Sysadmin Miniconf

A few useful Linux tools you might not know about

Simon Lyall
&
Edward Murphy

Reason For Talk:

- “What's Rsync? “
- “Why not use FTP?”
- “Just use a calculator”
- “Why is my lag so high?”

- Overview Only: If you like what you hear use Google.

Rsync

sync files between two places

http://rsync.samba.org

Rsync – Simple Cases

- Make two files the same

  ```
  $ rsync file file2
  ```

- Sync up two directories

  ```
  $ rsync -a dir1 dir2
  ```

- Sync over ssh between two machines

  ```
  $ rsync -e ssh localfile root@test.example.net:remotefile
  $ rsync -a -e ssh localdir root@test.example.net:remotedir
  ```

Rsync - Options

- Too many to list

```
$ rsync --help | grep "\-\-" | wc -l
93
```

Rsync - Securing commands over ssh

```
simon@green:~$ ssh root@test.example.net
root@test.example.net's password:

root@test:~#
```

```
simon@green:~$ ssh root@test.example.net ls
root@test.example.net's password:
hello.txt
simon@green:~$
```

Rsync - Securing commands over ssh

```
simon@green:~$ ssh –i key root@test.example.net ls
hello.txt
simon@green:~$
```

Rsync - Securing commands over ssh

```
root@test:~/.ssh$ cat authorized_keys
command="who" ssh–dss
AAAAB3NzaC1kc3MAAAEBAKl/4GOoYfeAjtZ9ZPj......
```

```
simon@green:~$ ssh –i key root@test.example.net ls
  root     pts/1   Jan 19 13:38 (green.darkmere.gen.nz)
simon@green:~$
```

```
simon@green:~$ ssh –i key root@test.example.net who –H
root     pts/1   Jan 19 13:38 (green.darkmere.gen.nz)
simon@green:~$
```

Rsync - Securing commands over ssh

```
command="rsync --server ." ssh-dss
  AAAAB3NzaC1kc3MAAAEBAK

simon@green:~$ rsync -e "ssh -i key" \
        testfile root@test.example.net:
simon@green:~$
```

Rsync - Securing commands over ssh

```
command="echo $SSH_ORIGINAL_COMMAND >> cmd.log"
  ssh-dss AAAAB3NzaC1kc3MAAAEBAKl/4GO

simon@green:~$ ssh -i key root@test.example.net \        ls
  /etc
simon@green:~$

root@test:~/.ssh$ cat ../cmd.log
ls /etc
root@test:~/.ssh$
```

Rsync - Securing commands over ssh

```
command="/home/admin/validate-cmd" ssh-dss
  AAAAB3NzaC1kc3MAAAEBAKl/4GO

root@test:~/.ssh$ cat ../validate-cmd
#!/bin/sh

case "$SSH_ORIGINAL_COMMAND" in
   ls\ /etc)
            $SSH_ORIGINAL_COMMAND
            ;;
   ls\ /home)
            $SSH_ORIGINAL_COMMAND
            ;;
   *)
            echo "Rejected"
            ;;
esac
```

Rsync - Securing commands over ssh

```
simon@green:~$ ssh -i key
 root@test.example.net ls /
Rejected
simon@green:~$
simon@green:~$
simon@green:~$ ssh -i key
 root@test.example.net ls /home
admin
simon@green:~$
```

Rsync - Securing commands over ssh

```
#!/bin/sh
case "$SSH_ORIGINAL_COMMAND" in
        *\&*)
                echo "Rejected"
                ;;
        *\(*)
                echo "Rejected"
                ;;
        *\{*)
                echo "Rejected"
                ;;
        *\;*)
                echo "Rejected"
                ;;
        *\<*)
                echo "Rejected"
```

Rsync - Securing commands over ssh

```
    *\`*)
        echo "Rejected"
        ;;
    rsync\ --server*/home/admin/incoming/)
        $SSH_ORIGINAL_COMMAND
        ;;
    ls\ /etc)
        $SSH_ORIGINAL_COMMAND
        ;;
    ls\ /home)
        $SSH_ORIGINAL_COMMAND
        ;;
    *)
        echo "Rejected"
        ;;
esac
```

Rsync - Securing commands over ssh

For more information see:

http://www.jdmz.net/ssh/

pwgen

Random Password Generator

pwgen – Generate Random Passwords

```
$ pwgen
Ashai3he pe3Uge3o aish5Bee eemuuZ5U aeg8uaT5
oodooB2V ieYae9ie iReeng7e sa2eiN8r Oe0wooqu EfieJ5ch
iwie8HaM ceuPh1as eCae0qui ooHaiF1e pai9au6E
of7GohCe oov8GaeZ EiB0baek AiZeJai4 Xohj4eex laiP9ohg
zi4Chi9i Shaema8h
uy8iuKae noS7aNee Eiv6eize xooQu0be eiZ3Ou9a fae8Oori
Xu7reini ook8Uvov Tai5que6 aihode5U tohBeeg2 EoLi5oa2
Weng3ohw fig4Beek shoh4Goo nae8eeGa Ejei5up0
OoquiM0f Maw5xai9 eitheo9A phaeY0Cu oe7Cheeb
AiZu0ooj fuX0aiTh
$
```

Add.pl

1 + 1 = 4?

add.pl – Add up a bunch of numbers

```
$ cat file.txt
3
5
6

$ add.pl file.txt
14

$ du -k /etc | sort -r -n |  head -20 | add.pl -
56729
```

add.pl – Code

```
#!/usr/bin/perl
$total=0;
$count=0;
open(FILE,"$ARGV[0]");
@length = <FILE>;
chop(@length);
while($count<@length) {
    ( $total=$total + $length[$count] );
    $count++;
    }
print "$total \n";
```

Netmask

Network Subnets Made Easy

netmask – Manipulate Network Lists

http://trap.mtview.ca.us/~talby/

Give the correct starting point for a Network

```
$ netmask 10.10.10.10/8
     10.0.0.0/8

$ netmask 10.0.6.0/22
    10.0.4.0/22
```

netmask – Output Formats

Show network range

```
$ netmask -r 10.0.0.0/8
      10.0.0.0-10.255.255.255 (16777216)
```

Cisco Format

```
$ netmask -i 10.0.0.0/8
    10.0.0.0 0.255.255.255
```

Address Format

```
$ netmask -s 10.0.0.0/8
    10.0.0.0 / 255.0.0.0
```

netmask – Tidy Lists

Remove Duplicate Networks

```
$ netmask 10.0.0.0/8 10.1.1.0/24
   10.0.0.0/8
$ cat netmask.sample
10.9.3.4/24
100.12.0.1/13
44.5.6.0/12
44.2.2.1/27
$ cat netmask.sample | xargs netmask | sed “s/^ *//”
10.9.3.0/24
44.0.0.0/12
100.8.0.0/13
$
```

HTMLDOC

HTML -> PDF or Postscript

http://www.htmldoc.org/ and
http://www.easysw.com/htmldoc/

HTMLDOC - Overview

- Take HTML Pages and converts to Postscript or PDF
- Multiple HTML Pages into a Single document
- Can be used from GUI, Command Line and CGI
- Can download HTML itself or work on local files
- Commercial Support Available

HTMLDOC - Uses

- Create Reports for Management
  - Sample MRTG Graphs
  - Snapshot of Website
  - Snapshot of Trouble Ticket System
- Print HTML from command line
- DATA -> HTML -> PDF
- Provide Documentation in Multiple formats

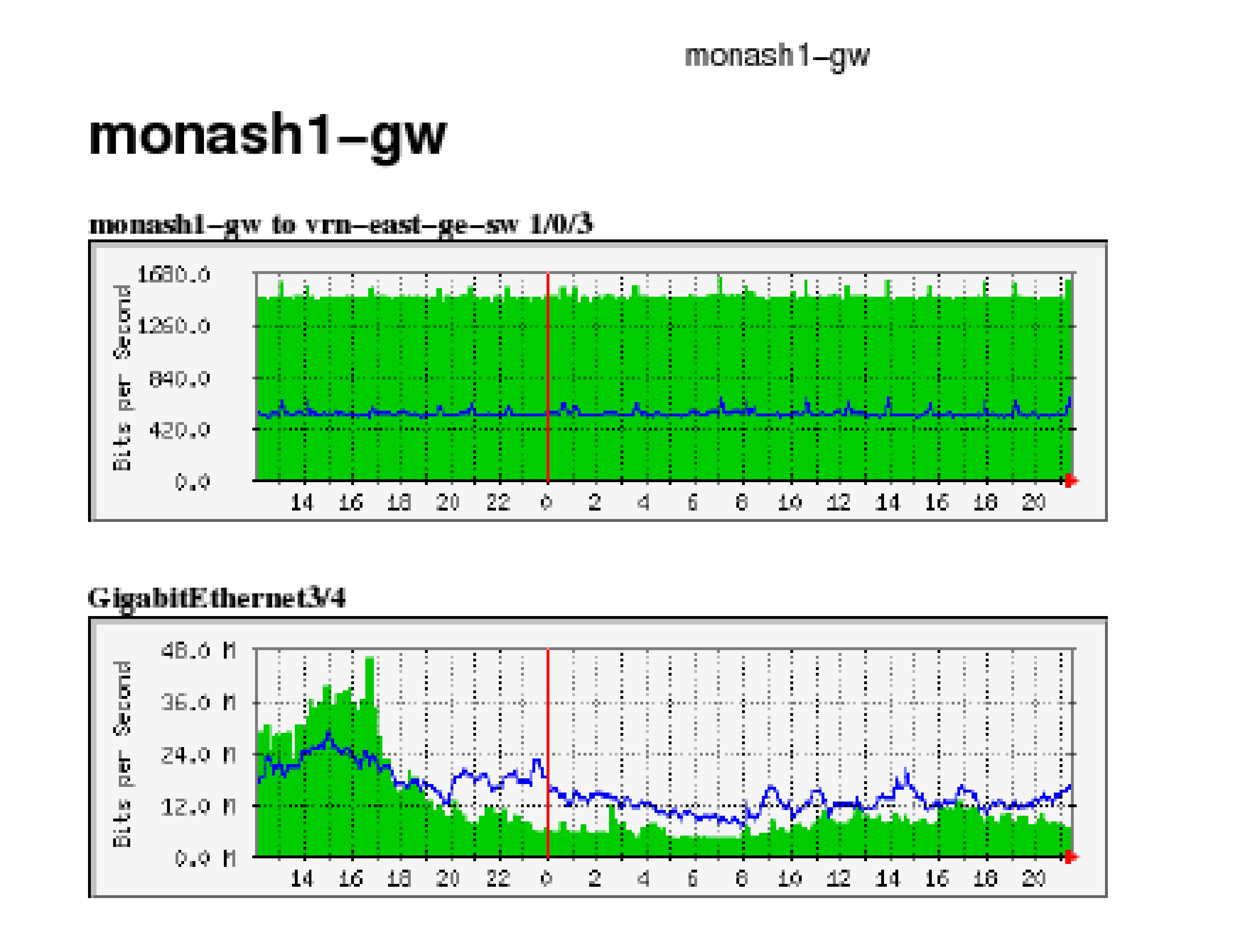
HTMLDOC - Disadvantages

- Tables and Stylesheets not properly supported
- HTTPS requires use of separate downloader

HTMLDOC - Example

```
wget -P temp -nH -p \
    http://mrtg.its.monash.edu.au/monash1-gw.html

htmldoc --continuous --webpage temp/monash1-gw.html \
--outfile sample1.pdf



htmldoc --webpage -f sample2.pdf http://www.google.com \
http://lwn.net

htmldoc --webpage -f sample3.pdf \
    http://sysadmin.miniconf.org/program.html
```

HTMLDOC – Example Output 1



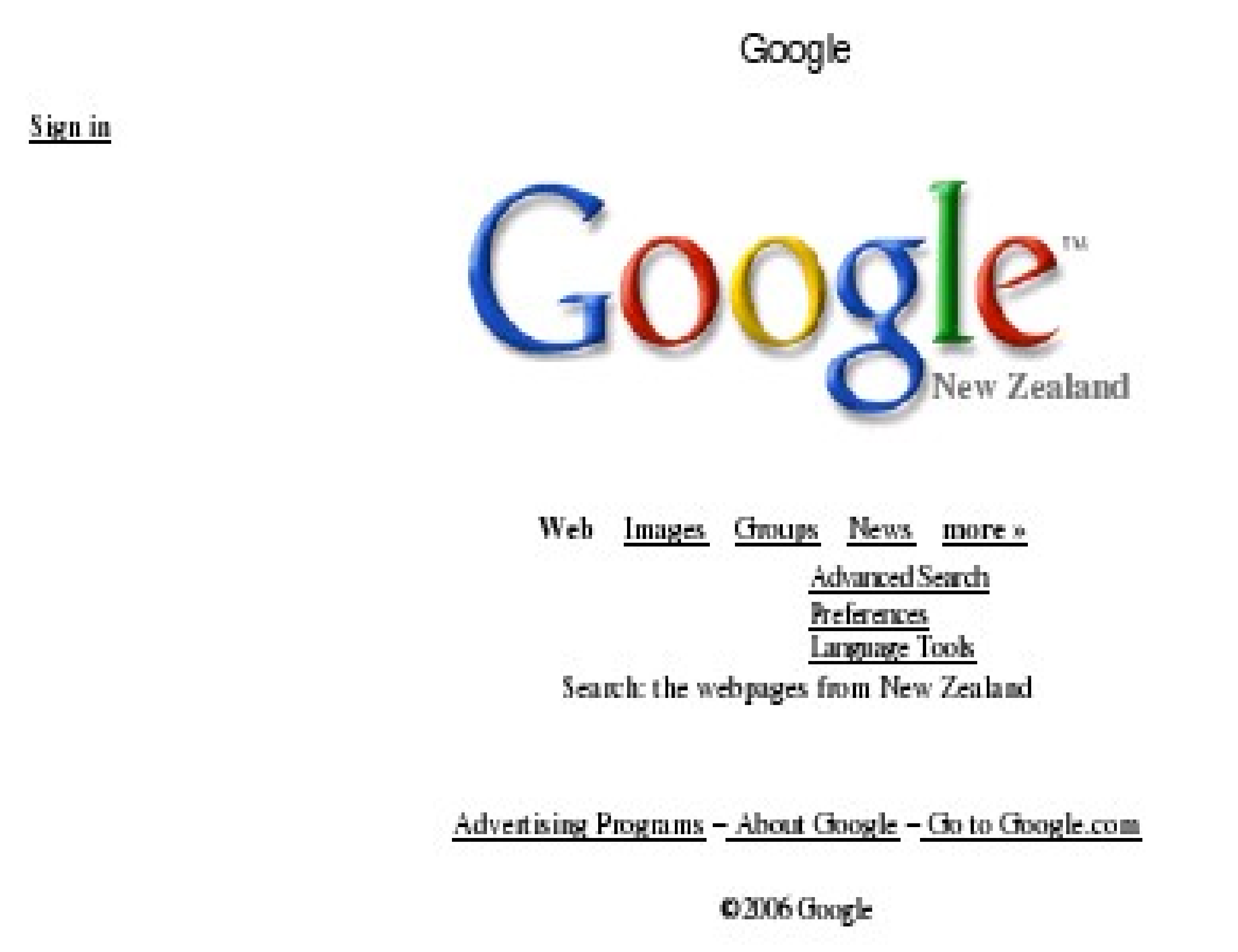
monash1–gw

monash1–gw

monash1–gw to vrn–east–ge–sw 1/0/3

GigabitEthernet3/4

HTMLDOC – Example Output 2



Google

Sign in

Web Images Groups News more »

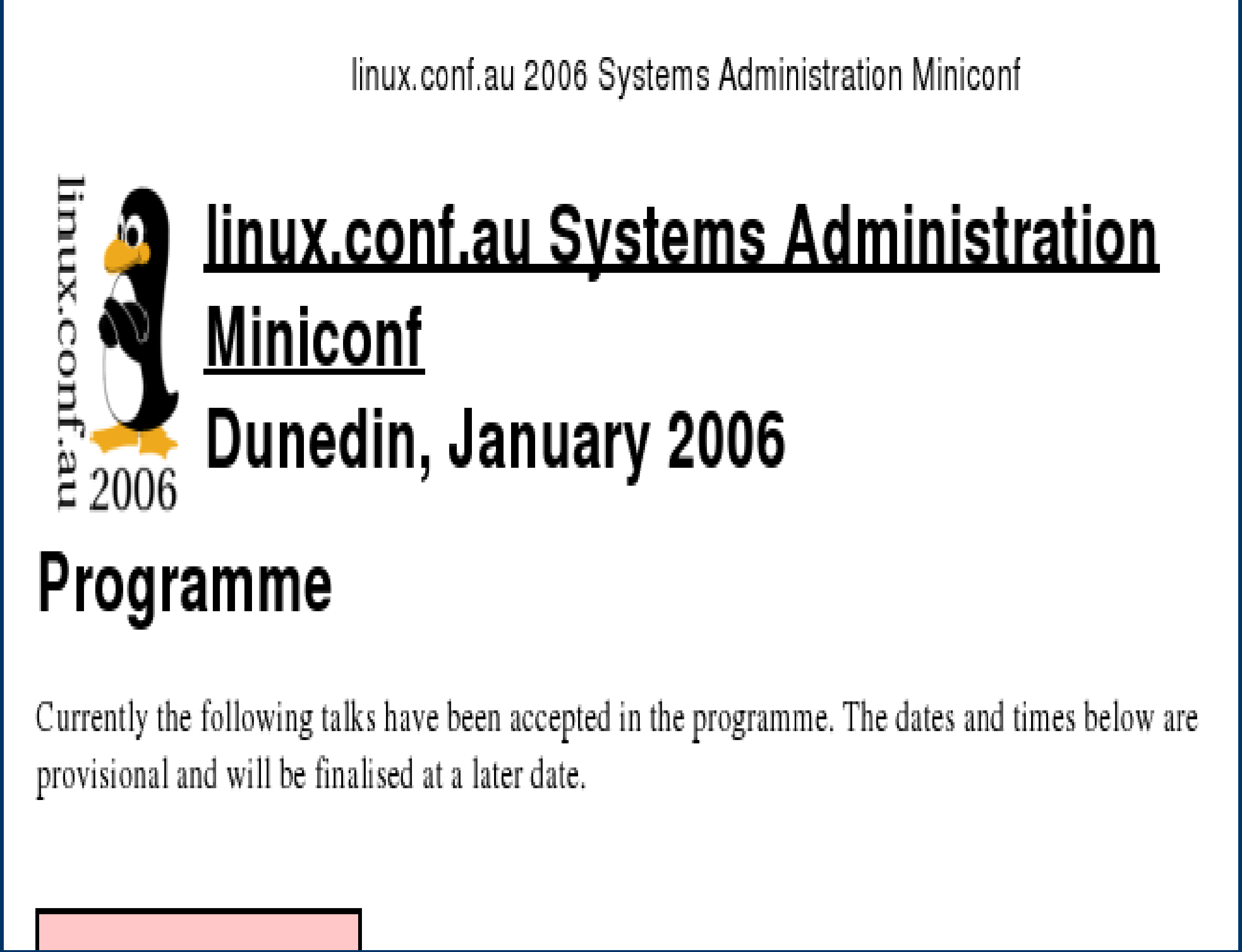
Advanced Search
Preferences
Language Tools

Search: the webpages from New Zealand

Advertising Programs – About Google – Go to Google.com

©2006 Google

HTMLDOC – Example Output 3



linux.conf.au 2006 Systems Administration Miniconf

linux.conf.au Systems Administration Miniconf

Dunedin, January 2006

Programme

Currently the following talks have been accepted in the programme. The dates and times below are provisional and will be finalised at a later date.

Netcat

Windows Hacking Tool gone Straight

Netcat - Overview

- Netcat is just like cat, except it reads and write across a network connection.
- Website: http://netcat.sourceforge.net/

Netcat - Features

- Incoming or Outgoing connections
- TCP or UDP, and ports
- Works like a good unix tool

Netcat Example: Telnet Clone

```
$ nc smtp.xtra.co.nz 25
220 mta4-rme.xtra.co.nz ESMTP server ready
```

Netcat Example: Monitoring Systems

```
echo "quit" | nc -w 3 smtp.xtra.co.nz 25 | grep "^220"
```

Netcat Example: Listening on ports

```
sys1$ nc -l -u 3333
sys2$ echo "Alert" | nc -v -u -w 3 sys1 3333
```

Netcat Example: Put It Together

```
#!/bin/bash
while [ 1 ]
do
  echo "quit" | nc -w 5 mx1.hotmail.com 25 \
     | grep "^220"
  if ! [ $? ]
  then
    echo "Hotmail SMTP Down" | nc -u -w 3 \
     alertmachine 3333
  fi
  sleep 30
done
```

Netcat - Uses

- Port Scanning
- File transfer ("nc machine 12345 < file")
- Port redirects
- Monitoring
- Ad Hoc anything

Netcat

- See Also: "socat"

Ptime

`Unix time now Human Readable.`

Ptime - Examples

```
$ cat bin/ptime
perl –e print\  localtime\(\$ARGV\[0\]\).\"\\n\" $1

$ ptime 1137240662
Sun Jan 15 01:11:02 2006

$ ptime 1137845497
Sun Jan 22 01:11:37 2006

$ ptime 1099220400
Mon Nov  1 00:00:00 2004
```

Munin

Host Metrics
Graphing tool

Munin – Host Statistics Graphing

- Server / Agent based installation
- Single Server polling Multiple Clients
- Can group by Domain
- Can incorporate Custom Checks
- Can send alarms to Nagios
- Uses RRD Back end
- Client Security through IP Regular Expression
- Plugins are easy to write

Munin – Why not MRTG / Cacti?

- Because Munin is easy to install
- Because there is minimal configuration
- Because you can script installation very easily

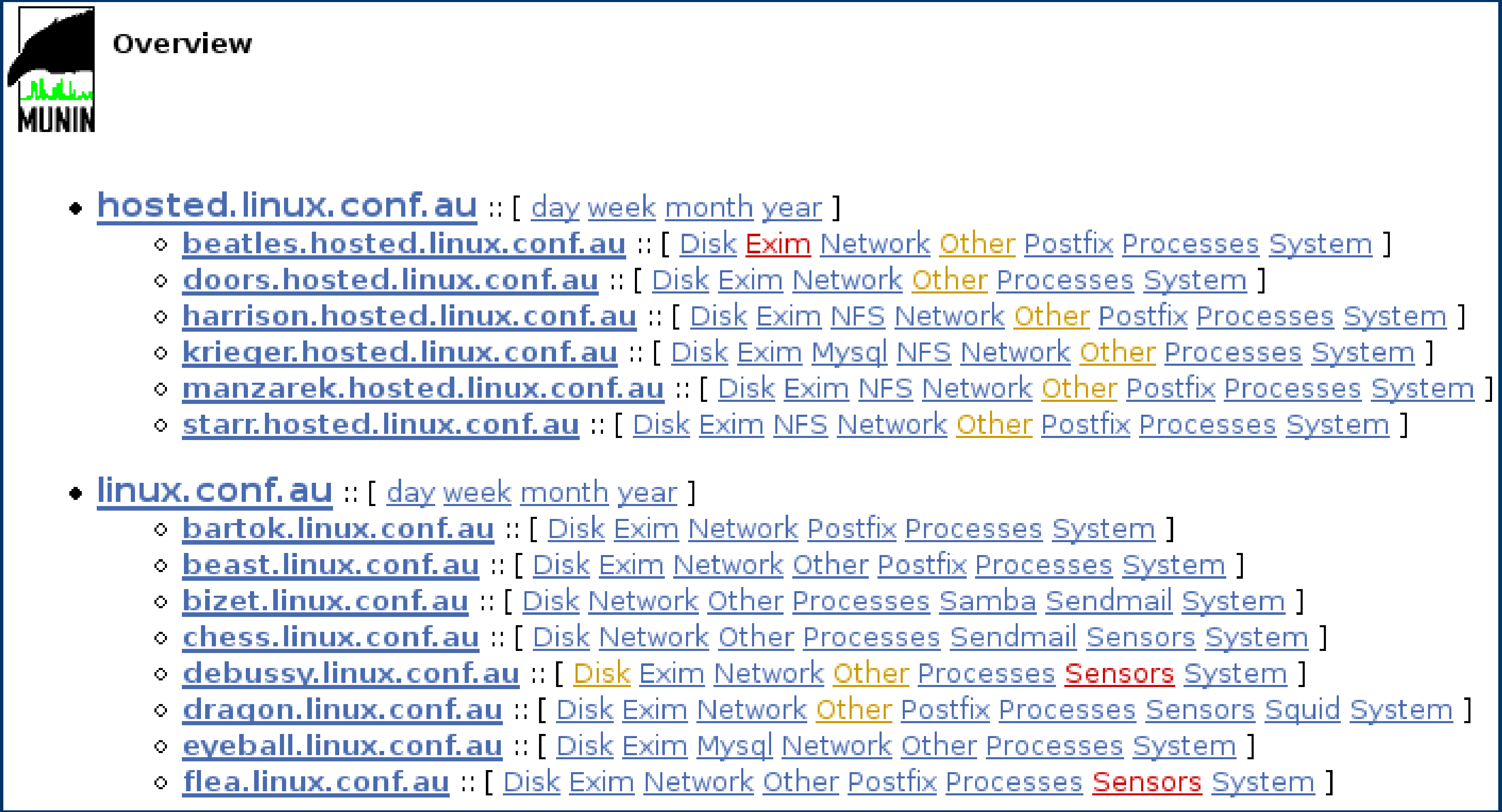
Munin - Disadvantages

- Single Server polling Several Nodes
- Host timeouts could mean poll skew (i.e. not all checks happen within a 5 min interval if one of the checks hangs)
- Runs through hosts in a linear mode

Munin – Plugins

- Language independent programs
- Added to daemon by symlinking to config directory
- Example plugins:
  - apache access/processes/volume
  - apt package updates pending
  - courier/exim/senmail/postfix stats
  - cpu / memory / disk size
  - entropy / forks / interrupts / iostat
  - mysql statistics
  - port session counts
  - snmp data
  - S.M.A.R.T values
  - sensors readings

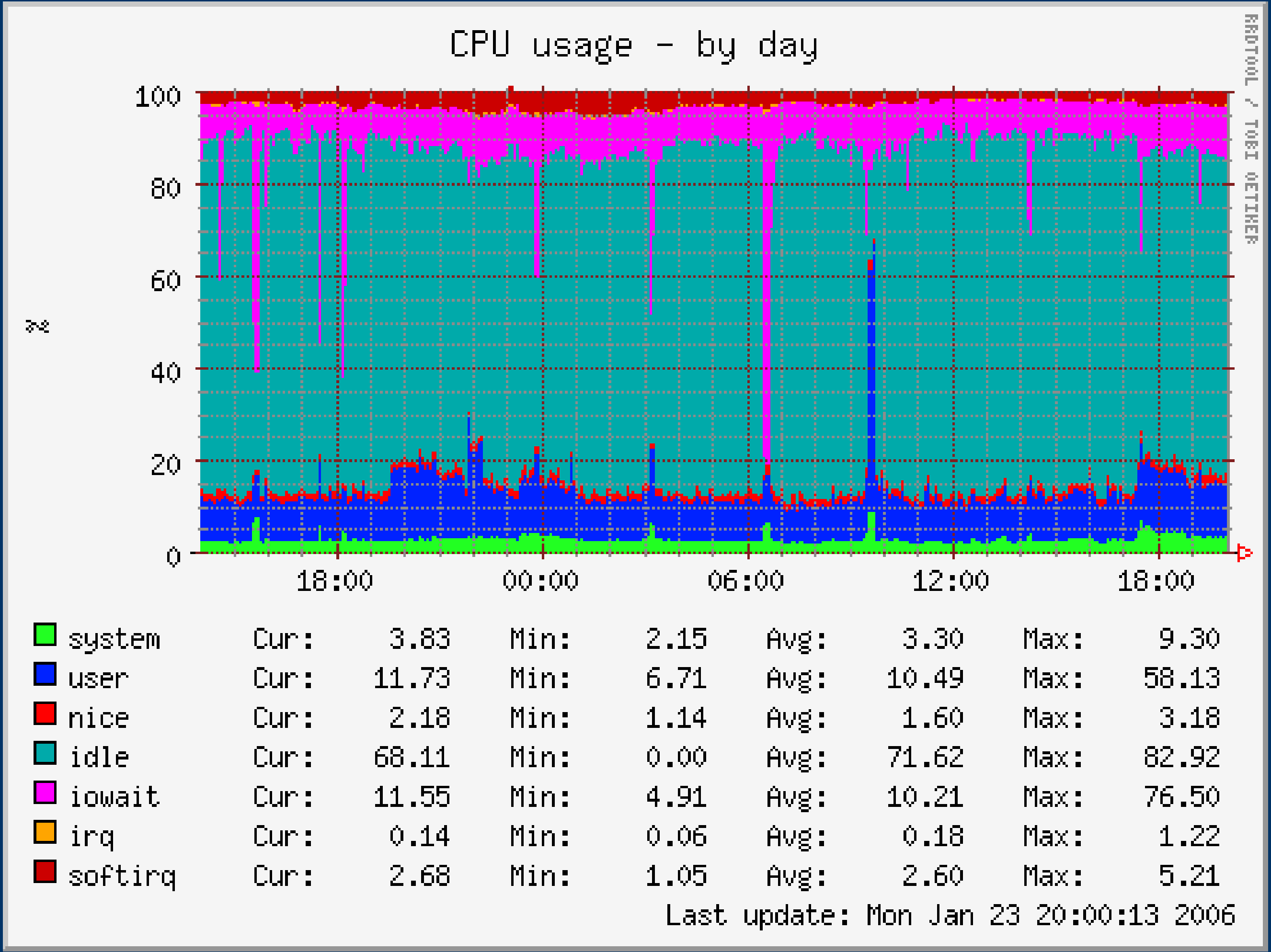
Munin – Example Index



Overview

- hosted.linux.conf.au :: [day week month year]
  - beatles.hosted.linux.conf.au :: [Disk Exim Network Other Postfix Processes System]
  - doors.hosted.linux.conf.au :: [Disk Exim Network Other Processes System]
  - harrison.hosted.linux.conf.au :: [Disk Exim NFS Network Other Postfix Processes System]
  - krieger.hosted.linux.conf.au :: [Disk Exim Mysql NFS Network Other Processes System]
  - manzarek.hosted.linux.conf.au :: [Disk Exim NFS Network Other Postfix Processes System]
  - starr.hosted.linux.conf.au :: [Disk Exim NFS Network Other Postfix Processes System]
- linux.conf.au :: [day week month year]
  - bartok.linux.conf.au :: [Disk Exim Network Postfix Processes System]
  - beast.linux.conf.au :: [Disk Exim Network Other Postfix Processes System]
  - bizet.linux.conf.au :: [Disk Network Other Processes Samba Sendmail System]
  - chess.linux.conf.au :: [Disk Network Other Processes Sendmail Sensors System]
  - debussy.linux.conf.au :: [Disk Exim Network Other Processes Sensors System]
  - dragon.linux.conf.au :: [Disk Exim Network Other Postfix Processes Sensors Squid System]
  - eyeball.linux.conf.au :: [Disk Exim Mysql Network Other Processes System]
  - flea.linux.conf.au :: [Disk Exim Network Other Postfix Processes Sensors System]

Munin – Example – Daily CPU

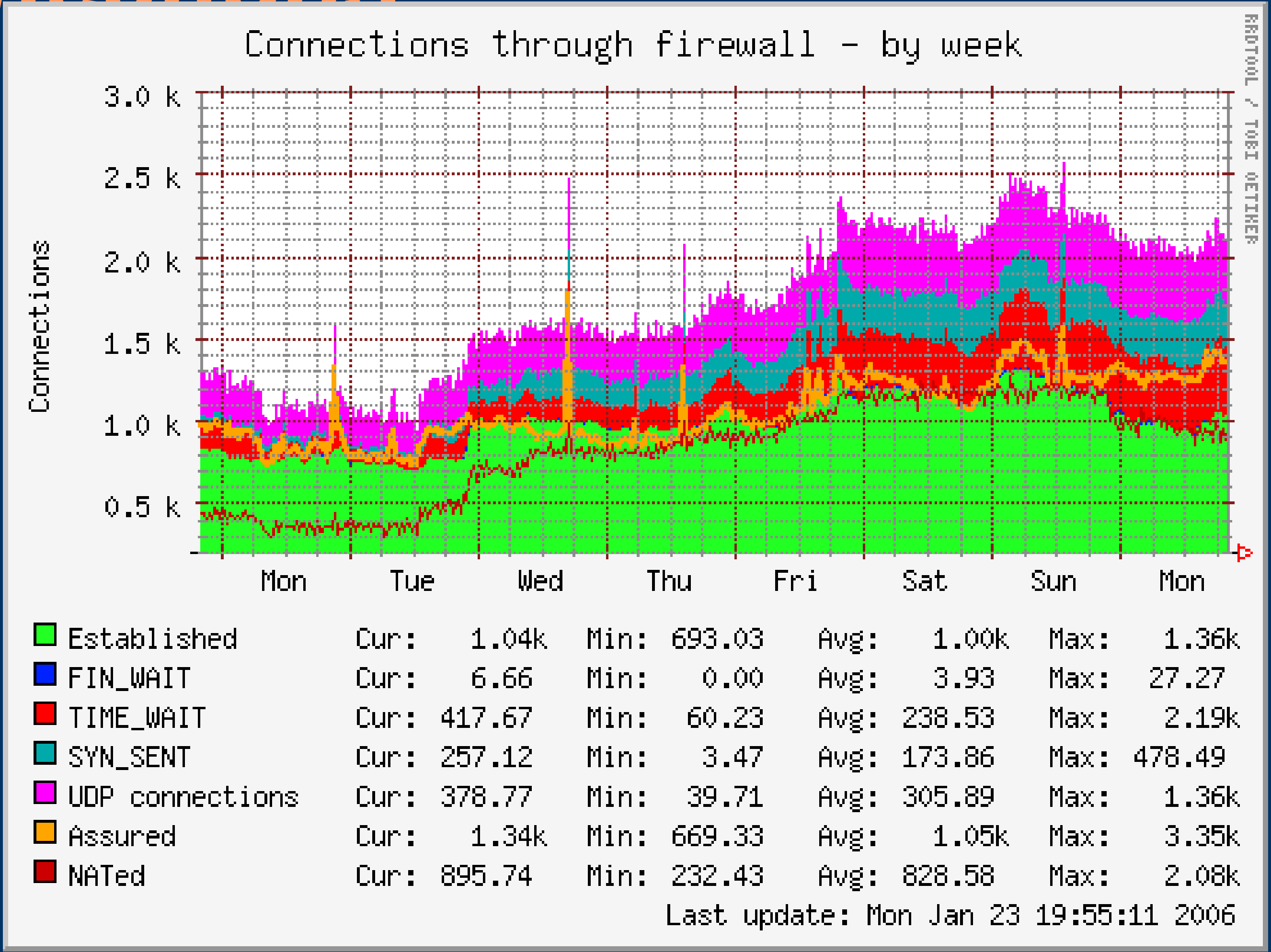


CPU usage - by day

🟩 system	Cur:	3.83	Min:	2.15	Avg:	3.30	Max:	9.30
🟦 user	Cur:	11.73	Min:	6.71	Avg:	10.49	Max:	58.13
🟥 nice	Cur:	2.18	Min:	1.14	Avg:	1.60	Max:	3.18
■ idle	Cur:	68.11	Min:	0.00	Avg:	71.62	Max:	82.92
🟪 iowait	Cur:	11.55	Min:	4.91	Avg:	10.21	Max:	76.50
🟧 irq	Cur:	0.14	Min:	0.06	Avg:	0.18	Max:	1.22
🟥 softirq	Cur:	2.68	Min:	1.05	Avg:	2.60	Max:	5.21

Last update: Mon Jan 23 20:00:13 2006

Munin – Example - Weekly Connections



🟩 Established	Cur: 1.04k	Min: 693.03	Avg: 1.00k	Max: 1.36k
🟦 FIN_WAIT	Cur: 6.66	Min: 0.00	Avg: 3.93	Max: 27.27
🟥 TIME_WAIT	Cur: 417.67	Min: 60.23	Avg: 238.53	Max: 2.19k
🟦 SYN_SENT	Cur: 257.12	Min: 3.47	Avg: 173.86	Max: 478.49
🟪 UDP connections	Cur: 378.77	Min: 39.71	Avg: 305.89	Max: 1.36k
🟧 Assured	Cur: 1.34k	Min: 669.33	Avg: 1.05k	Max: 3.35k
🟫 NATed	Cur: 895.74	Min: 232.43	Avg: 828.58	Max: 2.08k

Last update: Mon Jan 23 19:55:11 2006

Nload

Network Load Monitoring Tool

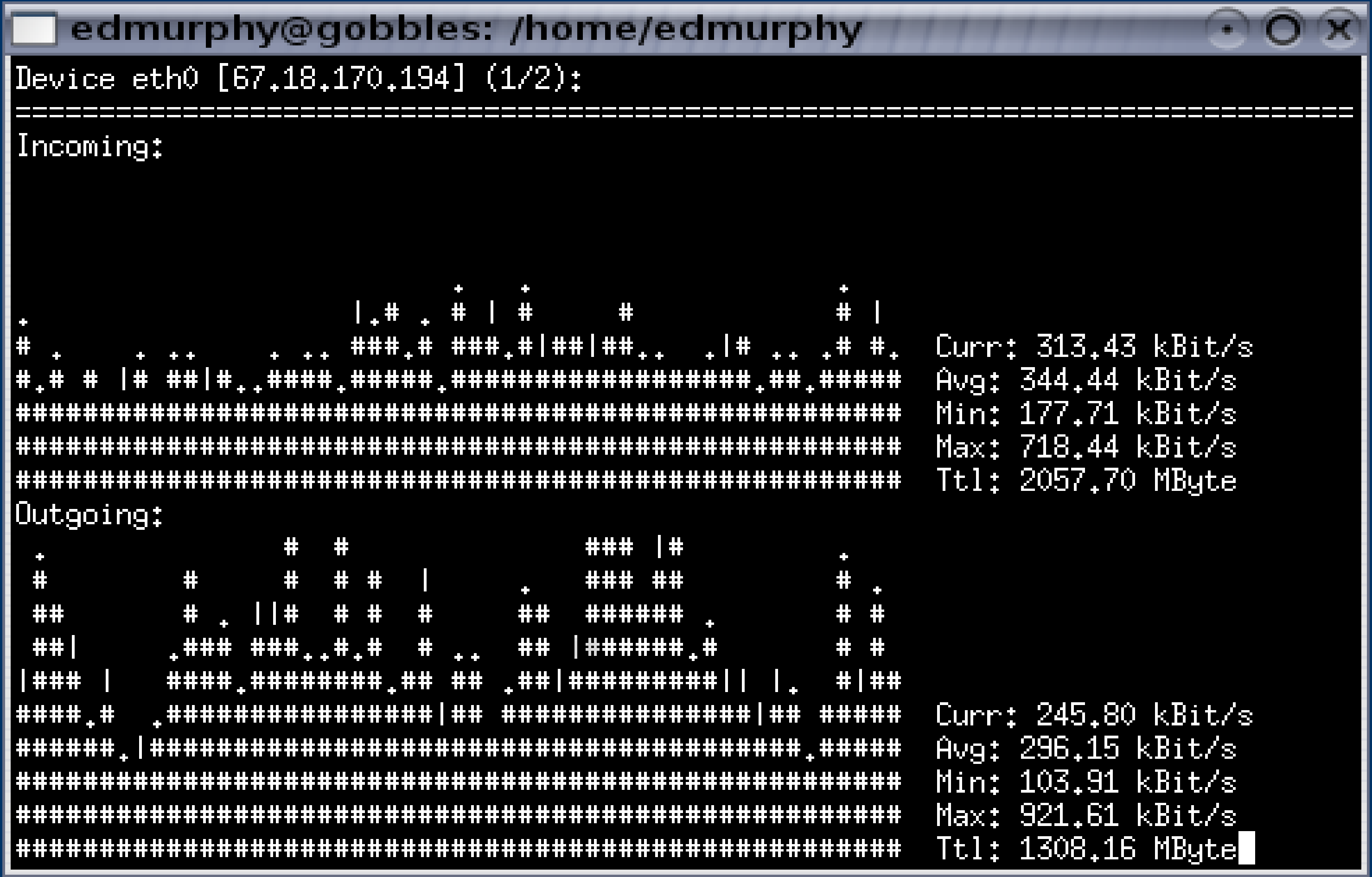
Nload – Overview

- Ncurses Based
- Real Time traffic visualization
- Separate Input and Output Graphs
- Configurable Peaks (Input/Output separate)
- Can switch between multiple interfaces without application reset

Nload - Overview

- Data shown
  - Current Throughput
  - Average Speed
  - Maximum Speed
  - Minimum Speed
  - Byte Throughput

Nload – Example Output



```
Device eth0 [67.18.170.194] (1/2):
================================================================================
Incoming:



                          .   .                  .
.                   |.# . # | #     #            # |
# .    . ..    . .. ###.# ###.#|##|##..  .|# .. .# #.  Curr: 313.43 kBit/s
#.# # |# ##|#..####.#####.##################.##.#####  Avg: 344.44 kBit/s
#####################################################  Min: 177.71 kBit/s
#####################################################  Max: 718.44 kBit/s
#####################################################  Ttl: 2057.70 MByte
Outgoing:
 .              #  #              ### |#         .
 #        #     #  # #  |     .   ### ##         # .
 ##       # . ||#  # #  #     ##  ###### .       # #
 ##|     .### ###..#.#  # ..  ## |######.#       # #
|### |   ####.########.## ## .##|#########|| |.  #|##
####.#  .################|## ###############|## #####  Curr: 245.80 kBit/s
######.|#######################################.#####  Avg: 296.15 kBit/s
#####################################################  Min: 103.91 kBit/s
#####################################################  Max: 921.61 kBit/s
#####################################################  Ttl: 1308.16 MByte
```

```
# nload-i 1000 -o 1000 eth0 eth1
```

IPTraf

Real Time Network Monitoring
and Debug Tool

IPTraf - Overview

- Ncurses Based real time traffic analysis tool
- Can monitor all interfaces or one interface at a time
- Modules:
  - Ip Socket Monitoring
  - General Interface Stats
  - Detailed Interface Stats
  - Statistical breakdown
  - Lan Statistics Monitor
  - Filters

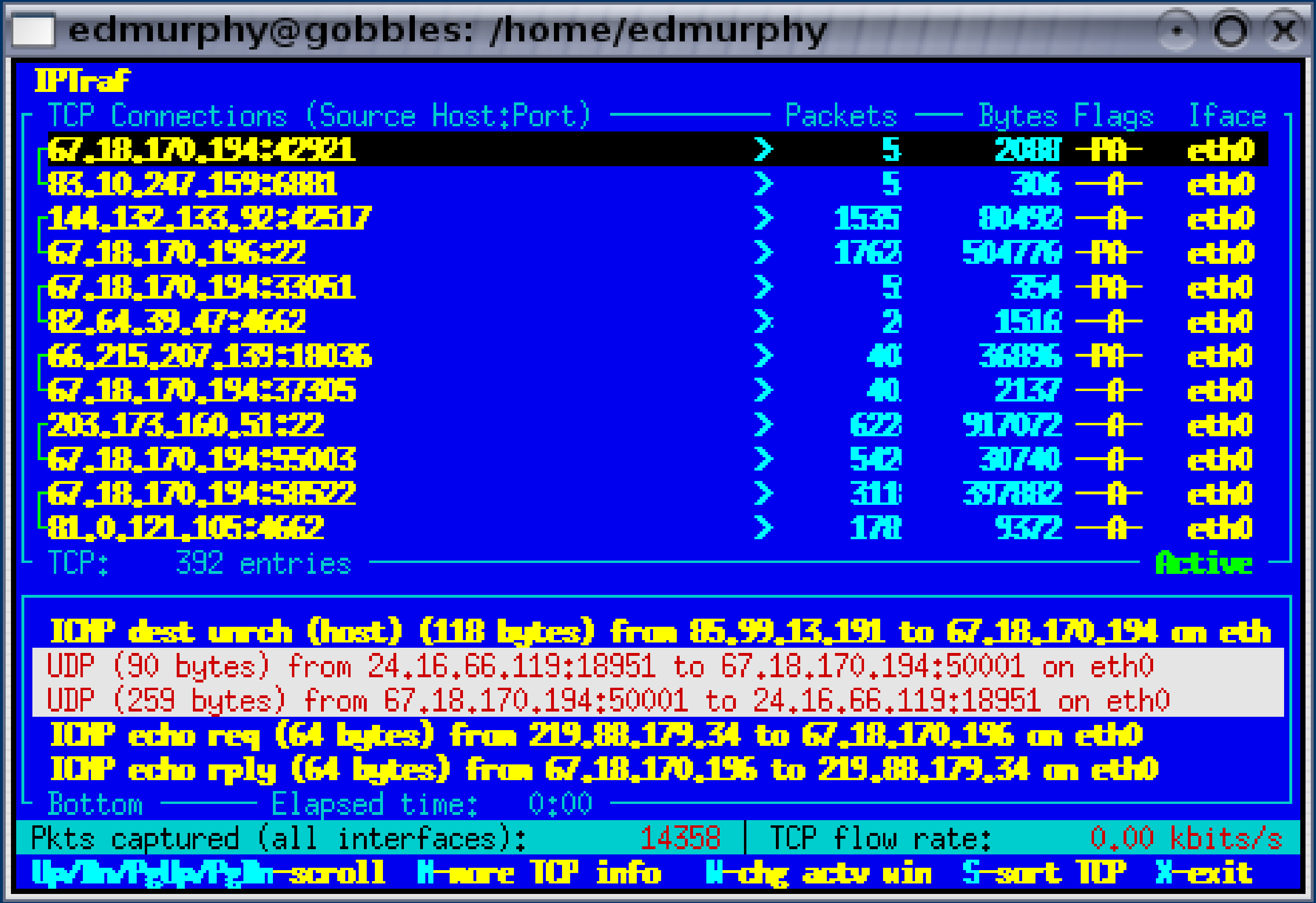
IPTraf - Filtering

- TCP Packets only
- UDP Packets only
- All Traffic
  - View/Hide TCP/UDP
  - View/Hide ARP/RARP
  - View/Hide Non-IP Packets

IPTraf – Other Features

- Logging
- Results shown in Bytes/sec or Bits/sec
- Port Range Filtering Available

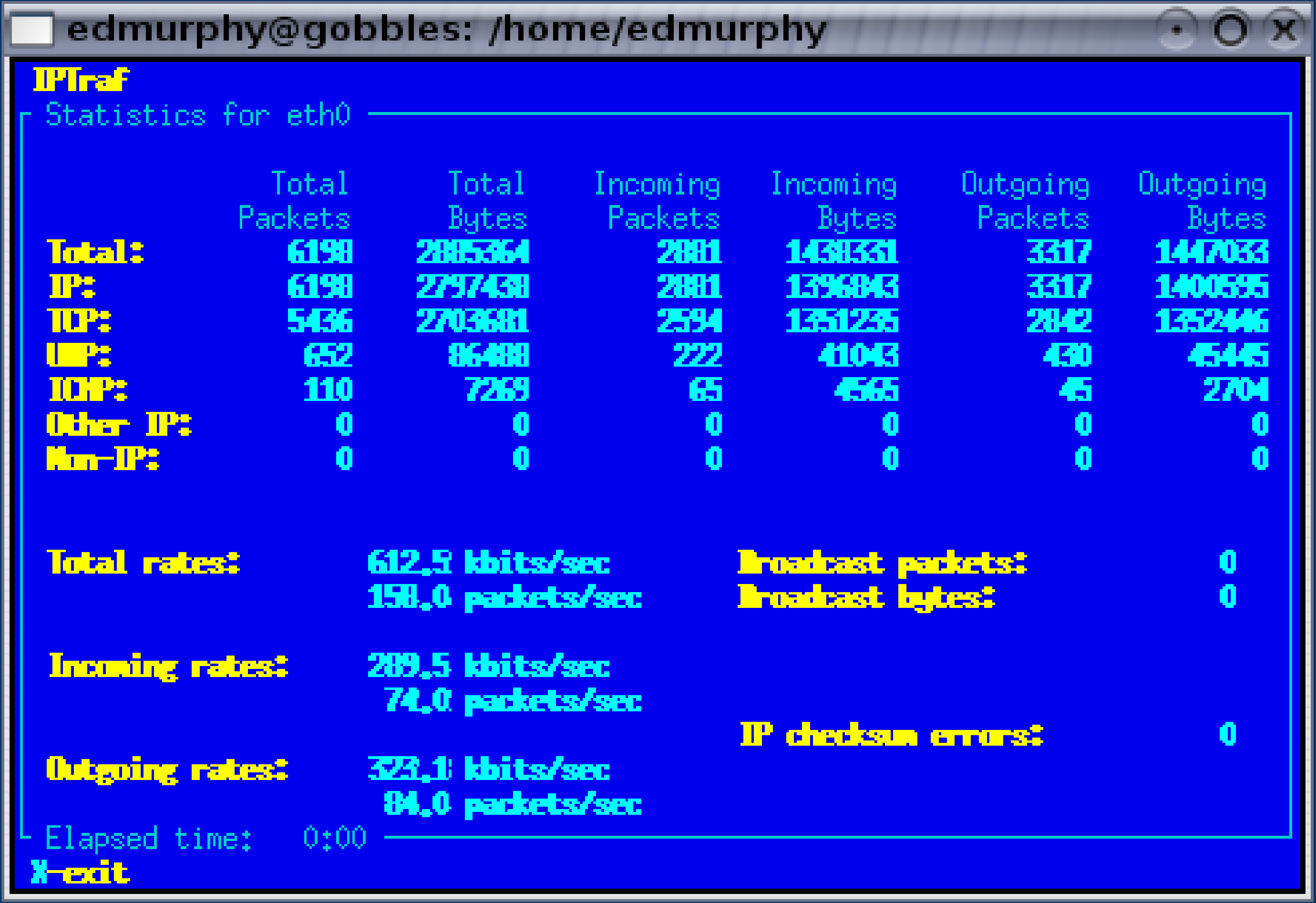
IPTraf - Examples



```
edmurphy@gobbles: /home/edmurphy

IPTraf
┌ TCP Connections (Source Host:Port) ──────────── Packets ──── Bytes Flags  Iface ┐
│┌67.18.170.194:42921                          >      5      2088 -PA-   eth0
│└83.10.247.159:6881                           >      5       306 --A-   eth0
│┌144.132.133.92:42517                         >   1535     80492 --A-   eth0
│└67.18.170.196:22                             >   1762    504776 -PA-   eth0
│┌67.18.170.194:33051                          >      9       354 -PA-   eth0
│└82.64.39.47:4662                             >      2      1516 --A-   eth0
│┌66.215.207.139:18036                         >     40     36896 -PA-   eth0
│└67.18.170.194:37305                          >     40      2137 --A-   eth0
│┌203.173.160.51:22                            >    622    917072 --A-   eth0
│└67.18.170.194:55003                          >    542     30740 --A-   eth0
│┌67.18.170.194:58522                          >    311    397882 --A-   eth0
│└81.0.121.105:4662                            >    178      9372 --A-   eth0
└ TCP:     392 entries ───────────────────────────────────────────────── Active ┘
┌──────────────────────────────────────────────────────────────────────────────┐
│ ICMP dest unrch (host) (118 bytes) from 85.99.13.191 to 67.18.170.194 on eth
│ UDP (90 bytes) from 24.16.66.119:18951 to 67.18.170.194:50001 on eth0
│ UDP (259 bytes) from 67.18.170.194:50001 to 24.16.66.119:18951 on eth0
│ ICMP echo req (64 bytes) from 219.88.179.34 to 67.18.170.196 on eth0
│ ICMP echo rply (64 bytes) from 67.18.170.196 to 219.88.179.34 on eth0
└ Bottom ────── Elapsed time:   0:00 ────────────────────────────────────────────┘
 Pkts captured (all interfaces):       14358 │ TCP flow rate:        0.00 kbits/s
 Up/Dn/PgUp/PgDn-scroll  M-more TCP info   W-chg actv win  S-sort TCP  X-exit
```

TCP Socket Connections

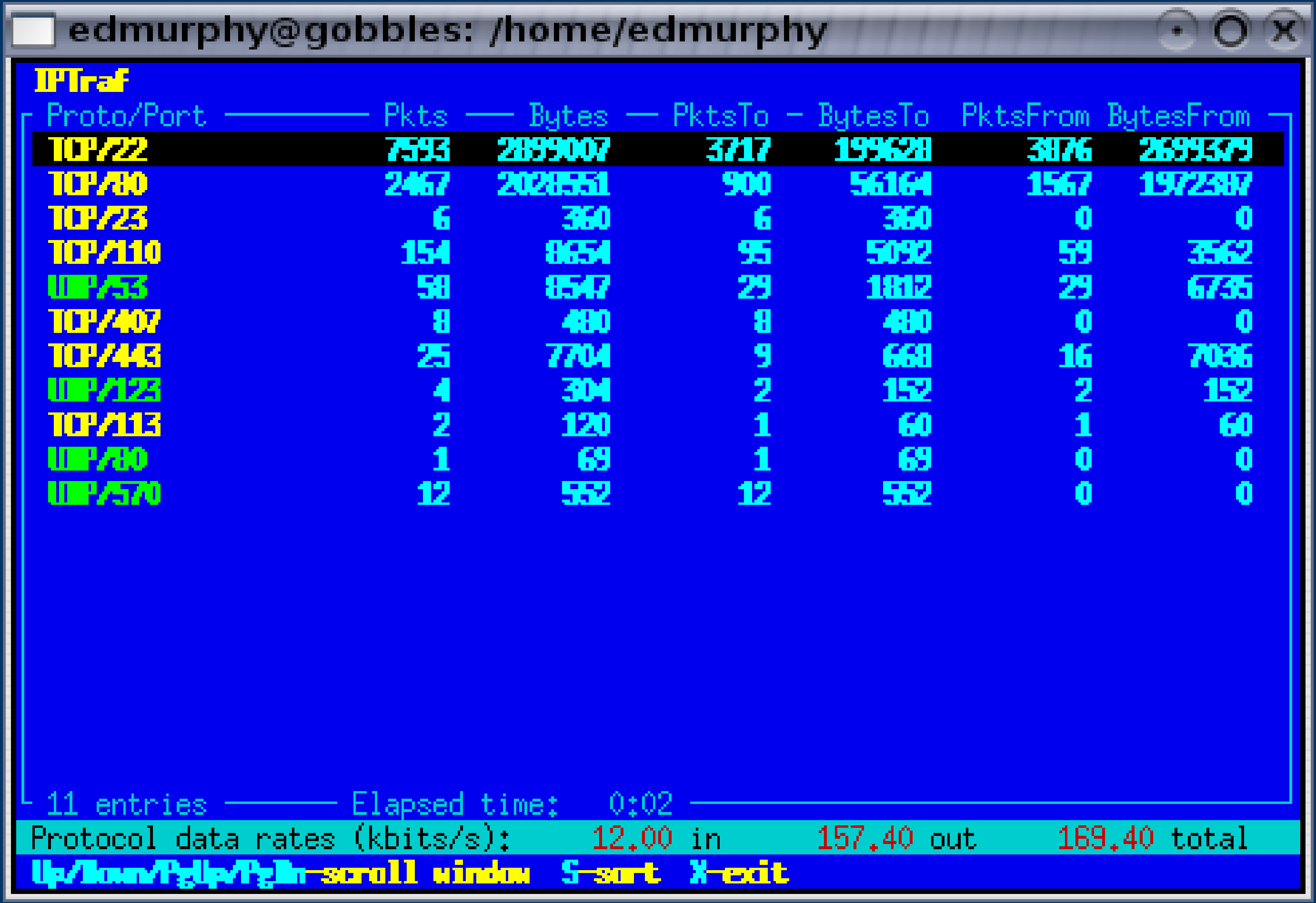
IPTraf - Examples



```
IPTraf
┌ Statistics for eth0 ─────────────────────────────────────────────────────────

                     Total      Total   Incoming   Incoming   Outgoing   Outgoing
                   Packets      Bytes    Packets      Bytes    Packets      Bytes
 Total:               6198    2885364       2881    1438331       3317    1447033
 IP:                  6198    2797438       2881    1396843       3317    1400595
 TCP:                 5436    2703681       2594    1351235       2842    1352446
 UDP:                  652      86488        222      41043        430      45445
 ICMP:                 110       7269         65       4565         45       2704
 Other IP:               0          0          0          0          0          0
 Non-IP:                 0          0          0          0          0          0


 Total rates:         612.5 kbits/sec         Broadcast packets:              0
                      158.0 packets/sec       Broadcast bytes:                0

 Incoming rates:      289.5 kbits/sec
                       74.0 packets/sec
                                              IP checksum errors:             0

 Outgoing rates:      323.1 kbits/sec
                       84.0 packets/sec
└ Elapsed time:   0:00 ──────────────────────────────────────────────────────────
X-exit
```

General Interface Statistics

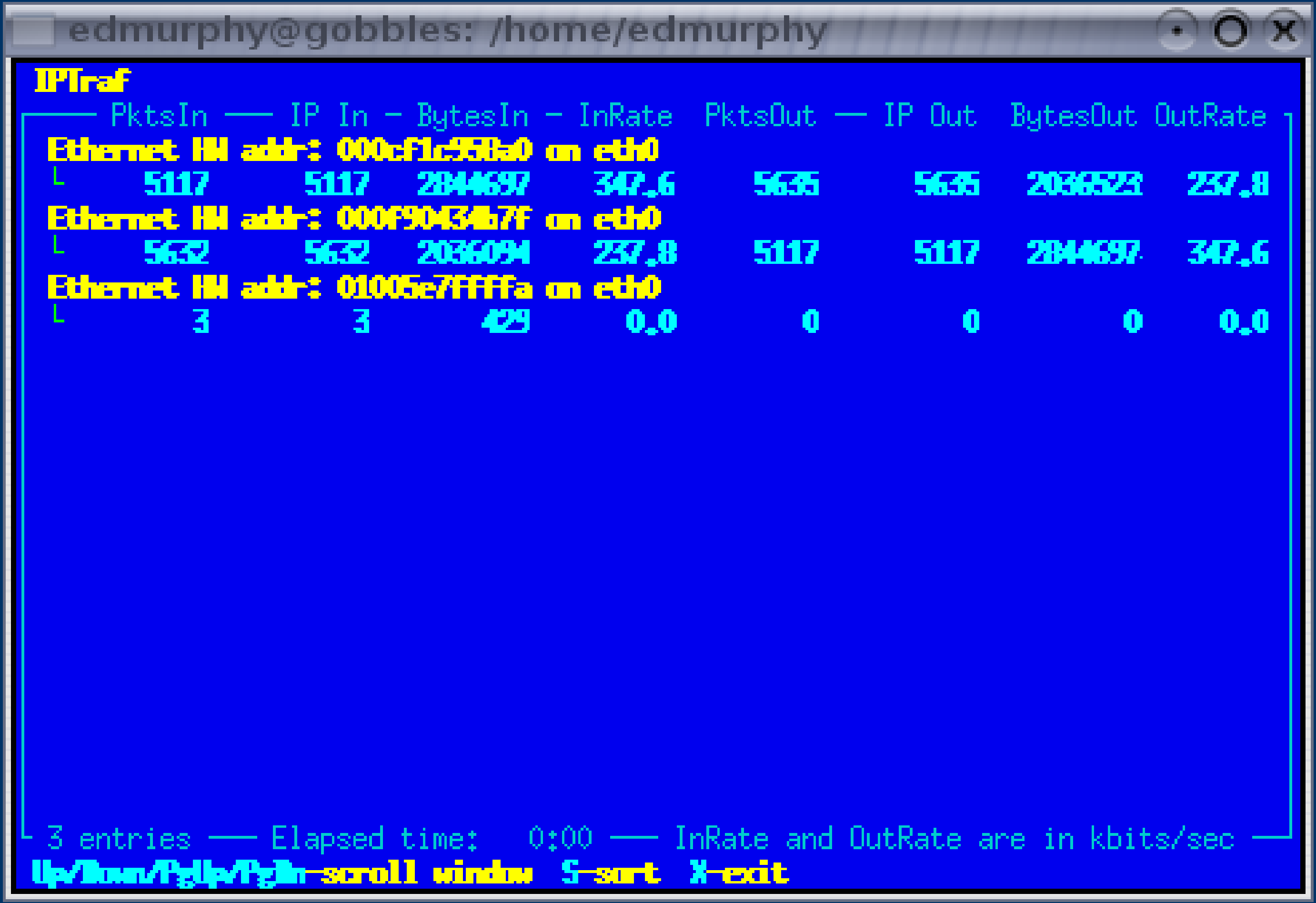
IPTraf - Examples



```
edmurphy@gobbles: /home/edmurphy

IPTraf
┌ Proto/Port ──────────── Pkts ─── Bytes ── PktsTo ─ BytesTo  PktsFrom BytesFrom ─┐
  TCP/22                  7593   2899007      3717    199628      3876   2699379
  TCP/80                  2467   2028551       900     56164      1567   1972387
  TCP/23                     6       360         6       360         0         0
  TCP/110                  154      8654        95      5092        59      3562
  UDP/53                    58      8547        29      1812        29      6735
  TCP/407                    8       480         8       480         0         0
  TCP/443                   25      7704         9       668        16      7036
  UDP/123                    4       304         2       152         2       152
  TCP/113                    2       120         1        60         1        60
  UDP/80                     1        69         1        69         0         0
  UDP/570                   12       552        12       552         0         0

└ 11 entries ─────────── Elapsed time:   0:02 ──────────────────────────────────────┘
 Protocol data rates (kbits/s):     12.00 in       157.40 out       169.40 total
 Up/Down/PgUp/PgDn-scroll window  S-sort  X-exit
```

Protocol Breakdown

IPTraf - Examples



```
IPTraf
┌──── PktsIn ─── IP In ─ BytesIn ─ InRate  PktsOut ── IP Out  BytesOut OutRate ┐
 Ethernet HW addr: 000cf1c958a0 on eth0
 └     5117      5117   2844697    347.6     5635      5635   2036523   237.8
 Ethernet HW addr: 000f90434b7f on eth0
 └     5632      5632   2036094    237.8     5117      5117   2844697   347.6
 Ethernet HW addr: 01005e7ffffa on eth0
 └        3         3       429      0.0        0         0         0     0.0

└ 3 entries ── Elapsed time:   0:00 ── InRate and OutRate are in kbits/sec ──┘
Up/Down/PgUp/PgDn-scroll window  S-sort  X-exit
```

Layer 2 Breakdown

Find

An Old tool with some
new applications

Find - Overview

- Part of the Unix and Linux Toolkits
- Commonly part of a Standard Operating Environment
- Multi Test Case searching tool

Find - Examples

```
# Display all files owned by user id 1000 in /home
find /home -uid 1000
find /home -user user1000


# Delete files that have been in /tmp for over 90 days
find /tmp -mtime +90  -delete
find /tmp ! -mtime -90  -exec rm -v {} \;
```

Find - Operators

```
              AND:    expr1         expr2
                      expr1 -a      expr2
                      expr1 -and    expr2
              NOT:    expr1 !       expr2
                      expr1 -not    expr2
               OR:    expr1 -o      expr2
                      expr1 -or     expr2
ALL (evaluate both):  expr1  ,      expr2
```

Find - Examples

```
# Recursive Grep for platforms who don't have grep -r

find . -type f -exec grep {} \; -exec echo {} \;

# Change Directory Permissions for Users Home Dir's to
# 700 and remove read/write to there fetchmail config files.

find /home (-type d ! -perm 700 -exec chmod 700 \;), (-type f
-iname ".fetchmailrc -exec chmod g-rw,o-rw \;)
```

Find - Examples

```
# Move Logfiles that are over 30 days old into /var/log/OLD/
# and attach what year and month they belong to.

find /var/log -mtime +30 -exec mv {} /var/log/OLD/{}.`date +%Y%M`
\; -exe bzip2 /home/backups/logs/OLD/{}.`date +%Y%M` \;

# Given a users MailDir is in /var/mail/<username>/ delete
# new email that is over 60 days old, and read email that is
# over 30 days old.
 find /var/mail -mindepth 3 -maxdepth 3 -type f  -mtime +60
-wholename "*/new/*" -o -mtime +30 -wholename "*/cur/*"
```

cfengine

Network Configuration
and Control Tool

A High Level Overview
and Quick Examples

cfengine - Introduction

- Tool for setting up and maintaining computer systems
- Extremely powerful for administrating a medium to large network
- Customizable for any sort of network layout
- Disadvantage: Steep Learning Curve.

cfengine - Components

- The Server: cfservd
  - Contains a collection of rules which you want to apply to your LAN
- The Client: cfagent
  - The Agent which is installed on each client you wish to remotely manage. Responsible for receiving instructions from a central server, and carrying out jobs which it has been instructed to conduct.

cfengine – Components (cont)

- The Scheduler cfexecd
  - Manages the execution of jobs and ensures the system operates smoothly.

- Other agents responsible for various other tasks such as setting up authentication keys (cfkeys), and running jobs manually (cfrun)

cfengine – Example Uses

- Checking file permissions and ownerships; fixing them if required.
- Restarting failed daemons/servers.
- Installing software remotely, including updates.
- Editing files remotely.
- Executing commands remotely.
- Configuring interfaces, routing, and DNS.
- Compressing, deleting, or otherwise managing files or directories.

cfengine - Rules

- Main rules file is cfagent.conf
- Rule file is broken into sections known as Actions
- Two types of actions:
  - Functional Actions: Actually do a job
  - Meta Actions: Control how cfengine should work.
- Order of execution controlled by "actionsequence" control option
- Order of action rules in file does not matter.

cfengine – Rule Format

```
control:
actionsequence = ( action1, action2, action3 )

action1:
action definition/commands

action2:
Class|Host|Domain
action definition/commands

action3:
! Class
action definition/commands
```

cfengine - Classes

- Used as test cases for hosts
- Matched in a IF, ELSE IF, ELSE style
- Predefined or Custom Classes
- Predefined Classes:

  ultrix, sun4, sun3, hpux, hpux10, aix, solaris, osf, irix4, irix, irix64 sco, freebsd, netbsd, openbsd, bsd4_3, newsos, solarisx86, aos, nextstep, bsdos, linux, debian, cray, unix_sv, GnU, NT

cfengine – cfagent.conf example

```
control:
        domain = ( linux.conf.au )
        access = ( root )
        cfrunCommand = ( "/usr/sbin/cfagent" )
        actionsequence = ( resolve )
        maxage = ( 7 )

resolve:
        "search linux.conf.au"
        192.168.255.254
        "# Automatically Edit with cfengine"
```

cfengine – Example Actions (1/4)

```
#
# Fix File Permissions

files:
/etc/sudoers mode=0440 owner=root group=root action=fixall
/etc/passwd mode=644 owner=root group=root action=fixall
/etc/shadow mode=640 owner=root group=shadow action=fixall
/etc/gshadow mode=440 owner=root group=root action=fixall
```

cfengine – Example Actions (2/4)

```
#
# Add a line to a config and restart daemon

editfiles:
          {
              /etc/munin/munin-node.conf
      AppendIfNoSuchLine "allow ^192\.168\.255\.1$"
      RunScript "/etc/init.d/munin-node restart"
    }
```

cfengine – Example Actions (3/4)

```
#
# Change SSHD Config to disallow root login

editfiles:
{
/etc/ssh/sshd_config
ReplaceAll "PermitRootLogin Yes" With "PermitRootLogin No"
RunScript "/etc/init.d/ssh reload"
}
```

cfengine – Example Actions (4/4)

```
# Distributing a global ssh_known_hosts
        control:
        macosx::
              ssh_known_hosts = ( /etc/ssh_known_hosts )

        freebsd|linux|openbsd::
              ssh_known_hosts = ( /etc/ssh/ssh_known_hosts )

        copy:
              any::
                    ${masterfiles}/etc/ssh/ssh_known_hosts
                    dest=${ssh_known_hosts}
                    mode=0444
                    server=${policyhost}
                    type=checksum backup=false
```

cfengine - References

- www.debian-administration.org
  - A simple overview of CFengin (good starting place)
- www.cfenging.org
  - The Cfengine Homepage including in-depth tutorial
- www.cfwiki.org
  - cfenging Wiki pages including example cfagent configs.

Others we didn't have time to present

But you may be interested in...

- Freenx
- dar
- fish
- vsftpd
- nickle
- ulog
- interfacemon
- check-updates
- named-checkconf
- xen
- wget
- screen
- ethereal
- tripwire
- rbackup
- nail

Questions?

Email:
simon@darkmere.gen.nz
edward@toomuchwork.net