June 1991 BayLISA

Designing, Creating, and Maintaining Large-scale Multi-protocol Inter-network Gateways Using DECWRL as an Extreme Example

Paul Vixie
vixie@decwrl.dec.com
decwrl!vixie
DECWRL::VIXIE

Western Research Laboratory

Goals and Constraints

- Exchange information with the ‘‘outside world’’
- Ease of use - should be transparent to users
- Well-defined failure/delay modes
- No handholding or pulsetaking
- Secure
- Auditable
- Scalable
- Reliable

Requirements of you

- You will need operating system source code and you must not be afraid to use it
- Note that Berkeley's versions of networking utilities such as sendmail are probably better than your vendor's
- Berkeley's stuff is freely available, too - in source form
- Carry a beeper but get mad if someone has to use it
- Be an information junkie -- read mail and usenet, early and often
- Get Perl and use it
- Remember, this is supposed to be fun

Who Are These People, Anyway?

- Internet (was "ARPAnet"); includes NSFnet, Alternet, etc.
- UUCP net ("... from my cold, dead fingers")
- USENET ("Netnews")
- BITNET (yesterday's technology tomorrow)
- X.mumble (you later than you think but still sooner than you'd like)

Services Provided

- Import and export files (FTP)
- Electronic mail and netnews (SMTP, UUCP rmail, BSMTP)
- Remote login (telnet, rlogin, tip)
- Packet-level services (NTP, DNS, distant internal gateways)

Security

- Information security, and the guys who wear their suit jackets indoors
- Controlling access
- FTP (anonymous-only incoming)
- Mail and Netnews (someone just posted sensitive company information to alt.paranoia. how do you notice and what should you do?)
- Remote login (restricted passwd file, nonshared passwords)
- Packet-level services (screening routers)
- Other application-level services (finger user@internalhost@gateway)

Auditing

Basically this means keeping lots of log files around.

- Has a security violation occurred? How do you know? (Company lawyers will want dumps of your disks)
- Are there problems with certain neighbors or data paths?
- Is the through-delay getting too high?
- What's your current capacity and how close are you to exceeding it?
- Why did this mail message bounce? (Or: why am I getting hundreds of copies of it?)
- Do your auditing on a separate computer; statistical computing is hard work and your gateway machines have real-time things to do

Auditing

- Mail Queue Size

```
inet-gw-1.pa.dec.com       Sendmail Queue Display  as of 91/06/20 13:42:32

Top 10 Hosts In Mail Queue  #/msgs      Oldest Message      Newest Message
-------------------------------------------------------------------------
fasolt.pa.dec.com               42   91/06/17 12:43:31   91/06/20 13:33:18
mercury.nwac.sea06.navy.mi      24   91/06/18 07:45:24   91/06/20 13:17:58
xerox.com                        5   91/06/20 13:29:15   91/06/20 13:40:20
decwrl.dec.com                   5   91/06/20 13:24:34   91/06/20 13:42:13
sgi.com                          4   91/06/20 12:44:10   91/06/20 13:40:20
rara.nyo.dec.com                 4   91/06/19 05:48:25   91/06/20 11:00:49
cs.columbia.edu                  3   91/06/20 13:15:39   91/06/20 13:29:48
crd.ge.com                       3   91/06/20 13:17:17   91/06/20 13:38:12
clove.uchicago.edu               3   91/06/20 12:05:52   91/06/20 13:23:05
microsoft.com                    2   91/06/20 13:29:15   91/06/20 13:30:29

TOTAL                          222   91/06/17 12:43:31   91/06/20 13:42:13
```

- Mail Statistics

```
 Syslog    Input: (total)      (mail11)     Output Statistics:
File Date  Msgs Kbytes AvgSz  Sndrs Rcips   Sent AvgDelay Dferd Que'd Other
.0 Jun 19  4710  25979  5648      0     0  10134    22:09  1269     0    41
.1 Jun 18  4508  27128  6162      0     0  13842    06:53   265     0    89
.2 Jun 17  4518  20812  4717      0     0  14223    02:00   272     1   112
.3 Jun 16  1437   8793  6266      0     0   4400    02:47    53     1    24
.4 Jun 15   221   3644 16885      0     0   1166    19:32    33     0     2
```

Scaling and Reliability

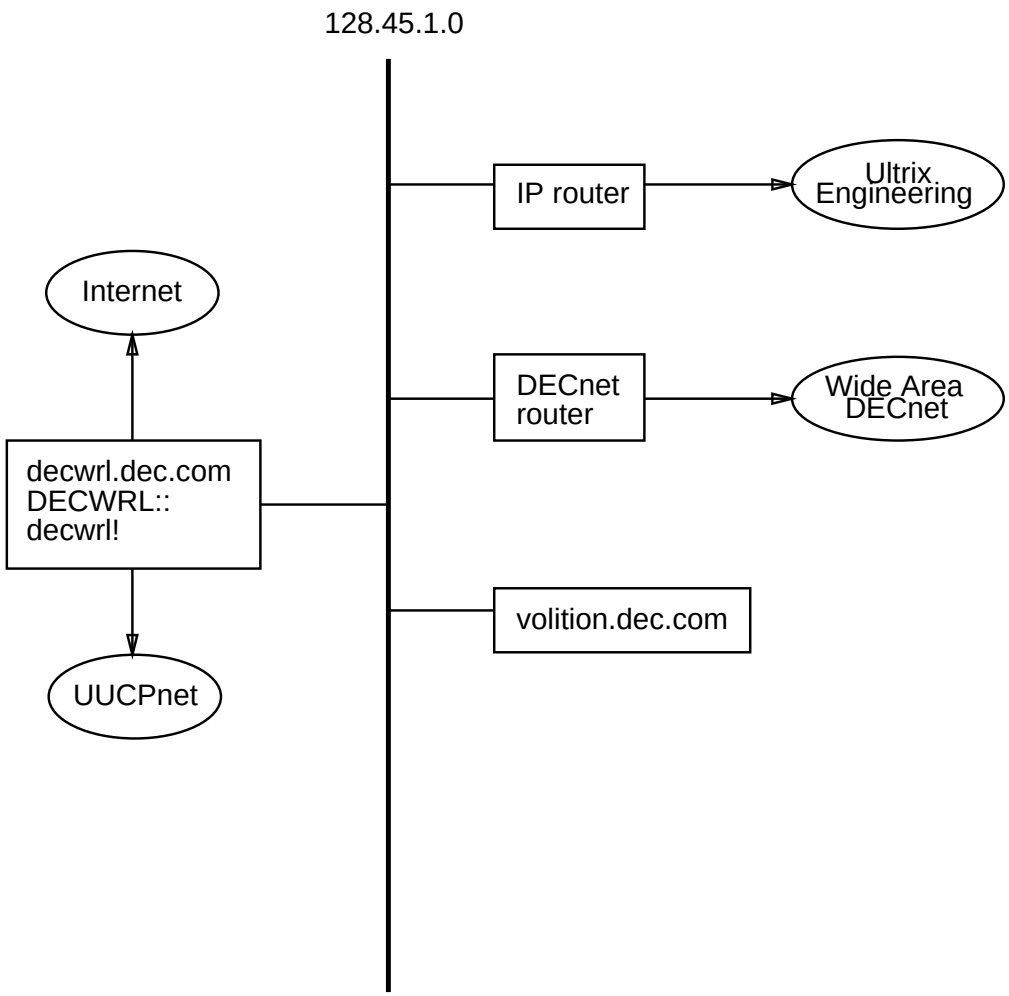
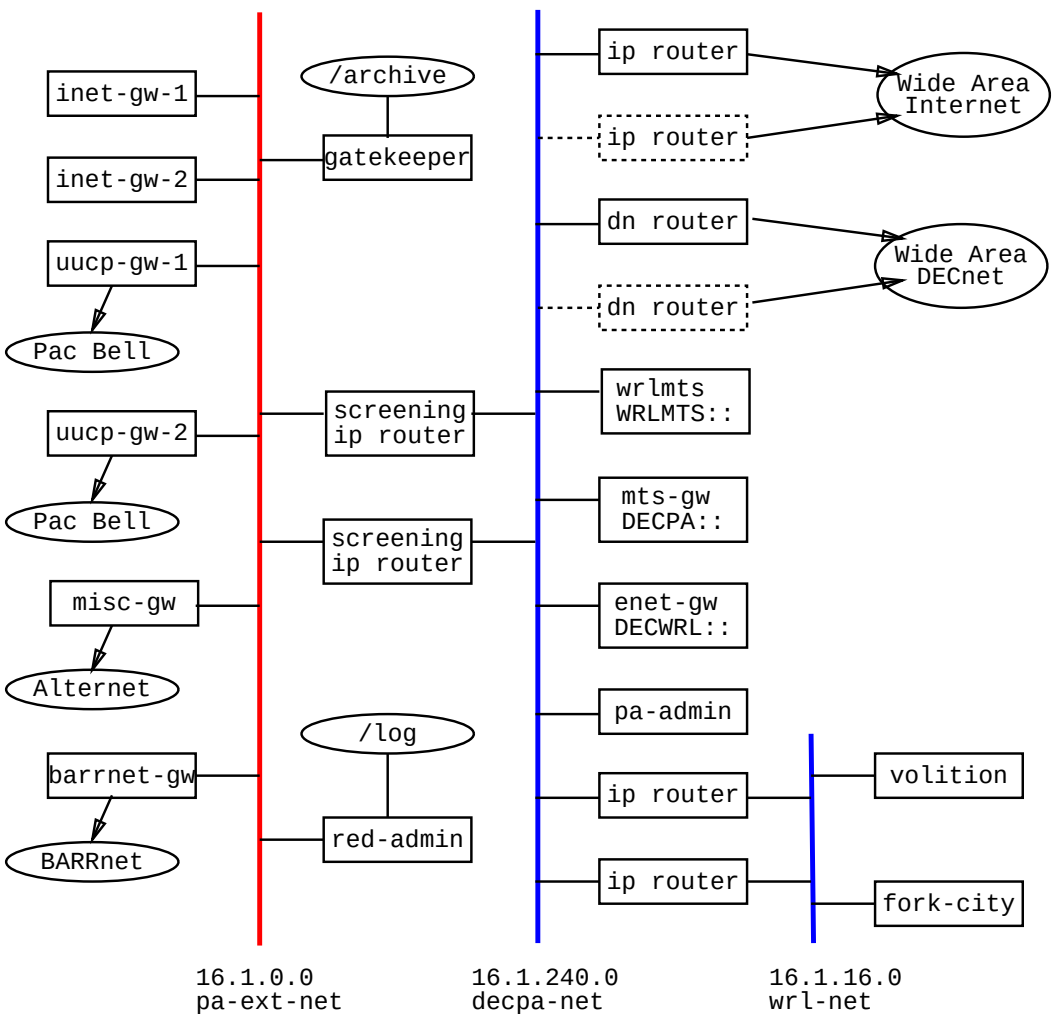
- Success disaster ("file table full", "out of inodes", high delay, etc)
- Single point of failure: one kernel panic and you lose everything
- Don’t put real hostnames in your "From:" headers
- Use MX or CNAME for all advertised names
- Start with a single host and grow as needed
- Convert disasters from "fix it now" to "fix it soon"
- Don’t use NFS or anything else that blocks in the kernel when some other computer is down; your gateway machines should all stand alone

Details: the gateway archive

General problem of safe file transfer not solvable with current technology. Gateway archive satisfies some of the need.

- file systems **`/archive`** and **`/archive/.1`**
- only root can write on it; users must ask to have something published from inside or cached from outside
- publishes world-readable information
- anonymous FTP to gatekeeper.dec.com - inside or out
- read-only NFS by special arrangement
- Available via UUCP as visible root of **`DECWRL!~/`** and **`DECWRL::`**

Digital's Internet in 1988



Digital Palo Alto's Internet in June, 1991