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

draft-ietf-core-coap-bp-01

Intended Status: Standards Track

Carles Gomez

Anna Calveras

Universitat Politècnica de Catalunya

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

Cofinanciado por la Unión Europea

AGENCIA ESTATAL DE INVESTIGACIÓN

This work was funded in part by the Spanish MCIU/AEI/10.13039/501100011033/FEDER/UE through project PID2023-146378NB-I00

IETF 124 Montreal, CoRE WG, November 2025

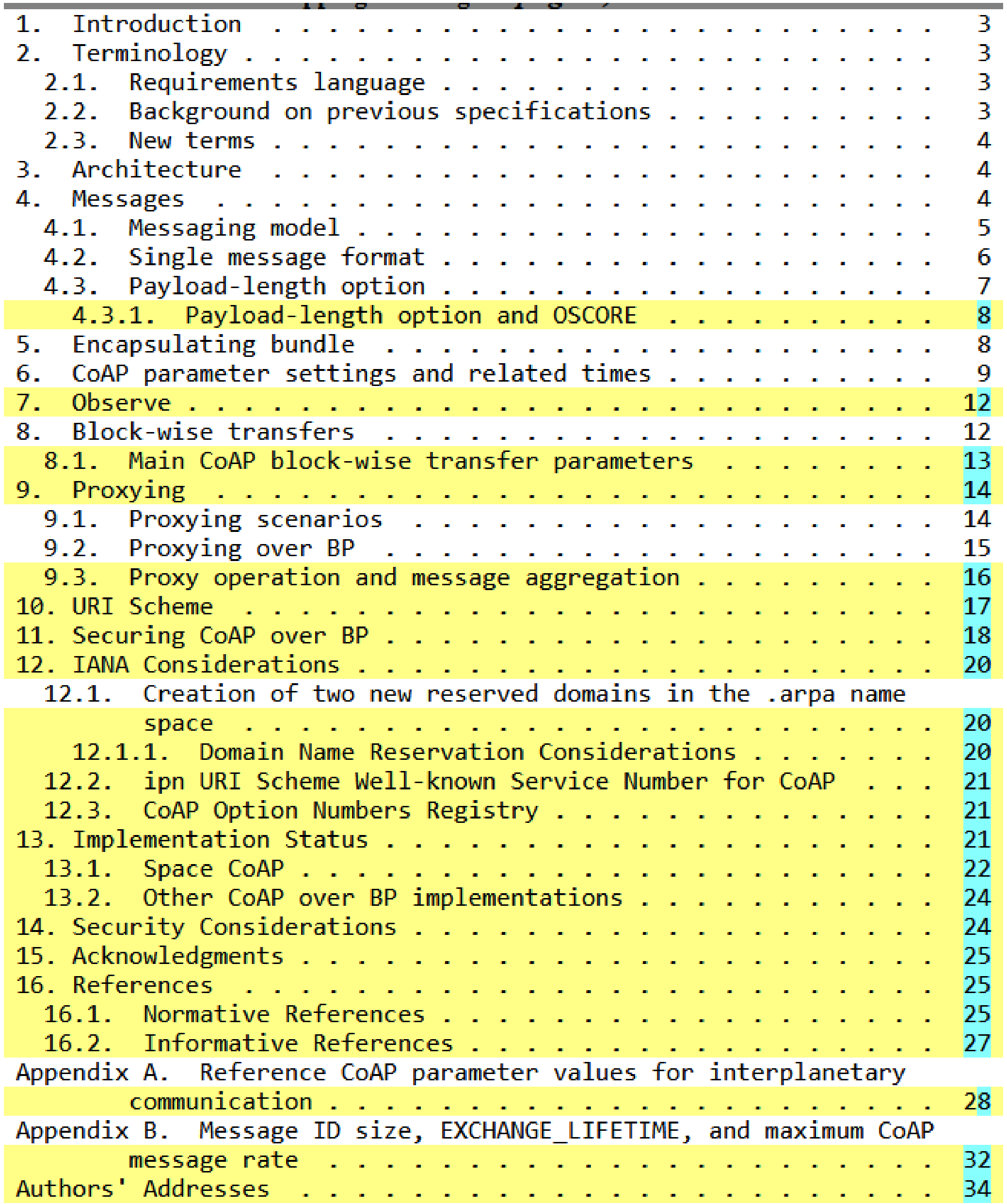
Status

- Draft adopted after IETF 123 (Madrid)
  - draft-gomez-core-coap-bp-04

- draft-ietf-core-coap-bp-00
  - Same technical content as draft-gomez-core-coap-bp-04
- draft-ietf-core-coap-bp-01
  - Address Marco Tiloca's review (many thanks!)

Table of contents

- Same structure as in -00



4.3. Payload-length option

- When encapsulated in a bundle, a CoAP message is represented as a definite-length CBOR byte string
  - Thus, the length of the CoAP message is unambiguously represented
  - The Payload-length option MUST NOT be included in a Single message

- 4.3.1. Payload-length option and OSCORE
  - Payload-length value may need to be updated
    - E.g., EDHOC + OSCORE request (RFC 9668)

5. Encapsulating bundle

- When a CoAP message needs to be sent in response to an incoming CoAP message, and to support one-to-many communication:
  - The Source Node ID SHOULD be the EID of the endpoint that produces the bundle encapsulating the CoAP message sent in response
  - The Source Node ID MAY be the null endpoint ID (anonymous source, RFC 9171)

6. CoAP parameter settings and related times

- CoAP group communication:
  - Minimum time between reuse of Token values for group requests: MIN_TOKEN_REUSE_TIME
  - By default, MIN_TOKEN_REUSE_TIME > 500 seconds.
  - Not suitable for many BP scenarios, needs to be increased, based on expected delay in the scenario
    - See Appendix A

9.3. Proxy operation and message aggregation (I/II)

- A proxy MAY aggregate CoAP messages destined for the same endpoint

NEW:

- Additional motivation: aggregate incoming messages while there is connectivity on the correspond. side of the proxy
- However, risk of contributing delay

```
+--------+                                     +---------------+
|Client 1|  <---+                      +---->  |Origin server X|
+--------+      |      +--------+      |       +---------------+
                +----> |        | <----+
+--------+             |        |              +---------------+
|Client 2|  <--------> | proxy  | <--------->  |Origin server Y|
+--------+             |        |              +---------------+
                +----> |        | <----+
+--------+      |      +--------+      |       +---------------+
|Client 3|  <---+                      +---->  |Origin server Z|
+--------+                                     +---------------+

  Earth               Mars orbiter                   Mars
```

9.3. Proxy operation and message aggregation (II/II)

- When a proxy aggregates CoAP messages, the proxy adds the Payload-length option to each Single message
  - The proxy MUST recompute the deltas of the outer CoAP options from each Single message accordingly
- When a proxy sends a Single message that was part of an Aggregate message, the proxy MUST remove its Payload-length option prior to its transmission.
  - The proxy MUST recompute the deltas of the outer CoAP options accordingly

11. Securing CoAP over BP (I/II)

- In the presence of CoAP proxies, BPSec cannot ensure the end-to-end protection of application-layer data.
  - OSCORE SHOULD be used to protect application-layer data between the two CoAP endpoints

NEW:

- BPSec is still useful to protect all fields of the carried CoAP message (including the Payload-length option: “Class U” for OSCORE) in each BP end-to-end path:
  - From the origin CoAP source until the first CoAP proxy,
  - between consecutive CoAP proxies, or
  - from the last CoAP proxy until the final CoAP destination

11. Securing CoAP over BP (II/II)

- BP freshness feature:
  - A bundle includes a creation timestamp and a lifetime field
  - Provides additional protection against replay attacks
- The Echo option in CoAP [RFC 9175] allows a server to verify the freshness of a request:
  - When the freshness of a request cannot be verified, the server rejects the request and includes the Echo option in the response
  - The client resends the original request with the Echo option value, also includes it in at least the next request
  - The round trip to check the freshness of the first request may incur significant delay penalty in BP environments.
  - In a scenario with proxies, the freshness of BP is limited to the scope of a BP path. The Echo option would be needed to verify the end-to-end freshness of a CoAP request

14. Security considerations

- Risk (Payload-length is “Class U” for OSCORE):
  - An attacker might infer some features of the communication based on the payload size of the messages

- Added:

NEW:

  - Exposing the individual sizes of the Single messages in an Aggregate message provides more information than the Aggregate message size
    - Assuming that the latter can be obtained by the attacker

Thanks!
Questions? Comments?

Carles Gomez

Anna Calveras

Universitat Politècnica de Catalunya

IETF 124 Montreal, CoRE WG, November 2025