Martine S. Lenders, TU Dresden, Germany (martine.lenders@tu-dresden.de)
Christian Amsüss, Unaffiliated, Vienna, Austria,
Carsten Bohrmann, Universität Bremen, TZI, Bremen, Germany,
Thomas C. Schmidt, HAW Hamburg, Hamburg, Germany,
Matthias Wählisch, TU Dresden, Barkhausen Institut, Dresden, Germany

Concise Binary Object Representation (CBOR) for DNS Messages and DNS over CoAP

Santa Marta, Colombia, ICANN DNS Symposium 2024, September 25, 2024

Outline

Outline

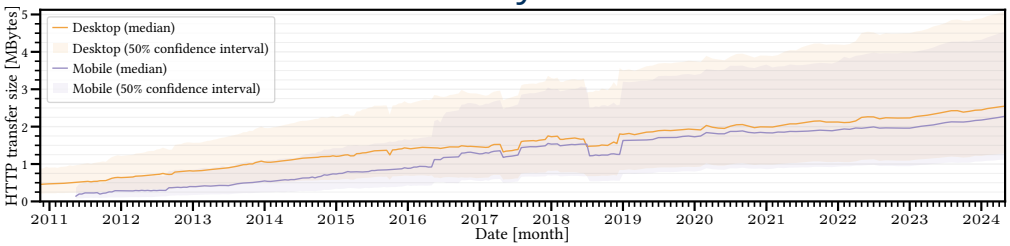
Global Access to the Web Requires ...

Fast Internet connectivity + High end devices

Global Access to the Web Requires ...

Fast Internet connectivity + High end devices

Why?



Source: `https://httparchive.org/reports/state-of-the-web`

Conflict: Modern Web Fosters Digital Inequality

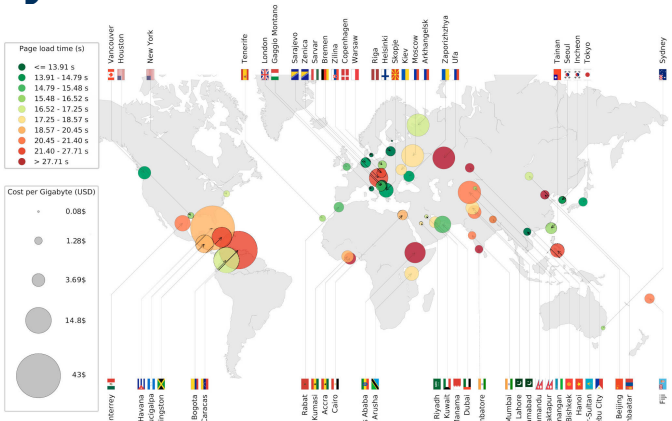


Figure source: M. Chaqfeh, *et al.*. 2023. **Towards a World Wide Web without digital inequality.** https://doi.org/10.1073/pnas.2212649120

How to Decrease Latency?

Get object sizes smaller
JSON contributes growing part of transfer size

Get message sizes smaller
DNS poses a latency bottleneck to Web

How to Decrease Latency?

Learn from constrained IoT?

Concise **B**inary **O**bject **R**epresentation (CBOR):

- CBOR is smaller than JSON
- CBOR allows for elision of message fields
- Packed CBOR allows for value compression

CBOR is smaller than JSON

A simple example, integers:

JSON

12

CBOR is smaller than JSON

A simple example, integers:

JSON

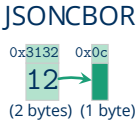
0x3132

12

(2 bytes)

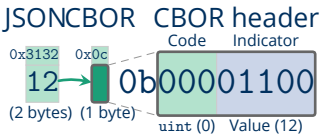
CBOR is smaller than JSON

A simple example, integers:



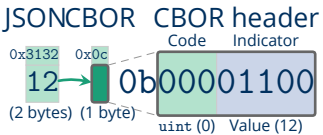
CBOR is smaller than JSON

A simple example, integers:

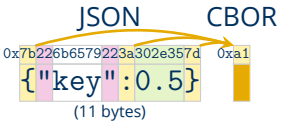


CBOR is smaller than JSON

A simple example, integers:

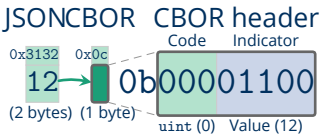


A more advanced example, maps:

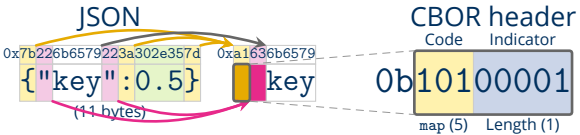


CBOR is smaller than JSON

A simple example, integers:

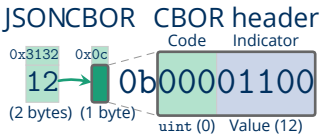


A more advanced example, maps:

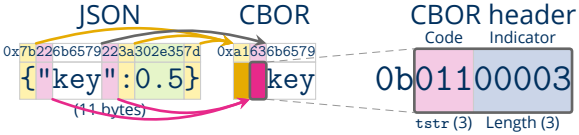


CBOR is smaller than JSON

A simple example, integers:

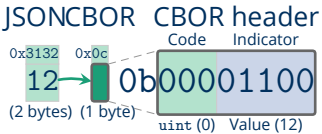


A more advanced example, maps:

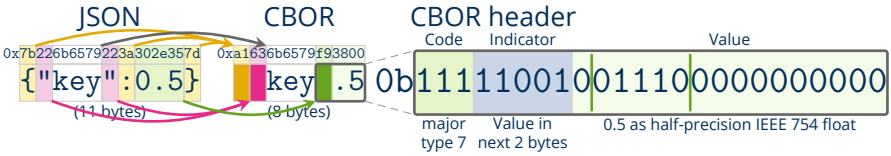


CBOR is smaller than JSON

A simple example, integers:

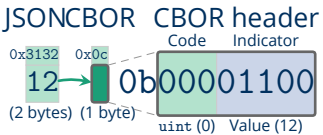


A more advanced example, maps:

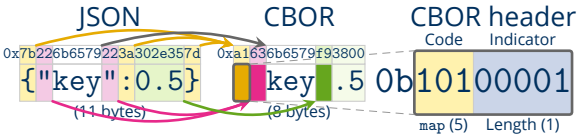


CBOR is smaller than JSON

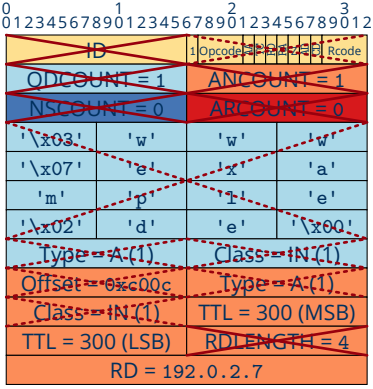
A simple example, integers:



A more advanced example, maps:



CBOR structure allows for elision



(48 bytes)

For example, CBOR to reduce DNS message sizes:

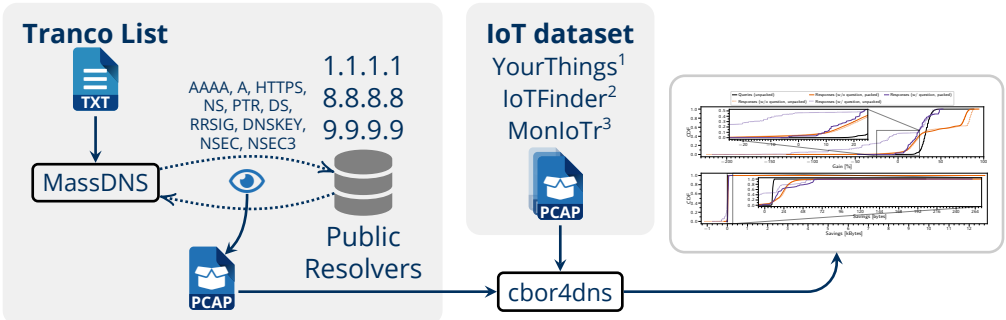
- Message sections as CBOR arrays:
  Elide count field in favor of array length
- Elide section if not used, use context clues to identify section
- Elide fields with commonly used values (e.g. `IN` record class)

```
[[[300,h'c0000207']]]
```

(11 bytes = `81 81 82 19012c 44c0000207`)

Outline

CBOR as DNS Message Format: Method

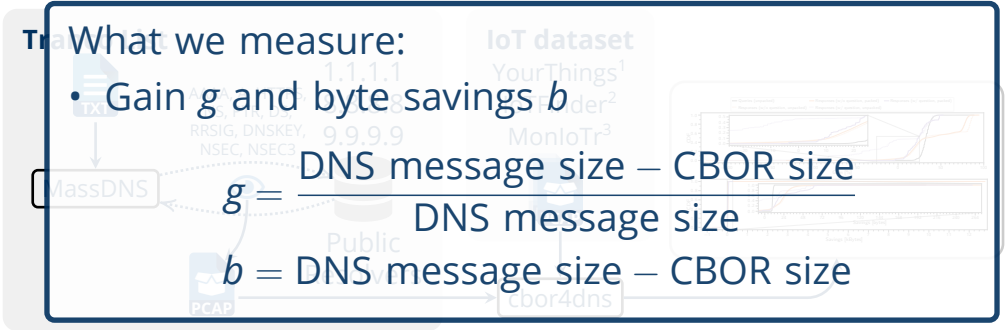


[1] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. 2019. **SoK: Security Evaluation of Home-Based IoT Deployments**. In *IEEE S&P 2019*. 1362–1380.

[2] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis. 2020. **IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis**. In *IEEE EuroS&P 2020*. 474–489.

[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

CBOR as DNS Message Format: Method



What we measure:

- Gain g and byte savings b

$$g = \frac{\text{DNS message size} - \text{CBOR size}}{\text{DNS message size}}$$

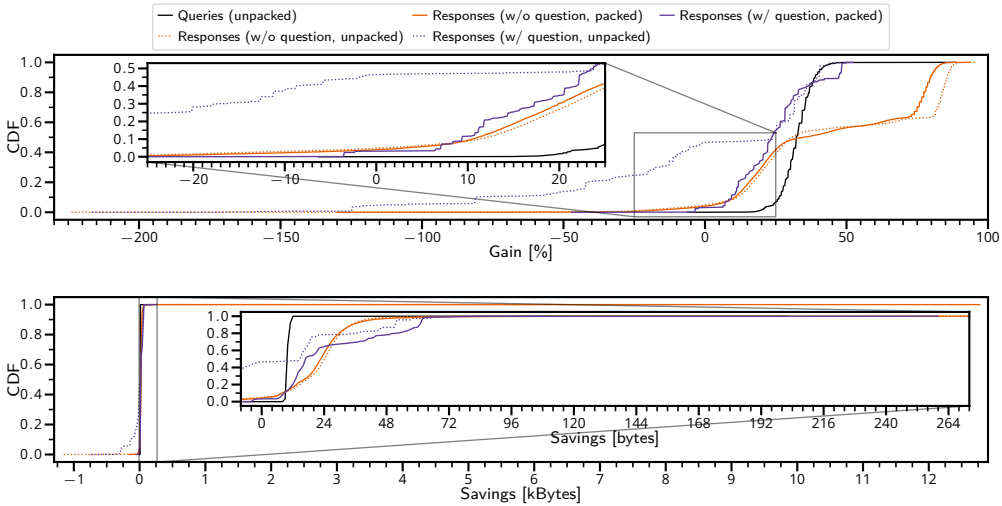
$$b = \text{DNS message size} - \text{CBOR size}$$

[1] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. 2019. **SoK: Security Evaluation of Home-Based IoT Deployments**. In *IEEE S&P 2019*. 1362–1380.

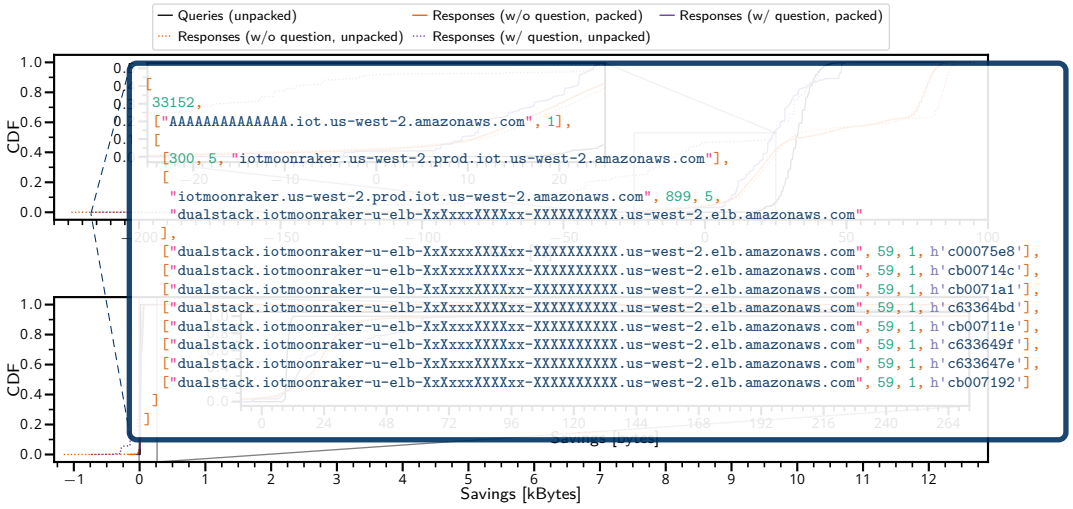
[2] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis. 2020. **IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis**. In *IEEE EuroS&P 2020*. 474–489.

[3] J. Ren, D.J. Dubois, D. Choffnes, A.M. Mandalari, R. Kolcun, and H. Haddadi. 2019. **Information Exposure for Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach**. In *Proc. of the Internet Measurement Conference (IMC)*. ACM.

Gain and Byte Savings CBOR-encoded DNS

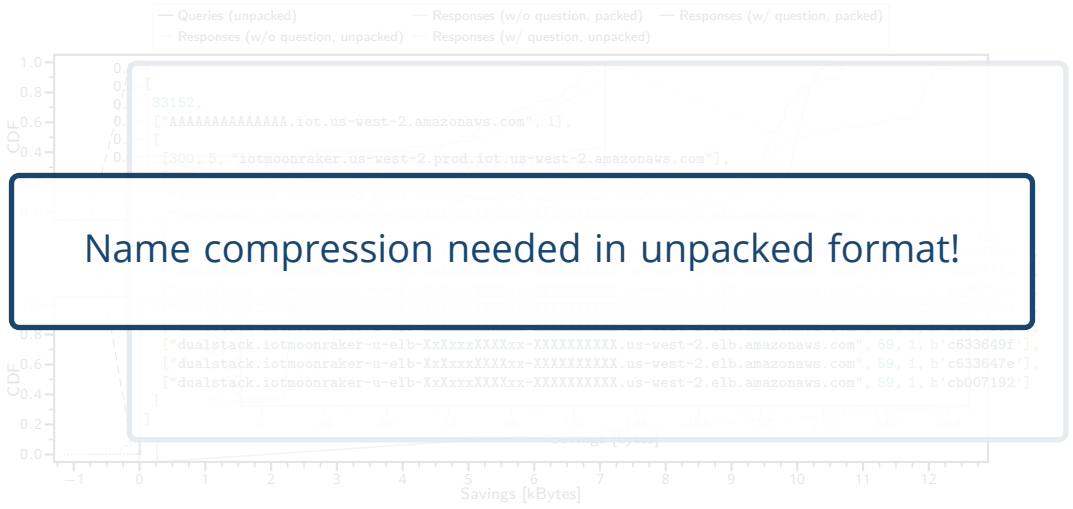


Gain and Byte Savings CBOR-encoded DNS




```
[
  33152,
  ["AAAAAAAAAAAAAA.iot.us-west-2.amazonaws.com", 1],
  [
   [300, 5, "iotmoonraker.us-west-2.prod.iot.us-west-2.amazonaws.com"],
   [
    "iotmoonraker.us-west-2.prod.iot.us-west-2.amazonaws.com", 899, 5,
    "dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com"
   ],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'c00075e8'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'cb00714c'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'cb0071a1'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'c63364bd'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'cb00711e'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'c633649f'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'c633647e'],
   ["dualstack.iotmoonraker-u-elb-XxXxxxXXXXxx-XXXXXXXXXX.us-west-2.elb.amazonaws.com", 59, 1, h'cb007192']
  ]
]
```

Gain and Byte Savings CBOR-encoded DNS



Name compression needed in unpacked format!

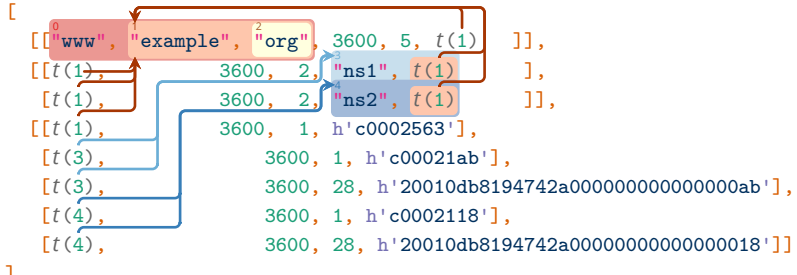
Name Component Referencing

```
[
  [["www.example.org", 3600, 5, "example.org"]],
  [["example.org", 3600,  2, "ns1.example.org"],
   ["example.org", 3600,  2, "ns2.example.org"]],
  [["example.org", 3600,  1, h'c0002563'],
   ["ns1.example.org", 3600, 1, h'c00021ab'],
   ["ns1.example.org", 3600, 28, h'20010db8194742a0000000000000000ab'],
   ["ns2.example.org", 3600, 1, h'c0002118'],
   ["ns2.example.org", 3600, 28, h'20010db8194742a00000000000000018']]
]
```

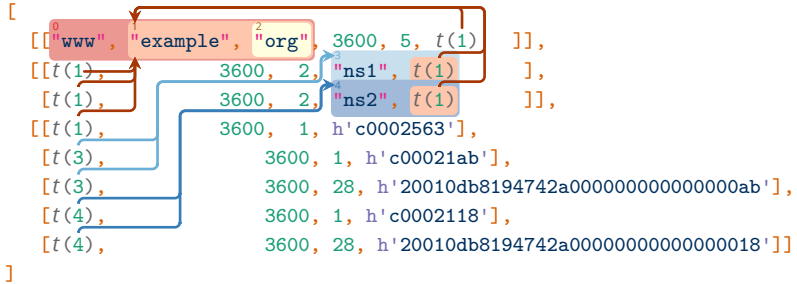
Name Component Referencing

```
[
  [["www", "example", "org", 3600, 5, t(1)   ]],
  [[t(1),          3600,  2, "ns1", t(1)      ],
   [t(1),          3600,  2, "ns2", t(1)      ]],
  [[t(1),          3600,  1, h'c0002563'],
   [t(3),              3600, 1, h'c00021ab'],
   [t(3),              3600, 28, h'20010db8194742a000000000000000ab'],
   [t(4),              3600, 1, h'c0002118'],
   [t(4),              3600, 28, h'20010db8194742a00000000000000018']]
]
```

Name Component Referencing



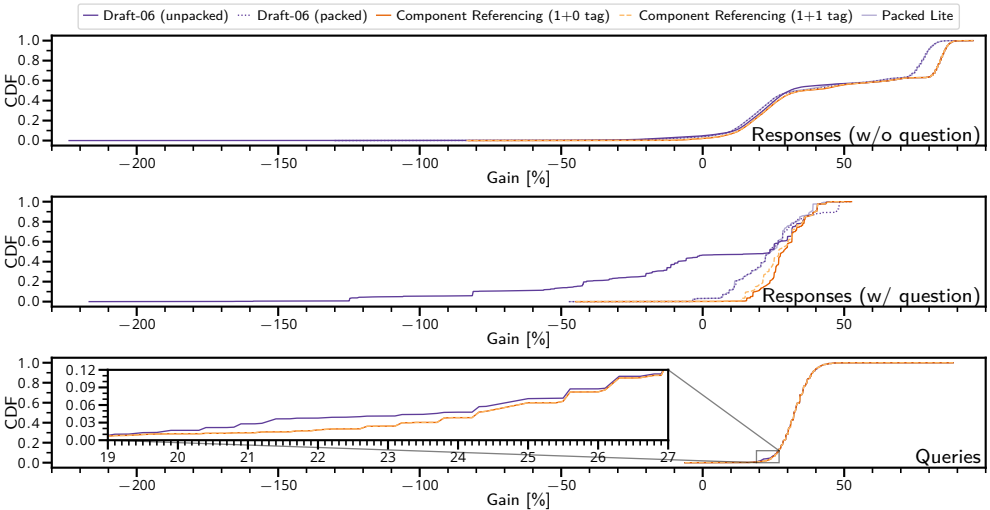
Name Component Referencing



For our evaluation:

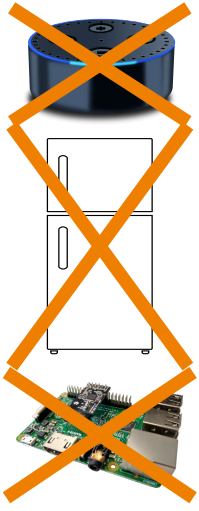
- $t = 7$ (c7 $\Rightarrow$ *1+0 (bytes) tag*)
- $t = 48$ (d8 30 $\Rightarrow$ *1+1 (bytes) tag*)

Gain with Name Compression



Outline

Challenge for Encrypted DNS: Constrained IoT



Constrained nodes (RFC 7228):

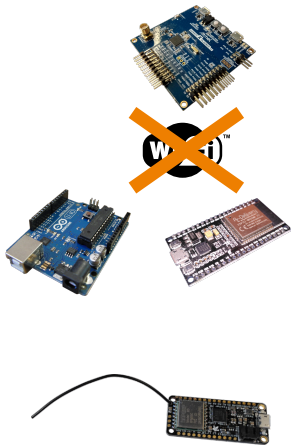
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Challenge for Encrypted DNS: Constrained IoT

Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Challenge for Encrypted DNS: Constrained IoT



Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT

BLE

zigbee

LoRa

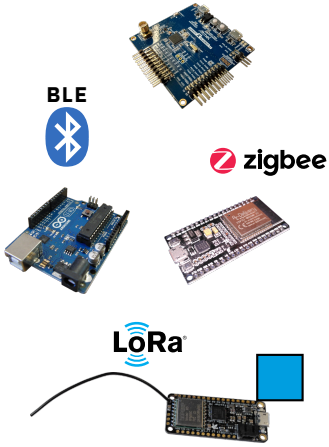
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



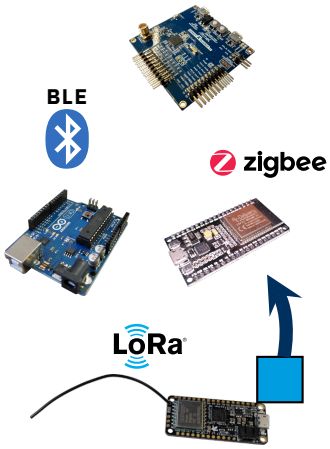
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



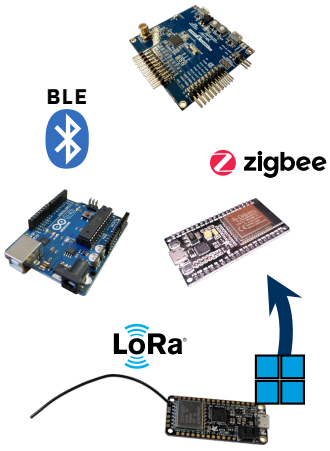
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



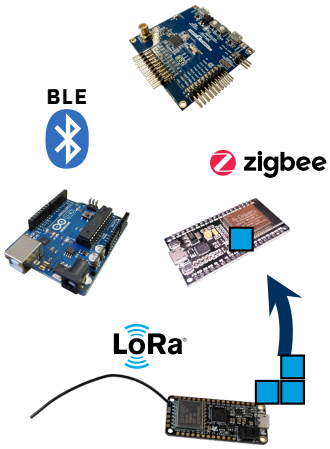
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



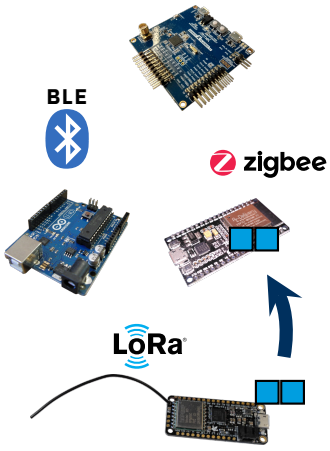
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



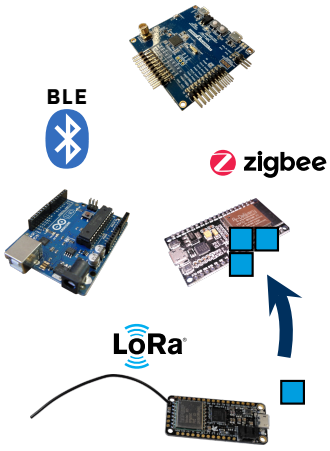
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



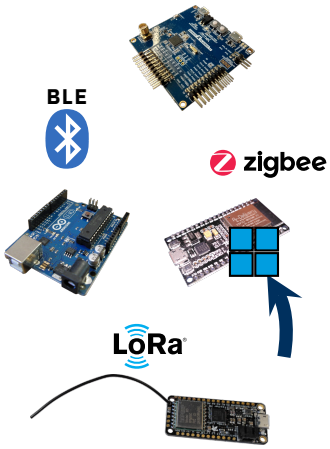
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



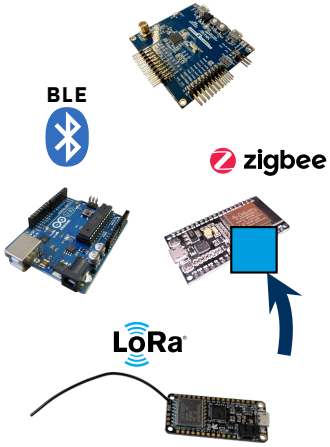
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



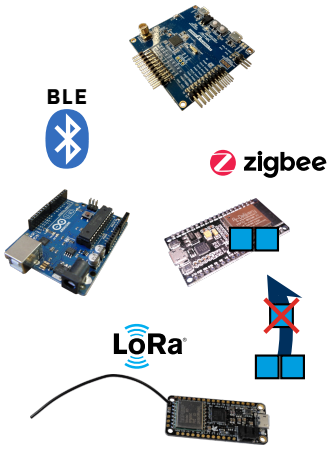
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



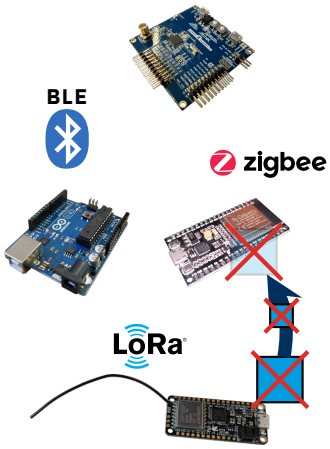
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



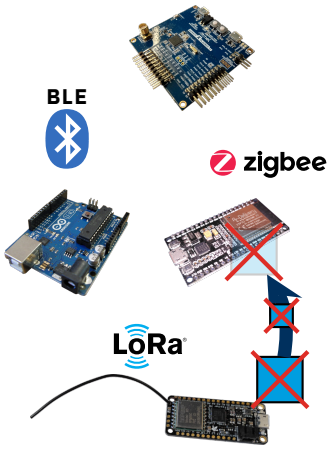
Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Challenge for Encrypted DNS: Constrained IoT



Constrained nodes (RFC 7228):

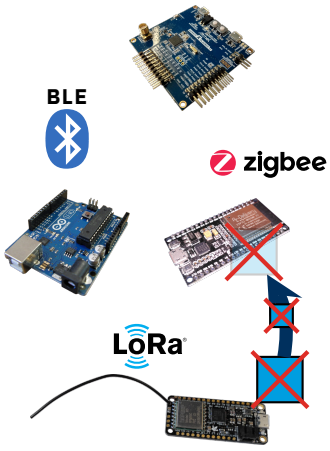
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Characteristic	IEEE 802.15.4	BLE	LoRaWAN
Data rate [kBit/s]	124–162	125–2000	0.3–5
Frame size [bytes]	127	≥ 1280	59–250

Challenge for Encrypted DNS: Constrained IoT



Constrained nodes (RFC 7228):

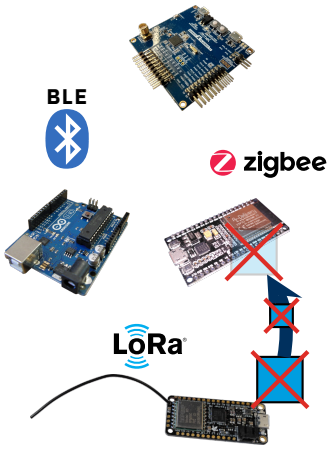
Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained networks:

- Low throughput, high packet loss, asymmetric link characteristics
- High penalties on large packets (link layer fragmentation)

Characteristic	IEEE 802.15.4	BLE	LoRaWAN
Data rate [kBit/s]	124–162	125–2000	0.3–5
Frame size [bytes]	127	≥ 1280	59–250

Challenge for Encrypted DNS: Constrained IoT



Constrained nodes (RFC 7228):

Characteristic	Class 0	Class 1	Class 2
Data size [KiB]	$\ll 10$	≈ 10	≈ 50
Code size [KiB]	$\ll 100$	≈ 100	≈ 250

Constrained

- Low thro… …nk characteristi…
- High penalties on large packets (link la… …fragmentation)

0.000003% – 0.0009%
slower than WiFi 6

Characteristic	IEEE 802.15.4	BLE	LoRaWAN
Data rate [kBit/s]	124–162	125–2000	0.3–5
Frame size [bytes]	127	≥ 1280	59–250

Possible Solutions for Encrypted DNS

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

Possible Solutions for Encrypted DNS

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

Possible Solutions for Encrypted DNS

DNS over HTTPS (RFC 8484)

DNS over TLS (RFC 7858)

DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions for Encrypted DNS

DNS over QUIC (RFC 9250)

DNS over DTLS (RFC 8094)

Possible Solutions for Encrypted DNS

Possible Solutions for Encrypted DNS

Possible Solutions for Encrypted DNS

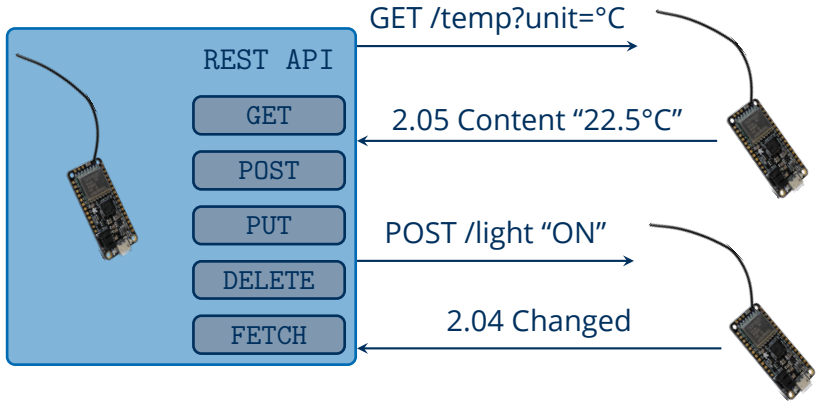
Our proposal: DNS over CoAP

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

- **Encrypted communication** based on DTLS or OSCORE
- **Block-wise message transfer** provides message segmentation
- **En-route caching** mitigates high link layer packet loss
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

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

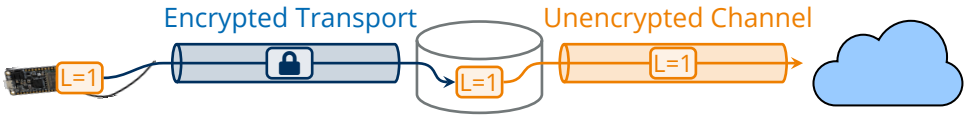
DTLS Datagram Transport Layer Security (≈ TLS over UDP)

CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)

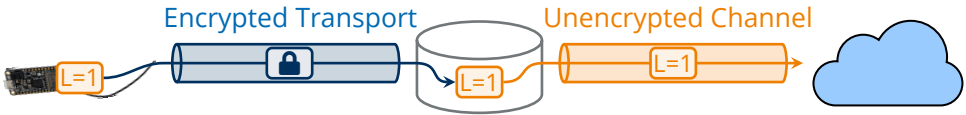
CoAP Security Modes

DTLS Datagram Transport Layer Security (≈ TLS over UDP)



CoAP Security Modes

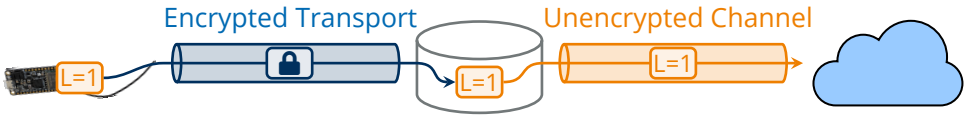
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



OSCORE Object Security for Constrained RESTful Environment

CoAP Security Modes

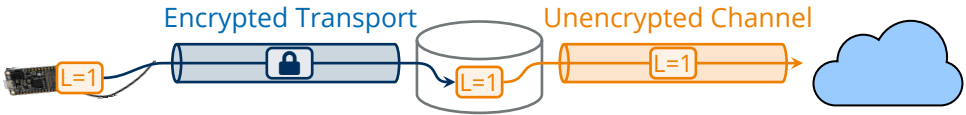
DTLS Datagram Transport Layer Security (≈ TLS over UDP)



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

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?

DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?

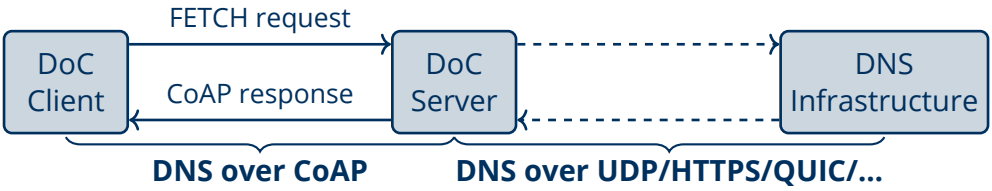
	HTTP	
	GET	POST
Responses cacheable	✓	✘
Application data carried in body	✘	✓
Block-wise transferable query	✘	✓

DNS over CoAP (DoC)

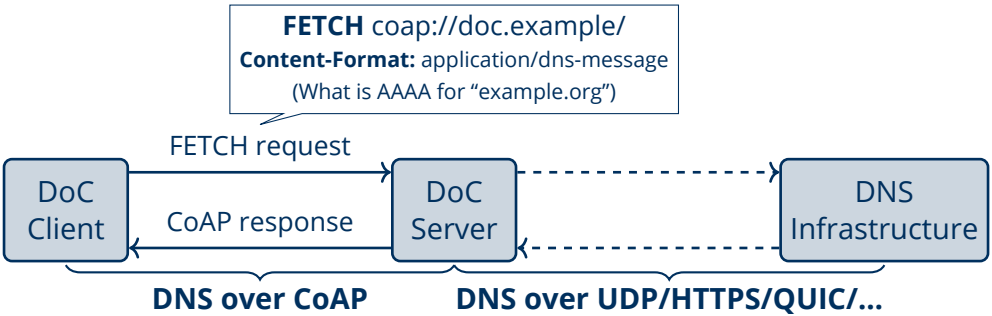
- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

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

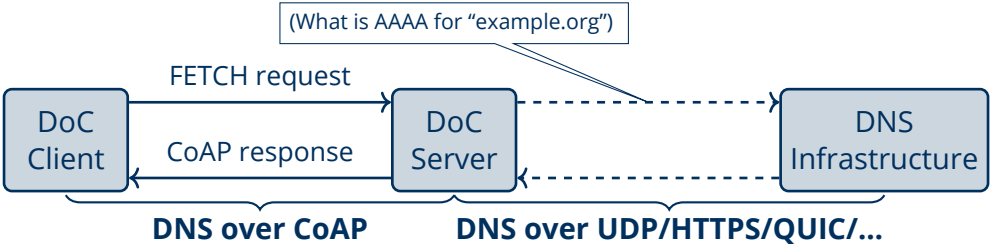
DNS over CoAP (DoC): Example Query



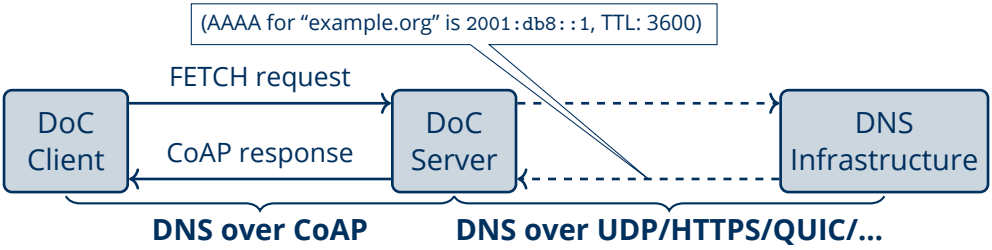
DNS over CoAP (DoC): Example Query



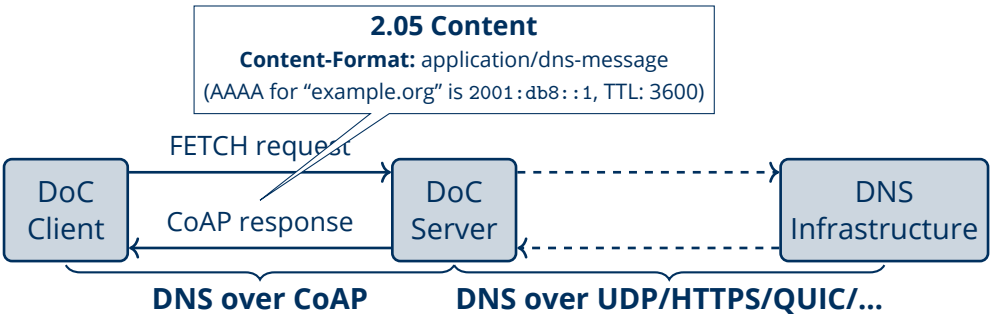
DNS over CoAP (DoC): Example Query



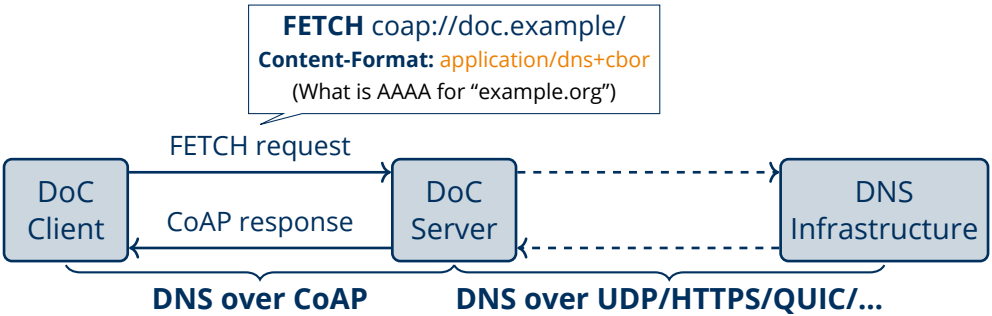
DNS over CoAP (DoC): Example Query



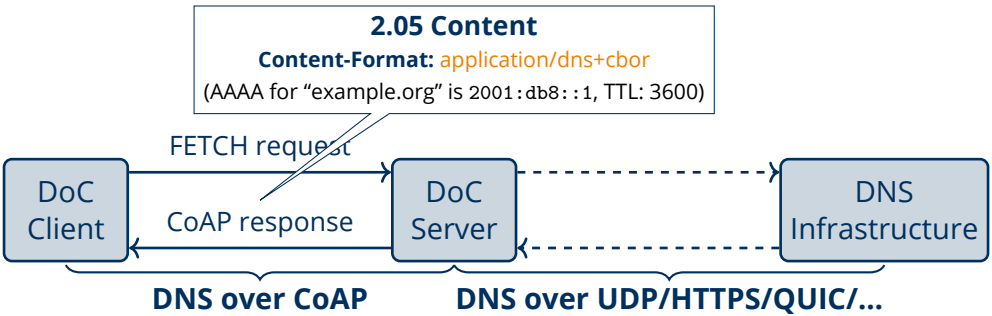
DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



DNS over CoAP (DoC): Example Query



Outline

Conclusion

Make DNS Messages smaller.

- Improved CBOR DNS message format preferred over classic DNS
- DoH or DoC as transport
- Protocol design can decrease latency:
  - Raw binary should be preferred over ASCII encoding
  - Use size-adaptive data types and delta compression where possible
  - Do not just convert blindly to CBOR, use CBOR features

We need your implementations!

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