An Anycast Federation for DNS Resolvers

Leandro M. Bertholdo*, Ralph Holtz*, Roland van Rijswijk-Deij*, Lisandro Granville†‡, Cristian Hesselman*§
*University of Twente †UFRGS ‡RNP §SIDN Labs

Abstract: The DNS resolution was planned to be a simple and fully distributed infrastructure. However, the current complexity of operating DNS, allied with the diversity of attacks involving DNS, demands expertise and a workforce often unavailable in small ISPs, and universities. For them, DNS operation is not a priority and is often perceived as a burden, thus being either outsourced or poorly operated. This leads us to the current scenario, where the adoption of DNS public resolvers has been increasing [1], and ISPs' misconfigurations are a major cause for old problems as open resolvers [2].

While the community still diverges on whether centralization of public resolvers is a problem [3] [4], initiatives such as CIRA Canadian Shield and DNS4EU build regional-level infrastructures for DNS resolution to face concerns about dependency, diversity, and centralization. On the other hand, public resolvers have contributed to accelerating the adoption of new DNS security standards, helping to make the Internet safer [5]. The influence of governments in DNS operations raises many concerns for ISPs and users, such as censorship, surveillance, and regulations in the sector.

The contribution of this abstract is to discuss the risks of DNS resolution and identify opportunities and challenges in adopting a federation of anycast. We discuss how a federation between access networks and DNS providers can help improve DNS resolution, increase the adoption of standards, and lower barriers for new players. While many legal, political, and sustainability challenges remain to be solved to make this technical solution viable, the success of federated authentication between Universities is a reality [6] [7].

We enumerate the following risks in DNS resolution: **(R1)** Lack of diversity, fear of dependency, and centralization; **(R2)** Cyber attacks involving DNS continue to rise; **(R3)** DNS is an operational burden; **(R4)** Lack of middle ground between ISPs and public resolvers - ISPs can not comply with court orders demanding to block domains when using public DNS;

We identify opportunities where a federation can take advantage of **(O1)** Keep DNS resolvers close to the user - public resolvers state to answer DNS queries up to 50ms for 95% of users [8], but ISPs target 5ms; **(O2)** Increase adoption of best practices and DNS improvements - several DNS attacks have already been addressed by best practices and novelties, but ISPs are reactive in DNS issues; **(O3)** Replicate multistakeholder infrastructure from root-server for resolvers.

For small access networks, public resolver is a positive development. The challenge lies in finding ways to spread other public resolver initiatives, which may not have the same level of infrastructure or financial backing, to distribute anycast copies of their servers globally and properly manage [9] [10]. For example, in regions such as Middle Africa, where the Google public resolver accounts for 40% of all DNS queries [11], this is particularity relevant.

The base of an anycast federation is a hosting-per-service-barter. The purpose is to bring trust and organization between small networks and specialized providers aiming for high-quality services close to end users. An anycast federation has two key partners: One provides the infrastructure (ISPs), and another provides an application that needs to run close to the end user (a public DNS resolver). A broker provides an agreement between both. After, an anycast instance from the resolver is automatically deployed in a federated host in the ISP datacenter (Figure 1). The federation's role is to accredit parts, facilitate contractual terms and deliver the service.

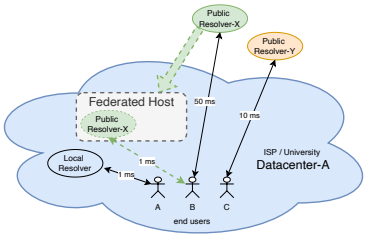

Fig. 1: Multiples resolver inside ISP through a federated host, improving response time by reducing the distance to end-users.

The main challenges we identify in running an anycast federation are: **(C1)** How to facilitate the entry of new players for DNS resolvers; **(C1)** How to make attractive for hosting institutions; **(C3)** How to make attractive for service providers; **(C4)** Federation sustainability and governance.

A federation is only as strong as its ability to attract and retain members. Small ISPs want to diminish DNS operational costs (R3) but do not want a unique provider (R1). They want to adopt novelties in DNS, but it is not a priority (R3, O2). Some ISPs report high RTT using public resolvers (O1). Enterprises look for features such as malware blocking (O6). None are interested in learning DNS crypto details (R2). ISP needs control of DNS filtering to comply with court orders (R4). ISP, Universities, and enterprises want DNS logs for thread intelligence and users troubleshooting (R4). Universities are prone to provide VMs and transit if their DNS operations improve (R3, O3). ISPs can provide transit for DNS providers under certain conditions (O3). DNS resolvers must build one or more customized versions of their software to run in a federated environment (R1). DNS resolvers like the idea of providing their service closer to users and growing their networks, especially in better conditions than lead resolvers (O1). NRENs have independent initiatives; they agree to share the software and operation since they have access to service metrics and can comply with local laws regarding privacy (R1-3, O1-3). The use of a federated model can diminish universities operational costs (R3), provide a better service closer to end users (R1), and with some extra incentive to build a global public resolvers for NRENs (O3). We are discussing this model with ISP, NRENs, and DNS public resolvers.

REFERENCES

[1] A. Durand, "DNS Resolvers Used in the EU," https://www.icann.org/en/system/files/files/octo-032-01mar22-en.pdf, 03 2022.

[2] R. Yazdani, R. v. Rijswijk-Deij, M. Jonker, and A. Sperotto, "A matter of degree: characterizing the amplification power of open DNS resolvers," in *International Conference on Passive and Active Network Measurement*. Springer, 2022, pp. 293–318.

[3] R. Radu and M. Hausding, "Consolidation in the DNS resolver market – how much, how fast, how dangerous?" *Journal of Cyber Policy*, vol. 5, no. 1, pp. 46–64, 2020.

[4] G. Huston, "DNS resolver centrality," https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/, 11 2022.

[5] ENISA - European Union Agency for Cybersecurity, "Security and privacy for public DNS resolvers," https://www.enisa.europa.eu/publications/security-and-privacy-for-public-dns-resolvers/, 02 2022, (Accessed on 01/18/2023).

[6] M. Oostdijk, B. Hulsebosch, M. Wegdam, R. van Rijswijk-Deij, J. van Dijk, P. van de Meulen, and E. van der Harst, "Step-up authentication-as-a-service," 2012.

[7] D. Pöhn, S. Metzger, and W. Hommel, "Géant-trustbroker: Dynamic, scalable management of saml-based inter-federation authentication and authorization infrastructures," in *IFIP International Information Security Conference*. Springer, 2014, pp. 307–320.

[8] Cloudflare, "Cloudflare global network data center locations cloudflare," https://www.cloudflare.com/network/, 05 2022, (Accessed On 31/12/2022 18:30).

[9] L. M. Bertholdo, J. M. Ceron, L. Z. Granville, G. C. Moura, C. Hesselman, and R. Van Rijswijk-Deij, "BGP anycast tuner: Intuitive route management for anycast services," in *16th International Conference on Network and Service Management, CNSM 2020, 2nd International Workshop on Analytics for Service and Application Management, AnServApp 2020 and 1st International Workshop on the Future Evolution of Internet Protocols, IPFutu*, 2020.

[10] A. Rizvi, L. Bertholdo, J. Ceron, and J. Heidemann, "Anycast agility: Network playbooks to fight ddos," in *Proceedings of the 31st USENIX Security Symposium, page to appear. USENIX*, 2022.

[11] APNIC, "Dns recursive resolver use metrics," 03 2020, (Accessed On 8/2/2023 21:33). [Online]. Available: https://stats.labs.apnic.net/rvrs