

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

draft-gomez-core-coap-bp-04

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)
 - -03 presented in IETF 122
 - CoRE and DTN WGs
- **Revision -04**
 - Address feedback
 - From IETF 122 on message aggregation
 - From a dedicated CoRE WG interim meeting (message aggregation)
 - Provide implementation status report

Table of contents

1. Introduction	3
2. Terminology	3
2.1. Requirements language	3
2.2. Background on previous specifications	3
2.3. New terms	4
3. Architecture	4
4. Messages	4
4.1. Messaging model	5
4.2. Single message format	6
4.3. Payload-length option	7
4.3.1. Payload-length option and OSCORE	7
5. Encapsulating bundle	8
6. CoAP parameter settings and related times	9
7. Observe	11
8. Block-wise transfers	12
8.1. Main CoAP block-wise transfer parameters	12
9. Proxying	13
9.1. Proxying scenarios	14
9.2. Proxying over BP	15
9.3. Proxy operation and message aggregation	15
10. URI Scheme	16
11. Securing CoAP over BP	16
12. IANA Considerations	18
12.1. Creation of two new reserved domains in the .arpa name space	18
12.1.1. Domain Name Reservation Considerations	18
12.2. ipn URI Scheme Well-known Service Number for CoAP	19
12.3. CoAP Option Numbers Registry	19
13. Implementation Status	19
13.1. Space CoAP	20
13.2. Other CoAP over BP implementations	22
14. Security Considerations	22
15. Acknowledgments	23
16. References	23
16.1. Normative References	23
16.2. Informative References	25
Appendix A. Reference CoAP parameter values for interplanetary communication	26
Appendix B. Message ID size, EXCHANGE_LIFETIME, and maximum CoAP message rate	30
Authors' Addresses	32

4.3. Payload-length option

- Indicates the CoAP message payload size
 - Allows message aggregation, **over various transports**
 - Aggregate message: a concatenation of Single messages that carry the Payload-length option
- Definition:

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

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

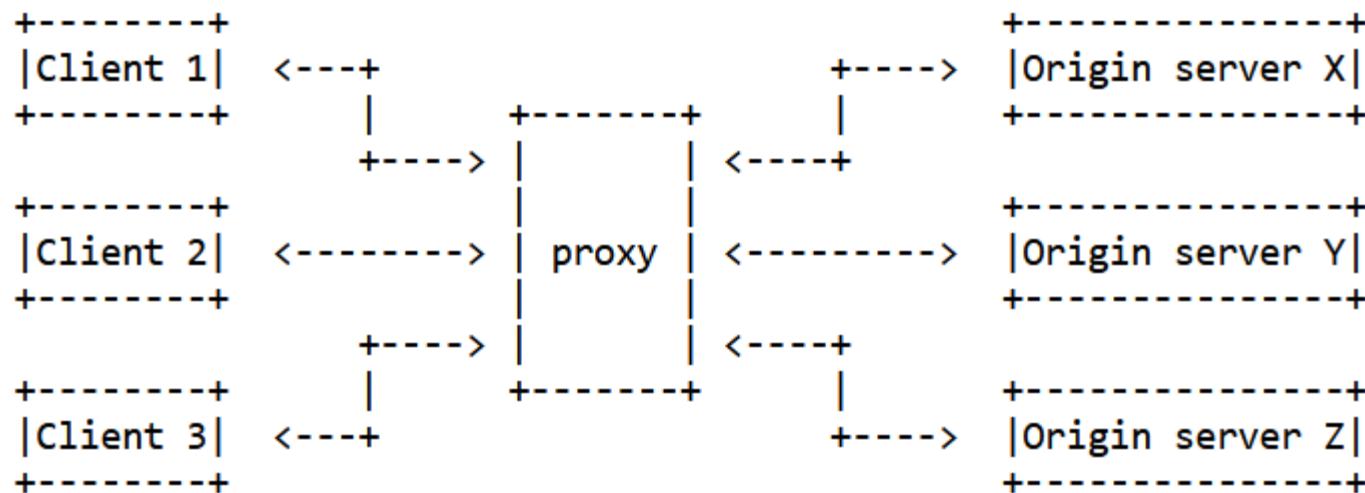
- First currently available suitable option number not actually low...

4.3.1. Payload-length option and OSCORE

- The Payload-length option is “Class U” (“Unprotected”) for OSCORE
- OSCORE-protected CoAP message and Payload-length:
 - 1st: the OSCORE message is created based on the CoAP message (RFC 8613)
 - 2nd: Payload-length option is inserted in the OSCORE message
 - The payload size indicated by Payload-length option is the OSCORE message payload size

9.3. Proxy operation and message aggregation

- A proxy that supports message aggregation disaggregates a received Aggregate message
 - Then proceeds “normally” (as in RFC 7252)
- A proxy MAY aggregate messages destined for the same endpoint



13. Implementation Status

- As recommended by RFC 7942
 - Section to be removed before eventual publication
- 13.1. Space CoAP
 - Organization: UPC (Main people: M. Karpov, A. Calveras)
 - Scenarios with and without proxies supported, based on aiocoap (CoAP) and μ D3TN (BP)
 - Compliant with draft-gomez-core-coap-bp-03
 - Level of maturity: research
 - Details and GitHub links in the draft
 - Demo video: <https://github.com/ENTEL-WNG/CoAPoverBP-proxy-version>
- 13.2. Other implementations
 - taraCoAP, BoAP
 - Prior to this I-D

14. Security considerations

- Payload-length is not protected by OSCORE
- Risk:
 - An attacker might infer some features of the communication based on the payload size of the messages
- Possible solutions:
 - Not using the Payload-length option, but then message aggregation not possible
 - Lower-layer security (e.g., BPSec) if available

WG adoption?

Thanks!

Questions? Comments?

Carles Gomez

Anna Calveras

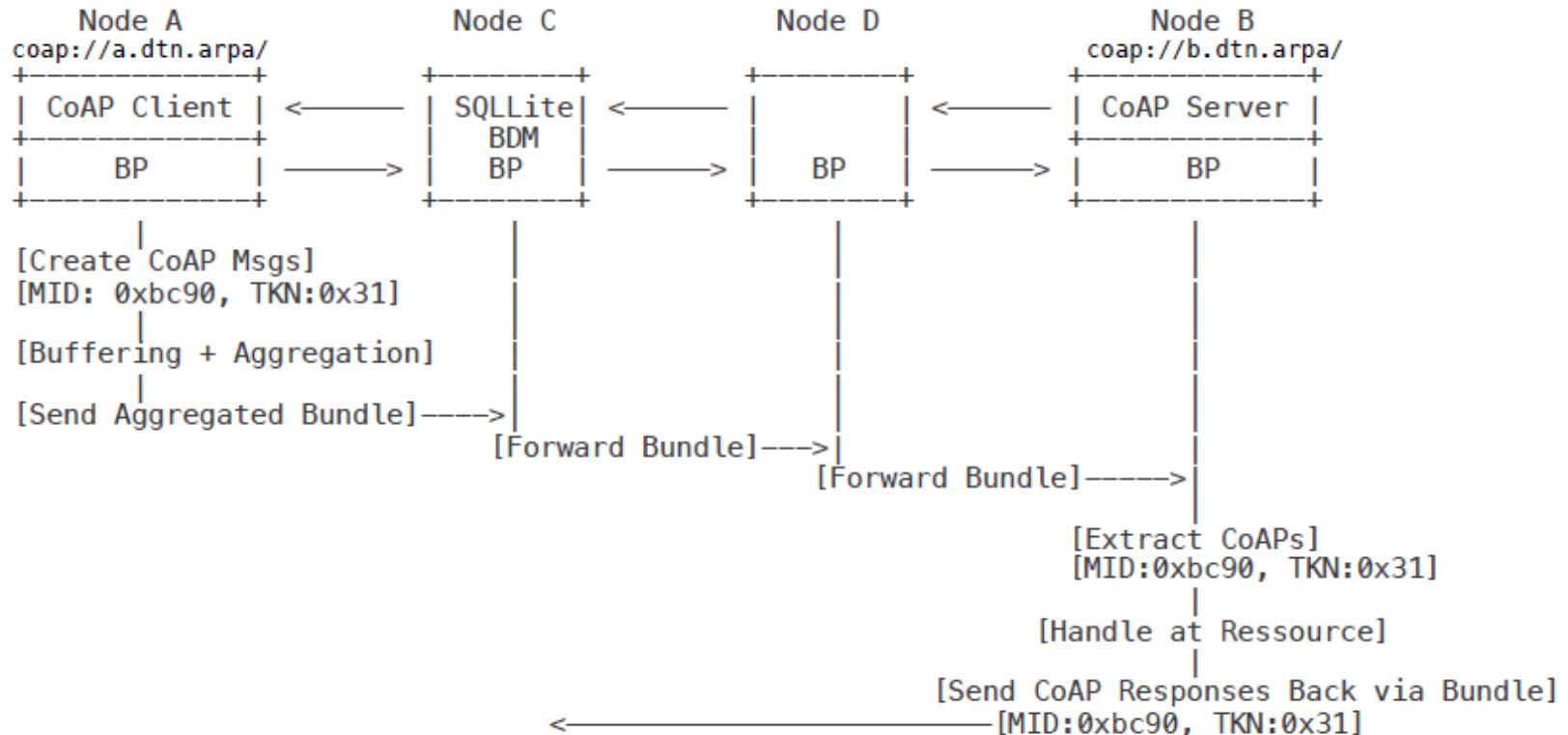
Universitat Politècnica de Catalunya

Annex: implementation main characteristics

- Two proxy and one non-proxy scenario
- CoAP Client and Server with multiple Bundle Nodes
- Contact plan scheduling for delay simulation
- Persistent storage on bundle node with bundle decision maker
- PUT, POST, GET, DELETE methods
- NON and CON message handling
- Hop-based token and MID matching. Round Trip is Piggybacked for simplicity
- Extended Message ID to 24 bit and Timers according to IETF draft
- Message aggregation and payload_length option field
- Space CoAP Lua dissector
- CoAP over Bundle URI Scheme

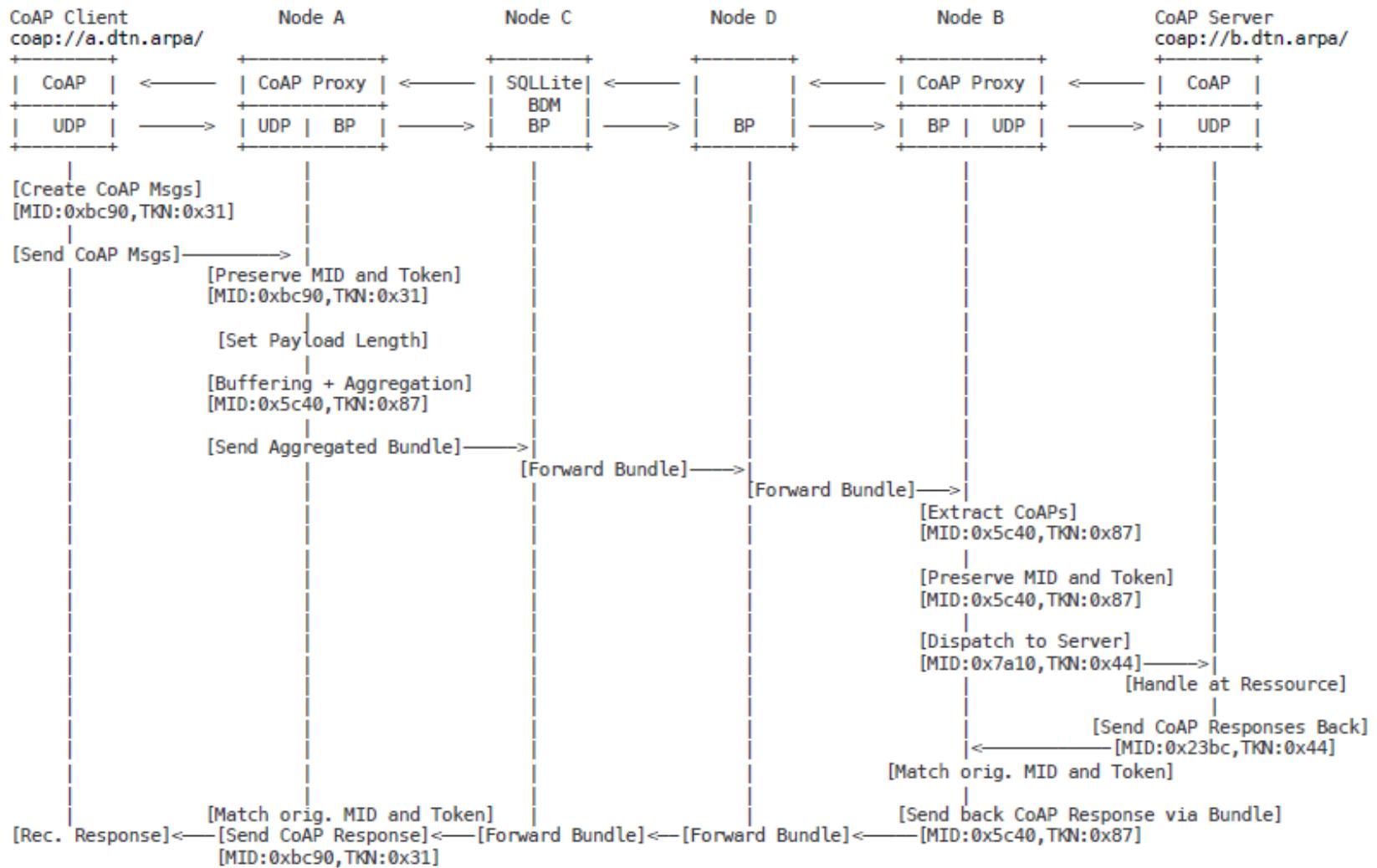
Non-Proxy Scenario

Topology and Logic



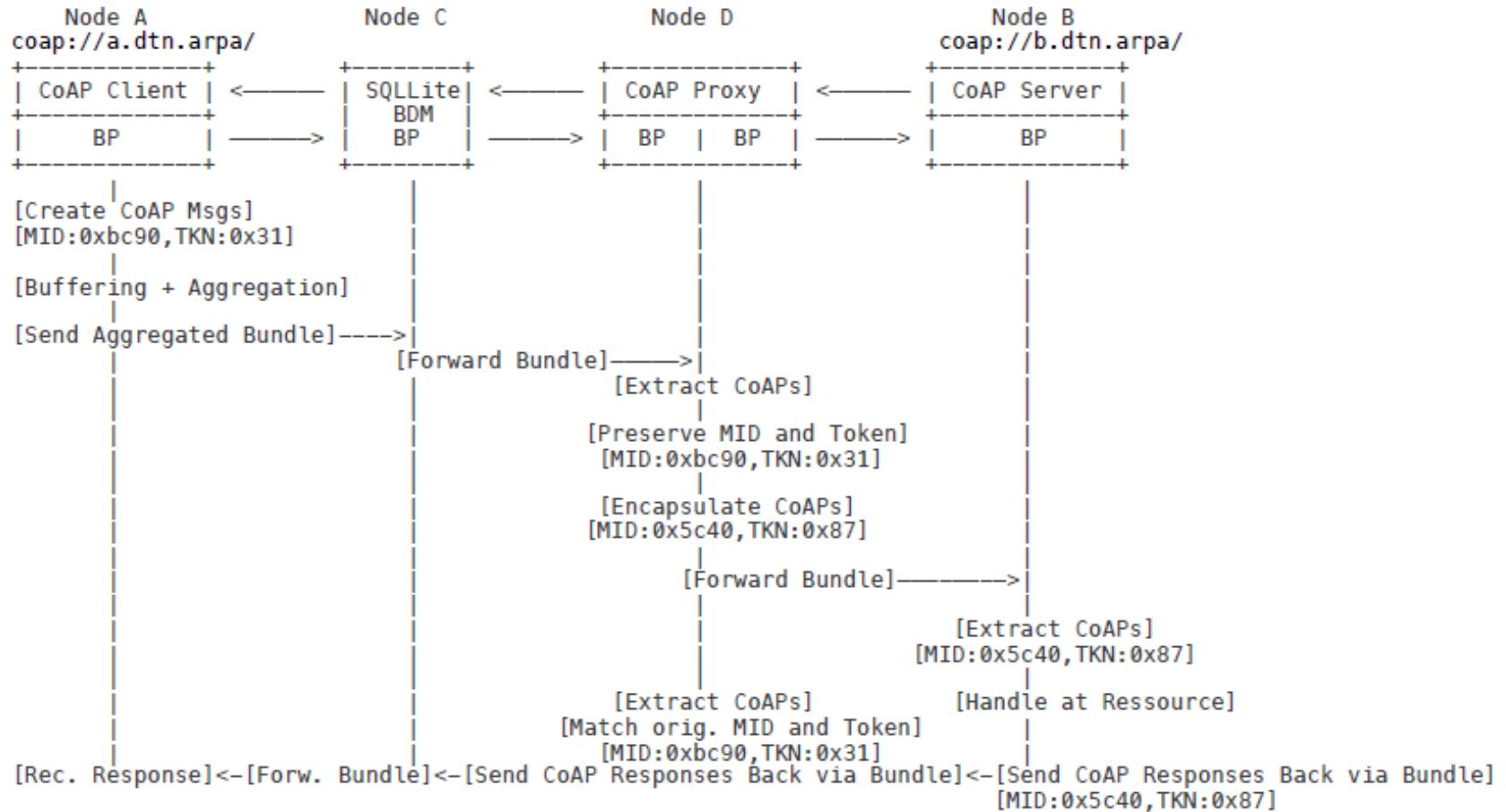
CoAP over UDP/BP Proxy Scenario

Topology and Logic



CoAP over BP Proxy Scenario

Topology and Logic



Main modifications

Changes to aiocoap library according to draft-gomez-core-coap-bp-03

- CoAP Message Format defined in RFC 7252

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Ver T TKL Code		Message ID	
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Token (if any, TKL bytes) ...			
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
Options (if any) ...			
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+
1 1 1 1 1 1 1 Payload (if any) ...			
+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+	+-----+-----+-----+-----+

- CoAP Message Format as defined in the draft

Main modifications

Changes to aiocoap library according to draft-gomez-core-coap-bp-03

Area	Original CoAP Behavior	Modification	Reason / Benefit
Message ID Range	16-bit MID (0..65535)	24-bit MID (0..16777215)	Support more concurrent exchanges, fewer MID collisions in challenged environments.
Message Header Parsing	2 bytes for MID	Adjusted to accommodate 24-bit MID, MID parsing changed to 3 bytes	Maintain compatibility with the expanded MID range.
Option: Payload Length	Not present	New option PAYLOAD_LENGTH = 65000	Supports message aggregation. (Used to determine, where the next CoAP message starts in an aggregated bundle).
Transport Parameters: ACK_TIMEOUT	2 seconds	2642 seconds	Finetuned retransmission timing for challenged environments.
Transport Parameters: ACK_RANDOM_FACTOR	1.5	1.0	Set to minimum.
Transport Parameters: MAX_RETRANSMIT	4 retries	0 retries	Disable retransmissions entirely for very lossy links where repeated transmission is impractical.
Transport Parameters: MAX_LATENCY	100 seconds	10000 seconds	Supports long network delays in challenged environments.
Wire Inspection	Standard CoAP Wireshark dissector	Custom Lua dissector for Space CoAP (24-bit MID support and payload_length option)	Enables packet inspection and validation of modified Space CoAP traffic.

Video Scenario Details

- Creation of new resource as a single sent CoAP message over Bundle
- PUT method used to send 4 temperatures to a temperature resource
 - The 4 messages are aggregated and transmitted in a single bundle from node A to node B
 - Node A is responsible for aggregation and Node B for disaggregation and dispatch to CoAP server
 - Both Nodes A and B are responsible for token matching on their ends and with each other
- Persistent storage on Node C with sqlite and bundle decision maker

Config Socket	Destination	Schedule (Offset, Period, Lifetime)	Reaches	Connect via TCPCLv3
ud3tn-a.aap2.socket	dtn://c.dtn/	1s offset, 600s period, 100000s lifetime	dtn://b.dtn/, dtn://d.dtn/	localhost:4226
ud3tn-c.aap2.socket	dtn://d.dtn/	30s offset, 600s period, 100000s lifetime	dtn://b.dtn/	localhost:4227
ud3tn-d.aap2.socket	dtn://c.dtn/	1s offset, 600s period, 100000s lifetime	dtn://a.dtn/	localhost:4226
ud3tn-d.aap2.socket	dtn://b.dtn/	1s offset, 600s period, 100000s lifetime	(explicit dtn://b.dtn/rec)	localhost:4225
ud3tn-c.aap2.socket	dtn://a.dtn/	1s offset, 600s period, 100000s lifetime	(explicit dtn://a.dtn/rec)	localhost:4224
ud3tn-b.aap2.socket	dtn://d.dtn/	1s offset, 600s period, 100000s lifetime	dtn://c.dtn/, dtn://a.dtn/	localhost:4227

