Optimizing Authoritative Servers Deployment on TLDs (abstract)

Ricardo de O. Schmidt[1]   Giovane C. M. Moura[2]   John Heidemann[3]
Moritz Müller[2]   Marco Davids[2]   Cristian Hesselman[2]

1: University of Twente   2: SIDN Labs   3: USC/Information Sciences Institute

If you were to setup *a new* top-level domain (TLD), *how many* authoritative servers would you deploy? Figure 1 shows that most TLDs ($\sim$ 50%) nowdays use 4 servers. *Where* would you deploy them (geographically)? And would you use anycast services (local on CDNs/ISPs, global elsewhere), unicast services or a combination of both? For existing TLDs, how can you *optimize* your authoritative servers setup to optimize round-trip time (RTT) to your clients, as well as better resilience against DDoS attacks [1]?

These are questions that TLD operators continuously face. Consider the example of the `.nl` TLD (the Netherlands), which has 8 authoritative servers. Figure 2 shows how they are deployed (3 employ IP anycast). A resolver, on the user's behalf, would resolve `example.nl` by contacting any of these eight servers, and the choice is based on the resolvers' implementation [4].

Due to IP anycast – which allows for an authoritative server to share the same IP address across multiple machines distributed around the globe –, not all authoritative servers have the same number of physical machines. Figure 3 shows the authoritative servers for `.nl`, in which the area of each authoritative server is proportional to their number of sites/locations. `netnod` auth. server is by far the largest.

As a result of these differences, one could expect that the `.nl` `netnod` auth. server would *receive more traffic than the others*. That is not the case. Figure 4 shows traffic to the auth servers (area proportional to the total number of incoming queries in June, 2016). First, `ns5` in fact handles more traffic than `netnod`. One of the reasons is that `ns5` is an *local anycast* server deployed in most of Dutch ISPs, which are responsible for a large portion of the total ammount of traffic [3]. Another interesting and not yet clear observation is that while `ns1`-`ns4` are all deployed in the Netherlands as unicast sites, `ns1` still gets 50% less traffic than the others.

What we can derive from these two observations is that the distribution of queries sources must be also taken into account when designing the deployment of a TLD. These two examples cry out for a systematic study that aims at optimizing TLD authoritative servers deployments, for both
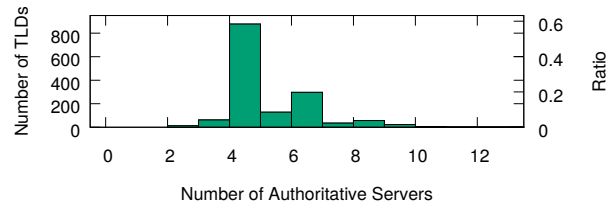

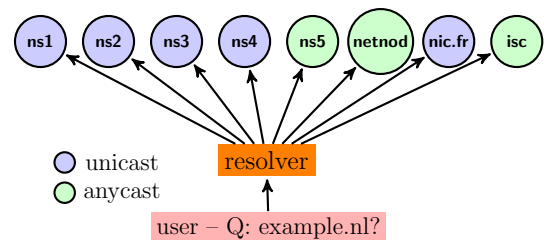**Figure 1: Number of Authoritative servers per TLD − Nov. 20th, 2016**
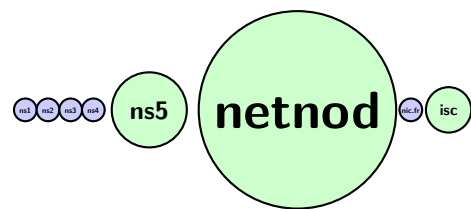

Figure 2: Resolving a Name on `.nl`

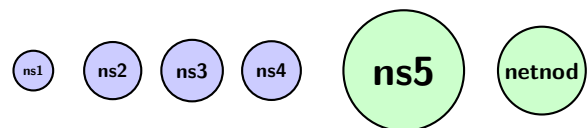**Figure 3: Authoritative Servers by Size (sites) - area proportional to number of sites**

Figure 4: Authoritative Servers by Query Volume (June 2016, missing nic.fr and isc numbers)

performance (shorter RTT) and DDoS resilience. We intend to use a similar approach presented by two of us in a previous study [2].

Acknowledgements

1. REFERENCES

[1] MOURA, G. C. M., DE O. SCHMIDT, R., HEIDEMANN, J., DE VRIES, W. B., MÜLLER, M., WEI, L., AND HESSELMAN, C. Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event. In *Proceedings of the ACM Internet Measurement Conference (IMC 2016)* (Nov. 2016).

[2] SCHMIDT, R. D. O., HEIDEMANN, J., AND KUIPERS, J. H. Anycast Latency: How Many Sites Are Enough? Tech. Rep. ISI-TR-2016-708, USC/Information Sciences Institute, May 2016.

[3] SIDN LABS. .nl stats and data: Insight into the use of .nl. http://stats.sidnlabs.nl/, 2016.

[4] YU, Y., WESSELS, D., LARSON, M., AND ZHANG, L. Authority Server Selection in DNS Caching Resolvers. *SIGCOMM Computer Communication Review 42*, 2 (Mar. 2012), pp. 80–86.