

-
-
-

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

Data created: Wed May 17 02:32:13 2000

Host	OS	Version
switchware.research.telcordia.com	N/A	N/A
active.netsec.tislabs.com	linux	RELEASE_1_5
peacock.cs.utah.edu	linux	RELEASE_1_4_1
son.isi.edu	bsd44	RELEASE_1_4_1
aegr.aero.org	bsd44	RELEASE_1_4_1
saregama.cis.upenn.edu	N/A	N/A
sys194.cs.washington.edu	linux	RELEASE_1_4_1
merce.cs.umass.edu	linux	RELEASE_1_4_1
Chengho.cs.ucla.edu	linux	RELEASE_1_4_1
Ulfus.CS.UCLA.EDU	linux	RELEASE_1_4_1
galileo.cere.pa.cnr.it	linux	RELEASE_1_4_1
capri.metanetworks.org	linux	RELEASE_1_4_1
sarod.dcs.uky.edu	N/A	N/A
mandolin.dcs.uky.edu	solaris	STABLE_1_SNAP_2000_04_20
dulcimer.dcs.uky.edu	N/A	N/A
isipc.cairn.net	bsd44	RELEASE_1_4_1
lblpc.cairn.net	bsd44	RELEASE_1_4_1
msrpc.cairn.net	bsd44	RELEASE_1_4_1



Managed Remotely using Anetd

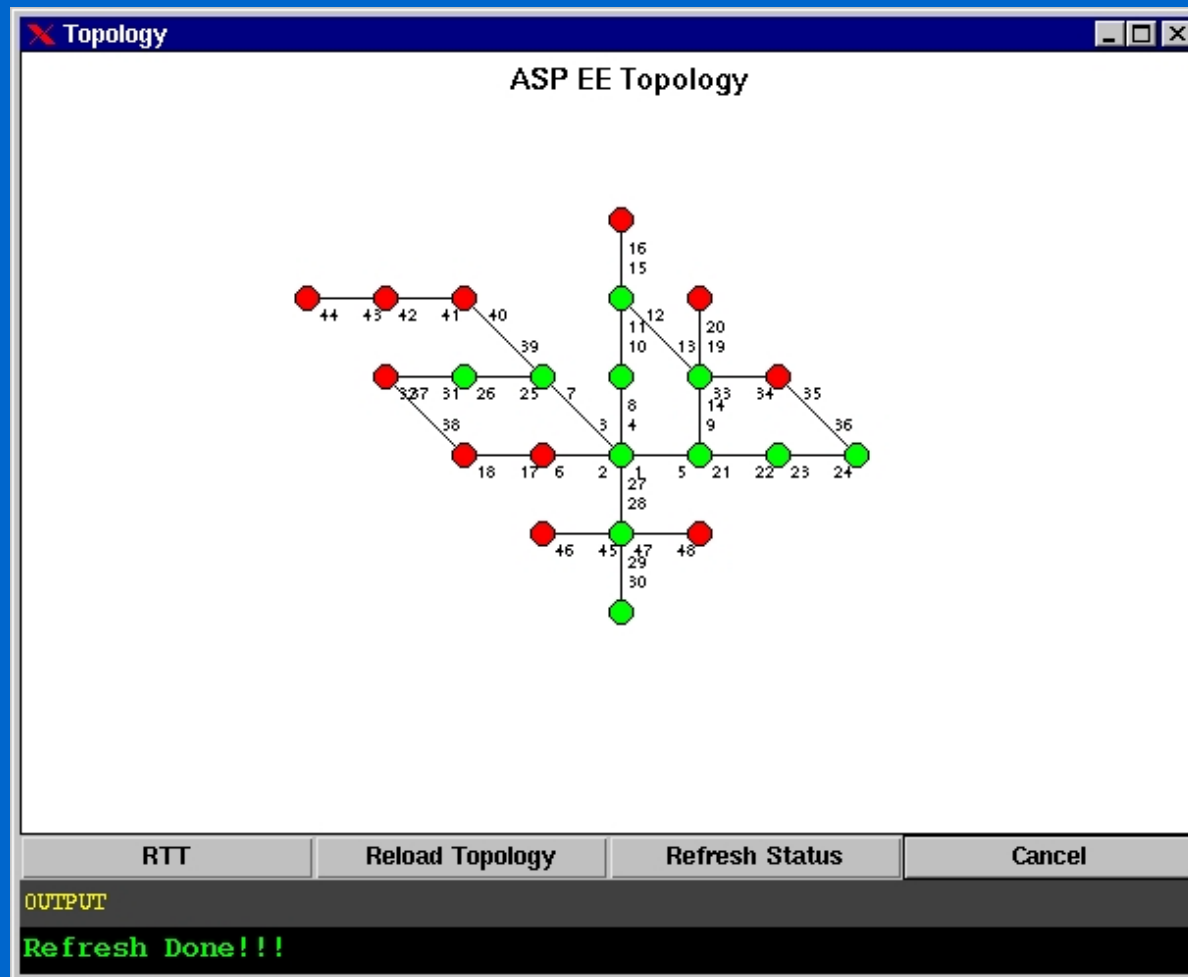
- Each node runs multiple Ees under Anetd control
- Node security: important issue [later in this talk].
- Only local node administrator has login & root passwords
- Anetd runs in USER mode

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





... Monitored by the ABOCC

- ABone Coordination Center
- Web pages <http://www.isi.edu/abone>
(includes many cross-refs to SRI Web pages)
- Registration [Dawson]
- Monitoring and configuration tools [Primitive beginning]
- Working with users



Injecting Active Packets

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.

-
-
-

Directory Structure

~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...

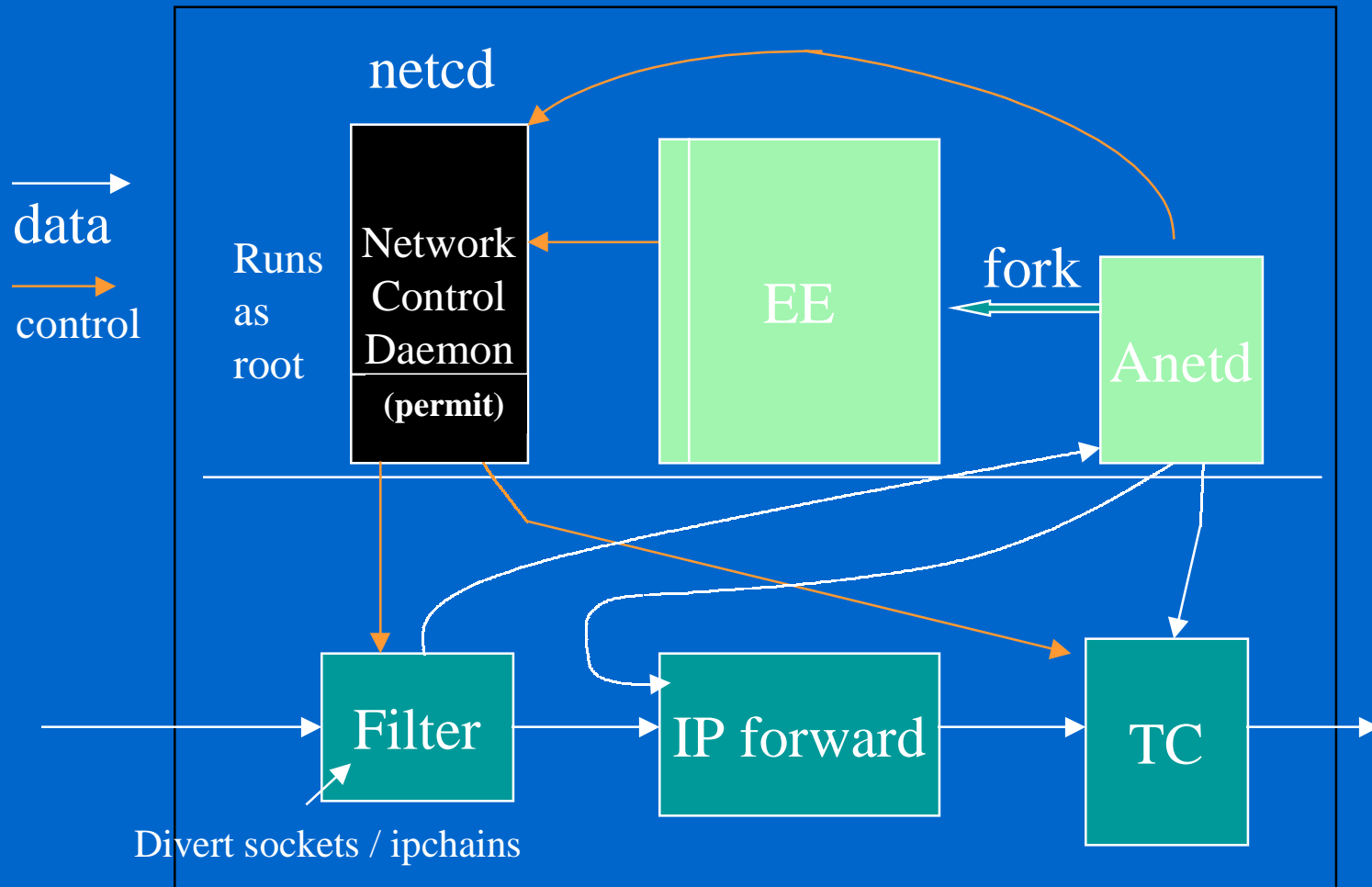
Data created: Wed May 17 11:24:08 2000

Host	OS	Account	Port	Version	EEs
active.netsec.tislabs.com	linux	anpub	3322	RELEASE_1_5	
		abocc	8000	RELEASE_1_5	
		anee1	8001	RELEASE_1_5	"128.9.160.165: ASP_EE " "128.9.160.85: ASP_EE "
		anee2	8003	RELEASE_1_5	
		anee3	8004	RELEASE_1_5	
		anee4	8005	RELEASE_1_5	
peacock.cs.utah.edu	linux	anpub	3322	RELEASE_1_4_1	
		abocc	8000	RELEASE_1_4_1	
		anee1	8001	RELEASE_1_4_1	"128.9.160.85: ASP_EE "
		anee2	8002	RELEASE_1_4_1	
		anee3	8003	RELEASE_1_4_1	
		anee4	8004	RELEASE_1_4_1	
		anee5	8006	RELEASE_1_5	"205.178.57.130: abonestat_server " "205.178.57.130: abonestat_client "
		anee5	8005	RELEASE_1_4_1	"205.178.57.130: abonestat_server " "205.178.57.130: abonestat_client "

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



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