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

- JANET
- LeNSE
- Campus
- BSD IPv6 Firewall
- Nokia IPv4 Firewall
- Cisco 6509
- Dual stack Subnets
- Cisco 3750
- Cisco 3750
Some pf log examples

- Repeated access from 6to4 host:
    2001:630:d0:f111:b9d8:7888:163f:c1f8.50681: S 1295485292:1295485292(0)
    win 8192 <mss 1220,nop,wscale 8,[tcp]>
    2001:630:d0:f111:5d66:4e5f:ac6b:74b8.50681: S 912913819:912913819(0) win
    8192 <mss 1220,nop,wscale 8,[tcp]>
  - ...
  - 82.29.87.117 = …cust884.nott.cable.ntl.com

- Odd source address and malformed packet:
    no next header
    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

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 Messages (0.2%)  Average messages: 294 Messages (0.1%)  Current messages: 314 Messages (0.2%)

**'Monthly' Graph (2 Hour Average)**

Max messages: 1046 Messages (0.7%)  Average messages: 379 Messages (0.2%)  Current messages: 314 Messages (0.2%)

**'Yearly' Graph (1 Day Average)**

Max messages: 1386 Messages (0.7%)  Average messages: 378 Messages (0.2%)  Current messages: 154 Messages (0.1%)
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)

*Monthly* Graph (2 Hour Average)

*Yearly* Graph (1 Day Average)
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
  - 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
** nftump -M /opt/nfsen/profiles-data/live/ford -T -R 2008/05/19/nfcapd.200805192100:2008/05/20/nfcapd.200805202025 -n 50 -8 ip/flows -6
ndump filter:

port 25

<table>
<thead>
<tr>
<th>Date first seen</th>
<th>Duration</th>
<th>IP Addr</th>
<th>Flows</th>
<th>Packets</th>
<th>Bytes</th>
<th>pps</th>
<th>bps</th>
<th>bpp</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:15:04:556</td>
<td>83050.496</td>
<td>638</td>
<td>13017</td>
<td>5.9 M</td>
<td>0</td>
<td>591</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:15:04:556</td>
<td>83178.728</td>
<td>170</td>
<td>3108</td>
<td>1.1 M</td>
<td>0</td>
<td>112</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:09:12:812</td>
<td>82284.860</td>
<td>157</td>
<td>1418</td>
<td>394616</td>
<td>0</td>
<td>38</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:10:02:084</td>
<td>82339.460</td>
<td>120</td>
<td>1074</td>
<td>326621</td>
<td>0</td>
<td>31</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:26:42:976</td>
<td>78567.612</td>
<td>110</td>
<td>880</td>
<td>21496</td>
<td>0</td>
<td>21</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:10:02:084</td>
<td>39175.332</td>
<td>99</td>
<td>478</td>
<td>129584</td>
<td>0</td>
<td>26</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:18:07:600</td>
<td>82800.456</td>
<td>96</td>
<td>96</td>
<td>6912</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:18:07:600</td>
<td>82800.456</td>
<td>96</td>
<td>96</td>
<td>6912</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2008-05-19</td>
<td></td>
<td>21:01:11:628</td>
<td>83970.244</td>
<td>85</td>
<td>833</td>
<td>148012</td>
<td>14</td>
<td>177</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>02:07:27:836</td>
<td>62401.692</td>
<td>46</td>
<td>1063</td>
<td>104000</td>
<td>1</td>
<td>102</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>07:18:13:076</td>
<td>38835.320</td>
<td>43</td>
<td>284</td>
<td>37637</td>
<td>7</td>
<td>132</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>10:49:15:800</td>
<td>39796.384</td>
<td>32</td>
<td>76</td>
<td>12539</td>
<td>1</td>
<td>164</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>15:57:16:052</td>
<td>7884.596</td>
<td>32</td>
<td>32</td>
<td>2240</td>
<td>0</td>
<td>70</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>15:57:16:052</td>
<td>7884.596</td>
<td>30</td>
<td>211</td>
<td>28620</td>
<td>29</td>
<td>135</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>03:19:41:564</td>
<td>61133.836</td>
<td>28</td>
<td>28</td>
<td>1960</td>
<td>0</td>
<td>70</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>00:11:31:272</td>
<td>64109.380</td>
<td>26</td>
<td>857</td>
<td>384877</td>
<td>50</td>
<td>449</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>11:25:11:284</td>
<td>185.996</td>
<td>25</td>
<td>244</td>
<td>26400</td>
<td>3</td>
<td>263</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>11:02:46:532</td>
<td>33194.904</td>
<td>24</td>
<td>104</td>
<td>8320</td>
<td>357</td>
<td>80</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>11:02:46:532</td>
<td>33194.904</td>
<td>22</td>
<td>802</td>
<td>362263</td>
<td>87</td>
<td>451</td>
</tr>
<tr>
<td>2008-05-20</td>
<td></td>
<td>11:02:46:532</td>
<td>33194.904</td>
<td>22</td>
<td>162</td>
<td>41730</td>
<td>6</td>
<td>257</td>
</tr>
<tr>
<td>Action</td>
<td>Proto</td>
<td>Src IP Addr:Port</td>
<td>Dst IP Addr:Port</td>
<td>Flags</td>
<td>Tos</td>
<td>Packets</td>
<td>Bytes</td>
<td>Flows</td>
</tr>
<tr>
<td>--------</td>
<td>-------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-------</td>
<td>-----</td>
<td>---------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>0.760</td>
<td>TCP</td>
<td>2001:630:c2ff:000:ad:43373</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.632</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.960</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.020</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.020</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.992</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.422</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.992</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.356</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.352</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.376</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.372</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.856</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.856</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.808</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.808</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.116</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.116</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.480</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.440</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.996</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.358</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.104</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.108</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.996</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.358</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.352</td>
<td>TCP</td>
<td>2001:630:0:86</td>
<td>.A.F.R.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

[Freeview and Third Party Audio Channels]
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…