“Day in the Life 2007”
Data Analysis

Sebastian Castro
secastro@caida.org
secastro@nic.cl

CAIDA
NIC Chile

DNS-OARC – November, 2007
DITL 2007

• This report is a continuation of Duane Wessels report on last OARC meeting

• Due to problems on the full DITL 2007 set (~48 hours), we selected the best coverage 24-hour set to work with.
  – January 9th 2007, 12:00:00 to January 10th 2007, 11:59:59

• All further analysis were done using that subset.
Analysis Software

- **C++ code**
  - Read pcap files, counts and analyze
  - Output SQL and plain text files
  - Range of analysis selected on compilation time
    - Client and query rate, AS/prefix coverage
    - Distribution of queries by query type
    - Node/cloud switching per client
    - Source port analysis
    - EDNS support and EDNS buffer size
    - Invalid queries
    - Others: RD queries, RFC1918/Bogon sources
  - Speed depends on the number of analysis selected

- **Data preprocessing**: Perl and shell script
- **Data plotting** using *ploticus*.
- **Unexpected feature**: Machine crasher
  - Lesson: Don’t let a perl geek work on C++ code 😊
## Overview

<table>
<thead>
<tr>
<th>Root</th>
<th>Node</th>
<th>Instances</th>
<th>Avg query rate per instance</th>
<th>Avg query rate all instances</th>
<th>Average client rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Global</td>
<td>4</td>
<td>1723.7 – 3804.3</td>
<td>2584.2</td>
<td>596.2 – 1178.5</td>
</tr>
<tr>
<td>F</td>
<td>Global</td>
<td>2</td>
<td>2012.7 – 2563.5</td>
<td>2288.1</td>
<td>589.2 – 1085.1</td>
</tr>
<tr>
<td>F</td>
<td>Local</td>
<td>34</td>
<td>3.0 – 1241.1</td>
<td>259.2</td>
<td>1.9 – 344.3</td>
</tr>
<tr>
<td>K</td>
<td>Global</td>
<td>5</td>
<td>403.8 – 4864.5</td>
<td>1853.0</td>
<td>134.1 – 1422.2</td>
</tr>
<tr>
<td>K</td>
<td>Local</td>
<td>9</td>
<td>3.3 – 259.1</td>
<td>66.9</td>
<td>2.3 – 37.1</td>
</tr>
<tr>
<td>M</td>
<td>Global</td>
<td>6</td>
<td>66.8 – 5836.8</td>
<td>1898.1</td>
<td>27.1 – 1930.0</td>
</tr>
</tbody>
</table>

![Graph showing query rate distribution](image-url)
Overview

AS Coverage

% of total AS

C global
F global
F local
K global
K local
M global

Aggregated AS - Min coverage per instance - Max coverage per instance
## General Stats

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of queries</td>
<td>4.92 * 10^9</td>
<td>3.84 * 10^9</td>
<td>4.1 * 10^6</td>
</tr>
<tr>
<td>RD traffic (% of queries)</td>
<td>3.61</td>
<td>17.04</td>
<td>11.59</td>
</tr>
<tr>
<td>TCP (%)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bytes</td>
<td>1.58</td>
<td>1.3</td>
<td>0.17</td>
</tr>
<tr>
<td>Packets</td>
<td>2.67</td>
<td>3.2</td>
<td>0.22</td>
</tr>
<tr>
<td>Queries</td>
<td>0.0184</td>
<td>0.0064</td>
<td>0.0118</td>
</tr>
<tr>
<td>Queries from RFC1918 space</td>
<td>2.15</td>
<td>4.26</td>
<td>0.3</td>
</tr>
</tbody>
</table>
Client Geography
Client Geography

- Local nodes show at least a 91% of clients from the same continent.
  - Exceptions are f-lga (65% from North America, 30% from Europe) and f-lax1 (82.5% from Asia, 14.1% from North America).

- Global nodes
  - F-sfo2 and F-pao1 reduced their Asian clients compared to 2006
    - Perhaps the presence of the local node in Beijing?
    - For Asian clients, F-sfo2 changed for 17% in 2006 to 8% in 2007. In terms of countries, 31.7% from Japan and 19.7 from Russia to 0.79% and 49.32%.
    - In F-pao1, Asia clients varied from 12.8% to 11%. For China clients, from 36% in 2006 to 2.1% in 2007.
Client Geography

• K-root
  – K-miami and K-tokyo present good correlation with their location.
    • K-miami, 78.4 from North America, 20% from South America.
    • K-tokyo, 88.4 from Asia, 6% from North America.
  – K-london and K-amsterdam have more diverse origins
  – K-delhi has 1/3 of the clients coming from North America.

• M-root
  – All instances receive some amount of traffic from Asia
Query Load

- From a range of 2.54 million clients
  - 438K (17%) sending only one query
    - 61.6% A-query
    - 10% PTR-query
    - 7.1% SOA-query
    - 6% NS-query
    - 4% MX-query
  - 10 sending more than ten million queries.
    - 7 unknown
    - 1 Microsoft Windows NT4
    - 1 Microsoft Windows 2003
    - 1 BIND8
Query Load

IV 13 Distribution of users binned by query rate intervals for F-root.

IV 11 Distribution of users binned by query rate intervals for K-root.
Query Load

• The clients with a query rate less than 1/100 q/s represent 96% of the total client population
  – But only 6% of the load
• For C, F and M, the interval of ‘1-10 q/s’ represents 29%, 39% and 30%.
• For K root, the interval of ’10-100 q/s’ represents 38.7% of the queries
Query Load

- The same categories per query rate
- Each column show the fraction of queries per type
- The two rightmost columns (higher query rates) present different behavior
  - M-root
    - 25% A queries
    - 50% PTR queries
    - 13% MX queries
  - K-root
    - 55% A queries
    - 35% SOA queries
    - 10% PTR queries
Query Load

- C-root and F-root similar
  - 90% A queries
  - 5% PTR queries
Client affinity

- 39% queried one cloud
- 28.3% queried all four
- Instance switch
  - C-root: 0.9%
  - F-root: 0.7%
  - K-root: 1.2%
  - M-root: 1.9%
Invalid queries

• Methodology
  – Updating the results from a paper of 2003.
  – Nine categories of invalid traffic
  – Evaluation one by one
  – For the last three, the analysis was per source address
    • Requires filter/split traffic per source
    • Using a sample (7.5% clients for each cloud)
      – Currently 213142 unique clients
      – The goal is reach 10% of clients per cloud
Invalid queries

- Unused query class: Any class not in IN, CHAOS, HESIOD, NONE or ANY
- A-for-A: A-type query for a name is already a IPv4 Address
  - <IN, A, 192.16.3.0>
- Invalid TLD: a query for a name with an invalid TLD
- Non-printable characters: a query for a name with characters not in [A-Z0-9\-] list
- Queries with ‘_’: Special category for the invalid but widely used character.
- RFC 1918 PTR: a PTR query for an IPv4 address in the private space
- Identical queries: a query with the same class, type, name and id (during the 24 hours period)
- Repeated queries: a query with the same class, type and name
- Referral-not-cached: a query seen with a referral previously given.
  - If a client sent <IN, A, www.example.net> and later <IN, NS, ripe.net> the second query counts as “referral-not-cached” because a referral to “net” nameservers was answered.
  - A tolerance parameter of 2 seconds was included on this analysis
  - Root servers are authoritative for .arpa, .in-addr.arpa and root-servers.net zones, were included as special cases.
Invalid queries
Invalid queries

Traffic validity on K-root
## Invalid queries

<table>
<thead>
<tr>
<th>Category</th>
<th>C-root</th>
<th>F-root</th>
<th>K-root</th>
<th>M-root</th>
<th>Total Sample</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Class</td>
<td>0.09</td>
<td>0.01</td>
<td>0.02</td>
<td>0.05</td>
<td>0.03</td>
<td>0.08</td>
</tr>
<tr>
<td>A-for-A</td>
<td>4.65</td>
<td>11.57</td>
<td>2.18</td>
<td>8.74</td>
<td>6.64</td>
<td>7.02</td>
</tr>
<tr>
<td>Invalid TLD</td>
<td>19.15</td>
<td>46.79</td>
<td>10.01</td>
<td>20.96</td>
<td>24.72</td>
<td>24.73</td>
</tr>
<tr>
<td>Non-printable Character</td>
<td>0.05</td>
<td>0.03</td>
<td>0.13</td>
<td>0.10</td>
<td>0.08</td>
<td>0.53</td>
</tr>
<tr>
<td>Queries with ‘_’</td>
<td>0.13</td>
<td>0.07</td>
<td>0.15</td>
<td>0.13</td>
<td>0.12</td>
<td>0.23</td>
</tr>
<tr>
<td>RFC-1918 PTR</td>
<td>0.84</td>
<td>0.28</td>
<td>0.22</td>
<td>0.74</td>
<td>0.44</td>
<td>0.67</td>
</tr>
<tr>
<td>Identical Queries</td>
<td>15.41</td>
<td>3.73</td>
<td>4.78</td>
<td>12.51</td>
<td>7.71</td>
<td>N/A</td>
</tr>
<tr>
<td>Repeated Queries</td>
<td>37.99</td>
<td>20.11</td>
<td>50.20</td>
<td>32.61</td>
<td>35.73</td>
<td>N/A</td>
</tr>
<tr>
<td>Referral not Cached</td>
<td>18.69</td>
<td>15.25</td>
<td>30.55</td>
<td>21.22</td>
<td>22.07</td>
<td>N/A</td>
</tr>
<tr>
<td>Legitimate Queries</td>
<td>3.01</td>
<td>2.17</td>
<td>1.76</td>
<td>2.95</td>
<td>2.46</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Invalid queries

- Common invalid TLD’s

<table>
<thead>
<tr>
<th>TLD</th>
<th>Percentage of queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>20.29</td>
</tr>
<tr>
<td>localhost</td>
<td>8.92</td>
</tr>
<tr>
<td>domain</td>
<td>3.15</td>
</tr>
<tr>
<td>invalid</td>
<td>2.43</td>
</tr>
<tr>
<td>lan</td>
<td>2.06</td>
</tr>
<tr>
<td>belkin</td>
<td>1.76</td>
</tr>
<tr>
<td>home</td>
<td>1.30</td>
</tr>
<tr>
<td>localdomain</td>
<td>1.29</td>
</tr>
<tr>
<td>wpad</td>
<td>0.74</td>
</tr>
<tr>
<td>txt</td>
<td>0.74</td>
</tr>
</tbody>
</table>
Invalid queries

• Refinements
  – We explored how many repeated queries could be originated by BIND9 ‘glue record refresh’.
  – We found at most 1% of the total queries from sample could be associated to that process
  – Still adjusting analysis to find common TTL parameters (and differentiate from dual stack clients sending A/AAAA queries for the same name).
Invalid queries

- Comparing with data from ORSN (Open Root Server Network)
Source port

Distribution of source port numbers

Port Number (log scale)

Number of Clients using this Port

Source port numbers:
- 49152
- 512-599
Source port

• The idea was suggested on last OARC meeting
• Presents the distribution of client by the source ports on queries received on root servers
• Use of port 0, 53, 512, 1024, 32768.
• 49152 = (32768 + 65536) / 2 (?!)
• Use of “privileged port range”
  – BSD kernel has settings to use ports starting at 600
• What about trying doing some O.S. fingerprinting using IP parameters and port range?
EDNS

• For every query with a pseudo-RR OPT in Additional section, calculated EDNS version and EDNS buffer size.
• Found some clients sending more than one buffer size (not included on the graphs)
• The EDNS version graphs are not new
  – Already supported by DSC
• The buffer size is a little more interesting.
  – Shows, for example, queries with buffer of 512 bytes (but not present on per client graph)
  – Explained by Mark Andrews: BIND9 falling back to 512 bytes.
EDNS
EDNS
Conclusions

• Reduced number of node switching compared with 2006
  – Previously seen on J-root analysis
• Still low TCP traffic
• After 4 years, the root still sees the same amount of trash
  – Should be reasonable/effective to take measures about this, from education to punishment?