ABone Status and Progress

Active Nets Workshop, Portland, OR
May 24, 2000

Bob Braden (ISI) and Steve Dawson (SRI)
ABone Overview

The ABone is composed of:
• diverse OS platforms distributed across many organizations,
• managed remotely using Anetd,
• executing permanent and temporary EEs, and
• monitored by ABone Coordination Center (ABOCC).
Diverse OS Platforms ...

- Now: 50 Unix-based core nodes:
  - 23 Linux nodes
  - 17 FreeBSD nodes
  - 5 Solaris nodes
  - 5 (down)
- No active nets node OSs yet

- Classes of nodes with different access/usage rules
  - 26 general Internet nodes
  - 14 CAIRN nodes
  - 10 Utah Testbed cluster
# Node/Anetd Status

- See [www.isi.edu/abone/abocc.html](http://www.isi.edu/abone/abocc.html)

<table>
<thead>
<tr>
<th>Host</th>
<th>OS</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>switchware.research.telcordia.com</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>active.netsec.tislabs.com</td>
<td>linux</td>
<td>RELEASE_1_5</td>
</tr>
<tr>
<td>peacock.cs.utah.edu</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>son.isi.edu</td>
<td>bsd44</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>aergr.aero.org</td>
<td>bsd44</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>saregama.cis.upenn.edu</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>sys94.cs.washington.edu</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>merce.cs.umass.edu</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>Chengho.cs.ucla.edu</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>Ultus.CS.UCLA.EDU</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>galileo.cere.pa.cnr.it</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>capri.metanetworks.org</td>
<td>linux</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>sarcd.dcs.uky.edu</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>mandolin.dcs.uky.edu</td>
<td>solaris</td>
<td>STABLE_1_SNAP_2000_04_20</td>
</tr>
<tr>
<td>dulcimer.dcs.uky.edu</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>isipc.cairn.net</td>
<td>bsd44</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>iblpc.cairn.net</td>
<td>bsd44</td>
<td>RELEASE_1_4_1</td>
</tr>
<tr>
<td>isrpc.cairn.net</td>
<td>bsd44</td>
<td>RELEASE_1_4_1</td>
</tr>
</tbody>
</table>
Managed Remotely using Anetd

- Each node runs multiple Ees under Anetd control
- Node security: important issue [later in this talk].
- Only local node administrator has login & root passwords
- Anetd runs in USER mode

Steve Dawson will discuss Anetd status and plans
... Executing Permanent EEs

- Permanent EEs now executing in the ABone:
  - ASP EE v. 1.1 (ISI)
  - ANTS v. 1.3.1 (U Washington) [djw will describe]
    See http://www.isi.edu/abone -> …

- Future permanent EEs (?)
  PLAN
  Netscript
  SANTS
  …?

- Temporary EEs:
  experimenter can always instantiate an EE for testing, for isolation, or for private virtual topology.
Per-EE Virtual Topology

ASP EE Topology

Refresh Done!!!
... Monitored by the ABOCC

- ABone Coordination Center
- Web pages http://www.isi.edu/abone
  (includes many cross-references to SRI Web pages)
- Registration [Dawson]
- Monitoring and configuration tools [Primitive beginning]
- Working with users
How do active packets get injected into the core?

A. Dynamic Active Nets Topology Extension -- DANTE
   - Couple an edge node into core EE’s virtual topology.
   - DHCP-analog.
   - EE-dependent protocol, but ISI spec has generic description.
   - So far, implemented for ANTS v1.3.1.

B. Remote User App (UA) API to EE
   - ASP EE on end system: listens on TCP port, accepts messages specifying AA and AA-specific payload.
   - Can also be used for remote out-of-band initiation of AAs.
   - ISI using this for launching active packets in core without DANTE, and for OOB active monitoring of ASP.
   - Will implement DANTE, too.
Node Security

- OS must be secure against code introduced by Anetd
  - NOT an option: cannot allow downloading arbitrary untrusted EE code
- Anetd client signs commands, and server gets public key from local ACL file.
  - ACL => what principal may execute Anetd commands under what account(s)?
  - TCL => code server from which EEs can be loaded
- ABOCC controls ACL, TCL entries
- Plan to use QCMD to update ACLs dynamically & securely
ABone Accounts

7 accounts on every node, for security partitioning:

- ~abocc: access to Anetd code, ACL, TCL, and JVM config
- ~anpub: all who register at (SRI) Web site
- ~anee1: EE developers for ASP and ANTS EEs [JVM 1.1]
- ~anee2: EE developers needing JVM 1.2
- ~anee3, ~anee4: unassigned
- ~anee5: ABOCC experimental

Each of these accounts has an Anetd process, a ACL file, and a TCL file, and may have specific JVM.
~abocc/ .anetd/ (ACL, TCL, config, log files for ~abocc)

  / anetd / ad.bsd44 (Anetd code)
   / jdk -> link to JDK version

  / <princ ID> / <EE subtree>

~anee1/ .anetd/ (ACL, TCL, config, log files for ~anee1)
  / anetd / -> link to ~abocc/anetd
  / <princ ID> / <EE subtree>

~anee2 / (etc)
• **Node security (cont’d)**

- Security from evil EE or EE developer: not perfect.
- Considering Anetd security improvements: setuid, chroot.
- Java sandboxing helps a lot.
- Anetd installs its own Security Manager for all Java-based EEs
  Each EE can install SM Extension to further restrict actions of its AAs
Account Configuration

- Same ABOCC Web page tool shown earlier...

<table>
<thead>
<tr>
<th>Host</th>
<th>OS</th>
<th>Account</th>
<th>Port</th>
<th>Version</th>
<th>EEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>active.netsec.tislabs.com</td>
<td>linux</td>
<td>anpub</td>
<td>3322</td>
<td>RELEASE_1_5</td>
<td></td>
</tr>
<tr>
<td>abocc</td>
<td></td>
<td></td>
<td>8000</td>
<td>RELEASE_1_5</td>
<td></td>
</tr>
<tr>
<td>anee1</td>
<td></td>
<td></td>
<td>8001</td>
<td>RELEASE_1_5</td>
<td>&quot;128.9.160.165: ASP_EE&quot;, &quot;128.9.160.85: ASP_EE&quot;</td>
</tr>
<tr>
<td>anee2</td>
<td></td>
<td></td>
<td>8003</td>
<td>RELEASE_1_5</td>
<td></td>
</tr>
<tr>
<td>anee3</td>
<td></td>
<td></td>
<td>8004</td>
<td>RELEASE_1_5</td>
<td></td>
</tr>
<tr>
<td>anee4</td>
<td></td>
<td></td>
<td>8005</td>
<td>RELEASE_1_5</td>
<td></td>
</tr>
<tr>
<td>anee5</td>
<td></td>
<td></td>
<td>8006</td>
<td>RELEASE_1_5</td>
<td>&quot;205.178.57.130: abonestat_server&quot;, &quot;205.178.57.130: abonestat_client&quot;</td>
</tr>
<tr>
<td>pcacock.cs.utah.edu</td>
<td>linux</td>
<td>anpub</td>
<td>3322</td>
<td>RELEASE_1_4_1</td>
<td></td>
</tr>
<tr>
<td>abocc</td>
<td></td>
<td></td>
<td>8000</td>
<td>RELEASE_1_4_1</td>
<td></td>
</tr>
<tr>
<td>anee1</td>
<td></td>
<td></td>
<td>8001</td>
<td>RELEASE_1_4_1</td>
<td>&quot;128.9.160.85: ASP_EE&quot;</td>
</tr>
<tr>
<td>anee2</td>
<td></td>
<td></td>
<td>8002</td>
<td>RELEASE_1_4_1</td>
<td></td>
</tr>
<tr>
<td>anee3</td>
<td></td>
<td></td>
<td>8003</td>
<td>RELEASE_1_4_1</td>
<td></td>
</tr>
<tr>
<td>anee4</td>
<td></td>
<td></td>
<td>8004</td>
<td>RELEASE_1_4_1</td>
<td></td>
</tr>
<tr>
<td>anee5</td>
<td></td>
<td></td>
<td>8005</td>
<td>RELEASE_1_4_1</td>
<td>&quot;205.178.57.130: abonestat_server&quot;, &quot;205.178.57.130: abonestat_client&quot;</td>
</tr>
</tbody>
</table>
Network I/O

- Anetd currently supports only **virtual connectivity**
  - UDP tunnels, per-EE virtual address space.
- We will add support for **native IP connectivity**
  - Running in the Internet ‘porridge’ with real IP addresses.
- The Third Way: **virtual native IP connectivity**
  - Virtual IP address space overlaid on the Internet.
  - Using X-Bone; solution for “raisins in the porridge”.
- Under Anetd: packets **[may be] received on stdin**.
  Better: receive packets on designated UDP file descriptor (i.e. local UDP association)
  - No EE change whether/not running in ABone
  - Symmetry for packet input & output
Native I/O Support in Unix

- netcd
  - Network Control Daemon (permit)
  - Runs as root
- EE
- Anetd
- fork
- Filter
- IP forward
- TC
- Divert sockets / ipchains
- Data
  - Control
Obstacles Encountered

… and at least partially overcome… (Whinge slide)

- Major Anetd updates [Dawson]
- CAIRN trunking reconstitution
- Continuing routing problems with CAIRN and vBNS
- JVM version differences, especially Security Manager
- OS version differences, especially FreeBSD
- Multicast (for audio conferences) broken
- Diversity: 40 nodes, 3 OSs, 2 administrative classes, 2 JVMs, 2 permanent EEs.

• Summary: “System integration is Hell!” [Unknown]
ABone Heros and Villains

- **Heros:**
  - Univ of Washington: Andrew Whitaker, David Wetherall
  - TASC: Diane Kiwior, Steve Zabele
  - TIS: Ed Lewis, Steve Schwab
  - ISI: Jeff Kann
  - UPenn: Pankaj Kakkar, Mike McDougall, Carl Gunter

- **Villains:**
  - ISI: Bob Braden, Steve Berson, Jeff Kann
  - Metanetworks: Livio Ricciulli
  - SRI: Steve Dawson, Marco Molteni, Sonia Tsui