Dresden University of Technology

Martine S. Lenders (martine.lenders@tu-dresden.de)

DNS over CoAP

Encrypted DNS for the Constrained IoT

DDI User Group Meeting • Sep 24, 2026 • Remote

Outline

Motivation

CoAP Crash Course

DNS over CoAP

Further Improvements

Conclusion & Outlook

Outline

Motivation

CoAP Crash Course

DNS over CoAP

Further Improvements

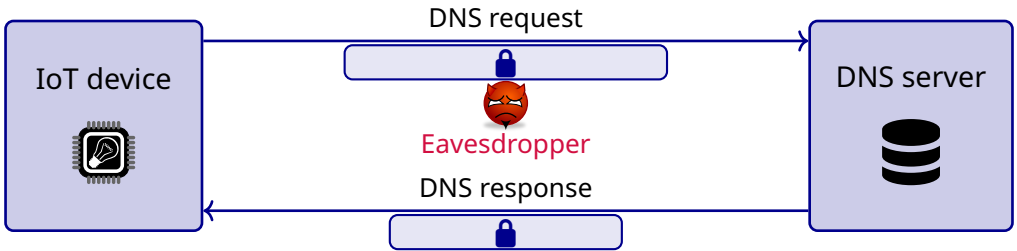
Conclusion & Outlook

Motivation

Attack Scenario: Eavesdropper wants to surveil name resolution in IoT

Motivation

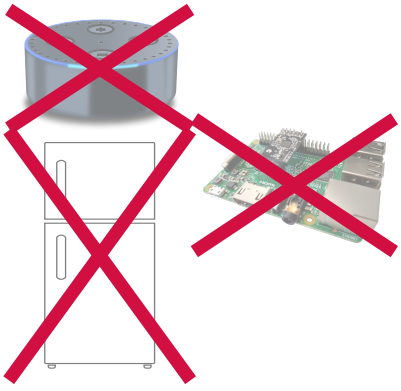
Attack Scenario: Eavesdropper wants to surveil name resolution in IoT



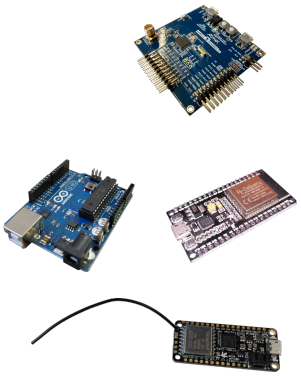
Countermeasure

Encrypt name resolution triggered by IoT devices against eavesdropping

Challenge I: Constrained IoT Nodes



Gigabytes
Terabytes



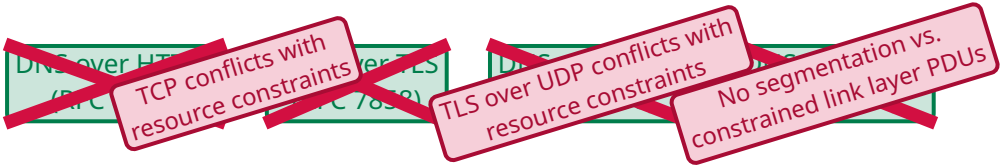
Kilobytes
Megabytes (at best!)

Challenge II: Constrained IoT Networks

- Low throughput, high packet loss, asymmetric link characteristics
- **High penalties on large packets** (link layer fragmentation)
- Typical data rates: **1 to 200 kBit/s**
- Typical frame sizes: **50 to 200 bytes**

Possible Solutions for Encrypted DNS

Possible Solutions for Encrypted DNS



New Proposal: DNS over CoAP (RFC 9953)

- **Encrypted communication**
  - Datagram *Transport Layer* Security (DTLS)
  - *Object Security* for Constrained RESTful Environments (OSCORE)
- **Block-wise message transfer**
  - Lightweight segmentation into blocks of *equal length*
- **En-route caching**
  - Mitigation of high link-layer packet loss

Outline

Motivation

CoAP Crash Course

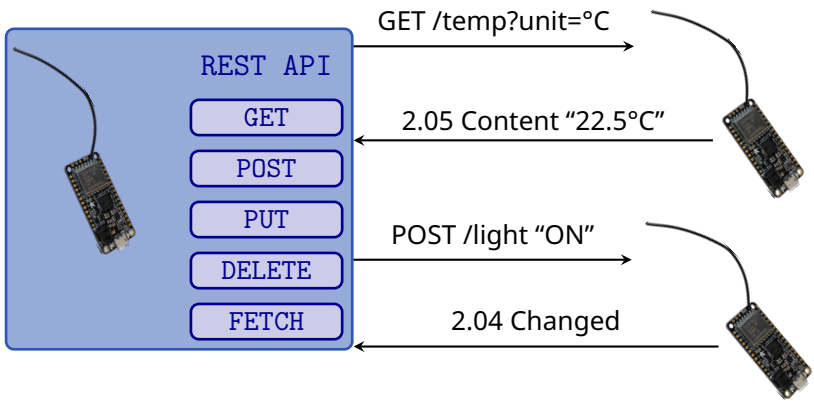
DNS over CoAP

Further Improvements

Conclusion & Outlook

CoAP: The Constrained Application Protocol

“REST over UDP” ~ The HTTP for IoT



CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

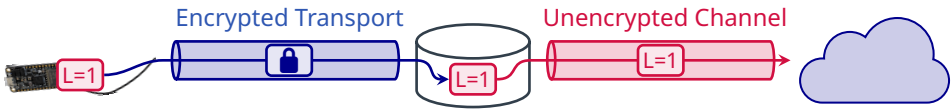
DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

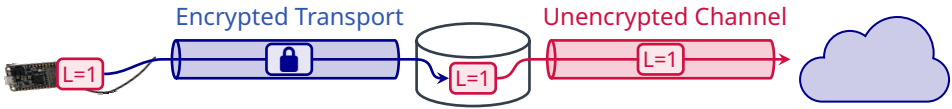
CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



CoAP Security Modes

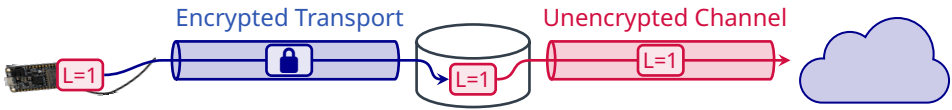
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

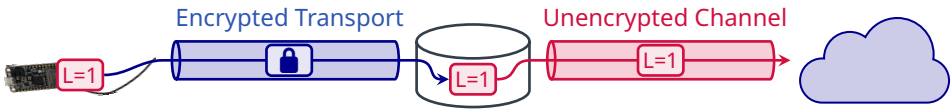
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



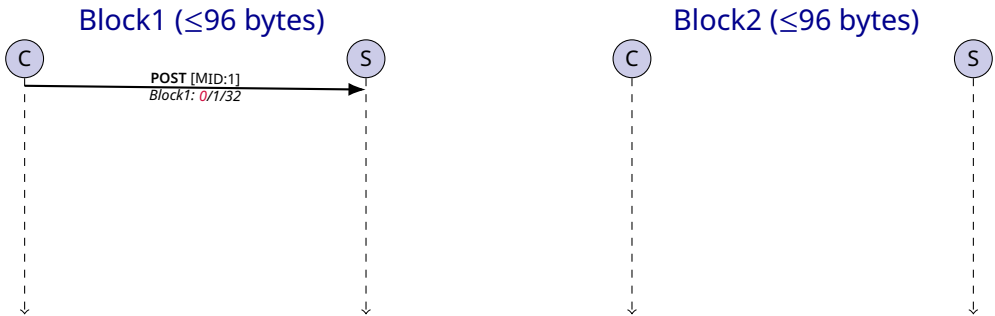
OSCORE Object Security for Constrained RESTful Environment

CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks

CoAP Block-wise Transfer

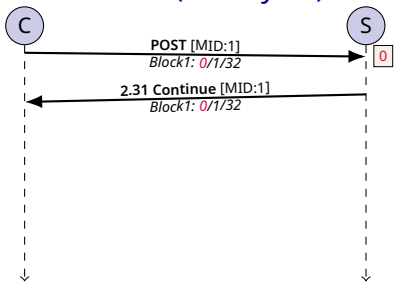
- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size



CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)

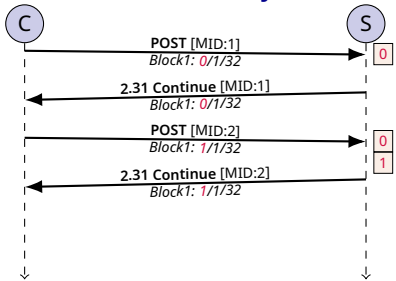


Block2 (≤96 bytes)

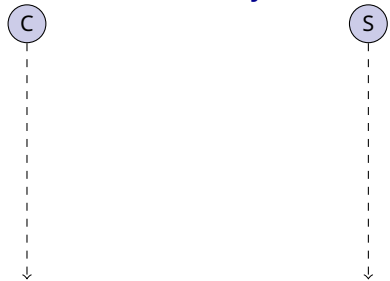
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



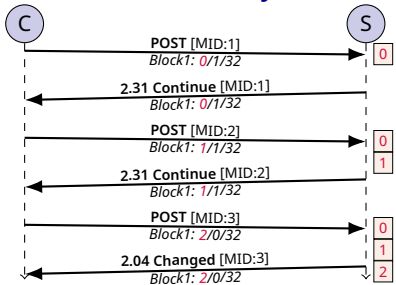
Block2 (≤96 bytes)



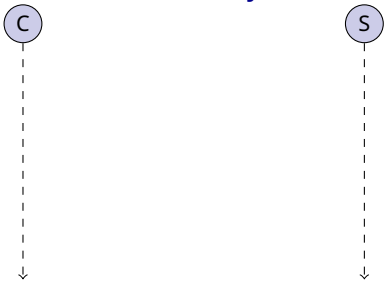
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



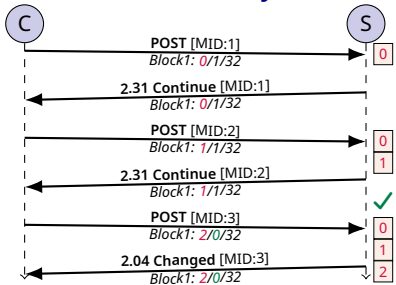
Block2 (≤96 bytes)



CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)

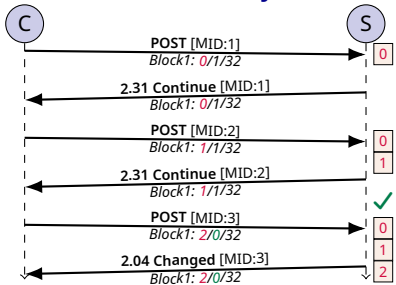


Block2 (≤96 bytes)

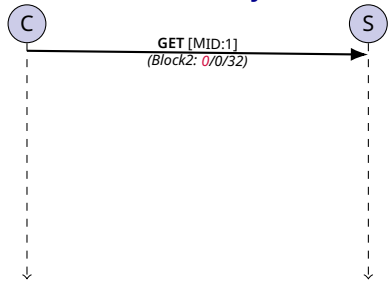
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



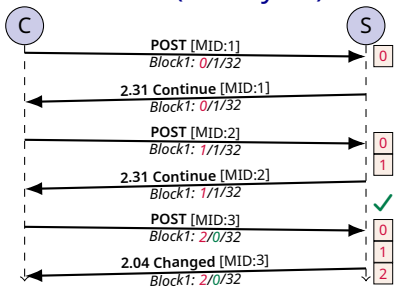
Block2 (≤96 bytes)



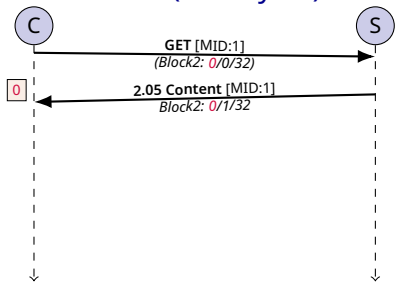
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



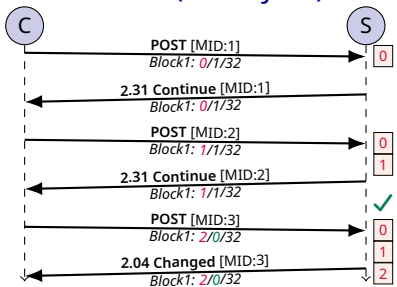
Block2 (≤96 bytes)



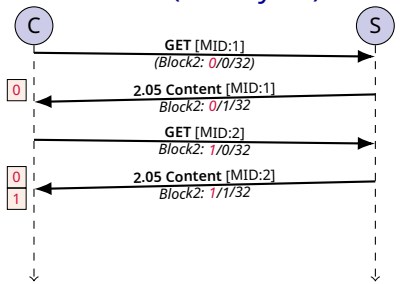
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



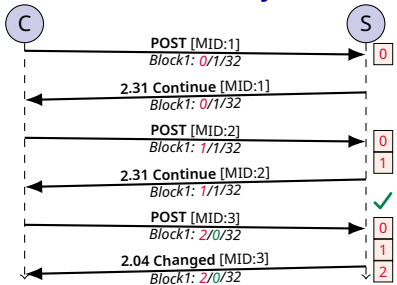
Block2 (≤96 bytes)



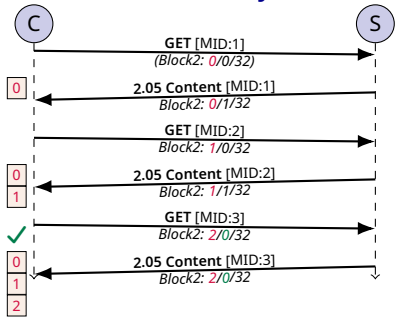
CoAP Block-wise Transfer

- Uses Block1 (for requests) and Block2 (for responses) option to segment messages into equal size blocks
- Values *n*/*m*/*s* in option: ***n*** = block number, ***m*** = more blocks, ***s*** = block size

Block1 (≤96 bytes)



Block2 (≤96 bytes)



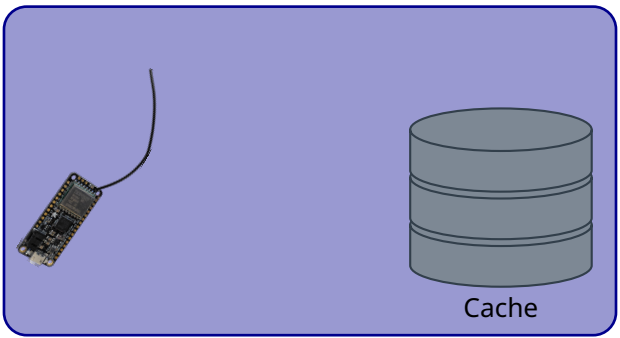
CoAP Caching

Client

Cache

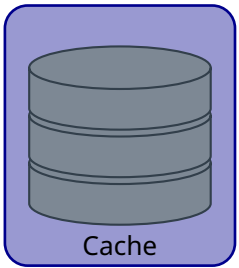
Server

CoAP Caching



CoAP Caching

Client

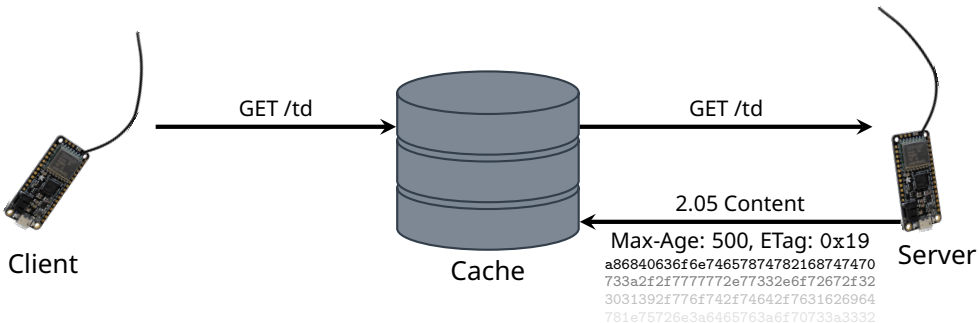


On proxy node

Server

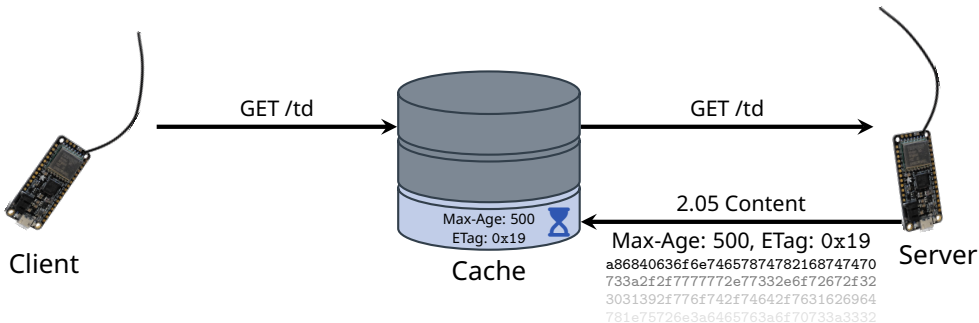
CoAP Caching

Caching provides **decoupling from packet loss**



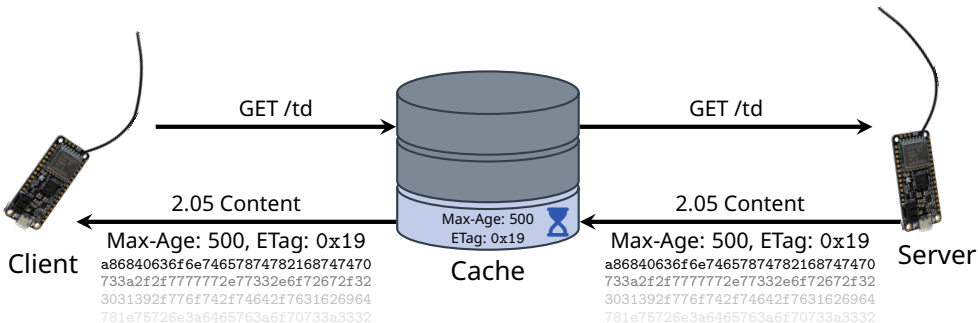
CoAP Caching

Caching provides **decoupling from packet loss**



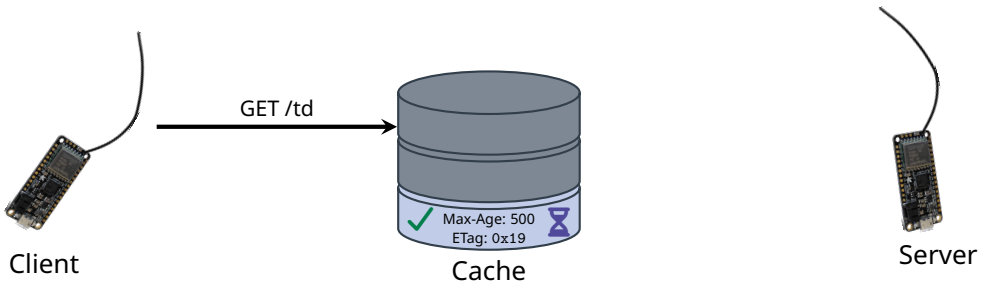
CoAP Caching

Caching provides **decoupling from packet loss**



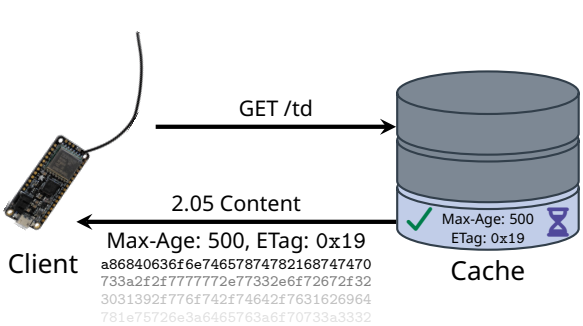
CoAP Caching

Caching provides **decoupling from packet loss**



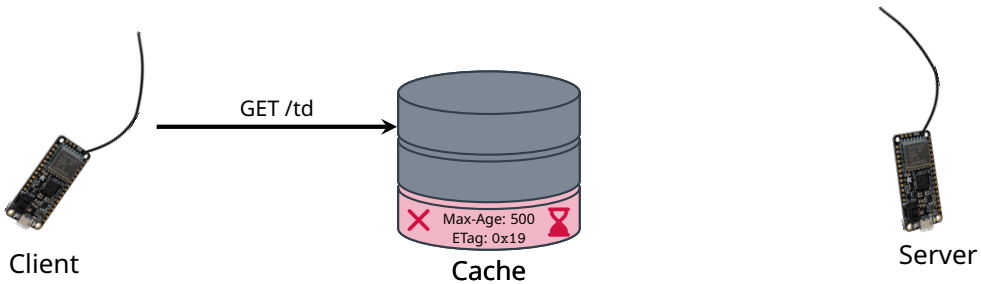
CoAP Caching

Caching provides **decoupling from packet loss**



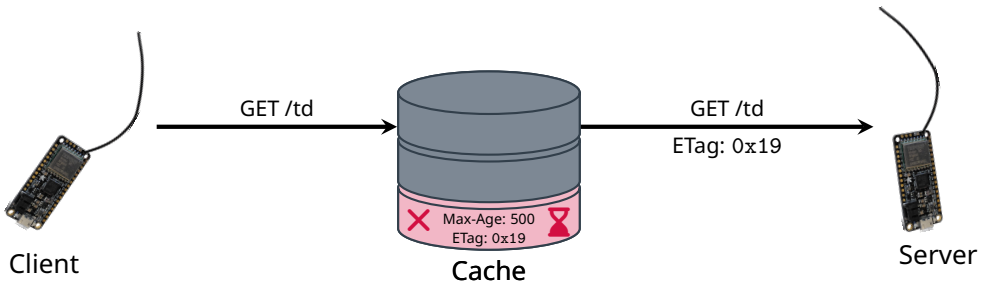
CoAP Caching

What if cache entry goes stale?



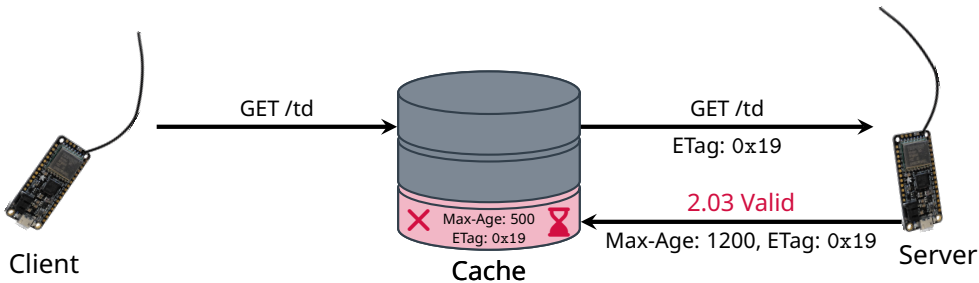
CoAP Caching

What if cache entry goes stale?



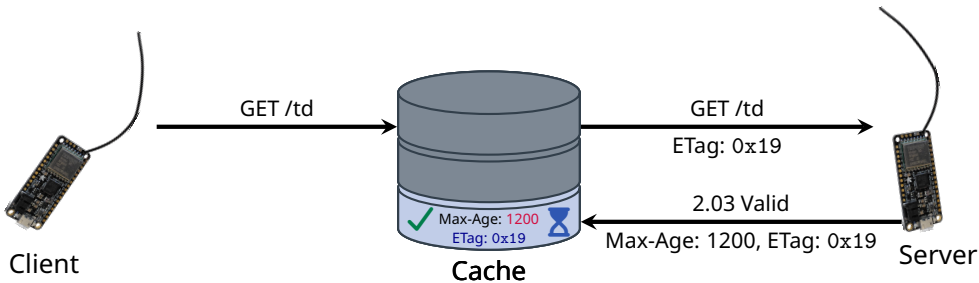
CoAP Caching

Cache validation **reduces data overhead**



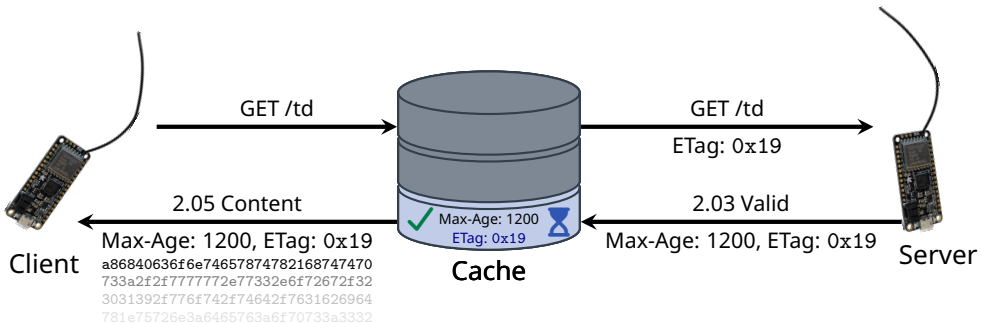
CoAP Caching

Cache validation **reduces data overhead**



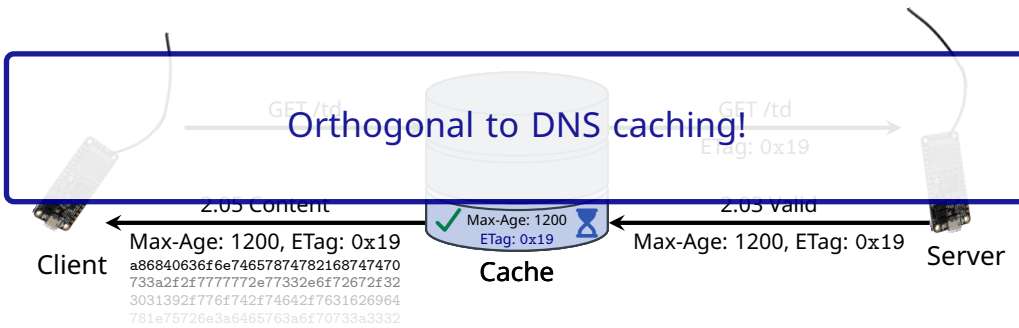
CoAP Caching

Cache validation **reduces data overhead**



CoAP Caching

Cache validation **reduces data overhead**



Outline

Motivation

CoAP Crash Course

DNS over CoAP

Further Improvements

Conclusion & Outlook

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST** (RFC 8484)?

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST** (RFC 8484)?

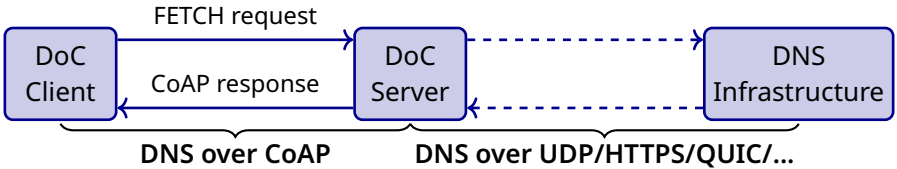
	HTTP	
	GET	POST
Responses cacheable	✓	✗
Application data carried in body	✗	✓
Block-wise transferable query	✗	✓

DNS over CoAP (DoC)

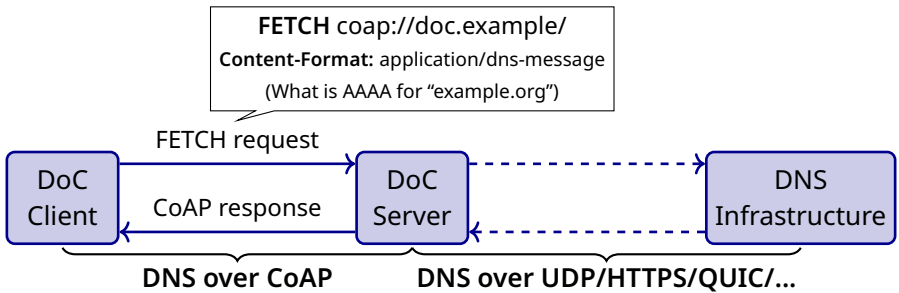
- Just map the DoH methods **GET** and **POST** (RFC 8484)?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

	CoAP		
	HTTP		
	GET	POST	FETCH
Responses cacheable	✓	✗	✓
Application data carried in body	✗	✓	✓
Block-wise transferable query	✗	✓	✓

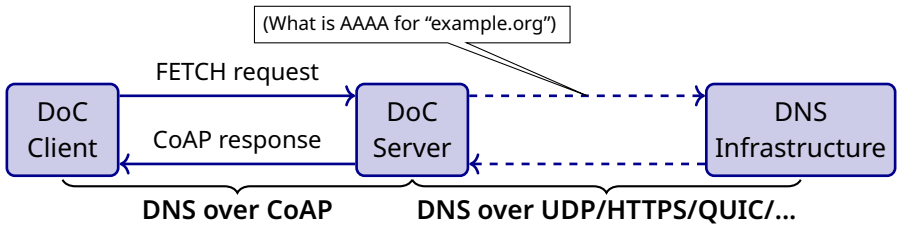
DNS over CoAP (DoC): Example Query



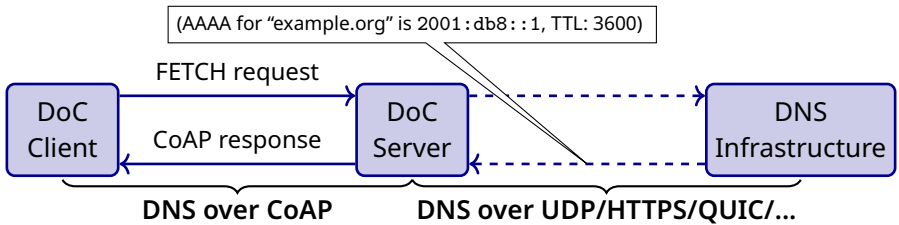
DNS over CoAP (DoC): Example Query



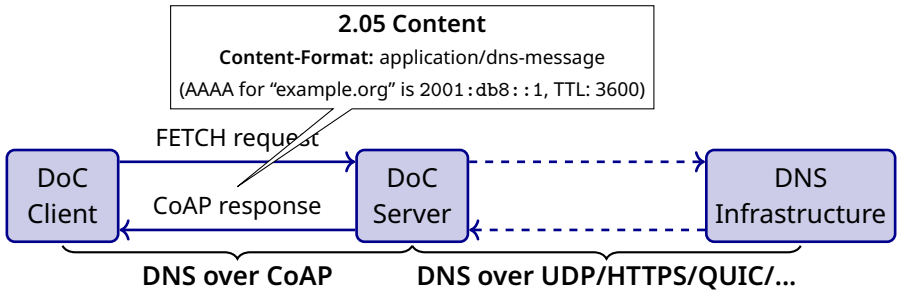
DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



Benefits of DoC

- As performant or slimmer as other UDP-based encrypted DNS solutions (e.g. DoDTLS, DoQ, …)
- When using Object Security (OSCORE): ≈ ½ memory usage & build size from Transport-Security-based solutions
- Comparable privacy guarantees to DoH
- Batteries included: Discoverable via SVCB records (RFC 9460), DHCP, RAs, etc. (RFC 9463) from the start

Outline

Motivation

CoAP Crash Course

DNS over CoAP

Further Improvements

Conclusion & Outlook

Further Improvements

Concise DNS Message Representation

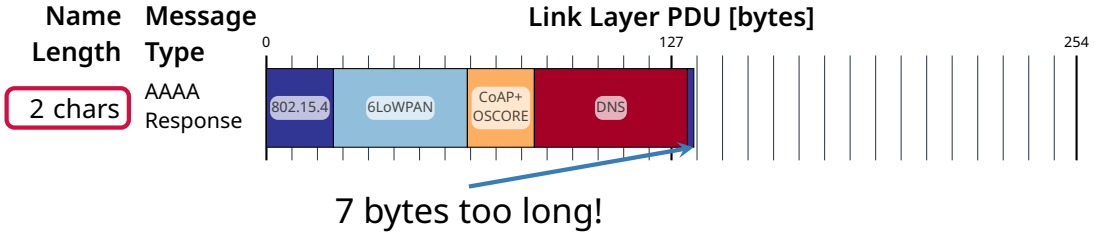
Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Name Length	
2 chars	(minimum)

Further Improvements

Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

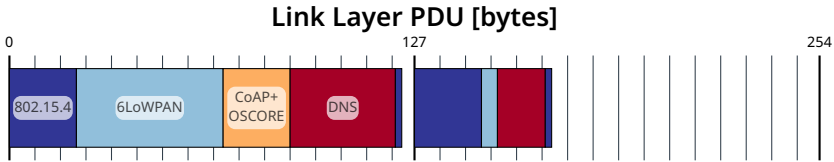


Further Improvements

Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes

Name Length	Message Type
2 chars	AAAA Response

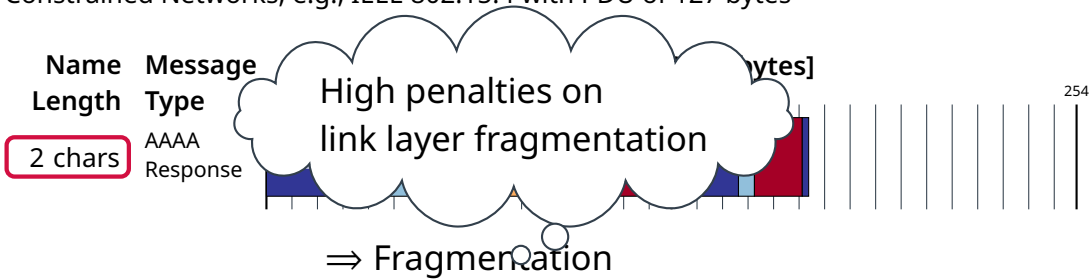


⇒ Fragmentation

Further Improvements

Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



Further Improvements

Concise DNS Message Representation

Concise DNS messages are needed

`application/dns+cbor`

Media Type and Content-Format

(*i.e.*, usable with both DoC and DoH)

`https://datatracker.ietf.org/doc/draft-lenders-dns-cbor/`

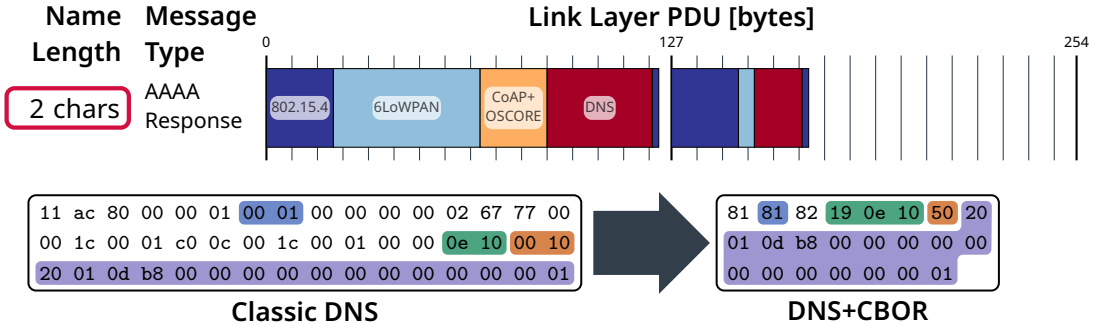
Objectives:

- Concise encoding of DNS messages using existing implementation (CBOR)
- Omits (redundant) DNS fields in DNS queries and responses
- Provides (optional) address and name compression using Packed CBOR

Further Improvements

Concise DNS Message Representation

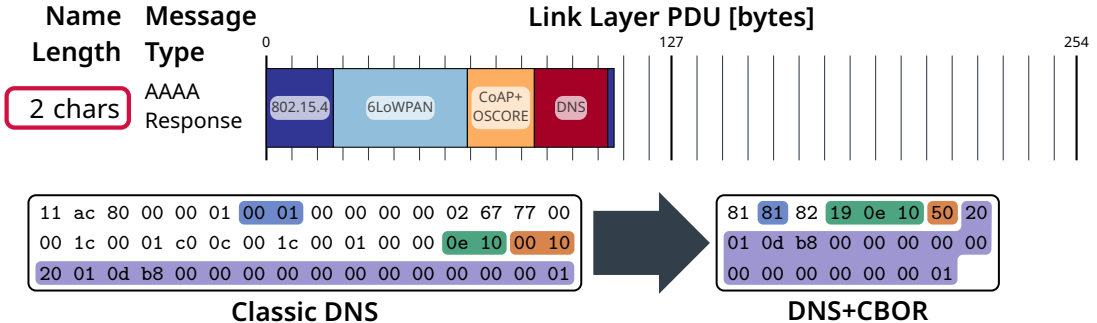
Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



Further Improvements

Concise DNS Message Representation

Constrained Networks, e.g., IEEE 802.15.4 with PDU of 127 bytes



Outline

Motivation

CoAP Crash Course

DNS over CoAP

Further Improvements

Conclusion & Outlook

Conclusion & Outlook

Secure & privacy-friendly DNS is ready for the constrained IoT:

- DoC with FETCH provides encrypted, cachable, and segmentable DNS
- En par in resolution time with existing UDP-based transfer protocols
- DNS over OSCORE outperforms DNS over DTLS, CoAPS, or QUIC
  both in packet and memory size

Outlook:

- CBOR-based DNS message format for smaller packet size
- Oblivious DNS over CoAP in the works
- Encrypted multicast DNS (i.e. DNS-SD/Bonjour/Avahi) could be an option

Implementations?

- Unbound Resolver WIP: `https://github.com/NLnetLabs/unbound/pull/1252`
- Client in RIOT OS `https://api.riot-os.org/group__net__gcoap__dns.html`

We want your help!

Get in Contact with Me

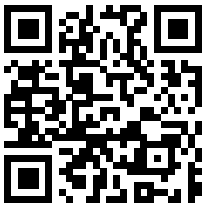
martine.lenders@tu-dresden.de

https://lenders.berlin

https://www.linkedin.com/in/martine-berlin

@miri64@ohai.social (@fedi.miri64.xyz in)

@miri64.xyz (@miri64@bsky.brid.gy in)



Further Reading I


M. S. Lenders, C. Amsüss, C. Gündogan, M. Nawrocki, T. C. Schmidt, and M. Wählisch. Sep. 2023.
Securing Name Resolution in the IoT: DNS over CoAP.
Proceedings of the ACM on Networking (PACMNET) 1, CoNEXT2 September 2023), 6:1–6:25.
doi:10.1145/3609423


M. S. Lenders, C. Amsüss, C. Gündoğan, T. C. Schmidt, and M. Wählisch. Mar. 2026.
DNS over CoAP (DoC).
RFC 9953. IETF.
doi:10.17487/RFC9953

Further Reading II


M. S. Lenders, C. Bormann, M. Gütschow, T. C. Schmidt, and M. Wählisch. Jul. 2026. *A Concise Binary Object Representation (CBOR) of DNS Messages*. Internet-Draft – work in progress 18. IETF. https://datatracker.ietf.org/doc/html/draft-lenders-dns-cbor-18


M. S. Lenders, T. C. Schmidt, and M. Wählisch. Jul. 2026. Secrets Best Not Shared: DNS Privacy Enhancements for the Constrained IoT. In *Proc. of the 11th IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, Piscataway, NJ, USA, 1475–1494. doi:10.1109/EuroSP68448.2026.00094

Further Reading III


M. S. Lenders, C. Bormann, T. C. Schmidt, and M. Wählisch. Aug. 2026.
A Leaner and Faster Web: How CBOR Can Improve Dynamic Content Encoding in JSON and DNS over HTTPS.
IEEE Transactions on Network and Service Management (TNSM) (2026).
doi:10.1109/TNSM.2026.3722114
Early Access.