Life and Times of J-ROOT

Piet Barber
Matt Larson
Mark Kosters
Pete Toscano
Agenda

+ History of J-Root
+ IP Address Change – Trends
+ Move to Anycast
J-Root: Historical Query Volume
(February 2001 to present)
J-Root: Query Volume Since Anycasting
(March 2003 to present)
J-Root: Query Volume Since Anycasting
(March 2003 to present, alternate format)
Traffic to a new instance of J in Japan

- New Instance did little to influence total (Green Line)
- Shows that roots have headroom
J-Root: Query Volume to Old/New IP Addresses

J Root Query Volume from 5 November 2002 to Present

- Current IP (192.58.128.30)
- Former IP (198.41.0.10)
J-Root: Address Change Query Volume “Crossover”

J Root Old/New IP Address Crossover in November 2002

Queries per second (4-second average)

Date

Current IP (192.58.128.30)

Former IP (188.41.0.10)
Why Does the old J-root still have traffic?

+ Who is querying the old J root IP address?
+ Methodology:
  + Record a week’s worth of source IP addresses
    + 6 October 2004 through 12 October 2004
  + Within each 24-hour period, retain only IPs that query the old J root at least three times (to rule out priming queries resulting from an out-of-date hints file)
    + 70,000-100,000 IPs per day
  + Aggregate all seven days’ IPs and retain unique list
    + 205,307 unique IP addresses
Who is Querying the old J-Root?

+ Used fpdns 0.9.1 to fingerprint all 205,307 addresses
  + http://www.rfc.se/fpdns
+ As expected, large number of them were unreachable:
  + 139,927 timed out (68%)
+ But those that were reachable proved to be a wide array of implementations
  + 141 different fpdns signatures/fingerprints
  + Details on next slide
Top 25 Implementations Seen at old J-Root

<table>
<thead>
<tr>
<th>Rank</th>
<th>Implementation</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>19453</td>
<td>BIND 9.2.0rc7</td>
<td>9.2.2-P3</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>10252</td>
<td>BIND 9.2.3rc1</td>
<td>9.4.0a0</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>9278</td>
<td>Microsoft Windows 2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4893</td>
<td>Microsoft Windows NT4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4085</td>
<td>TinyDNS 1.05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2756</td>
<td>BIND 9.1.0</td>
<td>9.1.3</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>2651</td>
<td>BIND 9.2.0rc7</td>
<td>9.2.2-P3</td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td>BIND 9.2.3rc1</td>
<td>9.4.0a0</td>
<td></td>
</tr>
<tr>
<td>1635</td>
<td>Microsoft Windows 2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1350</td>
<td>BIND 8.3.0-RC1</td>
<td>8.4.4</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>898</td>
<td>BIND 9.2.0a1</td>
<td>9.2.2-P3</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>781</td>
<td>BIND 8.1-REL</td>
<td>8.2.1-T4B</td>
<td>recursion enabled</td>
</tr>
<tr>
<td>603</td>
<td>BIND 9.2.0rc7</td>
<td>9.2.2-P3</td>
<td>recursion local</td>
</tr>
<tr>
<td>602</td>
<td>BIND 4.9.3</td>
<td>4.9.11</td>
<td></td>
</tr>
<tr>
<td>562</td>
<td>q0r?question section incomplete</td>
<td></td>
<td></td>
</tr>
<tr>
<td>479</td>
<td>q0tq0r?1,IQUERY,0,0,1,1,0,0,NOTIMP,0,0,0,0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>229</td>
<td>BIND 9.1.0</td>
<td>9.1.3</td>
<td></td>
</tr>
<tr>
<td>220</td>
<td>totd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>216</td>
<td>BIND 8.3.0-RC1</td>
<td>8.4.4</td>
<td>recursion local</td>
</tr>
<tr>
<td>209</td>
<td>q0r4q1r21q2r59q7r?connection failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>q0tq0r?1,IQUERY,0,0,1,0,0,0,FORMERR,1,0,0,0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>q0tq0tq7r?1,QUERY,0,0,1,0,0,0,REFUSED,1,0,0,0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>116</td>
<td>q0tq0tq7tq6r?1,UPDATE,0,0,0,1,0,0,NOERROR,1,0,0,0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>incognito DNS Commander v2.3.1.1</td>
<td>4.0.5.1</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>q0r?1,IQUERY,0,0,0,1,0,0,0,REFUSED,1,0,0,0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What’s Going On?

+ We don’t know
+ Old theory: Old J-Root gets traffic from implementations that don’t prime
+ Problem: Lots of recent BIND versions in that list, which are known (?) to prime correctly
+ We need a new theory
J-Root Anycast Structure

+ Each site globally visible behind AS 26415
+ Other roots have different policies on anycast instances
+ Local topology
  + Multiple boxes answering behind load balancers
  + Monitoring boxes sit in front of the load balancers
Analysis of Anycast Instances

+ Look at Geo-mapping – good eye candy
+ What types of systems are hitting these boxes
+ What systems are asking for invalid TLD
+ Interesting Behavior
Geo Mapping

+ Geo-mapped the sources and see if correlated to “physical site” location
+ Colors depict # packets generated over time
  + Colors change over standard deviation with mean between red and green
  + White (highest)
  + Yellow
  + Orange
  + Red
  + Green
  + Blue
  + Purple
  + Black (lowest)
Geo Mapping (C/Dulles, VA)
Geo Mapping (E/Los Angeles, CA)
Geo Mapping (G/Mountain View CA)
Geo Mapping (H/Amsterdam, NL)
Geo Mapping (K/London, UK)
Geo Mapping (L/Atlanta, GA)
Geo Mapping (M/Singapore)
Graphs look nice but what does it mean?

- Used to be routing Location != Topology
- As Internet grows, location is becoming more aligned with topology
Collected TTLs on IP packets

+ Gives a “rough” correlation on OS that sent the packet
+ < 30 AIX
+ < 64 Linux/BSD
+ < 128 Windows
+ < 255 Solaris/Cisco/HP
OS mapping

Queries by OS Group

- Linux / xBSD: 40%
- Windows: 32%
- Solaris / Cisco / HP: 27%
- AIX: 1%
OS Mapping to RCODE 3 responses

Invalid Queries by OS Group

- Linux / xBSD: 48%
- Solaris / Cisco / HP: 37%
- Windows: 14%
- AIX: 1%
Interesting Behaviors

+ Looked at sites that were seen in two or more anycast sites
+ 3.69% of all traffic over three days was seen at two or more sites
+ More than expected
+ Looked at a couple of examples…
Traffic from one IP seen at multiple sites

“Normal Jitter”

“Abnormal Jitter”
Take home

+ Expected to see a saw tooth distribution – instead have a noisy distribution in many cases
+ Does not affect UDP
+ DO NOT RUN Anycast with Stateful Transport
  + Will “No Export” mitigate this behavior?
Conclusions

+ Just In Time Presentation
  + Very little work done with others
  + Need to work with other roots and core routing people
+ Retired J Root
  + Reason for continued steady stream of traffic is unknown
+ Anycast
  + Roots have multiple ways of doing anycasting
  + Questions that come to mind
    + Is one way better than others?
    + Is the diversity worth having some “suboptimal” configurations
    + Influence on IPv6 and DNSSEC that may escalate interactions into stateful transport