Constrained Application Protocol (CoAP) over Bundle Protocol (BP)

draft-gomez-core-coap-bp-03

Intended Status: Standards Track

Carles Gomez

Anna Calveras

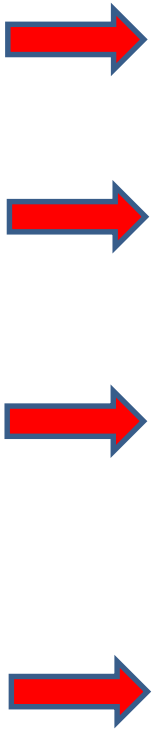
Universitat Politècnica de Catalunya

Status

- draft-gomez-core-coap-bp
  - -00 presented in IETF 119
    - CoRE and DTN WGs
  - -01 presented in IETF 120
    - CoRE and DTN WGs
  - -02 presented in IETF 121
    - CoRE WG (new CoAP option, enables message aggregation)

- Revisions -02 and -03
  - Address feedback from IETF 120 and IETF 121
  - Provide more content

Table of contents



2.3. New terms

- Single message:
  - CoAP message carried as the payload of the underlying layer PDU
  - In CoAP over BP, a Single message is carried as the block-type-specific data field of the Bundle Payload Block of the encapsulating bundle
- Aggregate message:
  - A concatenation of Single messages that carry the Payload-length option
  - In CoAP over BP, an Aggregate message is carried as the block-type-specific data field of the Bundle Payload Block of the encapsulating bundle

4.3. Payload-length option

- Indicates the size of the payload of a CoAP message
  - The option value is an integer number of bytes
  - Allows message aggregation
    - May be compatible with application requirements, while reducing protocol overhead

-

No.	C	U	N	R	Name	Format	Length	Default
TBD	x				Payload-length	uint	0 or more	(none)

C = Critical, U = Unsafe, N = NoCacheKey, R = Repeatable
(*) See below.

5. Encapsulating bundle

- MAX_AGGR_DELAY:
  - Maximum time since the first Single message is generated until the Aggregate message is passed to the BP layer

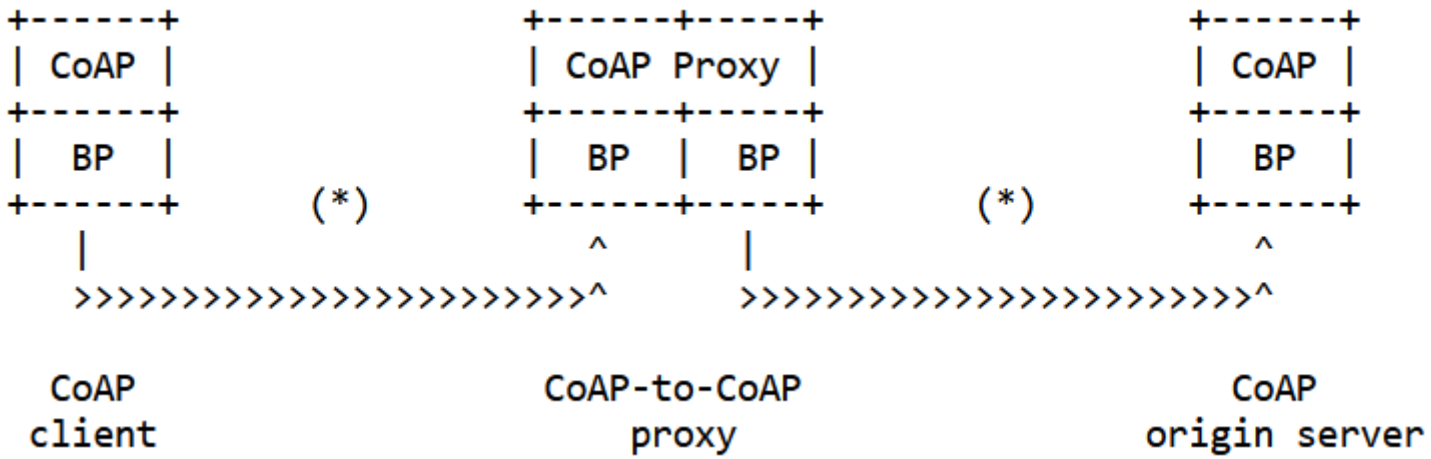
- Lifetime field of the bundle carrying an Aggregate message is set to:
  - EXCHANGE_LIFETIME + MAX_AGGR_DELAY
    - If the Aggregate message only comprises CON messages
  - NON_LIFETIME + MAX_AGGR_DELAY
    - If the Aggregate message only comprises NON messages
  - max (EXCHANGE_LIFETIME, NON_LIFETIME) + MAX_AGGR_DELAY
    - Otherwise

9. Proxying (I)

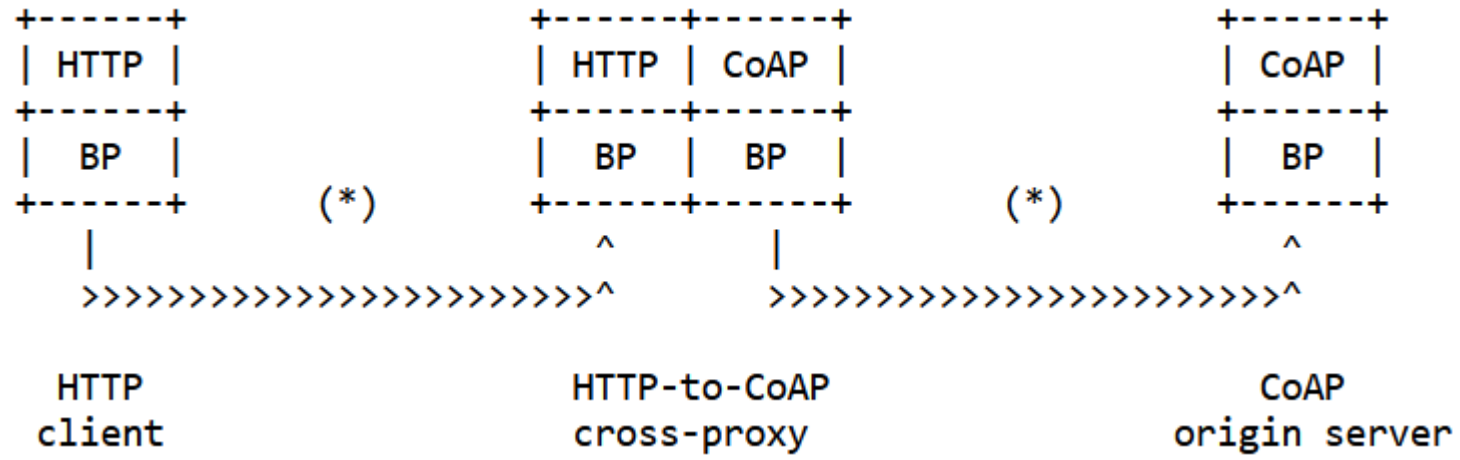
- CoAP proxy (RFC 7252)
  - A CoAP endpoint, an intermediary
  - Forwarding requests and relaying back responses
    - Caching, namespace translation, or protocol translation
  - Service responses from a cache in order to reduce response time, network bandwidth, and energy consumption
    - Useful benefits also where BP is used

9. Proxying (II)

- CoAP-to-CoAP proxy:



- HTTP-to-CoAP cross-proxy:



11. Securing CoAP over BP (I)

- BPSec allows to protect all fields of a CoAP message carried over BP

- In scenarios with CoAP proxies, BPSec cannot ensure the protection of application-layer data between a CoAP client and the CoAP origin server
  - In that case, OSCORE SHOULD be used to protect application-layer data between the two actual CoAP endpoints

11. Securing CoAP over BP (II)

- In scenarios without CoAP proxies, both OSCORE or BPSec MAY be used to provide end-to-end application-layer data protection

- Open question: is there any reason why both OSCORE and BPSec should be simultaneously used in a scenario known to be proxy-less?

12.3. CoAP option numbers registry

- IANA is requested to add the Payload-length option to the CoAP Option Numbers registry:

Number	Name	Reference
TBD1	Payload-length	[[this document]]

Other updates

- Section 4.1. Messaging Model:
  - No-Response option [RFC7967] now mentioned

- Section 7. Observe:
  - Determining whether a notification was sent by the server later than another notification MUST be performed based on the creation timestamps of the encapsulating bundles
  - draft-ietf-core-conditional-attributes now mentioned

Thanks!
Questions? Comments?

Carles Gomez

Anna Calveras

Universitat Politècnica de Catalunya