# CoAP in space
draft-gomez-core-coap-space-01

**Carles Gomez**

Universitat Politècnica de Catalunya

**Sergio Aguilar**

Sateliot

IETF 120 Vancouver, CoRE WG, July 2024

# Updates (I/II)

- Extended scope: spatial environments characterized by long delays and intermittent communication opportunities
  - Deep space
  - Some LEO satellite-based scenarios
    - Discontinous coverage, store-and-forward support
    - 3GPP in Rel. 19 [TR23.700-29]
- Section 4. Caching
  - Max-Age needs to be set according to expected latency of the scenario
    - If it makes sense to consider the response fresh after Max-Age
  - Maximum possible Max-Age value = $2^{32}$ – 1 seconds (~136 years)
- Section 5. Observe:
  - If the time between the two last notifications received is > 128 seconds, the last one is also the latest sent by the server
  - In delay-tolerant environments, duration to be chosen > MAX_LATENCY of the scenario

# Updates (II/II)

- Section 7. CoAP group communication
  - MIN_TOKEN_REUSE_TIME = 500 seconds
  - In delay-tolerant environments, needs to be set according to the scenario (deep space: 1-2 orders of magnitude greater)
- Section 8. Security
  - Group OSCORE protocol used to secure CoAP group communication
  - Protection against replay attacks:
    - OSCORE uses by default an anti-replay sliding window, window size of 32
    - If greater window size needed (e.g., due to high latency), it needs to be known by both endpoints at security context establishment

# CoAP over Bundle Protocol (BP)

## draft-gomez-core-coap-bp-01

**Carles Gomez**

**Anna Calveras**

Universitat Politècnica de Catalunya

IETF 120 Vancouver, CoRE WG, July 2024

# 5. Encapsulating bundle

- CoAP message carried as the block-type-specific data field of the Bundle Payload Block (block type 1)

- Lifetime of the encapsulating bundle MUST be:
  - EXCHANGE_LIFETIME (for CoAP CON messages)
  - NON_LIFETIME (for CoAP NON messages)

- Destination EID of a response is the Source Node ID of the sender of the message triggering the response

- Aggregation of CoAP messages in a bundle
  - Perhaps a transport-independent solution needed?
  - Suggested (over UDP) in draft-bormann-coap-misc-27
    - – Payload-Length Option

# 9. URI scheme

- The URI scheme for CoAP over BP is "coap"
  - Recommended in [draft-ietf-core-transport-indication]
- Two new reserved domains in the .arpa name space:
  - .dtn.arpa
  - .ipn.arpa
- Full Domain Name Reservation Considerations in IANA considerations section (as per RFC 6761)
- Examples, URI of the discovery resource
  - endpoint ID dtn://JupiterSensor
    - coap://JupiterSensor.dtn.arpa/.well-known/core
  - endpoint ID ipn:81.2
    - coap://81.2.ipn.arpa/.well-known/core

# 10. Securing CoAP over BP

- CoAP base spec (RFC 7252) defines a binding to DTLS
- Also, OSCORE (RFC 8613)
  - Optional, end-to-end application-layer payload protection
  - Shared security context, may be based on pre-shared materials, avoiding initial handshake
    - Use of DTLS for CoAP over BP is NOT RECOMMENDED
- BPSec (RFC 9172) provides security services for BP
  - Integrity and/or confidentiality for one or more blocks of a bundle
- OSCORE protects, with confidentiality and integrity:
  - CoAP message payload
  - One CoAP message header field

# Message ID discussion summary

- CoAP Message ID size: 16 bits
- Message ID size proposed for DTN scenarios: 24 bits
  - Pros:
    - Avoid a limitation of the message rate
  - Cons:
    - 1 additional byte of header overhead
    - Increased memory requirements for endpoints to keep track of Message IDs used
      - Sender: to retire Message IDs
      - Receiver: duplicate detection