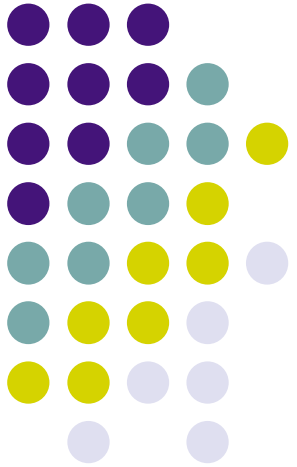
IPv6 Experiences at a campus site

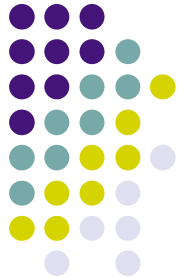


Tim Chown
tjc@ecs.soton.ac.uk
School of Electronics and Computer Science
University of Southampton

21st May 2008

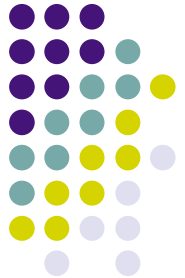
UKNOF 10, Wolverhampton

Scenario



- Large department network
  - 1,900 active IPv4 addresses in use
  - 4,200 user accounts
- Dual-stack IPv6 deployment
  - c. 50 Cisco switch/routers, 6509 at core
- Aim to offer all core services dual-stack
  - DNS, MX, www, login, etc
  - Facilitate option to use IPv6, and IPv6-only devices
- Upstream provider has IPv6
  - LeNSE regional network and JANET core

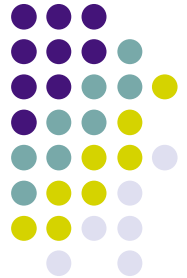
A selection of experiences



- Will try to cover a taste of some of the interesting topics we've encountered
- Lots of things Just Work too :)

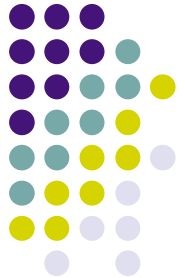
- Address management / DHCPv6
- Firewall / IDS
- IPv6 transport email / spam
- IPv6 Netflow
- Rogue RAs
- IPv6 multicast

Address management



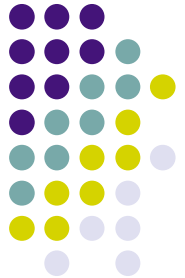
- Campus allocated 2001:630:d0::/48 by JANET
  - ECS Department using 2001:630:d0:f000::/52
  - We allocate IPv6 prefixes congruent with IPv4 prefixes
- No ‘proven’ DHCPv6 client/server available yet
  - ISC DHCPv6 just out (4.0), FreeRADIUS team starting
  - Windows Vista has DHCPv6 client
- Initial deployments use Stateless Autoconfiguration
  - Addresses manually added to DNS (yuk)
  - Manually configured server addresses
  - Ideally disable IPv6 Privacy Addresses

DHCPv6



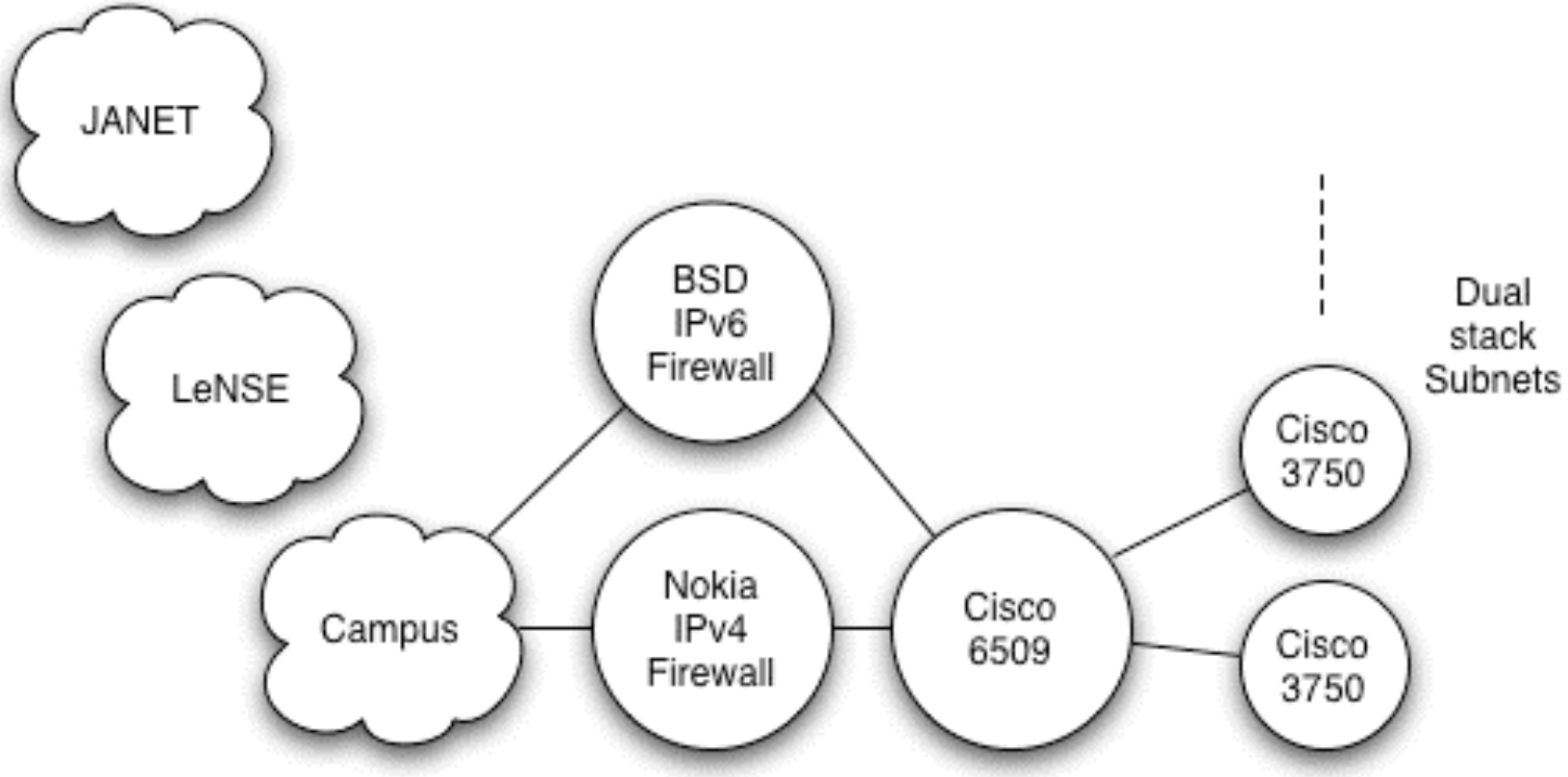
- We want to migrate to DHCPv6 as soon as we can
  - Testing ISC DHCPv6 now
- Prefer managed address approach
  - Familiar to our administrators from IPv4 usage
  - Improves accountability of users, though we are also deploying 802.1x (wireless now, wired later)
  - Can couple DHCPv6 with DNS management tools
  - Privacy addresses can make management complex
    - Which addresses belong to the same hosts?
- Some issues in dual-stack DHCPv6
  - Largely around response consistency (see RFC4477)

Firewall / IDS

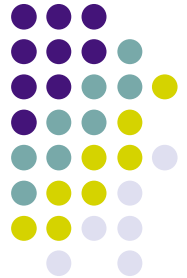


- Our IPv4 firewall is a Checkpoint product
  - IPv6 support not complete
  - Thus have parallel BSD IPv6 firewall running pf
- Overall pf is pretty good
  - Issue is keeping policy in sync with IPv4 firewall
- Snort IDS has IPv6 transport inspection in v2.8.0
  - But doesn't have IPv6 header-specific rules yet
- Traditional port scanning not practical in IPv6
  - See RFC5157, e.g. suggests random DHCPv6 pools
  - We usually only see 'sweeps' to published IPv6 addresses

Split firewalls

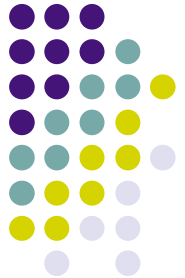


Some pf log examples



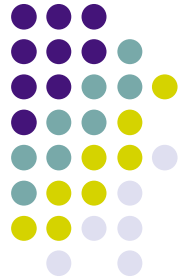
- Repeated access from 6to4 host:
  - 18:53:57.916696 2002:521c:5775::521c:5775.49198 > 2001:630:d0:f111:b9d8:7888:163f:c1f8.50681: S 1295485292:129 5485292(0) win 8192 <mss 1220,nop,wscale 8,[|tcp]>
  - 18:53:57.917067 2002:521c:5775::521c:5775.49197 > 2001:630:d0:f111:5d66:4e5f:ac6b:74b8.50681: S 912913819:9129 13819(0) win 8192 <mss 1220,nop,wscale 8,[|tcp]>
  - …
  - 82.29.87.117 = …cust884.nott.cable.ntl.com
- Odd source address and malformed packet:
  - 14:11:54.520861 2001:0:d5c7:a2ca:ce:1969:a527:c263 > 2001:630:d0:f102::25a: no next header
  - 14:11:54.985592 2001:0:d5c7:a2ca:ce:1969:a527:c263 > 2001:630:d0:f102::25b: no next header

IPv6 transport mail



- Guidelines documented in RFC 3974
  - Various scenarios discussed
  - Recommends both A and AAAA records for MXes
- We run with 4 MXes
  - mx.ecs.soton.ac.uk. 3600 IN AAAA 2001:630:d0:f110::25c
  - mx.ecs.soton.ac.uk. 3600 IN AAAA 2001:630:d0:f102::25b
  - mx.ecs.soton.ac.uk. 3600 IN AAAA 2001:630:d0:f102::25c
  - mx.ecs.soton.ac.uk. 3600 IN AAAA 2001:630:d0:f110::25b
  - mx.ecs.soton.ac.uk. 3600 IN A 152.78.68.132
  - mx.ecs.soton.ac.uk. 3600 IN A 152.78.68.137
  - mx.ecs.soton.ac.uk. 3600 IN A 152.78.71.14
  - mx.ecs.soton.ac.uk. 3600 IN A 152.78.71.210
- Appears to work well for us

IPv6 transport spam



- Started measuring email received over (last hop) IPv6 transport in April
  - Done by modification to MailScanner
  - [plug: a nice/free product written by Julian Field at ECS]
  - X- header added so users can detect transport protocol
- Typically c. 1000 IPv6 messages per day
  - Roughly half of that is spam
  - Level of spam has dropped recently (under investigation)
  - We're beginning to look at sources, type of spam, etc
- Approx 600,000 IPv4 transport mails per day

ECS Email Service: Messages Entering ECS Over IPv6

http://pigeon.ecs.soton.ac.uk/mrtg/v6mail/

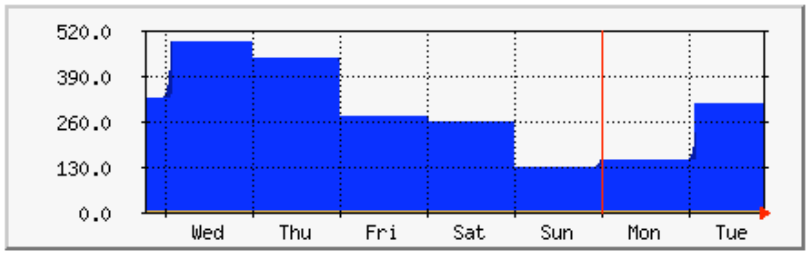
mac osx screen capture

ECS Email Service : Messages Entering ECS Over IPv6

This page will refresh automatically every 24 hours. These figures now include attempts to guess usernames.

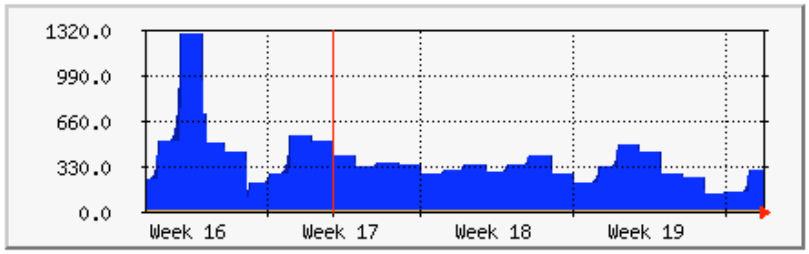
The statistics were last updated **Tuesday, 20 May 2008 at 21:35**

`Weekly' Graph (30 Minute Average)



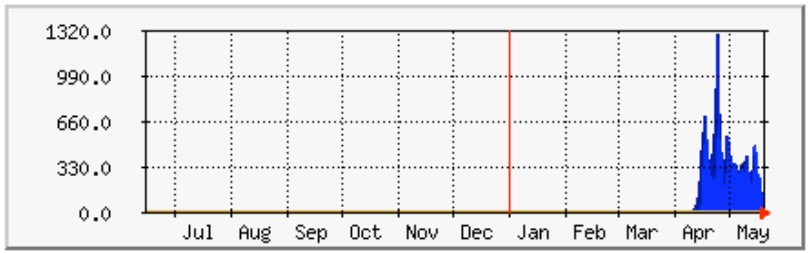
Max messages:493.0 Messages (0.2%) Average messages:294.0 Messages (0.1%) Current messages:314.0 Messages (0.2%)

`Monthly' Graph (2 Hour Average)



Max messages:1304.0 Messages (0.7%) Average messages:379.0 Messages (0.2%) Current messages:314.0 Messages (0.2%)

`Yearly' Graph (1 Day Average)



Max messages:1304.0 Messages (0.7%) Average messages:378.0 Messages (0.2%) Current messages:154.0 Messages (0.1%)

ECS Email Service: Spam E-Mail Messages Entering ECS Over IPv6

http://pigeon.ecs.soton.ac.uk/mrtg/v6spam/

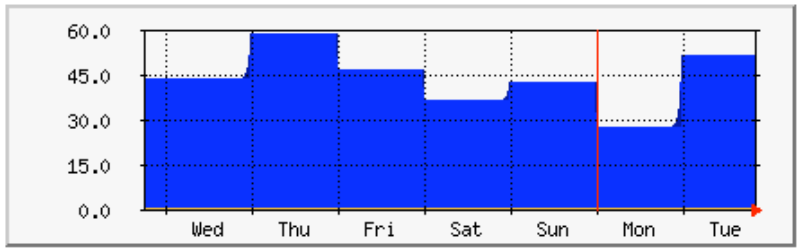
mac osx screen capture

ECS : Spam E-Mail Entering ECS Over IPv6

This page will refresh automatically every 24 hours. These figures now include attempts to guess usernames.

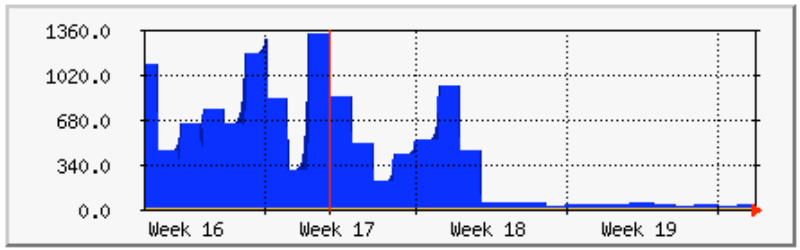
The statistics were last updated **Tuesday, 20 May 2008 at 21:35**

`Weekly' Graph (30 Minute Average)



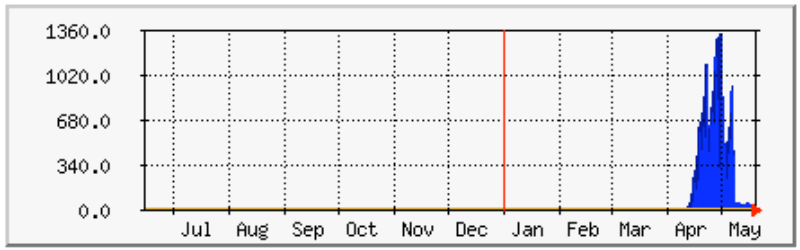
Max messages:59.0 Messages (0.0%) Average messages:44.0 Messages (0.0%) Current messages:52.0 Messages (0.0%)

`Monthly' Graph (2 Hour Average)



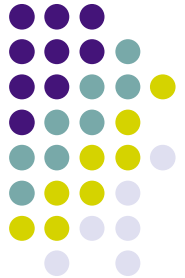
Max messages:1337.0 Messages (0.7%) Average messages:396.0 Messages (0.2%) Current messages:52.0 Messages (0.0%)

`Yearly' Graph (1 Day Average)



Max messages:1337.0 Messages (0.7%) Average messages:403.0 Messages (0.2%) Current messages:29.0 Messages (0.0%)

IPv6 Netflow



- Cisco IOS supports IPv6 Netflow (v9)
  - We send data from a 6509 core router
  - Collect and query/view data with nfsen
    - Supports Netflow v9 and IPv6 storage/queries
    - http://nfsen.sourceforge.net/
  - A nice, flexible Netflow visualisation tool
  - Can give us hints to out of profile activity

- Example:
  - Look at IPv6 port 25 (SMTP) flows in general
  - Drill down into specific port 25 activity

NFSEN – Profile live May 20 2008 – 08:40

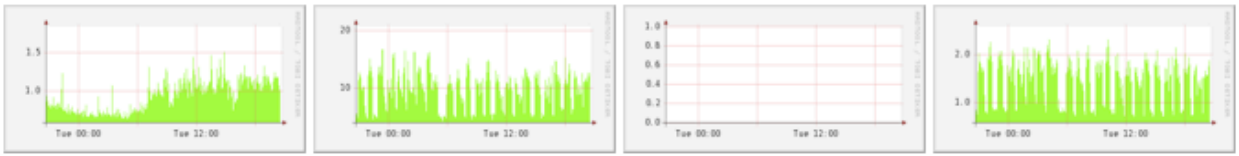
http://mrtg.ecs.soton.ac.uk/nfsen.php

Google

Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

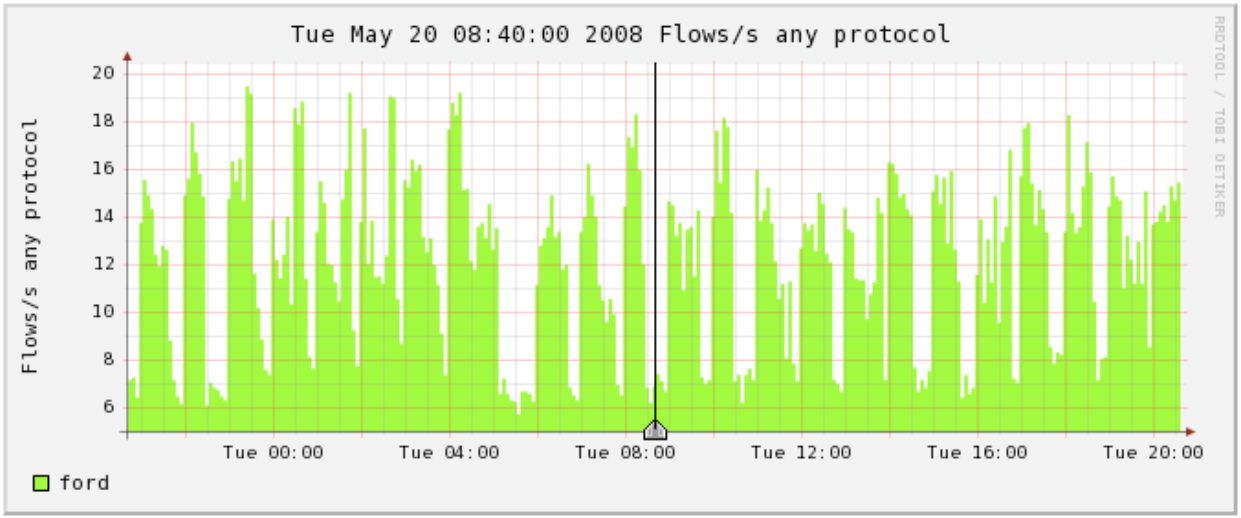
Profile: live

TCP **UDP** **ICMP** **other**



Profileinfo:

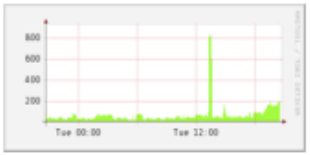
Type: live
Max: 100.0 GB
Exp: never
Start: Mar 15 2008 - 19:30 GMT
End: May 20 2008 - 20:40 GMT



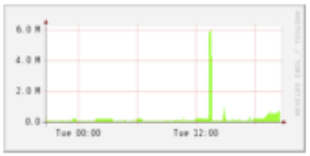
t_{start} 2008-05-20-08-40

t_{end} 2008-05-20-08-40

Packets



Traffic



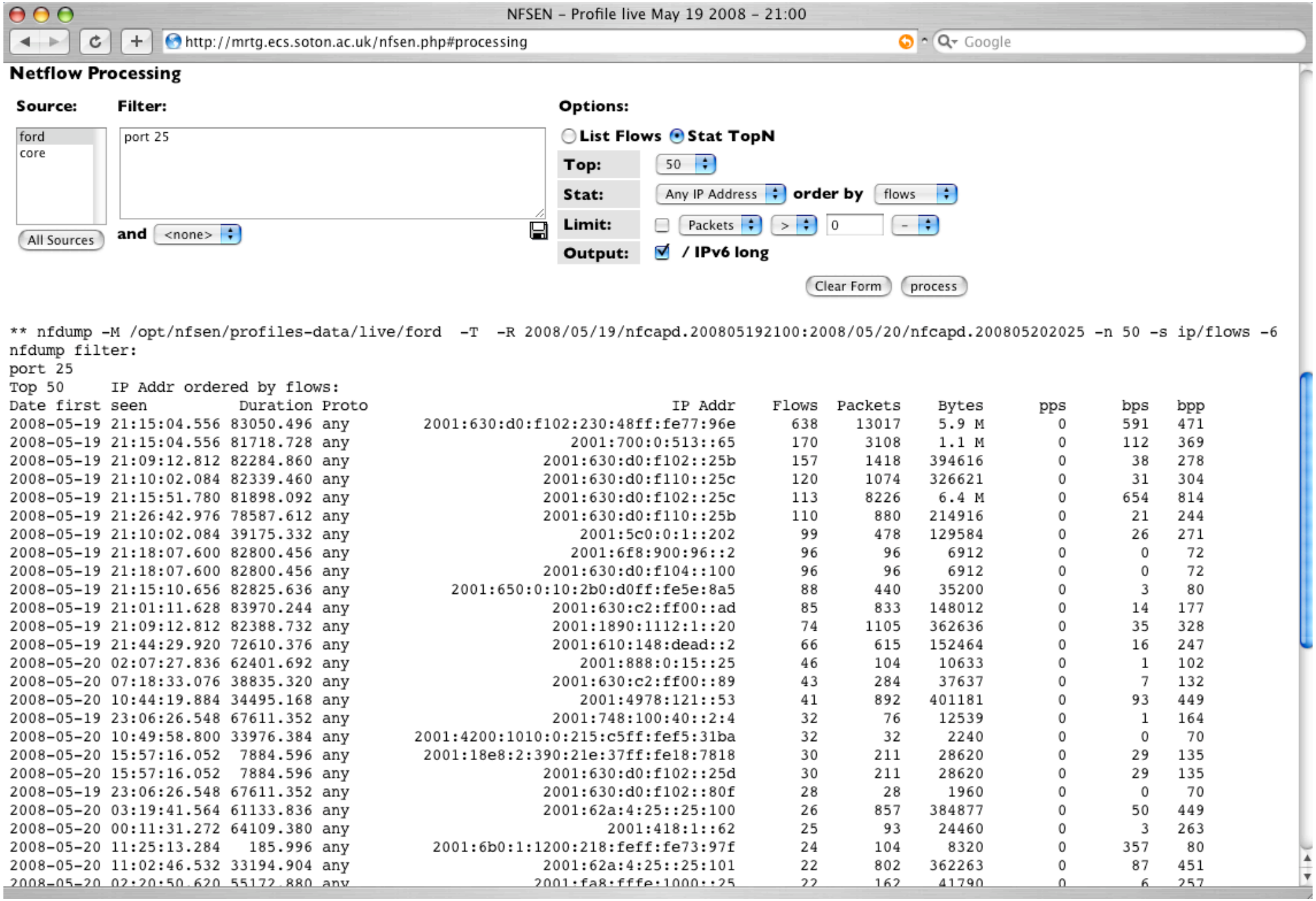
Select | Single Timeslot | Display: | 1 day | << | < | | | ^ | > | >> | >|

Lin Scale | Stacked Graph

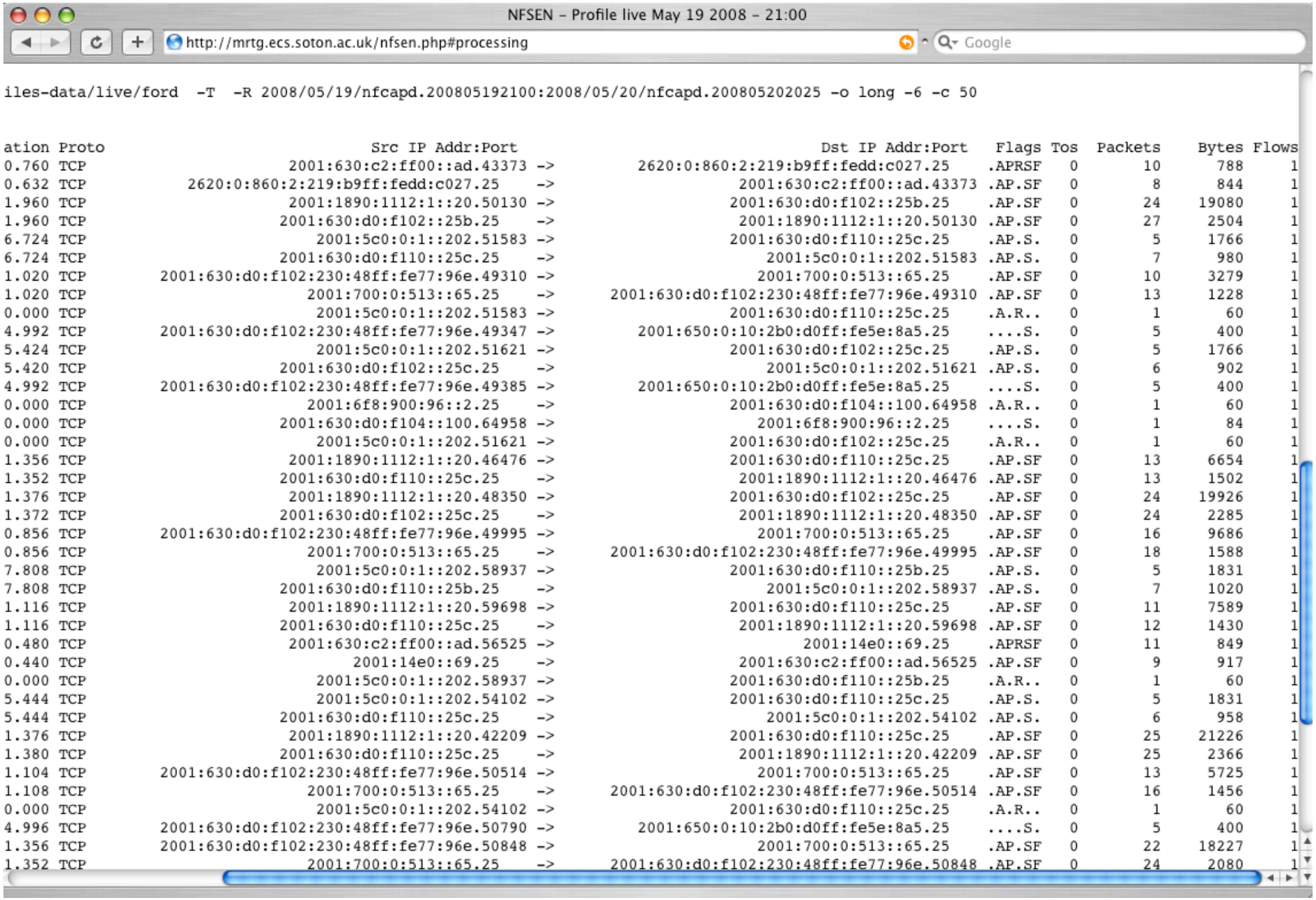
Log Scale | Line Graph

Statistics timeslot May 20 2008 - 08:40

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ ford	6.9 /s	0.9 /s	5.2 /s	0 /s	0.8 /s	23.3 /s	2.1 /s	18.9 /s	0 /s	2.3 /s	27.6 kb/s	2.5 kb/s	23.1 kb/s	0 b/s	2.1 kb/s
☐ core	213.0 /s	107.2 /s	102.5 /s	3.3 /s	0.0 /s	5.6 k/s	4.1 k/s	1.4 k/s	35.3 /s	152.9 /s	21.2 Mb/s	18.0 Mb/s	2.9 Mb/s	27.7 kb/s	186.9 kb/s

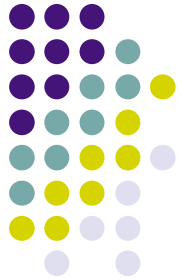



```
** nfdump -M /opt/nfsen/profiles-data/live/ford  -T  -R 2008/05/19/nfcapd.200805192100:2008/05/20/nfcapd.200805202025 -n 50 -s ip/flows -6
nfdump filter:
port 25
Top 50     IP Addr ordered by flows:
Date first seen          Duration Proto                                IP Addr     Flows  Packets    Bytes      pps      bps   bpp
2008-05-19 21:15:04.556 83050.496 any       2001:630:d0:f102:230:48ff:fe77:96e      638    13017    5.9 M        0      591   471
2008-05-19 21:15:04.556 81718.728 any                     2001:700:0:513::65      170     3108    1.1 M        0      112   369
2008-05-19 21:09:12.812 82284.860 any                  2001:630:d0:f102::25b      157     1418   394616        0       38   278
2008-05-19 21:10:02.084 82339.460 any                  2001:630:d0:f110::25c      120     1074   326621        0       31   304
2008-05-19 21:15:51.780 81898.092 any                  2001:630:d0:f102::25c      113     8226    6.4 M        0      654   814
2008-05-19 21:26:42.976 78587.612 any                  2001:630:d0:f110::25b      110      880   214916        0       21   244
2008-05-19 21:10:02.084 39175.332 any                     2001:5c0:0:1::202       99      478   129584        0       26   271
2008-05-19 21:18:07.600 82800.456 any                    2001:6f8:900:96::2       96       96     6912        0        0    72
2008-05-19 21:18:07.600 82800.456 any                  2001:630:d0:f104::100      96       96     6912        0        0    72
2008-05-19 21:15:10.656 82825.636 any          2001:650:0:10:2b0:d0ff:fe5e:8a5      88      440    35200        0        3    80
2008-05-19 21:01:11.628 83970.244 any                   2001:630:c2:ff00::ad      85      833   148012        0       14   177
2008-05-19 21:09:12.812 82388.732 any                   2001:1890:1112:1::20      74     1105   362636        0       35   328
2008-05-19 21:44:29.920 72610.376 any                   2001:610:148:dead::2      66      615   152464        0       16   247
2008-05-20 02:07:27.836 62401.692 any                     2001:888:0:15::25       46      104    10633        0        1   102
2008-05-20 07:18:33.076 38835.320 any                   2001:630:c2:ff00::89      43      284    37637        0        7   132
2008-05-20 10:44:19.884 34495.168 any                     2001:4978:121::53       41      892   401181        0       93   449
2008-05-19 23:06:26.548 67611.352 any                    2001:748:100:40::2:4     32       76    12539        0        1   164
2008-05-20 10:49:58.800 33976.384 any     2001:4200:1010:0:215:c5ff:fef5:31ba      32       32     2240        0        0    70
2008-05-20 15:57:16.052  7884.596 any      2001:18e8:2:390:21e:37ff:fe18:7818      30      211    28620        0       29   135
2008-05-20 15:57:16.052  7884.596 any                  2001:630:d0:f102::25d      30      211    28620        0       29   135
2008-05-19 23:06:26.548 67611.352 any                  2001:630:d0:f102::80f      28       28     1960        0        0    70
2008-05-20 03:19:41.564 61133.836 any                  2001:62a:4:25::25:100      26      857   384877        0       50   449
2008-05-20 00:11:31.272 64109.380 any                       2001:418:1::62        25       93    24460        0        3   263
2008-05-20 11:25:13.284   185.996 any       2001:6b0:1:1200:218:feff:fe73:97f      24      104     8320        0      357    80
2008-05-20 11:02:46.532 33194.904 any                  2001:62a:4:25::25:101      22      802   362263        0       87   451
2008-05-20 02:20:50.620 55172.880 any                  2001:fa8:fffe:1000::25     22      162    41790        0        6   257
```



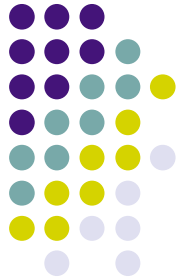

```
iles-data/live/ford  -T  -R 2008/05/19/nfcapd.200805192100:2008/05/20/nfcapd.200805202025 -o long -6 -c 50

ation Proto                          Src IP Addr:Port                                Dst IP Addr:Port   Flags Tos  Packets     Bytes Flows
0.760 TCP                    2001:630:c2:ff00::ad.43373 ->        2620:0:860:2:219:b9ff:fedd:c027.25    .APRSF   0       10       788     1
0.632 TCP          2620:0:860:2:219:b9ff:fedd:c027.25    ->                  2001:630:c2:ff00::ad.43373 .AP.SF   0        8       844     1
1.960 TCP                    2001:1890:1112:1::20.50130 ->                 2001:630:d0:f102::25b.25    .AP.SF   0       24     19080     1
1.960 TCP                   2001:630:d0:f102::25b.25    ->                  2001:1890:1112:1::20.50130 .AP.SF   0       27      2504     1
6.724 TCP                       2001:5c0:0:1::202.51583 ->                 2001:630:d0:f110::25c.25    .AP.S.   0        5      1766     1
6.724 TCP                   2001:630:d0:f110::25c.25    ->                     2001:5c0:0:1::202.51583 .AP.S.   0        7       980     1
1.020 TCP        2001:630:d0:f102:230:48ff:fe77:96e.49310 ->                   2001:700:0:513::65.25    .AP.SF   0       10      3279     1
1.020 TCP                    2001:700:0:513::65.25    ->      2001:630:d0:f102:230:48ff:fe77:96e.49310 .AP.SF   0       13      1228     1
0.000 TCP                    2001:5c0:0:1::202.51583 ->                 2001:630:d0:f110::25c.25    .A.R..   0        1        60     1
4.992 TCP        2001:630:d0:f102:230:48ff:fe77:96e.49347 ->    2001:650:0:10:2b0:d0ff:fe5e:8a5.25    ....S.   0        5       400     1
5.424 TCP                    2001:5c0:0:1::202.51621 ->                 2001:630:d0:f102::25c.25    .AP.S.   0        5      1766     1
5.420 TCP                   2001:630:d0:f102::25c.25    ->                  2001:5c0:0:1::202.51621 .AP.S.   0        6       902     1
4.992 TCP        2001:630:d0:f102:230:48ff:fe77:96e.49385 ->    2001:650:0:10:2b0:d0ff:fe5e:8a5.25    ....S.   0        5       400     1
0.000 TCP                    2001:6f8:900:96::2.25    ->                 2001:630:d0:f104::100.64958 .A.R..   0        1        60     1
0.000 TCP                   2001:630:d0:f104::100.64958 ->                    2001:6f8:900:96::2.25    ....S.   0        1        84     1
0.000 TCP                       2001:5c0:0:1::202.51621 ->                 2001:630:d0:f102::25c.25    .A.R..   0        1        60     1
1.356 TCP                    2001:1890:1112:1::20.46476 ->                 2001:630:d0:f110::25c.25    .AP.SF   0       13      6654     1
1.352 TCP                   2001:630:d0:f110::25c.25    ->                  2001:1890:1112:1::20.46476 .AP.SF   0       13      1502     1
1.376 TCP                    2001:1890:1112:1::20.48350 ->                 2001:630:d0:f102::25c.25    .AP.SF   0       24     19926     1
1.372 TCP                   2001:630:d0:f102::25c.25    ->                  2001:1890:1112:1::20.48350 .AP.SF   0       24      2285     1
0.856 TCP        2001:630:d0:f102:230:48ff:fe77:96e.49995 ->                   2001:700:0:513::65.25    .AP.SF   0       16      9686     1
0.856 TCP                    2001:700:0:513::65.25    ->      2001:630:d0:f102:230:48ff:fe77:96e.49995 .AP.SF   0       18      1588     1
7.808 TCP                    2001:5c0:0:1::202.58937 ->                 2001:630:d0:f110::25b.25    .AP.S.   0        5      1831     1
7.808 TCP                   2001:630:d0:f110::25b.25    ->                     2001:5c0:0:1::202.58937 .AP.S.   0        7      1020     1
1.116 TCP                    2001:1890:1112:1::20.59698 ->                 2001:630:d0:f110::25c.25    .AP.SF   0       11      7589     1
1.116 TCP                   2001:630:d0:f110::25c.25    ->                  2001:1890:1112:1::20.59698 .AP.SF   0       12      1430     1
0.480 TCP                    2001:630:c2:ff00::ad.56525 ->                       2001:14e0::69.25    .APRSF   0       11       849     1
0.440 TCP                          2001:14e0::69.25    ->                 2001:630:c2:ff00::ad.56525 .AP.SF   0        9       917     1
0.000 TCP                    2001:5c0:0:1::202.58937 ->                 2001:630:d0:f110::25b.25    .A.R..   0        1        60     1
5.444 TCP                    2001:5c0:0:1::202.54102 ->                 2001:630:d0:f110::25c.25    .AP.S.   0        5      1831     1
5.444 TCP                   2001:630:d0:f110::25c.25    ->                     2001:5c0:0:1::202.54102 .AP.S.   0        6       958     1
1.376 TCP                    2001:1890:1112:1::20.42209 ->                 2001:630:d0:f110::25c.25    .AP.SF   0       25     21226     1
1.380 TCP                   2001:630:d0:f110::25c.25    ->                  2001:1890:1112:1::20.42209 .AP.SF   0       25      2366     1
1.104 TCP        2001:630:d0:f102:230:48ff:fe77:96e.50514 ->                   2001:700:0:513::65.25    .AP.SF   0       13      5725     1
1.108 TCP                    2001:700:0:513::65.25    ->      2001:630:d0:f102:230:48ff:fe77:96e.50514 .AP.SF   0       16      1456     1
0.000 TCP                    2001:5c0:0:1::202.54102 ->                 2001:630:d0:f110::25c.25    .A.R..   0        1        60     1
4.996 TCP        2001:630:d0:f102:230:48ff:fe77:96e.50790 ->    2001:650:0:10:2b0:d0ff:fe5e:8a5.25    ....S.   0        5       400     1
1.356 TCP        2001:630:d0:f102:230:48ff:fe77:96e.50848 ->                   2001:700:0:513::65.25    .AP.SF   0       22     18227     1
1.352 TCP                    2001:700:0:513::65.25    ->      2001:630:d0:f102:230:48ff:fe77:96e.50848 .AP.SF   0       24      2080     1
```

Rogue RAs



- Seeing the problem quite often
- Multiple prefixes and default routers on a link
  - Discussed in draft-chown-v6ops-rogue-ra-00
  - Administrator error (perhaps on VLAN)
  - User error (almost always Windows ICS)
  - Malicious intent
    - cf. THC hack kit: http://freeworld.thc.org/thc-ipv6/
- Need to detect and correct
  - When Windows ICS is used the rogue RA appears as a 6to4 (2002::/16) prefix **and** a site local prefix
  - ICS can also be a problem for IPv4 (DHCP)
  - Have written an improved rafixd
- IETF says ‘use SeND’, but not ready, even if wanted

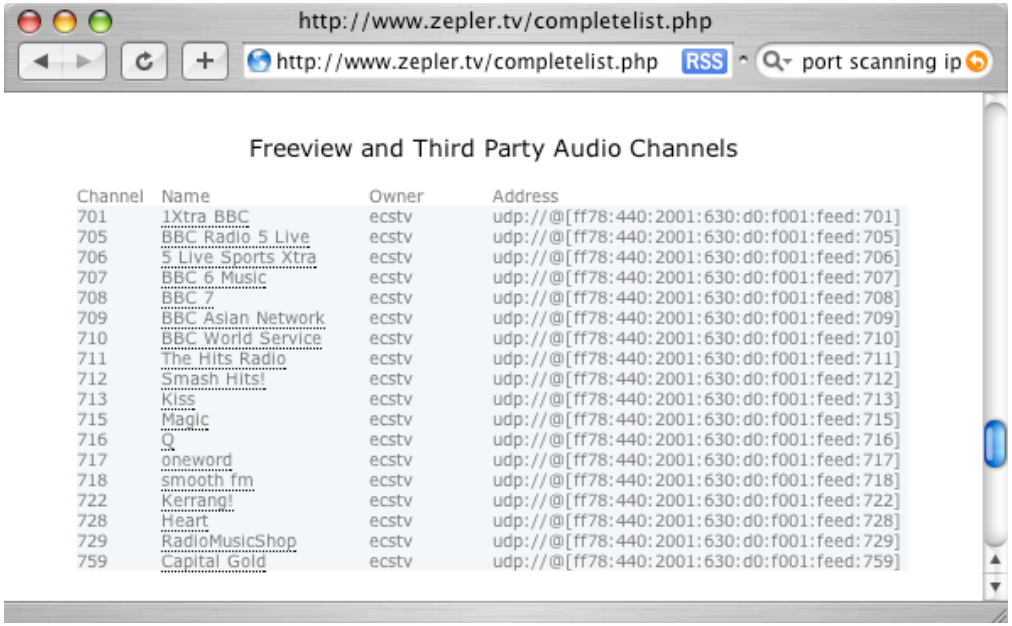
IPv6 multicast



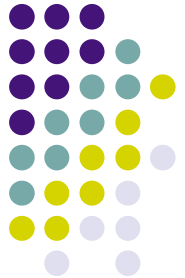
- We use IPv6 multicast for all our multicast services
  - Hard to get global group addresses for IPv4
- IPv6 has some nice advantages
  - Embedded RP (RFC3956) - addresses easy to get, and no MSDP involved
  - Scoping explicit in the group address - helps with scope boundary filters
- Currently have a tunnel to a JANET router
  - But IPv6 multicast widely deployed in academic networks
- Have 100+ freeview/radio groups in ECS
  - ECS-TV uses VideoLAN, etc

ECS-TV

- Freeview IPv6 multicast TV and radio
  - Also unicast VoD of archived content
- Uses Embedded-RP addresses
  - Run IPv6 RP on a Cisco 7206
  - Content is mainly organisational scope

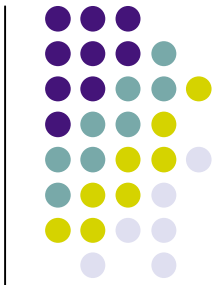


Training material



- We have run some IPv6 workshops
  - Includes hands-on exercises etc
  - See http://www.ipv6.org.uk (link to workshop)
- Working on material within projects
  - 6DISS: http://www.6diss.org
  - 6DEPLOY: http://www.6deploy.org
- Much has been developed from 6NET experience
  - Huge volume of reports at http://www.6net.org
- All training material is freely reusable given acknowledgement of source

Summary



- There's still a few rough edges to IPv6 deployment for a campus-type site
  - But at the same time we've not been adversely affected by going dual-stack early, and have gained lots of experience
- Also some interesting research/experiment areas
  - Address management with DHCPv6
  - Handling Rogue RAs and detecting (THC) attacks
  - IPv6 transport-specific IDS rules
  - IPv6 spam/virus sources
  - Activity from IPv6 transition-based sources (Teredo etc)
- Very interested to work with ISPs…