Exploring Anycast-Based Public DNS Resolvers

Julien Gamba*†, Álvaro Feal*† and Narseo Vallina-Rodriguez*‡

*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:

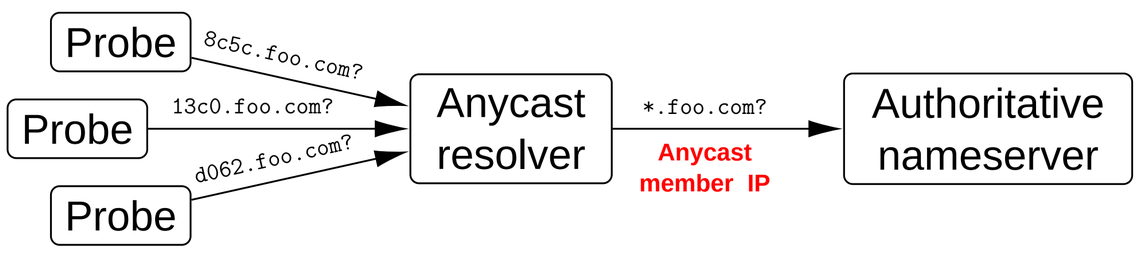
- Their infrastructure
- Their performance and reachability

Resolvers studied

Discovering anycast resolvers infrastructure

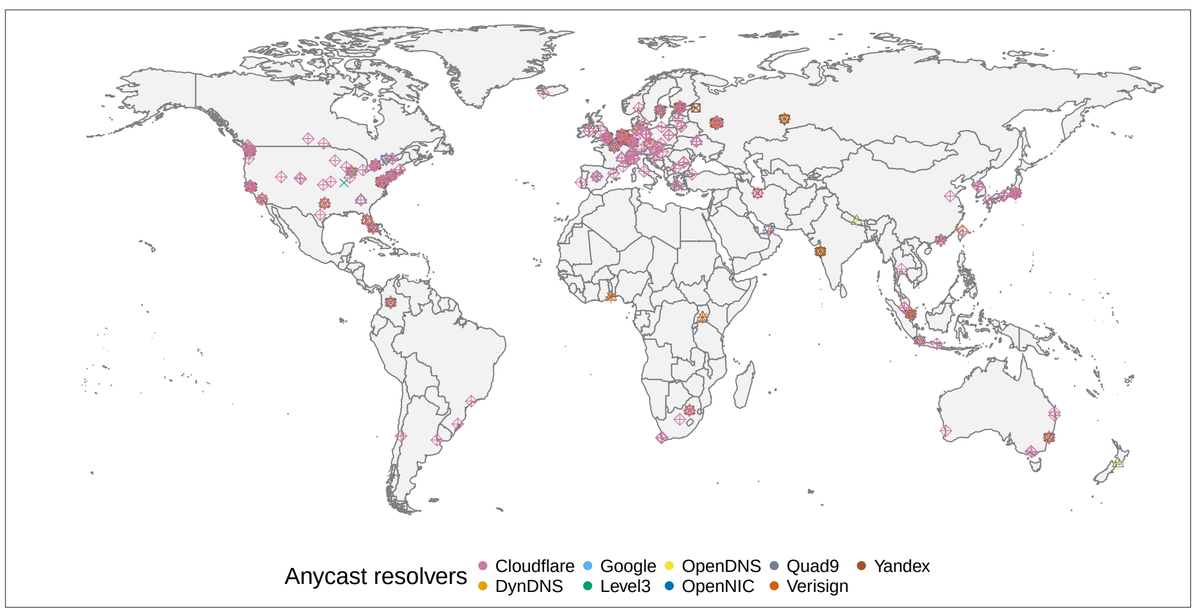
Discovery method:

- 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.

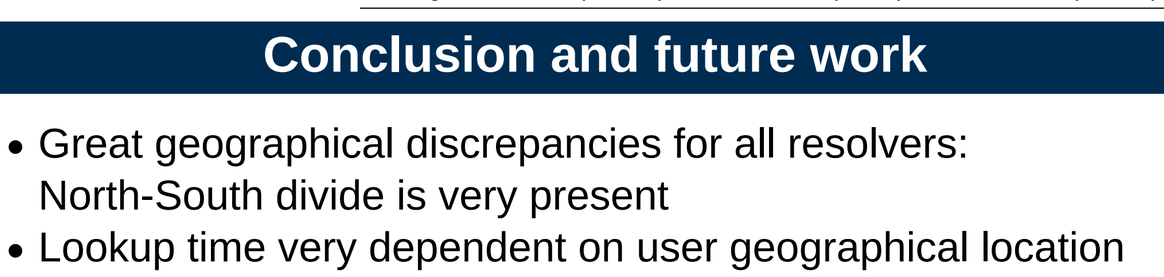


Resolvers all share similar infrastructure patterns:

- Points of presence (PoP) overwhelmingly located in western Europe and North America
- High concentration in some locations (*e.g.* all nine resolvers are present in Amsterdam, London and New York), possibly due to IXP presence
- Very few PoPs in South America (2.23%) and Africa (2.57%)

Performance

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



- Good performances in Europe: 50% of requests take $\leq$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

Country	Best lookup time median (stdev)
NL	38ms (Google)
USA	51ms (Verisign)
Russia	67ms (Google)
Greece	86ms (OpenNIC)
Nigeria	125ms (DynDNS)
Australia	235ms (Cloudflare)
Chile	239ms (DynDNS)
China	252ms (Verisign)

Resolver	Mean lookup time median (stdev)	Best country median (stdev)	Worst country median (stdev)
Google	157ms (171ms)	GB - 41ms (11ms)	BI - 718ms (695ms)
Quad9	179ms (523ms)	GB - 42ms (56ms)	MW - 3245ms (1607ms)
Cloudflare	240ms (205ms)	ES - 21ms (41ms)	GU - 675ms (55ms)
DynDNS	187ms (289ms)	NL - 51ms (6ms)	ET - 1072ms (1113ms)
Yandex	221ms (120ms)	FI - 71ms (7ms)	CD - 536ms (438ms)
OpenDNS	249ms (334ms)	FR - 83ms (29ms)	OM - 1612ms (370ms)
OpenNIC	205ms (557ms)	BE - 65ms (662ms)	CH - 2760ms (1936ms)
Level3	185ms (303ms)	GB - 43ms (23ms)	PE - 1395ms (126ms)
Verisign	203ms (160ms)	GB - 51ms (47ms)	CD - 787ms (880ms)

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

[1] Google, "Google Public DNS and Location-Sensitive DNS Responses," https://webmasters.googleblog.com/2014/12/google-public-dns-and-location.html, 2014, accessed: 2018-06-08.

[2] OpenDNS, "Cisco Umbrella Global Network," https://umbrella.cisco.com/products/our-cloud, 2018, accessed: 2018-06-08.

[3] W. B. de Vries, R. van Rijswijk-Deij, P.-T. de Boer, and A. Pras, "Passive observations of a large dns service: 2.5 years in the life of google," *Proc. TMA conference*, 2018.

[4] Patrick McManus, "Firefox nightly secure dns experimental results," blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results/, 2018, accessed: 2018-10-25.

[5] RIPE NCC, "RIPE Atlas," https://atlas.ripe.net, 2010, accessed: 2018-10-25.

[6] ——, "RIPE IPmap," https://openipmap.ripe.net, 2018, accessed: 2018-10-25.