Exploring Anycast-Based Public DNS Resolvers

Julien Gamba†, Álvaro Feal† and Narseo Vallina-Rodríguez†
†IMDEA Networks Institute, ‡Universidad Carlos III de Madrid, †ICSI

Motivation

- Anycast-based DNS resolvers are widely used by millions of users at a global scale [1, 2]
- Users tend to switch to third party DNS resolvers when their local/ISP provided resolver is under performing or censoring domains, and tend not to switch back [3]
- Firefox may make Cloudflare its default DNS resolver soon [4]
- Have not been widely studied yet

We want to study the characteristics of anycast-enabled public DNS resolvers:
- Their infrastructure
- Their performance and reachability

Resolvers studied

<table>
<thead>
<tr>
<th>Country</th>
<th>Best lookup time (ms)</th>
<th>Mean lookup time (ms)</th>
<th>Best country (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NL</td>
<td>31ms (Google)</td>
<td>51ms (Level3)</td>
<td>GB - 41ms (12ms)</td>
</tr>
<tr>
<td>USA</td>
<td>51ms (Verisign)</td>
<td>177ms (OpenNIC)</td>
<td>MA - 29ms (8ms)</td>
</tr>
<tr>
<td>Russia</td>
<td>67ms (Google)</td>
<td>170ms (OpenDNS)</td>
<td>RU - 16ms (5ms)</td>
</tr>
<tr>
<td>Greece</td>
<td>86ms (OpenNIC)</td>
<td>240ms (Cloudflare)</td>
<td>DE - 21ms (4ms)</td>
</tr>
<tr>
<td>Nigeria</td>
<td>125ms (DynDNS)</td>
<td>187ms (OpenDNS)</td>
<td>LA - 51ms (6ms)</td>
</tr>
<tr>
<td>Australia</td>
<td>235ms (Cloudflare)</td>
<td>87ms (OpenDNS)</td>
<td>BE - 17ms (3ms)</td>
</tr>
<tr>
<td>Chile</td>
<td>233ms (DynDNS)</td>
<td>249ms (OpenDNS)</td>
<td>CL - 51ms (6ms)</td>
</tr>
<tr>
<td>China</td>
<td>252ms (Verisign)</td>
<td>185ms (Level3)</td>
<td>CH - 11ms (3ms)</td>
</tr>
</tbody>
</table>

Performance

- Good performances in Europe: 50% of requests take ≤100ms
- Performances are degraded in other regions: e.g. in South Asia 50% of the requests take more 300ms
- Significant differences in median lookup time per resolver

Response times in Europe, South Asia and Africa per resolver when having to get DNS information from Europe:

Europe (999 probes)

South Asia (190 probes)

Africa (206 probes)

Discovering anycast resolvers infrastructure

Discovery method:
- Set up an authoritative name server under our control
- Instruct RIPE Atlas probes [5] (=10K vantage points) to resolve an nonexistent, unique and random subdomain

The resolvers will be forced to query us, therefore revealing their actual IP.

We use RIPE IP Map [6] to geolocate these IP addresses using active measurements.
Results may be biased by the probes locations: there are more probes in Europe and North America than in other regions.

Conclusion and future work

- Great geographical discrepancies for all resolvers: North-South divide is very present
- Lookup time very dependent on user geographical location with e.g. performance three times worse in South Asia as compared with Europe
- Performances are especially degraded when having to get DNS information afar from user’s location

We plan to extend or work to answer the following questions:

**Resolvers performance:**
- Conduct new experiments with authoritative nameservers in different locations values to measure the effect of the resolvers caching policies
- Conduct new experiments with websites with different TTL values to measure the effect of the resolvers caching policies
- Study development challenges and barriers

**Inference of the resolvers pools:**
- Can we know if a resolver virtualizes its infrastructure?
- If so, can we infer the size of resolver pools?

**Privacy and security guarantees:** some resolvers claim to offer more security and privacy to attract customers
- What privacy enhancing techniques are deployed by each resolvers?
- Do they manipulate some responses, or block some websites? If so, are these behaviors global or country specific? Are the resolvers influenced by censorship?

References