Constrained RESTful Environments WG (core)

Chairs:

Jaime Jiménez <jaime.jimenez@ericsson.com>

Carsten Bormann <cabo@tzi.org>

Mailing List:

core@ietf.org

Jabber:

core@jabber.ietf.org

- **We assume people have read the drafts**

- **Meetings serve to advance difficult issues by making good use of face-to-face communications**

- **Note Well: Be aware of the IPR principles, according to RFC 3979 and its updates**

- Blue sheets
- Scribe(s): http://tools.ietf.org/wg/core/minutes

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session
The IESG, or any member thereof on behalf of the IESG
Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
Any IETF working group or portion thereof
Any Birds of a Feather (BOF) session
The IAB or any member thereof on behalf of the IAB
The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda Bashing

All times are in time-warped KST

Wednesday (90 min)

- 13:30–13:40 Intro, WG status
- 13:40–14:10 CoAP over reliable (BR)
- 14:10–14:20 Protocol negotiation (BS – remote)
- 14:20–14:32 Resource Directory (chairs)
- 14:32–14:52 Object Security (FP)
- 14:52–15:00 dynlink (CG)
- 15:00–15:00 interfaces (CG)

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- **13:30–13:30 Intro**
- **13:30–13:40 Links-JSON (CB)**
- **13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)**
- **14:00–14:10 Object Security for multicast (FP)**
- **14:10–14:20 Delegated Observe (ZC)**
- **14:20–14:30 CoAP over WebRTC DC (CG)**

- **14:30–15:00 Flextime**

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

Milestones (from WG charter page)

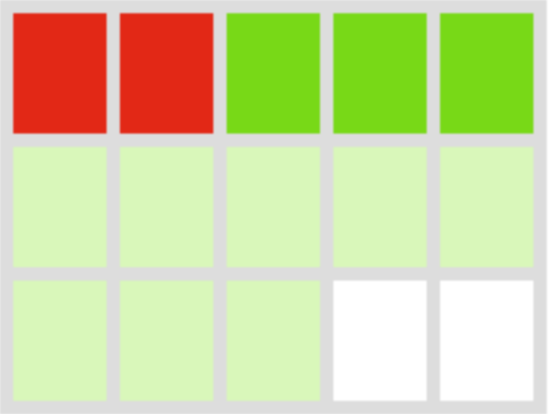
http://datatracker.ietf.org/wg/core/charter/

Mar 2017	CoRE Interfaces submitted to IESG	draft-ietf-core-interfaces
Dec 2016	Management over CoAP submitted to IESG for PS	draft-vanderstok-core-comi , draft-veillette-core-cool
Dec 2016	CBOR Encoding of Data Modeled with YANG submitted to IESG for PS	draft-ietf-core-yang-cbor
Oct 2016	CoAP over TCP, TLS, and WebSockets submitted to IESG for PS	draft-bormann-core-coap-tcp
Sep 2016	CoRE Resource Directory submitted to IESG for PS	draft-ietf-core-resource-directory
Aug 2016	WG adoption for Management over CoAP	draft-vanderstok-core-comi draft-veillette-core-cool
Aug 2016	Media Types for Sensor Measurement Lists (SenML) submitted to IESG for PS	draft-ietf-core-senml
Done	**Patch and Fetch Methods for CoAP submitted to IESG for PS**	**draft-ietf-core-etch**
Aug 2016	Representing CoRE Link Collections in JSON submitted to IESG	draft-ietf-core-links-json
Done	**Best Practices for HTTP-CoAP Mapping Implementation submitted to IESG**	**draft-ietf-core-http-mapping**
Done	**Blockwise transfers in CoAP submitted to IESG**	**draft-ietf-core-block — RFC 7959**

draft-ietf-core-block → RFC 7959 ✓

Published 2016-08-27

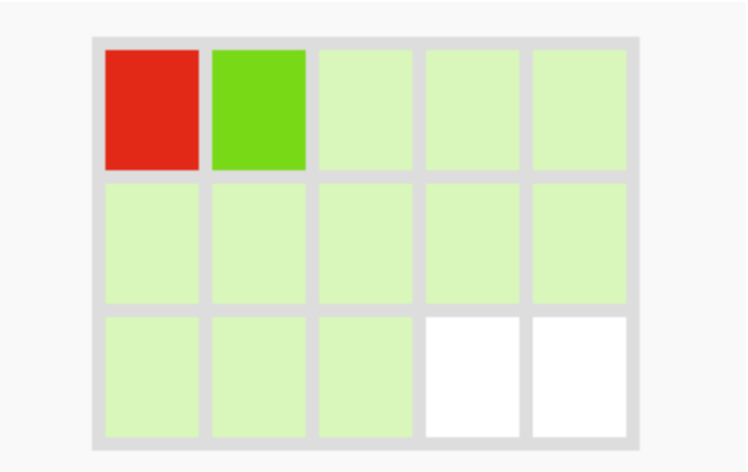
draft-ietf-core-http-mapping



- (Intended status: Informational)
- Most recent: –16 (reacts to apps-dir review)
- Brownian motion
- New appendix A with code for media type mapping
- Open DISCUSSes:
  - Should this be anything else but informational?
  - Not enough security admonition

- Next steps after publishing this:
  - How does the HTTP mapping for FETCH/PATCH look like?
  - Maybe again gather some experience before writing this up.

draft-ietf-core-etch



- (Intended status: Standards-Track)
- Recent –04 should answer all outstanding IESG comments
  - waiting for Alissa Cooper’s DISCUSS to clear
- More explicit rules about choice between PATCH and iPATCH
- More text about media type choices for FETCH
- More explicit text about error handling for FETCH
- Better Security Considerations

- Next steps: get this into the implementations!

All times are in time-warped KST

Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

coap-tcp-tls @ IETF 97

Brian Raymor

Since IETF 96

- **coap-tcp-tls-04** – addressed all issues discussed at IETF 96
  - Added mandatory exchange of Capabilities and Settings messages after connecting
  - Added support for coaps+tcp port 5684 and more details on Application-Layer Protocol Negotiation (ALPN)
  - Added guidance on CoAP Signaling Ping-Pong versus WebSocket Ping-Pong
  - Updated references and requirements for TLS security considerations
- **coap-tcp-tls-05**
  - Added Appendix: Updates to RFC7641 Observing Resources in the Constrained Application Protocol (CoAP)

WGLC (in progress)

https://github.com/core-wg/coap-tcp-tls/issues/
https://github.com/core-wg/coap-tcp-tls/pull/67 (editorial)

Revisiting Security Considerations: Making TLS a MUST

https://github.com/core-wg/coap-tcp-tls/issues/11

Guidance

Security Challenges For the Internet Of Things (2011):

It is essential that IoT protocol suites specify a ***mandatory to implement but optional to use security solution****. This will ensure security is available in all implementations, but configurable to use when not necessary (e.g., in closed environment).*

IAB Statement on Internet Confidentiality (2014):

Newly designed protocols should prefer encryption to cleartext operation.

All times are in time-warped KST

Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

CoAP Protocol Negotiation

draft-silverajan-core-coap-protocol-negotiation

Bill Silverajan TUT

Main change from -03

- Previous drafts used `.well-known/core` to expose CoAP origin server's available alternative transports
- Discussions in Berlin led towards dropping `.well-known/core` and using CoRE Resource Directory and CoRE Link Format

Current changes from -03:

Removal: link attribute & relation type

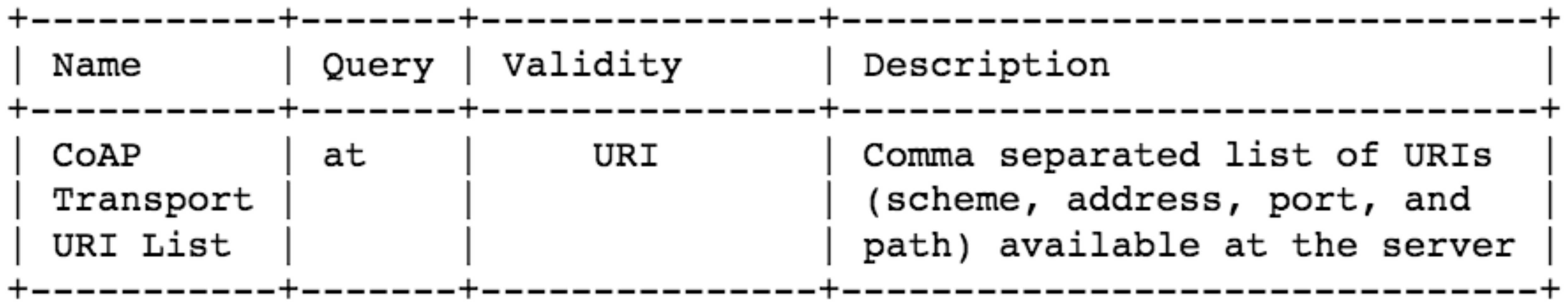
- ’tt’ link attribute and ’altloc’ link relation type discontinued (see below in red)

```
REQ: GET /.well-known/core

RES: 2.05 Content
</sensors>;ct=40;title="Sensor Index", tt="tcp ws sms",
</sensors/temp>;rt="temperature-c";if="sensor",
</sensors/light>;rt="light-lux";if="sensor",
<coap+tcp://server.example.com/>;rel="altloc",
<coaps+tcp://server.example.net/>;rel="altloc",
<coap+ws://server.example.com/ws-endpoint>; rel="altloc",
<coap+sms://001234567>;rel="altloc”
```

Changes in -04:
New optional 'at' RD parameter

- Extend the Resource Directory's Registration and Update Interfaces



Name	Query	Validity	Description
CoAP Transport URI List	at	URI	Comma separated list of URIs (scheme, address, port, and path) available at the server

- Interaction: EP -> RD

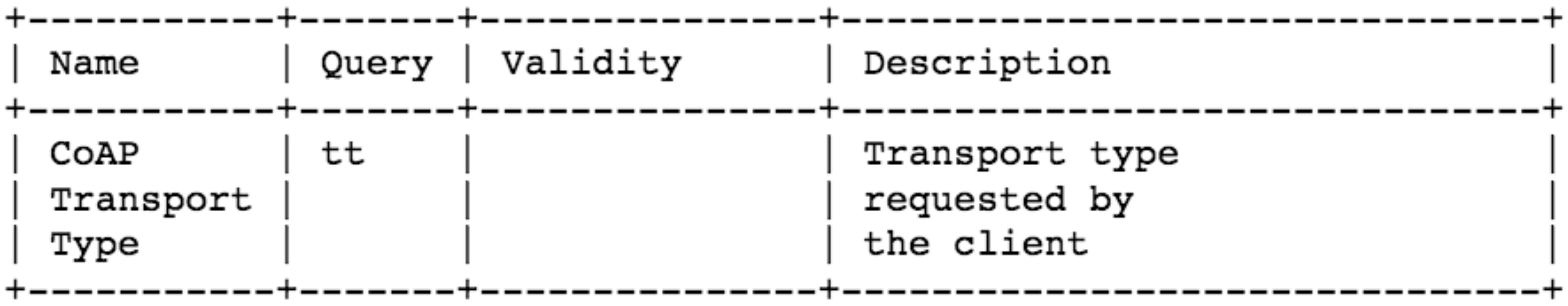
```
Req: POST coap://rd.example.com/rd?ep=node1&
         at=coap+tcp://server.example.com
Content-Format: 40
Payload:
</sensors/temp>;ct=41;rt="temperature-f"; if="sensor",
</sensors/door>;ct=41;rt="door";if="sensor"


Res: 2.01 Created
Location: /rd/4521
```

Changes in -04:

New optional ‘tt’ RD parameter

- Extend the Resource Directory’s Lookup Interface



Name	Query	Validity	Description
CoAP Transport Type	tt		Transport type requested by the client

- Interaction: Client -> RD

```
Req: GET /rd-lookup/ep?ep=node5&tt=*

Res: 2.05 Content
<coap+tcp://[FDFD::123]:61616>;ep="node5",
<coap+ws://[FDFD::123]:61616>;ep="node5"
```

Advantages

- RD provides well-defined interfaces with easy way to extend functionality
- Consistent API: Registrations and Updates managed by origin servers based on lifetime values
- Group function set provides new possibilities
- Support for commissioning tools (via ‘con’)
- RD also supports HTTP
- DNS SD and DNS-based Service Discovery may be possible

Drawbacks

- Alternative transport lifetime currently bound to registration lifetime (unless we introduce a new RD parameter per transport, which is challenging)
- A simple means for clients to signal a server to temporarily enable an alternative transport (for energy-constrained origin servers) is missing

All times are in time-warped KST

Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

Questions and todos on RD

- Re-Registration keeps parameters unchanged (what does this mean?)
- “read” interface vs. lookup interface
- Fix merge-patch examples; examples with multiple endpoints, all using the same address
- "This can be done, for example by responding to wild card lookups only over DTLS or TLS or TCP."
- Guidelines for IANA designated expert
- More minor technical, major editorial, …

RD usage today?

- LWM2M: only the registration interface
- Need more feedback on lookup interface etc.
- Need feedback on DNS-SD adaptation
  - e.g., character sets, “href” vs. “path”, …

All times are in time-warped KST

Wednesday (90 min)

- 13:30–13:40 Intro, WG status
- 13:40–14:10 CoAP over reliable (BR)
- 14:10–14:20 Protocol negotiation (BS – remote)
- 14:20–14:32 Resource Directory (chairs)
- 14:32–14:52 Object Security (FP)
- 14:52–15:00 dynlink (CG)
- 15:00–15:00 interfaces (CG)

Object Security of CoAP (OSCOAP)

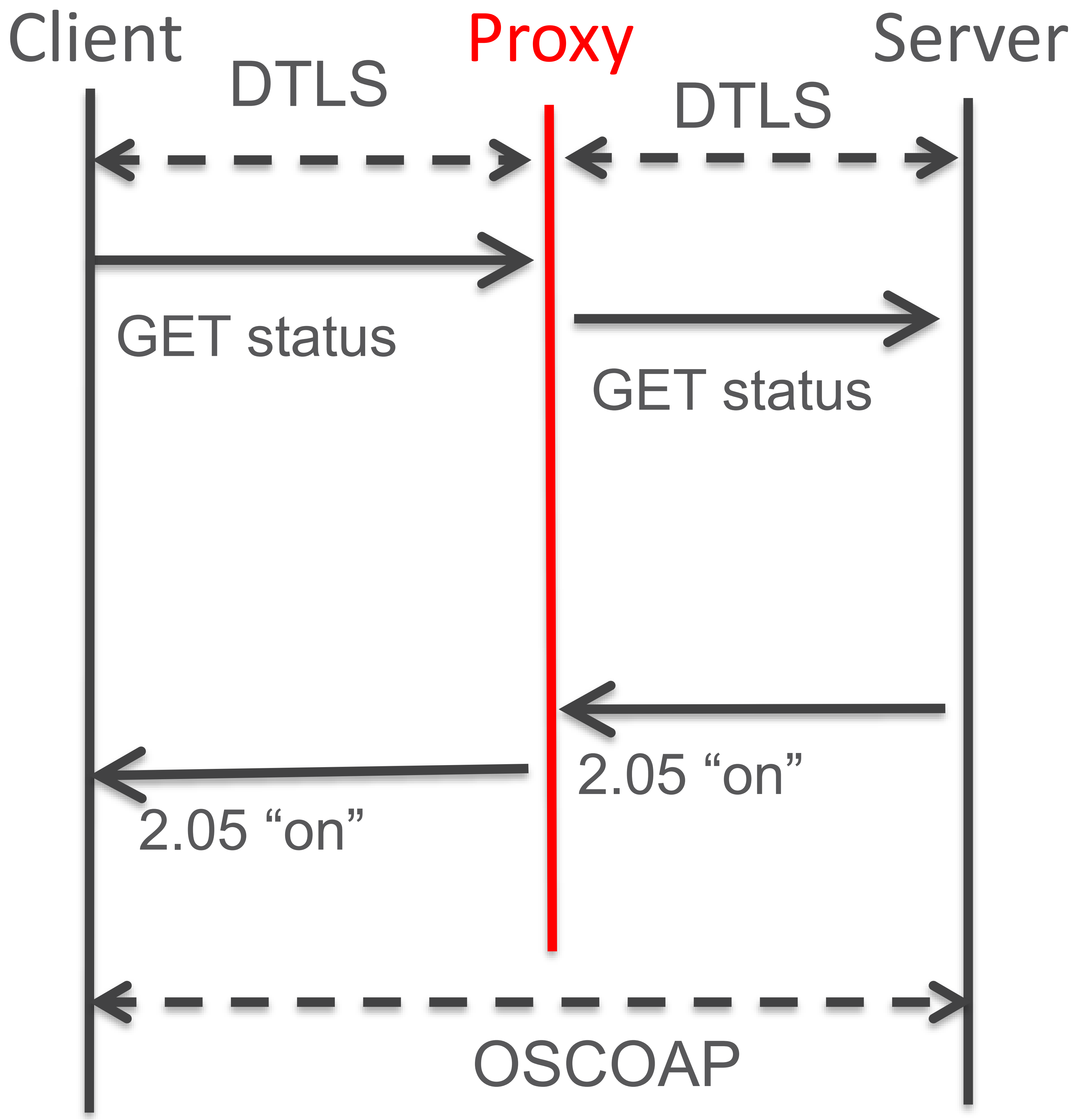
draft-ietf-core-object-security-00

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

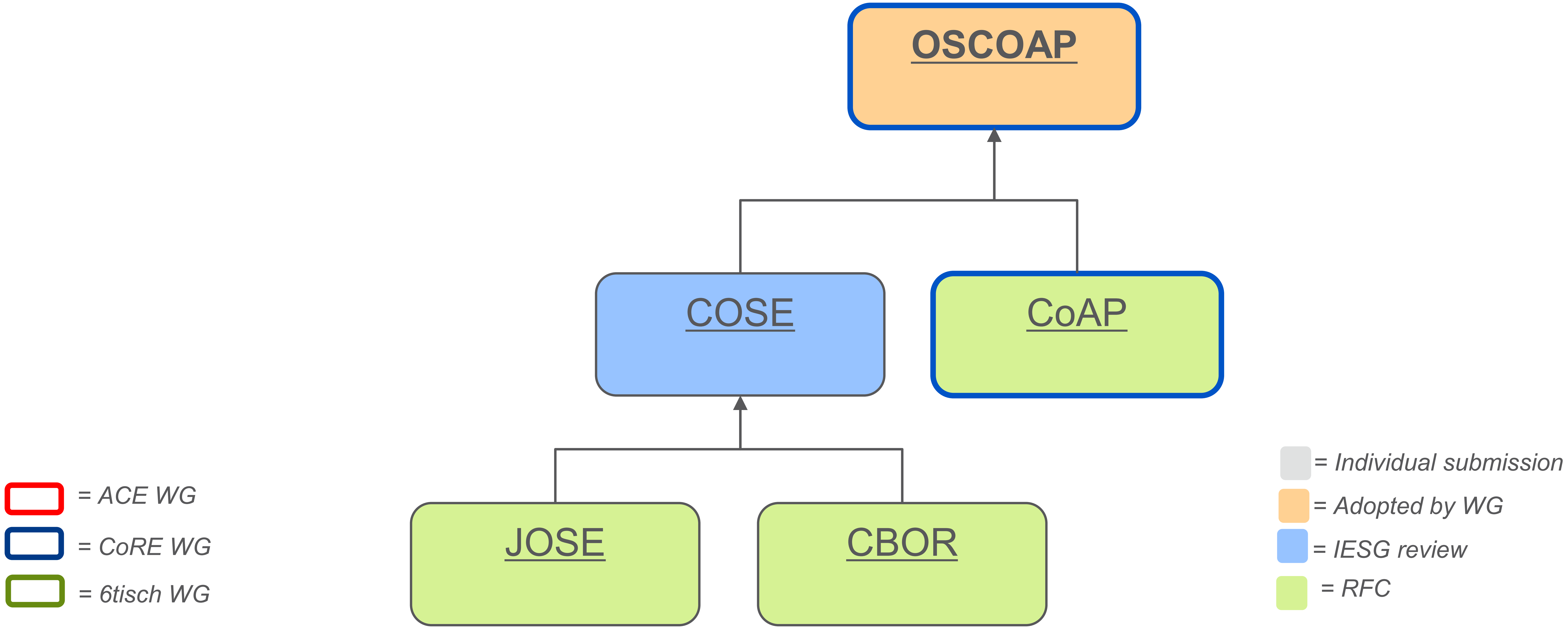
IETF 97, CORE WG, Seoul, Nov 16, 2016

OSCOAP

- OSCOAP defines a method for in-layer security of CoAP message exchanges using the COSE format.
- OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations
- Independent of how CoAP is transported (UDP, TCP, Bluetooth, 802.15.4, foo…)
- Requirements: draft-hartke-core-e2e-security-reqs



Related Work



OSCOAP

COSE

CoAP

JOSE

CBOR

= ACE WG

= CoRE WG

= 6tisch WG

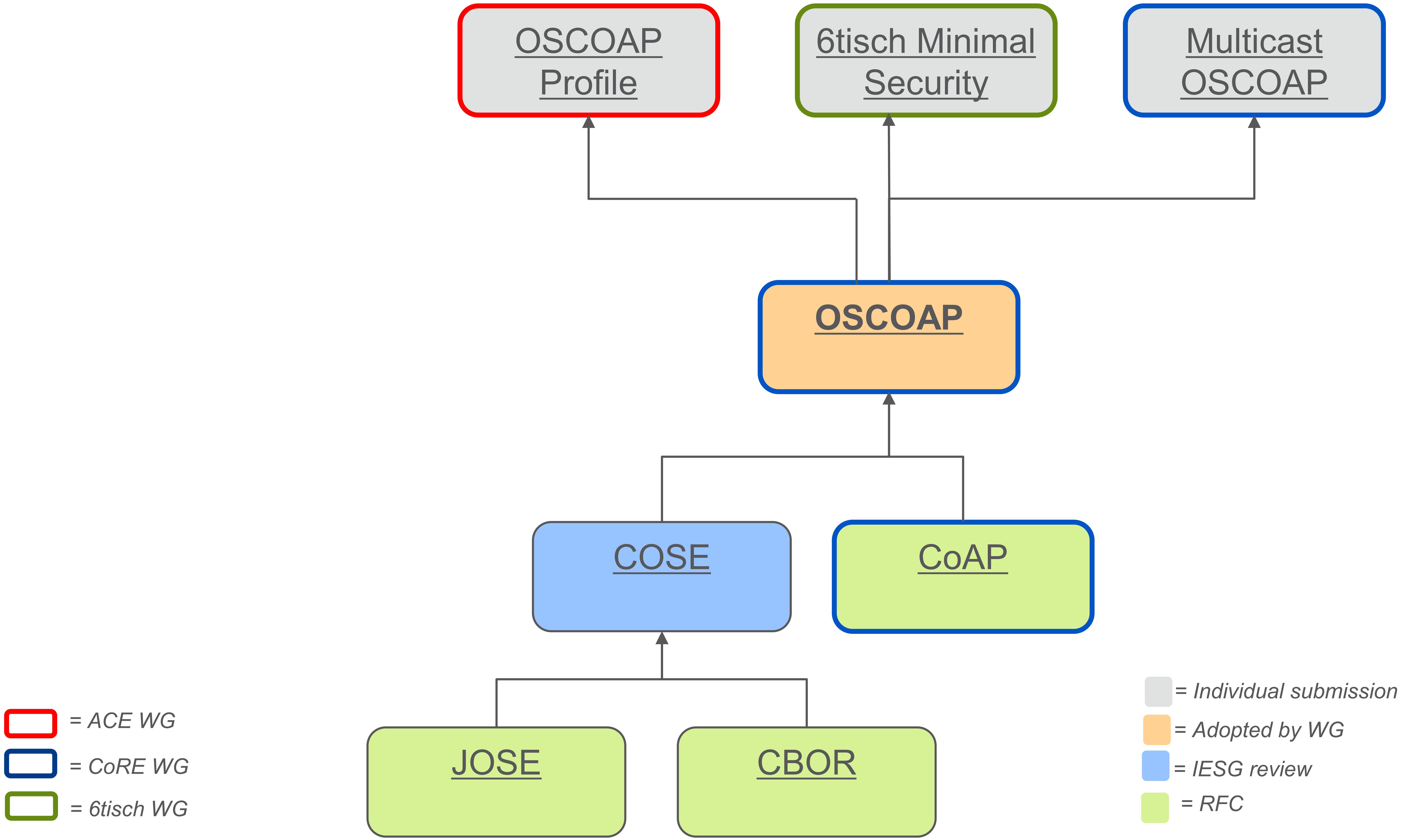
= Individual submission

= Adopted by WG

= IESG review

= RFC

Related Work



OSCOAP Profile

6tisch Minimal Security

Multicast OSCOAP

OSCOAP

COSE

CoAP

JOSE

CBOR

□ = ACE WG

□ = CoRE WG

□ = 6tisch WG

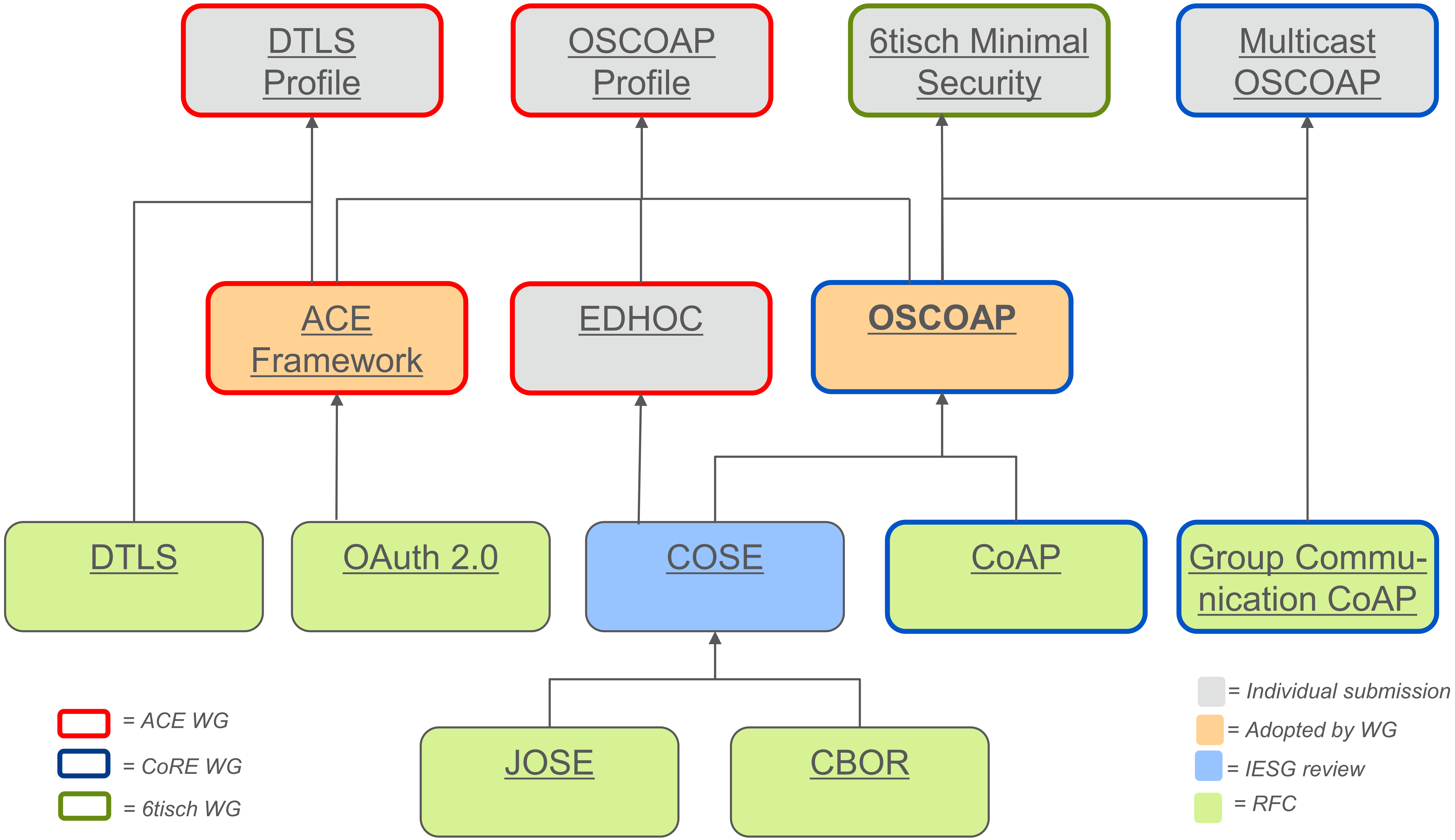
■ = Individual submission

■ = Adopted by WG

■ = IESG review

■ = RFC

Related Work



DTLS Profile

OSCOAP Profile

6tisch Minimal Security

Multicast OSCOAP

ACE Framework

EDHOC

OSCOAP

DTLS

OAuth 2.0

COSE

CoAP

Group Communication CoAP

JOSE

CBOR

▭ = *ACE WG*

▭ = *CoRE WG*

▭ = *6tisch WG*

⬜ = *Individual submission*

🟧 = *Adopted by WG*

🟦 = *IESG review*

🟩 = *RFC*

Draft Status

- Stable: https://github.com/EricssonResearch/OSCOAP
- Some changes (next slide)

- Used in secure join process in 6tisch (draft-vucinic-6tisch-minimal-security)
- Used in OSCOAP profile for ACE (draft-seitz-ace-oscoap-profile)
- Implementation: JAVA (link), C (link) released open source, work in progress

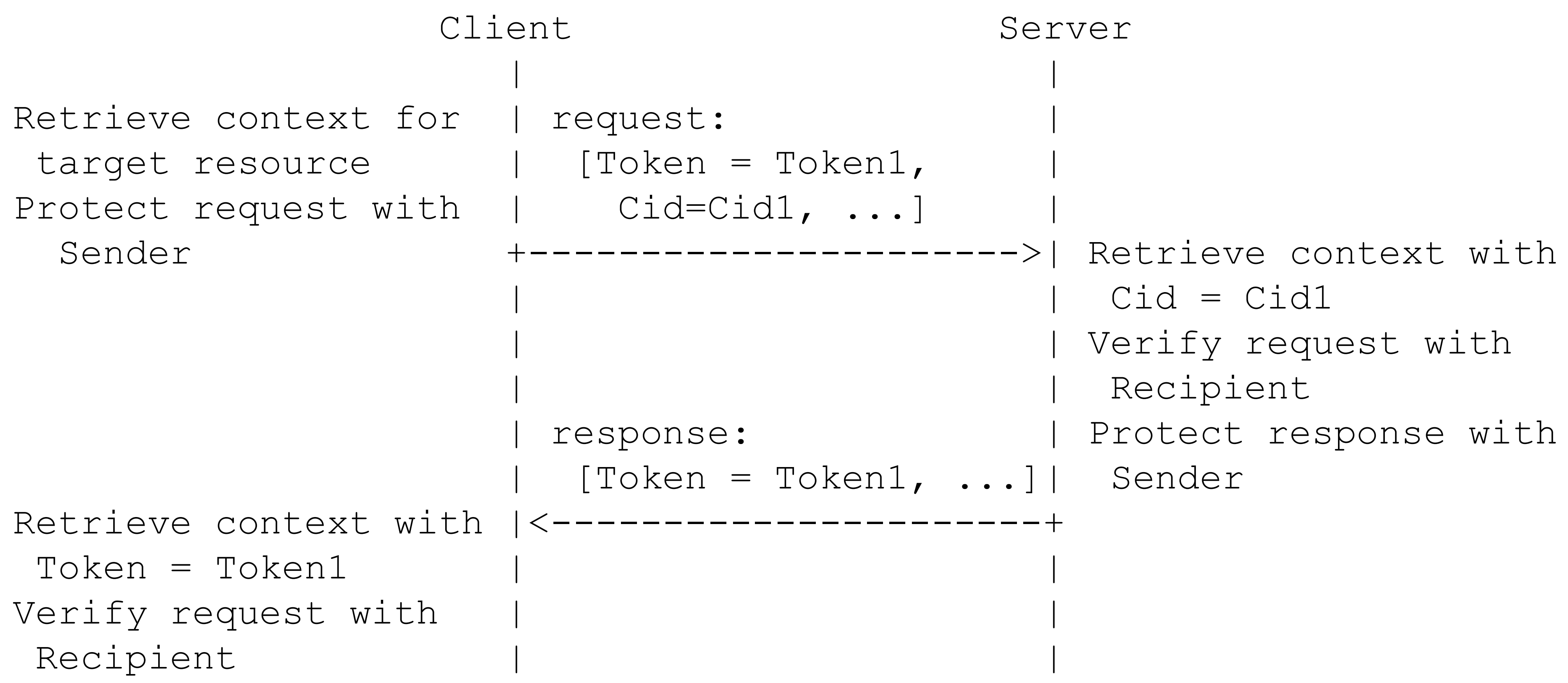
What’s new
(draft-ietf-core-object-security-00)

- Context Definition
- Context Derivation → Context Establishment
  - Derivation of Keys, IVs, initialization of Sequence Numbers
  - Context Identifier and Sender/Recipient ID
- Cid is 64 bits pseudo-random → globally unique
  - Sender/Recipient ID are locally unique
- Optionally, Sender ID is sent in the message
  - New COSE Header parameter, ”sid”

Context Definition

- The security context is the set of information elements necessary to carry out the cryptographic operations in OSCOAP.

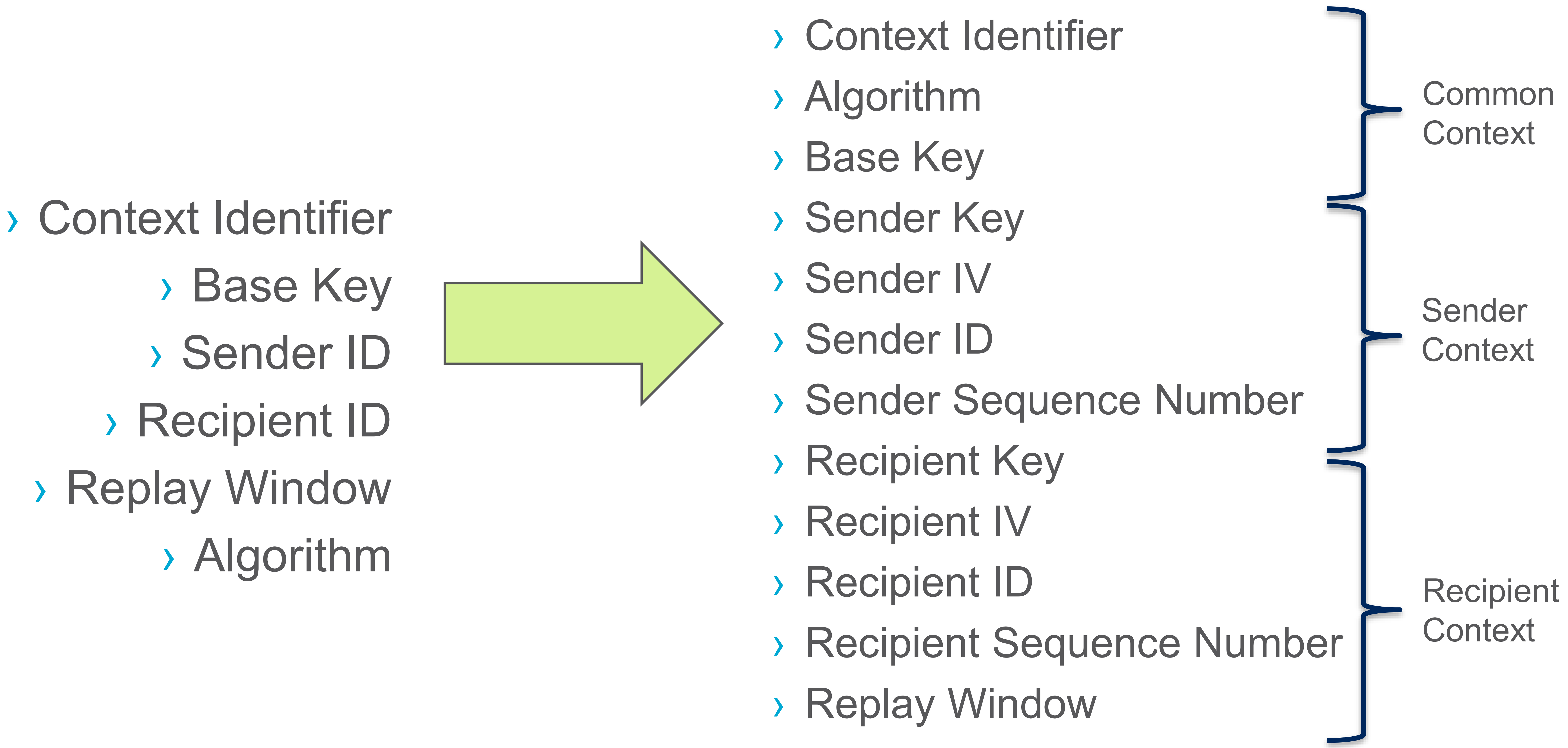
- Security Context includes:
- Common Context:
  - Context Identifier
  - Algorithm
  - Base Key
- Sender Context:
  - **Sender Identifier:** Identifier of the endpoint itself
  - Sender Key, IV
  - Sender Seq Num
- Recipient Context:
  - **Recipient Identifier:** identifier of the other endpoint
  - Recipient Key, IV
  - Recipient Seq Num
  - Replay Window



```
                   Client                  Server
                      |                       |
Retrieve context for  | request:              |
 target resource      |  [Token = Token1,     |
Protect request with  |    Cid=Cid1, ...]     |
  Sender              +---------------------->| Retrieve context with
                      |                       |  Cid = Cid1
                      |                       | Verify request with
                      |                       |  Recipient
                      | response:             | Protect response with
                      |  [Token = Token1, ...]|  Sender
Retrieve context with |<----------------------+
 Token = Token1       |                       |
Verify request with   |                       |
 Recipient            |                       |
```

Figure 3: Retrieval and use of the Security Context

Context Establishment



- Context Identifier
- Base Key
- Sender ID
- Recipient ID
- Replay Window
- Algorithm

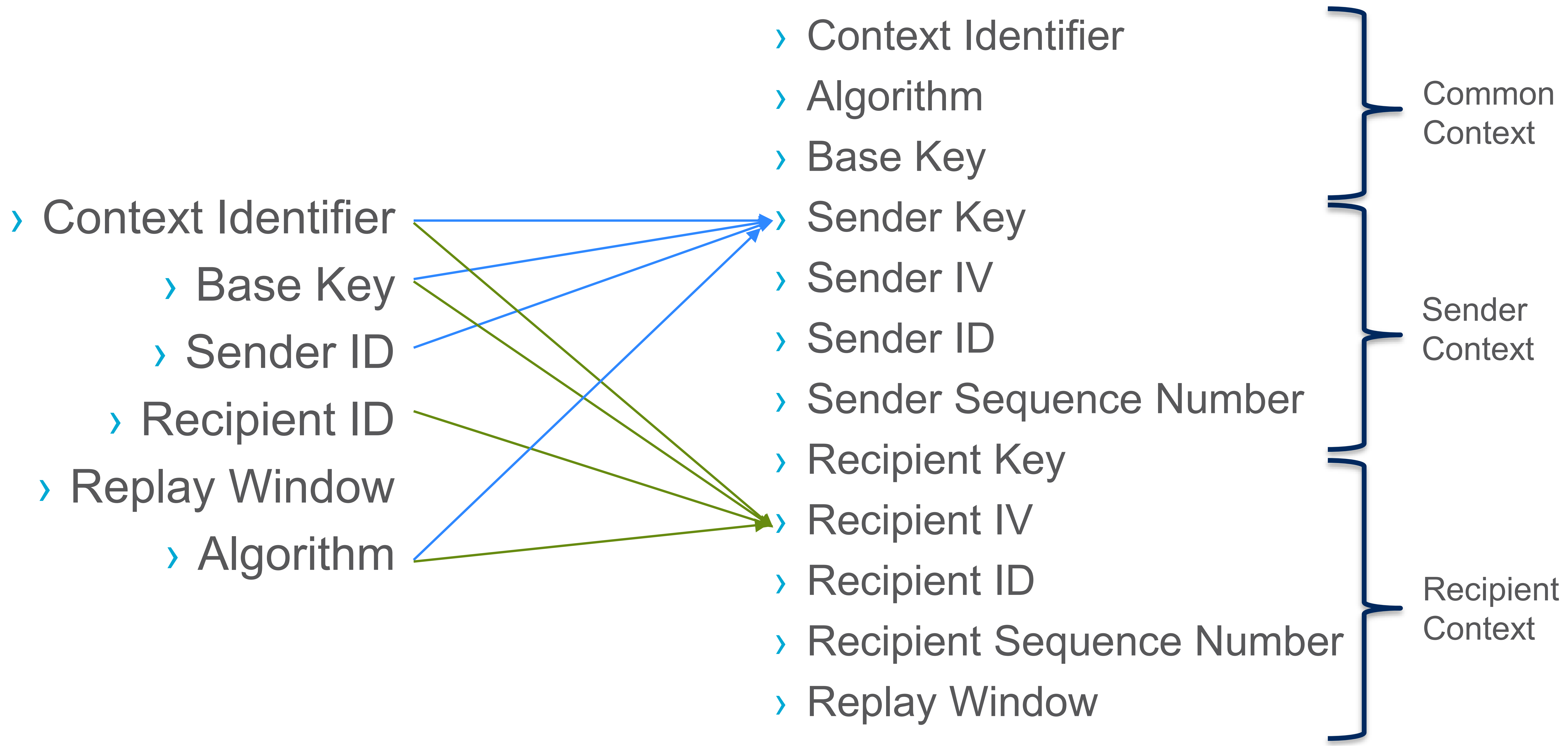
- Context Identifier
- Algorithm
- Base Key
- Sender Key
- Sender IV
- Sender ID
- Sender Sequence Number
- Recipient Key
- Recipient IV
- Recipient ID
- Recipient Sequence Number
- Replay Window

Common Context

Sender Context

Recipient Context

Context Establishment

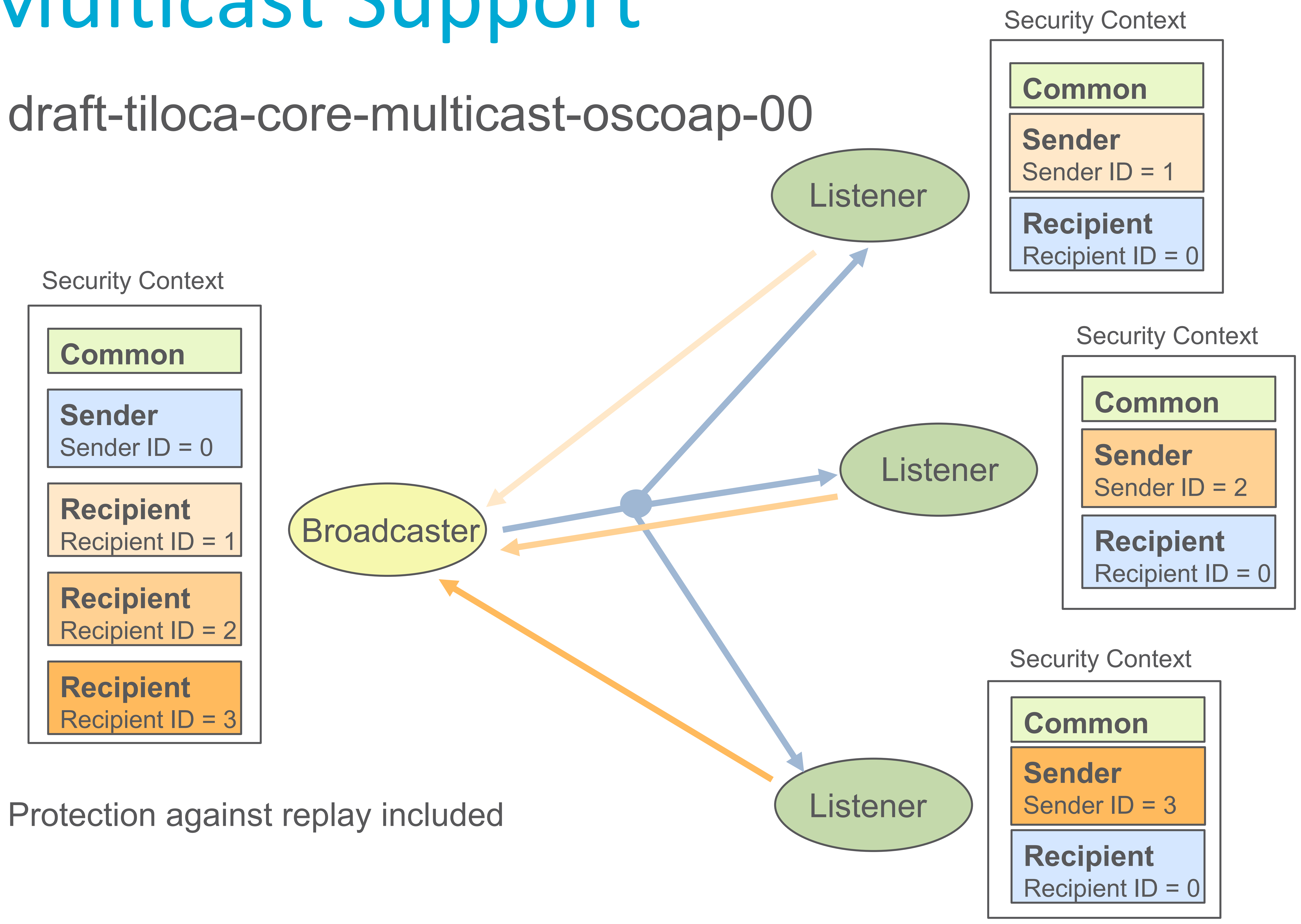


- Context Identifier
- Base Key
- Sender ID
- Recipient ID
- Replay Window
- Algorithm

- Context Identifier
- Algorithm
- Base Key
- Sender Key
- Sender IV
- Sender ID
- Sender Sequence Number
- Recipient Key
- Recipient IV
- Recipient ID
- Recipient Sequence Number
- Replay Window

Multicast Support

› draft-tiloca-core-multicast-oscoap-00



Security Context

Common

Sender
Sender ID = 0

Recipient
Recipient ID = 1

Recipient
Recipient ID = 2

Recipient
Recipient ID = 3

Broadcaster

Listener

Security Context

Common

Sender
Sender ID = 1

Recipient
Recipient ID = 0

Listener

Security Context

Common

Sender
Sender ID = 2

Recipient
Recipient ID = 0

Listener

Security Context

Common

Sender
Sender ID = 3

Recipient
Recipient ID = 0

› Protection against replay included

Minor Modifications

- Transaction Identifier is now (Cid, **Sender ID**, Sender Seq Num)
- Request URI is integrity protected and not encrypted;
  - Contains all URI-* but Uri-Path/Query which are encrypted
  - When Proxy-Uri is used, it contains Proxy-Uri minus Uri-Path/Query
- External AAD is now a CBOR array

- Check the issue tracker! https://github.com/EricssonResearch/OSCOAP/issues

- Thanks Malisa, Jim, Martin and Joakim for reviewing.

Java implementation

From IETF 96 – Berlin

- https://github.com/joakimb/OSCoAP
- Californium: a CoAP Java implementation*
- OSCOAP: patch for Californium, easy to maintain
- Dependencies: COSE Java implementation (that uses CBOR and tinyDTLS)

* http://www.eclipse.org/californium/

C Implementation

- https://github.com/Gunzter/contiki-oscoap

- based on Erbium CoAP: a CoAP library in Contiki OS*
- v-04 of the draft, with some differences:
  - No protected Observe option
  - No sliding window for sequence numbers

- Removed external dependencies:
  - COSE tailor made
  - Crypto libraries

- Dynamic memory usage removed → better performance

* http://people.inf.ethz.ch/mkovatsc/erbium.php

Summary

- Draft is stable and ready for implementation
- We have had several security reviews
- We have 2 implementations: JAVA (link), C (link) (from SICS)

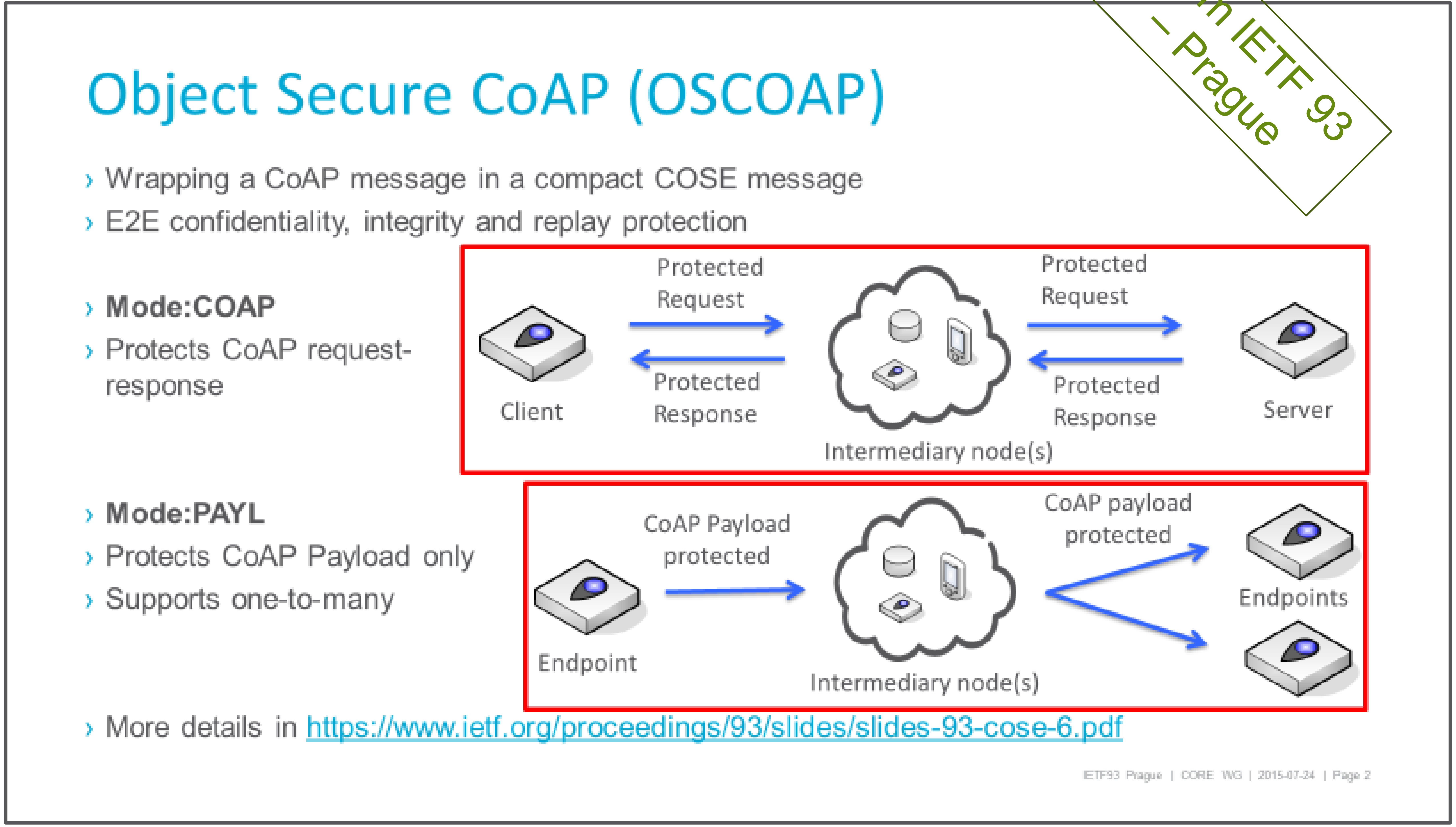
- Further reviews (from CoAP experts) are welcome
- More implementations for interoperability testing appreciated

Thank you!

Comments/questions?

OSCOAP vs OSCON

From IETF 93 – Prague



Object Secure CoAP (OSCOAP)

- Wrapping a CoAP message in a compact COSE message
- E2E confidentiality, integrity and replay protection

- **Mode:COAP**
- Protects CoAP request-response

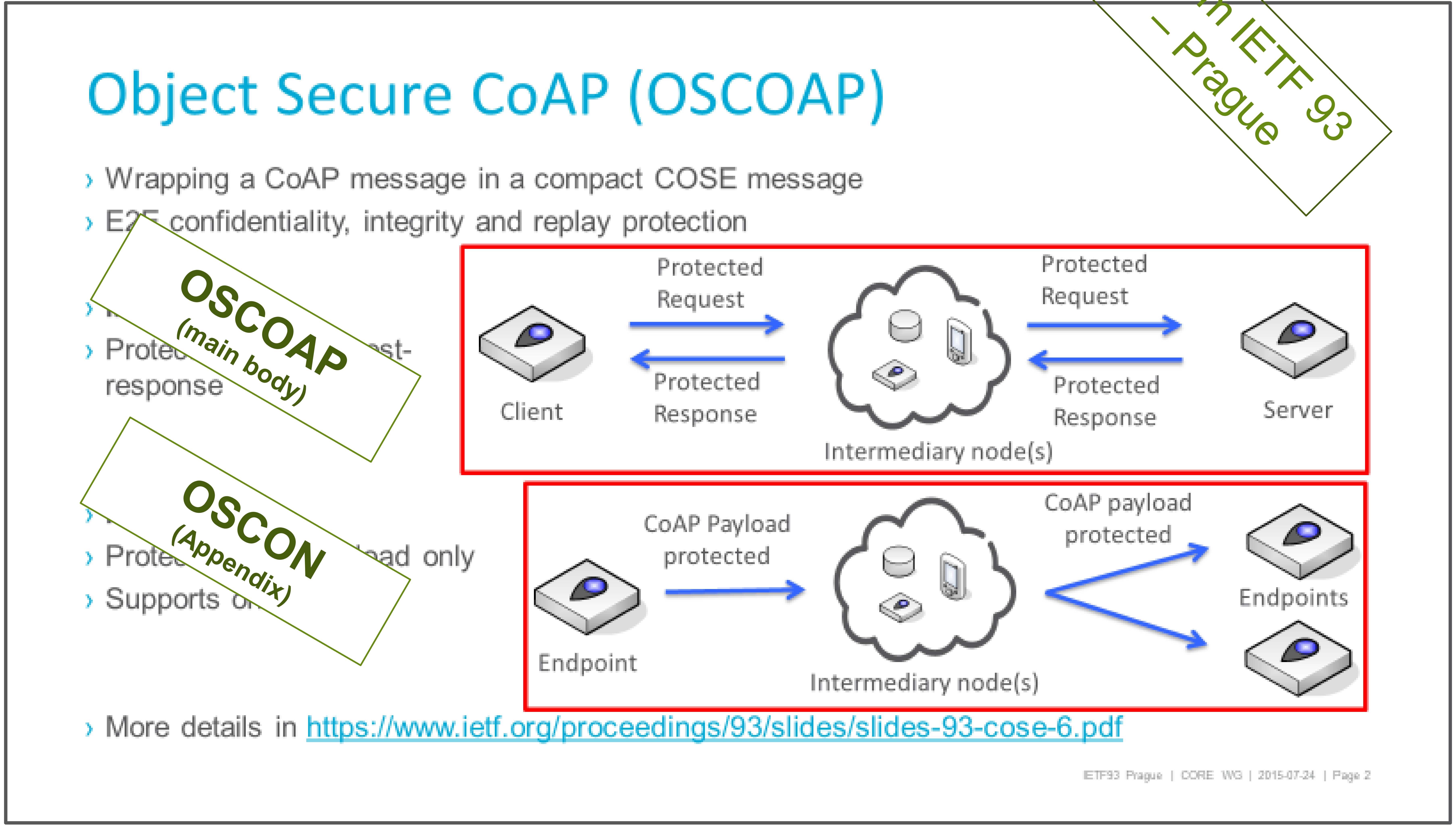
- **Mode:PAYL**
- Protects CoAP Payload only
- Supports one-to-many

- More details in https://www.ietf.org/proceedings/93/slides/slides-93-cose-6.pdf

IETF93 Prague | CORE WG | 2015-07-24 | Page 2

OSCOAP vs OSCON

From IETF 93 – Prague



Object Secure CoAP (OSCOAP)

- › Wrapping a CoAP message in a compact COSE message
- › E2E confidentiality, integrity and replay protection

OSCOAP (main body)

- › Prote ...st- response

OSCON (Appendix)

- › Prote ...ad only
- › Supports o...
- › More details in https://www.ietf.org/proceedings/93/slides/slides-93-cose-6.pdf

IETF93 Prague | CORE WG | 2015-07-24 | Page 2

All times are in time-warped KST

Wednesday (90 min)

- 13:30–13:40 Intro, WG status
- 13:40–14:10 CoAP over reliable (BR)
- 14:10–14:20 Protocol negotiation (BS – remote)
- 14:20–14:32 Resource Directory (chairs)
- 14:32–14:52 Object Security (FP)
- 14:52–15:00 dynlink (CG)
- 15:00–15:00 interfaces (CG)

Dynamic Resource Linking for Constrained RESTful Environments

draft-ietf-core-dynlink-01

IETF #97 Seoul

Christian Groves

Status update (1)

- Now a WG document
- V1 changes:
  - Tweaked document structure
  - Term “State synchronization” introduced to account for different update methods.
  - The description of binding attributes has been updated.
  - A new clause describing attribute interactions has been added.

Status update (2)

- Duplication between binding and Observe attributes description has been removed.
- Updated text on deletion of item in a binding table
- Formalised the IANA considerations

Next steps

- Confirm current understanding of the behaviour of the binding/observe attributes
- Need to add wrapping to gt/lt due to draft-koster-t2trg-hsml
- Confirm structure/direction of updates
- Binding Interface name should be core.bnd
- Add additional attributes related to initialization and bands.

All times are in time-warped KST

Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

Reusable Interface Definitions for Constrained RESTful Environments

draft-ietf-core-interfaces-06

IETF #97 Seoul

Christian Groves

Updates

- Updated the abstract and introduction.
- Section 2: Removed the collections definition in favour of the complete definition in the collections section.
- Removed section 3 on interfaces in favour of an updated definition in section 1.3.
- General: Changed interface type to interface description as that is the term defined in RFC6690.
- Removed section on future interfaces.
- Section 8: Updated IANA considerations.
- Added Appendix A “Current Usage of Interfaces and Function Sets”

Appendix A – Issues (1)

- Seeks to survey the current landscape to see how collections, interfaces and function sets/profiles are being used.
  - Documentation of interfaces is not consistent.
  - Function descriptions even less so.
- RFC6690 introduces the “if” attribute and procedure about registration BUT is silent on what should be in a description document. Should this be elaborated on?

Appendix A – Issues (2)

- ietf-core-resource-directory uses interfaces but does not an assign interface description identifiers to them?
- OCF have defined several interfaces that are quite similar to the ones in the draft? Should we look to harmonise them?
- Update/versioning of interface descriptions?
- draft-vanderstok-core-comi needs to be added uses interface core.c and function set.
- draft-koster-t2trg-hsml also needs to be added due to interface usage.

Next steps?

- Would function set be better as a separate draft or simply removed?
  - Function sets specification seem less defined
  - Whether to split probably depends on ambition level

- We assume people have read the drafts

- Meetings serve to advance difficult issues by making good use of face-to-face communications

- Note Well: Be aware of the IPR principles, according to RFC 3979 and its updates

✓Blue sheets
✓Scribe(s)

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session
The IESG, or any member thereof on behalf of the IESG
Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
Any IETF working group or portion thereof
Any Birds of a Feather (BOF) session
The IAB or any member thereof on behalf of the IAB
The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- **13:30–13:30 Intro**
- **13:30–13:40 Links-JSON (CB)**
- **13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)**
- **14:00–14:10 Object Security for multicast (FP)**
- **14:10–14:20 Delegated Observe (ZC)**
- **14:20–14:30 CoAP over WebRTC DC (CG)**

- **14:30–15:00 Flextime**

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- **13:30–13:30 Intro**
- **13:30–13:40 Links-JSON (CB)**
- **13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)**
- **14:00–14:10 Object Security for multicast (FP)**
- **14:10–14:20 Delegated Observe (ZC)**
- **14:20–14:30 CoAP over WebRTC DC (CG)**

- **14:30–15:00 Flextime**

```
  </sensors>;ct=40;title="Sensor Index",
  </sensors/temp>;rt="temperature-c";if="sensor",
  </sensors/light>;rt="light-lux";if="sensor",
  <http://www.example.com/sensors/t123>
   ;anchor="/sensors/temp";rel="describedby",
  </t>;anchor="/sensors/temp";rel="alternate"
➔
  [{"href":"/sensors","ct":"40","title":"Sensor Index"},
   {"href":"/sensors/temp","rt":"temperature-c","if":"sensor"},
   {"href":"/sensors/light","rt":"light-lux","if":"sensor"},
   {"href":"http://www.example.com/sensors/t123",
    "anchor":"/sensors/temp","rel":"describedby"},
   {"href":"/t","anchor":"/sensors/temp","rel":"alternate"}]
```

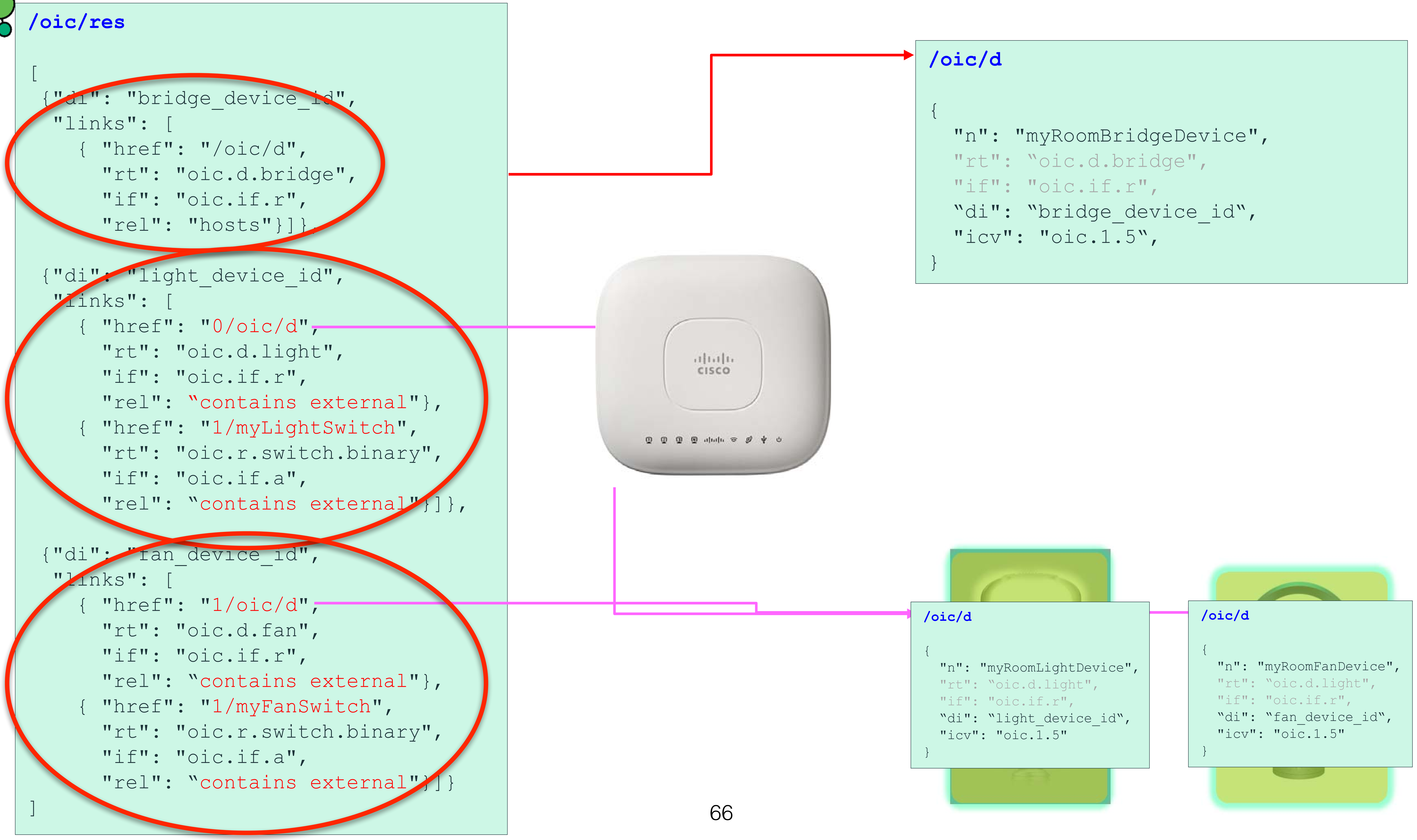
Potential Issue: How to update

- Structure: Array of links
- RD update might
  - add links: trivial
  - change links: replace on href as key?
  - remove links (how to indicate this?)
- draft-ietf-appsawg-json-merge-patch was defined to solve problems like this
  - but does not fit: only can update object (map), not array
- → make sure that cbor-merge-patch works for this

Status

- WGLC completed July 30th
- Christian Amsüss: what about JSON-LD?
- Michael Koster: “requirement for core-links-json tobe a 1:1 bidirectionally lossless mapping to CoRE Link-Format” [ct=40]
- So what about other formats carrying links?
  - e.g., Coral and HSML?

Bridging relationship with oic/res



/oic/res

```
[
 {"di": "bridge_device_id",
  "links": [
    { "href": "/oic/d",
      "rt": "oic.d.bridge",
      "if": "oic.if.r",
      "rel": "hosts"}]},

 {"di": "light_device_id",
  "links": [
    { "href": "0/oic/d",
      "rt": "oic.d.light",
      "if": "oic.if.r",
      "rel": “contains external"},
    { "href": "1/myLightSwitch",
      "rt": "oic.r.switch.binary",
      "if": "oic.if.a",
      "rel": “contains external"}]},

 {"di": "fan_device_id",
  "links": [
    { "href": "1/oic/d",
      "rt": "oic.d.fan",
      "if": "oic.if.r",
      "rel": “contains external"},
    { "href": "1/myFanSwitch",
      "rt": "oic.r.switch.binary",
      "if": "oic.if.a",
      "rel": “contains external"}]}
]
```

/oic/d

```
{
  "n": "myRoomBridgeDevice",
  "rt": “oic.d.bridge",
  "if": "oic.if.r",
  “di": “bridge_device_id“,
  "icv": "oic.1.5“,
}
```

/oic/d

```
{
  "n": "myRoomLightDevice",
  "rt": “oic.d.light",
  "if": "oic.if.r",
  “di": “light_device_id“,
  "icv": "oic.1.5"
}
```

/oic/d

```
{
  "n": "myRoomFanDevice",
  "rt": “oic.d.light",
  "if": "oic.if.r",
  “di": “fan_device_id“,
  "icv": "oic.1.5"
}
```

To Do

- Make extensibility of link-format more explicit in the CDDL
- Fix the Content-Format IANA registrations
- Remove material that discusses JSON-LD and friends
  - But do make use of Christian's input for some improved explanation

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- **13:30–13:30 Intro**
- **13:30–13:40 Links-JSON (CB)**
- **13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)**
- **14:00–14:10 Object Security for multicast (FP)**
- **14:10–14:20 Delegated Observe (ZC)**
- **14:20–14:30 CoAP over WebRTC DC (CG)**

- **14:30–15:00 Flextime**

CoRE working group

EST over CoAPs
draft-vanderstok-core-coap-est-00

69

P. van der Stok, K. Sandeep

Motivation

ANIMA WG works on:
Bootstrapping of Remote Secure Key Infrastructures (BRSKI)

- BRSKI specifies how a new node joins a secure network
- Also interesting for constrained devices on constrained networks.

- A constrained network (CN) in enterprise settings will often be managed by an IT department.
- That department is responsible for a larger network including CN.
- Relying on one similar protocol to accept devices securey is for many IT departments a condition for connecting the CN to the managed network

EST-coaps why

Enrollment over Secure Transport (EST) is basic building block of BRSKI

EST uses https from joining node to the Registrar (certificate providing node)

The provision of EST over DTLS secured CoAP (EST-coaps) between joining node and Registrar makes BRSKI deployable on a larger set of CNs.

EST-coaps contents

- Uses DTLS over CoAP instead of TLS over HTTP
- Reduces number of supported message types
- Introduces content formats to CoAP registry
- Explains use of block and DTLS
- Uses binary instead of base64 encoding
- CoAP response code 2.06 specified for delayed answers

Very similar: draft-pritikin-coap-bootstrap

- Discusses DTLS instead of TLS for BRSKI/EST transactions
- Provides bindings of BRSKI/EST messages to COAP
- Address fragmentation with COAP Blocks
- Addresses HTTP Proxying
- Addresses COAP and DTLS session parameters

Potentially have one draft in the end that incorporates everything.

Questions

1. Interest in BRSKI for CN?
2. Agree with EST over CoAPs with BRSKI or something new?
3. Full EST or subset of EST for EST-coaps?
4. Interest to implement, comment,….?

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- 13:30–13:30 Intro
- 13:30–13:40 Links-JSON (CB)
- 13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)
- 14:00–14:10 Object Security for multicast (FP)
- 14:10–14:20 Delegated Observe (ZC)
- 14:20–14:30 CoAP over WebRTC DC (CG)

- 14:30–15:00 Flextime

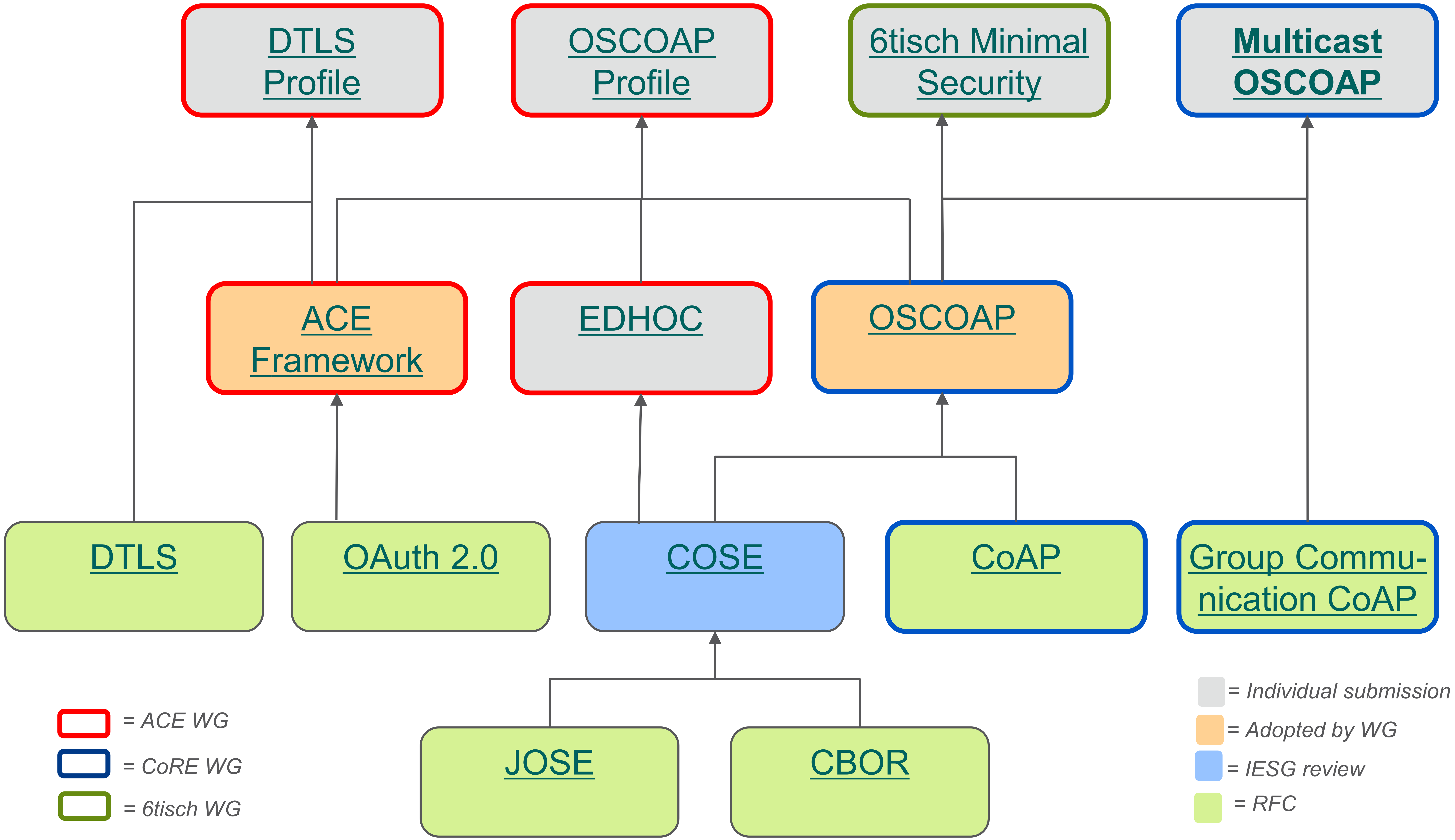
Secure group communication for CoAP

draft-tiloca-core-multicast-oscoap-00

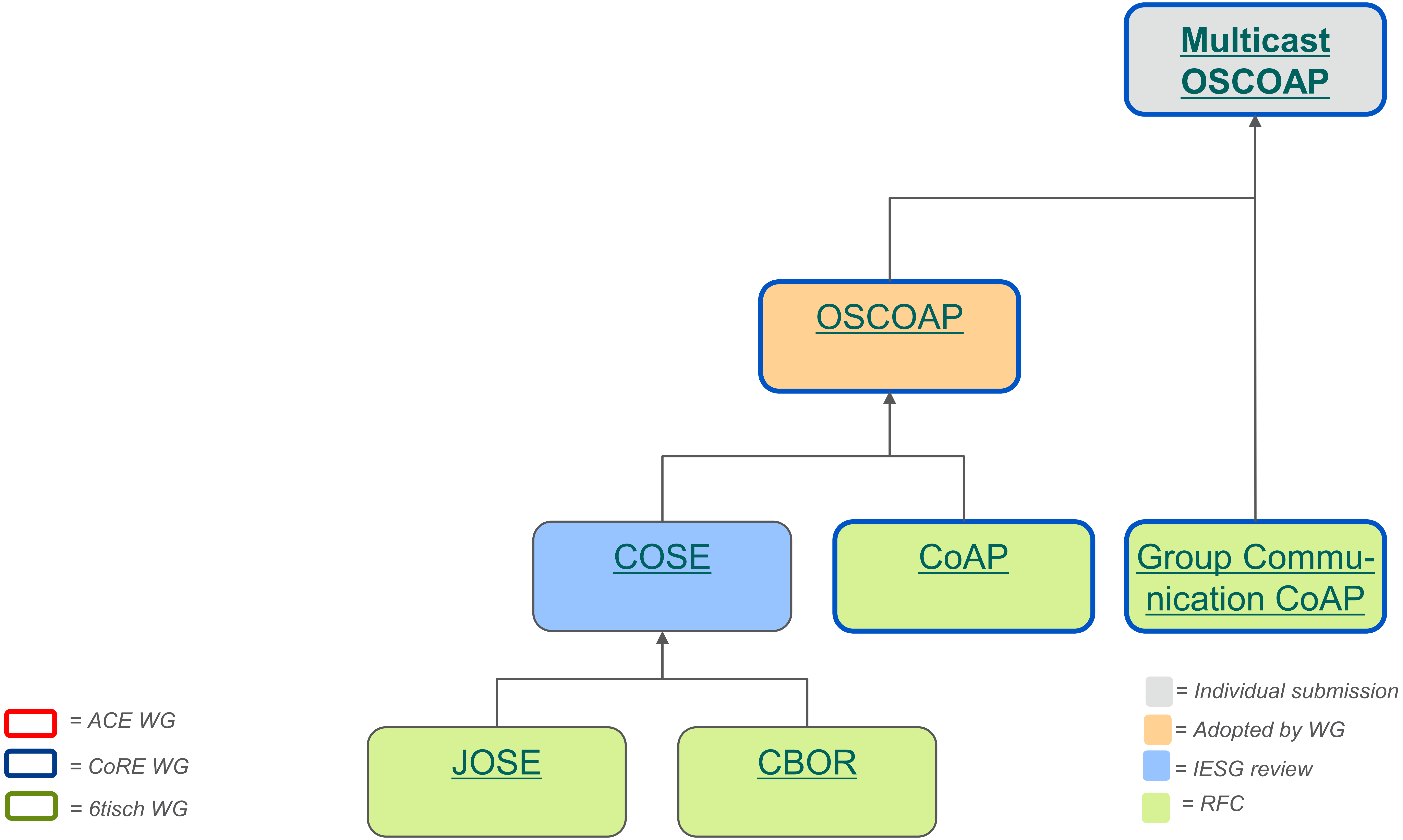
Marco Tiloca, SICS Swedish ICT
Göran Selander, Ericsson
Francesca Palombini, Ericsson

IETF 97, CORE WG, Seoul, Nov 17, 2016

Related Work



Related Work



Multicast OSCOAP

OSCOAP

COSE

CoAP

Group Communication CoAP

JOSE

CBOR

🟥 = ACE WG

🟦 = CoRE WG

🟩 = 6tisch WG

⬜ = Individual submission

🟧 = Adopted by WG

🟦 = IESG review

🟩 = RFC

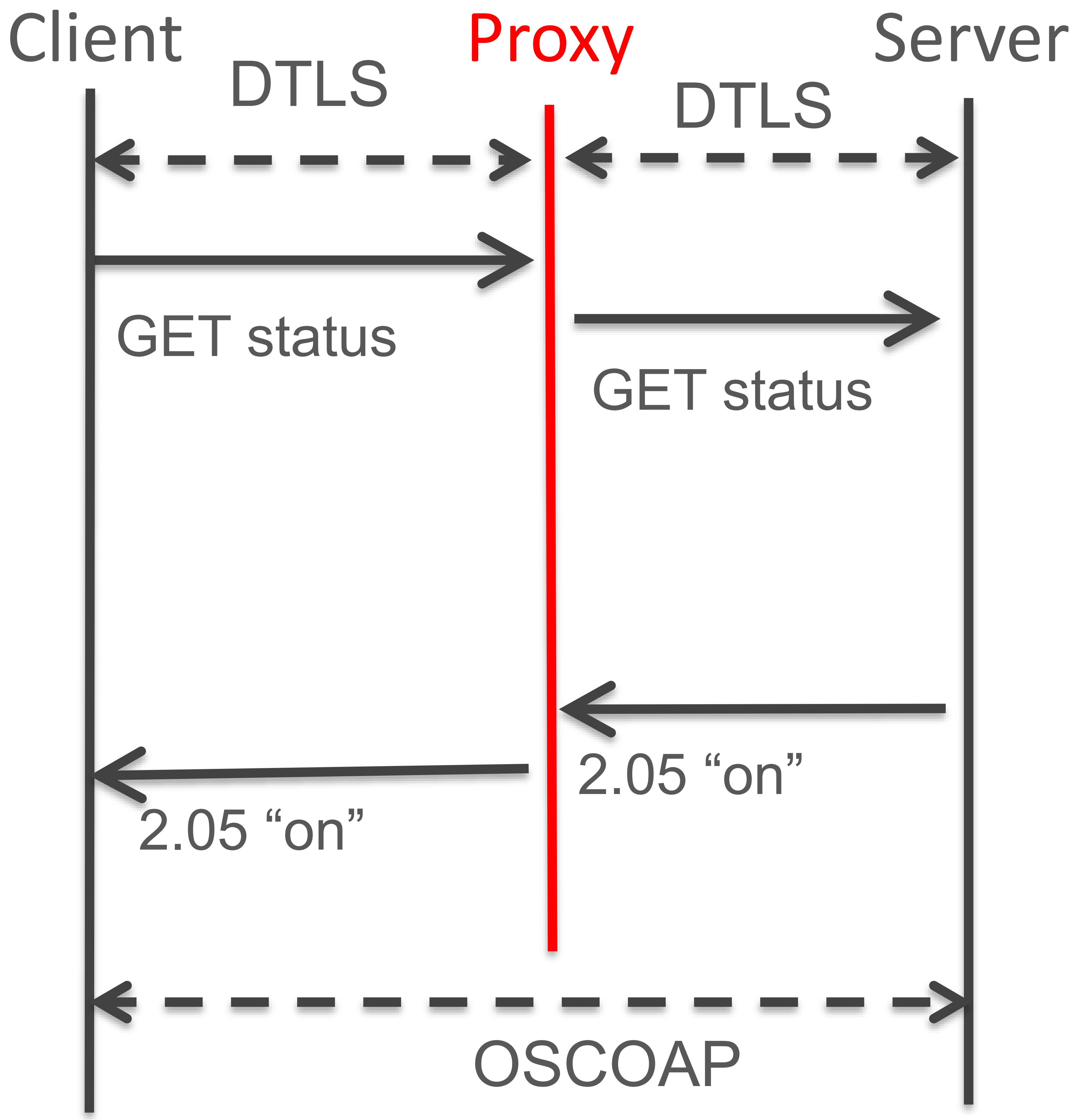
OSCOAP

- OSCOAP defines a method for in-layer security of CoAP message exchanges using the COSE format.

- OSCOAP protects CoAP end-to-end and can be used instead of DTLS
  - Allows legitimate proxy operations
  - Detects illegitimate proxy operations

- Independent of how CoAP is transported (UDP, TCP, Bluetooth, 802.15.4, foo…)

- Requirements: draft-hartke-core-e2e-security-reqs



Motivation

- RFC7390* Section 5.3.3 : ” In the future, to further mitigate the threats, security enhancements need to be developed at the IETF for group communications.”
- CoRE WG requested Multicast OSCOAP (IETF95, mailing list, …)

- draft-somaraju-ace-multicast relies on OSCOAP to secure group messages, but doesn’t define how.

- Multicast OSCOAP fills this gap and is use case independent

*RFC7390: Group Communication for the Constrained Application Protocol (CoAP)

Main Features

- How to use OSCOAP in group communication

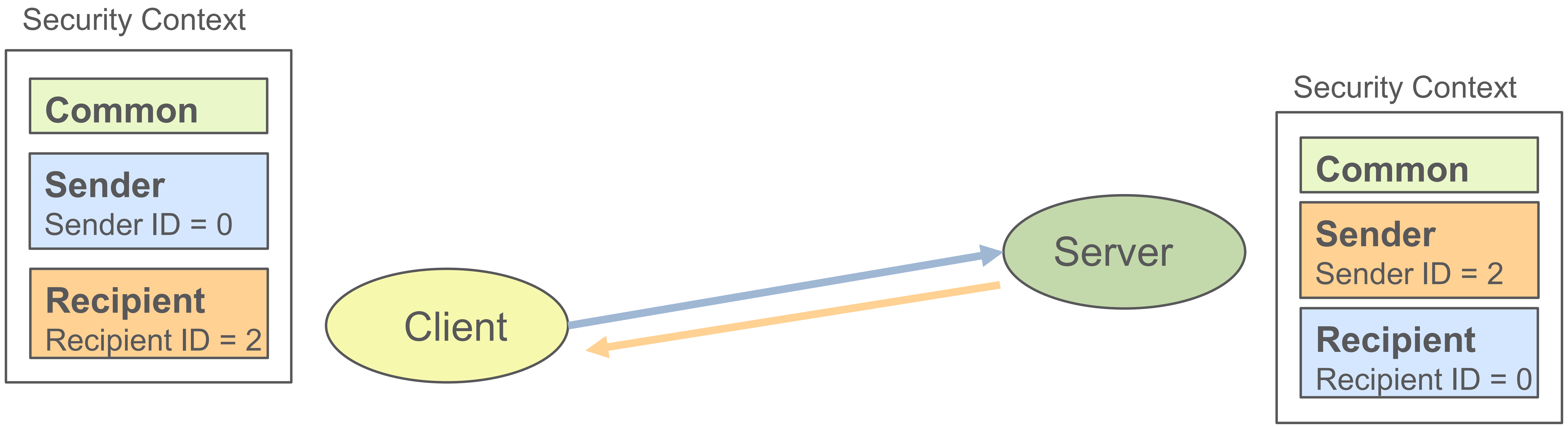
- Confidentiality and Integrity: Shared keying material to protect communication within the group (using OSCOAP mechanisms)

- Source authentication:
  - Asymmetric-key counter signatures
  - Embedded in the COSE object

- Same structures, constructs, mechanisms of OSCOAP

OSCOAP

› draft-ietf-core-object-security-00



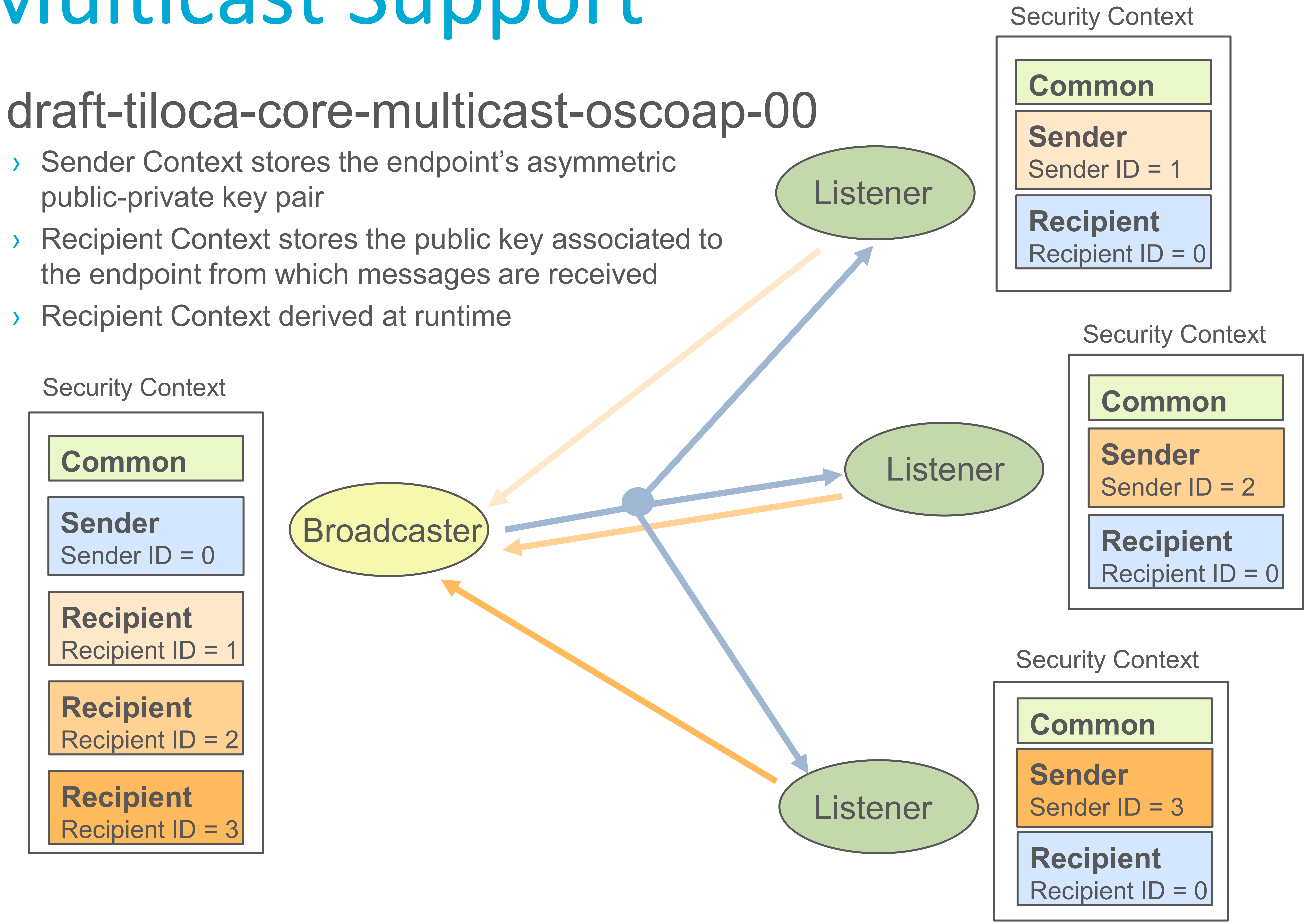
› Secure end-to-end communication in the presence of intermediaries (Protection against replay included)

› Uniquely bind the CoAP response to the CoAP request

› Protects payload and parts of CoAP metadata (header, options….)

Multicast Support

- draft-tiloca-core-multicast-oscoap-00
  - Sender Context stores the endpoint's asymmetric public-private key pair
  - Recipient Context stores the public key associated to the endpoint from which messages are received
  - Recipient Context derived at runtime



What’s Different from OSCOAP

- Adds asymmetric keys in Sender/Recipient Context
- Sender ID is always sent in the message (Optional in OSCOAP) and is used to retrieve the right Recipient Context
- Recipient Contexts created at runtime upon receiving the first message from the respective endpoint
- Counter Signature added to COSE_Encrypt0 object

Thank you!

Comments/questions?

https://ericssonresearch.github.io/Multicast-OSCOAP/

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- 13:30–13:30 Intro
- 13:30–13:40 Links-JSON (CB)
- 13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)
- 14:00–14:10 Object Security for multicast (FP)
- 14:10–14:20 Delegated Observe (ZC)
- 14:20–14:30 CoAP over WebRTC DC (CG)

- 14:30–15:00 Flextime

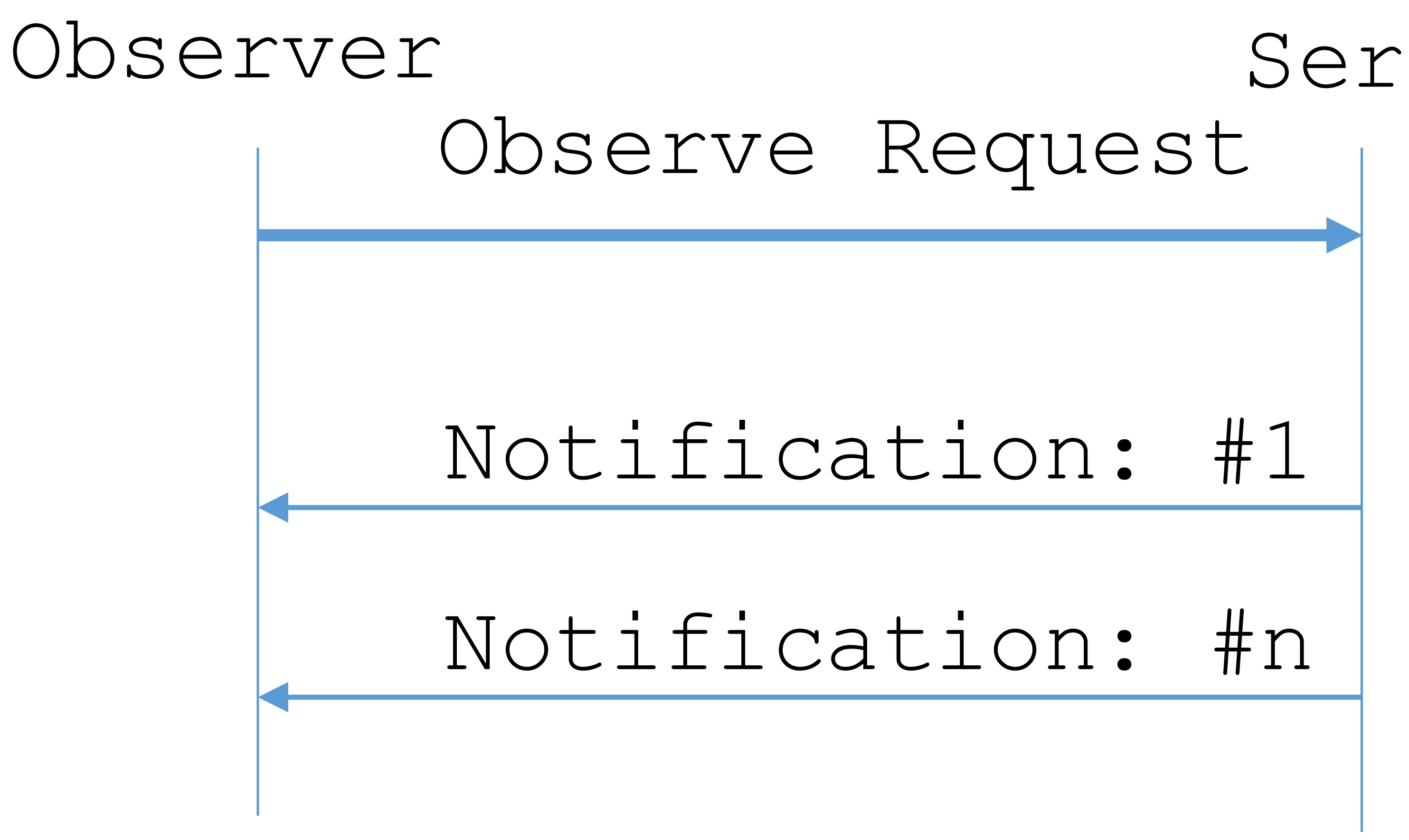
CoAP Delegated Observation

draft-cao-core-delegated-observe-00

Zhen Cao & Rahul Jadhav

Huawei

Recap: direct Observe



Observer

Server

Observe Request

Notification: #1

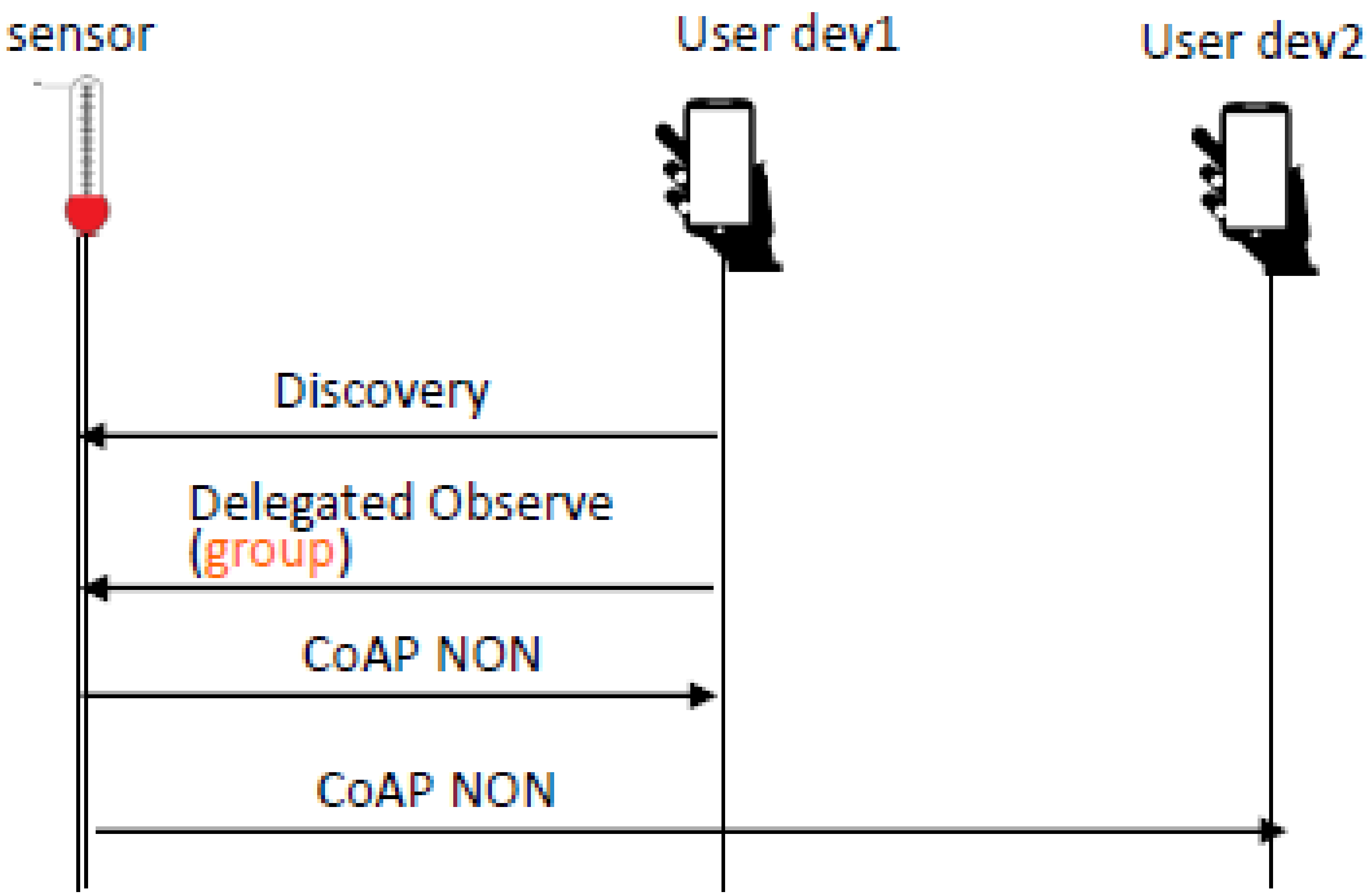
Notification: #n

Create mapping:
<URI, (IP, Port)>

The notification mapping is created between
the URI and (IP, Port) of the Observer.
The IP &Port are from the IP&UDP header.

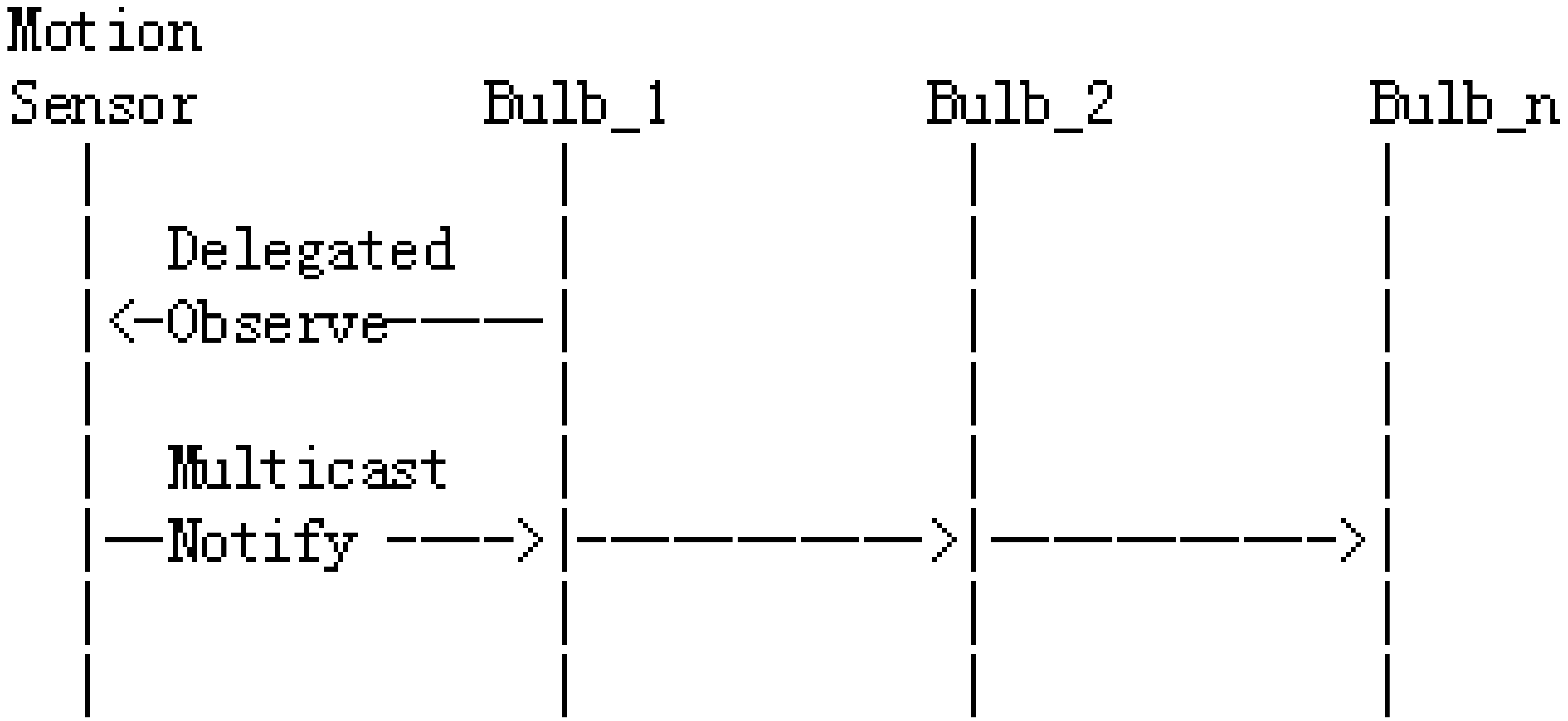
If the Observer hide behind any NAT,
notification will normally fail.

Delegated Observe Scenario: Multi-Devices



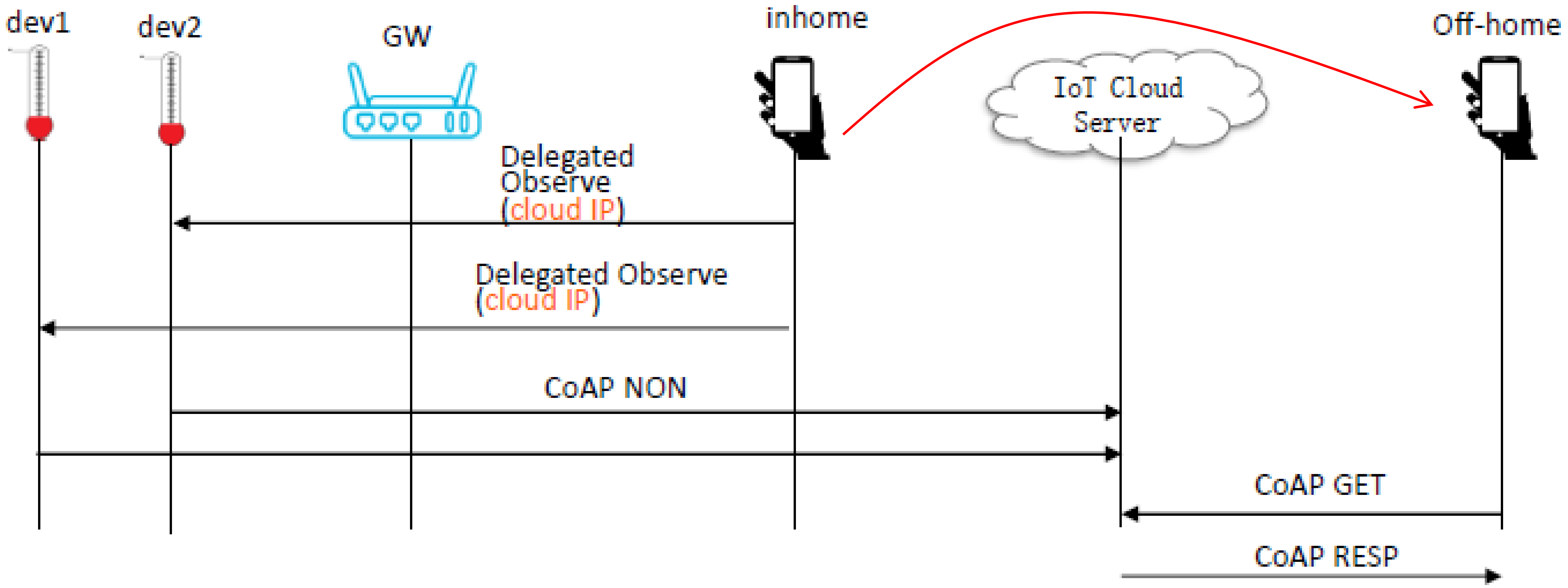
- The user has multiple devices (it’s a common scenario nowadays) and need to subscribe the information on the sensor
- Avoiding the need of sending observe request on the group of devices, one could just delegate
- The notification will send to the subscribed Group

Multicast



- E.g., A number of light bulbs need to adjust its lighting intensity based on the location of the observed motion object.
- Instead of let each device register an interest on the motion sensor, one of them could simply delegate the observe to this multicast group, so that the location update notifications will be send to the multicast address that they belong to.

Delegate to the Cloud



- The mobile device want to keep notified about its home sensor information both in-home and off-home;
- But while off-home, its reachability will be broken due to NAT
- Let the mobile-dev send a delegated observe request while at home, instructing the home sensors send notifications to the device's representative cloud server, so that the device can always fetch the information from it cloud service while off-home.

Discussion

- Delegated observe may increase the risk of amplification attacks
- This negative effect can be controlled by several implementation considerations:
  - a) the delegating node can negotiate with the delegated node before sending delegated observe, out of band;
  - b) the source node will strictly control the rate of the notifications, so that flooding will be avoided;
  - c) the delegated node can block any notifications beyond a certain data rate.

Next steps

- Anyone else identify similar problems ?
- Anyone would like to work together or review the current draft?

- Interest to continue working on this in the CORE WG?

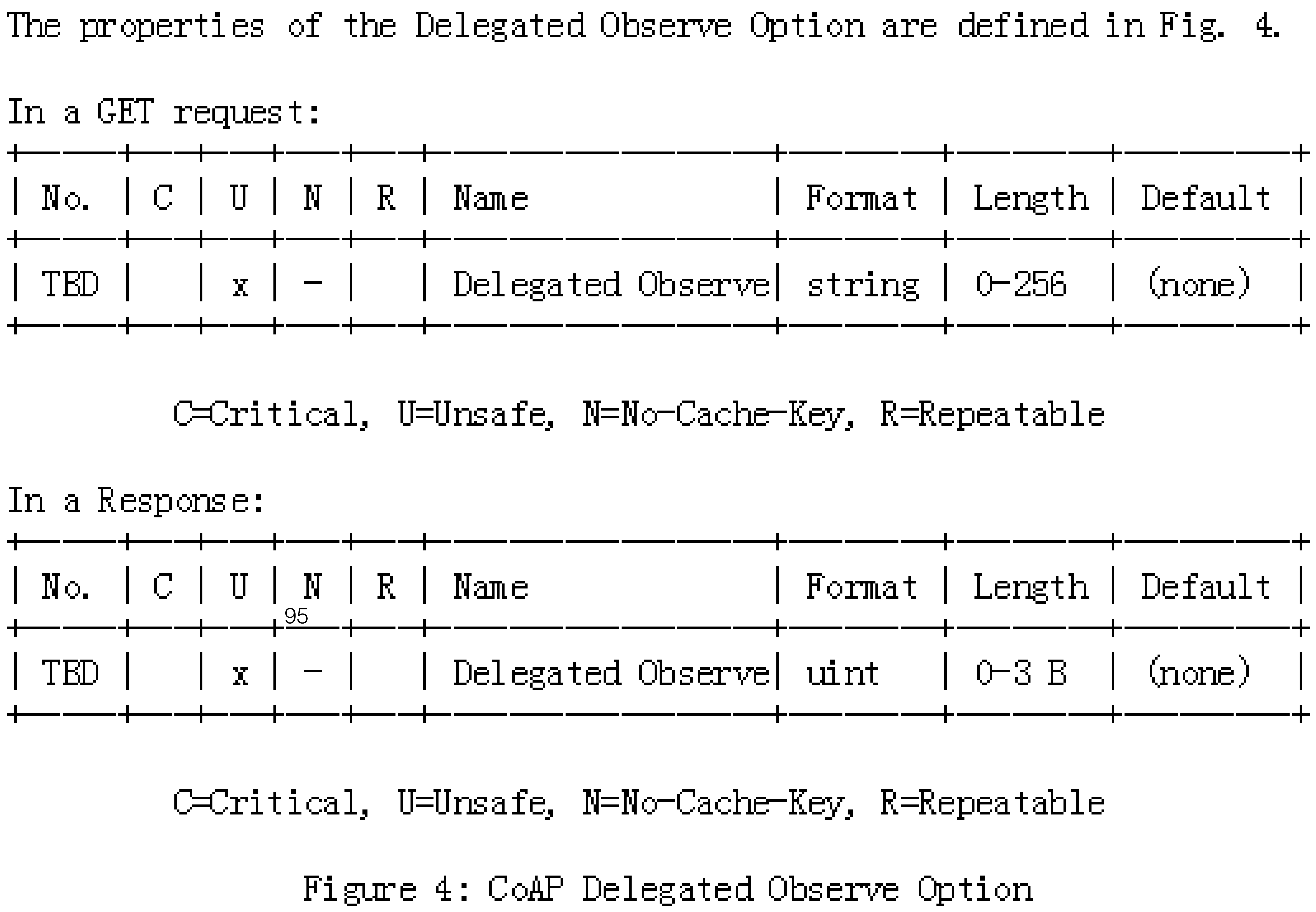
- **Acknowledgement:** comments & suggestion by Christian Amsüss

Appendix: What else in the draft

Proposed Delegated Observe Option

Examples

Proposed Delegated Observe Option in the draft



The properties of the Delegated Observe Option are defined in Fig. 4.

In a GET request:

No.	C	U	N	R	Name	Format	Length	Default
TBD		x	-		Delegated Observe	string	0-256	(none)

C=Critical, U=Unsafe, N=No-Cache-Key, R=Repeatable

In a Response:

No.	C	U	N	R	Name	Format	Length	Default
TBD		x	-		Delegated Observe	uint	0-3 B	(none)

C=Critical, U=Unsafe, N=No-Cache-Key, R=Repeatable

Figure 4: CoAP Delegated Observe Option

Example

```
Source        Initiating    Cloud
 Node           Node         Node
  |              |            |
  |  Delegated   |            |     Header: GET 0x 86868686
  |<-Observe-----|            |      Token: 0x55
  |              |            |   Uri-Path: temp
  |              |            |  D-Observe: 10.0.0.2:5683
  |              |            |
  |              |            |
  |              |            |     Header: GET 0x 86868686
  |--Notify(2.05)------------>|      Token: 0x55
  |              |            |  D-Observe: 9
  |              |            |    Max-age: 15
  |              |            |    Payload: "18.8 Cel"
  |              |            |
  |              |            |     Header: GET 0x 8686ab99
  |--Notify(2.05)------------>|      Token: 0x55
  |              |            |  D-Observe: 16
  |              |            |    Max-age: 15
  |              |            |    Payload: "19.2 Cel"
```

Example: multicast

```
Source        Initiating Multicast Group
 Node           Node         Nodes
  |              |            |
  |  Delegated   |            |     Header: GET 0x 86868686
  |<-Observe-----|            |      Token: 0x55
  |              |            |   Uri-Path: temp
  |              |            |  D-Observe: 224.0.y.x:5683
  |              |            |
  |              |            |
  |              |            |     Header: GET 0x 86868686
  |-Notify(2.05)-+------------>      Token: 0x55
  |              |            |  D-Observe: 9
  |              |            |    Max-age: 15
  |              |            |    Payload: "18.8 Cel"
  |              |            |
  |              |            |     Header: GET 0x 8686ab99
  |--Notify(2.05)+----------->|      Token: 0x55
  |              |            |  D-Observe: 16
  |              |            |    Max-age: 15
  |              |            |    Payload: "18.2 Cel"
```

All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- 13:30–13:30 Intro
- 13:30–13:40 Links-JSON (CB)
- 13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)
- 14:00–14:10 Object Security for multicast (FP)
- 14:10–14:20 Delegated Observe (ZC)
- 14:20–14:30 CoAP over WebRTC DC (CG)
- 14:30–15:00 Flextime

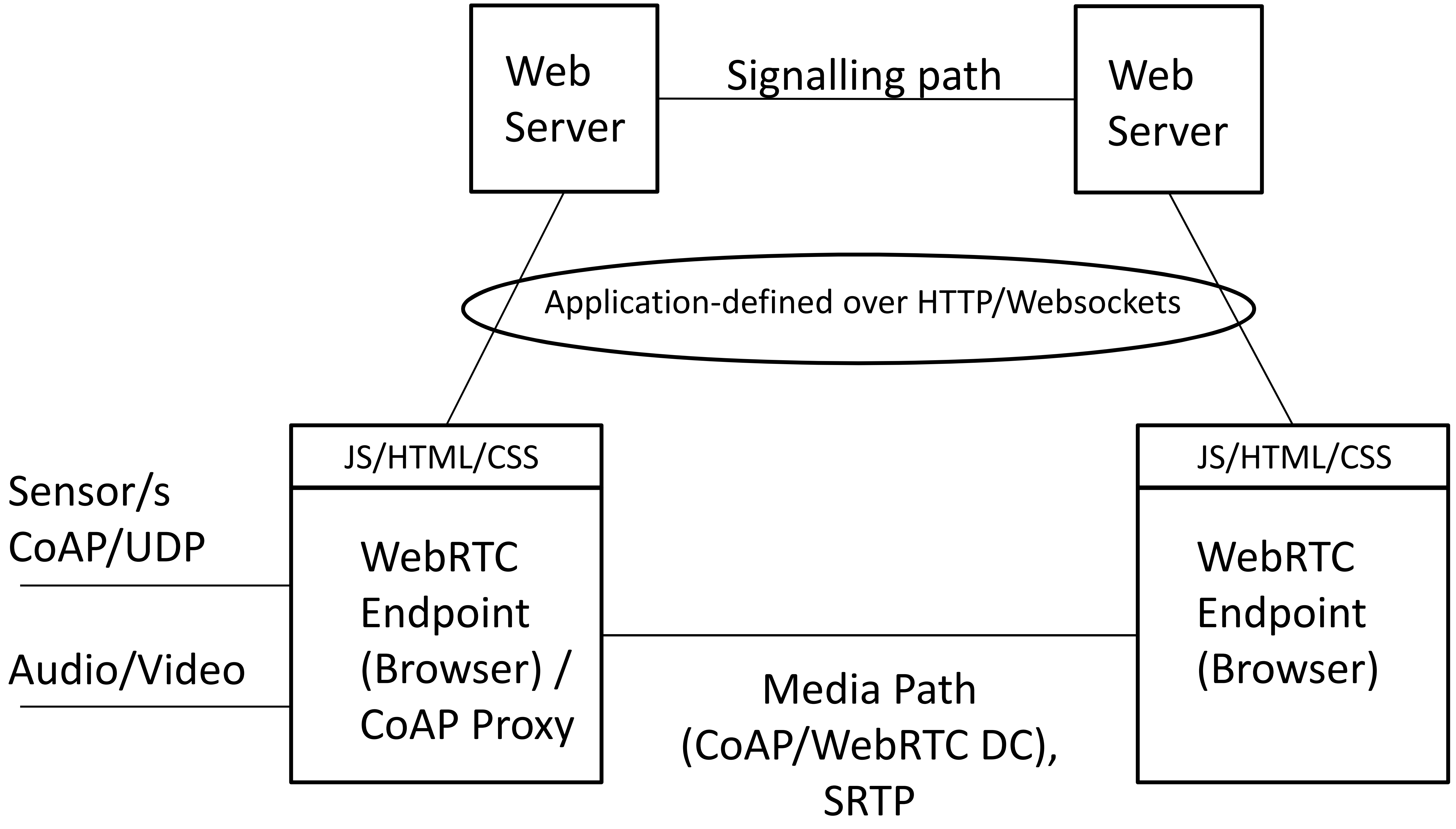
CoAP over WebRTC Datachannel

draft-groves-coap-webrtcdc–01

IETF #97 Seoul

Christian Groves

Architecture



Web Server

Signalling path

Web Server

Application-defined over HTTP/Websockets

Sensor/s CoAP/UDP

Audio/Video

JS/HTML/CSS

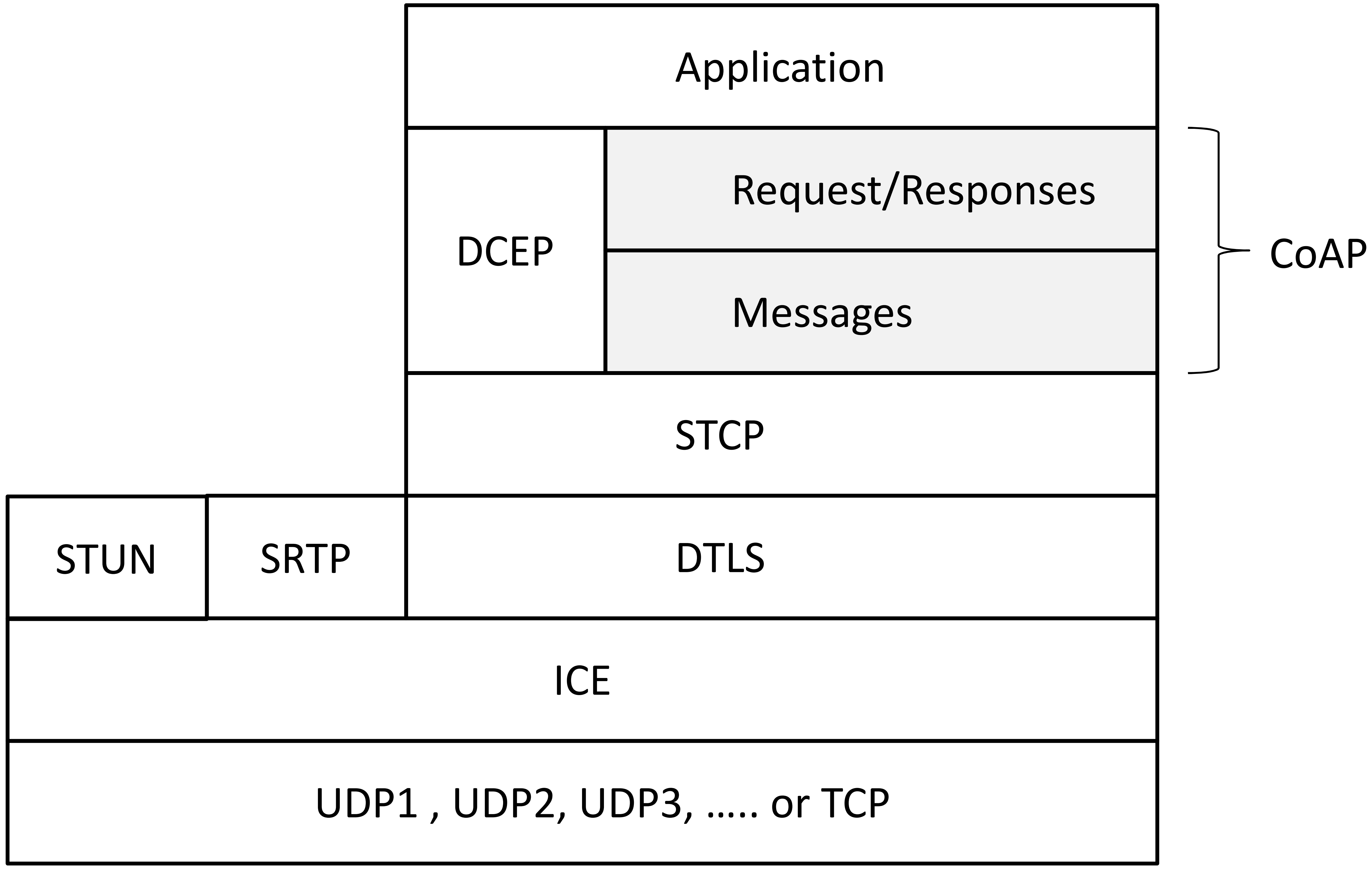
WebRTC Endpoint (Browser) / CoAP Proxy

Media Path (CoAP/WebRTC DC), SRTP

JS/HTML/CSS

WebRTC Endpoint (Browser)

Stack



Application

DCEP

Request/Responses

Messages

CoAP

STCP

STUN

SRTP

DTLS

ICE

UDP1 , UDP2, UDP3, ….. or TCP

Features

- Allows peer to peer CoAP message exchange
- NAT traversal & security provided by WebRTC
- Allows multiplexing over a single DTLS connection
- DC allows reliable and partial reliable modes similar to CoAP
- Like CoAP/TCP, CoAP reliability mechanisms aren’t needed (e.g. ACK and duplicate detection).
- Provides transport keepalive.
- WebRTC DC manages establishment / release

V1 Update: Message Design

Length
(Set to 0, Not needed)

Message ID Removed
(Redundant)

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Len   |  TKL  |      Code       | TKL bytes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Options (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 1 1 1 1 1 1|    Payload (if any)...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Now uses same format as TCP/TLS and Websockets (draft-ietf-core-coap-tcp-tls)

V1 Updates: cont.

- Added description of opening handshake to align with draft-ietf-core-coap-tcp-tls.
- Added CoAP capability setting message (CSM) and BERT support.

Next steps

Is this something interesting for the CoRE WG?

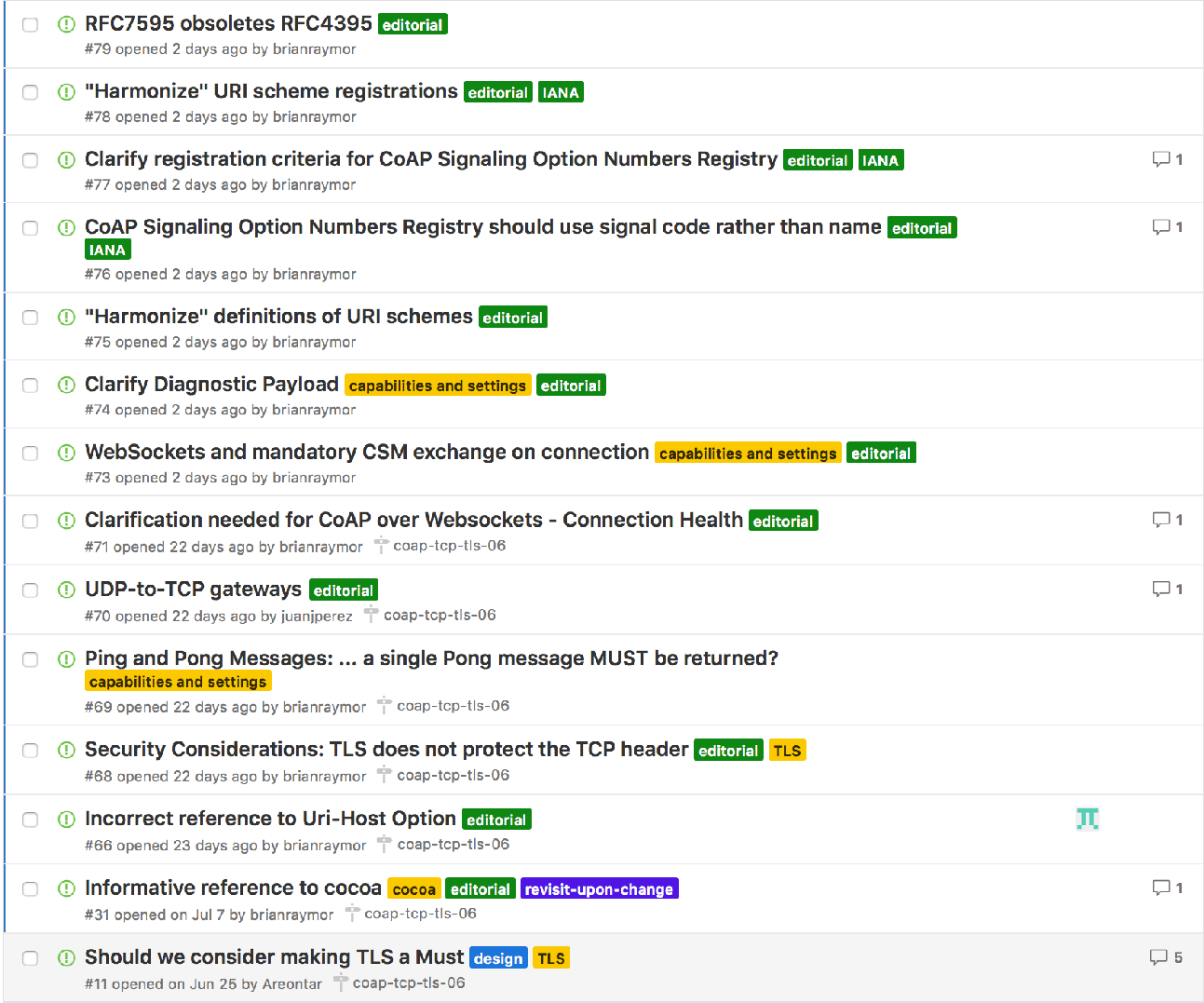
All times are in time-warped KST

Thursday: hallway meeting (Park BR 3)

- 13:30–13:30 Intro
- 13:30–13:40 Links-JSON (CB)
- 13:40–14:00 CoAP in ANIMA (BRSKI, EST-coap) (PV)
- 14:00–14:10 Object Security for multicast (FP)
- 14:10–14:20 Delegated Observe (ZC)
- 14:20–14:30 CoAP over WebRTC DC (CG)

- 14:30–15:00 Flextime
  - TCP nits
  - CoCoA ACC
  - DTLS over COAP

CoAP/TCP design nits



□ RFC7595 obsoletes RFC4395 editorial
#79 opened 2 days ago by brianraymor

□ "Harmonize" URI scheme registrations editorial IANA
#78 opened 2 days ago by brianraymor

□ Clarify registration criteria for CoAP Signaling Option Numbers Registry editorial IANA 💬 1
#77 opened 2 days ago by brianraymor

□ CoAP Signaling Option Numbers Registry should use signal code rather than name editorial IANA 💬 1
#76 opened 2 days ago by brianraymor

□ "Harmonize" definitions of URI schemes editorial
#75 opened 2 days ago by brianraymor

□ Clarify Diagnostic Payload capabilities and settings editorial
#74 opened 2 days ago by brianraymor

□ WebSockets and mandatory CSM exchange on connection capabilities and settings editorial
#73 opened 2 days ago by brianraymor

□ Clarification needed for CoAP over Websockets - Connection Health editorial 💬 1
#71 opened 22 days ago by brianraymor coap-tcp-tls-06

□ UDP-to-TCP gateways editorial 💬 1
#70 opened 22 days ago by juanjperez coap-tcp-tls-06

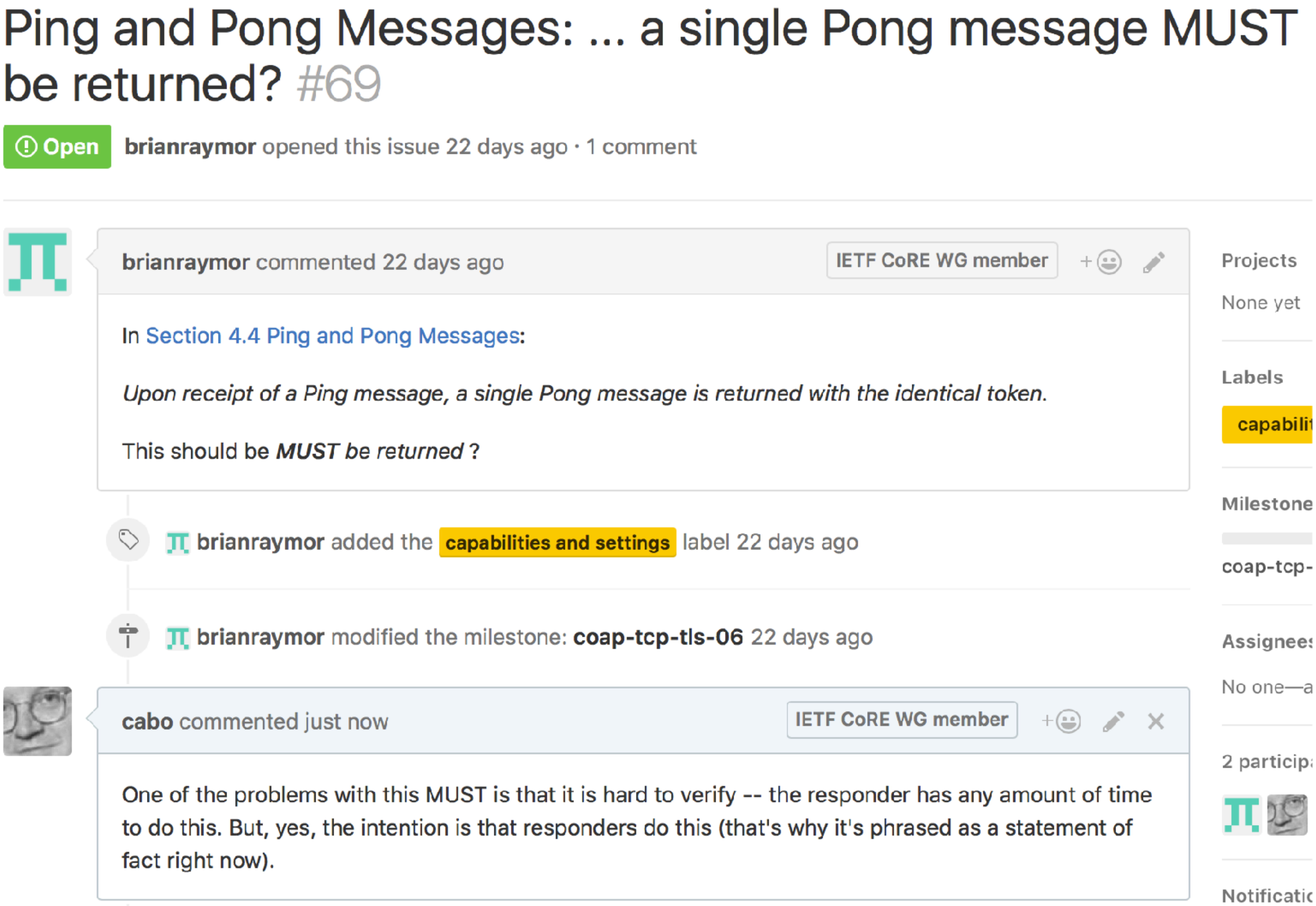
□ Ping and Pong Messages: ... a single Pong message MUST be returned? capabilities and settings
#69 opened 22 days ago by brianraymor coap-tcp-tls-06

□ Security Considerations: TLS does not protect the TCP header editorial TLS
#68 opened 22 days ago by brianraymor coap-tcp-tls-06

□ Incorrect reference to Uri-Host Option editorial
#66 opened 23 days ago by brianraymor coap-tcp-tls-06

□ Informative reference to cocoa cocoa editorial revisit-upon-change 💬 1
#31 opened on Jul 7 by brianraymor coap-tcp-tls-06

□ Should we consider making TLS a Must design TLS 💬 5
#11 opened on Jun 25 by Areontar coap-tcp-tls-06



Ping and Pong Messages: ... a single Pong message MUST be returned? #69

brianraymor opened this issue 22 days ago · 1 comment

brianraymor commented 22 days ago

In Section 4.4 Ping and Pong Messages:

Upon receipt of a Ping message, a single Pong message is returned with the identical token.

This should be ***MUST** be returned* ?

brianraymor added the **capabilities and settings** label 22 days ago

brianraymor modified the milestone: **coap-tcp-tls-06** 22 days ago

cabo commented just now

One of the problems with this MUST is that it is hard to verify -- the responder has any amount of time to do this. But, yes, the intention is that responders do this (that's why it's phrased as a statement of fact right now).

CSM Mandatory?

- Before summer, there were no CSM
  - existing implementations just start exchanging messages
- Now, CSM mandatory
  - Both MUST send as first message
  - “Client” need not wait for “server” CSM (but v.v.?) (still not quite clear what the permissible waiting behaviors are.)
- Do we want an OCF 1.0 compatibility mode?

Scheme names (as an application developer would view it)

COAP	COAPS	?
coap$_{\mathit{+udp}}$	**coaps**$_{\mathit{+udp}}$	*coap+dtls*
coap+tcp	**coaps+tcp**	coap+tls
coap+ws	coaps+ws	**coap+wss**

Evaluation of Aggregate Congestion Control

(Appendix of draft-ietf-core-cocoa-00)

Carsten Bormann (Universität Bremen TZI)
August Betzler, Carles Gomez, Ilker Demirkol (UPC/i2cat)
Jon Crowcroft (University of Cambridge)
carlesgo@entel.upc.edu

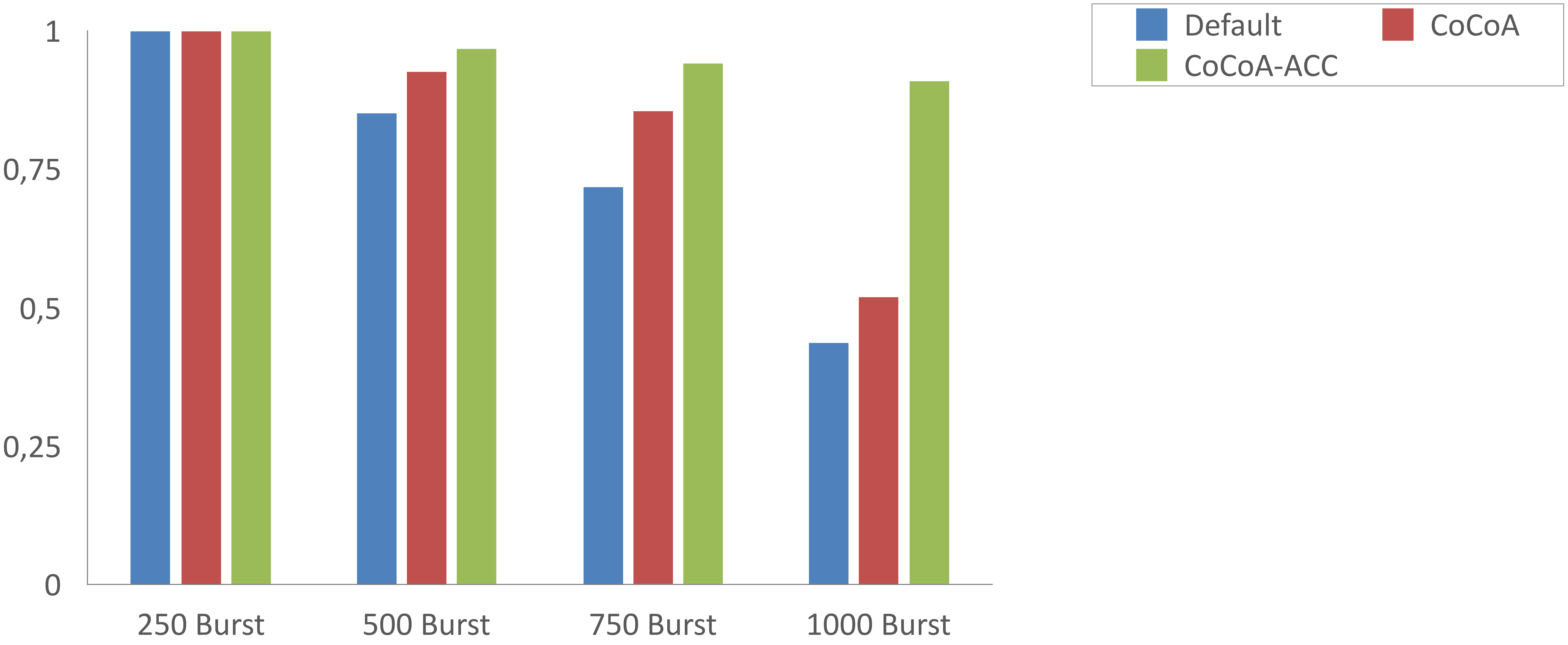
IETF 97 – Seoul, November 2017

Introduction

- CoCoA provides adaptive congestion control for CoAP
  - Specifically designed considering CNN features
- Appendix: Aggregate Congestion Control (ACC)
  - Control burstiness of aggregate traffic from unconstrained device talking to many other endpoints
- Performance evaluation in GPRS emulated scenario
  - Californium CoAP implementation
  - Transmission of requests to several devices
  - Default CoAP, CoCoA, CoCoA-ACC

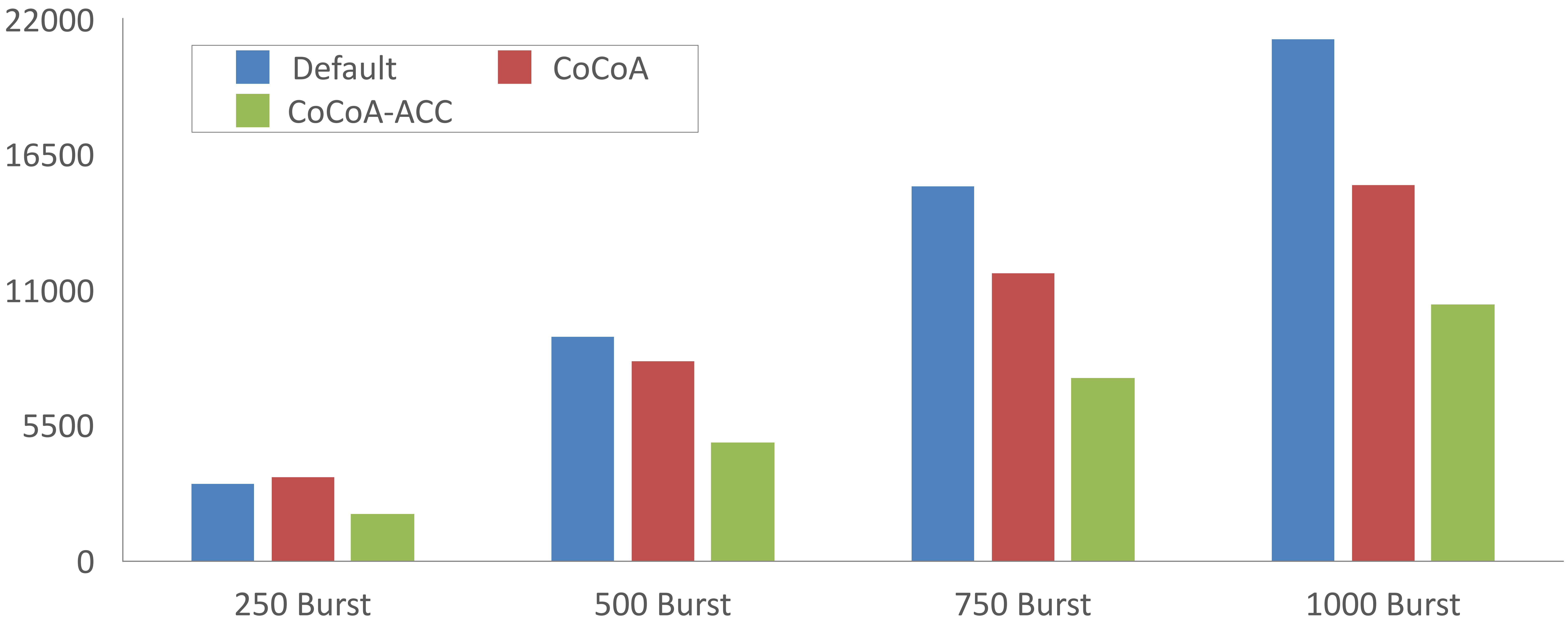
Results (I/IV)

- Burst-only traffic
  - PDR



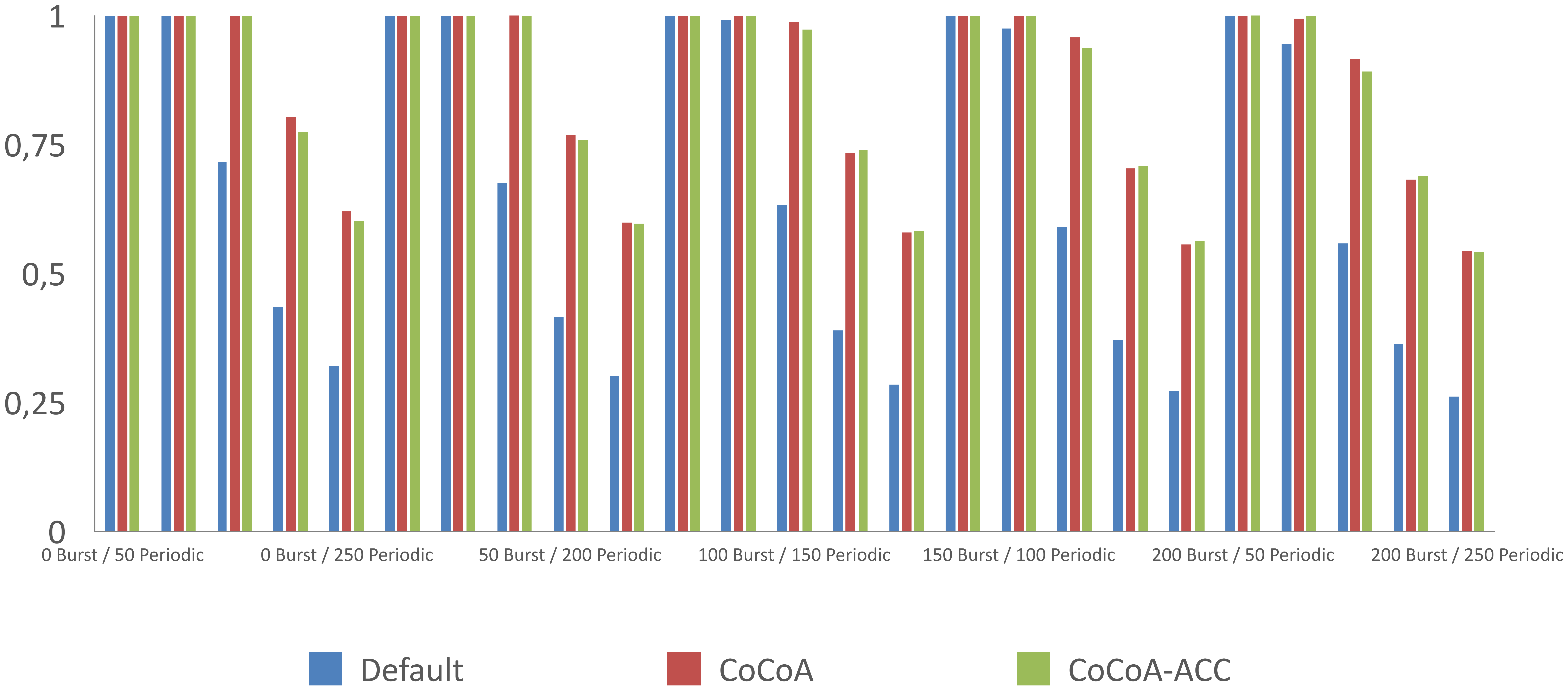
Results (II/IV)

- Burst-only traffic
  - Retries



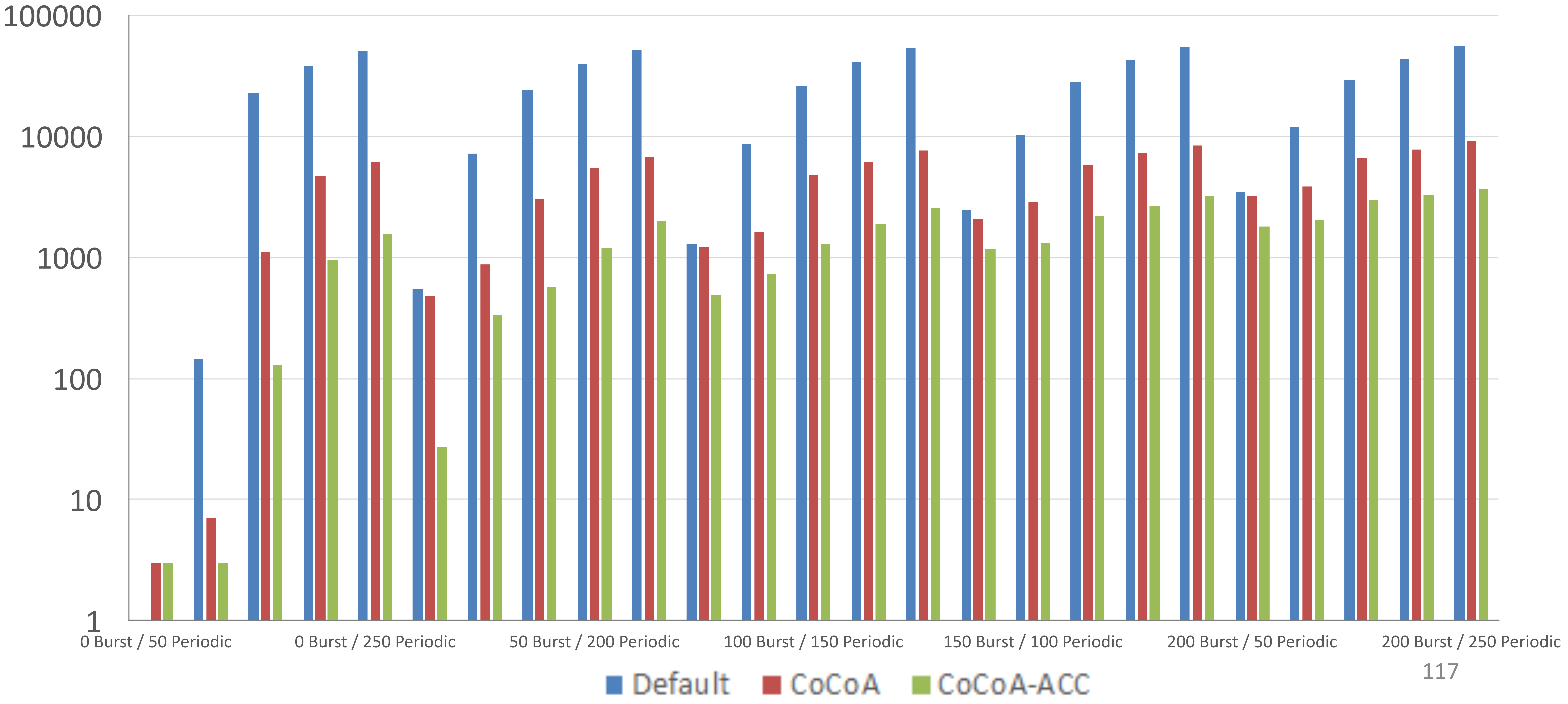
Results (III/IV)

- Mixed traffic (periodic/burst)
  - PDR



Results (IV/IV)

- Mixed traffic (periodic/burst)
  - Retries



Conclusions

- Burst traffic
  - CoCoA-ACC: greater PDR than CoCoA
  - CoCoA-ACC: lower number of retries
- Mixed traffic
  - CoCoA-ACC: same PDR as CoCoA
  - CoCoA-ACC: very low number of retries
- Benefits at the expense of greater delay
  - CoCoA-ACC: greater than default CoAP
  - CoCoA-ACC: lower than CoCoA for high traffic

Future work

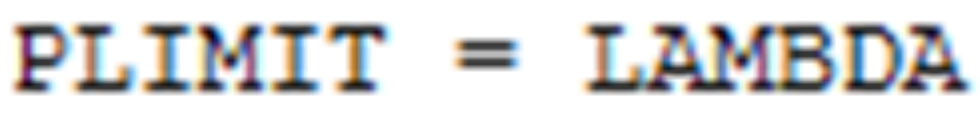
- Perform experiments in the IoT-Lab
  - IEEE 802.15.4 multihop testbed

Questions ?

Carsten Bormann (Universität Bremen TZI)
August Betzler, Carles Gomez, Ilker Demirkol (UPC/i2cat)
Jon Crowcroft (University of Cambridge)
carlesgo@entel.upc.edu

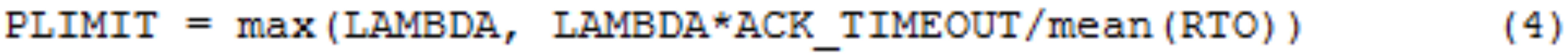
Back-up slide: ACC algorithm

- If no RTO info available for a destination



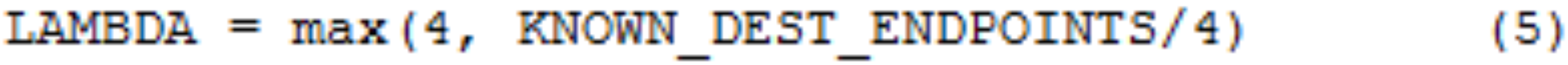
```
PLIMIT = LAMBDA
```

- Otherwise



```
PLIMIT = max(LAMBDA, LAMBDA*ACK_TIMEOUT/mean(RTO))          (4)
```

- LAMBDA is computed as



```
LAMBDA = max(4, KNOWN_DEST_ENDPOINTS/4)          (5)
```

DTLS over CoAP

draft-schmertmann-dice-codtls-01.txt

Lars Schmertmann, Klaus Hartke,
Carsten Bormann

DTLS = Handshake + Record

- DTLS handshake assumes reasonably good UDP connectivity
- Timeouts inflexible; no “stop retransmitting”
- ➔ Use CoAP for handling the handshake

- Side-effect: This can be run over proxies
  ➔ nice e2e key agreement protocol…

Handshake 1: ClientHello

```
Client                                Server
------                                ------

POST /
ClientHello                  ----->

                                      4.01 Unauthorized
                             <-----   HelloVerifyRequest


POST /
ClientHello                  ----->

                                      2.01 Created /dCST0E
                                      ServerHello
                                      Certificate*
                                      ServerKeyExchange*
                                      CertificateRequest*
                             <-----   ServerHelloDone
```

Handshake 2: ClientHello

```
Client                                Server
------                                ------

PATCH /dCST0E
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                     ----->

                                      2.04 Changed
                                      [ChangeCipherSpec]
                             <-----   Finished
```

Implementation

Size (KiB)	Function
2.41	ECC functions
0.95	AES modes (CCM + CMAC)
0.80	Storage management
0.79	Session management
0.15	PRF
1.78	CoAP Resource implementing handshake
0.32	Parse & Send

Issues

- Document defines compression of DTLS fields
- `Finished` messages still would need to compute the hash from the expanded header
    - or would they?

- **We assume people have read the drafts**
- **Meetings serve to advance difficult issues by making good use of face-to-face communications**
- **Note Well: Be aware of the IPR principles, according to RFC 3979 and its updates**

✓Blue sheets
✓Scribe(s)

http://www.ietf.org/about/note-well.html

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

The IETF plenary session
The IESG, or any member thereof on behalf of the IESG
Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
Any IETF working group or portion thereof
Any Birds of a Feather (BOF) session
The IAB or any member thereof on behalf of the IAB
The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

draft-tcs-coap-no-response-option → RFC 7967 ✓

Published 2016-08-30

Independent Submission

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:50–10:00 SenML BTO (CG)
- 09:30–09:50 SenML (AK)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

All times are in time-warped KST

Leftover from Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

Summary from Thursday hallway meeting

- draft-ietf-core-links-json Presentation about status and updates. Proceeding further as planned.
- draft-vanderstok-core-coap-est and draft-pritikin-coap-bootstrap: how to use EST over CoAP. To be done in ACE WG. Issue: Do we need a new 2.06?
- draft-tiloca-core-multicast-oscoap Solves RFC7390 issue with securing multicast but independent of use case.
- draft-cao-core-delegated-observe enables delivery of observe responses to different addresses than where the request came from. Feedback: of interest to others. Security (spoofing) is an issue. Documentation of the problem can be done as draft-ietf-lwig-coap addition or T2TRG topic.
- draft-groves-coap-webrtcdc: like CoAP-TCP/Websockets, but over WebRTC data channel. Should go ahead after CoAP-TCP is done.

Summary from Thursday hallway meeting

- **draft-ietf-core-coap-tcp-tls:**
  - **Do we want to make additional mandates on how a peer has to pong on a ping? E.g., timeliness. Discuss on mailing list now.**
  - **CSM was made mandatory in IETF96, SDOs should be aware of that (no need for a compatibility mode). Exact state machine still undefined.**
- **Fixing the bug in scheme naming. Still a bikeshed. Still a bug.**

All times are in time-warped KST

Leftover from Wednesday (90 min)

- **13:30–13:40 Intro, WG status**
- **13:40–14:10 CoAP over reliable (BR)**
- **14:10–14:20 Protocol negotiation (BS – remote)**
- **14:20–14:32 Resource Directory (chairs)**
- **14:32–14:52 Object Security (FP)**
- **14:52–15:00 dynlink (CG)**
- **15:00–15:00 interfaces (CG)**

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

SenML Base Time Offset Attribute

draft-groves-core-senml-bto-00

IETF #97 Seoul

Christian Groves

Issue

- Aim: to minimise SenML pack size when multiple constant time increasing (or decreasing) records are contained. E.g.

```
[ {"bn": "urn:dev:ow:10e2073a01080063",
      "bt": 1320067464,
      "bu": "%RH",
      "v": 21.2},
      { "v": 21.3, "t": 10},
      { "v": 21.4, "t": 20},
      { "v": 21.4, "t": 30},
      { "v": 21.5, "t": 40}, ...
```

Proposal: new “Base Time Offset” (bto) attribute.

- Bto attribute specifies the time interval between records.

```
[ {"bn": "urn:dev:ow:10e2073a01080063",
      "bt": 1320067464,
      "bto": 10,
      "bu": "%RH",
      "v": 21.2},
      { "v": 21.3},
      { "v": 21.4},
      { "v": 21.4},
      { "v": 21.5}, ...
```

Issues (bto)

- Using bto two SenML records in a pack cannot have the same time. E.g. 2 sensors cannot have the same time.
- Negative time offset with the last record equal to t=0 is not possible.
- Usage of time “t” within a record not possible.
- There are potential work arounds for the above but would introduce complexity.
- Need to add text on what happens if bto is not understood (time will be missing).

Issues (SenML Extension)

- CBOR and XML/EXI extension are different.
- For CBOR just register string map key “bto”
- XML need to extend XML to add attribute and then update EXI XSD schema and introduce new schemaID options value indicating new version. Must include all previously registered attributes.
- The later seems to imply that all attributes are supported. The CBOR seems to imply optionality.
- How to indicate which attributes are actually supported?

Next steps

- Is there support to continue with the proposal?

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

Media Types for Sensor Measurement Lists (SenML)

draft-ietf-core-senml-04

IETF 97, Seoul, South Korea

Ari Keränen
ari.keranen@ericsson.com

Updates since -02

- New name: Media Types for Sensor **Measurement Lists** (SenML)
- Added text and examples about actuator use
- Added base sum
- Lots of clarifications, including
  - "resolved records"
  - why no new CBOR labels
- Media type registration considerations

Extensibility

- Schema (RelaxNG to XSD, CDDL) extensions
  - Always include full schema with all extensions defined so far with RelaxNG
  - CBOR: extension point ("socket")
- Instructions for designated expert
  - All defined SenML labels must be included
  - EXI Schema ID updated

Fragment support?

- Referring to parts of SenML **at the client**
  - fragment identifiers are not sent on wire
- Proposal: fragment ID modeled after RFC 7111 (row part)
- MUST resolve (i.e., fill base values) to the same values as the given range in the whole pack would
- Examples:

  sensors/temp#rec=3
  sensors/temp#rec=4-7
  sensors/temp#rec=4-*

Copy-pasting SenML?

- Is SenML potentially exchanged over clipboard? Content types need:
  - MacOS Uniform Type Identifiers
  - Windows Clipboard Names
- Proposal: why not

Metadata

- Free form text (full UTF-8) describing a Pack and/or Records
  - Example:
    {"n":"temp", "v":23, "u":"Cel", **"m": "München"**}
- But we need proper internationalization (language tags?) – "it is more complicated than you think" [RFC1925]
- Some use cases, but not a top priority: let's do as extension and ship SenML base spec now

All times are in time-warped KST

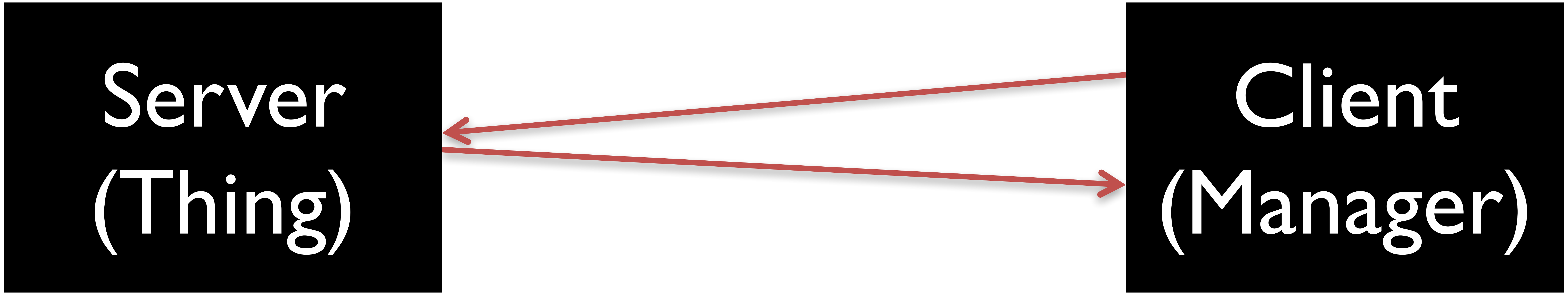
Friday (120 min)

- **09:30–09:30 Intro**
- **09:30–09:50 SenML (AK)**
- **09:50–10:00 SenML BTO (CG)**
- **10:00–10:40 Management over CoAP (COMI/COOL)**
  - **10:00–10:10 YANG over CBOR (AP)**
  - **10:10–10:20 SIDs**
  - **10:20–10:40 COMI/COOL**
- **10:40–11:00 Redirect (DT)**
- **11:00–11:10 YANG/LWM2M (PV)**
- **11:10–11:20 RFC6690 update (prefixes) (CG)**
- **11:20–11:30 Flextime**

YANG/CoMI

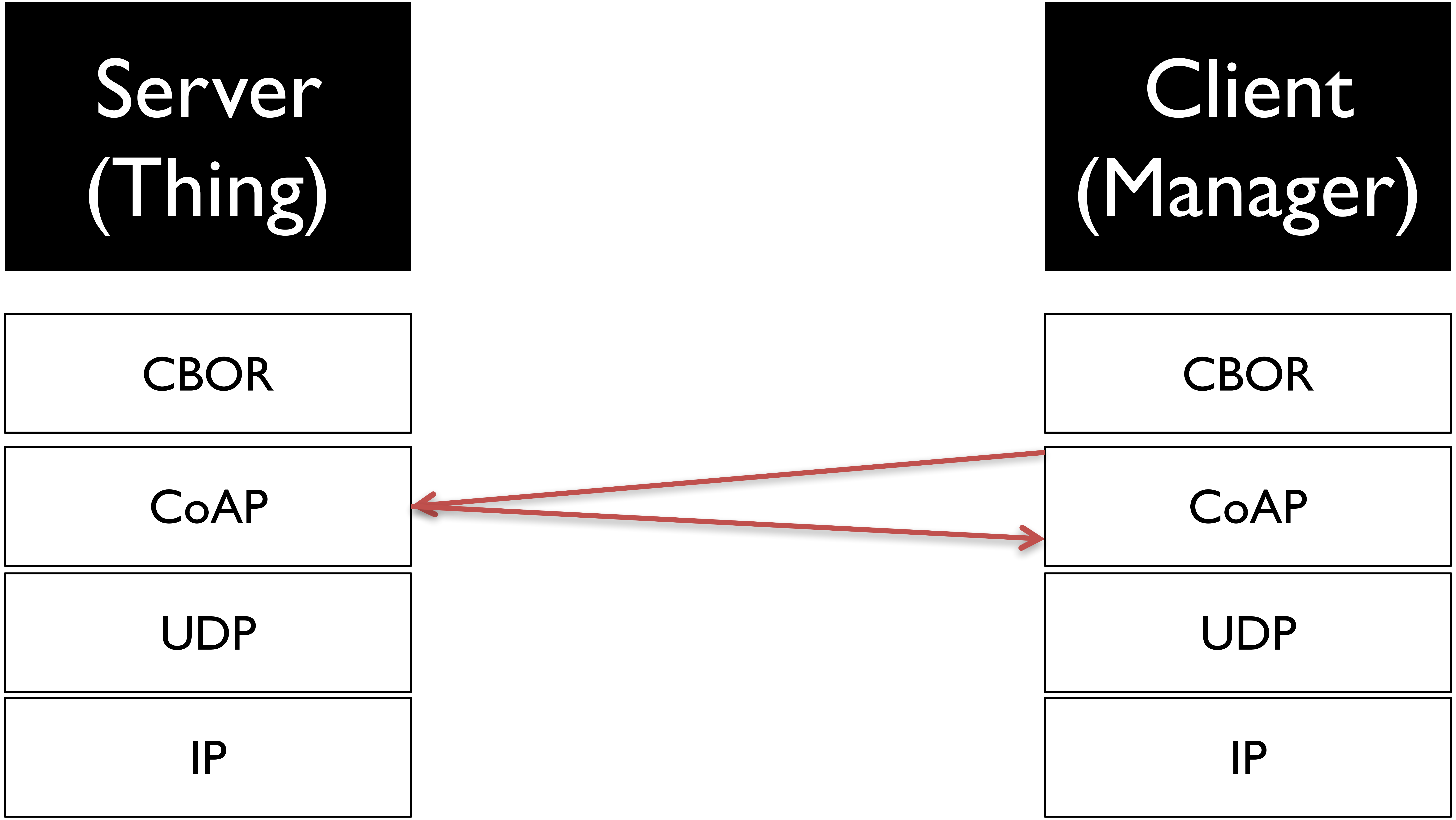
draft-ietf-core-yang-cbor-03
draft-ietf-core-sid-00
draft-vanderstok-core-comi-10

Peter van der Stok
Andy Bierman
Michel Veillette
Alexander Pelov
Abhinav Sumaraju
Randy Turner
Ana Minaburo



Server
(Thing)

Client
(Manager)



Server (Thing)

CBOR

CoAP

UDP

IP

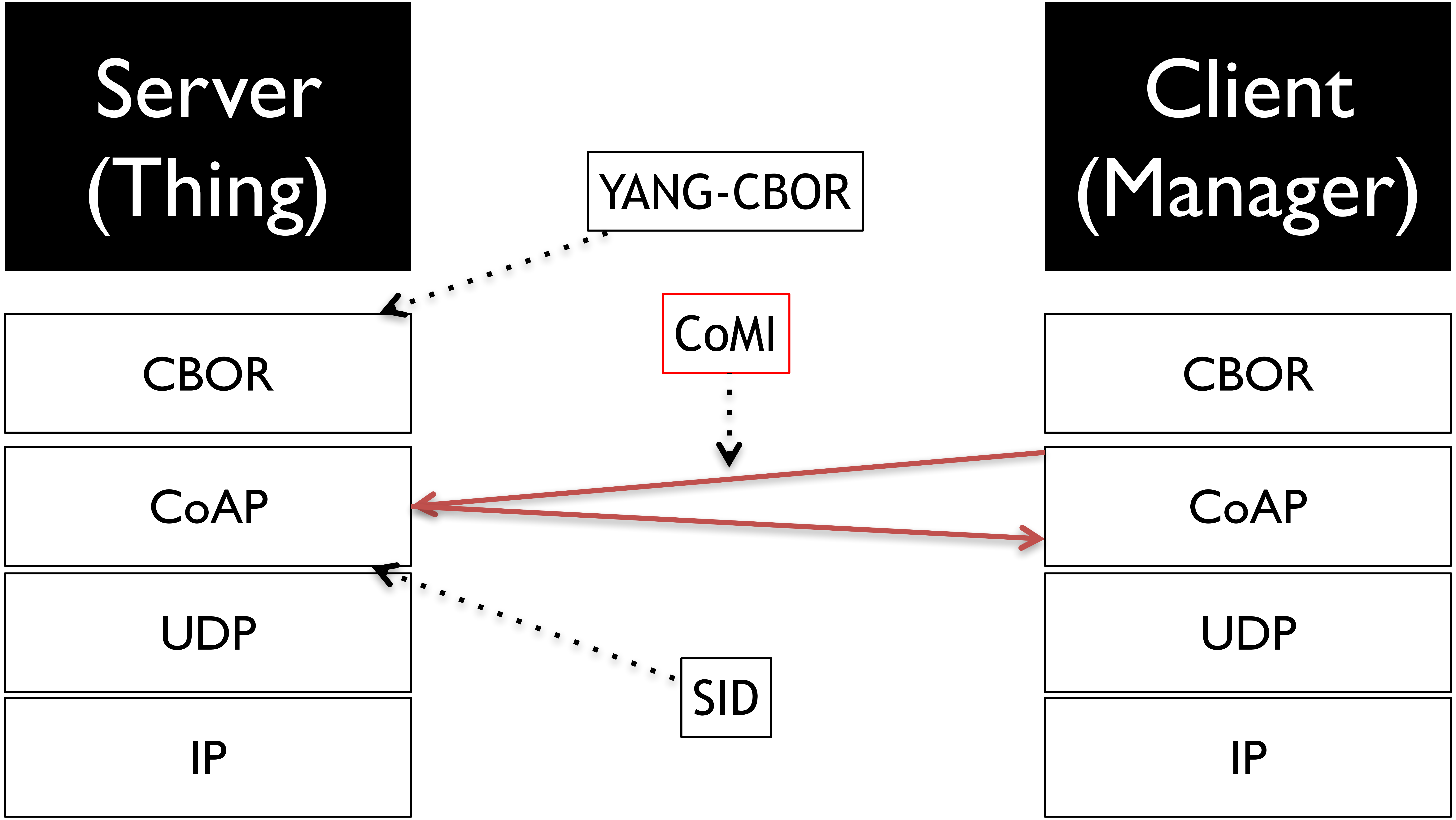
Client (Manager)

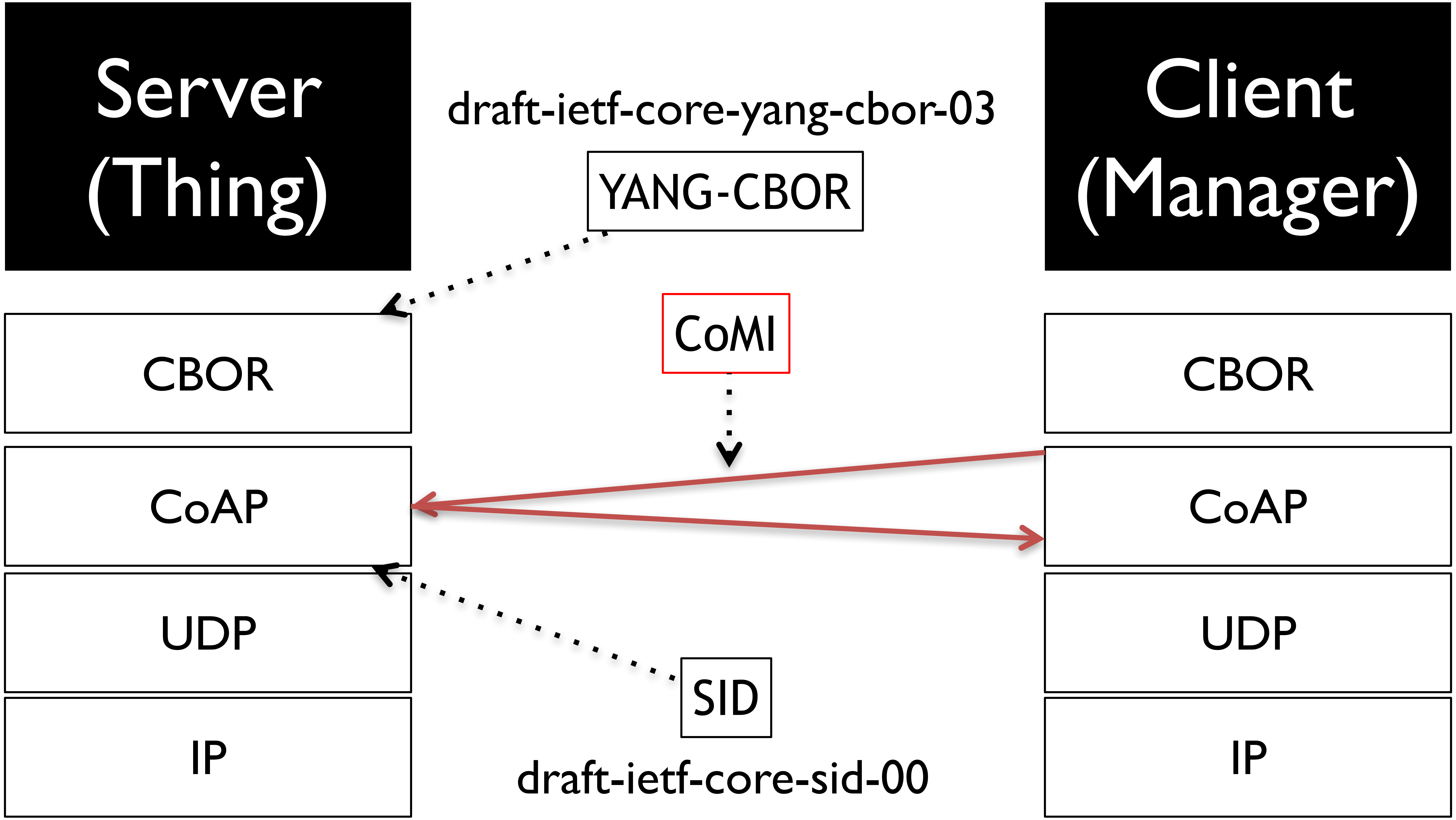
CBOR

CoAP

UDP

IP


Server
(Thing)
YANG-CBOR
Client
(Manager)
CBOR
CoMI
CBOR
CoAP
CoAP
UDP
UDP
SID
IP
IP



Server (Thing)

draft-ietf-core-yang-cbor-03

YANG-CBOR

Client (Manager)

CBOR

CoMI

CBOR

CoAP

CoAP

UDP

UDP

IP

SID

draft-ietf-core-sid-00

IP

Work

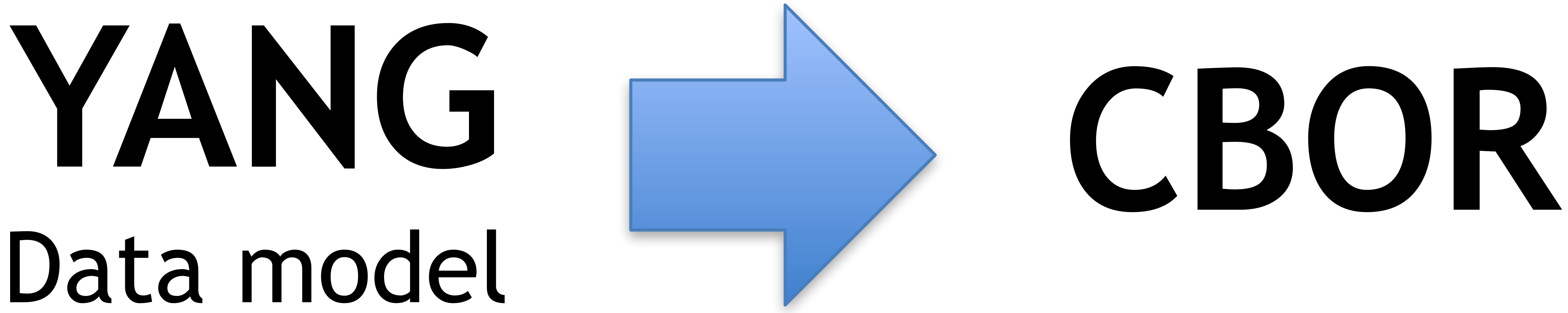
- Since IETF96
  - Design team work done
    - Now all discussions will be @CoRE ML
  - All core drafts out
    - YANG-CBOR almost complete
    - SID – can be completed by next IETF
- CoMI is the main draft
  - CoOL will be for more advanced/extended features
  - Can be completed by next IETF

YANG-CBOR mapping
draft-ietf-core-yang-cbor-03

Michel Veillette
Alexander Pelov
Abhinav Sumaraju
Randy Turner
Ana Minaburo

Goal

Define the serialization rules to encode YANG data nodes in CBOR



YANG

Data model

CBOR

I-D. ietf-netmod-yang-json performs the same task for JSON. The table of content of both drafts are similar.

What YANG has?

- Simple data types
  - unsigned integer, integer, string, enumeration, bits, binary, empty
- Unions
- Labels (identity)
- References to labels, data items, etc.
- Collections
  - Sets, lists
- Structures (composite types)

What YANG has?

- Simple data types
  - unsigned integer, integer, string, enumeration, bits, binary, empty

✓ **CBOR types**

- Unions
- Labels (identity)
- References to labels, data items, etc.
- Collections
  - Sets, lists
- Structures (composite types)

What YANG has?

- Simple data types ✓ **CBOR types**
  - unsigned integer, integer, string, enumeration, bits, binary, empty
- Unions * ✓ **Tagged CBOR types**
- Labels (identity)
- References to labels, data items, etc.
- Collections
  - Sets, lists
- Structures (composite types)

What YANG has?

- Simple data types ✓ **CBOR types**
  - unsigned integer, integer, string, enumeration, bits, binary, empty
- Unions * ✓ **Tagged CBOR types**
- Labels (identity)
- References to labels, data items, etc. * ✓ **Name / SID**
- Collections
  - Sets, lists
- Structures (composite types)

What YANG has?

- Simple data types
  - unsigned integer, integer, string, enumeration, bits, binary, empty

✓ **CBOR types**

- Unions * ✓ **Tagged CBOR types**

- Labels (identity)
- References to labels, data items, etc. * ✓ **Name / SID**

- Collections
  - Sets, lists
- Structures (composite types)

✓ **CBOR maps**
CBOR arrays

From last time

- Main issues fixed from last time
  - Use CBOR decimal fractions for Decimal64
  - Unions
    - Always Add a CBOR Tag to distinguish between CBOR ints
      - TODO: allocate 4 tags for explicit
  - Enumerations
    - Always encode as integer

Conclusion on YANG-CBOR

- draft-ietf-core-yang-cbor is almost ready
  - Initial implementations ongoing
- Next steps...
  - Submit finalized version by end of January
- Intermediate interop in February
- Interop meeting in Chicago
- Question
  - Discuss on NETMOD?

- Please, read the draft – the wording may need improvement, are the examples enough?

All times are in time-warped KST

Friday (120 min)

- **09:30–09:30 Intro**
- **09:30–09:50 SenML (AK)**
- **09:50–10:00 SenML BTO (CG)**
- **10:00–10:40 Management over CoAP (COMI/COOL)**
  - **10:00–10:10 YANG over CBOR (AP)**
  - **10:10–10:20 SIDs**
  - **10:20–10:40 COMI/COOL**
- **10:40–11:00 Redirect (DT)**
- **11:00–11:10 YANG/LWM2M (PV)**
- **11:10–11:20 RFC6690 update (prefixes) (CG)**
- **11:20–11:30 Flextime**

Schema Item iDentifier (SID)
draft-ietf-core-sid-00

Abhinav Sumaraju
Michel Veillette
Alexander Pelov
Randy Turner
Ana Minaburo

Refresher

- Compact, globally unique identifier
- Fix, unaltered by revisions (modules, includes, imports)
- Assigned to YANG items
  - Modules & Submodules
  - Features
  - Data nodes
  - RPCs & Actions
  - Notifications
  - Identities
- Allocated by range
- Multiple disjoint ranges can be assigned to a module.

SID

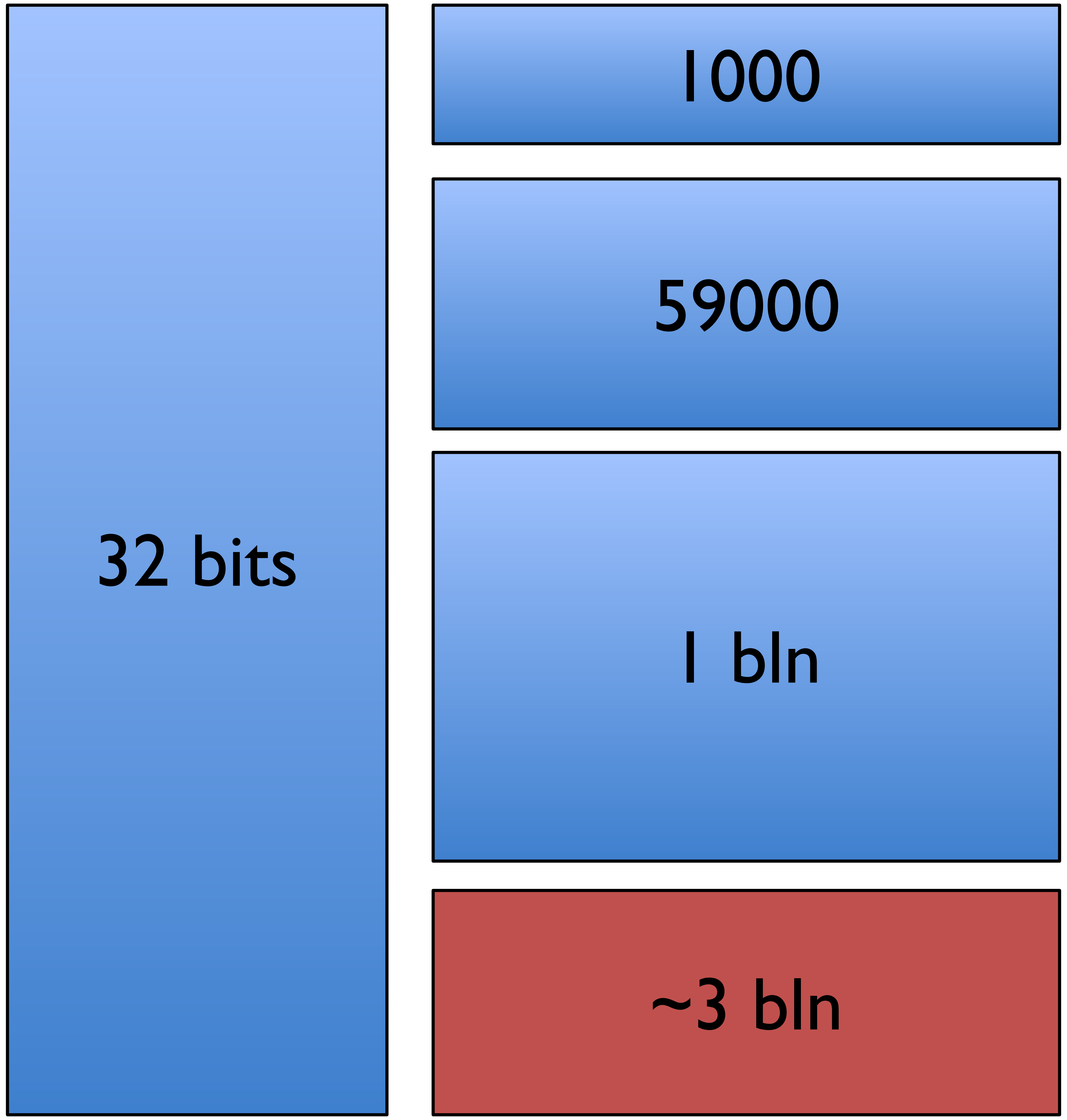
- It’s a number !
  - Assigned to “items” in the YANG schema (data items, modules, etc. etc.)
  - Use the number instead of RESTCONF/YANG name
- An assigned number never changes
  - Globally unique and stable
  - Initial space is 32 bits (future is 64 bits+)

.SID

- It’s a file !
  - YANG identifier <-> the allocated number

```
...
{ "type": "identity", "label": "toaster:toast-type", "sid": 20003 },
{ "type": "identity", "label": "toaster:wheat-bread", "sid": 20004 },
{ "type": "identity", "label": "toaster:white-bread", "sid": 20005 },
...
```

It’s an allocation system



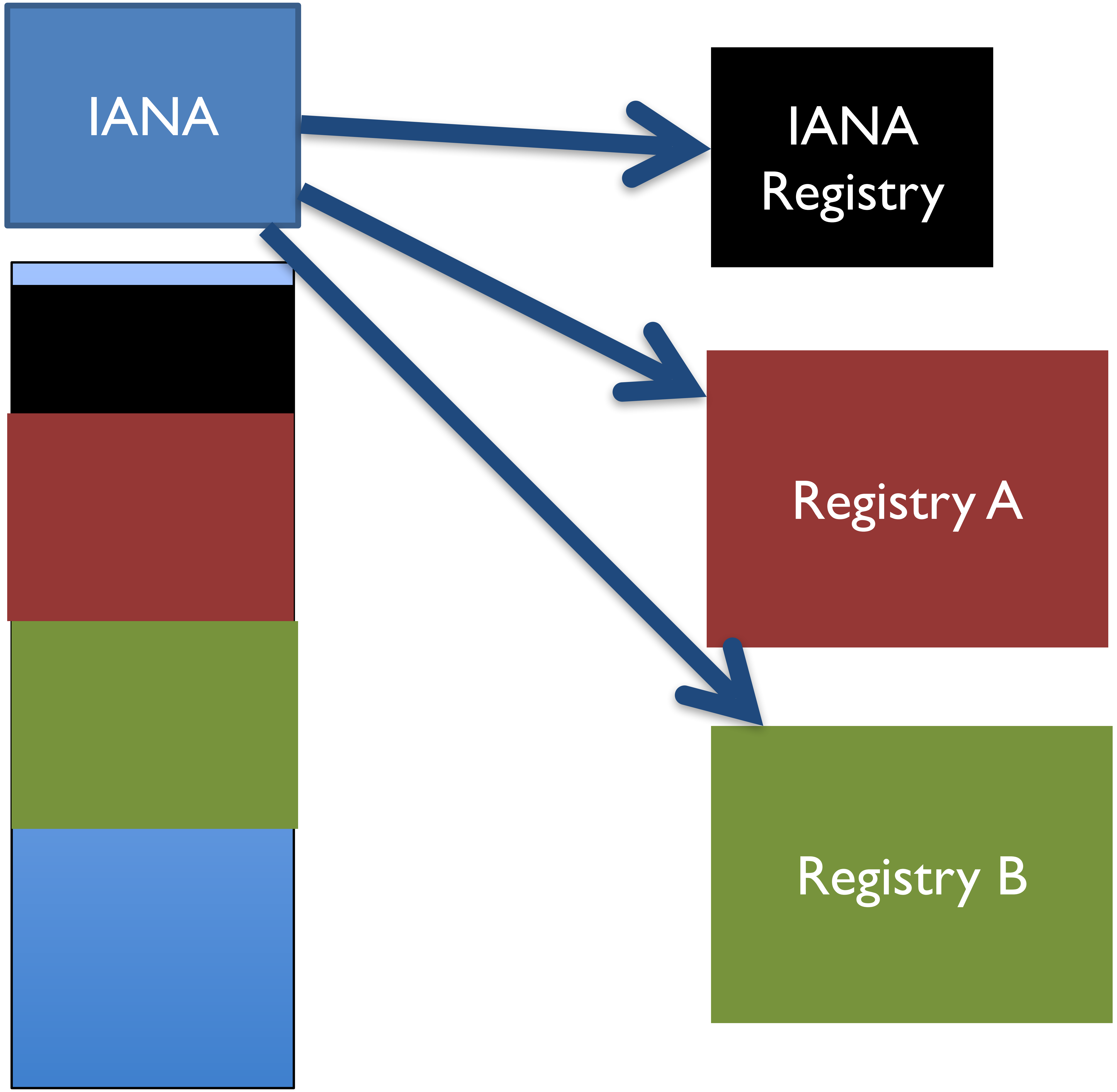
32 bits

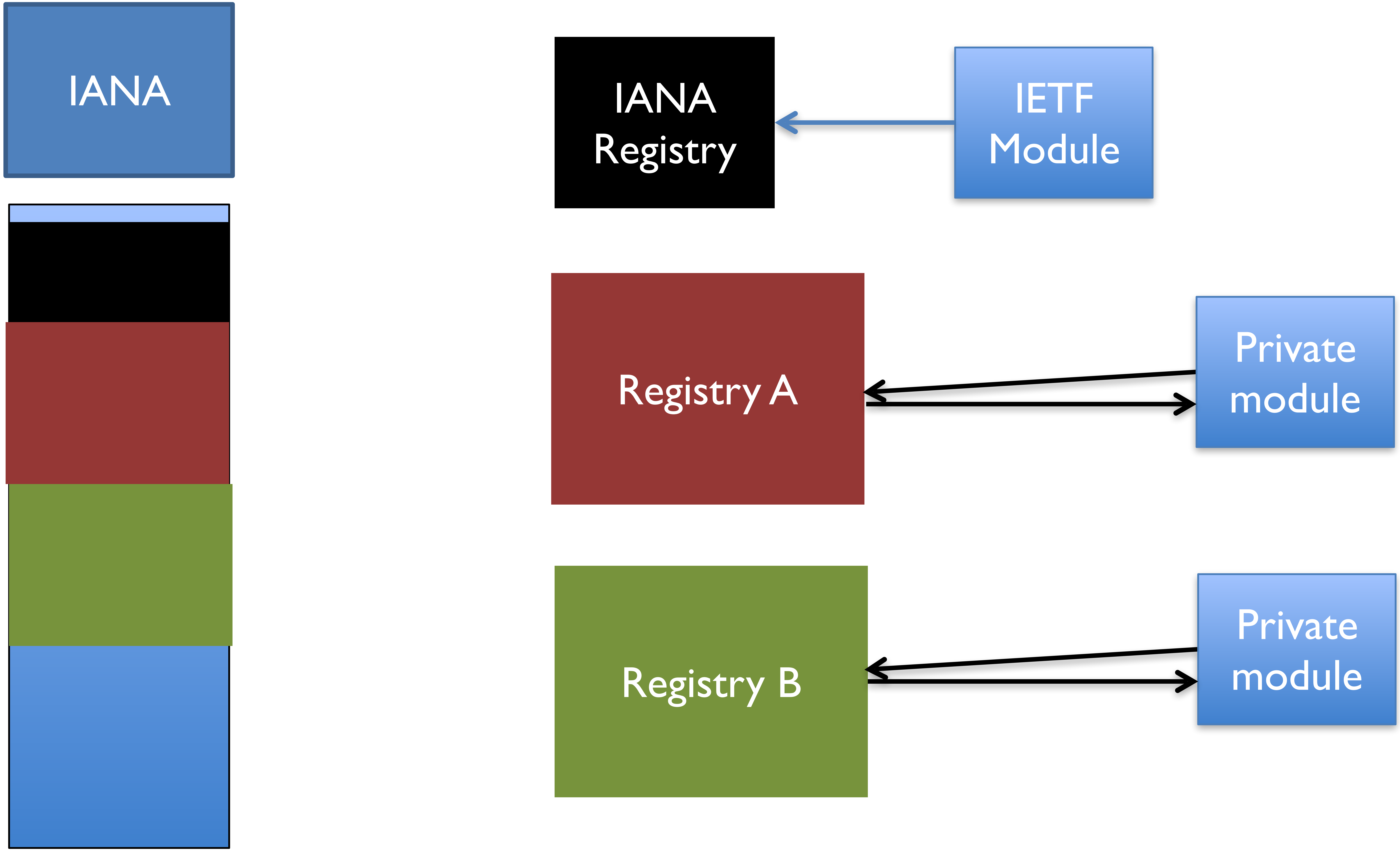
1000 — IETF / IESG expert review

59000 — Specification and associated ".yang" and ".sid" files required

1 bln — First-come, first-served basis
(IANA talks on defining this)
- 1’000’000 per third-party registrars (Expert review)

~3 bln — Reserved


IANA
IANA Registry
Registry A
Registry B



IANA

IANA Registry

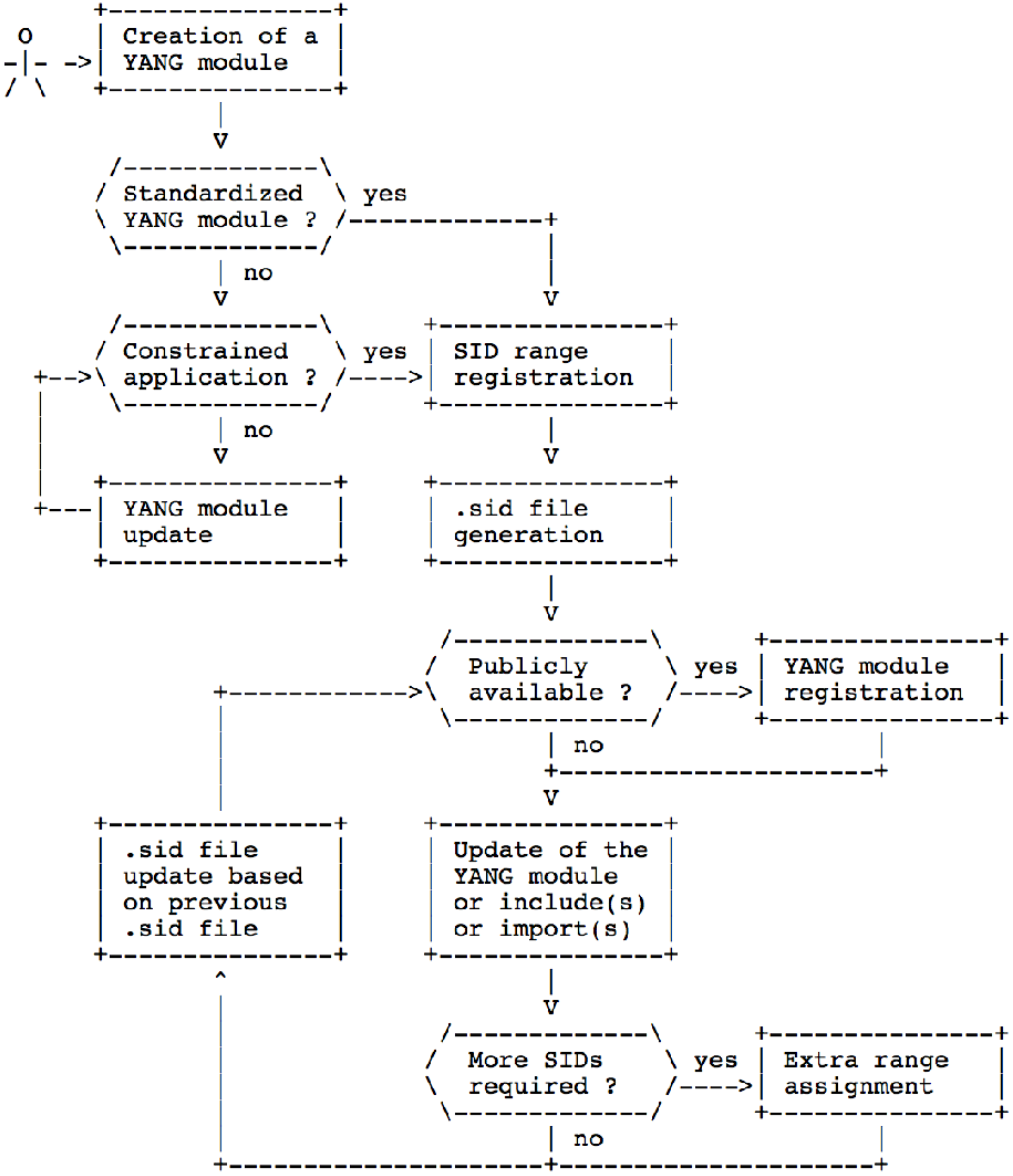
IETF Module

Registry A

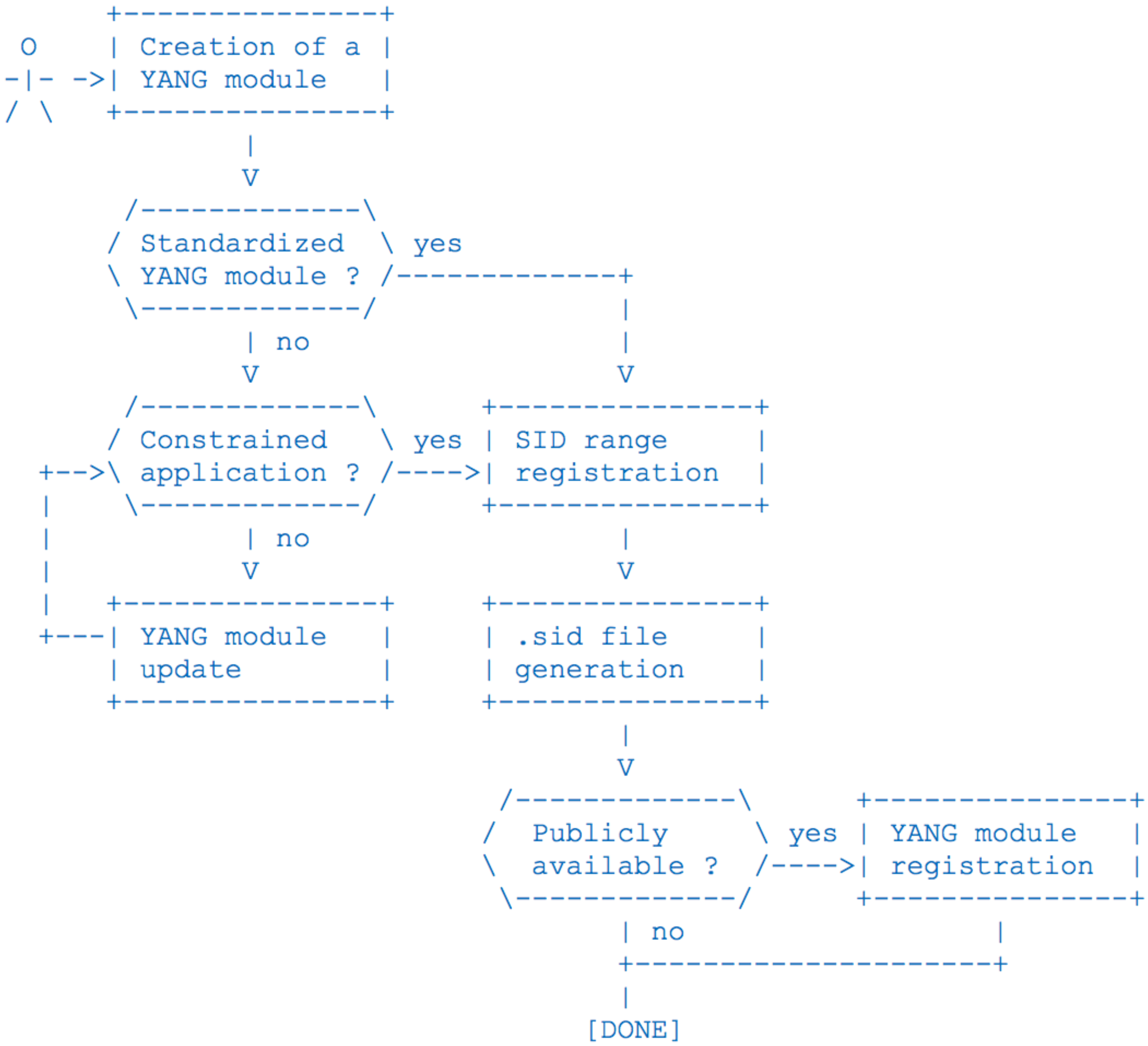
Private module

Registry B

Private module



```
      +---------------+
 o    | Creation of a |
-|- ->| YANG module   |
/ \   +---------------+
              |
              V
       /-------------\
      / Standardized  \ yes
      \ YANG module ? /-------------+
       \-------------/              |
              | no                  |
              V                     V
       /-------------\      +---------------+
      / Constrained   \ yes | SID range     |
  +-->\ application ? /---->| registration  |
  |    \-------------/      +---------------+
  |           | no                  |
  |           V                     V
  |   +---------------+     +---------------+
  +---| YANG module   |     | .sid file     |
      | update        |     | generation    |
      +---------------+     +---------------+
                                    |
                                    V
                             /-------------\      +---------------+
                            /  Publicly     \ yes | YANG module   |
              +------------>\  available ?  /---->| registration  |
              |              \-------------/      +---------------+
              |                     | no                  |
              |                     +---------------------+
              |                     V
      +---------------+     +---------------+
      | .sid file     |     | Update of the |
      | update based  |     | YANG module   |
      | on previous   |     | or include(s) |
      | .sid file     |     | or import(s)  |
      +---------------+     +---------------+
              ^                     |
              |                     V
              |              /-------------\      +---------------+
              |             /  More SIDs    \ yes | Extra range   |
              |             \  required ?   /---->| assignment    |
              |              \-------------/      +---------------+
              |                     | no                  |
              +---------------------+---------------------+
```



```
      +---------------+
 O    | Creation of a |
-|- ->| YANG module   |
/ \   +---------------+
              |
              V
       /-------------\
      / Standardized  \ yes
      \ YANG module ? /-------------+
       \-------------/              |
              | no                  |
              V                     V
       /-------------\      +---------------+
      / Constrained   \ yes | SID range     |
  +-->\ application ? /---->| registration  |
  |    \-------------/      +---------------+
  |           | no                  |
  |           V                     V
  |   +---------------+     +---------------+
  +---| YANG module   |     | .sid file     |
      | update        |     | generation    |
      +---------------+     +---------------+
                                    |
                                    V
                             /-------------\      +---------------+
                            /  Publicly     \ yes | YANG module   |
                            \  available ?  /---->| registration  |
                             \-------------/      +---------------+
                                    | no                  |
                                    +---------------------+
                                    |
                                  [DONE]
      +----------------+
 O    | Update of the  |
-|- ->| YANG module    |
/ \   | or include(s)  |
      | or import(s)   |
      +----------------+
               |
               V
       /--------------\      +----------------+
      /  More SIDs     \ yes | Extra range    |
      \  required ?    /---->| assignment     |
       \--------------/      +----------------+
               | no                   |
               +----------------------+
               |
               V
      +----------------+
      | .sid file      |
      | update based   |
      | on previous    |
      | .sid file      |
      +----------------+
               |
               V
       /--------------\      +----------------+
      /  Publicly      \ yes | YANG module    |
      \  available ?   /---->| registration   |
       \--------------/      +----------------+
               | no                   |
               +----------------------+
               |
             [DONE]
```

Conclusion and questions

- Keep one scheme or split in two?
- Ranges of SIDs
  - Revisit some of the values

- There will be some questions on policy of registrar allocation
  - Passionate IANA stuff
  - We want HATEOAS for the YANG schema discovery

- Read the draft, make comments, raise issues…

- Goal
  - Have the REGISTRY running for IETF99
  - Last call WG in March

All times are in time-warped KST

Friday (120 min)

- **09:30–09:30 Intro**
- **09:30–09:50 SenML (AK)**
- **09:50–10:00 SenML BTO (CG)**
- **10:00–10:40 Management over CoAP (COMI/COOL)**
  - **10:00–10:10 YANG over CBOR (AP)**
  - **10:10–10:20 SIDs**
  - **10:20–10:40 COMI/COOL**
- **10:40–11:00 Redirect (DT)**
- **11:00–11:10 YANG/LWM2M (PV)**
- **11:10–11:20 RFC6690 update (prefixes) (CG)**
- **11:20–11:30 Flextime**

CoRE working group

CoAP Management Interface
draft-vanderstok-core-comi-10

P. van der Stok, A. Bierman, A. Pelov, M. Veillette

State with respect to version 9

Current version 10

- Conversion of names to SID from ietf-core-sid with delta encoding
- Use iPATCH and FETCH from ietf-core-etch
- YANG to CBOR from ietf-core-yang-cbor
- List instance access simplified
- Content-format in construction e.g. bormann-appsawg-cbor-merge-patch
- query parameters changed.
- default handling changed

CoMI specifies basic access to YANG servers

Extensions will be proposed as CoOL.

Syntax examples (1)

GET /c/<instance-identifier> [retrieve a data node]
2.05 Content
<data node value>

<instance-identifier> can be leaf, leaf-list, container, list, list instance
or anyxml, anydata (under discussion)

For example:
GET coap://example.com/c/a1 [retrieves “clock” node]
GET coap://example.com/c/Bf4?k=“eth0” [retrieves “description” leaf of “interface” list instance]

a1= 1717; Bf4=1537

Same syntax for DELETE, POST, PUT

Syntax examples (2)

iPATCH /c [delete/replace/add set of data node instances of datastore]

<set of (identifier:value) pairs>

2.04 Changed

FETCH /c [retrieve part(s) of datastore]

<CBOR array of instance identifiers>

2.05 Content

Instance identifier is SID or CBOR array of list SID, followed by key values

Example: [1717, [-186, “eth0”]]

1719-186=1533

Syntax examples (3)

POST /c/<instance identifier> [execute RPC or ACTION]

<input node value>

2.05 Content

<output node value>

GET /c/s observe(0) [receive notification from default stream]

2.05 Content

<set of data node instances>

Differences with RESTCONF

RESTCONF	CoMI
HTTP/TCP	CoAP/UDP
JSON/XML	CBOR
YANG names	Numeric identifiers (SID)
Insert, Insertion - modes	No ordering
Start/Stop events	No timing assumed
Fields parameter	Not supported
Filter query (content, depth, ….)	Not supported
3 default values	Only trim mode
URI …./instance=number/….	URI …..?k=number

Next steps and to be discussed

- Remove “TODOs”
- Error handling extended
- Discuss notification/stream functionality
- Data model discovery (CoOL ?)
- Remove mistakes and Typooes

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

Privacy and CoAP Redirects

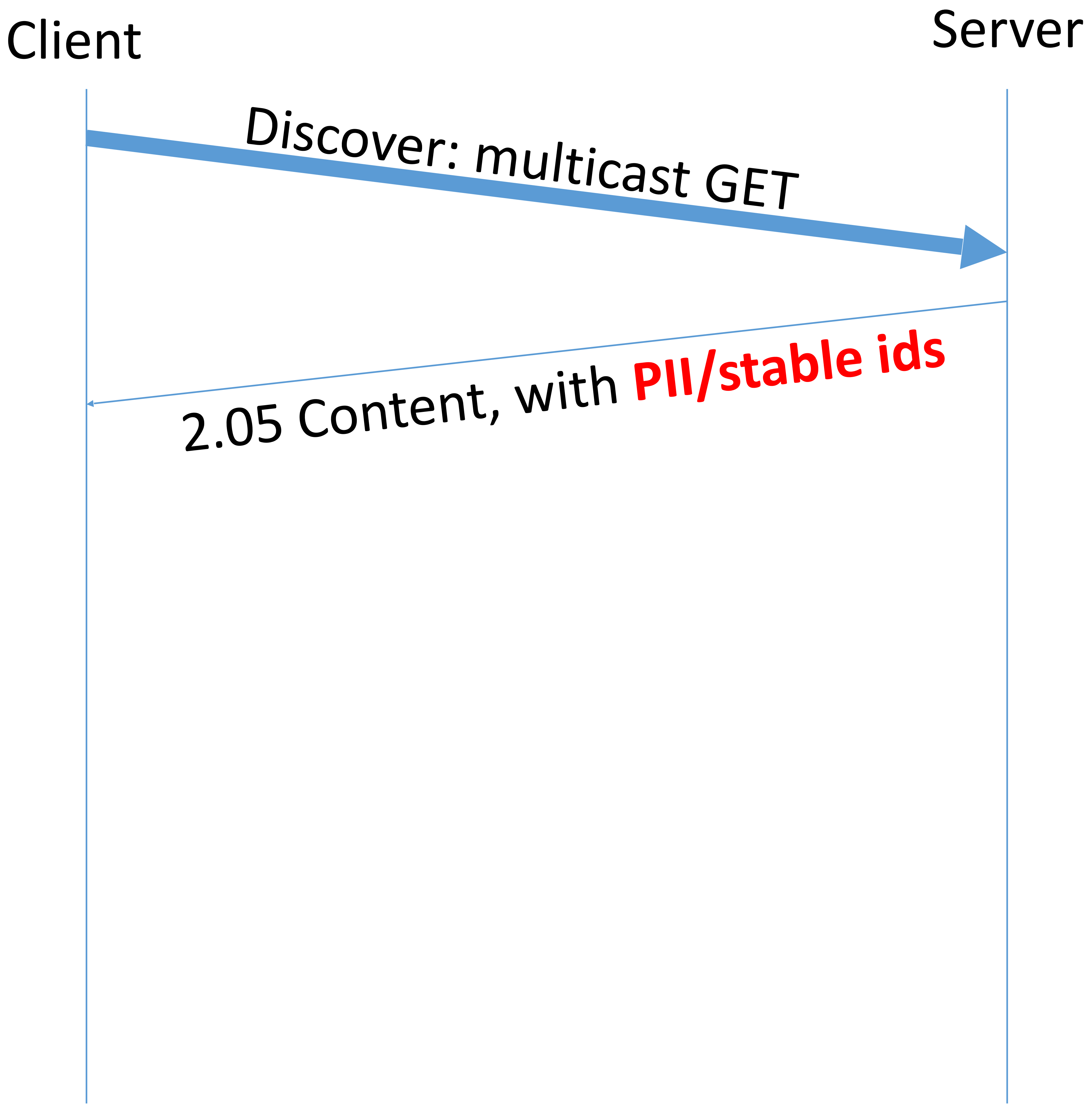
https://tools.ietf.org/html/draft-thaler-core-redirect

Background

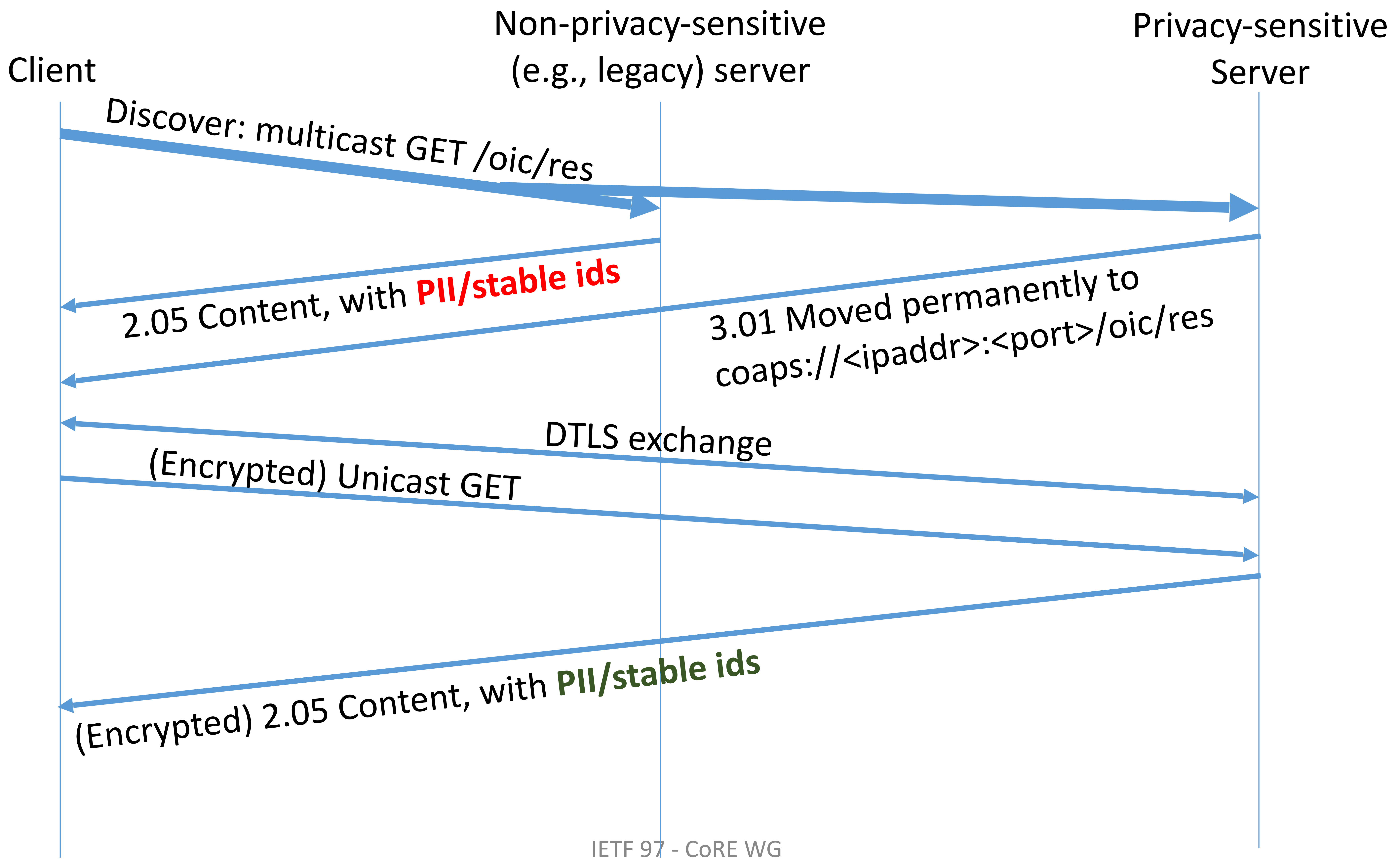
Open Connectivity Foundation (OCF) does IoT schemas, certification, etc.

- OCF uses COAP
- OCF does not want to fork COAP
- OCF found privacy issues
- OCF needs some solution regardless of whether IETF or not
- OCF strongly prefers a generic (non-OCF-specific) solution
- OCF prefers it be done by IETF

Today’s problem with PII and stable id’s



With redirect



Client

Non-privacy-sensitive (e.g., legacy) server

Privacy-sensitive Server

Discover: multicast GET /oic/res

2.05 Content, with **PII/stable ids**

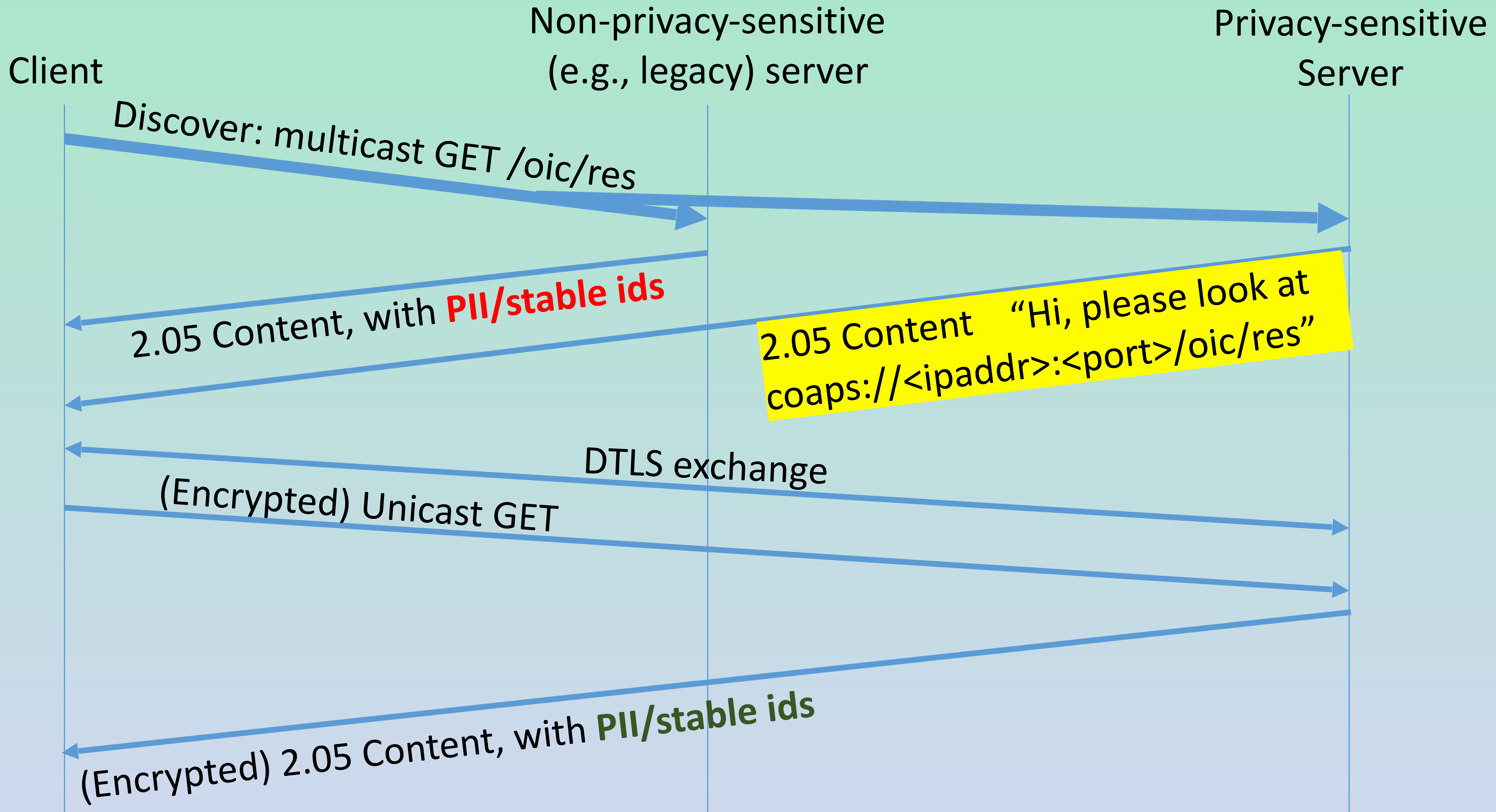
3.01 Moved permanently to coaps://<ipaddr>:<port>/oic/res

DTLS exchange

(Encrypted) Unicast GET

(Encrypted) 2.05 Content, with **PII/stable ids**

Sketch for an approach without redirect


Client
Non-privacy-sensitive
(e.g., legacy) server
Privacy-sensitive
Server
Discover: multicast GET /oic/res
2.05 Content, with PII/stable ids
2.05 Content “Hi, please look at coaps://<ipaddr>:<port>/oic/res”
DTLS exchange
(Encrypted) Unicast GET
(Encrypted) 2.05 Content, with PII/stable ids

Alternatives considered

- Use a Resource Directory
  - Same issue can arise with discovering RD to start with
  - Don’t want to have to depend on deploying an RD in all cases
- Use a success response with different content
  - More complex & error-prone since requires each relevant entity handler (e.g., app) to be aware rather than base coap layer in one place
  - Different from other protocols (http, etc.)
- Alternative-Address option in coap-tcp-tls
  - Requires same URI scheme, so cannot redirect from coap to coaps
- Use a multicast security mechanism
  - Good if it can exist longer term, but don’t see it happening soon

Details

- RFC 7252 today:
  - Location-Path and Location-Query already exist
  - Other values reserved for future Location-* options
- Add Option numbers for Location-Scheme and Location-Authority
- Add Response Code “3.01 Moved Permanently” for parity with HTTP

Redirect alone is not sufficient

There is a separate CFRG problem:

- one must also use an authentication scheme that does not reveal a stable identifier to clients before authentication is complete
- mutual auth schemes exist (e.g., “secret handshake” paper in SOSP 2003) that only reveal the identity of both endpoints if authentication succeeds, but not yet available in current standards and popular code bases

Discussion

- WG adoption?

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

CoRE Working Group

Mapping LWM2M model to CoMI YANG
draft-vanderstok-core-yang-LWM2M-00

Peter van der Stok, Jaime Jiménez

Purpose

Motivation: Difficult to understand differences and commonality between CoMI/YANG and OMA LWM2M (advantages, disadvantages)

This Draft: specifies an automatic mapping from a LWM2M xml-based device specification to a YANG MODULE for CoMI consumption.

Purpose: better understanding of relations between YANG Module and OMA LWM2M specification

Info: CoMI at IETF (draft-vanderstok-core-comi-10) describes a network management interface based on CoAP and YANG.

Method

- Standard organizations use hierarchical models that can be specified in XML and describe classes with attributes and operations that can be instantiated on servers.

- OMA LWM2M and IPSO standardize numbered object types and resources.

- YANG module specifies data models with named objects and leafs.

- Goal: Specify a mapping from a LWM2M xml-based device specification to a YANG MODULE for CoMI consumption.

Example: Humidity Object

Object definition

Name	Object ID	Instances	Mandatory	Object URN
Humidity	3304	Multiple	Mandatory	urn:oma:lwm2m:ipso:3304

Resource definitions

ID	Name	Operations	Instances	Mandatory	Type	Units	Description
5700	Sensor Value	R	Single	Mandatory	Float	…	…
5601	Min Measured Value	R	Single	Optional	Float	…	…
5602	Max Measured Value	R	Single	Optional	Float	…	…
5603	Min Range Value	R	Single	Optional	Float	…	…
5604	Max Range Value	R	Single	Optional	Float	…	…
5701	Sensor Units	R	Single	Optional	String	…	…
5605	Reset Min and Max	E	Single	Optional	Opaque	…	…

Conversion Rules

LWM2M	YANG (RFC6020)
optional /mandatory attribute	Mandatory false/true statement
R, W attributes	Config statement (False=R, True=W)
E attribute	YANG RPC/ACTION
range attribute	range statement
units	units statement
201 device	YANG list
resources	leafs of device YANG list
object Instance	YANG List instance identified with key

URI Conversion

LWM2M	YANG
URI: coap+lwm2m://example.com/object/instance/resource	RESTCONF URI (example 3): http://example.com/object/instance=number/resource
	CoMI URI (example 3): coap://example.com/c/identifier?k=number if only one instance then coap://example.com/c/identifier

- ?k=number, as query parameter for instance number.
- /c signifies comi server data (discovery returned)
- /identifier equals object*1000 + resource

Generated YANG module

```
module: ietf-yang-humidityNM
     +--ro IPSO-humidity* [instance_number]
        +--ro instance_number          uint16
        +--ro Sensor_Value             decimal64
        +--ro Units?                   string
        +--ro Min_Measured_Value?      decimal64
        +--ro Max_Measured_Value?      decimal64
        +--ro Min_Range_Value?         decimal64
        +--ro Max_Range_Value?         decimal64
        +---x Reset_Min_and_Max_measured_values
```

[ ]	list keys
rw	configuration data (read and write)
ro	state data (read only)
*	list and leaf list
x	action

Takeaways

- Example 1 (module: ietf-yang-humidityID) is a bit forced and lacks the Resource Name.
- Example 2 (module: ietf-yang-humidityNM) seems to be the best fit.
- Example 3 (ietf-yang-humidityLF) seems too complex.
- Both .XML (3482 characters) and .YANG (4570 characters) have a lot of “noise” in them.
- YANG is much more expressive than LWM2M,
- There are many design choices for the mapping algorithm.
- Key leafs are just one possible way to represent instances.
- Access Control mapping might be done better.
- YANG has no Float, we use 64 bit precision (float is 32).
- Need to script automatic conversion.
- Where would a converter run? GWs, devices, server?

Links

- https://tools.ietf.org/html/rfc6020
- http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/oma-lightweightm2m-v1-0
- http://ipso-alliance.github.io/pub/
- (Preliminary work) http://jaimejim.github.io/drafts/draft-vanderstok-core-yang-lwm2m-00.txt
- jaimejim.github.io/drafts/3304.xml
- jaimejim.github.io/drafts/3304.yang

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
  - 10:00–10:10 YANG over CBOR (AP)
  - 10:10–10:20 SIDs
  - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime

Addition of organisation prefix to RFC6690 IANA CoRE parameters registration

draft-groves-core-rfc6690up-00

IETF #97 Seoul

Christian Groves

Problem

- RFC6690 defines IANA registration procedures for resource type (rt) and interface description (if) link attributes.
- Each link attribute must have a separate IANA registration.
- Potentially there will be 100s (1000s?) of resource types. Interfaces likely to be less.

Result

- More work all around (organisations, IANA, expert etc.)
- Delay in registration
- Or not at all (too hard)

Proposal – Update to RFC6690

- Allow for a organizational prefix to be registered.
- Allowing organizations to manage their namespace.
- To do so they must provide a specification indicating the rules for the namespace.
- MUST comply with RFC6690 conventions
- SHOULD provide a reference to where registrations can be found.

OCF

- Have had feedback from several OCF members that they support the approach.
- Proposal for a prefix “x.” that allows a reverse domain name to be used without registration.

  e.g. “x.org.openconnectivity.r.widget”

  Organizational prefix used for compactness:

  e.g. “oic.r.widget”

Next Steps

- Is there any support to the prefix mechanism?
- Is there any support to add an “x.” prefix for reverse domain names?

All times are in time-warped KST

Friday (120 min)

- 09:30–09:30 Intro
- 09:30–09:50 SenML (AK)
- 09:50–10:00 SenML BTO (CG)
- 10:00–10:40 Management over CoAP (COMI/COOL)
    - 10:00–10:10 YANG over CBOR (AP)
    - 10:10–10:20 SIDs
    - 10:20–10:40 COMI/COOL
- 10:40–11:00 Redirect (DT)
- 11:00–11:10 YANG/LWM2M (PV)
- 11:10–11:20 RFC6690 update (prefixes) (CG)
- 11:20–11:30 Flextime