Constrained RESTful Environments WG (core)

Chairs:

Andrew McGregor <andrewmcgr@gmail.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

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

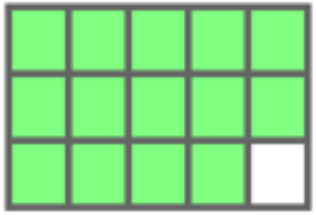
Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

Observe

- **draft-ietf-core-observe–16 (2014-12-30) cleared all the DISCUSSes and addresses the COMMENTS**

  Still to do: Discuss Summary list of addressed COMMENTS with IESG



- **Some of the interesting COMMENTs may instead turn into text changes in draft-ietf-lwig-coap — we need to pay more attention to documenting implementation information!**

WG documents

- draft-ietf-core-block — 3rd WGLC completed
  - looking for a shepherd
- draft-ietf-core-http-mapping — Fri
  - WGLC very soon
- draft-ietf-core-links-json
  - still waiting for more implementation experience?
- draft-ietf-core-resource-directory — Thu
  - charter work needed (today), added authors
- draft-ietf-core-interfaces
  - to resume activity!

CoCoA: Congestion Control/Advanced

- Several interactions with transport people at previous meetings; leading to refined analysis
- No changes to proposal since last discussion
  - instead, research was continued
  - e.g., affirming results from the FlockLab testbed
- Discussed in ICCRG this week
  - Discussion did not expose any remaining roadblocks
- Time for WG adoption?
  - could agree today to raise WG adoption question on the mailing list

What else is going on?

- ACE WG: Authentication and Authorization for Constrained Environments
  - stuck on informational documents
- DICE WG: DTLS In Constrained Environments
  - finishing DTLS profile
  - stuck on multicast
- JOSE: → COSE
- T2TRG (proposed): Thing-to-Thing RG
  - Security, Lifecycle
  - REST and beyond REST
  - Management in IoT
- 6Lo, 6TiSCH: Security (→ tonight 1900 Pavilion)

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

CoRE working group

CoAP Management Interface
draft-vanderstok-core-comi-06

P. van der Stok, B. Greevenbosch, A. Bierman, J. Schoenwalder, A. Sehgal

March 26, 2015

Motivation

Provide transport over CoAP between clients and “reduced resource” servers to access standardized resources (specified in SMI or YANG) to:

- Do statistics (e.g. fragmentation percentage in LoWPAN packets)
- Initialize parameters (e.g. DIOIntervalMin in RPL)

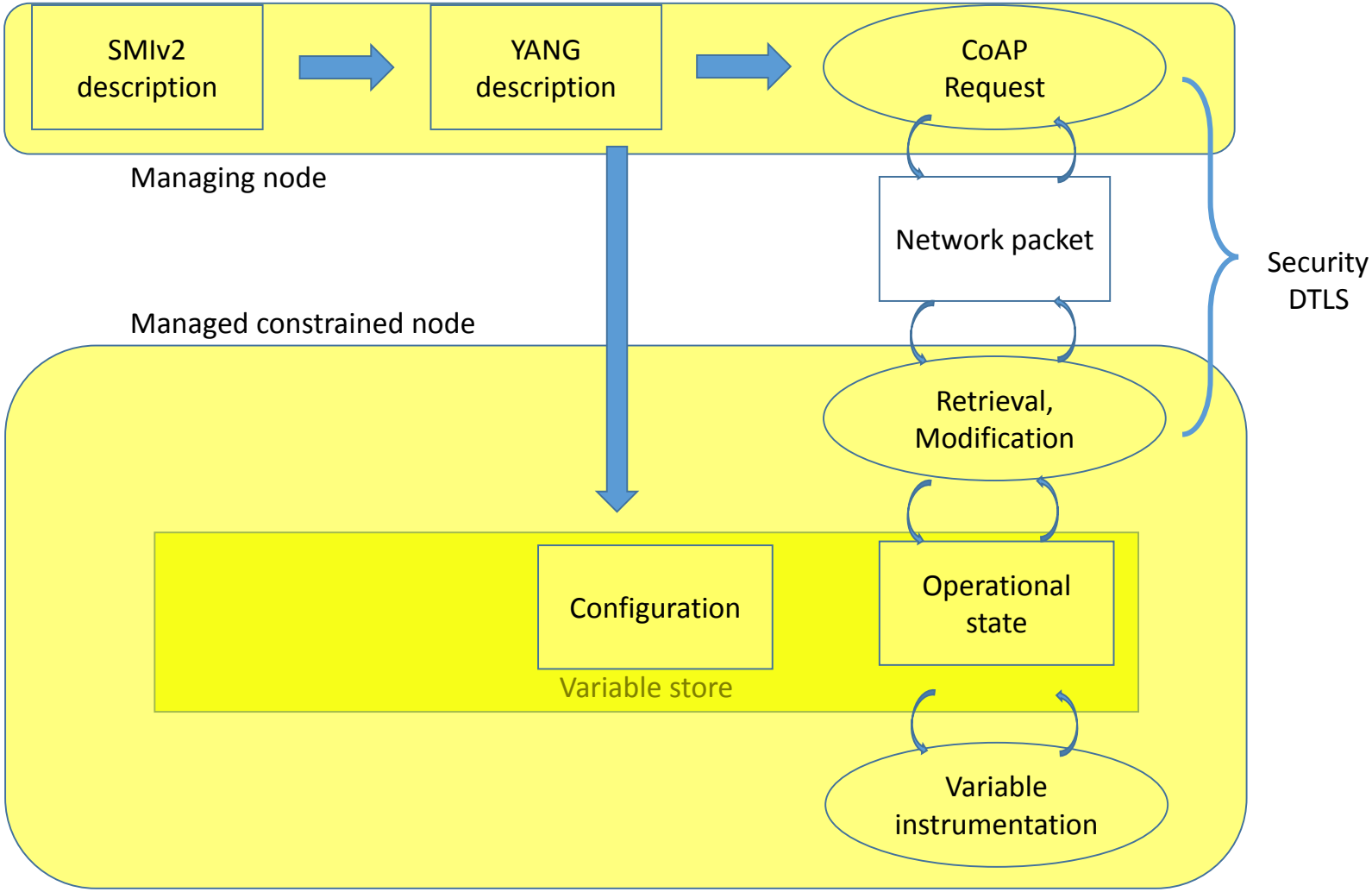
With the wish to:

- Provide small payloads and transport overhead
- Based on CoAP transport and security recommendations

State

Current version 6

- Aligned with RESTconf (which uses http)
- CBOR payload
- Hash for name strings
- Discovery
- Access granularity
- Dependence on Block and Observe


SMIv2 description
YANG description
CoAP Request
Managing node
Network packet
Security DTLS
Managed constrained node
Retrieval, Modification
Configuration
Operational state
Variable store
Variable instrumentation

Profile of CoMI Function set

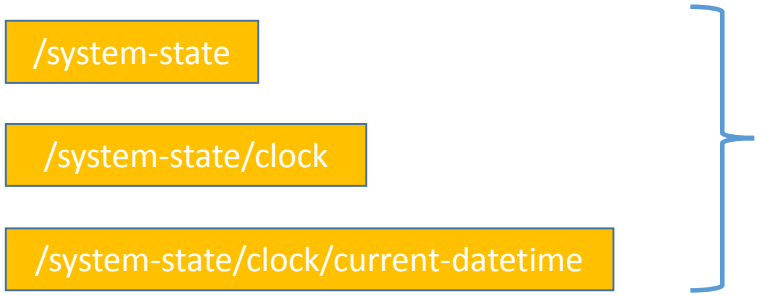
name	path	rt	Data type
Management	/mg	Core.mg	n/a
data	/mg	Core.mg.data	Application/cbor
Module set URI	/mg/mod.uri	Core.mg.moduri	Application/cbor
YANG Hash Info	/mg/yang.hash	Core/mg.yang-hash	Application/cbor

YANG module and MIB

URI in request specifies the data envelop

```
REQ: GET example.com/mg/system-state/clock/current-datetime

REQ: GET example.com/mg/system-state/clock
```



Hash to 30 bit number
Baseb 64 representation in uri
Hexadecimal representation in JSON
Unsigned int in CBOR

On 1700+ YANG objects, the average YANG identifier local-name length is between 9 and 10 bytes.
Proposed Hash function: murmur3

No Hash collision detected yet.

Rehash requirements

Required: Hash code for given object identical over all servers.

Note:

- Clashes between servers are irrelevant
    - Client can use same hash for different objects on different servers
- Clash on a server needs to be notified with rehash

Key query parameter

A YANG data node has a one instance

With exception of node with TYPE: list

Each list instance has a unique key identifier composed of a subset of the list attributes

Instances are selected in uri.

Discovery

Discovery information exported to “YANG module” servers
Managed server only knows hash codes,
names are present on “YANG module” server

/Moduri provides link to external ietf-yang-library module

Managed servers can add data items, identified by hash code, to
/.well-known/core with their rt value

TODO plan

- Comparison with LWM2M and IPSO management
- Use of PATCH
- More text on Block
- A “select” option example
- Extended error code specification

CoRE working group

CoAP PATCH
draft-vanderstok-core-patch-00

P. van der Stok, A Sehgal

March 26, 2015

Motivation

The PUT method exists to overwrite a resource with completely new contents, and cannot be used to perform partial changes.

PATCH is also specified for HTTP in [RFC5789]. Most of the motivation for PATCH described in [RFC5789] also applies here.

CoMI applications will wish to make to changes to parts of a YANG data resource

Transferring all data associated with a YANG data resource unnecessarily burdens the constrained communication medium.

Open topics

Use of error codes

Notification of formats (which formats?)

Accept patch needed ?

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

CoRE Resource Directory

draft-ietf-core-resource-directory (work in progress on -03)

Z. Shelby, C. Bormann

CoRE WG, IETF-92 Dallas

Adding new authors

- Michael Koster (Editor)
  - Contribution to improvements to the RD, and alignment with next LWM2M version
- Peter van der Stok
  - Contributions to DNS-SD mapping, group operations and examples

Advanced Examples

- Lighting example with group interface usage
- LWM2M example showing how the RD interfaces are used by LWM2M throughout a device's lifecycle

Link collection interface

- Goal
  - For an endpoint (or installation tool) to manage collections of links after registration
- Interface
  - REST interface at /{+location} (returned in registration)
  - Get link collection
  - Add a link
  - Remove a link
  - Replace a link
- Design proposals welcome, but let’s not make this an excuse to invent a patch mechanism unless really useful

Simple Directory Discovery

- No strong use case
- Confusing
- No lifetime for updates and link management
- We recommend to remove this section

When are we done?

1. Do one more editing round for -03
2. Known issues for -03
   - Link maintenance collection interface needed at /{+location} after registration (see next slide)
   - Advanced examples
     - Lighting example (received from Peter)
     - LWM2M example (Michael to write)
3. And add this to our charter ☺
4. Get at least 3 expert reviews, at least one from OMA as part of a WGLC

Resource Directory Names for Certificate Mode DTLS

March 26, 2015

Problem Statement

If you want to do *Certificate mode* DTLS and you don't have DNS[1], then you are in trouble.

[1] Which is not unrealistic if you look at p2p scenarios...

Current Requirements

- "Client MUST make sure that server certificate has SAN.URI matching the authority of the requested URI" [RFC 7252]
- "SAN.URI MUST contain either a fully qualified DNS hostname (FQDN) or an IP literal" [RFC 5280]
- "SNI only accepts a FQDN of the server in the HostName" [RFC 6066]

$\Longrightarrow$ Certificate Mode is incompatible with DNS-free deployments.

Challenges for a DNS-free deployment

- What identifiers should be used in the certificate?
- What identifier should be contained in the `hostname` part of the endpoint URI?
- What identifier should be communicated in the SNI during the TLS/DTLS exchange?
- How can the identifier in the CoAP URI be mapped to an IP address?

Questions for the Working Group

- Is there any interest in the p2p use case?
- Are there any plans not to use DNS?

Possible Solution

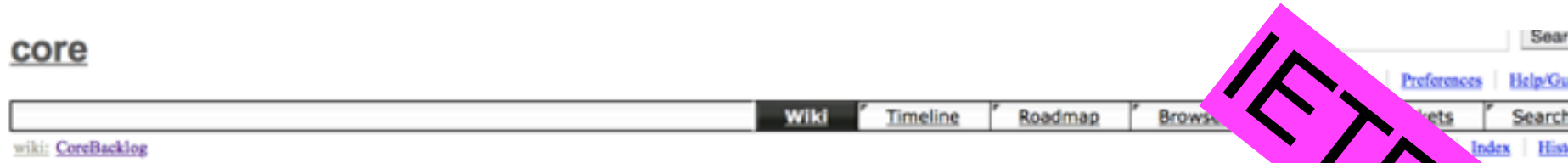
Use Resource Directory endpoint names (and domains) as an alternative to DNS names?

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

http://trac.tools.ietf.org/wg/core/trac/wiki/CoreBacklog



IETF91

This page maintains a backlog of work that the WG has identified as highest priority to work on next.

Work Item	Priority	Status	Related Work
Observe	High	IESG	draft-ietf-core-observe
Block	High	WG Document	draft-ietf-core-block
Resource Director	High	WG Document	draft-ietf-core-resource-directory
CoAP over TCP	High		draft-bormann-core-coap-tcp, draft-tschofenig-core-coap-tcp-tls, draft-silverajan-core-coap-alternative-transports
JSON Links	Normal	WG Document	draft-ietf-core-links-json
HTTP Mapping	Normal	WG Document	draft-ietf-core-http-mapping
SenML	Normal		draft-jennings-senml
CoRE Interfaces	Normal	WG Document	draft-ietf-core-interfaces
CoAP Management	Normal		draft-vanderstok-core-comi
CoAP Timeout Estimation	Low		draft-bormann-core-cocoa
CoAP Pub Sub	Low		draft-koster-core-coap-pubsub
CBOR Links	Low		draft-li-core-links-cbor

The following priority levels are used:

- High: This work item is high priority, and should be the next to try and progress through the WG
- Normal: This work item is normal priority
- Low: This work item is low priority, and would be nice to have, but should wait until higher priority work is complete

https://svn.tools.ietf.org/svn/wg/core/charter-ietf-core.txt

The WG will perform maintenance on its first four standards-track specifications (RFC 6690, RFC 7252, -observe, -block) and will continue to evolve the experimental group communications support (RFC 7390). The working group will not develop a reliable multicast solution.

CoAP today works over UDP and DTLS. The WG will define transport mappings for alternative transports as required, both IP (starting with TCP and a secure version over TLS) and non-IP (e.g., SMS, working with DICE on potentially addressing the security gap); this includes defining appropriate URI schemes. Continued compatibility with CoAP over SMS as defined in OMA LWM2M will be considered.

…

https://svn.tools.ietf.org/svn/wg/core/charter-ietf-core.txt

CoRE will continue and complete its work on its resource-directory, as already partially adopted by OMA LWM2M. Interoperability with DNS-SD (and the work of the dnssd working group) will be a primary consideration.

CoRE will work on related data formats, such as alternative representations of RFC 6690 link format and RFC 7390 group communication information. The WG will complete the SenML specification, again with consideration to its adoption in OMA LWM2M.

RFC 7252 defines a basic HTTP mapping for CoAP. This will be evolved and supported by further informational documents.

…

https://svn.tools.ietf.org/svn/wg/core/charter-ietf-core.txt

Beside continuing to examine operational and manageability aspects of the CoAP protocol itself, CoRE will also develop a way to make RESTCONF-style management functions available via CoAP that is appropriate for constrained node networks. This will require close coordination with NETCONF and other operations and management WGs.

The WG has selected DTLS as the basis for the communications security in CoAP. CoRE will work with DICE on the efficiency of this solution. The preferred cipher suites will evolve in cooperation with the TLS working and CFRG research groups. ACE is expected to provide solutions to authorization that may need complementary elements on the CoRE side. Object security as defined in JOSE and possibly adapted to the constrained node network requirements also may need additions on the CoRE side.

…

https://svn.tools.ietf.org/svn/wg/core/charter-ietf-core.txt

The WG will coordinate on requirements from many organizations and SDO. The WG will closely coordinate with other IETF WGs, particularly of the constrained node networks cluster (6Lo, LWIG, 6TiSCH, ROLL, DICE, ACE), and appropriate groups in the IETF OPS and Security areas.

Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

The REST model

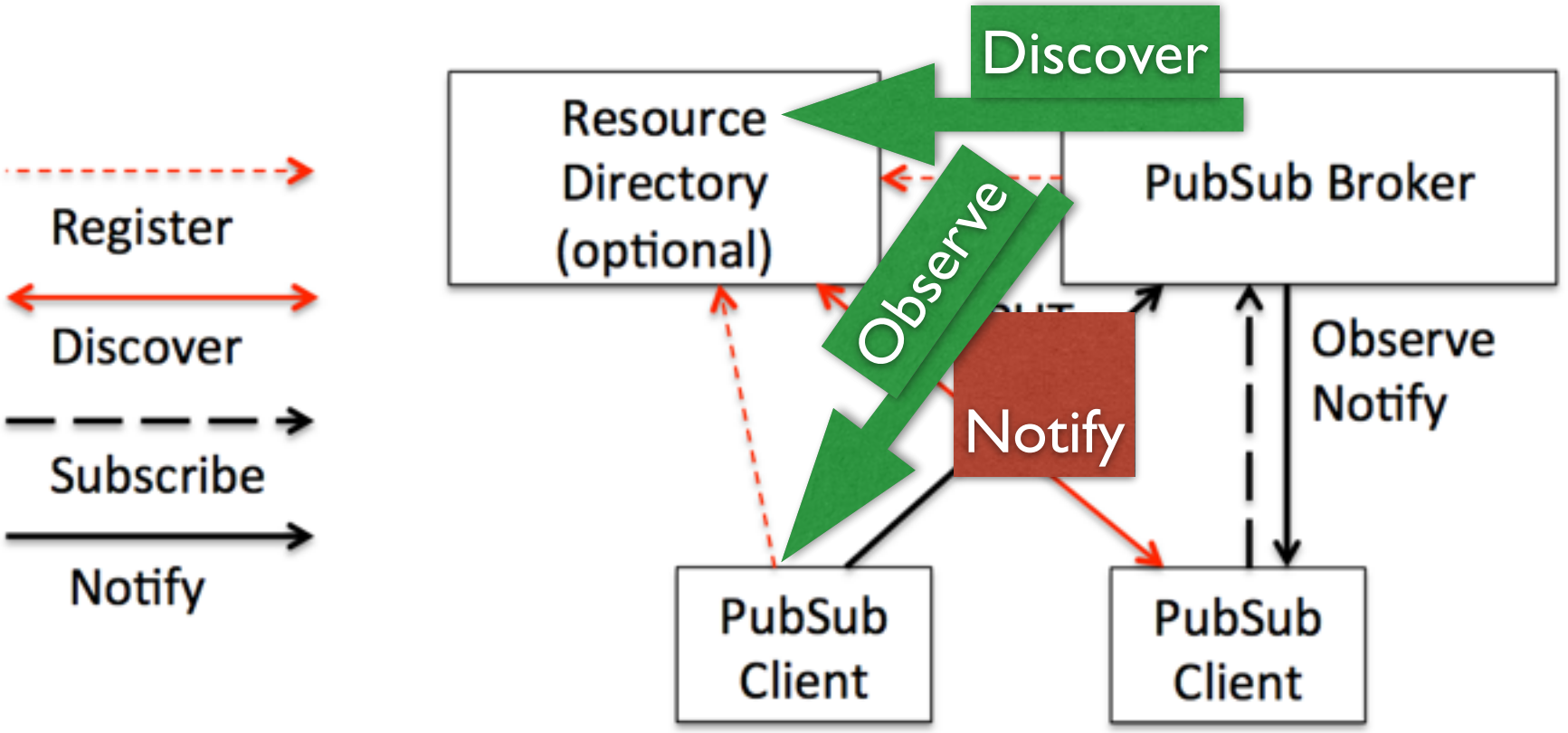
- Server is origin of data, packaged into a resource
- Use GET to get a copy (»representation«)
- CoAP: Add Observe to give server initiative to update that copy
- Observe needs initial GET to determine recipient of copy
  - might invent a management primitive for this as well

The PUTters

- Device-to-cloud crowd: device comes configured with DNS of recipient of data
- Only ever need PUT to update a resource in the cloud with data + origin id
- Side-effect: no need think about NATs

- works great without security or management

Do this right?



CoAP PubSub

draft-koster-core-coap-pubsub-02

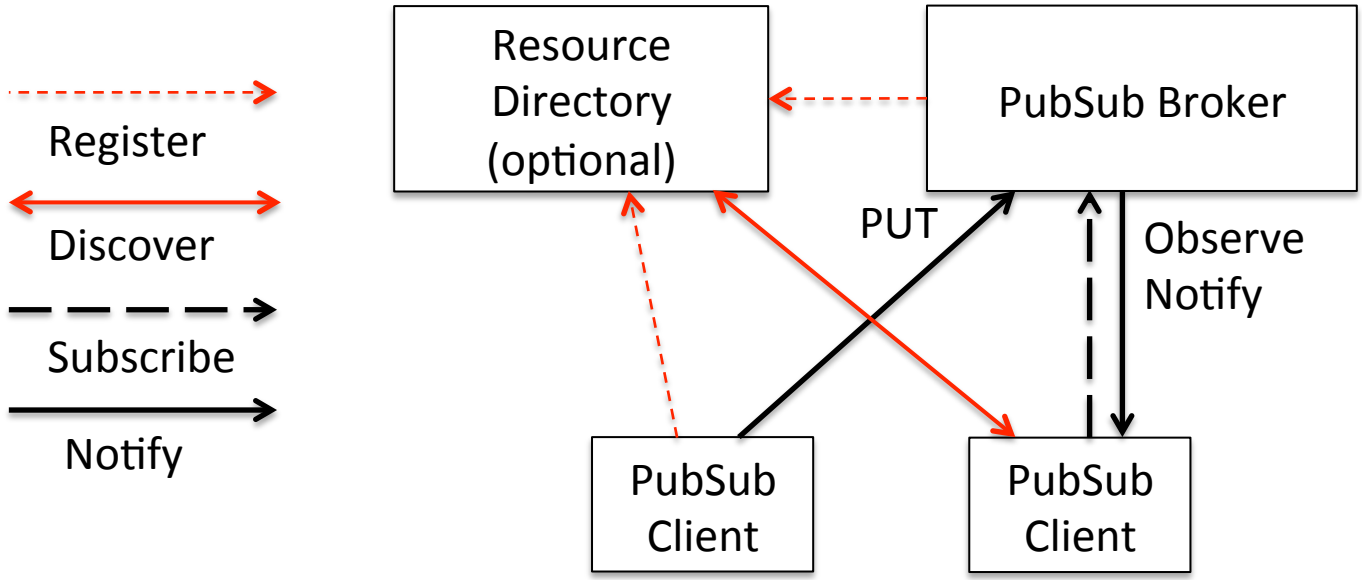
Review

- CoAP PubSub is a mapping of Publish-Subscribe semantics to CoAP
- Defines a CoAP PubSub Broker, through which messages are exchanged between publishers and subscribers
- The draft was updated to remove too many confusing roles and cases

Draft Updates

- The CoAP PubSub broker is now a standalone CoAP server and is not integrated with RD
- Devices and applications are CoAP clients
- Use of RD is optional, and may register the broker itself and topics on the broker
- Using POST to create topics, PUT to publish to the broker, DELETE to remove topics
- Using Observe to subscribe to topics

Architecture



Discussion

- What is needed to enable sleeping nodes?
- Is flow control needed?
- Should there be data series retention?
- PUT vs. Notify?
- Other?

Thursday

All times are in time-warped CDT

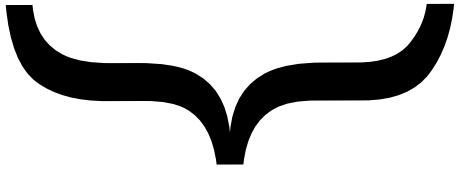
- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

Size Comparisons

Jim Schaad: slides-92-jose-0.pptx

- Overheads only – ignores contents

	JOSE	Bormann	Schaad
1 Signer	*64 + base64*	*13*	*13*
1 MAC recipient	*64 + base64*	*13*	*14*
1 Encryption Recip	*94 + base64*	*14*	*14*



COSE

ERICSSON

Object Security for CoAP

draft-selander-ace-object-security-01

Göran Selander, Ericsson
John Mattsson, Ericsson
Ludwig Seitz, SICS

IETF 92 CoRE WG, Dallas, March 26, 2015

Background

- End-to-end security between endpoints; encryption by default
  - Intermediary nodes; proxying, storing-and-forwarding, caching, pubsub-brokering, . . .
  - Object security as a complement to DTLS or standalone
  - Also part of the authorization solutions (e.g. access tokens)
- COSE: New mailing list, and charter in drafting for defining a secure object format suitable for constrained devices.

New CoAP Options

No.	C	U	N	R	Name	Format	Length
TBD	x		x		Sig	opaque	12-TBD

No.	C	U	N	R	Name	Format	Length *)
TBD	x		x		Enc	opaque	0 or 12-TBD

*) Additional length added to the total length of all CoAP options.

- 12 B (Sig, Enc) is a lower bound of Length, estimated using a tailor made message format. Actual length interval depends on message format.
- 0 B in Enc indicates that the JWE (or similar) is in the payload.

Secure Object Overhead

› JWS

Header: {"alg":"HS256", "kid":"a1534e3c5fdc09bd", "seq":"00000142", "mod":"0”}

› JWE

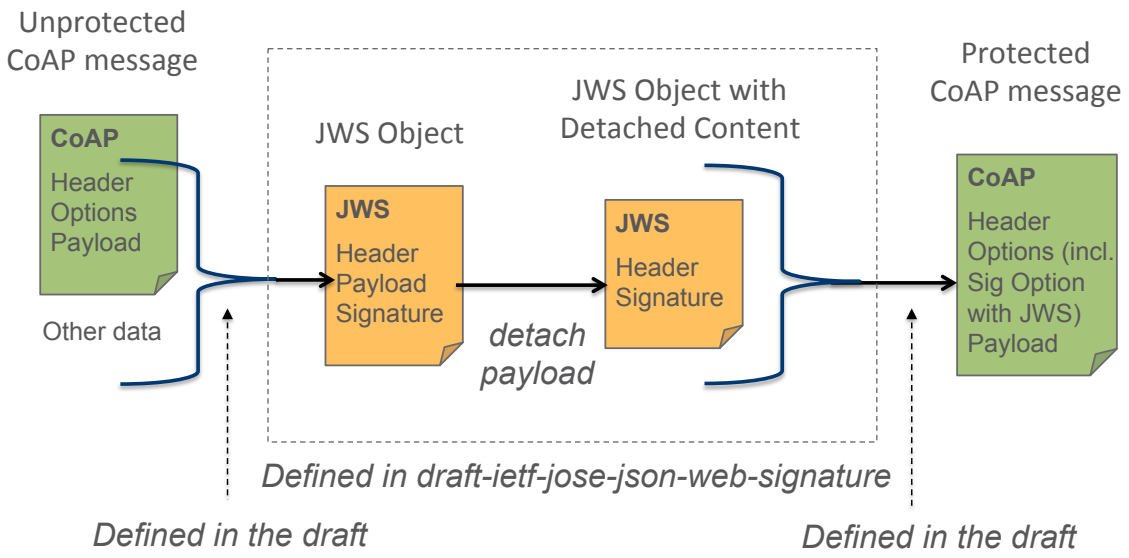
- Header: {"alg":"dir", "kid":"a1534e3c5fdc09bd", "enc":"A128GCM", "mod":"0"}
- IV contains sequence number

Scheme	Over-head
JWS	135 B
COSE-00	70 B
Lower bound	28 B

Scheme	Over-head
JWE	127 B
COSE-00	70 B
Lower bound	20 B

Signature of CoAP message, e.g. using JWS

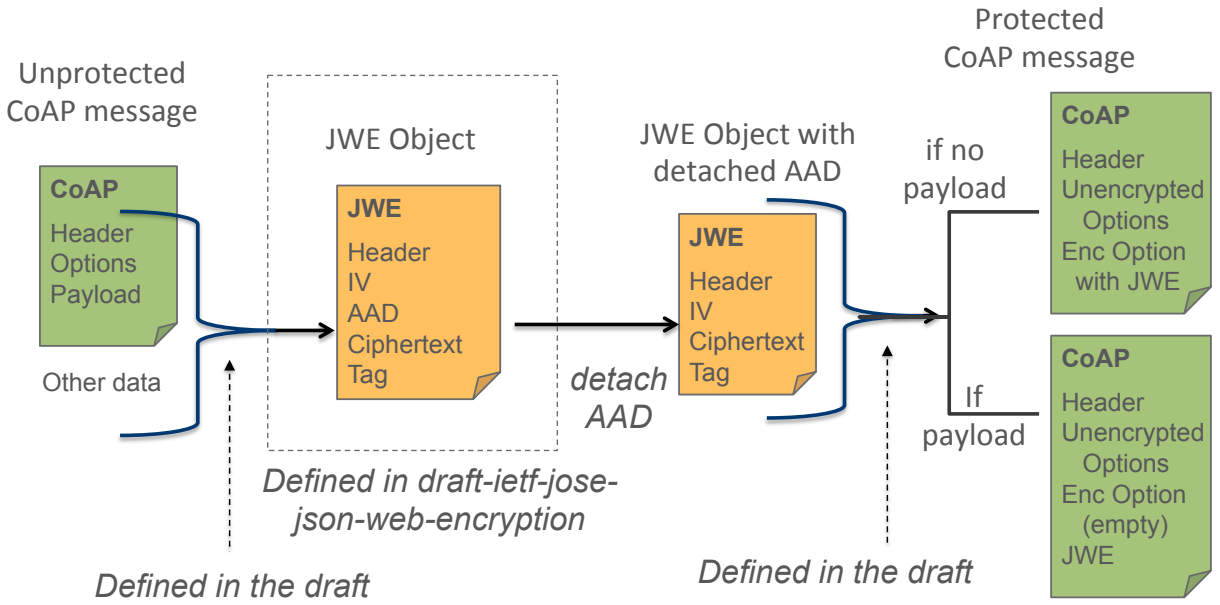
- Integrity and replay protection of CoAP message
- CoAP Option "Sig" Containing a JWS (signature) of the message
- Other data: Used in response to verify freshness



Subset of CoAP Header, Options, Payload and other data wrapped in a JWS Object

Encryption of CoAP Message, e.g. using JWE

- Encryption, integrity and replay protection of CoAP message
- CoAP Option "Enc": Indicating presence of a JWE
- Other data: Used in response to verify freshness



Subset of CoAP Header, Options, Payload and other data wrapped in a JWE Object

Which Options to Protect?

- Integrity protection:
  - Safe-to-forward
  - Not changed by proxy

  (Uri-related on later slide)
- Encryption:
  - By default
  - Not read by proxy

  (Uri-related on later slide)

No.	C	U	N	R	Name	Format	Length	E	IP
1	x			x	If-Match	opaque	0-8	x	x
3	x	x	-		Uri-Host	string	1-255		a
4				x	ETag	opaque	1-8	x	x
5	x				If-None-Match	empty	0	x	x
6		x	-		Observe	uint	0-3		
7	x	x	-		Uri-Port	uint	0-2		a
8				x	Location-Path	string	0-255	x	x
11	x	x	-	x	Uri-Path	string	0-255	x	b
12					Content-Format	uint	0-2	x	x
14		x	-		Max-Age	uint	0-4		
15	x	x	-	x	Uri-Query	string	0-255	x	b
17	x				Accept	uint	0-2	x	x
20				x	Location-Query	string	0-255	x	x
35	x	x	-		Proxy-Uri	string	1-1034		x
39	x	x	-		Proxy-Scheme	string	1-255		
60			x		Size1	uint	0-4	x	x

Table

Pre-processing before crypto

- JWS Payload
  - CoAP Header field Code
  - CoAP Options marked "IP" in the Table
  - CoAP Payload (if any)
- JWE Plaintext
  - CoAP Options marked "E" in the Table
  - CoAP Payload (if any)
- JWE Additional Authenticated Data
  - CoAP Header field Code
  - CoAP Options marked "IP" but not "E" in the Table

Uri-related options

- CoAP messages may include instructions for a proxy to performing certain actions
- Changes which are not predictable cannot be integrity protected end-to-end
  - E.g. Max-age, Observe
- But some changes are predictable and the corresponding data can be integrity protected end-to-end
- However the change must be accounted for before verifying the received secure object
- A forward proxy decomposes the Proxy-Uri into the Uri-* options
- Integrity protection of Uri-related options:
  - The sender signs the Proxy-Uri (option 35)
  - The receiver composes the Uri from the Uri-* options and places it in option 35 before verifying integrity

Implementation (work in progress)

- Variant of version-00
  - CSM format instead of JOSE
- Erbium REST Engine for Contiki
- TI CC2538 (32 bit, 32 KB RAM, 512 KB flash)
  - AES_CCM_8 in software
- First measurements
  - Comparison with plain CoAP
  - The impact on required RAM, flash, and on processing is essentially due to the memory and processing associated to the crypto algorithm
  - In comparison with this, the added code, processing times etc. for message processing were negligible

Thank you!
Questions?

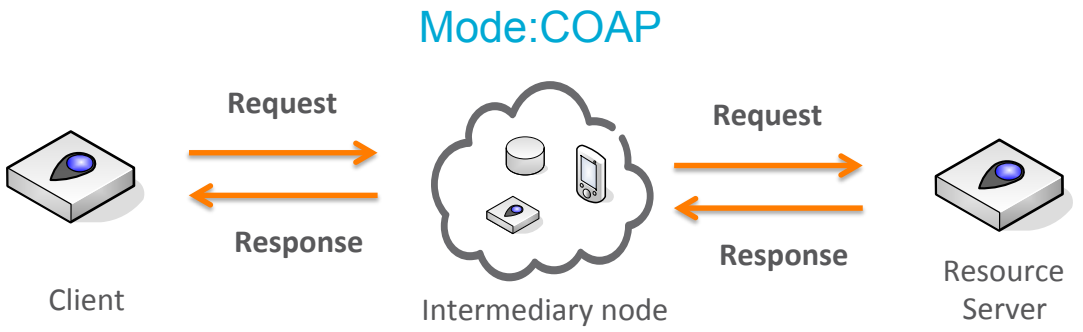
Reading hints

- End-to-end security considerations (Sec. 2-3)
  - End-to-end security between endpoints in the presence of intermediary nodes.
- Message format (Sec. 4, App. B-C)
  - Encryption, integrity protection and replay protection.
  - Focus on AEAD in this version of the draft.
- CoAP layer protection (Sec. 5.1, App. A)
  - New CoAP Options
  - Client-server challenge-response protocol.
- Application layer protection (Sec. 5.2)
  - Point-to-point/multipoint, e.g. caching, publish-subscribe.
- Examples (App. D)

Different modes

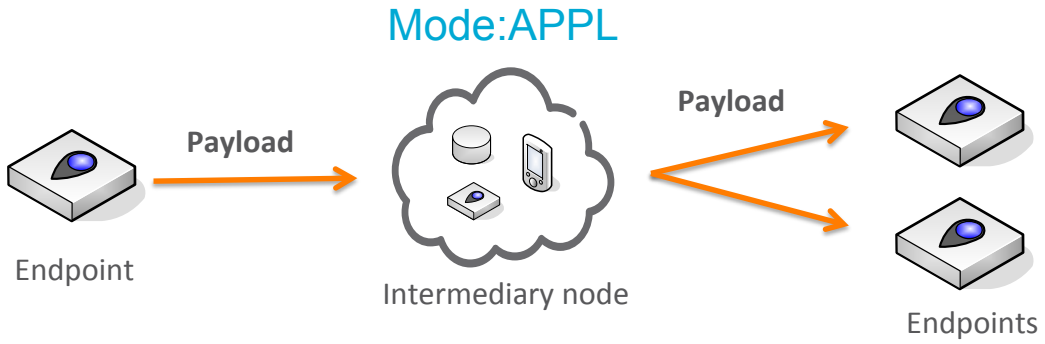
Mode:COAP

- Point-to-point
- CoAP message
- Replay protection
- Challenge-response
- Forward proxy



Mode:APPL

- Point-to-multipoint
- Application layer data
- Replay protection
- Caching/PubSub



Items to ponder for the CoRE WG

- Security options: Significant extension to CoAP
- Goes through proxies:
  More general than existing commsec
  - De-emphasize DTLS?
- Object Security itself likely to be done in COSE
- Establishment of security associations: ACE
- CoAP extension: CoRE

- **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.

Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

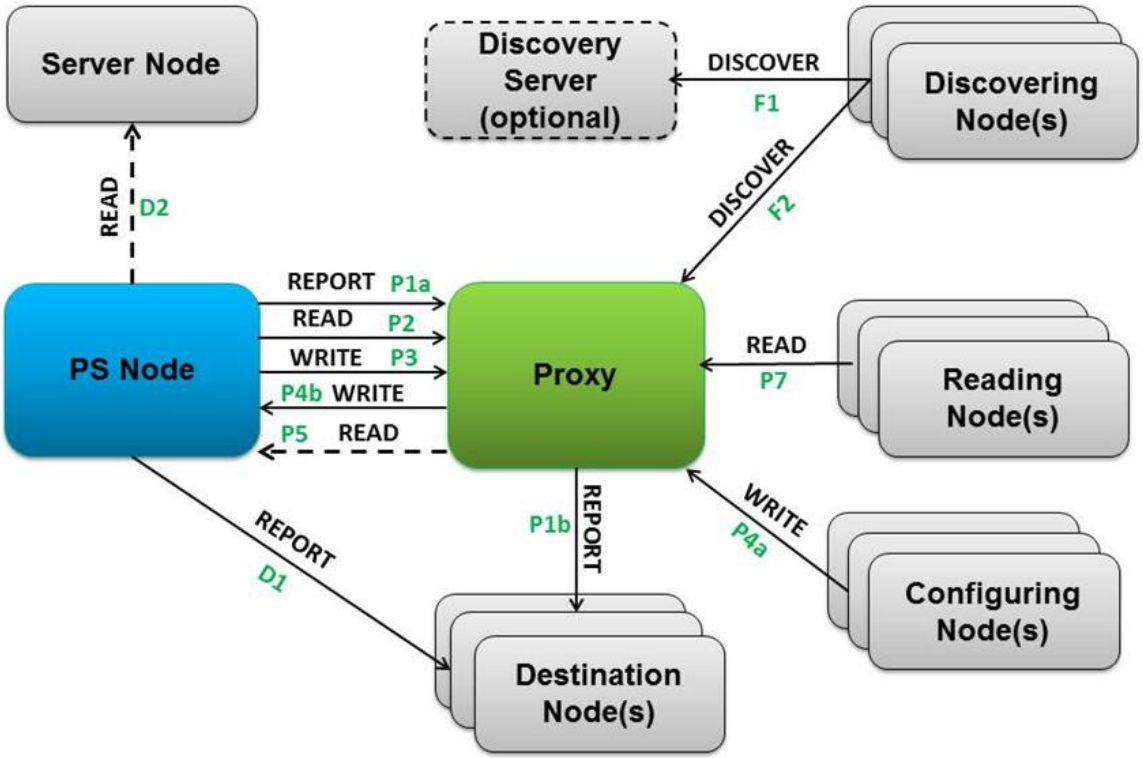
CoRE working group

Sleepy nodes
draft-zotti-core-sleepy-nodes-02

T. Zotti, P. van der Stok, E. Dijk

March 26, 2015

Role of nodes around sleepy node



Thursday

All times are in time-warped CDT

- **15:20–15:30 Intro**
- **15:30–16:00 CoMI (PV)**
- **16:00–16:05 Resource Directory (ZS)**
- **16:05–16:20 Recharter Discussion**
- **16:20–16:25 The REST issue (CB)**
- **16:25–16:40 Pubsub (MK, PV)**
- **16:40–17:00 Security (MK, PV)**
- **17:00–17:20 Alternative Transports (HT, BS)**

CoAP Communication with Alternative Transports

draft-silverajan-core-coap-alternative-transports

Bill Silverajan Tampere Univ of Technology
Teemu Savolainen Nokia Technologies

History and Status

- Versions -00 and -01 in Feb 2013, introduced in IETF 86 in Orlando
  - Discussed need for new alt. transport URI and analysed alt transport properties
  - Proposal to carry transport info in URI scheme, path or query
  - Existing non-standard practices also highlighted
- Version -02 presented in IETF 87 in Berlin
  - Feedback was to explore more URI options and rigorous evaluation
- Version -03 presented in IETF 88 in Vancouver
  - significant rewrite, introduced new options to carry transport information to CoAP nodes (including DNS records)
- Version -04 presented in IETF 89 in London
  - added use cases, introduced transport classification and URIs for multiple transports
- Version -05
  - URI work concluded with transport information in URI scheme
- Version -06 and -07
  - Recommendation to use *coaps+<transport>* scheme for DTLS-encoded CoAP
  - Contains use cases, URI format, properties and requirements of CoAP transports
  - Appendix contains historical work and discarded options

Next steps

- Alternative transports URI format WG discussion seems to have concluded
- Draft would benefit from more reviewers, also from implementers/authors of various transports
  - CoRE meeting at IETF 90 in Toronto indicated several interested reviewers
- Ready and waiting for WG adoption

CoAP Protocol Negotiation

draft-silverajan-core-coap-protocol-negotiation

Bill Silverajan Tampere Univ of Technology

Background

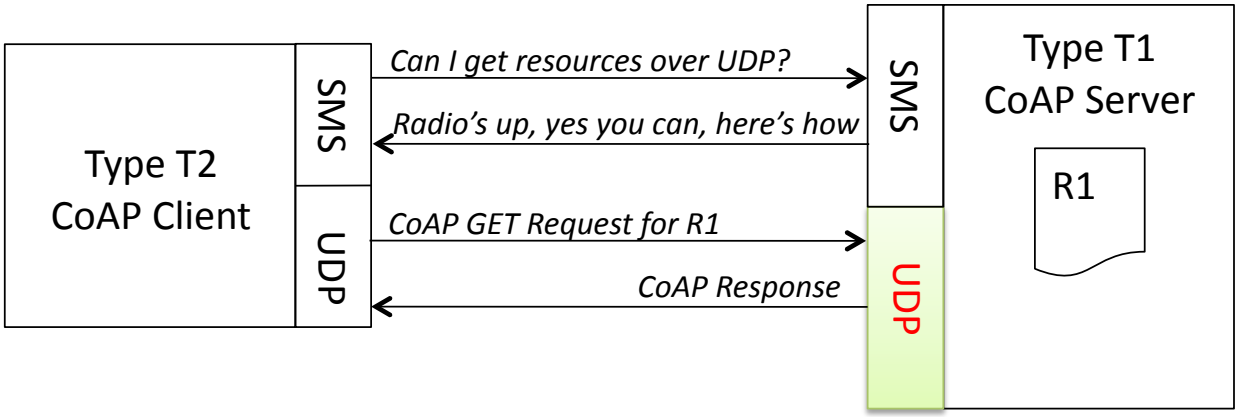
- Aimed at CoAP endpoints wishing for multiple transports and/or locations to exchange CoAP requests and responses
- Transport availability falls into the following node categories
  - Type T0 nodes have a single transport
  - Type T1 nodes have 1 or more transports, which may be in unreachable/off states but at least 1 active transport
  - Type T2 nodes have multiple active transports

Why we need this
(..and we do ☺)

- Enables client-side discovery of server transports
- Reduces URI aliasing at origin server
- Eliminates URI path complexity

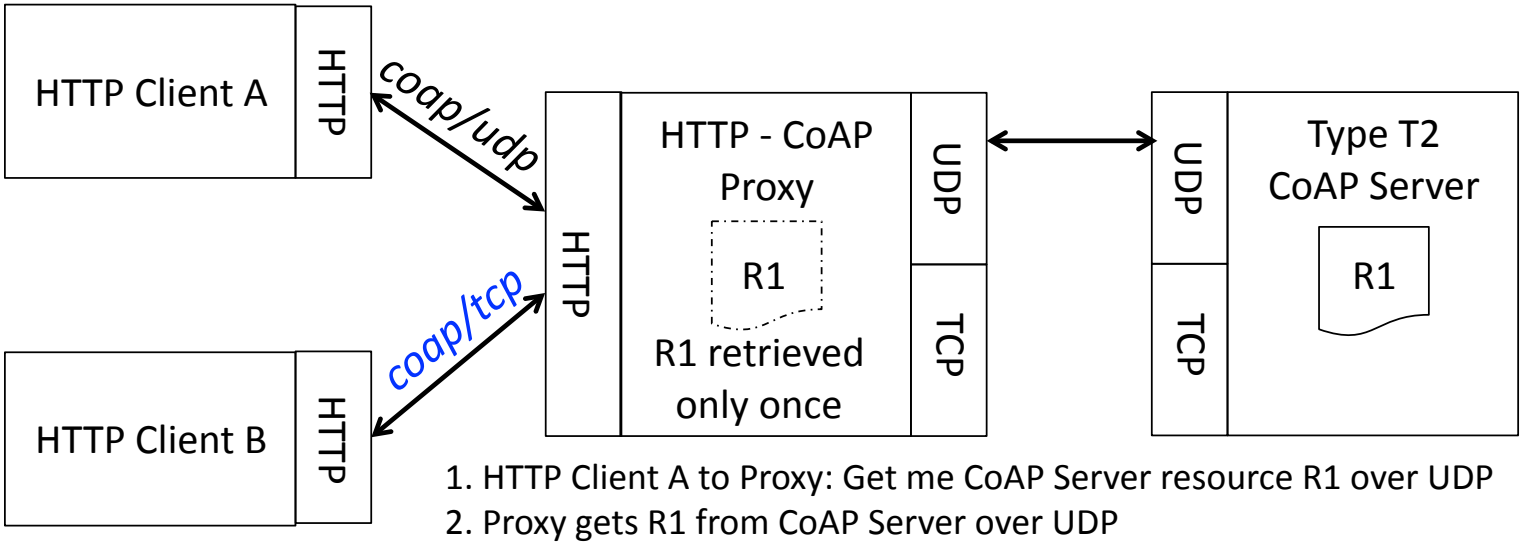
Allow Discovery

- CoAP clients to discover active transports on an origin server



Avoid URI aliasing

- Express same/related resource in alternate transports and locations



1. HTTP Client A to Proxy: Get me CoAP Server resource R1 over UDP
2. Proxy gets R1 from CoAP Server over UDP
3. HTTP Client B to Proxy: Get me CoAP Server resource R1 over TCP
4. Proxy to CoAP Server over UDP: Is it the same resource over TCP?
5. CoAP Server to Proxy over UDP: Yes, it is
6. Proxy Server returns cached R1 to HTTP Client B

Reduce URI path complexity

- Separate locator (endpoint subpath) from identifier (resource subpath)

Example CoAP over WebSocket URI from earlier work (discarded owing to complexity):

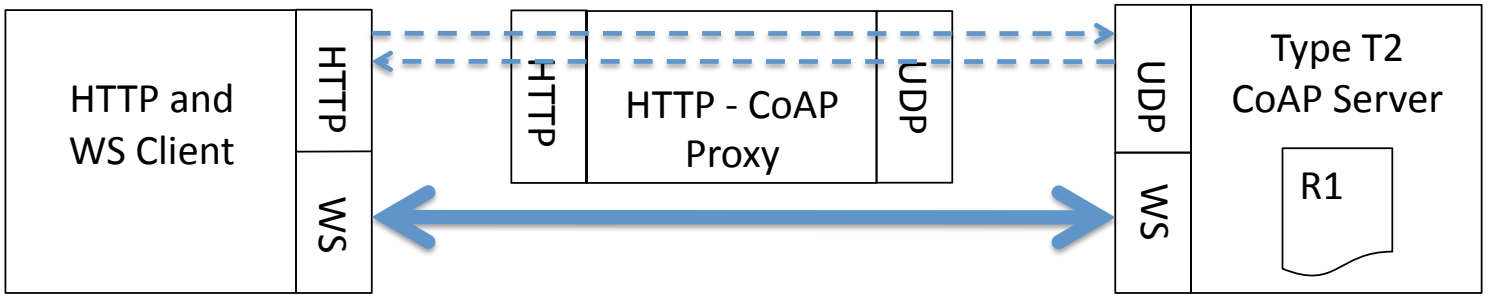
coap-at:ws://www.example.com/WebSocket?/sensors/temperature

WebSocket endpoint locator

CoAP resource Identifier

Reduce URI path complexity

- Separate locator (endpoint subpath) from identifier (resource subpath)



1. HTTP Client uses proxy to reach CoAP Server at UDP endpoint, server.example.com
2. HTTP Client solicits CoAP Server for WebSocket transport and endpoint info
3. CoAP Server responds giving WebSocket endpoint location as server.example.com/path/to/websocket
4. HTTP Client initiates WebSocket handshake with CoAP Server and negotiates CoAP subprotocol
5. Client switches to CoAP over WebSocket and retrieves resources from CoAP Server

How can this be achieved?

- Origin server simply exposes with .well-known/core:
  - a new link attribute "tt" containing list of priority ordered transport types for *coap* and *coaps* resources
  - a new link relation type "alt-loc" containing alternate *endpoint locations* (and not resource path)

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",
<coap+tcp://server.example.net/>;rel="altloc",
<coap+ws://server.example.com/ws-endpoint/>;rel="altloc",
<coaps+sms://12147205269/>;rel="altloc"

Next Steps to consider

- Still lots of open work, contributions welcome!
- Lifetime value for transport types?
- Observe relationship to detect new / expired CoAP transports?
- Is session continuity/resumption across new transports needed?
- Support alt-loc for Type T0 (single transport) nodes too? (eg sleepy node, pub/sub support, etc)
- Security considerations

Coap over TCP

draft-tschofenig-core-coap-tcp-tls
v02

Motivation

- CoAP over tcp/tls solves the NAT problem that enterprise will encounter

Current Draft

- Presentation is done for how version 2 of draft stands now

Redundancy with TCP

- Reliable delivery
- Fragmentation
- Reassembly
- Congestion control, at the CoAP level

Feature modifcation

- Message should be of type NON
- Add a Shim layer
  - Currently (as the document stand) uses a 2 byte header

CoAP URI

- coap-tcp-URI = "coap+tcp:" "//" host [":” port] path-abempty ["?" query]

Port

- The port subcomponent indicates the TCP port at which the CoAP server is located.
- If it is empty or not given, then the default port 5683 is assumed, as with UDP.

CoAPs URI

- coaps-tcp-URI = "coaps+tcp:" "//" host [":" port] path-abempty ["?" query]

Port

- The port subcomponent indicates the TCP port at which the TLS server for the CoAP server is located.
- If it is empty or not given, then the default port 443 is assumed
  - If use on 443, TLS Application Layer Protocol Negotiation Extension MUST be used to allow demultiplexing at server side

Security consideration

- Must be used with TLSv1.2

ALPN Protocol ID

- Protocol:
  - CoAP
- Identification Sequence:
  - 0x63 0x6f 0x61 0x70 ("coap")

Discussion topic

- CON vs NON -> SHOULD/MUST
- Message header
  - 2bytes
  - 4bytes
  - CBOR Style
  - Alternate protocol call for larger than Xbyte

Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

Guidelines for HTTP-CoAP Mapping Implementations

Angelo Castellani, Salvatore Loreto, Akbar Rahman, Thomas Fossati, Esko Dijk

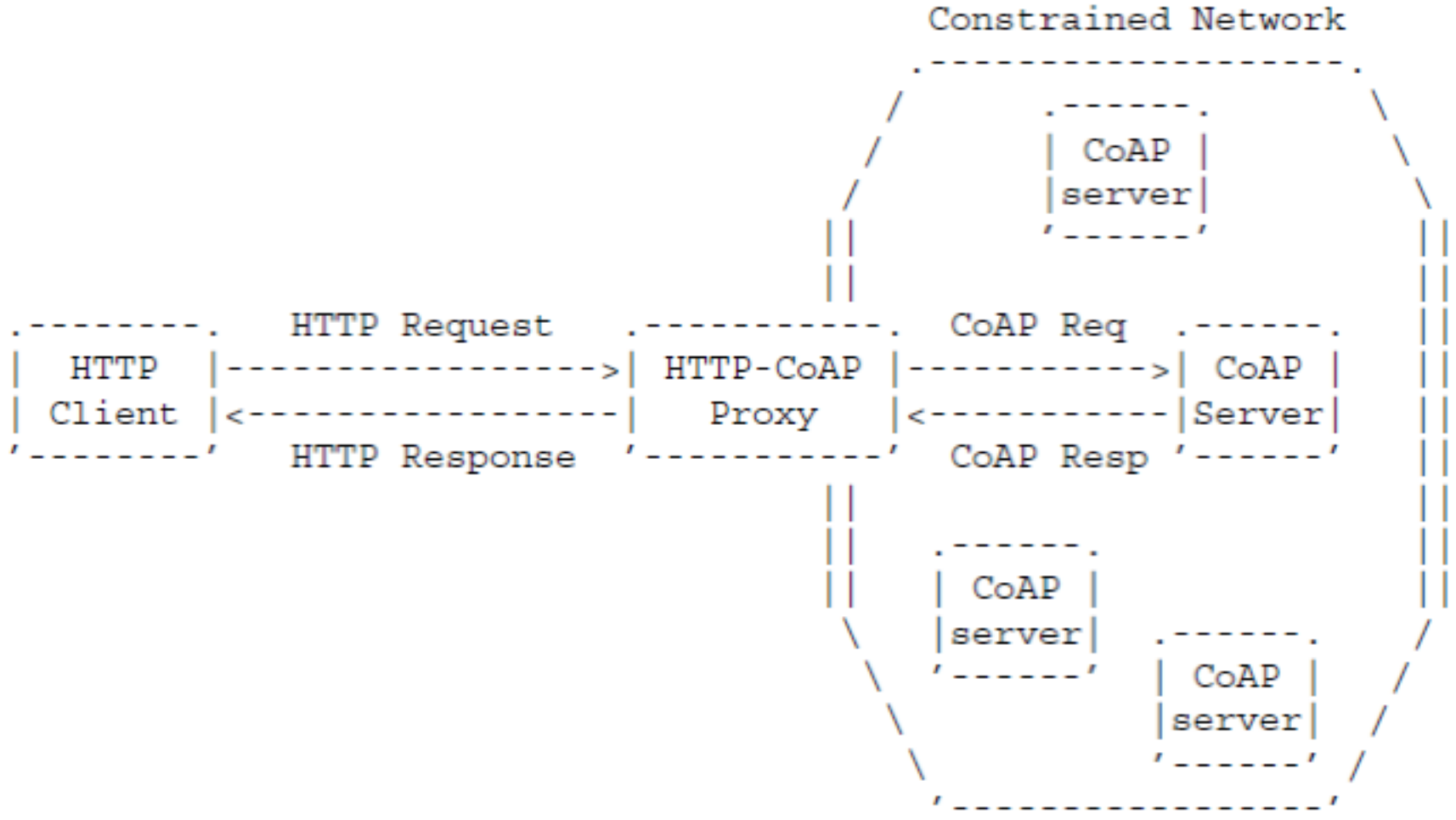
IETF-92, March 2015

http://tools.ietf.org/html/draft-ietf-core-http-mapping-06

Main Changes (from IETF-91 Hawaii)

- Changes from ietf-05 to ietf-06:
  - Addressed Ticket #376 (CoAP 4.05 response mapped to HTTP 405 with use of empty Allow field)
  - Addressed Ticket #379 (Major editorial restructuring to bring more introductory material to beginning)
  - Addressed Ticket #380 (Added IANA request for RT = “core.hc”)
  - Addressed Ticket #381 (Added mapping CoAP 4.01 to HTTP 401 Unauthorized)
  - Addressed Ticket #382 (Fixed error in enhanced form URI template definition of q)
  - Addressed review comments from Chair (Carsten Bormann)
  - Various editorial improvements

Reverse Cross-Protocol Proxy Deployment Scenario



Reminder: Focus of I-D is reverse HTTP-CoAP (HC) Cross Proxy

Open Tickets (1/2)

- Ticket #377 (Define an open ended HTTP media type “application/x-coap<n>)?)
  - Summary: Do we want to allow media type and content formats to evolve freely at the two ends of the translation chain, without the HTTP-CoAP proxy becoming the point where media type information is lost in translation?
    - See message: http://www.ietf.org/mail-archive/web/core/current/msg05798.html
  - Proposal: Define an open ended HTTP media type "application/x-coap-<n>" - where n is the decimal representation of the corresponding CoAP content format - to handle the mapping of CoAP content formats that are unknown to the proxy, instead of falling back to the completely opaque "application/octet-stream".

Open Tickets (2/2)

- Ticket #378 (Include reference to automatic media type mapping update mechanism?)
  - Summary:
  - For HTTP media type to CoAP content format mapping and vice versa: to include a reference to <new I-D> which describes an approach for automatic updating of the media type mapping.
    - See message http://www.ietf.org/mail-archive/web/core/current/msg05798.html
  - Discussion:
  - For example, if there is a running process at IANA to auto-assign CoAP content format numbers to all HTTP media type registry entries, an API could be created to retrieve this list or query media types / content formats. Then a proxy upon encountering a (new) unknown HTTP content format for example could just query via a web API to find the matching CoAP content format.

Ticket Solution to Discuss

- Ticket #376 (CoAP 4.05 response mapped to HTTP 405 with use of empty Allow field)
- Summary:
- HTTP code 405 (Method Not Allowed) MUST include an "Allow" response-header field (Section 7.4.1 of [RFC7231]). However, a CoAP response does not include information about which methods are allowed on the resource. Therefore, if the proxy does not have further information about which methods are allowed on the resource it SHOULD include an empty field value in the Allow header field. The intended interpretation of an empty Allow in this case is "resource temporarily allows no methods" which complies fully to [RFC7231].

- Discussion:
- Is HTTP 405 (Method Not Allowed) with the use of empty Allow field the right solution?
- Or should HTTP 400 (Bad Request) be used?
- Or should there a new CoAP option be defined to map to HTTP Allow header?

Next Steps

- Is the WG satisfied with the closure of the tickets in the current draft?
- What is the best approach for the remaining open issues?
  - For example, do we want to move the issues that require protocol changes to another draft (as this draft is Informative)?

Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

draft-ietf-core-links-json-00.txt

- RFC 6690 (link-format) documents are somewhat foreign to many web app developers
  - would prefer to have them in JSON format
- There is no standard way to represent link-format documents in applications
  - but everyone knows how to handle JSON

→ Define a standard JSON translation for link-format

```
</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"}]
```

CBOR Equivalents of CoRE JSON Formats

Kepeng Li, Ruinan Sun, Akbar Rahman

IETF-92, March 2015

http://tools.ietf.org/html/draft-li-core-cbor-equivalents-00

Scope (1/2)

- JavaScript Object Notation (JSON - RFC 7159) is a text-based data interchange format popular in the Web development environment
- Concise Binary Object Representation (CBOR – RFC 7049) is a binary data format which is very efficient for constrained environments
- This draft defines a common approach for translating JSON objects applicable to the CORE WG into CBOR format
  - When converting many small decisions must be made which if left without guidance can produce slightly incompatible translations
  - Draft also considers converting from other formats to CBOR where applicable
  - (Draft is still preliminary and not all the guidance has been established yet)

Scope (2/2)

- Main scenarios covered:
  - CoRE Link Format (RFC 6690) to CBOR
  - CoRE Link Format in JSON (draft-ietf-core-links-json) to CBOR
  - Groupcomm management JSON (RFC 7390) to CBOR

Example – CoRE Link Format to CBOR

2.4.1. Link Format to CBOR Example

This examples shows conversion from link format to CBOR format.

```
</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"
```

Figure 3: Example from page 15 of [RFC6690]

becomes

```
85                                  # array(number of data items:5)
   a3                               # map(number of pairs of data items:3)
      01                            # unsigned integer(value:1, "href")
      68                            # text string(8 bytes)
         2f73656e736f7273           # "/sensors"
      0c                            # unsigned integer(value:12,"ct")
      18 28                         # unsigned integer(value:40)
      07                            # unsigned integer(value:7,"title")
```

...

Next Steps

- Does the WG think this is a useful topic?
- Are there are other types of JSON objects (to CBOR conversion) that we should cover?

Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

SenML

- Has been around since 2010
- Batching format for multiple sensor values
  - in time
  - from different sub sensors
- Idea has been adopted by OMA LWM2M
  - want to stay compatible
- Proposal: finish the spec, maintaining compatibility
  - add CBOR variant
  - status of XML/EXI variant?
  - check the units table
  - general editorial

SenML in CDDL

```
SenML = {
    ? bn: tstr,         ; Base Name
    ? bt: number,       ; Base Time
    ? bu: tstr,         ; Base Units
    ? ver: number,          ; Version
    * tstr => any,      ; (Extension)
    e: [+ meas],        ; Measurements
}

meas = {
    ? n: tstr,          ; Name
    ? u: tstr,          ; Units
    ? v: float,         ; Value: at least one s or one of v, sv, bv
    ? sv: tstr,         ; String Value
    ? bv: bool,         ; Boolean Value
    ? s: float,         ; Value Sum
    ? t: number,        ; Time
    ? ut: number,       ; Update Time
}
```

Friday

- **09:00–09:03 Intro** All times are in time-warped CDT
- **09:03–09:23 HTTP-CoAP Mapping**
- **09:23–09:36 Formats 1 (Links/Groupcomm)**
- **09:36–09:56 Formats 2 (SenML)**
- **09:56–11:30 Flextime**

Flextime