Advanced Networking

NXDomains – Project Proposal

Neta Peleg

Matan Sabag

Overview

A DNS cache is a temporary database, which contains records of recent visits to websites and other internet domains. This Cache allows to refer to previous DNS lookups, when trying to resolve a DNS query. The DNS protocol relies on the caching mechanism to reduce latency and load on servers. There are DNS caches in all along the path of a DNS query. There are caches on the stub resolvers and on the recursive resolvers.

When a resolver receives a positive response to a query, it caches it for the duration of the TTL specified by the record. For negative responses, NXDOMAIN, there is no answer to the query question. For this case, the response contains the Start of Authority (SOA) record of the zone in the authority section. Negative caching is specified in RFC 2308 as the minimum of the SOA record's TTL and the SOA minimum field

Goal

The goal of our project is to measure the numbers of resolvers that perform caching for NXDomains.

Experiment

We will use an AWS authoritative server for the domain dns_caching.com. we will set the SOA record of the domain with a NXDomain TTL. Using RIPE Atlas we will send DNS queries for non-existing domains, we expect to receive NXDomain responses. After time t< NXDomain TTL we will send another query.

In the AWS – authoritative we will record the DNS requests that are received and analyze the number of resolvers that perform NXDomain caching. Each vantage point will perform a DNS query for a unique domain so we will be able to identify which queries were cached and which weren't.

To avoid outliers of non-cached NXDomain records due to cache-eviction, resolver crashes etc. we will repeat the test from each vantage point a several times.

Another interesting aspect of NXDomain DNS caching that can be analyzed is whether DNS cache respects the TTL of the NXDomain and removes the cache record. We will obtain this by sending another DNS query from vantage point we identified that have NXDomain cachin, after the SOA TTL expires.

Open questions

These are open questions and points we need to pay attention during the research.

1) Do the RIPE Atlas Vantage points have stub resolvers, and do these resolvers cache NXDomains? If so we will need to see if we can flush the vantage point cache between requests, because we are interested in the resolver caching.
2) Figure out which vantage points have the same resolver. Analyze the data according to vantage points that have different resolvers. (As described in the article [1] the distribution of the vantage points is not uniformly across the world).

References

[1] https://www.isi.edu/~johnh/PAPERS/Moura18a.pdf

[2] https://www.lifewire.com/what-is-a-dns-cache-817514

[3] https://tools.ietf.org/html/rfc2308

[4] https://securityblog.switch.ch/2016/05/02/optimizing-negative-caching-time-in-dns/