Continuous Data-driven Analysis of Root Stability (CDAR)

Preliminary Results

Giovane C. M. Moura
SIDN Labs
giovane.moura@sidn.nl

IEPG - IETF 95
Buenos Aires, Argentina
April 3rd, 2016
Together with NLNet Labs and TNO, we’ve won a RFP from ICANN

CDAR project: http://cdar.nl

RQ: What’s the impact of the new gTLD program on the Root DNS stability?

Approach

- Data-driven, using wide variety of DNS data

Interaction with the broader tech community

- ICANN and advisory committees, RSOs, DNS-OARC, IEPG/IETF
DNS Root and name resolution

Figure: Resolving a Name
DNS Root and name resolution

**Figure**: Resolving a Name
DNS Root and name resolution

Figure: Resolving a Name
DNS Root and name resolution

Figure: Resolving a Name
DNS Root and name resolution

Figure: Resolving a Name
DNS Root and name resolution

(1) example.nl
(2) .nl ?
(3) .nl is ...
(4) example.nl ?
(5) example.nl is ..
(6) example.nl is

Figure: Resolving a Name
The Root DNS System

- Lists records for TLDs
- Extremely redundant to improve performance and availability:
  - 13 letters (A through M)
  - Each letter hosts several to more than 100 servers (Anycast)
  - Distributed all over the world
  - Has been up and running for many years
- Survived some major DDoS attacks
- Letters are ran by different organizations worldwide
- It’s dynamic: more servers, lines added frequently
How many TLDs are out there?

Figure: Timeseries of TLDs in the Root Servers

Is it too many? .com has 126+ million domains
What’s the root traffic like (DITL = 1 day/year)

**Figure:** DITL data → new gTLD traffic is still too small
Correlation between TLDs size and number of root queries

<table>
<thead>
<tr>
<th>TLD</th>
<th>Queries</th>
<th>Zone Size</th>
<th>Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>779.171.677</td>
<td>120.585.440</td>
<td>6.46</td>
</tr>
<tr>
<td>.org</td>
<td>91.095.714</td>
<td>10.569.583</td>
<td>8.62</td>
</tr>
<tr>
<td>.cn</td>
<td>51.949.760</td>
<td>11.678.026</td>
<td>4.45</td>
</tr>
<tr>
<td>.br</td>
<td>15.696.021</td>
<td>3.568.492</td>
<td>4.40</td>
</tr>
<tr>
<td>.club</td>
<td>651.082</td>
<td>202.519</td>
<td>3.21</td>
</tr>
<tr>
<td>.xyz</td>
<td>420.885</td>
<td>842.340</td>
<td>0.50</td>
</tr>
</tbody>
</table>

Table: DITL 2015 Data for K-root - Valid Queries only

- Ratio rarely exceeds 10 for DITL 13, 14, 15, and recent H-root
- new gTLDs ratios are lower
- Limitation datasets: 1 day only per year
  - hard to generalize
So far:

- DITL data set is great; but it is a snapshot
  - Hard to generalize conclusions
  - Have to combine with other analysis
- Is there any other longitudinal dataset out there?
  - YES! RIPE Atlas monitors every single root server letter :)
  - Every 4 min (except A)
  - They’ve been doing this for YEARS now
  - Limitation: influenced by other network errors
  - Pro: a good approximation of a resolver
Active Measurements with RIPE Atlas

- We can measure RTT, errors, on various levels:
  - letter ($\alpha = A-M$)
  - site ($s_n = \text{city}$)
  - instance/server ($i_n = \text{actual machine}$)
Measurement plan with RIPE Atlas

1. Choose 30 dates in which new gTLDs were included in the root zone in the last years

2. For each day $d$, gets -2 and +2 days of data from RIPE Atlas, for each letter

3. Analyze RTT, responses per root server letter, site, and server

We have some preliminary results
16 New TLDs: changes overall performance?
10 New TLDs: changes overall performance?
New gTLDs: changes overall performance?

- We are still working on the RIPE data
- Statistical tests to determine if there’s variation
- So far, it seems to not impact that much
  - Root DNS is very robust
  - It’s designed to “take the punch”
  - It would be weird to see major problems
- Other events can happen: DDoS Nov 30th/Dec 1st
  - See Matt Weinberg/Duane Wessels (A/J Root) DNS OARC Presentation
Summary

- Study aims at determining impact of new gTLD on Root DNS stability/security
- Various datasets; each one with its own limitation
- So far, new gTLD seem to have no significant impact the Root DNS system
- Next: continue our analysis to draw final conclusions
  - More metrics, more data, more analysis
Questions?

**CDAR Project Team**

- Bart Gijsen (TNO)
- Benno Overeinder (NLnet Labs)
- Cristian Hesselman (SIDN)
- Daniël Worm (TNO)
- Giovane C. M. Moura (SIDN)
- Jaap Akkerhuis (NLnet Labs)

Giovane C. M. Moura - giovane.moura@sidn.nl
CDAR website: http://www.cdar.nl