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

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

All times are in time-warped CEST

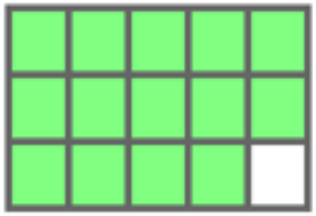
Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

Observe

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

  Now on RFC editor queue



- **Some of the interesting COMMENTs now in draft-ietf-lwig-coap — next slot (1740–1840, Berlin/Brussels)!**

WG documents

- draft-ietf-core-block — 3rd WGLC completed
  - waiting for shepherd writeup
- draft-ietf-core-http-mapping — Fri
  - WGLC very soon
- draft-ietf-core-links-json
  - merged with draft-li-core-cbor-equivalents
- draft-ietf-core-resource-directory — Tue
  - charter work needed (today), added authors
- draft-ietf-core-interfaces
  - to resume activity!

Option 284: No-Response

- Started out as a contribution to CoRE
- Received considerable WG review
- Now a registered option in Specification Required space

- Points to draft-tcs-coap-no-response-option-11
- Plan: make this an RFC via ISE submission
- Review from WG experts is still useful

What else is going on?

- ACE WG: Authentication and Authorization for Constrained Environments
  - finishes being stuck on informational documents
- DICE WG: DTLS In Constrained Environments
  - finishing DTLS profile
  - struck multicast
- COSE: spawned from JOSE (see object security)
- T2TRG (proposed): Thing-to-Thing RG
  - (Summary meeting: Monday, ~ 130 people)
- 6Lo, 6TiSCH, LWIG, ROLL

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

IETF91

core

Search

Preferences | Help/Guide

Wiki | Timeline | Roadmap | Browse | Search

wiki: CoreBacklog

Index | History

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. The WG will also work on a specification enabling broker-based publish-subscribe-style communication over CoAP.

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, with further discussion in -http-mapping. This mapping will be evolved and supported by further 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 very 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 being adapted to the constrained node network requirements in COSE 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, 6TiSCH, LWIG, ROLL, ACE, COSE, DICE), and appropriate groups in the IETF OPS and Security areas. Work on these subjects, as well as on interaction models and design patterns (including follow-up work around the CoRE Interfaces draft) may benefit from close cooperation with the proposed Thing-to-Thing Research Group.

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

A TCP and TLS Transport for the Constrained Application Protocol

draft-tschofenig-core-coap-tcp-tls-04.txt

IETF 92 - Dallas

- Talk about motivation
- Initiate the talk on shim length
- UDP/TCP proxy consideration
- Initiate the talk about Message type
- Sync up with the Web socket Draft

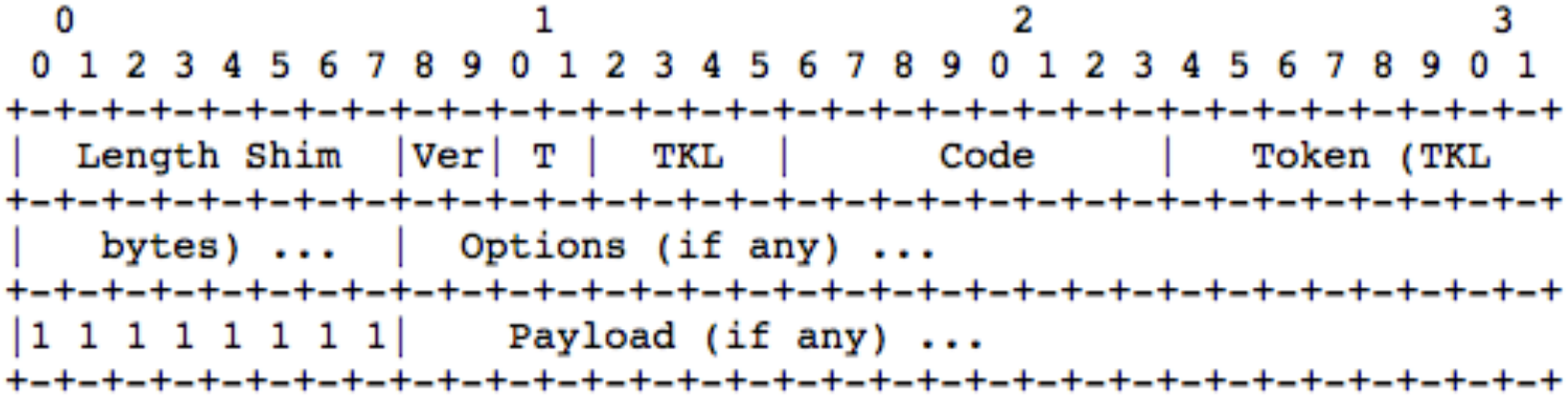
Thank you

Big thanks to all who reviewed

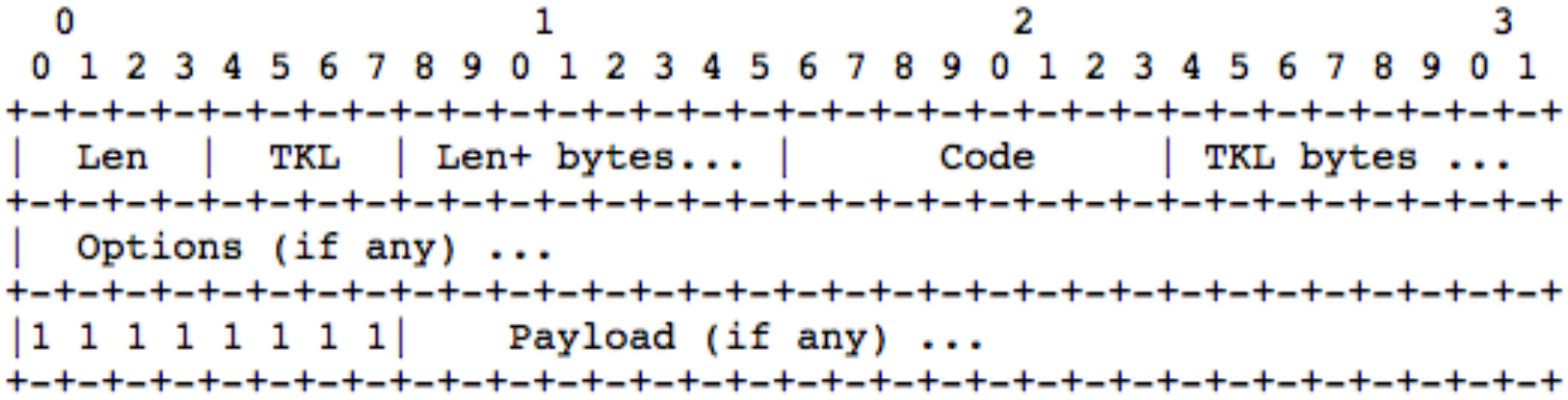
Draft 4 - Length

- 3 type
  - 2 bytes shim
  - CBOR style
  - Option Like

Shim and CBOR



Option Like


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

CON/NON

- Not needed with TCP
- CON and NON are in place for transport reliability (UDP)
- Request/response semantics offers information on processes
- No need for messageID

UDP/TCP Proxy

- Note was added in the draft (no enough)
- Raises questions about blocking

Transmission

- No resilience
- Every TCP session have n number of transaction
- If the connection fails, pending requests are discarded

What’s ahead

Format

- Spelling, grammar
- Section structure
- Cleanup

UDP/TCP proxy impl

- Need to create a proxy to better understand what is needed
- This will also help figure out questions around Blocking

Transmission

- More example
- Give better overview of what happens in alternative paths (connection lost, errors etc..)
- Better explanation for new comers

General

- More transaction diagram
- Better explanation, more diagram
- Not reuse terms that are no applicable e.g. NON
- Resynch with Alternative transport doc to make sure that everything checks

Adoption?

- MUST (rfc2119) be a working group item

Thank you

IETF#93 CoRE Standard Primitives vs Transport Specific Adaptation

Timothy Carey, Alcatel-Lucent, July 2015

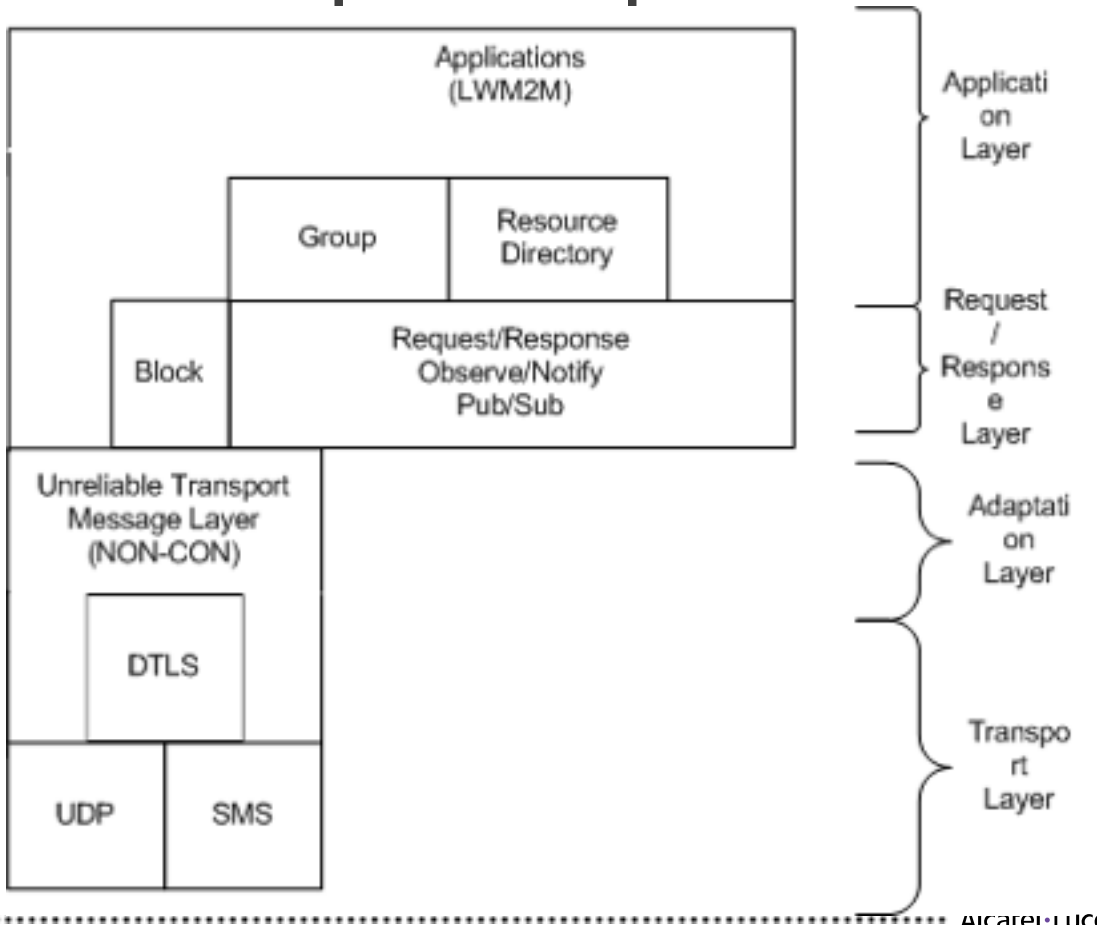
Background

- In review of draft-tschofenig-core-coap-tcp-tls-03, we realized that this draft:
  - Didn't support the CoAP message layer's use of ACK/RST in CON and NON message types or the message-id. In fact, the draft explicitly removed support for CON message types and didn't support CoAP ACK mechanisms – relying on the TCP ack/rst/fin messages and timeout mechanisms.
  - Didn't explicitly discuss how piggy backed responses would be handled.
  - Made the assumption that the Blockwise protocol was supported but did not describe how Blockwise would be supported within the concept of TCP connections.
  - Didn't explicitly discuss how TCP connections related to the higher layer Request-Response/Observe-Notify and the newer Publish and Subscribe message exchange patterns.

- In general this draft caused confusion in how the CoAP message layer should be used by the developers of the Application, Request/Response and Transport layers for CoAP.

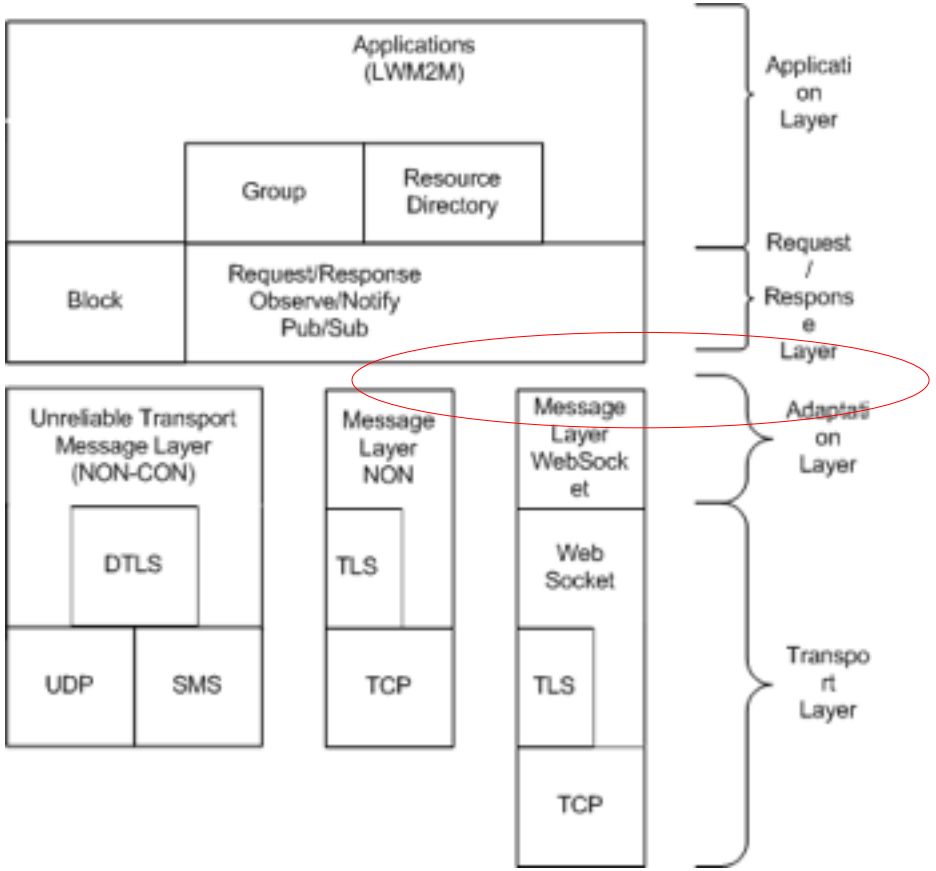
Current CoAP Layers with Request/Response features

- This figure depicts the current CoAP layers for UDP/SMS with the NON-CON message layer consistent for UDP and SMS



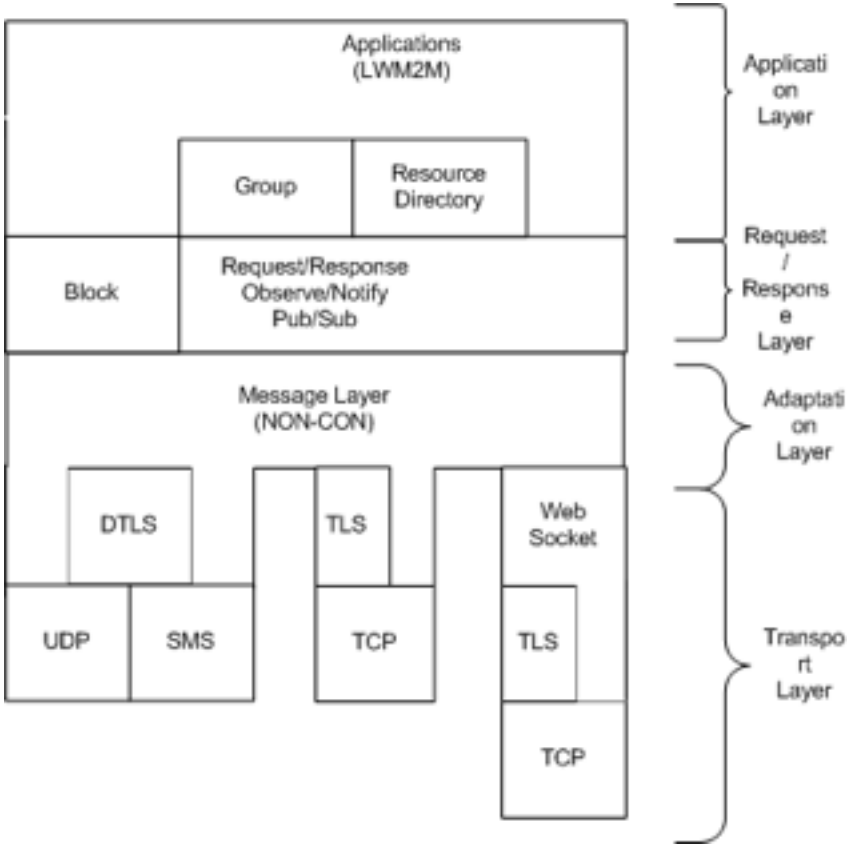
CoAP Layers – With new Transports

- With the new transports there isn't a single consistent interface between the Adaptation Layer and the Request/ Response Layer.
- Since we do not have standard set of messaging primitives each Transport protocol will have to say how it adapts to the various elements of the Request/ Response Layer rather than say how they would implement the standard set of messaging primitives.



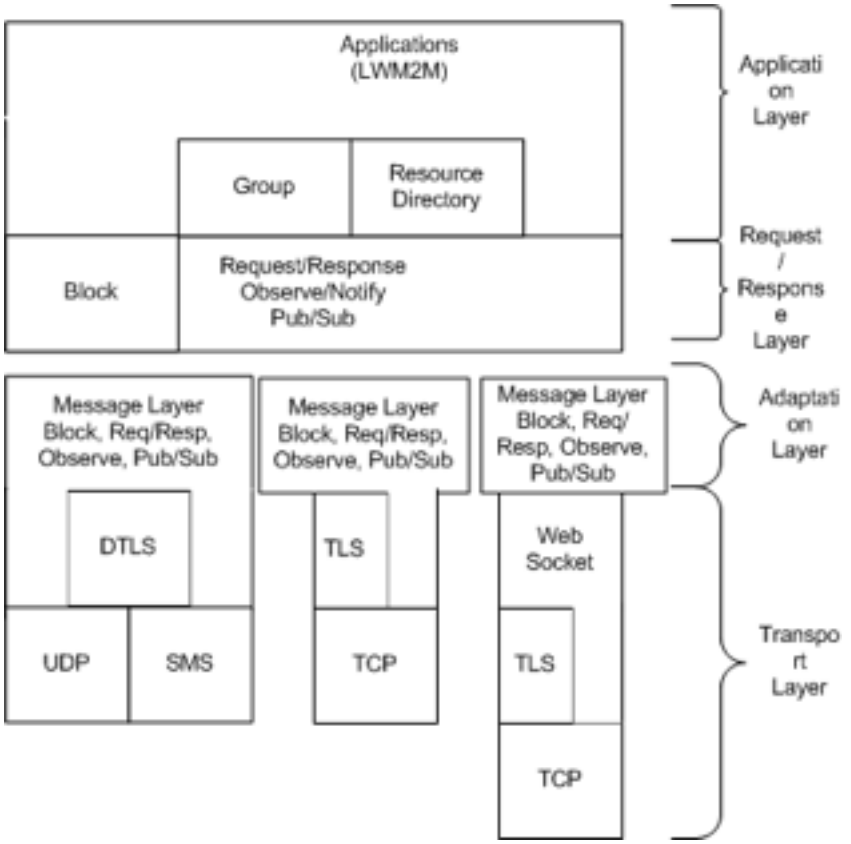
CoAP Protocol Layers – Standard Message Layer

- Standard Primitives
  - Transport protocol would describe how to implement the CON, NON messages with ACK, RST responses.
  - Transport protocol would describe how to adapt timeouts and state processing



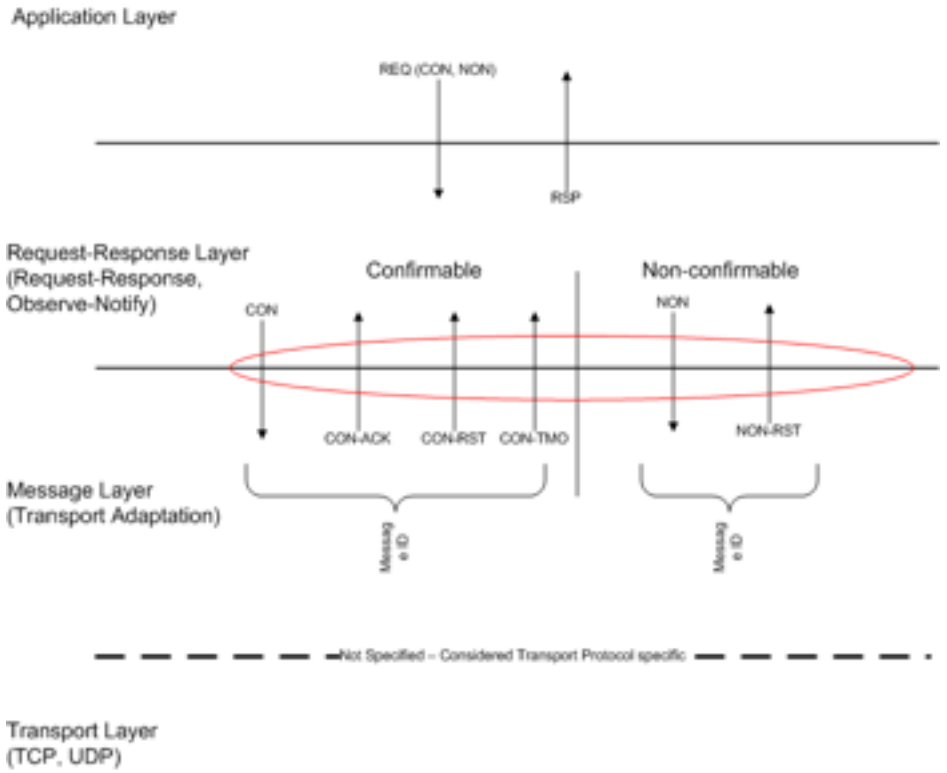
CoAP Protocol Layers –Transport Specific Adaptation

- Transport Specific Adaptation
  - Transport protocol would specify how the Request/Response Layer exchange patterns and features would be adapted by the Transport protocol



CoAP Protocol Layers – Benefits of Standard Primitives Between the Request/Response Layer and the Message (Adaptation) Layer

- IETF Drafts that focus on features in Request/Response Layer will know what is provided by any Transport protocol.
- IETF Drafts (Request/Response, Transport Layers) will know the messages needed to be implemented and provided
- We are not suggesting Message Layer mechanisms like Timeout processing would be exposed just the messages.



CoAP Protocol Layers – Application Layer Use of Confirmable and Non-confirmable Messages

- RFC-7252 specified 2 message type indications to be filled in by the end application (NON, CON)

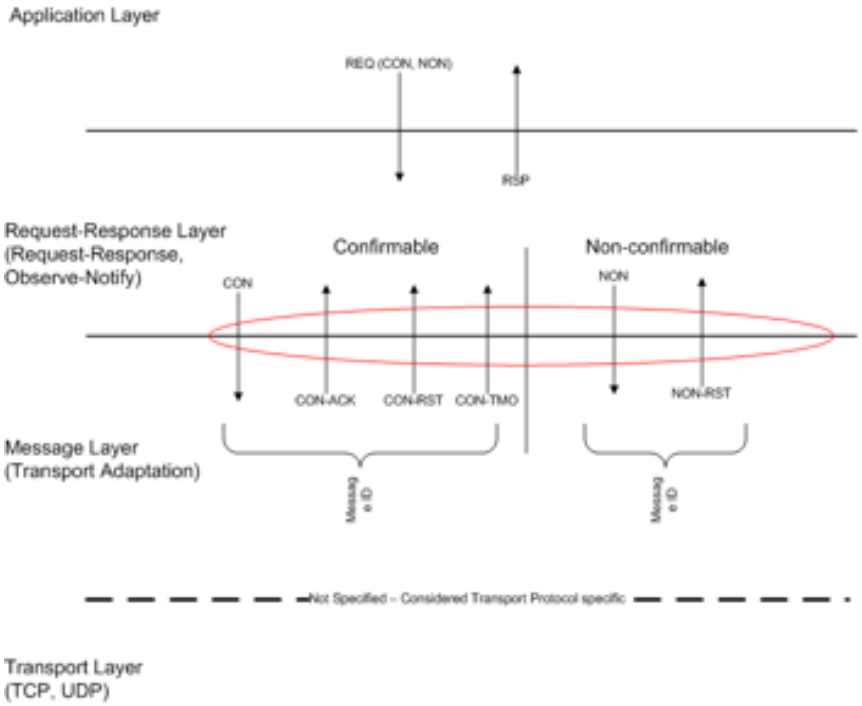
- If the standards primitives are not implemented then Applications MUST be aware of the Transport protocol when invoking requests (not good)

    If (confirmable) then

        If (TCP) then sendNON

        elseIf (UDP) then sendCON

        …



Modifications to TCP draft to account for Request/ Response Layer Usage

- TCP Connections
  - Need to include support for persistent/long TCP Connection with multiple Request/Responses. The draft provides the text taken from Web Sockets **but still doesn't allow for responses be allowed over different TCP connections as the originating Request. We should not care which TCP/TLS connection conveys a Request or Response. This is important for Notifications to extend past TLS sessions.**
- Blockwise Transfer
  - Need to include explicit support for Block transfers along with the use of TCP ack
- Observe
  - Use of Confirmable messages in the Observe draft (section 1.2, 3.5, 3.6, 4.5, 4.5.1)
  - Use of Message Id in Non-confirmable messages in the Observe draft (section 4.5)
  - Adaptation of congestion control (section 4.5.1)
- Use of Message Id
  - Use of Message Id to ensure no duplication can occur through the Request/Response layer.
  - TCP will only ensure no duplication at the TCP layer. It doesn't prevent an invoking Request/Response layer from sending the message more than once for any reason (good or bad).

Every success has its network

How to confuse an implementor (1)

- CoAP Message Layer has choice between reliable and unreliable
  - unreliable needed for multicast, useful for regular, non-critical updates
- “unreliable” sounds unreliable
  → “confirmable”/“non-confirmable”

How to confuse an implementor (2)

- Imply that a message layer ACK is only provided after request/response layer has checked message structure (RST otherwise)
  - ACK starts to look like an application layer confirmation

How to confuse an implementor (3)

- Just to have something to put into a now unused field, talk about “non-confirmable” messages.

Transport layer reliability vs. Application Layer (1)

- CON means that a transport layer reliability is desired
  - Always provided by TCP variant
- NON means that transport layer reliability is not required
  - Can't do anything with this information on TCP

Transport layer reliability vs. Application Layer (2)

- ACK means that the sender can stop sending retransmissions
  - Not a statement from the application
- Application layer response comes at the response layer: in the 2.05 or 4.06 etc.

The desire for custody transfer

- When does an information source know that the information has been acted on (e.g., committed to stable storage)?
  - Information in request: by response
  - Information in response: ———, hmm.

How to do custody transfer of response? (1)

- (Important for buffer management as a result of GET or observe notifications.)
- Hack with UDP/DTLS CoAP: Consider the ACK to be the transfer confirmation.
  - But that comes from the message layer, so this assumes something that is not interoperable

How to do custody transfer of response? (2)

- Define an explicit, interoperable mechanism?
- For TCP, can amortize stable storage operations over multiple exchanges.
  - Simple confirmable checkpoint does it.
- For UDP, need to link explicitly (three-way).

Do we want to do something about custody transfer?

- Use case?
- Do we ignore UDP and let people continue to use the ACK hack?
- (Easy to add to sequenced transfer like TCP.)

Any other transport-related surprises/opportunities?

- E.g.:
  do we need the observe sequence number for TCP?

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

CoRE Resource Directory

draft-ietf-core-resource-directory-04

Updates

- Lighting Example with DNS integration
- Example use of RD by OMA LWM2M
- Function Set Protocol Binding to HTML interface
- Read Links function for inspection of links
  - Returns a representation of the link-format metadata registered for an endpoint

Open Issues

- LWM2M allows creation and removal of resources (object instances); today this would be done by unregistering and re-registering the new link-format metadata
- Section 4.0 Simple Directory Discovery provides no means for managing the registration or links
  - IETF 92 intended to remove but got feedback that it is being used

Roadmap

- Add PATCH operation to enable incremental modification of the link-format metadata for endpoints
- Clean up security section and add specific recommendations, requirements

Advanced Resource Directory Features

Akbar Rahman

IETF-93 (Prague), July 2015

https://tools.ietf.org/html/draft-rahman-core-advanced-rd-features-00

Introduction

- The Resource Directory (RD) is a key element for successful deployments of constrained networks
- Similar to the HTTP web search engines (e.g. Google), the RD for CoAP should also support useful search query responses beyond a basic listing of relevant links
- This draft proposes several new features to be considered for the RD. The only goal of this draft is to trigger discussion in the CORE WG so that all relevant features for RD evolution are taken into account during CORE re-charter activities

Proposed RD Additional Features (1/)

- Explicit HTTP interfaces
  - The current CoRE specifications are written explicitly with CoAP examples. The specifications should be expanded to also explicitly support HTTP (e.g. HTTP request and response codes).
  - There may be some RD interfaces, such as multicast and Group Function, that may not be supported by HTTP and those should also be explicitly identified and excluded.

Proposed RD Additional Features (2/)

- Mirror Server
  - The CoRE WG has previously discussed the concept of a mirror server in relation to supporting sleepy devices.
  - Specifically, [I-D.vial-core-mirror-server] recommends to create a new class of RDs which store the actual resource representations (as opposed to simply storing the URI) in a special type of RD called the Mirror Server.
  - Communicating devices can both lookup the resource, and then also fetch directly the resource representation, from the Mirror Server regardless of the state of the sleepy server.

Proposed RD Additional Features (3/)

- Re-direction to another RD
  - A given RD may not have the URIs being queried for registered in its database. The given RD should have the capability to re-direct the querying client to another RD which may have the information of interest.
- URI Ranking
  - Current Internet search engines have extensive methods for ranking the URIs returned to a human initiated search query
  - For example, the concept of Search Engine Optimization (SEO) has spawned a large industry in the web world for specifically this purpose
  - The concept of URI ranking (to indicate the "value" of the URI) should also be supported by the RD

Proposed RD Additional Features (4/)

- Indication of transport protocol
  - Several proposals exist (e.g. [I-D.silverajan-core-coap-alternative-transports]) in the CoRE WG to support alternative transports (e.g. TCP, SMS) for CoAP beyond the current UDP transport
  - It would be very useful if search results from a RD indicated the type of transport supported by a given URI

Next Steps

- The proposed set of feature extensions for the RD will improve the constrained environment search capability and make deployments more efficient
- These RD feature extensions should be individually considered during the CoRE re-charter discussions
- Evolution and forward thinking is required for the CoRE RD, as constantly occurs in the current Internet for HTTP web search engines

All times are in time-warped CEST

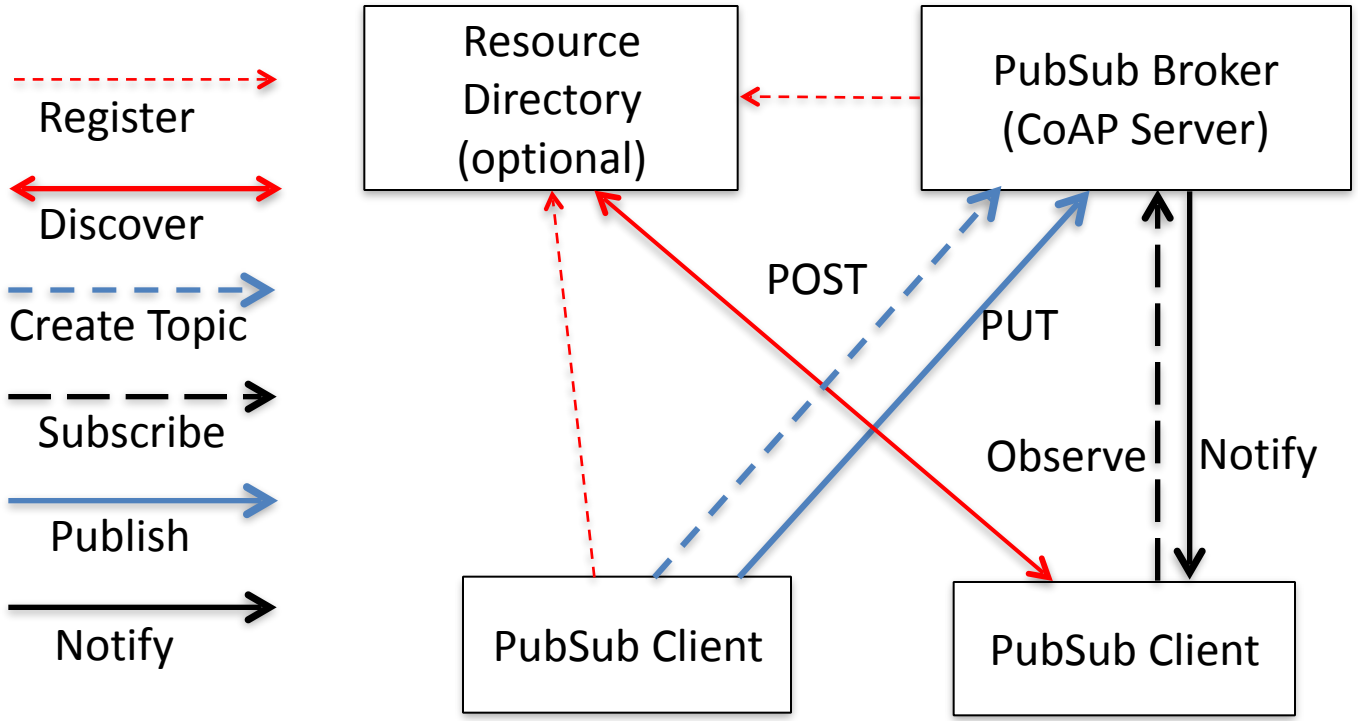
Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

CoAP pub/sub

draft-koster-core-coap-pubsub-03

Architecture Review



Updates

- Added source feedback flow control using a new CoAP response code 4.29 (Too Many Messages)
  - Using Max-Age to set retry interval; should we define another option for Retry-After?
- Content-formats are now decoupled between publishers and subscribers
- Content-format is set upon topic creation
- Changed PUBLISH to NOTIFY for subscriber state updates

Running Code

- At least one implementation exists from VTT
- Implemented simple discovery, no security
- Good implementation notes, few corrections
- One interesting note:
  - Subscribe uses CON, therefore notifications use CON regardless of what publishes use (libcoap feature)

Issues and Feedback

- Matthieu Vial review
  - Pub/sub isn't either RESTful OR traditional pub/sub with QoS and queueing – some of the same issues as mirror server
  - Explain topic registration better
  - What about disconnected clients, is there queueing?
  - Explain or constrain the content-format for publish vs. subscribe, can a broker convert formats?
  - Default Max-Age for topics and updates

Open Issues carried over

- How to handle CoAP block transfers
- Should we allow POST as well as PUT for publish operations?
  - Pubsub doesn't propagate POST operations to subscribers, just sends notifications
- Data series retention: time series object + queue per subscriber?

Roadmap

- Define handling of block transactions
- Clean up security section and add specific recommendations, requirements
- QoS description based on NON, CON
- Explain broker-as-origin
  - Broker is the definitive data source and resource identifier
  - Publish is an update from a “stateless” client
  - ACLs live on the broker, bind to TLS identity?
- Improve explanations of some other things

- **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 CEST

Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

All times are in time-warped CEST

Friday

- 11:50–11:55 Intro
- 11:55–12:10 HTTP-CoAP Mapping (TF)
- 12:10–12:25 CoRE Interfaces (MK)
- 12:25–12:45 Object Security (GS)
- 12:45–13:00 SenML (AK)
- 13:00–13:05 CoRE Formats (Links/Groupcomm)
- 13:05–13:13 HTTP/2 (GM)
- 13:13–13:20 Flextime

All times are in time-warped CEST

Tuesday II

- ~~15:20–15:30 Intro, WG status~~
- 15:30–16:10 CoAP over reliable (SL, TC, BS)
- ~~16:10–16:35 Resource Directory ()~~
- ~~16:35–16:55 Pubsub,~~ normally-off (MK, PV)
- 16:55–17:15 COMI (MK, PV)
- 17:15–17:20 PATCH (PV)

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

CoRE working group

CoAP Management Interface
draft-vanderstok-core-comi-07

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

July 21, 2015

Motivation

Provide transport over CoAP between “reduced resource” clients and 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 with respect to version 6

Many additions were suggested by Michel Veillette

Current version 7

- Rehash error return changed
- LWM2M comparison
- Notification handling
- Use of Patch
- Discover alternative name encoding
- Select and keys parameters usage
- And others

Rehash error return, description

Hash collision occurs when two names have the same hash in a given server
With 30.000 names in one server probability about 10%

The conflicting names have to be rehashed in the server.

When conflicting hash is invoked by client,
new hashes are returned accompanied by module name
to distinguish clashing names
(assumption: names in a module do not conflict)

Rehash error return, example

Example (h2 is clashing hash):

REQ: GET example.com/mg/h2

RES: 4.00 “Bad Request”

```
{
“ietf-yang-hash:yang-hash” : {
  “rehash” : [
     { “hash” : h2,
    “object” : [
        {  “module” : “foo”,
          “newhash” : h21 },
        {  “module” : “bar”,
           “newhash” : h22 }
     ] }
  ]}
}
```

Alternative name encoding

The default name size reduction scheme is hashing the names with 30-bit murmur3

Other name size reduction schemes are possible (see 6tisch discussions)

The resource /mg/num.typ returns the scheme in use.
The default hashing scheme returns the string: “yanghash”

Alternative schemes need to be documented in other drafts

Notification, description

The yang notification is taken over in CoMI

Events can generate notifications
which are appended to one single default stream: /mg/stream
A new notification replaces the current one. (Queue of one)

Reception of generated notification instances is enabled with Observe

Notification, example

```
Module example-port{
Notification-example-port-fault {
  leaf port-name{ type string; }
  leaf port-fault{ type string;}
}
}
```

```
GET example.com/mg/stream
(observe option register)

RES 2.05 Content
{
    “example-port-fault”: {
        “port-name” : “0/4/21”,
        “port-fault”   : “Open pin 2” }
}
```

Select and keys parameters, description

"Keys" parameter selects an instance of a list
"Select" parameter selects subtrees of containers

When select is used, key parameters are specified in brackets

?select=sub-tree_hash(indexfield1_value,indexfield2_value)

Short for:
?select=sub-tree_hash; keys=indexfield1_value,indexfield2_value

Select and keys parameters, example

Index of list is specified by field2 and field3 values

REQ: GET example.com/mg?select=wt7w_(“ipv4”, “reachable”)
RES: 2.05 Content

```
{   0x1067f289 : [ {
    field1:  value,
    field2: “ipv4”,
    field3: “reachable”,
    field4: another_value
}]
}
```

TODO plan

- Any suggestions
- WG acceptance?

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

CoRE working group

Patch method for CoAP
draft-vanderstok-core-patch-01

P. van der Stok, A. Sehgal

July 21, 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.

For example: 6tisch applications will wish to change one entry of a YANG list

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

Progress with respect to version 0

Klaus Hartke pointed out essential differences between CoAP and HTTP

- Caching
- Response codes, and error handling

Added a concrete example using RFC6902

Made motivation text more general

Formulation improved at many places.

Open issues

- Content format standard:
  - Link-format,
  - draft-ietf-netconf-yang-patch-05,
  - RFC 6902,
  - RFC7396,
  - CBOR
- Idempotent, atomic? (in this version, taken from CoAP PUT)
- Introduce additional CoAP errors?

Ready for WG adoption?

July 21, 2015

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 Pubsub, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

Insert Simon's slides here

CoAP Communication with Alternative Transports

draft-silverajan-core-coap-alternative-transports

Bill Silverajan Tampere Univ of Technology
Teemu Savolainen Nokia Technologies

Current Status

- Version – 08
  - Draft being streamlined based on reviewer comments
  - Unnecessary use cases and/or discussions on speculative transports have been removed
  - Some minor clarifications and fixes

Next version: Issues TBD (1/4)

- Establishing CoAP Transport URI Governance, Semantics, Ownership
  - Namespaces and nested prefixes don't exist in URI schemes
  - Do we need governance or ownership of certain transport URIs? **(YES/NO)**
    - Eg coap+udp:// or coap+lwm2m://

Next version: Issues TBD (2/4)

- Establishing CoAP Transport URI Governance, Semantics, Ownership
  - Do we establish recommendations (eg transport implementation documents MUST include URI scheme for secure versions), and why? **(YES/NO)**
    - <coap+*transport*>**s**:// or <coap**s**+*transport*>:// or something else (Draft already has some pointers here)
    - coaps+tcp:// vs coap+tcps:// vs coap+tls://
    - coaps+sms:// vs coap+smss:// vs coap+dtls+sms://
    - coap+wss:// vs coaps+wss:// ☺

Next version: Issues TBD (3/4)

- Draft also has Transport Analysis and Properties Section
  - Guidelines for implementors to consider pitfalls and challenges when transporting CoAP Request/Reponse messages
  - Continue this to reflect/align with existing discussions, design choices and contributions? **(YES/NO)**
    - Eg for reliable transports, we now also have other drafts, like draft-carey-core-std-msg-vs-trans-adapt

Next version: Issues TBD (4/4)

- Retain work on Transport URI format
  - Main body contains URI design requirements and CoAP Transport URI format
  - Appendix contains all the discarded various URI formats and reasons for discarding
  - Should more be done *within the main body* to explain why transport identifier is in URI scheme? **(YES/NO)**

CoAP Protocol Negotiation

draft-silverajan-core-coap-protocol-negotiation

Bill Silverajan Tampere Univ of Technology

Background: CoAP Transport URI

Transport Info in URI	RFC 3986 Conformance	Relative references	URI aliasing	Location Precision
Scheme	●	●	●	●
Authority	●	●	●	●
Path	●	●	●	●

Choice was then made

Transport Info in URI	RFC 3986 Conformance	Relative references	URI aliasing	Req 4.1.4
Scheme	●	●	○	●

Design Requirements

- For ID-core-coap-alternative-transports:
  - Conformance to RFC 3986 encoding rules
  - Precise description of transport and location
  - Ensure relative URIs are resolved correctly
- For ID-core-coap-protocol-negotiation:
  - Expose transport options to interested clients
  - Using CORE link format to tackle resource caching and multiple representations
  - Eliminate URI path (locator/identifier) complexity

What is in the pipeline

- 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 always-active transports
- For T2 nodes
  - Investigate need for session continuity/resumption from one transport to another, and required context for transfer
- For T1 nodes
  - Lifetime value for transport types
  - Observe relationship to detect new / expired CoAP transports
- For T1 nodes
  - Support for alt-loc relationship (eg sleepy node, pub/sub support, etc)
- Security considerations

All times are in time-warped CEST

Tuesday

- **15:20–15:30 Intro, WG status**
- **15:30–16:10 CoAP over reliable (SL, TC, BS)**
- **16:10–16:35 Resource Directory ()**
- **16:35–16:55 ~~Pubsub~~, normally-off (MK, PV)**
- **16:55–17:15 COMI (MK, PV)**
- **17:15–17:20 PATCH (PV)**

CoRE working group

Sleepy Nodes
draft-zotti-core-sleepy-nodes-03

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

July 21, 2015

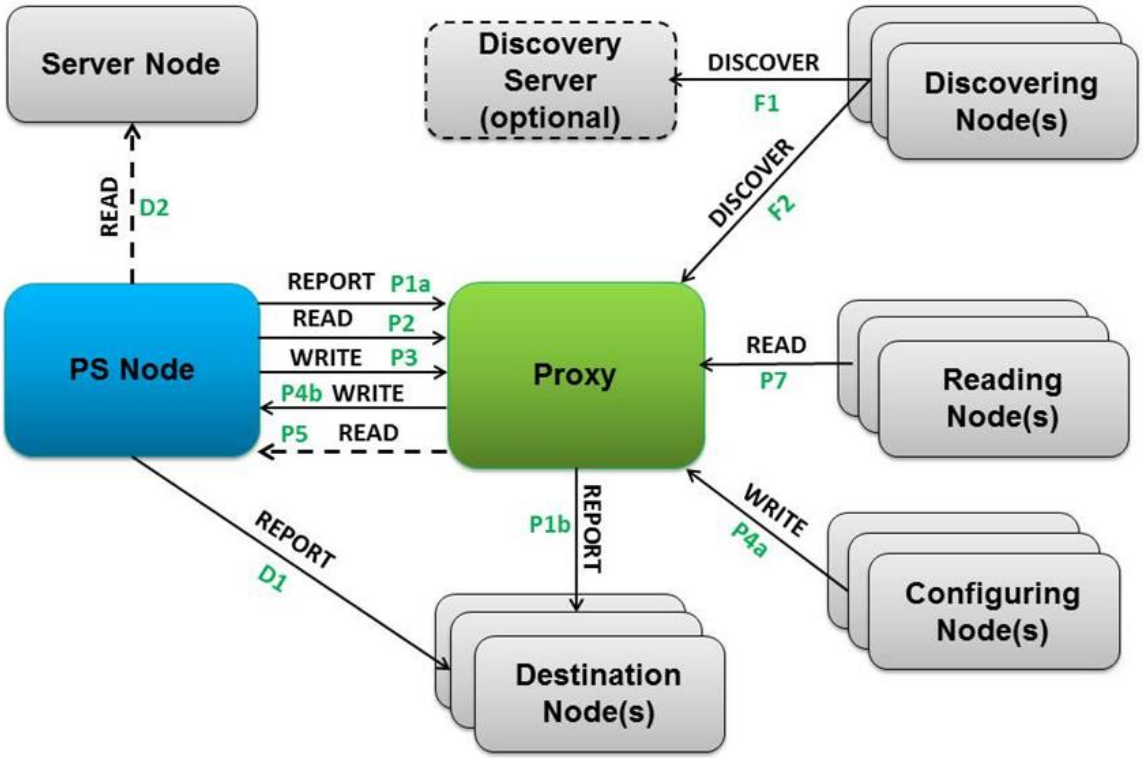
Changes with respect to 02

Many thanks to Matthieu Vial who allowed us to copy large parts of text and examples from draft-vial-core-mirror-server-01

Detailed specification of interfaces

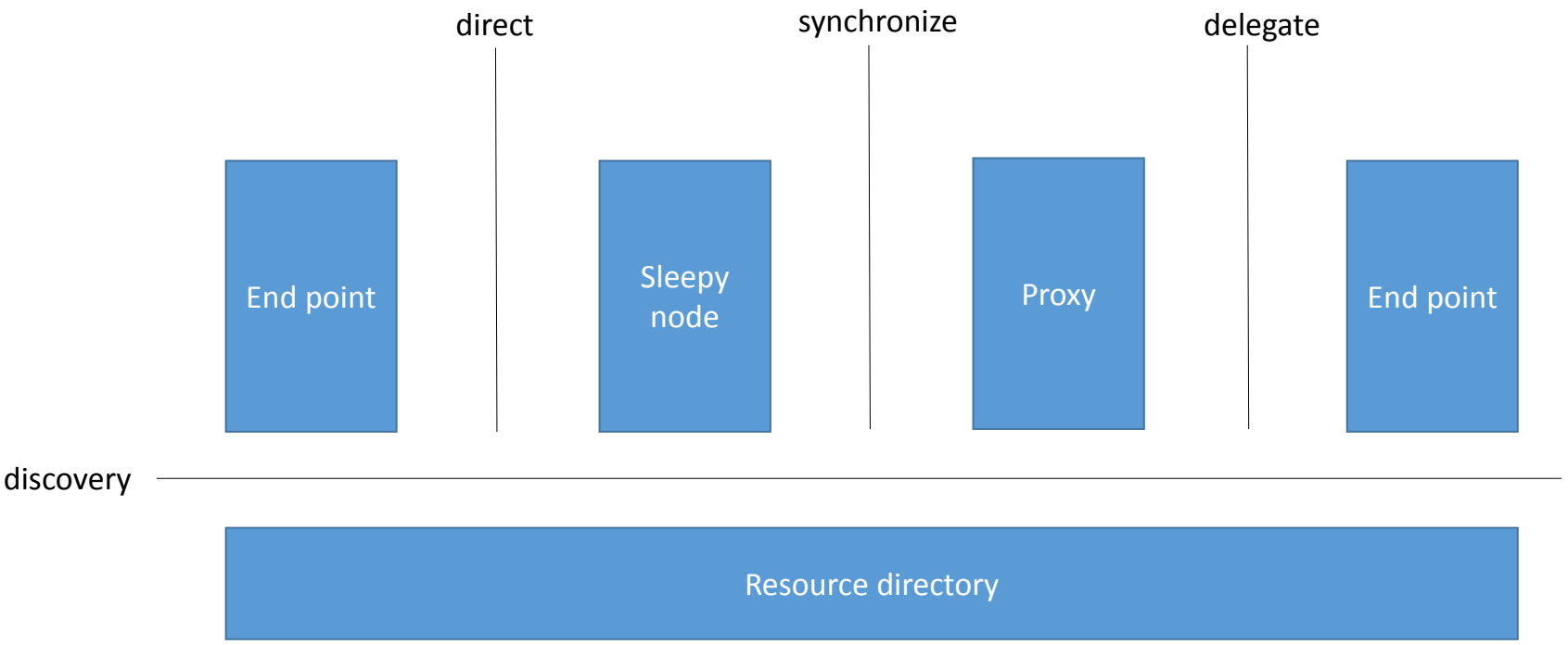
July 21, 2015

Role of nodes around sleepy node



July 21, 2015

Interfaces around sleepy node



July 21, 2015

Interfaces around sleepy node

Discovery interface: updating proxy and resource directory

Synchronize interface: How to register, initialize and update delegated resources, and update values in sleepy node

Delegate interface: Reading writing delegated resources at proxy

Direct interface: Direct Notification from Sleepy node to End-points

PubSub and Sleepy node proxy

In Delegate interface (proxy->EP) Observe is used.

Little improvement from PubSub to replace Observe, because

- No multiple producers (only one proxy)
- Client discovers resources (not topics)

WG document?

All times are in time-warped CEST

Friday

- 11:50–11:55 Intro
- 11:55–12:10 HTTP-CoAP Mapping (TF)
- 12:10–12:25 CoRE Interfaces (MK)
- 12:25–12:45 Object Security (GS)
- 12:45–13:00 SenML (AK)
- 13:00–13:05 CoRE Formats (Links/Groupcomm)
- 13:05–13:13 HTTP/2 (GM)
- 13:13–13:20 Flextime

Guidelines for HTTP-CoAP Mapping Implementations

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

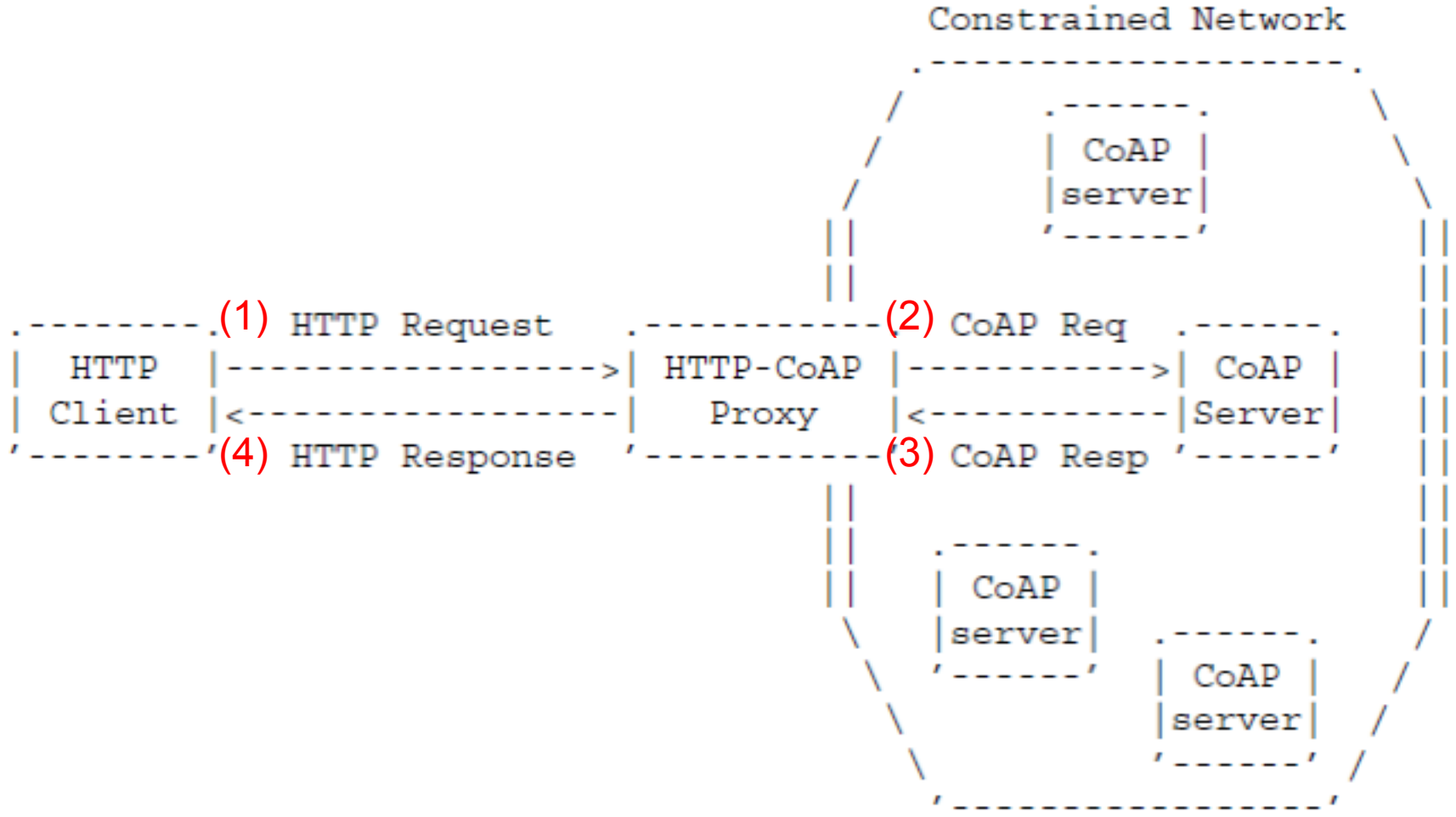
IETF-93 (Prague), July 2015

https://tools.ietf.org/html/draft-ietf-core-http-mapping-07

Main Changes (from IETF-92, Dallas)

- Changes from ietf-06 to ietf-07:
  - Addressed Ticket #384 (Unclear how to discover CoAP resources from a HTTP client through a Proxy)
  - Addressed Ticket #378 (Include reference to automatic media type mapping update mechanism?)
  - Addressed Ticket #377 (Define an open ended HTTP media type “application/x-coap<n>”?)
  - Addressed Ticket #376 (CoAP 4.05 response can’t be translated to HTTP 405 by HC Proxy)
  - Added note to comply to ABNF when translating CoAP diagnostic payload to reason-phrase
  - Currently no open tickets!

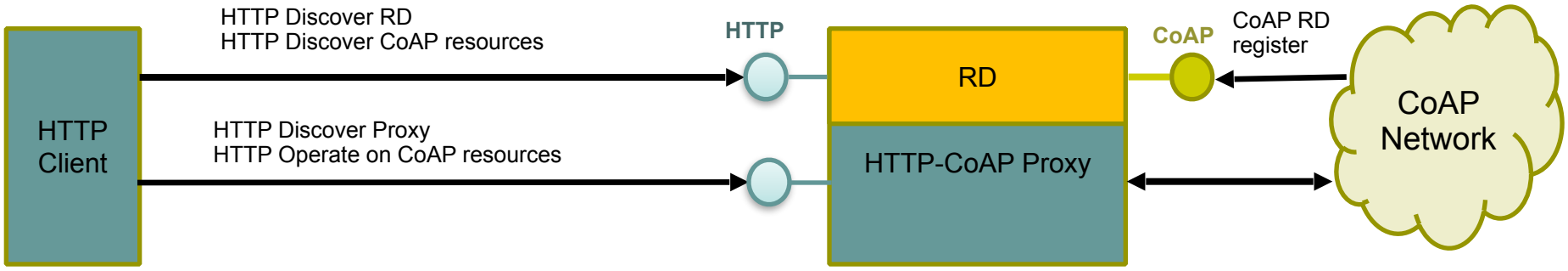
Reverse Cross-Protocol Proxy Deployment Scenario



Reminder: Focus of I-D is reverse HTTP-CoAP (HC) Cross Proxy (i.e. Starts with HTTP Request (1) coming to Proxy)

Summary of Ticket Solutions (1/3)

- Ticket #384 (Unclear how to discover CoAP resources from a HTTP client through a Proxy)
  - Solution - Section 5.4.1 describes briefly (informative) how to discover CoAP resources from an HTTP client that can interface with a Resource Directory (RD)
  - I.E. HTTP client can discover CoAP resources of interest by doing an RD lookup to the RD (if integrated with a Proxy)



Summary of Ticket Solutions (2/3)

- Ticket #378 (Include reference to automatic media type mapping update mechanism?)
  - Solution - For HTTP media type to CoAP content format mapping and vice versa: a new draft (TBD) may be proposed in CoRE which describes an approach for automatic updating of the media type mapping.
    → No updates to this draft.
  - See also Solution to Ticket #377

Summary of Ticket Solutions (3/3)

- Ticket #377 (Define an open ended HTTP media type “application/x-coap<n>”?)
  - Solution - Added IANA section that defines a new HTTP media type "application/coap-payload" and created new Section 6.2 on how to use it.

- Addressed Ticket #376 (CoAP 4.05 response can’t be translated to HTTP 405 by HC Proxy)
  - Solution - Updated Table 2 (and corresponding note 7) to indicate that a CoAP 4.05 (Method Not Allowed) Response Code should be mapped to a HTTP 400 (Bad Request).

Next Steps

- Is the WG satisfied with the closure of the tickets in the current draft?
  - Currently no open tickets!
- Are we ready for WGLC?

All times are in time-warped CEST

Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

CoRE Interfaces

draft-ietf-core-interfaces-03

Overview

- Design Patterns using CoAP and related standards
- Defines the concept of a function set consisting of URI template and functions mapped to interface descriptions
  - Also used in CoRE RD to describe it's interfaces
- Defines Observe Attributes pmin, pmax, st, lt, gt which are set on a resource using query parameters
- Defines "bindings" to resources which synchronize the state of resources in different endpoints, through the exchange of resource representations
  - A binding implements the client role and associates a source resource with a destination resource
  - Polling, Observe, and Push type bindings
  - Bindings use observe attributes
- Defines some function sets for simple machine interactions
  - sensor, actuator, batch, link list, linked batch, parameter, and binding

Updates

- Harmonized the Observation Attributes within the document between bindings in section 4 and attributes in section 5.9
- Changed the definition of attributes lt, gt
- Added Observation Attributes to the WADL description
  - Created getattr and setattr methods for handling Observe Attributes and added them to the observable resources

Open Issues

- Clarifications needed for the sensor, etc. interfaces
- Should this be moved to standards track?
- Should this be how we recommend people to use CoAP?
- What about hypermedia controls instead of function templates?
- draft-hartke-core-apps-01

All times are in time-warped CEST

Friday

- 11:50–11:55 Intro
- 11:55–12:10 HTTP-CoAP Mapping (TF)
- 12:10–12:25 CoRE Interfaces (MK)
- 12:25–12:45 Object Security (GS)
- 12:45–13:00 SenML (AK)
- 13:00–13:05 CoRE Formats (Links/Groupcomm)
- 13:05–13:13 HTTP/2 (GM)
- 13:13–13:20 Flextime

ERICSSON

Object Security for COAP

draft-selander-ace-object-security-02

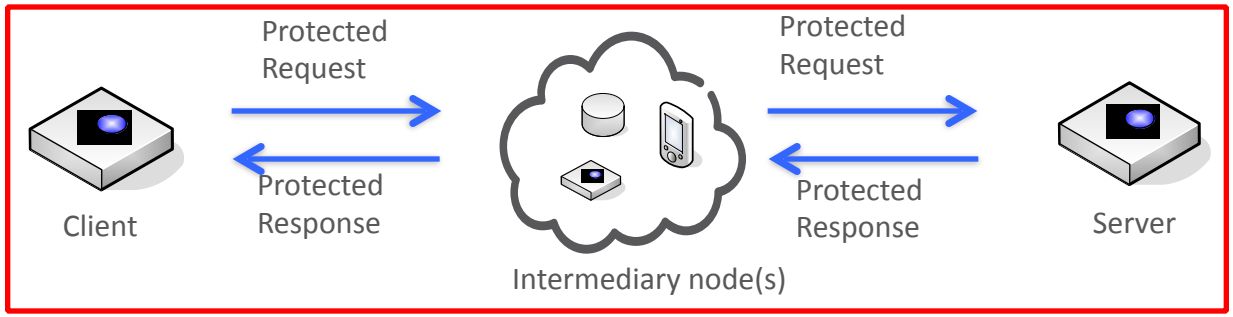
Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, SICS Swedish ICT

IETF 93 CORE WG, Prague, July 24, 2015

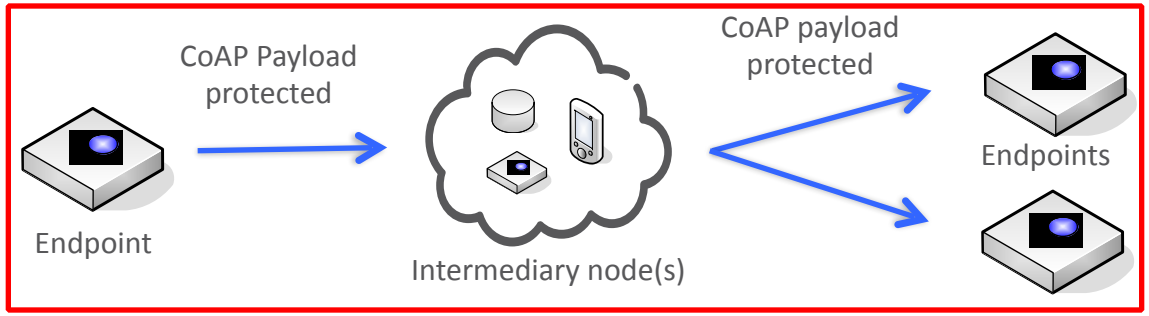
Object Secure CoAP (OSCOAP)

› 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

Updates in version -02

› Main content changes from version -01:
  – Appendix A: Included Block options
  – Appendix D: New. COSE profile of Secure Message. Proposed optimizations of COSE.
  – Appendix E: Updated message size estimates
  – Lots of rewritten text
  – Change of name on terms (Mode:PAYL, Context Identifier)

› Next steps
  – Update blockwise
  – Continue transition to COSE
  – Align CoAP Option handling for Encryption/Integrity protection only
  – Add assumed crypto support

Message overhead examples

› AES-CCM:

Scheme	Header	Tag	Total Overhead
COSE	44 B	16 B	60 bytes
mod-COSE	31 B	8 B	39 bytes
CSM	13 B	8 B	21 bytes

› ECDSA with 64 bytes signature:

Scheme	Header	Tag	Total Overhead
JWS	74 B	86 B	162 bytes
COSE	36 B	64 B	100 bytes
mod-COSE	30 B	64 B	94 bytes
CSM	13 B	64 B	77 bytes

ERICSSON

Thank you!

Comments/questions?

All times are in time-warped CEST

Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

Media Types for Sensor Markup Language (SenML)

draft-jennings-core-senml-01

IETF 93, Prague
July 24th, 2015

Ari Keränen
ari.keranen@ericsson.com

Background

- Presenting simple sensor measurements and device parameters with JSON/CBOR and XML/EXI
- Data model: single object with “base” attributes and array of entries
- New in -01: added CBOR serialization

SenML JSON Example

```
{"bn": "urn:dev:mac:0024beffe804ff1/",
 "bt": 1276020076,
 "bu": "A",
 "e":[
      { "n": "voltage", "u": "V", "v": 120.1 },
      { "n": "current", "t": -3, "v": 0.14e1 },
      { "n": "current", "t": -2, "v": 1.5 },
      { "n": "current", "t": -1, "v": 1.6 },
      { "n": "current", "t": 0, "v": 1.7 }]
}
```

Way forward

- Some proposed changes would change syntax and break backward compatibility
- Are we OK with that?

Location of base values

- No fixed order for members (name/value pairs) in JSON object
  - base values possibly in the end of serialized SenML
- When parsing, don't know full name/time/units before end of structure
  - Need full structure to memory or parse it twice
  - Block transfer: may not have the end or full structure easily accessible
- Currently RECOMMENDED to start with base
  - Can't rely on this behavior: not any good?

Location of base values

- Possible solution: array root

```
[{
   "bn": "urn:dev:mac:0024beffe804ff1/",
   "bt": 1276020076,
   "bu": "A"
 },
 [{ "n": "voltage", "u": "V", "v": 120.1 },
  { "n": "current", "t": -3, "v": 0.14e1 },
  { "n": "current", "t": -2, "v": 1.5 },
  { "n": "current", "t": -1, "v": 1.6 },
  { "n": "current", "t": 0, "v": 1.7 }]
]
```

Multiple bases

- Don’t want to repeat e.g., name or unit for each measurement in mixed scenario

```
{"bn": "urn:dev:mac:0024befffe804ff1/",
 "bt": 1276020076,
 "bu": "A",
 "e":[
      { "n": "voltage", "u": "V", "v": 120.1 },
      ...
      { "n": "current", "t": -3, "v": 0.14e1 },
      { "n": "current", "t": -2, "v": 1.5 },
      { "n": "current", "t": -1, "v": 1.6 },
      { "n": "current", "t": 0, "v": 1.7 }]
}
```

Multiple bases

```
[{
  "bn": "urn:dev:mac:0024befffe804ff1/voltage",
  "bt": 1276020076,
  "bu": "V"
 },
  [{"v": 120.1 },
    ...
  ],
 {"bn": "urn:dev:mac:0024befffe804ff1/current",
  "bu": "A" },
  [{"t": -3, "v": 0.14e1 },
    {"t": -2, "v": 1.5 },
    {"t": -1, "v": 1.6 },
    {"t": 0, "v": 1.7 }]
]
```

JSON Merge Patch format
RFC 7396

Alternatives for multiple bases

```
{"bn": "urn:dev:mac:0024befffe804ff1/",
 "bt": 1276020076,
 "nested":[{
  "bu": "V",
  "bn": "voltage",
  "e":[
    { "t": -1, "v": 120.5 },
    { "t": 0,  "v": 120.1 }]
  },{
  "bu": "A",
  "bn": "current",
     "e":[
       { "t": -4, "v": 1.30 },
```

- Keeps object root element
- Adds complexity

```
{"bn": "urn:dev:mac:0024befffe804ff1/",
   "bt": 1276020076,
   "bu": "A",
   "e":[
     {"n": "voltage", "t": [-5,-3,-1], "u": "V", "v": [120.1, 120.4, 120.5] },
     {"n": "current", "t": [-4, -3, -2, -1], "v": [1.30, 0.14e1, 1.5, 1.6] },
  }
```

All times are in time-warped CEST

Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

Representing CoRE Formats in JSON and CBOR

-- https://tools.ietf.org/html/draft-ietf-core-links-json-03

Kepeng Li
Akbar Rahman
Carsten Bormann

Recap

- Changes from -02 to -03
  - Merged with draft-li-core-cbor-equivalents-00

Main Scenarios

- CoRE Link Format (RFC 6690) to JSON (RFC7390)
- CoRE Link Format (RFC 6690) to CBOR (RFC7049)
- CBOR Groupcomm management JSON (RFC 7390) to CBOR (RFC7049)

Example

2.4.1. Link Format to CBOR Example

This examples shows conversion from link format to CBOR format.

The link-format document in Figure 3 becomes (in CBOR diagnostic format):

```
[{1: "/sensors", 12: "40", 7: "Sensor Index"},
 {1: "/sensors/temp", 9: "temperature-c", 10: "sensor"},
 {1: "/sensors/light", 9: "light-lux", 10: "sensor"},
 {1: "http://www.example.com/sensors/t123", 3: "/sensors/temp",
  2: "describedby"},
 {1: "/t", 3: "/sensors/temp", 2: "alternate"}]
```

or, in hexadecimal (203 bytes):

```
85                                  # array(number of data items:5)
   a3                               # map(# data item pairs:3)
      01                            # unsigned integer(value:1,"href")
      68                            # text string(8 bytes)
         2f73656e736f7273           # "/sensors"
      0c                            # unsigned integer(value:12,"ct")
      62                            # text(2)
         3430                       # "40"
      07                            # unsigned integer(value:7,"title")
      6c                            # text string(12 bytes)
         53656e736f7220496e646578   # "Sensor Index"
```

Next Step

- Are there are other types of CoRE Formats (to JSON and CBOR conversion) that we should cover?

All times are in time-warped CEST

Friday

- 11:50–11:55 Intro
- 11:55–12:10 HTTP-CoAP Mapping (TF)
- 12:10–12:25 CoRE Interfaces (MK)
- 12:25–12:45 Object Security (GS)
- 12:45–13:00 SenML (AK)
- 13:00–13:05 CoRE Formats (Links/Groupcomm)
- 13:05–13:13 HTTP/2 (GM)
- 13:13–13:20 Flextime

HTTP/2 for IoT

Gabriel Montenegro, Microsoft

IETF 93, July 2015

Communication Patterns

	Constrained	*Internet*
Node-to-node	***X***	
Node to gateway	***X***	
Gateway to cloud		***X***
Node to cloud		***X***

NOTE: Internet traffic is assumed to be carried over TLS

Application Transport Alternatives and their strengths: CoAP (1/2)

*21% of devs in 2015 survey**

- Beginning, 6lowpan base publications (2007-2012)
- Need for application layer solution
- Requirements not met by HTTP/1.1
- CoAP is being defined (base publications: 2014-ongoing)
- Important to revisit requirements now with HTTP/2

** IoT Developer Survey 2015: http://www.slideshare.net/IanSkerrett/iot-developer-survey-2015*

Application Transport Alternatives and their strengths: CoAP (2/2)

- popular in constrained scenario (node to node, node to gateway)
- UDP is limiting for internet scenario and firewall traversal
- Support for group communication based on experimental multicast mechanism.
- Not generally available in cloud services
- Several related drafts to complete the picture:
  - BLOCK draft for TCP
  - OBSERVE draft for HTTP/2 PUSH
  - congestion control in core coap and in separate drafts
  - HTTP mapping draft, etc

Application Transport Alternatives and their strengths

- AMQP and XMPP: 11% of devs in 2015 survey
- MQTT: 53% of devs in 2015 survey
  - Publish/subscribe, created by IBM, now in OASIS
  - popular in internet scenario (node to cloud, gateway to cloud)
  - Nice and small
  - But SSL is nowadays mandatory on the internet, so some advantage is lost anyways
  - Uses port 8883 for MQTT-over-SSL (1883 without SSL)
  - Firewall issues
- HTTP/1.1: 63% of developers in 2015 survey (!!!)
  - VERY popular still despite its terrible characteristics
  - Widespread know-how
  - Many implementations, tools, support, etc
  - The power of mainstream

HTTP/2: the best *general* alternative

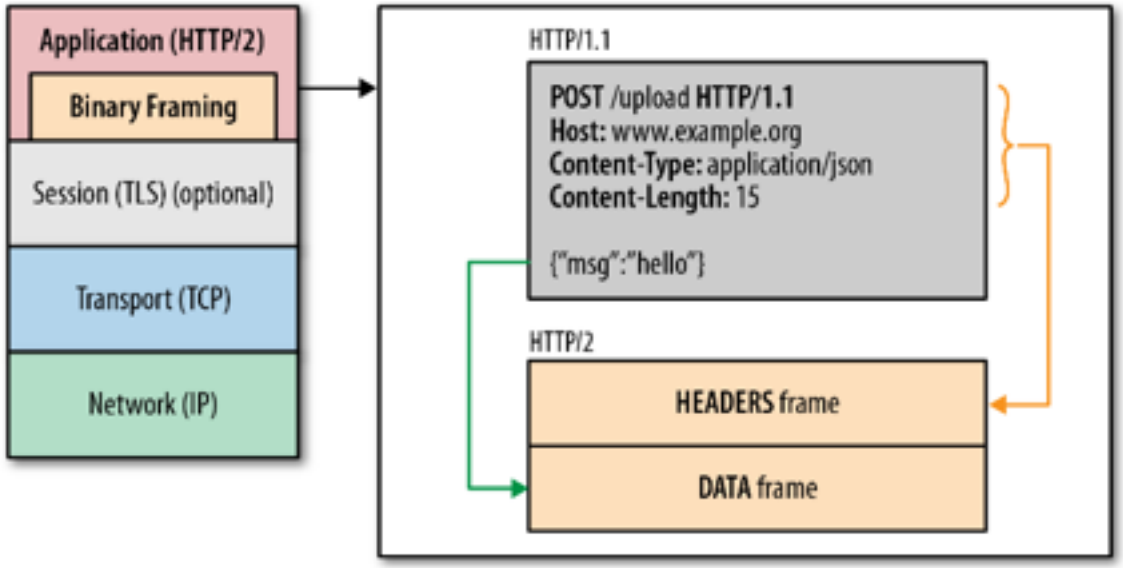
- Fine for constrained environments (some experiments ongoing already) given small code size, binary encoding for transport (potentially usable directly for even more compactness), resource-friendly header compression, reuse of a single TCP connection, PUSH for subscriptions, etc
- By far, the most reliable alternative for internet scenario (firewall issues)
- Only alternative suitable for both *constrained* and *internet* scenarios.
  - Given the limits of code space, constrained devices benefit from a single stack for multiple scenarios.
- The power of mainstream (yes, given current deployment/usage numbers)
  - Analogous to benefits of IP in https://tools.ietf.org/html/rfc4919#section-3
- *Note: UDP possibility (currently available in a proprietary fashion via QUIC)*
  - *DTLS 1.3 and DICE*

HTTP/2 Status and info

- HTTP/2 page on github maintained by IETF HTTPbis WG:
  http://http2.github.io/
- HTTP/2 is defined by:
  - Hypertext Transfer Protocol version 2 - RFC7540
  - HPACK - Header Compression for HTTP/2 - RFC7541
- Supported in major browsers, clients, servers, proxies, etc
  - https://github.com/http2/http2-spec/wiki/Implementations
- HTTP/2 and IoT
  - On a CC3200 Launchpad board
    http://robbysimpson.com/2015/02/16/first-iot-device-with-http2/
  - Relevant blogs:
    http://robbysimpson.com/2015/01/26/http2-and-the-internet-of-things/
    http://www.limmat.co/2015/02/18/http-2-the-new-iot-protocol/
  - Good intro in *High Performance Computing* by Ilya Grigorik:
    http://chimera.labs.oreilly.com/books/1230000000545/ch12.html

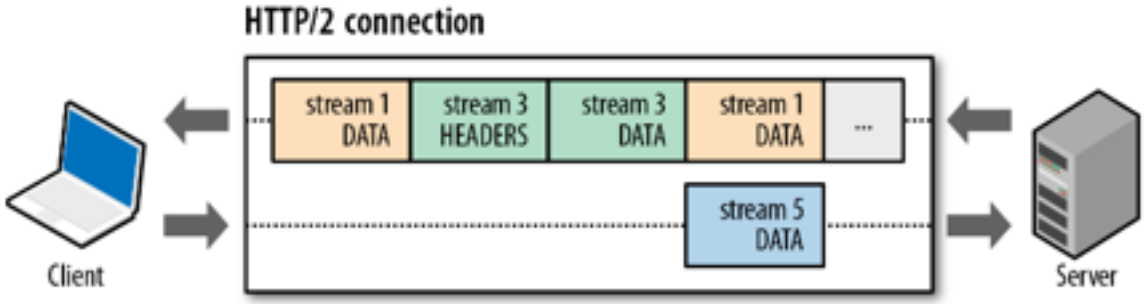
Extra Slides

HTTP/2 in one slide



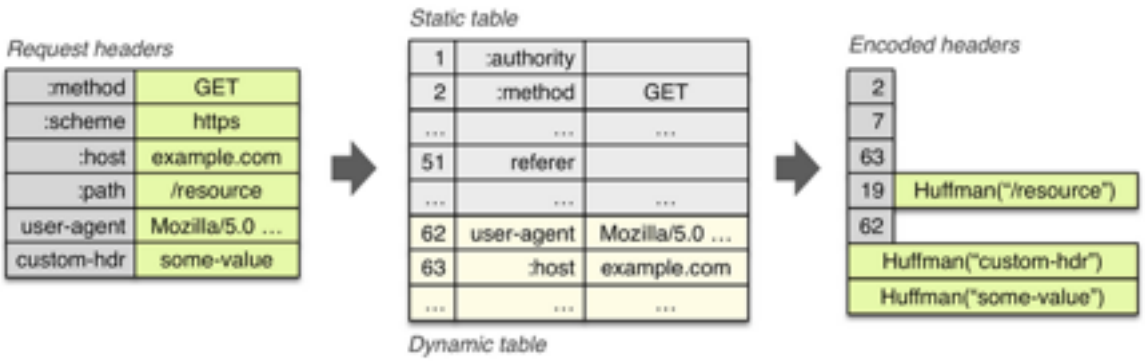
Source: *High Performance Computing* by Ilya Grigorik

HTTP/2 multiplexing



Source: *High Performance Computing* by Ilya Grigorik

HPACK for header compression



Source: *High Performance Computing* by Ilya Grigorik

Common 9-byte frame header

Bit	+0..7	+8..15	+16..23	+24..31
0	Length			Type
32	Flags			
40	R	Stream Identifier		
...	*Frame Payload*			

Source: *High Performance Computing* by Ilya Grigorik

IoT Profiles for HTTP/2

- General constrained profile (usable on both constrained and internet scenarios)
  - Along the lines of constrained profile in https://tools.ietf.org/html/draft-montenegro-httpbis-http2-server-profiles-00
  - SETTINGS_HEADER_TABLE_SIZE: 512 (versus 4096)
  - SETTINGS_ENABLE_PUSH: 1 (this is the default)
  - SETTINGS_MAX_CONCURRENT_STREAMS: value: 1 or 2 or 3? (versus infinite)
  - SETTINGS_INITIAL_WINDOW_SIZE: value: 2K (versus 64K)
  - SETTINGS_MAX_FRAME_SIZE : 1K (versus 16K)
  - SETTINGS_MAX_HEADER_LIST_SIZE: 1K (versus infinite)
- *Constrained* communication profile (for node to node, node to gateway)
  - In 6lowpan environments, e.g., Thread
  - ND option for HTTP/2 and optionally to allow reuse of lower-layer (e.g., 802.15.4) security ciphers and services (HTTP/2 “in-the-clear” if allowed within that 6lowpan context
  - In-the-clear but no Upgrade dance: “prior” knowledge (obtained from HTTP/2 ND option)
- *Internet* communication profile (for gateway to cloud, node to cloud)
  - E.g., Cloud IoT environments
  - TLS always on per usual HTTP/2 ciphers

Negotiating the HTTP/2 usage profile

- Constrained usage profile:
  - ND option similar to 6CO and ABRO (potentially in DHCPv6 option as well)
  - Signal:
    - Use of HTTP/2
    - Optional reuse of lower-layer security services (e.g., for 802.15.4)
- Internet usage profile:
  - ALPN (no longer used for token binding, so less explosion, but still some concern)
  - Prior knowledge based on the application
  - Initial setup based on first message exchange
    - Simpler than general HTTP/2 case: no in-the-clear Upgrade path means the client is always in control of first message

All times are in time-warped CEST

Friday

- **11:50–11:55 Intro**
- **11:55–12:10 HTTP-CoAP Mapping (TF)**
- **12:10–12:25 CoRE Interfaces (MK)**
- **12:25–12:45 Object Security (GS)**
- **12:45–13:00 SenML (AK)**
- **13:00–13:05 CoRE Formats (Links/Groupcomm)**
- **13:05–13:13 HTTP/2 (GM)**
- **13:13–13:20 Flextime**

Flextime