

# Glasgow Site Report

June 2010

A. Pickford



# Desktops/Laptops

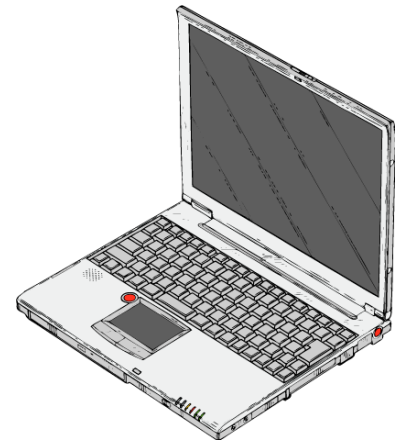
- Desktops

- Relatively unchanged for last few years
- ~ 50 'front line' desktop/lab pcs + older pcs
- Mix of SL5, SL4 & WinXP
- current spec 3.0 GHz dual core cpu, 4 GB ram
- unattended install (kickstart) for SL + cfengine configuration
- unattended install for WinXP (+ batch script for add on)



- Laptops

- ~ 40 laptops
- Older laptops mix of Dells and Lenovos
- Moved to Macbook Pros for latest purchase
- VirtualBox for SL4/5 environment emulation



# Batch System



- Demand for both SL4 and SL5 batch systems
- Currently have:
  - 3 x 1U Intel boxes, 2 x systems per box
  - 2 x 2.50GHz Quad core processors, 16 GB ram
  - torque/maui
  - scientific linux 4 (64 bit)
- Plan to add ex Scotgrid nodes to take over SL4 batch service and upgrade new machines to SL5
- On/off usage pattern mostly unchanged - either fully loaded (30%) or nothing



# Services



- Disc access via nfs and samba
- Backup – to disc, using dirvish, 6 month history
  - User home areas only (20 GB per user)
  - Backup machine located outside the building
- Typical user facing services:
  - local web pages and TWiki
  - printing
  - subversion repo
  - windows terminal servers

# Servers

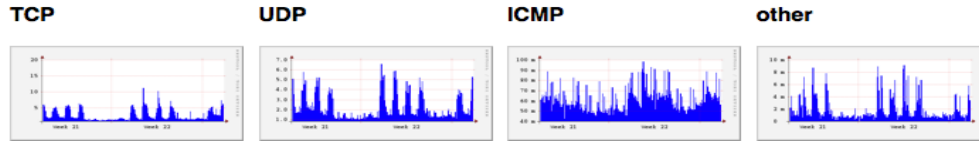
- 2 storage machines
  - 48 x 1TB discs, raid 6 ~ 72TB usable storage
  - SL5, xfs filesystem
- Other servers mostly SL5 with some legacy SL4 system to be phased out this summer + Windows 2003 terminal and printer server boxes
- Moving away from many low spec spec servers to fewer higher spec machines running Xen virtualization
  - Each guest running one service
- Firebridge box between PPE network and outside world
  - Monitor traffic with softflowd and nfsen



# Softflowd & nfsen

Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▾

Profile: live

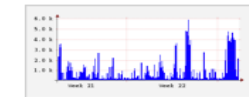


**Profileinfo:**  
 Type: live  
 Max: unlimited  
 Exp: never  
 Start: Aug 30 2009 - 00:00 GMT  
 End: Jun 08 2010 - 15:20 GMT

t<sub>start</sub> 2010-05-31-15:25

t<sub>end</sub> 2010-06-05-14:25

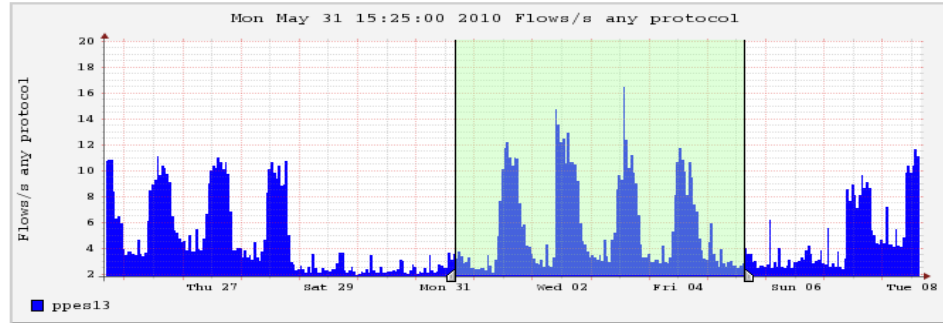
Packets



Traffic



Lin Scale  Stacked Graph  
 Log Scale  Line Graph



Select Time Window Display: 2 weeks << < | ^ > >> >|

▼ Statistics timeslot May 31 2010 - 15:25 - Jun 05 2010 - 14:25

Channel:	Flows:					Packets:				Traffic:					
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> ppes13	5.7/s	3.0/s	2.5/s	0.1/s	0.0/s	978.9/s	941.6/s	37.0/s	0.2/s	0.0/s	7.5 Mb/s	7.4 Mb/s	76.7 kb/s	125.6 b/s	12.5 b/s

All None Display:  Sum  Rate

## Netflow Processing

Source: Filter:

ppes13

All Sources and <none>

```
** nfdump -M /var/nfsen/profiles-data/live/ppes13 -T -R 2010/05/31/nfcapd.201005311525:2010/06/05/nfcapd.201006051425 -n 20
nfdump filter:
any
```

Aggregated flows 1764768

Top 20 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Tos	Packets	Bytes	Flows
2010-06-01 02:03:26.999	4295323.617	TCP	130.209.203.16:22	172.20.220.231:34151	.AP.SF	0	5.3 M	7.8 G	4
2010-06-02 10:06:26.999	4311239.075	TCP	142.90.115.206:80	194.36.1.2:2331	.AP.SF	0	5.2 M	7.2 G	4
2010-06-02 10:06:25.997	4311535.098	TCP	142.90.115.205:80	194.36.1.2:2316	.AP.SF	0	5.1 M	7.1 G	4
2010-06-02 02:03:30.999	4295327.870	TCP	130.209.203.16:22	172.20.220.231:56950	.AP.SF	0	4.5 M	6.6 G	4
2010-06-02 10:56:35.998	4306150.627	TCP	142.90.115.203:80	194.36.1.2:2325	.AP.SF	0	3.8 M	5.2 G	3
2010-06-04 02:04:34.999	4295149.227	TCP	130.209.203.16:22	172.20.220.231:59648	.AP.SF	0	3.2 M	4.7 G	3
2010-06-05 02:09:18.999	4295145.603	TCP	130.209.203.16:22	172.20.220.231:39763	.AP.SF	0	3.1 M	4.6 G	3
2010-06-02 11:43:07.995	4308996.499	TCP	142.90.115.204:80	194.36.1.2:2338	.AP.SF	0	3.0 M	4.2 G	3
2010-06-03 15:06:01.712	4296338.899	TCP	172.20.19.104:445	130.209.203.62:49169	.AP.SF	0	1.6 M	2.4 G	3
2010-06-03 14:21:33.997	4294968.004	TCP	130.209.16.58:445	130.209.203.61:49169	.AP.SF	0	1.6 M	2.4 G	2
2010-06-01 12:00:33.999	4294156.721	TCP	84.53.138.65:80	194.36.1.2:49622	.AP.SF	0	1.4 M	2.0 G	1
2010-06-03 02:10:43.909	4293005.283	TCP	130.209.203.16:22	172.20.220.231:34650	.AP.SF	0	1021632	1.4 G	1
2010-06-04 16:24:47.834	4287297.476	TCP	84.53.133.143:80	194.36.1.119:2058	.AP.SF	0	845431	766.0 M	1
2010-06-02 16:18:41.936	4286526.651	TCP	95.140.226.137:1935	194.36.1.120:4097	.AP.SF	0	513630	691.6 M	1
2010-06-01 11:21:53.133	4294489.725	TCP	131.169.98.135:23523	194.36.1.217:52396	.AP.SF	0	487139	659.7 M	1
2010-06-01 11:21:42.965	4294500.854	TCP	131.169.98.46:20990	194.36.1.217:54944	.AP.SF	0	476236	644.9 M	1
2010-06-02 14:04:33.530	4293731.201	TCP	194.36.1.2:37796	130.246.44.150:22	.AP.SF	0	524603	623.7 M	1
2010-05-31 15:52:34.977	4633540.537	UDP	194.80.134.6:46015	194.36.1.2:46015	.....	0	1.7 M	592.6 M	7
2010-06-01 11:30:49.348	4294842.990	TCP	128.142.222.136:20383	194.36.1.217:59727	.AP.SF	0	403668	546.6 M	1
2010-06-01 11:31:14.615	4294816.593	TCP	128.142.211.5:20383	194.36.1.217:49360	.AP.SF	0	387394	524.6 M	1

Summary: total flows: 2428466, total bytes: 373.9 G, total packets: 400.2 M, avg bps: 679406, avg pps: 88, avg bpp: 956  
 Time window: 2010-05-31 14:20:17 - 2010-07-25 07:25:37  
 Total flows processed: 2428466, Records skipped: 0, Bytes read: 126348140  
 Sys: 2.327s flows/second: 1043314.6 Wall: 3.518s flows/second: 690216.3

# Twiki Server

- Twiki server hacked in August 2009
  - Used mangled twiki search to execute arbitrary code
  - Tried several kernel exploits to (successfully) get root privilege
  - Started using twiki server in a denial of service attack
  - A lesson in always keeping outward facing services fully patched
  - Added an nfsen alert to pick up excess network traffic

# Nfsen alerts

Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

**Alerts details: TrafficFlood**

Trigger	Status	Last Triggered
armed	<input checked="" type="checkbox"/> enabled	2009-09-01-13:50

Filter applied to 'live' profile:  
ppes13 any

Conditions based on total flow summary:

0 Flows/s > 500  
10 min average value

Conditions based on individual Top 1 statistics:

Conditions based on plugin:

**Trigger:**  
Each time after 1 x condition = true, and block next trigger for 3 cycles

**Action:**  
 No action  
 Send alert email To: a.pickford@physics.gla.ac.uk  
 Subject: nfsen alert: traffic flood  
 Call plugin: No alert plugins available

**Alert Infos:**  
Last cycle: 2010-06-08-15:35





# Future

- Ditch nfs
  - Just not secure
  - Move to afs
- Servers
  - Finnish move to SL5
  - More virtualization
- Batch system
  - Add SL5 batch system