DNS Queries over CoAP (DoC)

draft-lenders-dns-over-coap
(https://datatracker.ietf.org/doc/draft-lenders-dns-over-coap/)

Martine S. Lenders, Christian Amsüss, Cenk Gündoğan,
Thomas C. Schmidt, Matthias Wählisch

IETF CoRE WG Interim Meeting, 2022-05-11

Outline

Introduction

Discussion

- Caching and Max-Age vs. DNS TTL
- How abstract should the draft be?
- Further discussion points

Motivation

Attack Scenario

Countermeasure: Encrypt name resolution triggered by IoT devices

Our proposal: DNS over CoAP

- **Encrypted communication** based on DTLS or OSCORE

Additional advantages:

- **Block-wise message transfer** to overcome Path MTU problem
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

Discussion: Caching and Max-Age vs. DNS TTL

Problem: CoAP Max-Age and DNS TTL may get out of sync at caching proxy

Option 1 (DoH-like, PR#17): Do it like DoH

Server:	*Client:*
Max-Age = min(TTLs)	TTL_{new} = TTL_{old} - (min(TTLs) - Max-Age)

Option 2 (EOL TTLs, PR#19): Do it like DoH but

Server:	*Client:*
Max-Age = min(TTLs)	TTL_{new} = TTL_{old} + Max-Age
TTL_{new} = TTL_{old} - min(TTLs)	

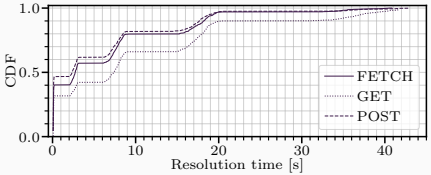
Option 3 (EOL TTLs, simplified): Do it like DoH but

Server:	*Client:*
Max-Age = min(TTLs)	TTL_{new} = Max-Age
TTL_{new} = 0	

Assumes only one RRset in response.

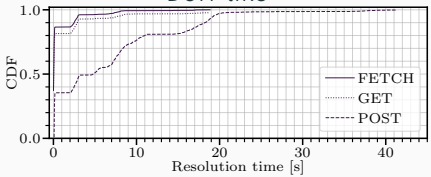
Evaluation: Caching and Max-Age vs. DNS TTL

Without caching

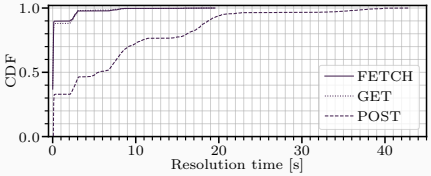


With caching

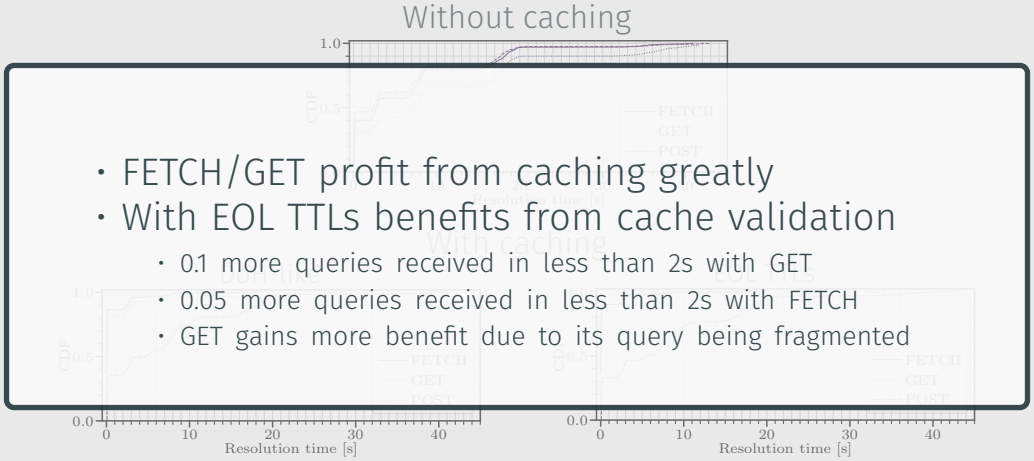
DoH-like



EOL TTLs



Evaluation: Caching and Max-Age vs. DNS TTL



- FETCH/GET profit from caching greatly
- With EOL TTLs benefits from cache validation
  - 0.1 more queries received in less than 2s with GET
  - 0.05 more queries received in less than 2s with FETCH
  - GET gains more benefit due to its query being fragmented

How abstract should the draft be? CoAP vs. REST

Issue #18 by Klaus Hartke proposes

- Specify REST API to retrieve DNS information from CoAP server instead
- Leave protocol details to implementation

Carsten Bormann on mailing list:

- Klaus was pointing out “Restatement Anti-Pattern”?

Further discussion points

(see mailing list posts from 2022-03-25)

- Do we need to consider Observe?
- CBOR-based content format