2021-05-26: Obsoleted by “6TiSCH Overhead Estimator”: https://docs.google.com/spreadsheets/d/1FjlGrgVu6ZSw2bt1KxAS9O5gtGXxBoGnqK3QeVFGx1Q/edit?usp=sharing

2021-05-26: Erratum: “Available UDP Payload” calculation for R -> JP path does not include 8 bytes of UDP overhead.

Key exchange over CoAP during network access in 6TiSCH

- Overhead counted from a dump of the latest 6TiSCH reference implementation (openwsn.org)
- IEEE 802.15.4 MTU is **127** bytes
  - 802.15.4 headers + L2 security
  - 6LoWPAN overhead
  - UDP overhead
  - CoAP overhead + CoAP options to go pass through a proxy at network access time, as specified in draft-ietf-6tisch-minimal-security-09
- Abbreviations:
  - **P**: Pledge, constrained node attempting to join the network
  - **JP**: Join Proxy, constrained node that is already part of the network that plays the role of a CoAP proxy for the pledge to reach the JRC
  - **JRC**: Join Registrar/Coordinator, cloud-based entity
  - **R**: DAG Root, root node in the 6TiSCH network

========================
AVAILABLE COAP PAYLOAD = AVAILABLE UDP PAYLOAD - COAP OVERHEAD
========================

	Max CoAP payload before fragmentation at L2 (bytes)	**Comment**
Uplink	**47**	min(P->JP, JP->R)
Downlink	**51 / 45**	min(R->JP, JP->P), devices from same/different vendor, see the assumption on topology below

P -> JP: 72 - 25 = 47
JP -> R: 67 - 17 = 50
R -> JP: 66/60 - 15 = 51 / 45 (same/different vendor)
JP -> P: 75 - 5 = 70
========================
AVAILABLE UDP PAYLOAD
========================

	UDP payload before fragmentation (bytes)	**Comment**
Uplink	**67**	min(P->JP, JP->R)
Downlink	**66 / 60**	min(R->JP, JP->P), devices from same/different vendor, see the assumption on topology below

Assumptions:

- Topology: (R) <--> (2) <---> (3) <---> (JP) <---> (P)
- 2 and 3 are 6TiSCH-based IPv6 routers

P -> JP: 127 - (23 + 24 + 8) = 72
JP -> R: 127 - (23 + L2SEC + 23 + 8) = 67
R -> JP: 127 - (23 + L2SEC + 22 + N * EUI64_SOURCE_ENCODING) = 66/60
JP -> P: 127 - (23 + 21 + 8) = 75

EUI64_SOURCE_ENCODING = 8 (As per RFC6554, assuming nodes (2) and (3) are from 2 *different* vendors)
EUI64_SOURCE_ENCODING = 5 (As per RFC6554, assuming nodes (2) and (3) are from the *same* vendor)
L2SEC = 6 (2 bytes for signaling + 4-byte authentication tag)
N = 2 (when R sends a packet to 4, it needs to include addresses of 2 and 3 in the packet)

========================
COAP OVERHEAD WITHOUT OSCORE AND NO TOKEN:
========================
P -> JP: (A + B + C + D + E) = 25
JP -> R: (A + D + E + F) = 17
R -> JP: (A + E + F) = 15
JP -> P: (A + E) = 5

A = 4 (COAP HEADER OVERHEAD W/O TOKEN)
B = 12 (COAP-URI-HOST 6TISCH.ARPA)
C = 6 (COAP-PROXY-SCHEME)
D = 2 (COAP-1B-URIPATH)
E = 1 (COAP-PAYLOAD-MARKER)
F = 10 (COAP-STATELESS-PROXY)