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 CDT

Tuesday (90 min)

- **13:00–13:10 Intro, Agenda, Status**
- **13:10–13:25 Post-WGLC: CoAP-TCP, Links-JSON**
- **13:25–13:40 Up for WGLC: CoCoA, RD**
- **13:40–14:00 Management over CoAP (COMI)**
- **14:00–14:30 Object Security (OSCOAP)**

All times are in time-warped CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

Milestones (from WG charter page)

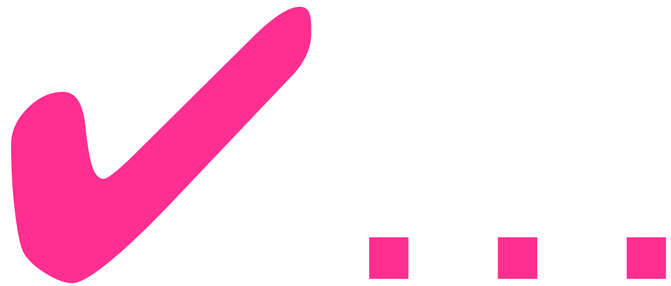
http://datatracker.ietf.org/wg/core/charter/

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
Done	**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
Done	**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 — RFC 8075**
Done	**Blockwise transfers in CoAP submitted to IESG — RFC 7959**

draft-ietf-core-http-mapping
→ RFC 8075

Published 2017-02-28

draft-ietf-core-etch
→ RFC 8132-to-be



In AUTH48 since 2017-03-20

LPWAN

SCHC for CoAP

draft-ietf-lpwan-coap-static-context-hc-01

Ana Minaburo – Laurent Toutain

IETF 98 - Chicago

CoAP Compression

- LPWAN: new category of network
  - Limited payload (10 B to 200 B)
- SCHC: Static Context Header Compression
  - Fixed number of flows, star topology
  - SCHC for IPv6 and UDP
  - SCHC for CoAP
    - Reduce field size, multiple fields, asymmetry
- lpwan meeting: Wednesday 1300-1500

Time for more Interops

- OSCOAP already had two virtual interops
- CoAP-TCP/-TLS/-Websockets?
- Links-JSON?
- Etch?
- SenML?

- RFCs are implementation drafts
- Which other ones are?

- Plan: about monthly (end of month) Apr, May, June
- Get ETSI support for a Prague Interop?

All times are in time-warped CDT

Tuesday (90 min)

- 13:00–13:10 Intro, Agenda, Status
- 13:10–13:25 Post-WGLC: CoAP-TCP, Links-JSON
- 13:25–13:40 Up for WGLC: CoCoA, RD
- 13:40–14:00 Management over CoAP (COMI)
- 14:00–14:30 Object Security (OSCOAP)

coap-tcp-tls @ IETF 98

Brian Raymor

coap-tcp-tls-06

- Resolved 33 issues from Working Group Last Call (1)
- Added Securing CoAP section and informative reference to OSCOAP
- Removed the Server-Name and Bad-Server-Name Options
- Clarified the Capability and Settings Message (CSM) exchange
- Updated Pong response requirements

coap-tcp-tls-07

- Resolved issues from Working Group Last Call (2) – feedback from Esko Dijk
- Added guidance on malformed / message format errors
- Added Semantics for multiple Alternative-Address
- Status: Submitted to IESG for Publication

coap-tcp-tls-08 (pending)

- Resolved issues – mostly editorial
- Addressed URI Fragment identifiers [RFC7252 erratum]

Next Steps

- AD Review for coap-tcp-tls-07 is completed
- IETF Last call announced - March 26 - April 9
- Carsten: *… should we stage an interop event?*

Core-Links-JSON

- Decided to cut down grand claims in Berlin
- No technical changes

- Finished 2nd WGLC now; preparing write-up

All times are in time-warped CDT

Tuesday (90 min)

- 13:00–13:10 Intro, Agenda, Status
- 13:10–13:25 Post-WGLC: CoAP-TCP, Links-JSON
- 13:25–13:40 Up for WGLC: CoCoA, RD
- 13:40–14:00 Management over CoAP (COMI)
- 14:00–14:30 Object Security (OSCOAP)

CoAP Simple Congestion Control/Advanced (CoCoA)

draft-ietf-core-cocoa-01

Carsten Bormann – Universität Bremen TZI
cabo@tzi.org
August Betzler, Carles Gomez, Ilker Demirkol
Universitat Politècnica de Catalunya
carlesgo@entel.upc.edu

Status

- WG document since October 2016

- Last update is -01
  - Mostly stable
  - New Appendix B: "Supporting evidence"
  - Update of weak estimator discussion (4.2.2)
    - RFC 8085 "UDP Usage Guidelines"

Updates in -01 (I/II)

- Appendix B. Supporting evidence
  - Summary of evaluation results plus references
  - Overall result
    - CoCoA: adaptive, good use of RTT sample
    - Default CoAP: insensitive to network conditions
  - Throughput/PDR, settling time, fairness, latency
  - NONs
  - Also references on early versions of CoCoA
- **Question for the WG:**
  - **Should this Appendix be included if/when the document is published?**

Updates in -01 (II/II)

- 4.2.2. Discussion (measured RTO estimate)
  - CoCoA uses *strong* and *weak* RTTs
  - RFC 8085:
    - "latency samples MUST NOT be derived from ambiguous transactions"
  - However, weak RTTs are not combined into the strong estimator
    - Used to correct the limited knowledge from strong RTTs by employing an additional RTT estimator
    - Evidence from experiments appears to support that this is beneficial (see Appendix B)

Running code

- Californium (Cf) with CoCoA is publicly available
  - Cf: CoAP implementation for unconstrained devices
  - https://github.com/eclipse/californium
    - cf-cocoa example
    - org.eclipse.californium.core.network.stack.congestioncontrol
- CoCoA implementation for Erbium (Er)
  - Er: official CoAP implementation for Contiki OS
- libcoap ported to Android with CoCoA
  - By Zheng et al

WG Last Call ?

- Document ready for WGLC…
  - Minus Appendix A ?
    - Aggregate Congestion Control
    - To be extracted into a separate document ?

Thanks!

Carsten Bormann – Universität Bremen TZI
cabo@tzi.org
August Betzler, Carles Gomez, Ilker Demirkol
Universitat Politècnica de Catalunya
carlesgo@entel.upc.edu

Back-up slides

- CoCoA algorithm is stable, well performing
  - Maturity has been reached
    - Simulation, emulation, experiments
    - IEEE 802.15.4 multihop networks, GPRS, UMTS, Wi-Fi
    - CONs/NONs, different traffic patterns
    - Several alternatives tested (strong-only, PH, Linux TCP…)
- Presentations
  - IETF 87, IETF 89, IETF 90, IETF 91, IETF 92 (ICCRG), IETF 94, IETF 96

Back-up slides

- Papers or other documents on the topic
  - Evaluation Internet Draft:
    - F. Zheng, B. Fu, Z. Cao, “CoAP Latency Evaluation”, draft-zheng-core-coap-lantency-evaluation-00, 2016 (work in progress)
  - Conferences/workshops

- Bhalerao, Rahul, Sridhar Srinivasa Subramanian, and Joseph Pasquale. "An analysis and improvement of congestion control in the CoAP Internet-of-Things protocol." 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2016.

- I Järvinen, L Daniel, M Kojo, "Experimental evaluation of alternative congestion control algorithms for Constrained Application Protocol (CoAP)", IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015.

- Balandina, Ekaterina, Yevgeni Koucheryavy, and Andrei Gurtov. "Computing the retransmission timeout in coap." Internet of Things, Smart Spaces, and Next Generation Networking. Springer Berlin Heidelberg, 2013. 352-362.

Back-up slides

- Papers or other documents on the topic
  - Conferences/workshops

- A. Betzler, C. Gomez, I. Demirkol, "Evaluation of Advanced Congestion Control Mechanisms for Unreliable CoAP Communications", ACM PE-WASUN, Cancún, Mexico, 2015.

- A. Betzler, C. Gomez, I. Demirkol, M. Kovatsch, "Congestion Control for CoAP cloud services", 8th International Workshop on Service-Oriented Cyber-Physical Systems in Converging Networked Environments (SOCNE) 2014, Barcelona, Spain, Sept. 2014.

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "Congestion Control in Reliable CoAP Communication", 16th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM'13), Barcelona, Spain, Nov. 2013.

Back-up slides

- Papers or other documents on the topic
  - Journals/magazines

- A. Betzler, J. Isern, C. Gomez, I. Demirkol, J. Paradells, "Experimental Evaluation of Congestion Control for CoAP Communications without End-to-End Reliability", Ad-Hoc Networks journal (in press).

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "CoAP congestion control for the Internet of Things", IEEE Communications Magazine (accepted for publication, probably in July 2016).

- A. Betzler, C. Gomez, I. Demirkol, J. Paradells, "CoCoA+: an advanced congestion control mechanism for CoAP", Ad-hoc Networks journal, 2015.

  - Dr. August Betzler's PhD
    - A. Betzler "Improvements to End-to-End Performance of Low-Power Wireless Networks", 2015

draft-ietf-core-resource-directory-10

- Quite Stable Content
- Partially in use in other SDOs (e.g., LWM2M)
- Slow progress of i-dotting and t-stroking
- Seoul: Splitting off DNS-SD into separate document?
- Recently added editor: Christian Amsüss

Proposal: Continue with the split

- Fresh blood on DNS-SD part
- Make DNS-SD part more visible in DNS-SD community
- Run work on the same time scale (“cluster”)

Proposal: Operate with process successful for CoAP-TCP

- github, collect issues, make PRs, editor merges

draft-ietf-core-resource-directory-10

Michael Koster

Status

- Incorporated comments and resolved issues, a lot of clean-up work
- Reorganized the discovery section into RD discovery vs. resource discovery
- Cleaned up the registration API part, patch will be included
- Split lookup functions into separate resource types
- Draft split to accommodate RD mapping to DNS-SD
- Document editor assigned to do final edits

Open Questions

- Is rd-lookup optional?
- Draft Split
- [1] https://github.com/core-wg/resource-directory
- [2] https://github.com/core-wg/rd-dns-sd

Implementations

- LWM2M (Device Registration Interface)
  - Californium
  - Eclipse Leshan
  - ARM mbed server
- Other implementations
  - Christian Amsuss

All times are in time-warped CDT

Tuesday (90 min)

- 13:00–13:10 Intro, Agenda, Status
- 13:10–13:25 Post-WGLC: CoAP-TCP, Links-JSON
- 13:25–13:40 Up for WGLC: CoCoA, RD
- 13:40–14:00 Management over CoAP (COMI)
- 14:00–14:30 Object Security (OSCOAP)

draft-ietf-core-yang-cbor

- "CBOR Encoding of Data Modeled with YANG"
  - Same approach as "JSON Encoding of Data Modeled with YANG" [RFC 7951]

- Normative reference in [draft-ietf-core-comi]

- No comments received since last update (February 07)

Ready for WG last call?

CoRE working group

CoAP Management Interface
draft-ietf-core-comi-0

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

State of version 0

- 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
- Three issues:
    - iPATCH content-format
    - FETCH content-format
    - Notification payload

CoMI specifies basic access to YANG servers

PATCH content format

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

<set of (identifier: value) pairs>

2.04 Changed

Proposed:

Use draft-bormann-appsawg-cbor-merge-patch

Extends JSON-merge-patch: patching array elements with key attributes.

CoMI-only notation uses YANG spec, unknown to cbor-merge (->overhead)

Example: set **enabled** field to true in **interface** list element with **key="eth0"**

CBOR-merge: [{1537: "eth0", 1535: true}]

CoMI-only: [[1535, "eth0"]: true]

FETCH content format

FETCH /c [retrieve part(s) of datastore]
<CBOR array of instance identifiers>
2.05 Content

Possible:
Specify NEW content format for general query in CBOR document
Extends CoMI-only with wild cards, and name strings next to SIDs
Example: Select **current-datetime** and **interface** list elements with **key=“eth*”**
CBOR-select: [1717:?, [-180: “eth*”, -184: ?]]
CoMI-only: [1717, [-184, “eth0”]]

1717-184=1533

Notification payload

For single notifcation

YANG to CBOR encoding without root container

```
2.05 Content
Content-Format(application/YANG-patch+cbor)
Observe(12) Token(0x93)
{
 60010 : {
  +1 : "0/4/21",
  +2 : "Open pin 2"
 }
}
```

For multiple notifcations

YANG to CBOR encoding within a CBOR array

```
2.05 Content
Content-Format(application/YANG-patch+cbor)
Observe(12) Token(0x93)
[
 {
  60010 : {
   +1 : "0/4/21",
   +2 : "Open pin 2"
  },
  60010 : {
   +1 : "1/4/21",
   +2 : "Open pin 5"
  }
 }
]
```

Next steps

- Remove “TODOs”
- Error handling review
- Content-format review
- Insert default notification/stream functionality
- Remove mistakes and Typooes

And then WGLC

iPATCH - Example

Initial datastore content

```
{
 "system" : {                                    / SID 1715 /
  "ntp" : {                                      / SID 1750 /
   "enabled" : false,                            / SID 1751 /
   "server" : [                                  / SID 1752 /
    {
     "name" : "tic.nrc.ca",                      / SID 1755 /
     "udp" : {                                   / SID 1757 /
      "address" : "132.246.11.231",              / SID 1758 /
      "port" : 123                               / SID 1759 /
     }
    }
   ]
  }
 }
}
```

#1 Update

#2 Delete

Final datastore content

```
{
 "system" : {
  "ntp" : {
   "enabled" : true,
   "server" : [
    {
     "name" : "tac.nrc.ca",
     "udp" : {
      "address" : "132.246.11.232"
     }
    }
   ]
  }
 }
}
```

#3 Create

iPATCH – Current solution

YANG Instance-identifier (In blue)

```
iPATCH /c
[
 1751 : true,                      / Update "enabled" to true /
 [1, "tic.nrc.ca"] : null,         / Delete "server" with key "tic.nrc.ca" /
 0 : {                             / Create "server" with key "tac.nrc.ca" /
       "name" : "tac.nrc.ca",
       "udp" : {
        "address" : "132.246.11.232"
      }
     }
}
```

Value (In red)

Implementations can reuse the CoAP DELETE and PUT primitives.

```
iPatchImplementation ()
{
  For each pair {
    if value == "null"
      coapDatanodeDelete(instanceIdentifier)
    else
      coapDatanodePut(instanceIdentifier, value)
}
```

iPATCH – draft-bormann-appsawg-cbor-merge-patch

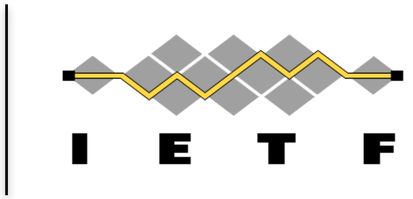
```
iPATCH /c
{
 1715 : {                       / system (SID 1715) /
  +35 : {                       / ntp (SID 1750) /
   +1 : true,                   / enabled (SID 1751) /

   +2: [                        / server (SID 1752) /
    +3 : "tac.nrc.ca",          / name (SID 1755) /
    +2 : {                      / udp (SID 1757) /
     +1 : "132.246.11.232"      / address (SID 1758) /
    }
   ]
  }
 }
}
```

"server" with key "tic.nrc.ca" can't be deleted

Specific merge logic, not based on simple DELETE and PUT datanode primitives

draft-veillette-core-yang-library



"Constrained YANG Module Library"

- Same approach as "YANG Module Library" [RFC 7895]
- Normative reference in [draft-ietf-core-comi]

```
+--ro modules-state
  +--ro module-set-id
    +--ro module* [sid revision]
      +--ro sid
      +--ro revision
      +--ro ~~schema~~?
      +--ro ~~namespace~~
      +--ro feature*
      +--ro deviation*
      |  +--ro sid
      |  +--ro revision
+--ro conformance-type
      +--ro submodule*
        +--ro sid
        +--ro revision
        +--ro ~~schema~~?
notifications:
   +---n yang-library-change
     +--ro module-set-id
```

Caching mechanism extended to multi-server

All items in red are SIDs (Integer instead of string)

"namespace" removed, not required by SID
"schema" removed, schema retrieved using module SID if needed

Enumeration (Encoded as integer instead of string)

Ready for WG adoption*?*

All times are in time-warped CDT

Tuesday (90 min)

- **13:00–13:10 Intro, Agenda, Status**
- **13:10–13:25 Post-WGLC: CoAP-TCP, Links-JSON**
- **13:25–13:40 Up for WGLC: CoCoA, RD**
- **13:40–14:00 Management over CoAP (COMI)**
- **14:00–14:30 Object Security (OSCOAP)**

References to draft-ietf-core-object-security

This is an experimental product. These dependencies are extracted using heuristics looking for strings with particular prefixes. Notably, this means that references to I-Ds by title only are not reflected here. If it's really important, please inspect the documents' references sections directly.

Showing RFCs and active Internet-Drafts, sorted by reference type, then document name.

Document	Title	Status	Type	Downref
draft-cuellar-ace-pat-priv-enhanced-authz-tokens	**Privacy-Enhanced Tokens for Authorization in ACE** Refs Ref'd by		normatively references	
draft-garcia-core-app-layer-sec-with-dtls-record	**Application Layer Security for CoAP using the (D)TLS Record Layer** Refs Ref'd by		normatively references	
draft-ietf-6tisch-dtsecurity-secure-join	**6tisch Secure Join protocol** Refs Ref'd by		normatively references	
draft-ietf-6tisch-minimal-security	**Minimal Security Framework for 6TiSCH** Refs Ref'd by		normatively references	
draft-keranen-t2trg-rest-iot	**RESTful Design for Internet of Things Systems** Refs Ref'd by		normatively references	
draft-richardson-6tisch-minimal-rekey	**Minimal Security rekeying mechanism for 6TiSCH** Refs Ref'd by		normatively references	
draft-seitz-ace-oscoap-profile	**OSCOAP profile of ACE** Refs Ref'd by		normatively references	
draft-selander-ace-eals	**Enrollment with Application Layer Security** Refs Ref'd by		normatively references	
draft-tiloca-core-multicast-oscoap	**Secure group communication for CoAP** Refs Ref'd by		normatively references	
draft-amsuess-core-request-tag	**Request-Tag option** Refs Ref'd by		informatively references	
draft-bormann-t2trg-slipmux	**Slipmux: Using an UART interface for diagnostics, configuration, and packet transfer** Refs Ref'd by		informatively references	
draft-bormann-t2trg-sworn	**SWORN: Secure Wake on Radio Nudging** Refs Ref'd by		informatively references	
draft-gerdes-ace-dtls-authorize	**Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)** Refs Ref'd by		informatively references	
draft-ietf-ace-actors	**An architecture for authorization in constrained environments** Refs Ref'd by		informatively references	
draft-ietf-ace-oauth-authz	**Authentication and Authorization for Constrained Environments (ACE)** Refs Ref'd by	Proposed Standard	informatively references	
draft-ietf-core-coap-tcp-tls	**CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets** Refs Ref'd by	Proposed Standard	informatively references	
draft-jimenez-t2trg-coap-functionality-lwm2m	**CoAP functionality expected in a LWM2M system** Refs Ref'd by		informatively references	
draft-mattsson-core-security-overhead	**Message Size Overhead of CoAP Security Protocols** Refs Ref'd by		informatively references	
draft-selander-ace-cose-ecdhe	**Ephemeral Diffie-Hellman Over COSE (EDHOC)** Refs Ref'd by		informatively references	
draft-vanderstok-ace-coap-est	**EST over secure CoAP (EST-coaps)**		informatively references	

Message Size Overhead of CoAP Security Protocols

draft-mattsson-core-security-overhead-00

John Mattsson, Ericsson

IETF 98, CoRE WG, Chicago, Mar 27, 2017

Message Size Overhead of CoAP Security Protocols

Protocol	*Overhead (B) for Sequence Number = '05'*	*Overhead (B) for Sequence Number = '1005'*	*Overhead (B) for Sequence Number = '100005'*
DTLS 1.2	29	29	29
DTLS 1.3	21	21	21
TLS 1.2	21	21	21
TLS 1.3	21	21	21
DTLS 1.2 (GHC)	16	16	17
DTLS 1.2 (Raza)	13	13	14
TLS 1.3 (GHC)	14	14	15
TLS 1.3 (Raza)	13	13	14
TLS 1.2 (GHC)	17	18	19
TLS 1.3 (GHC)	17	18	19
OSCOAP Request	13	14	15
OSCOAP Response	9	9	9

draft-mattsson-core-security-overhead –00

Object Security of CoAP (OSCOAP)

draft-ietf-core-object-security-02

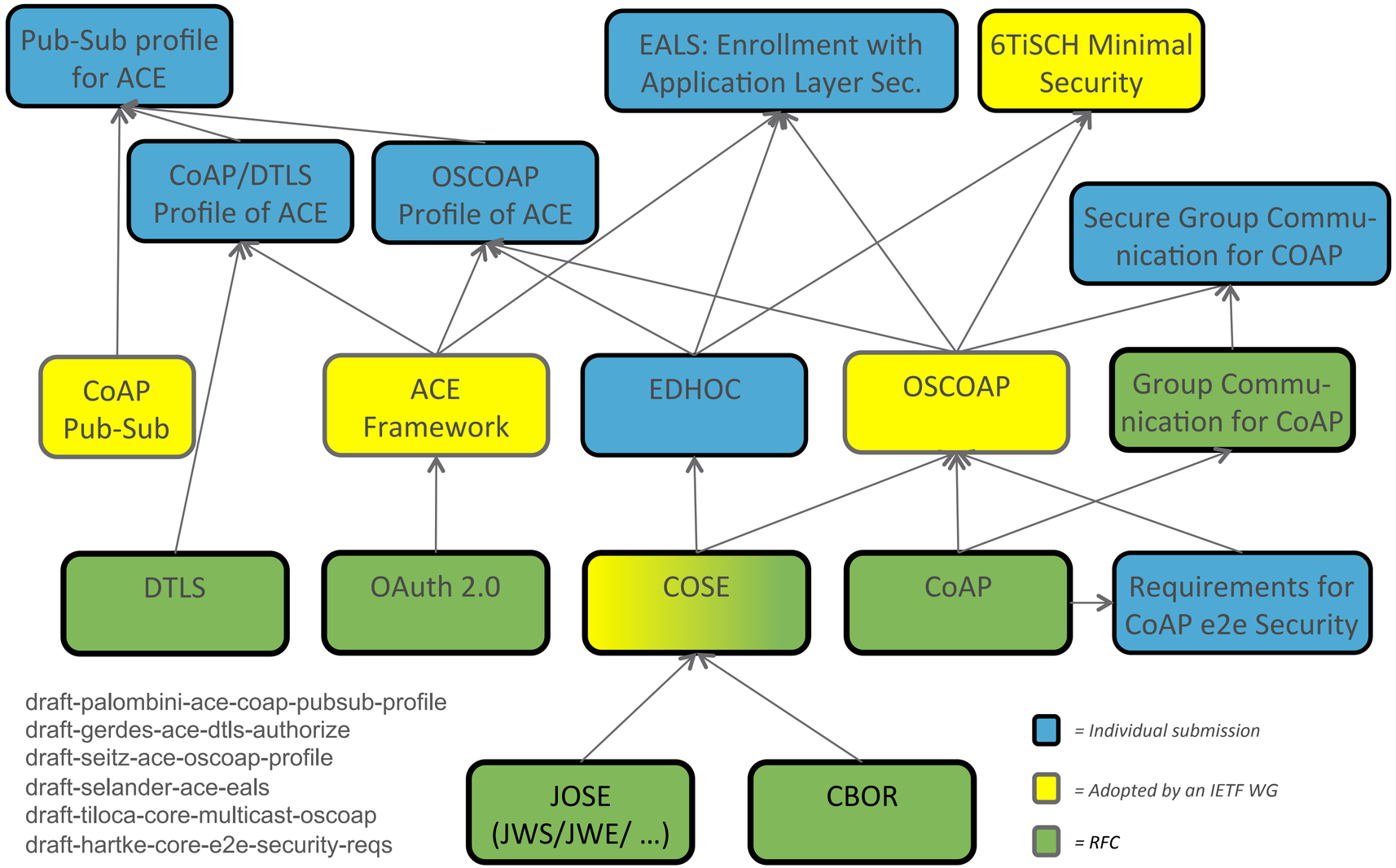
Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 98, CoRE WG, Chicago, Mar 27, 2017

OSCOAP – what and why?

- A security option built into CoAP
- Provides end-to-end confidentiality, integrity and replay protection for CoAP over any/mixed transport (UDP, TCP, IPv4, IPv6, SMS, BLE, 802.15.4 IE, ...)
- Supports CoAP proxy forwarding operations
- Works with Observe and Blockwise (discussed today)
- Supports client and server changing roles
- Can be extended to secure CoAP group communications (separate draft, discussed today).
- Is lightweight, e.g. in terms of message overhead (discussed today)

Related Work



draft-palombini-ace-coap-pubsub-profile
draft-gerdes-ace-dtls-authorize
draft-seitz-ace-oscoap-profile
draft-selander-ace-eals
draft-tiloca-core-multicast-oscoap
draft-hartke-core-e2e-security-reqs

Draft Status (1/2)

- https://github.com/core-wg/oscoap

- Changes implemented according to requests:
  - Per packet overhead reduction
    - COSE object compression
    - No sequence number in responses
    - Sender Id is sent in requests (instead of Context Id)
    - Max-age and Observe special processing
  - Memory usage reduction
    - Reduced Security Context
    - Replay window
  - Node restart handling
  - Clarify section about options processing

Draft Status (2/2)

- Check the issue tracker!
  https://github.com/core-wg/oscoap/issues
  - Thanks Christian, Jim, Mališa, Martin for useful inputs!

Interop I – 27th Feb 2017

- Test specifications and result: https://github.com/EricssonResearch/OSCOAP

- 2h30
- 2 implementations tested in both roles (client, server)
- 17 tests
- Successfully interoperated
- Good feedback about test spec
- Tests v-01

Interop II – 26th Mar 2017

- 1h
- 2 implementations tested in both roles (client, server)
- 11 tests
- Successfully interoperated
- Tests version -02 (+)

- More interop to come!

Issue: Blockwise

- Blockwise does not distinguish between multiple concurrent requests
  - This is true independently of OSCOAP (true for DTLS as well)
  - Sequence of packages creates server state – but sequence is not secured within replay window

- Christian's proposal: Request tag
  - draft-amsuess-core-request-tag
  - Similar to ETag
  - Client-chosen, single-use with defined recycling
  - Server must not combine payloads across request tags
  - Extends OSCOAP (or DTLS) protection to request bodies

Attack: Firmware patches

- PUT /firmware/baseband, payload=v10, 2 blocks
  - First block gets through
  - Second block stored by attacker, retransmissions blocked
- later: PUT /firmware/baseband, payload=v11, 2 blocks
  - First block let through
  - Second block injected from earlier
  - Atomic PUT successful with mixed content. Device bricked from secure operation.
- Is this a bad application to OSCOAP or DTLS? Yes.
- Will such applications expect security nevertheless? Yes.

Request-Tag: What else?

- Could allow interleaved transfers
  - OSCOAP has need for that when proxy in use because, to the proxy, all POSTs look like POST to /
- Defined Request-Tag recycling allows zero byte overhead
  - Needs a controlled replay window, though – can DTLS do that?
- Alternatives?
  - Deeper integration of sequence numbers
  - Option to discriminate within endpoint / security context
  - We might still need this for the interleaved transfers (see above)

Summary

- All major updates are done
- Blockwise main outstanding issue
- We have had several security reviews
- We know of 4 implementations and 2 more are planned

- Next steps:
- Further reviews (from CoAP experts) are requested!
- More interop to come: first week of May, and in Prague
- WGLC

Secure group communication for CoAP

draft-tiloca-core-multicast-oscoap-01

Marco Tiloca, RISE SICS
Göran Selander, Ericsson
Francesca Palombini, Ericsson

IETF 98, CoRE WG, Chicago, Mar 27, 2017

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 repeatedly has requested Multicast OSCOAP (IETF95, mailing list, …)
- draft-somaraju-ace-multicast references OSCOAP to secure group messages – this draft explains how OSCOAP is used for that

- This draft fills this gap and is use case independent

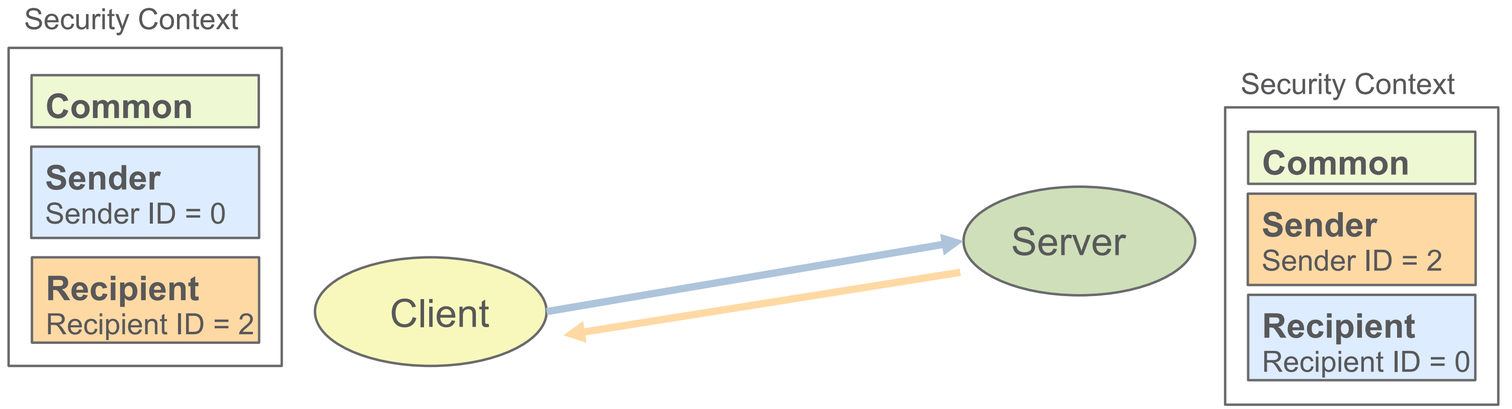
*RFC7390: Group Communication for the Constrained Application Protocol (CoAP)

Main Features

- How to use OSCOAP in group communication
  - Supports multiple listners and multiple broadcasters
- Confidentiality, integrity and replay protocation
- Shared keying material to protect communication within the group (using OSCOAP mechanisms)
- Source authentication: Digital signatures
  - Embedded in the COSE object
- Same structures/constructs/mechanisms as OSCOAP

OSCOAP

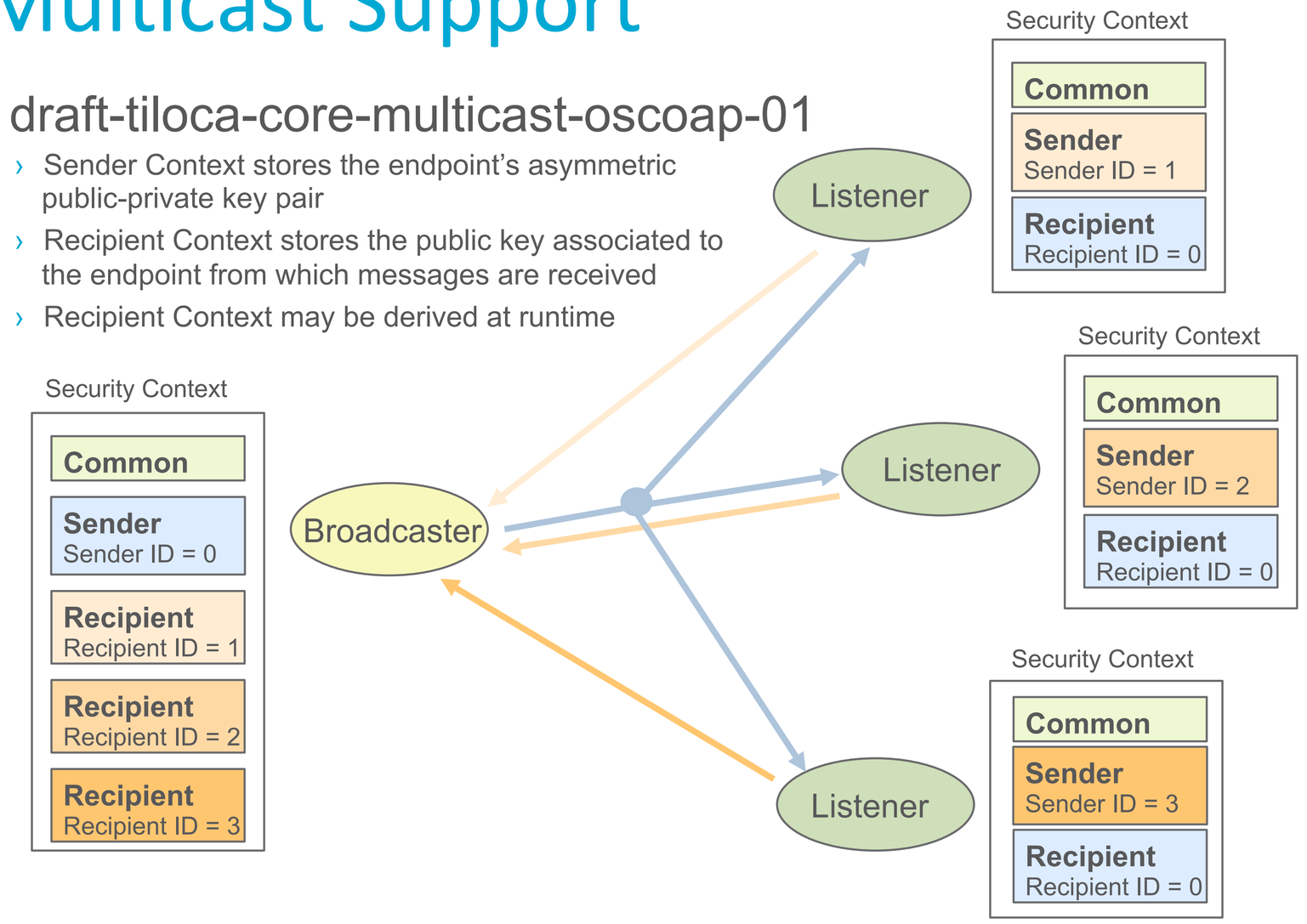
› draft-ietf-core-object-security-02



- 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-01
  - 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 may be derived at runtime



Draft Update (v-01)

- Adapted to OSCOAP v-02 (next slide)
- Restructuring
- Added a Join profile for ACE in Appendix (following comments at IETF97)

What's different from OSCOAP v-02

- Defines Context ID, always sent in the message (not in oscoap-02)
- Sender ID is always sent in the message (optional in oscoap-02)
- Defines a Transaction ID includes Context ID, Sender ID, Partial IV (not in oscoap-02)
- Adds asymmetric keys in Sender/Recipient Context
- Counter Signature added to COSE_Encrypt0 object

Thank you!

Comments/questions?

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

Requirements for CoAP End-To-End Security

draft-hartke-core-e2e-security-reqs

Göran Selander, Ericsson
Francesca Palombini, Ericsson
Klaus Hartke, University of Bremen

IETF 98, CoRE WG, Chicago, Mar 27, 2017

Requirements for CoAP end-to-end Security

- Draft is stable
- Planned: include comments from Jim
- More reviews are welcome

- **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 CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

All times are in time-warped CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

Spillover agenda

- Peter: Pending (because he has to run to the airport right after the start of the meeting)
- Michel: SIDs and IANA (since yang-cbor is nearing WGLC)
- Francesca: Rest of OSCOAP, including actuator and request tag discussion

- Discuss Stateless-Proxy at the end

‘Pending’ response code

Peter van der Stok, Klaus Hartke

IETF 98 - CoRE Working Group

Motivation

Bootstrapping of Remote Secure Key Infrastructures (BRSKI)
[ietf-anima-bootstrapping-keyinfra]
uses Enrollment over Secure Transport (EST) [RFC7030]

CoAP-EST specifies EST over CoAP in ACE WG
EST uses http status code 202 when response takes “some” time

This draft specifies CoAP response code 2.06 for the same purpose.

Details

- Pending response indicates that target resource exists, but no representation is available yet.
- Location may be specified where result will become available.
- Client has to retry with GETrequest after Max-Age.
- Can be used in conjunction with “observe”

- Interesting for this WG?

All times are in time-warped CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

Media Types for Sensor Measurement Lists (SenML)

draft-ietf-core-senml-05

IETF 98, Chicago, IL, USA

Ari Keränen
ari.keranen@ericsson.com

Updates since -04

- Clipboard format support to media types
- Fragment identifier support
- Editorial fixes

One more thing

- Received Signal Strength Indicator (RSSI) unit
  - Suggestion: dBm
    (for RSSI and others with same unit)
  - Alternatives: no unit, percentage; "device specific value"

Must-understand extensions in a SenML document

- Currently unknown extensions ignored
- What happens if you have SenML pack in a database or file?
- Some extensions (e.g., BTO) need to be understood for SenML Pack to make sense
  - Or rather: need to know if can not understand
- Proposal: All must-understand extensions start with reserved character (e.g., "z")

WGLC

- Anything else needed **for the base spec**?

SenML Updates

draft-groves-core-senml-bto-00

&

draft-groves-core-senml-options-00

IETF #98 Chicago

Christian Groves

Status

- draft-groves-core-senml-bto : No update pending resolution of optionality issue.

- draft-groves-core-senml-options: New draft to address optionality of new Senml extension attributes.

draft-groves-core-senml-options (1)

- Issue: No way to determine whether an extension attribute is supported between a client and server.
- Solution Proposal:
  - Use a similar approach to draft-ietf-cose-msg.
  - Define an optional media type parameter to indicate the SenML extension attributes it uses or accepts.
  - A solution should be in the base SenML document.

draft-groves-core-senml-options (2)

- Works for HTTP and Senml however there are issues with CoAP.
- Currently CoAP assigns an ID to each media type option. This doesn’t scale when an option can have multiple combinations/values. Due to many media types for Senml each extension attribute requires 8 ids. Each additional attribute increases the combinations.

draft-groves-core-senml-options (3)

- Possible solution for CoAP:
  - Introduce two new options: Accept Media Type Parameter (AMTP) and Content-Format Media-Type Parameter option (CFMTP).
  - The options allow optional media type parameters to be sent in CoAP messages.
  - This would conserve content format IDs.
  - It’s a generic mechanism that could also be used for cose.
  - Easier mapping between HTTP and CoAP.

Next steps

- To agree on the need for a mechanism and its inclusion in SenML.
- To determine whether the AMTP and CFMTP options are useful.

All times are in time-warped CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

Reusable Interface Definitions for Constrained RESTful Environments

draft-ietf-core-interfaces-09

IETF #98 Chicago

Christian Groves

Updates since v6 (Seoul)

- Corrected Figure 1 sub-resource names e.g. tmp to temp and hum to humidity.
- Addressed the editor's note in section 4.2 in returned links.
- Removed section on function sets and profiles as agreed to at the IETF#97.
- Modified Accepts to Accept header option in section 3.3.
- Addressed the editor's note in section 4.1 to clarify the use of the Accept option.

Updates since v6 (Seoul) (2)

- Modified section 3.6 to indicate that the entire collection resource is returned.
- General: Added editor's note with open issues.

Next steps?

- Two proposals from Michael Koster:

1. Removal of the binding interface in favour of using the link list interface.
2. Changing the “rel” type from one attribute to two attributes to indicate source and destination.

Dynamic Resource Linking for Constrained RESTful Environments

draft-ietf-core-dynlink-03

IETF #98 Chicago

Christian Groves

Status update (1)

- Changes since v1 (Seoul):
  - Section 4.2: Update the Href to use "switch" instead of "light".
  - General: Added editor's notes for issues to be resolved at IETF98.
  - General: Changed the name of the greater than attribute "gt" to "gth" and the name of the less than attribute "lt" to "lth" due to conflict with the core resource directory draft lifetime "lt" attribute.

Status update (2)

- Clause 6.1: Addressed the editor's note by changing the link target attribute to "core.binding".
- Added Appendix A for examples.

Next steps

- Solve outstanding issues:
  1. Naming of lth and gth. Should they revert back to lt and gt due to use by other SDOs?
  2. Proposal to use the query parameters on the GET Observe as the default pattern. This allows multiple observations of the same resource. The PUT behaviour below would be treated as a legacy option. Is this agreeable? (i.e. as per Appendix A examples).

Next steps (2)

3. To avoid query parameter naming overlap. Propose to update draft-ietf-core-resource-directory IANA registration section to general query parameter registration and to add a column indicating their scope, e.g. interface etc.

Additional CoAP Binding and Observe Attributes

draft-groves-core-obsattr-00

IETF #98 Chicago

Christian Groves

- New Draft proposing 6 new dynamic linking attributes:
  - Initialization Value
  - Band Minimum Notification
  - Band Maximum Notification
  - Band Step
  - Sample Number Window
  - Sample Time Window

- Initialization Value
  - The attribute indicates the initialization value to be used to determine when a change step is notified. E.g.

Req: POST /bnd/ (Content-Format: application/link-format)
<coap://sensor.example.com/s/temperature>; rel="boundto";anchor="/a/temperature";bind="obs";pmin="10";pmax="60";st="5",iv="20"

The above will result in:

o STinit being set to 20 due to iv.

o A state synchronization through an Observe:

* Every 60 seconds if the temperature does not differ from STinit by 5.

* When the temperature differs from STinit by 5 at least every 10 seconds.

- Band Minimum Notification
  - This attribute defines the lower bound for the notification band. State synchronization occurs when the resource value is equal to or above the notification band minimum.
- Band Maximum Notification
  - This attribute defines the upper bound for the notification band. State synchronization occurs when the resource value is equal to or less than the notification band maximum.

E.g.

Req: POST /bnd/ (Content-Format: application/link-format)
<coap://sensor.example.com/s/temperature>; rel="boundto";anchor="/a/temperature";bind="obs";pmin="10";pmax="60";bmn="20",bmx="40"

The above will result in a state synchronization through an Observe:

- Every 60 seconds if the value is not between 20 and 40.
- When the temperature is equal to or between 20 and 40 at least every 10 seconds.

- Band Step
  - Like change step (st) this attribute indicates how much the value of a resource SHOULD change before triggering a state synchronization. The difference however is that the values used for the band step calculation are based on a constant step rather than being based on the synchronized value.
  - For example: Given a bst=10 and an initialization value=25. This defines a series of band step thresholds: i.e. ..., (5,15],(15,25],(25,35], ...

- Sample Number Window
  - If queuing of a number of state synchronizations are required then the sample number window attribute is set to the desired size of the window.
  - When a state synchronization is triggered due to the other attributes the resource value is added to the list of samples instead of resulting in state synchronization.
  - Only when the number of samples in the window reaches the sample number window is a state sychronization performed for the resource.

e.g.

Req: POST /bnd/ (Content-Format: application/link-format)
<coap://sensor.example.com/s/temperature>; rel="boundto";anchor="/a/temperature";bind="obs";pmin="10";pmax="60";bmn="50";snw="5"

The above will result in:

- A state sychronization added to the queue at pmax or whenever the value changes and is equal to or above 50.
- A state sychronization through an Observe occurring once 5 synchronizations have been added to the queue resulting in multiple values being synchronized between the source and destination resources.

- Sample Time Window
  - As per Sample number window but the queue is synchronized after a period of time.

Next steps?

- Is there interest to add these parameters to draft-ietf-core-dynlink?

Binding Attribute Scope

draft-groves-core-bas-01

IETF #98 Chicago

Christian Groves

- New Draft proposing a new “BAS” CoAP binding attribute that allows other binding attributes (e.g. lth, st, bm etc.) to be scoped to an item (sub-resource) in a collection resource.
- The linked batch / batch interface can be used to create a collection of interest.
- Benefit: Allows one resource to trigger to notification of the entire collection. It minimises the number of messages to get the information.

- # Examples (1) Item Binding Attribute

Given the resource links:

Req: GET /.well-known/core

Res: 2.05 Content (application/link-format)

</s/>;rt="simple.sen";if="core.b",

</s/light>;rt="simple.sen.light";if="core.s",

</s/temp>;rt="simple.sen.tmp";if="core.s";obs,

</s/humidity>;rt="simple.sen.hum";if="core.s“

A Req: GET /s?bas="temp"&gt=37

Token: 0x4a

Observe: 0

would produce the following when temp exceeds 37:

Res: 2.05 Content (application/senml+json)

Token: 0x4a

{"e":[

{ "n": "/s/light", "v": 123, "u": "lx" },

{ "n": "/s/temp", "v": 38, "u": "degC" },

{ "n": "/s/humidity", "v": 80, "u": "%RH" }],

- # Examples (2) Multiple Observes

In addition to the GET in example 1 the client could also request a notification when the humidity raises above 90%.

A Req: GET /s?bas="humidity"&gt=90
Token: 0x4b
Observe: 0
would produce the following when humidity exceeds 90:

Res: 2.05 Content (application/senml+json)
Token: 0x4b

```
{"e":[
  { "n": "/s/light", "v": 123, "u": "lx" },
  { "n": "/s/temp", "v": 16, "u": "degC" },
  { "n": "/s/humidity", "v": 92, "u": "%RH" }],
}
```

- Advanced functionality
  - BAS only applies to a single sub-resource. To allow conditions from multiple sub-resources to be combined a separate method could be defined. E.g.

```
FETCH /s/?pmin=1&pmax=100 content-type=application/conditionals+json
  [
   {
    "n": "/s/light",
    "st": 5
   },
   {
    "n": "/s/temp",
    "st": 1
   },
   {
    "n": "/s/humidity",
    "lt": 40,
    "gt" 70
   }
  ]
```

Next steps?

- Is there interest to in the BAS attribute?
- If so, should it be combined with the dynlink draft or a separate draft?
- Is there interest in an advanced mechanism based on FETCH? Now or later?

All times are in time-warped CDT

Friday (90 min)

- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

draft-becker-core-coap-sms-gprs-06

- Has been dormant for a while
- New editor team found
- Relevant part from coap-misc integrated

- Do we want to finish this now?
- Can we?

draft-silverajan-core-coap-protocol-negotiation-04

- Has been dormant for a while
- Now increasingly relevant with multiple transports

- Expect some activity on the way to Prague
- Time to read and think is now

All times are in time-warped CDT

Friday (90 min)

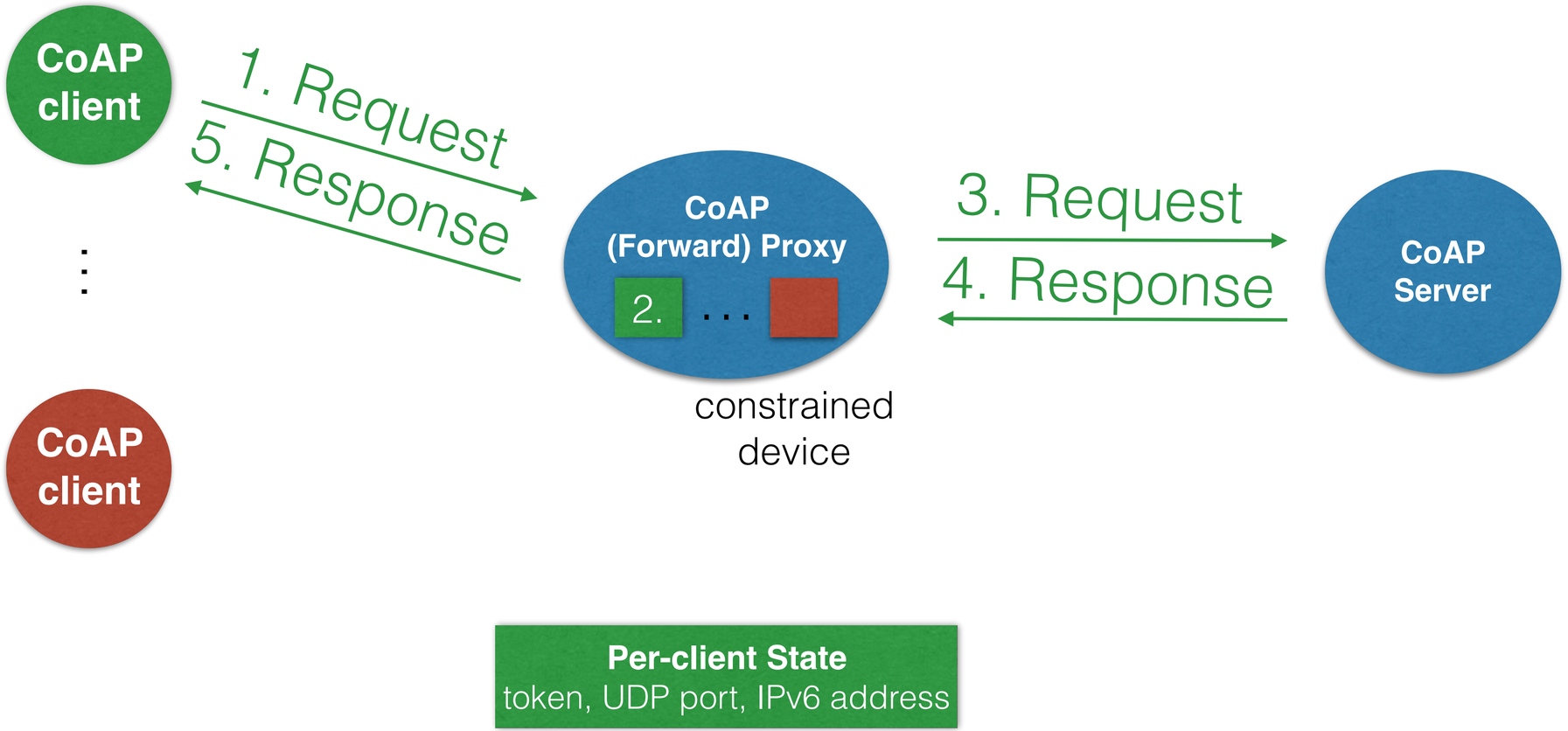
- 11:50–11:55 Intro, Agenda, Status
- 11:55–12:15 Spillover from Tuesday
- 12:15–12:35 SenML
- 12:35–12:50 Other WG drafts (Interfaces, Dynlink)
- 12:50–13:00 Transports
- 13:00–13:20 Open Discussion
  - Pending
  - Delegated Observe
  - …

‘Stateless-Proxy’ CoAP Option

Mališa Vučinić

IETF 98 - CoRE Working Group

DoS Susceptibility of the Proxy



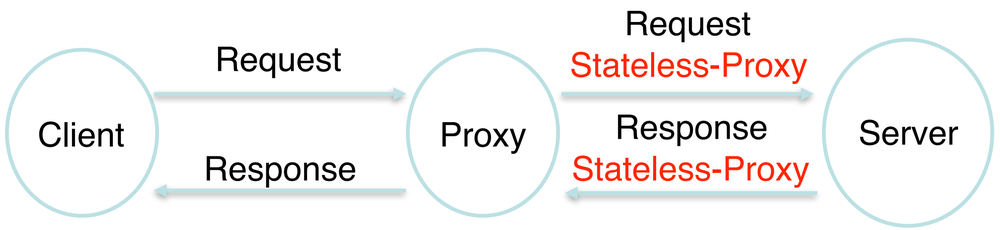
Stateless-Proxy Option

- New CoAP option carrying state between Proxy and Server

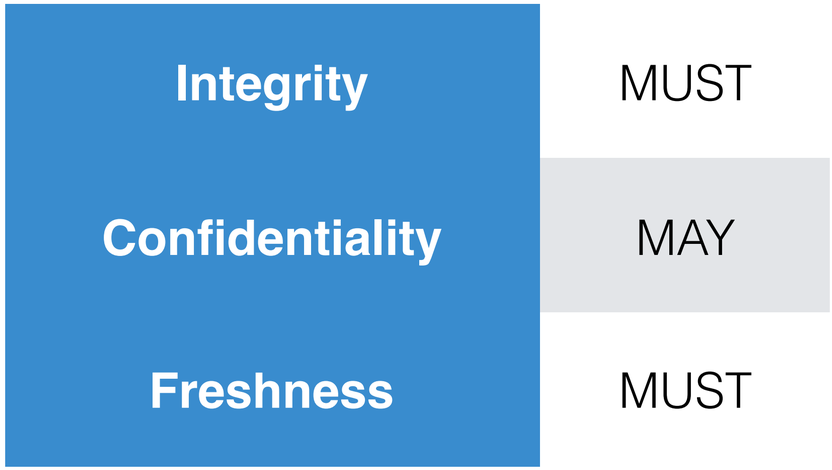
No.	C	U	N	R	Name	Format	Length
TBD	x		x		Stateless-Proxy	opaque	1-255

C=Critical, U=Unsafe, N=NoCacheKey, R=Repeatable

Figure 2: Stateless-Proxy CoAP Option



Security Properties



- Proxy generates a key known only to itself and uses it to protect the option value
- Pitfall of the option: Empty CoAP ACK does not carry any options so the proxy doesn't know where to forward it. Can we mandate the option to be present in the empty ACK?
- For more information: https://datatracker.ietf.org/doc/draft-ietf-6tisch-minimal-security/

See you…

- at the Interops
- in Prague