Negative Caching of DNS Resolution Failures

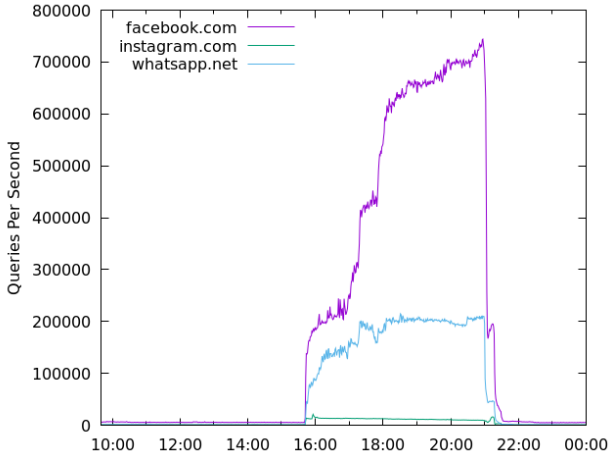
draft-ietf-dnsop-caching-resolution-failures

IETF 115 November 2022

Reminder

- Some recursive name servers are bad at caching resolution failures.
- Looking to strengthen requirements for caching resolution failures and avoid unnecessary repeated queries.
- "A DNS resolution failure occurs when none of the servers available to a resolver client provide any useful response data for a particular query name, type, and class."

Facebook outage, October 4, 2021



Rephrased Requirements

Old:

> Resolution failures MUST be cached against the specific query tuple <query name, type, class, server IP address>.

New:

> Resolvers MUST implement a cache for resolution failures. The purpose of this cache is to eliminate repeated upstream queries that cannot be resolved. When an incoming query matches a cached resolution failure, the resolver MUST NOT send any corresponding outgoing queries until after the cache entries expire.
>
> Implementation details [requirements?] for such a cache are not specified in this document. The implementation might cache different resolution failure conditions differently. For example, DNSSEC validation failures might be cached according to the queried name, class, and type, whereas unresponsive servers might be cached only according to the server's IP address.

Protecting the Self

New:

> Notwithstanding the above, resolvers SHOULD implement measures to mitigate resource exhaustion attacks on the failed resolution cache. That is, the resolver should limit the amount of memory and/or processing time devoted to this cache.

Five Second Rule

For Discussion:

Resolvers MUST cache resolution failures for at least 5 seconds. The value of 5 seconds is chosen as a reasonable amount of time that an end user could be expected to wait.

Resolvers SHOULD employ an exponential backoff algorithm to increase the amount of time for subsequent resolution failures. For example, the initial time for negatively caching a resolution failure is set to 5 seconds. The time is doubled after each retry that results in another resolution failure. Consistent with RFC2308, resolution failures MUST NOT be cached for longer than 5 minutes.

EDNS Client Subnet Interaction

For Discussion:

- Can we say that resolvers SHOULD/MUST cache resolution failures independently of EDNS client subnet?

Discussion