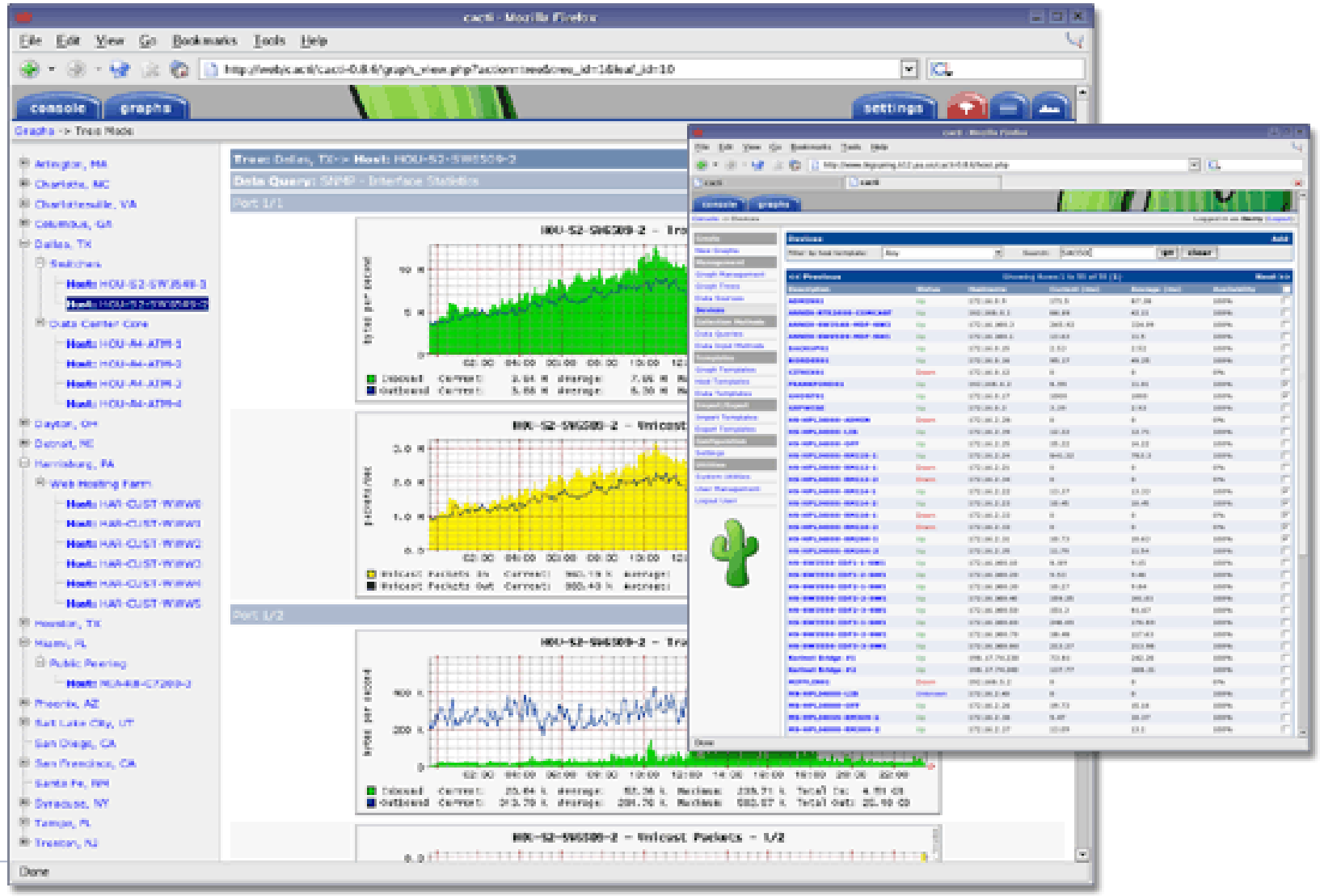
Search... Go

Showing 1-25 of 46 total records

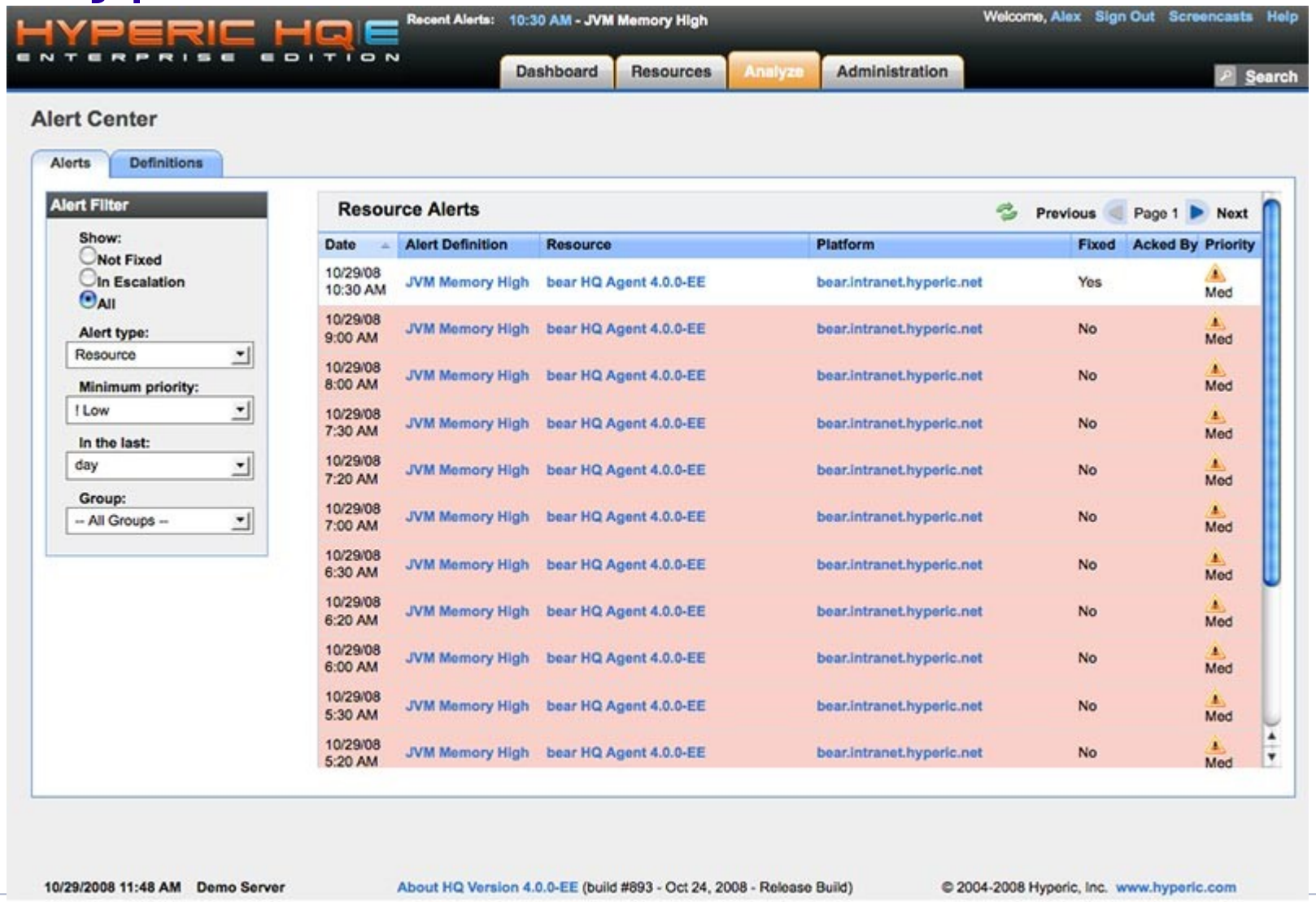
Filters: **Host**=Up **Service**=Warning,Unknown,Critical,Not Acknowledged,Not In Downtime

Host	Service	Status	Duration	Attempt	Last Check	Status Information
mstarr	Memory Usage	Critical	234d 6h 44m 45s	5/5	2011-04-09 11:17:19	CRITICAL - Socket timeout after 10 seconds
	test	Critical	234d 6h 43m 24s	5/5	2011-04-09 11:17:19	CRITICAL - Socket timeout after 10 seconds
	Drive C: Disk Usage	Critical	234d 6h 45m 36s	5/5	2011-04-09 11:17:19	CRITICAL - Socket timeout after 10 seconds
	FTP	Critical	234d 6h 44m 50s	5/5	2011-04-09 11:17:19	CRITICAL - Socket timeout after 10 seconds
	CPU Usage	Critical	234d 6h 46m 27s	5/5	2011-04-09 11:17:19	CRITICAL - Socket timeout after 10 seconds
192.168.1.253	Port 9 Status	Critical	82d 1h 35m 28s	5/5	2011-04-09 11:17:14	CRITICAL: Interface EtherNet Port on unit 1, port:9 (index 9) down due to lower layer being down.
www.cnn.com	Web Transaction	Critical	1m 7s	1/5	2011-04-09 11:16:47	WebInject CRITICAL - Test case number 1 failed
192.168.1.253	Port 26 Status	Critical	131d 19h 21m 46s	5/5	2011-04-09 11:16:09	CRITICAL: Interface EtherNet Port on unit 1, port:26 (index 26) down due to lower layer being down.
	Port 21 Status	Critical	131d 19h 23m 2s	5/5	2011-04-09 11:16:09	CRITICAL: Interface EtherNet Port on unit 1, port:21 (index 21) down due to lower layer being down.
	Port 12 Status	Critical	72d 3h 56m 45s	5/5	2011-04-09 11:16:09	CRITICAL: Interface EtherNet Port on unit 1, port:12 (index 12) down due to lower layer being down.
	Port 7 Status	Critical	72d 3h 56m 44s	5/5	2011-04-09 11:16:03	CRITICAL: Interface EtherNet Port on unit 1, port:7 (index 7) down due to lower layer being down.
www.nagios.com	HTTP	Warning	12m 35s	5/5	2011-04-09 11:15:19	HTTP WARNING: HTTP/1.1 404 Not Found
localhost	MySQL InnoDB Buffer Pool Hit Rate	Critical	234d 6h 48m 50s	5/5	2011-04-09 11:15:11	(Return code of 127 is out of bounds - plugin may be missing)
192.168.1.4	SQL Server	Unknown	28d 10h 57m 56s	5/5	2011-04-09 11:15:11	NSClient - ERROR: Invalid password.
192.168.1.253	Port 8 Status	Critical	131d 19h 23m 2s	5/5	2011-04-09 11:15:11	CRITICAL: Interface EtherNet Port on unit 1, port:8 (index 8) down due to lower layer being down.
	Port 19 Status	Critical	131d 19h 23m 11s	5/5	2011-04-09 11:15:00	CRITICAL: Interface EtherNet Port on unit 1, port:19 (index 19)

cacti


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
console
graphs
settings
Graphs -> Tree Mode
Done

Hyperic HQ


HYPERIC HQE
ENTERPRISE EDITION
Recent Alerts: 10:30 AM - JVM Memory High
Welcome, Alex Sign Out Screencasts Help
Dashboard Resources Analyze Administration
Search
Alert Center
Alerts Definitions
Alert Filter
Show:
Not Fixed
In Escalation
All
Alert type:
Resource
Minimum priority:
! Low
In the last:
day
Group:
-- All Groups --
Resource Alerts
Previous Page 1 Next
Date Alert Definition Resource Platform Fixed Acked By Priority
10/29/08 10:30 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net Yes Med
10/29/08 9:00 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 8:00 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 7:30 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 7:20 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 7:00 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 6:30 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 6:20 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 6:00 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 5:30 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/08 5:20 AM JVM Memory High bear HQ Agent 4.0.0-EE bear.intranet.hyperic.net No Med
10/29/2008 11:48 AM Demo Server
About HQ Version 4.0.0-EE (build #893 - Oct 24, 2008 - Release Build)
© 2004-2008 Hyperic, Inc. www.hyperic.com

Monitoreo

- ¿Qué hacer cuando algo falla?
  - Definir políticas de alertas
  - Grupos de operación con roles
  - distintos niveles de alertas (error en pantalla/ salida estandar / mail / celular, etc)
- Objetivo debe ser, como mínimo, cumplir con SLA.
- SLA debe ser realista

Monitoreo

- Smokeping
  - “ping” con historia a diversos servicios/ servidores
- Diversos scripts a medida (shell / perl / python, etc)

smokeping

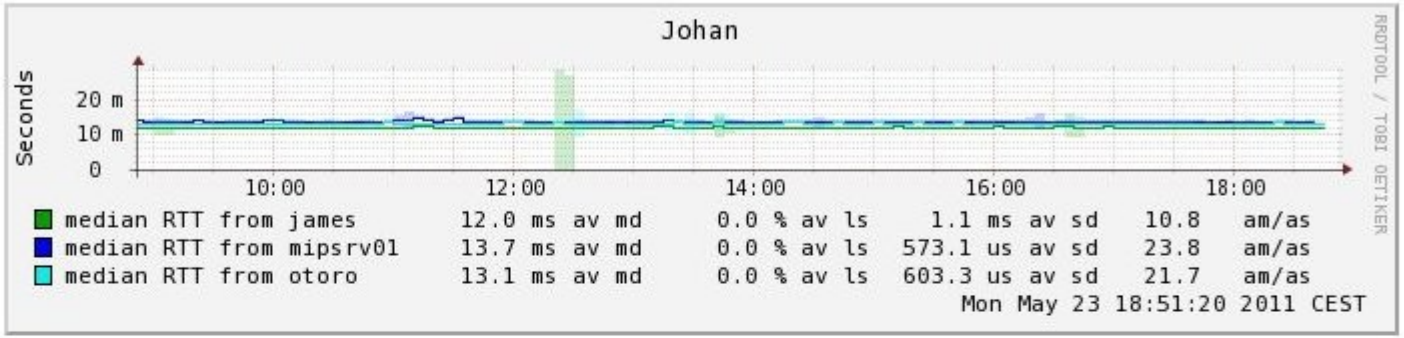
SmokePing Targets:

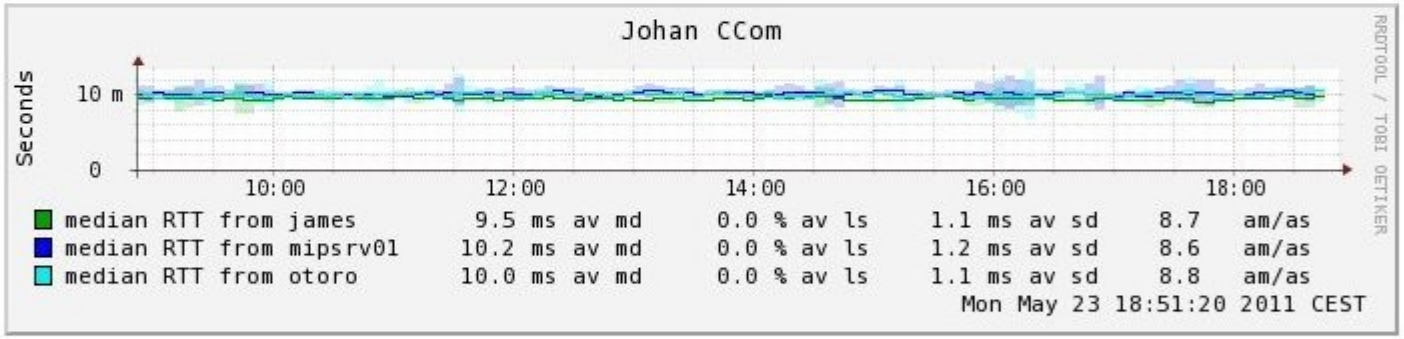
Hierarchy: Default Hierarchy

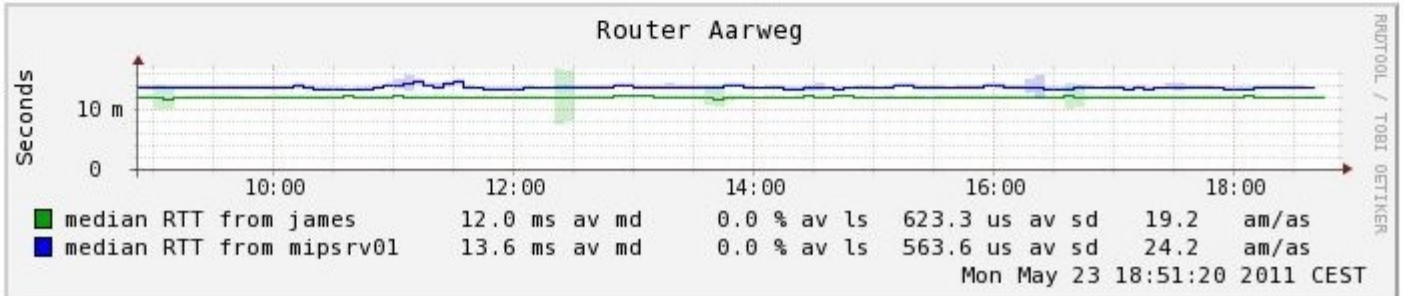
Filter:

- Charts
- O+P Managed
  - BCP *
  - Horyzon *
  - MEROF
  - ESPROS Boxes
  - Ivic *
  - IT'IS Boxes
  - ODELPMOK *
  - PNN *
  - LSA Servers
  - MOBIFLICK
  - MIP
  - O+P Internal
    - Johan *
    - Johan CCom *
    - Router Aarweg *
    - James *
    - James Console *
    - Henry *
    - Henry Console *
    - james-vm *
    - Zimbox *
- O+P Home
- World
- Root Name Servers
- Multi Target Graphs
- VoipGateway *

O+P AG Servers







Cómo diagnosticar una falla

- Escuchar a los usuarios
  - 99% es problema de ellos
  - 1% no lo es
- Recolectar toda la información que sea necesaria para identificar la falla
  - Tratar de almacenar logs relevantes
- Existen diversas herramientas que pueden ayudar al diagnóstico

Cómo diagnosticar una falla

- tcpdump
  - sniffer para paquetes de red. Puede utilizar diversos filtros.
- wireshark
  - lo mismo anterior pero gráfico (no siempre hay ambiente gráfico)
- telnet
  - abre conexiones tcp a puertos en host indicado (texto plano)
- nc
  - Puede hacer lo mismo de telnet, perto además maneja udp

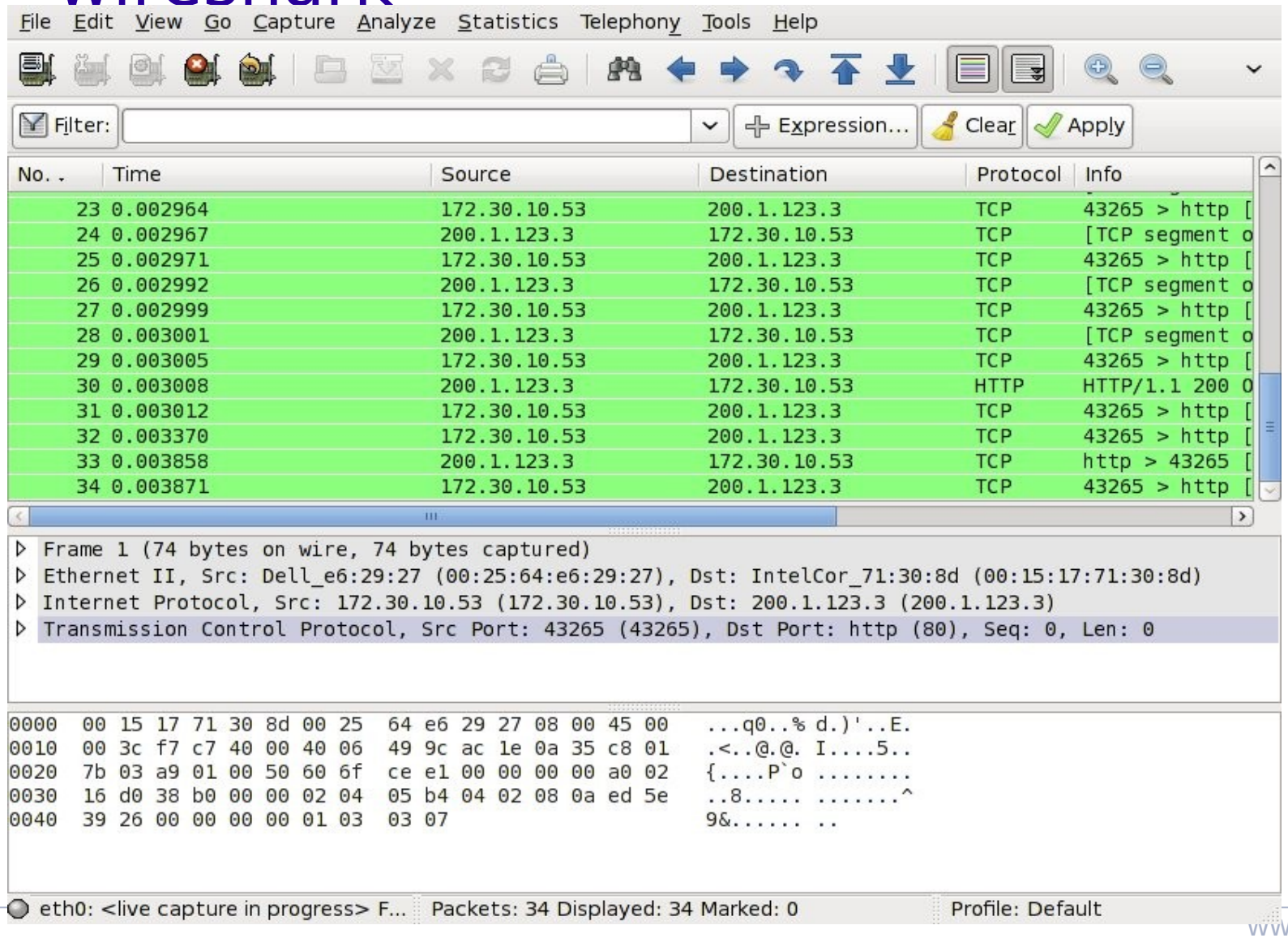
tcpdump

File Edit View Terminal Tabs Help

Terminal | Terminal

```
[root@zion crrojas]# tcpdump -ni any port 80 and host www.nic.cl
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 65535 bytes
16:29:08.941595 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [S.], seq 1313542240, ack 1
006982716, win 5792, options [mss 1460,sackOK,TS val 459202850 ecr 3978227867,nop,wscale 7]
, length 0
16:29:08.941612 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [.], ack 1, win 46, options
 [nop,nop,TS val 3978227868 ecr 459202850], length 0
16:29:08.941749 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [P.], seq 1:109, ack 1, win
 46, options [nop,nop,TS val 3978227868 ecr 459202850], length 108
16:29:08.942226 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [.], ack 109, win 46, optio
ns [nop,nop,TS val 459202851 ecr 3978227868], length 0
16:29:08.942565 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [.], seq 1:1449, ack 109, w
in 46, options [nop,nop,TS val 459202851 ecr 3978227868], length 1448
16:29:08.942572 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [.], ack 1449, win 69, opti
ons [nop,nop,TS val 3978227869 ecr 459202851], length 0
16:29:08.942576 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [.], seq 1449:2897, ack 109
, win 46, options [nop,nop,TS val 459202851 ecr 3978227868], length 1448
16:29:08.942581 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [.], ack 2897, win 91, opti
ons [nop,nop,TS val 3978227869 ecr 459202851], length 0
16:29:08.942583 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [.], seq 2897:4345, ack 109
, win 46, options [nop,nop,TS val 459202851 ecr 3978227868], length 1448
16:29:08.942589 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [.], ack 4345, win 114, opt
ions [nop,nop,TS val 3978227869 ecr 459202851], length 0
16:29:08.943167 IP 200.1.123.3.http > 172.30.10.53.60043: Flags [.], seq 4345:5793, ack 109
, win 46, options [nop,nop,TS val 459202852 ecr 3978227869], length 1448
16:29:08.943176 IP 172.30.10.53.60043 > 200.1.123.3.http: Flags [.], ack 5793, win 137, opt
ions [nop,nop,TS val 3978227869 ecr 459202852], length 0
```

wireshark


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
23 0.002964 172.30.10.53 200.1.123.3 TCP 43265 > http [
24 0.002967 200.1.123.3 172.30.10.53 TCP [TCP segment o
25 0.002971 172.30.10.53 200.1.123.3 TCP 43265 > http [
26 0.002992 200.1.123.3 172.30.10.53 TCP [TCP segment o
27 0.002999 172.30.10.53 200.1.123.3 TCP 43265 > http [
28 0.003001 200.1.123.3 172.30.10.53 TCP [TCP segment o
29 0.003005 172.30.10.53 200.1.123.3 TCP 43265 > http [
30 0.003008 200.1.123.3 172.30.10.53 HTTP HTTP/1.1 200 O
31 0.003012 172.30.10.53 200.1.123.3 TCP 43265 > http [
32 0.003370 172.30.10.53 200.1.123.3 TCP 43265 > http [
33 0.003858 200.1.123.3 172.30.10.53 TCP http > 43265 [
34 0.003871 172.30.10.53 200.1.123.3 TCP 43265 > http [
Frame 1 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: Dell_e6:29:27 (00:25:64:e6:29:27), Dst: IntelCor_71:30:8d (00:15:17:71:30:8d)
Internet Protocol, Src: 172.30.10.53 (172.30.10.53), Dst: 200.1.123.3 (200.1.123.3)
Transmission Control Protocol, Src Port: 43265 (43265), Dst Port: http (80), Seq: 0, Len: 0
0000 00 15 17 71 30 8d 00 25 64 e6 29 27 08 00 45 00 ...q0..% d.)'..E.
0010 00 3c f7 c7 40 00 40 06 49 9c ac 1e 0a 35 c8 01 .<..@.@. I....5..
0020 7b 03 a9 01 00 50 60 6f ce e1 00 00 00 00 a0 02 {....P`o ....
0030 16 d0 38 b0 00 00 02 04 05 b4 04 02 08 0a ed 5e ..8..... ....^
0040 39 26 00 00 00 00 01 03 03 07 9&...... ..
eth0: <live capture in progress> F... Packets: 34 Displayed: 34 Marked: 0 Profile: Default

telnet

File Edit View Terminal Tabs Help

Terminal | Terminal

```
[root@zion crrojas]# telnet www.nic.cl 80
Trying 200.1.123.3...
Connected to www.nic.cl.
Escape character is '^]'.
GET /
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="es">
<head>
<TITLE>NIC Chile - Dominio CL</TITLE>
<meta name="description" content="Inscripción y manejo del dominio .cl , con autoridad dele
gada por ICANN">
<meta name="keywords" content="cl dominio dominios nic domain dns name server nombres">
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="/estilos/nic.css" rel="stylesheet" type="text/css">
<link rel="alternate" type="application/rdf+xml" title="RSS Anuncios NIC Chile" href="http:
//www.nic.cl/anuncios/anuncios.rdf">
</head>

<body bgcolor="#ffffff" text="#000000" link="blue" vlink="purple">
<table border=0 width="95%" cellpadding="5" align="center">
<tbody>
  <tr>
<td align=left valign=middle><img width="150" height="100" alt="NIC Chile" src="images/logo
-eslogan-R.png"></td>
<td valign="top" align="center">
 
</td>
    <td align=right valign=top> <a href="http://www.uchile.cl"><img border="0" src="logouch
2.jpg" width="100" height="95" alt="Universidad de Chile"></a></td>
```

Como diagnosticar una falla

- dig
  - Herramienta para consultas de dns
- nslookup
  - idem
- hping
  - Permite enviar paquetes tcp/ip personalizados. Es más un scanner de red que ping.

dig

File Edit View Terminal Tabs Help

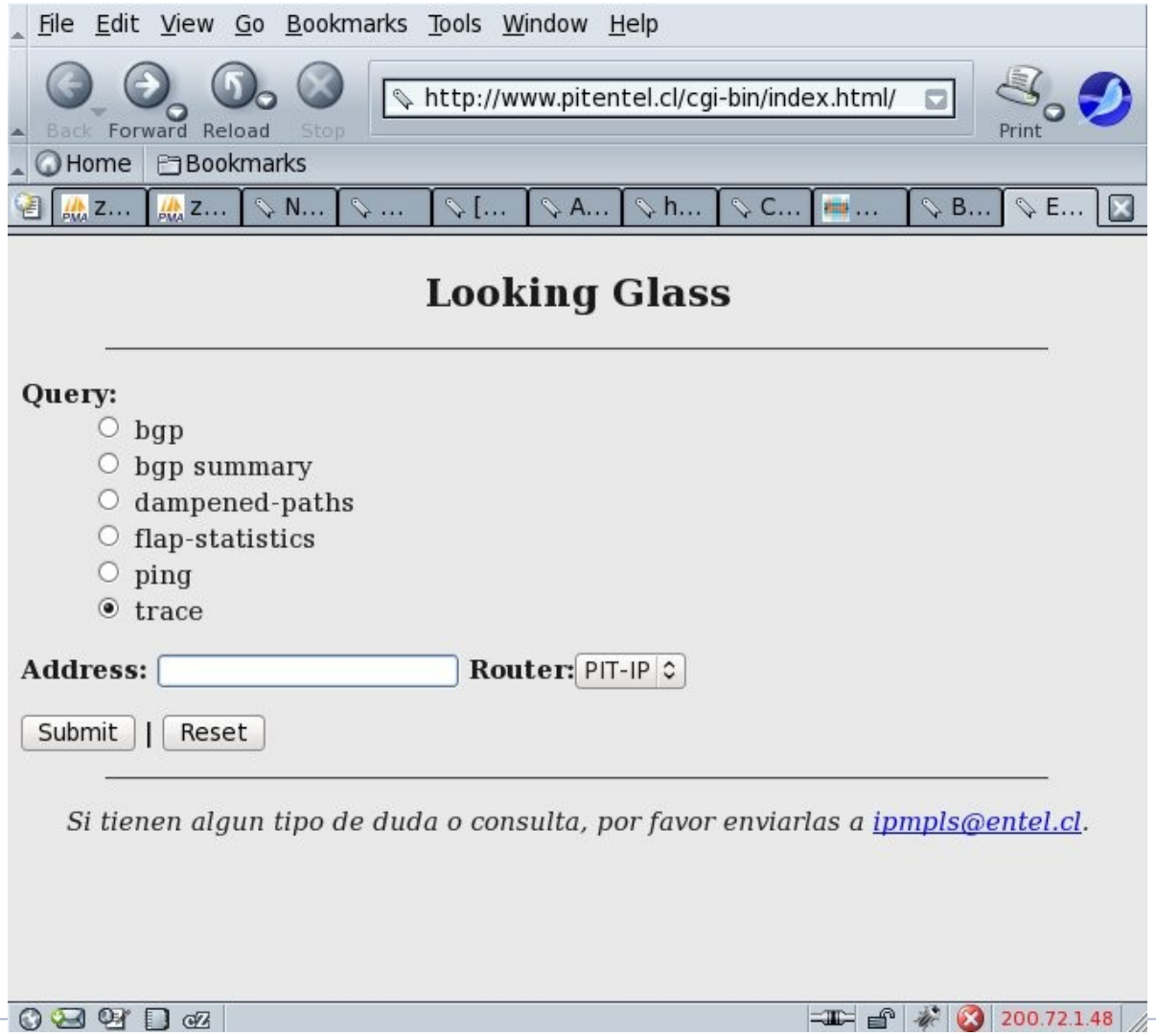
Terminal | Terminal

```
[crrojas@zion: ~]% dig @a.nic.cl uchile.cl any

; <<>> DiG 9.7.1rc1-RedHat-9.7.1-0.2.rc1.fc12 <<>> @a.nic.cl uchile.cl any
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14159
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;uchile.cl.                     IN      ANY

;; AUTHORITY SECTION:
uchile.cl.              3600    IN      NS      ns2.uchile.cl.
uchile.cl.              3600    IN      NS      ns1.uchile.cl.

;; ADDITIONAL SECTION:
ns1.uchile.cl.          3600    IN      A       200.89.70.3
ns2.uchile.cl.          3600    IN      A       200.89.70.70

;; Query time: 1 msec
;; SERVER: 200.1.121.10#53(200.1.121.10)
;; WHEN: Mon May 23 16:46:31 2011
;; MSG SIZE  rcvd: 95

[crrojas@zion: ~]%
```

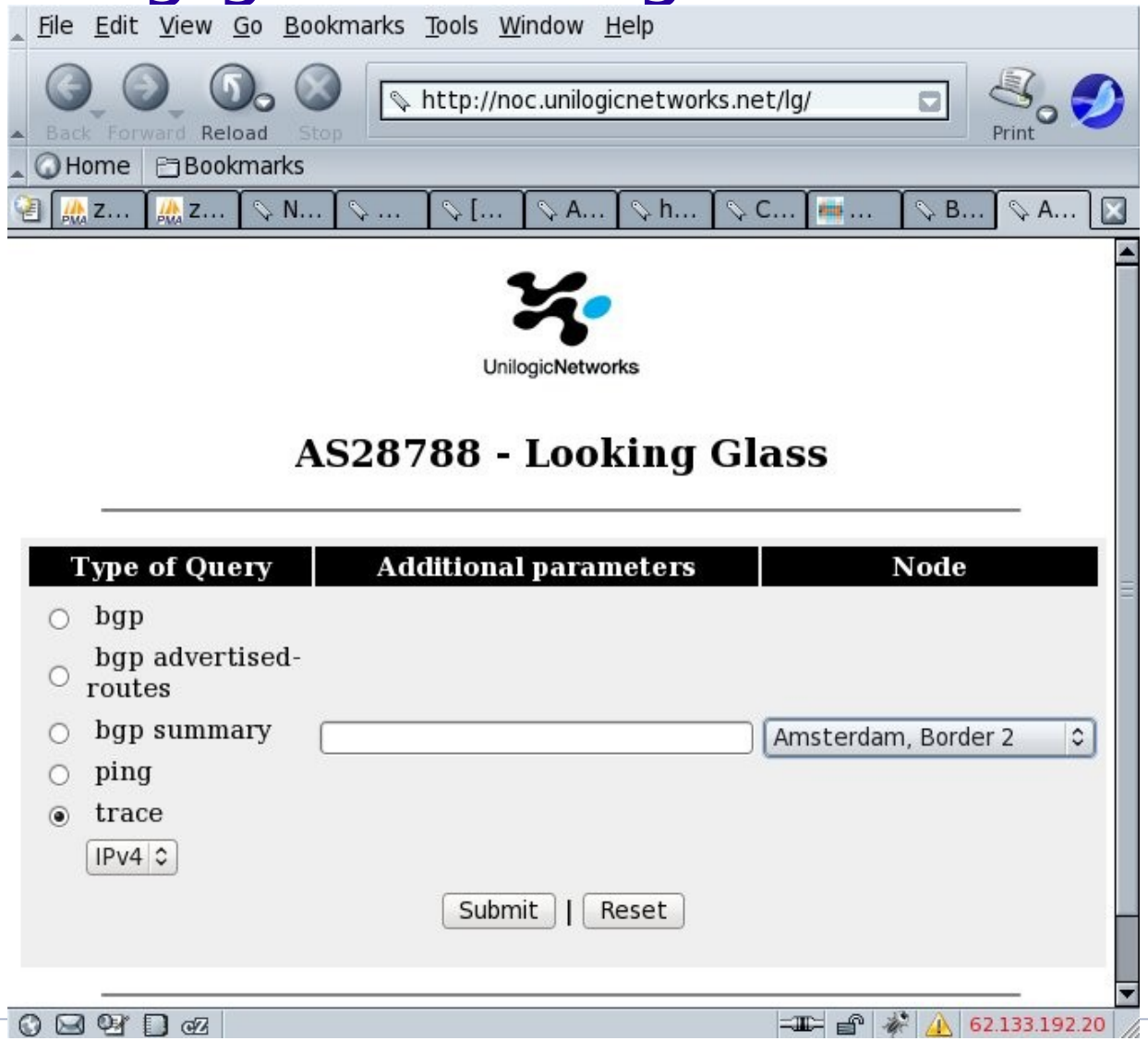
Looking glasses

- Los looking glasses permiten probar la conectividad desde un ISP hasta un destino.
- Muchos isp tienen looking glasses para que otros operadores prueben el comportamiento de la red
- No hay un estandar
- Listado de LG:
  - http://www.bgp4.as/looking-glasses
    - http://www.pitentel.cl/cgi-bin/index.html/
    - http://lg.netglobalis.net/

looking glass entel



looking glass unilogic



¿Consultas?