Constrained RESTful Environments WG (core)

Chairs:
Jaime Jiménez <jaime.jimenez@ericsson.com>
Carsten Bormann <cabo@tzi.org>
Mailing List:
core@ietf.org
Jabber:
core@jabber.ietf.org

- **We assume people have read the drafts**
- **Meetings serve to advance difficult issues by making good use of face-to-face communications**
- **Note Well: Be aware of the IPR principles, according to RFC 8179 and its updates**

üBlue sheets
üScribe(s)

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:

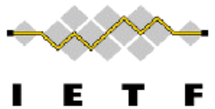
- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **Any Birds 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 8179.

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 8179 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.



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

Agenda Bashing

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

CoAP over TCP: Status

- WGLC long completed
- URI-scheme brouhaha completed
- -10 should clear all IESG DISCUSSES
- In RFC editor queue soon
  (AD approval needed)
- Dependent on hybi-ws-wk

CoAP-over-TCP @ Hackathon @ IETF100

- 2½ implementations: libcoap, augustcellars, coap.me
- Managed to GET /.well-known/core
- Issues raised
  - Fix example and a naming inconsistency
  - Do not send requests after sending release
  - Text could be clearer on not handling custody
- Could do this in a -11 together with any further IESG comments

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

CoAP Simple Congestion Control/Advanced (CoCoA)

draft-ietf-core-cocoa-02

Carsten Bormann – Universität Bremen TZI
August Betzler – Fundació i2Cat
Carles Gomez, Ilker Demirkol – Univ. Politècnica de Catalunya

Status

- Last revision is -02
- Heads up on -01 before WGLC sent to CoRE, TCPM, ICCRG
  - Two reviews (thanks!)
    - Michael Scharf
    - Ingemar Johansson
- -02 intended:
  - To address the comments received
  - For WGLC

Technical update

- Impact of strong and weak estimators is now tunable

- Old
  - RTO := 0.25 * E_weak_ + 0.75 * RTO (1)
  - RTO := 0.5 * E_strong_ + 0.5 * RTO (2)

- New
  - RTO := w_weak * E_weak_ + (1 - w_weak) * RTO (1)
  - RTO := w_strong * E_strong_ + (1 - w_strong) * RTO (2)

Editorial updates (I)

- Abstract
  - The core of the specification is an RTO algorithm
- Section 1
  - Was almost empty, now a proper introduction
- Section 3: Area of Applicability
  - Algorithm defined, intended for a wide range of network conditions
- Section 4: RTO Estimation
  - Wide spectrum of RTTs
  - RTT variability discussion: added details on TCP delayed ACKs
    - Vs application processing times in CoAP RTT

Editorial updates (II)

- Section 4.2.2. Measured RTO estimate. Discussion
  - Weak estimator allows to update the RTO estimator when RTTs are mostly weak
    - Lossy links or congestion
    - In the latter, spurious timeouts are avoided, rate of retries reduced, congestion decrease

Editorial updates (III)

- Added references to RFC 7252
  - For readers not so familiar with CoAP
    - Specific sections
- Section 7. Security considerations
  - Attacker preventing packet delivery, RTO increase
    - Not specific for CoCoA (or CoAP)
  - Mitigated by network access control
  - If radio jamming, recovery in reasonable time
    - Weak estimator increases the chances of obtaining RTT samples

Editorial updates (IV)

- Appendices
  - Old appendix “Aggregate Congestion Control”
    - Removed from the document
  - Appendix B: Pseudocode
    - Updating the RTO estimator
    - RTO aging
    - Variable Backoff Factor
  - Appendix C: Examples
    - Weak RTTs
    - VBF and aging
  - Appendix D: Analysis
    - Strong vs weak estimator

Thanks!

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

WGLC — keep tcpm etc. in the loop
AD: Processing after WGLC

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

Resource Directory

draft-ietf-core-resource-directory-12

draft-ietf-core-rd-dns-sd-01

Zach Shelby, Michael Koster, Carsten Bormann,
Peter van der Stok, *Christian Amsüss*

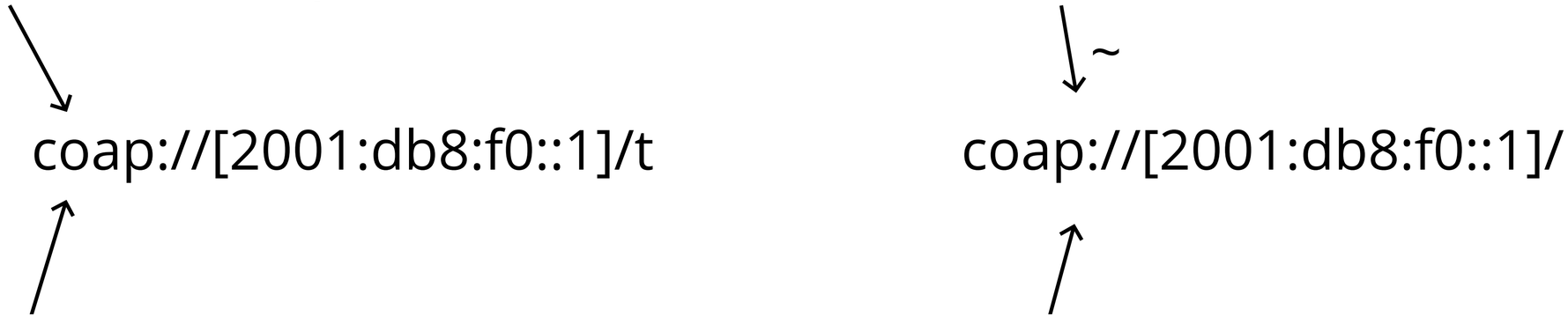
What does an RD do: Principles

- RD stores and caches links provided by endpoints
- Clients look up links with minimal differences compared to .well-known/core based discovery
- RD facilitates discovery operations where otherwise impossible or inefficient

What is in an RD: Links

From coap://[2001:db8:f0::1]/.well-known/core:

```
</t>;rt=temp;ct=0;rel="hosts";anchor=""
```



Looked up in RD at coap://directory/rd-lookup/res?rt=temp:

```
</t>;rt=temp;ct=0;rel="hosts";
  anchor="coap://[2001:db8:f0::1]"
```

What else is in an RD

Groups

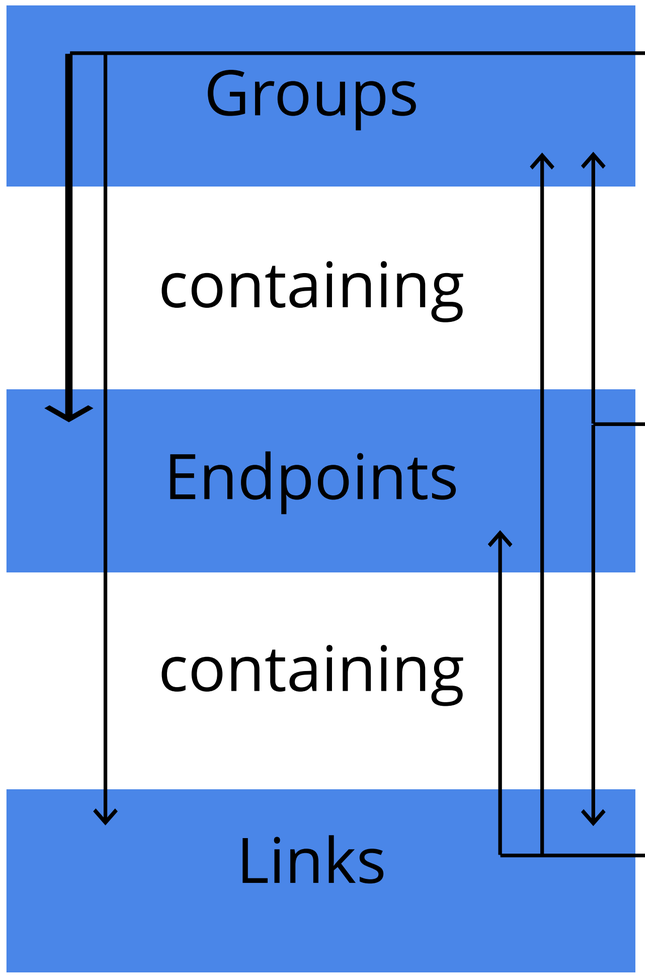
containing

Endpoints

containing

Links

What can be queried from it



From /lookup/gp?ep=node1

```
</reg/gp123>;gp="room-5-23";
con="coap://[ff35:..:1]";
d="rooms"
```

From /lookup/ep?gp=rooms

```
</reg/ep456>;ep="node-42";
con="coap://[2001:db8:..:42]'
et="wallmounted-remote"
```

From /lookup/res?et=wallmounted-...

```
</t>;rt="temp";if="core.s";
anchor="coap://[2001:..:42]";
```

More RD changes

- added Content Model section, including ER diagram
- removed domain lookup interface; domains are now plain attributes of groups and endpoints
- updated chapter "Finding a Resource Directory"; now distinguishes configuration-provided, network-provided and heuristic sources
- improved text on: atomicity, idempotency, lookup with multiple parameters, endpoint removal, simple registration
- updated LWM2M description
- clarified where relative references are resolved, and how context and anchor interact
- new appendix on the interaction with RFCs 6690, 5988 and 3986
- lookup interface: group and endpoint lookup return group and registration resources as link targets
- lookup interface: search parameters work the same across all entities
- removed all methods that modify links in an existing registration (POST with payload, PATCH and iPATCH)
- removed plurality definition (was only needed for link modification)
- enhanced IANA registry text
- state that lookup resources can be observable

Next steps

Pending changes for -13

- Register a dedicated "All Resource Directories" multicast address
- Precise semantics of query parameters in lookup ("up" and "down" directions in "What can be queried from")
- Editorial fixes

Open questions for -13

- Think through group members from foreign RDs
- Interface versioning

Please visit the issue tracker at
https://github.com/core-wg/resource-directory/issues

Reviews

- Thank you to Jim and Hannes for their comprehensive reviews of -11
- Need more like that
- Need more input from implementors

Porting links into DNS-SD

- RD provides all data needed for the export
- Origin servers provide metadata (exp, ins)
- Works from .well-known/core as well

Porting links into DNS-SD

From /lookup/res?exp&d=floor1.example.com

```
</t>;rt="sdo.temp";exp;ins="Room 85 temperature";
    anchor="coap://env85-fl1.nodes.example.com/"
```

To DNS:

```
_sdo._udp.floor1.example.com IN PTR
  "Room 85 temperature._sdo._udp.floor1.example.com"

temp._sub._sdo.floor1.example.com IN PTR [same]

"Room 85 temperature._sdo._udp.floor1.example.com"
  IN SRV 0 0 5683 env85-fl1.nodes.example.com.
"Room 85 temperature._sdo._udp.floor1.example.com"
  IN TXT txtver=1;path=/t
```

Porting links into DNS-SD

From /lookup/res?exp&d=floor1.example.com

```
</t>;rt="sdo.temp";exp;ins="Room 85 temperature";
     anchor="coap://env85-fl1.nodes.example.com/"
```

To DNS:

```
_sdo._udp.floor1.example.com IN PTR
   "Room 85 temperature._sdo._udp.floor1.example.com"

temp._sub._sdo.floor1.example.com IN PTR [same]

"Room 85 temperature._sdo._udp.floor1.example.com"
  IN SRV 0 0 5683 env85-fl1.nodes.example.com.
"Room 85 temperature._sdo._udp.floor1.example.com"
  IN TXT txtver=1;path=/t
```

Open questions for DNS-SD

- Handling unregistered / unknown resource types and services
- Interface versioning

Please visit the issue tracker at
https://github.com/core-wg/rd-dns-sd/issues

Questions

Thanks

Backup slides

Getting host names for DNS

(for PTR targets)

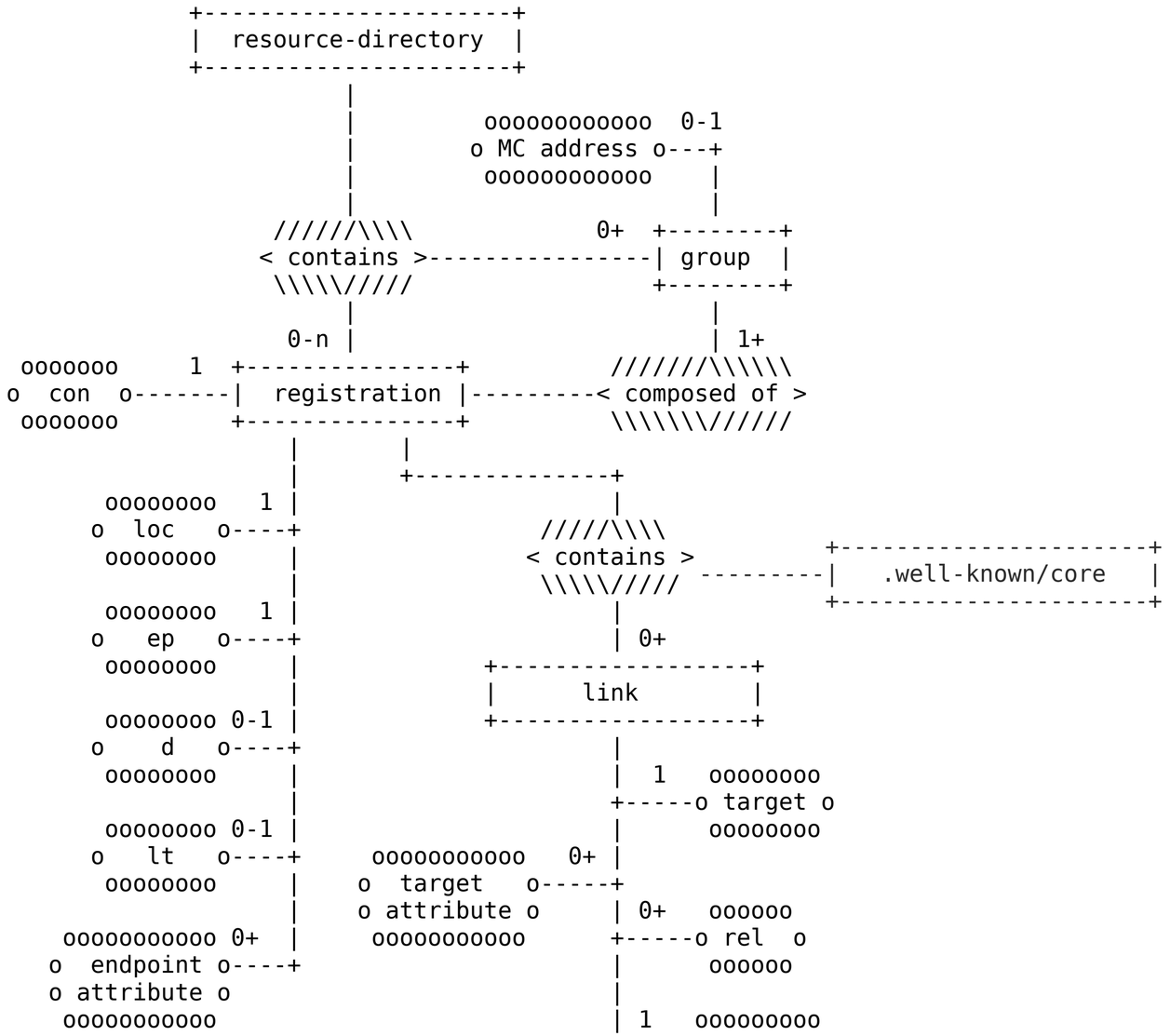
From /lookup/ep?d=floor1.example.com

```
</reg/1234>;ep="env85";
        d="floor1.example.com";
        con="coap://[2001:db8:1::85]"
```

To DNS:

```
env85.floor1.example.com IN AAAA
2001:db8:1::85
```

Information model



Discovery and registration

```
Req: GET coap://[ff02::fd]/.well-known/
     core?rt=core.rd
Res from 2001:db8::d: 2.05 Content
</rd>;rt="core.rd";ct=40

Req: POST coap://[2001:db8::d]/rd?
     ep=node1&d=example.com&et=wallmounted
</t>;rt="temp"
Res: 2.04 Created
Location: </res/4521>
```

Endpoint lookup

```
Req: GET /rd-lookup/ep?d=example.com
Res: 2.05 Content
</reg/4521>;ep="node1";d="example.com";
    et="wallmounted";lt=84600;
    context="coap://[2001:db8::1]"

Req: GET /rd-lookup/ep?gp=lights1
Res: 2.05 Content
</reg/123>;ep="led1";d="example.org";
    lt=84600;context="coap://led1.e.o",
</reg/124>;ep="led2";d="example.org";…
```

Resource lookup

```
Req: GET /rd-lookup/res?rt=temp
Res: 2.05 Content
</t>;rt="temp";anchor="coap://[2001:db8::1]"

Req: GET /rd-lookup/res?ep=led1
Res: 2.05 Content
</b>;rt="brightness";if="core.a";
    anchor="coap://led1.example.org",
</wb>;rt="whitebalance";if="core.rp";
    anchor="coap://led1.example.org",
<http://ex.com/doc/wb>;rel="describedby";
    anchor="coap://led1.example.org/wb"
```

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

CoMI – update

draft-ietf-core-comi-01

Andy Bierman

Michel Veillette

Peter van der Stok

Alexander Pelov <a@ackl.io>

Draft status

Actions from last time:
- Review drafts
- Perform interop
- Deploy SID registry

Interop

Draft	Version	Status	
ietf-core-yang-cbor	5 ~~4~~	Stable since IETF 97	Ready for WGLC?
ietf-core-sid	1	Stable since IETF 98	Ready for WGLC?
ietf-core-comi	2 ~~1~~	Stable since IETF 99	More review needed
veillette-core-yang-library	0	Stable since IETF 98	More review needed In scope for Core? Normative reference in CoMI

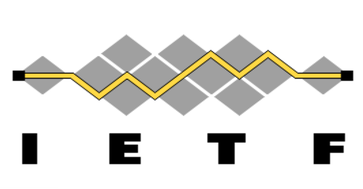
Implementations
CoMI with YANG-CBOR

- Existing implementations
  - GoLang: server + client
  - C: server + client
  - 2 more partial proprietary implementations

- Goal interop + hackathon @ IETF100
  - Define interop scenarios
    - Start with ietf-system
  - Perform full cross-functionality interop

- Many key people not present, scaled back on expectations

Virtual interop during hackathon weekend



	GET	PUT	POST CREATE	DELETE	FETCH	IPATCH	POST RPC	IPv4	IPv6
Trilliant	✗	✗	✗	✗	✓	✓	✓	✗	✓
Acklio	✓	✓	✓	✓	✓	✓	✓	✓	✓

```
module: ietf-system
  +--rw system
  |  +--rw contact?         string
  |  +--rw hostname?          inet:domain-name
  |  +--rw location?        String
...
  +--ro system-state
    +--ro platform
    |  +--ro os-name?      string
    |  +--ro os-release?   string
    |  +--ro os-version?   string
    |  +--ro machine?      string
    +--ro clock
      +--ro current-datetime?   yang:date-and-time
      +--ro boot-datetime?      yang:date-and-time
```

Virtual interop during hackathon weekend

	GET	PUT	POST CREATE	DELETE	FETCH	IPATCH	POST RPC	IPv4	IPv6
Trilliant	✗	✗	✗	✗	✓	✓	✓	✗	✓
Acklio	✓	✓	✓	✓	✓	✓	✓	✓	✓

```
module: ietf-system
  +--rw system
  |  +--rw contact?        string
  |  +--rw hostname?       inet:domain-name
  |  +--rw location?       String
...
  +--ro system-state
    +--ro platform
    |  +--ro os-name?      string
    |  +--ro os-release?   string
    |  +--ro os-version?   string
    |  +--ro machine?      string
    +--ro clock
      +--ro current-datetime?   yang:date-and-time
      +--ro boot-datetime?      yang:date-and-time
```

```
{
  "type": "node",
  "label": "/system-state/clock",
  "sid": 1717
},
{
  "type": "node",
  "label": "/system-state/clock/boot-datetime",
  "sid": 1718
},
{
  "type": "node",
  "label": "/system-state/clock/current-datetime",
  "sid": 1719
},
{
  "type": "node",
  "label": "/system-state/platform",
  "sid": 1720
},
```

Virtual interop during hackathon weekend

	GET	PUT	POST CREATE	DELETE	FETCH	IPATCH	POST RPC	IPv4	IPv6
Trilliant	✗	✗	✗	✗	✓	✓	✓	✗	✓
Acklio	✓	✓	✓	✓	✓	✓	✓	✓	✓

```
module: ietf-system
  +--rw system
  |  +--rw contact?        string
  |  +--rw hostname?       inet:domain-name
  |  +--rw location?       String
...
  +--ro system-state
    +--ro platform
    |  +--ro os-name?      string
    |  +--ro os-release?   string
    |  +--ro os-version?   string
    |  +--ro machine?      string
    +--ro clock
      +--ro current-datetime?   yang:date-and-time
      +--ro boot-datetime?      yang:date-and-time
```

```
{
  "type": "node",
  "label": "/system-state/clock",
  "sid": 1717
},
{
  "type": "node",
  "label": "/system-state/clock/boot-datetime",
  "sid": 1718
},
{
  "type": "node",
  "label": "/system-state/clock/current-datetime",
  "sid": 1719
},
{
  "type": "node",
  "label": "/system-state/platform",
  "sid": 1720
},
```

- ✓ FETCH single value
- ✓ FETCH container
- ✓ FETCH two values
- ≈ FETCH three values, delta=0

- ✓ YANG-CBOR string
- ✓ YANG-CBOR derived type
  YANG-CBOR container

- ✓ SID delta encoding
- ✓ FETCH delta URI reference

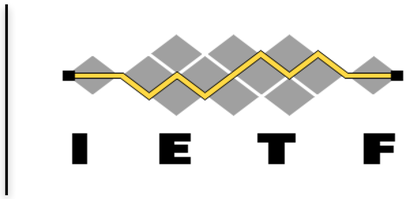
Lessons learned

- ietf-system is not the easiest module to try full functionality
  - Will define a suite of baseline modules for testing basic + extended functions
  - (Maybe NETMOD already have such?)

- Debugging can be somewhat tedious with delta-SIDs and complex queries.
  - While we are still missing the tools and using bare eyes to look at traces
  - Proposal:
    - Use CBOR tag 39 (identifier) to indicate that the value is a SID (and not a delta-SID)
    - If server and/or client support debugging – run with debug option and use only SIDs
      - Minor change to delta-SID dereferencer, no other changes to code / semantics
  - Key point: efficient on the wire, allows easy debug when necessary

- We can have a minimal set of operations that covers the entire set of functionalities of CoMI
  - CoMI-minimal + CoMI-extended ?
    - (especially if we can have CoMI-extended expressed entirely through CoMI-minimal, e.g. can work as a Proxy)
  - CoMI draft is still a little heavy on the description side because of the many handled cases – try to split in different sections and/or documents (after validation)

Hackathon @ IETF 100



- Started open-source implementation in Python
  - With a specific module in mind – running SCHC context provisioning over CoMI
  - Partial success
    - Module bindings and basic functionality OK
    - Bad choice of YANG library (for 2 day work)
  - After discussion with NETMOD guys
    - Rebase development with YDK

- Next steps
  - Open-source YDK-based CoMI implementation by IETF 101
  - Official Hackathon @ IETF 101

Next steps

- Bi-weekly meetings on CoMI Interop
- Full interop by IETF 101
  - FETCH+PATCH (CoMI-minimal?)
  - Over an extended set of operations and modules (TBD)
- Hackathon @ IETF 101 and open-source implementation

- YANG-CBOR document
  - Introduce use of CBOR option 39 ?

- CoMI document
  - Improve readability, simplify

YANG Schema Item iDentifier (SID)

draft-ietf-core-sid-01

Andy Bierman

Michel Veillette

Peter van der Stok

Alexander Pelov <a@ackl.io>

Status and next steps

Four main topics

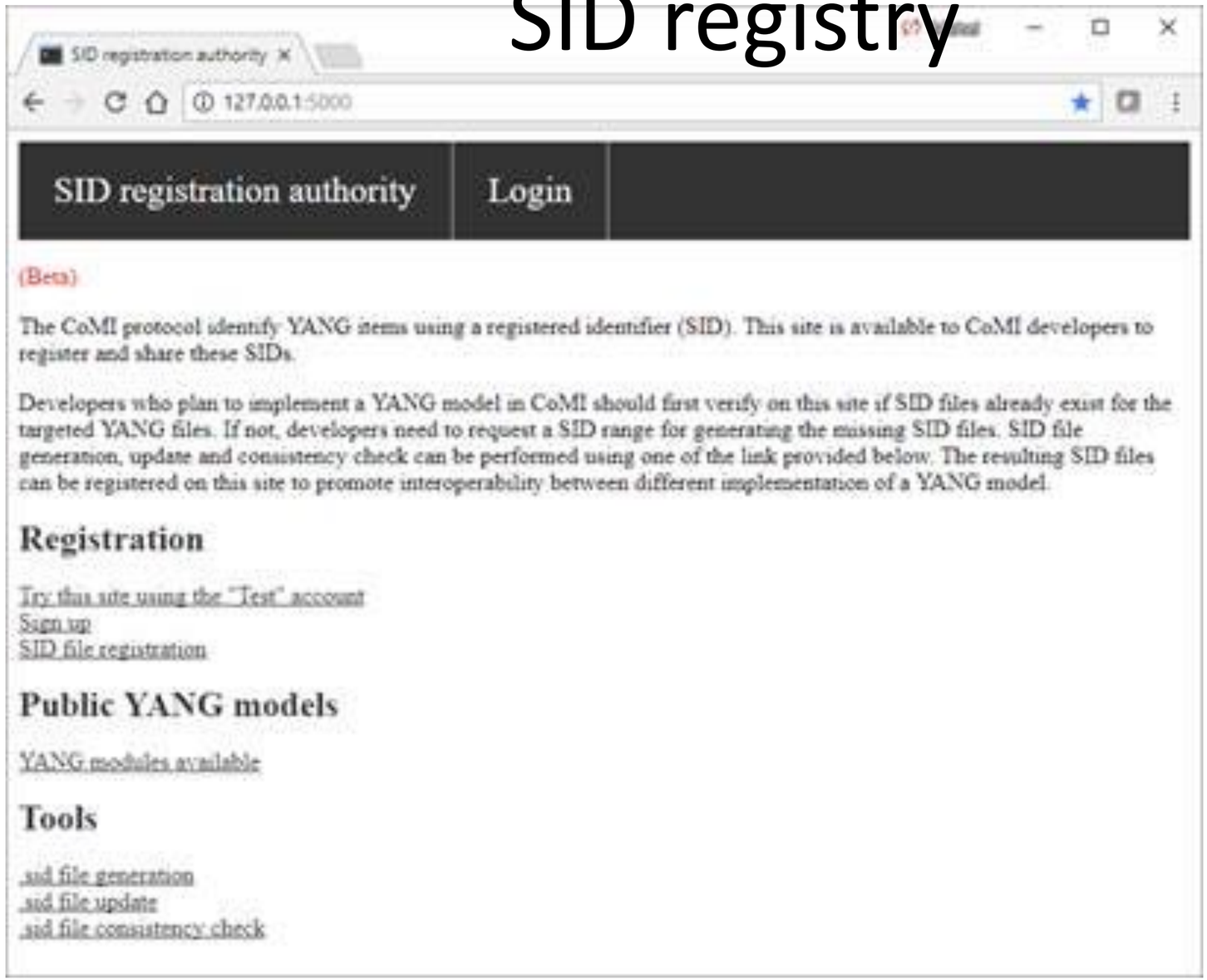
- SID definition (semantic)
  - 64 bit identifier assigned to all YANG identifiers
- SID file format (.sid)
  - YANG Schema -> JSON format
- SID file lifecycle
  - Range registration, .sid generation, .sid update
- Allocation policies
  - Two-tier allocation system
    - MegaRange (1M SIDs) and Range (~1000 SIDs flexible size)
  - Review allocation policy with IANA

Status and next steps

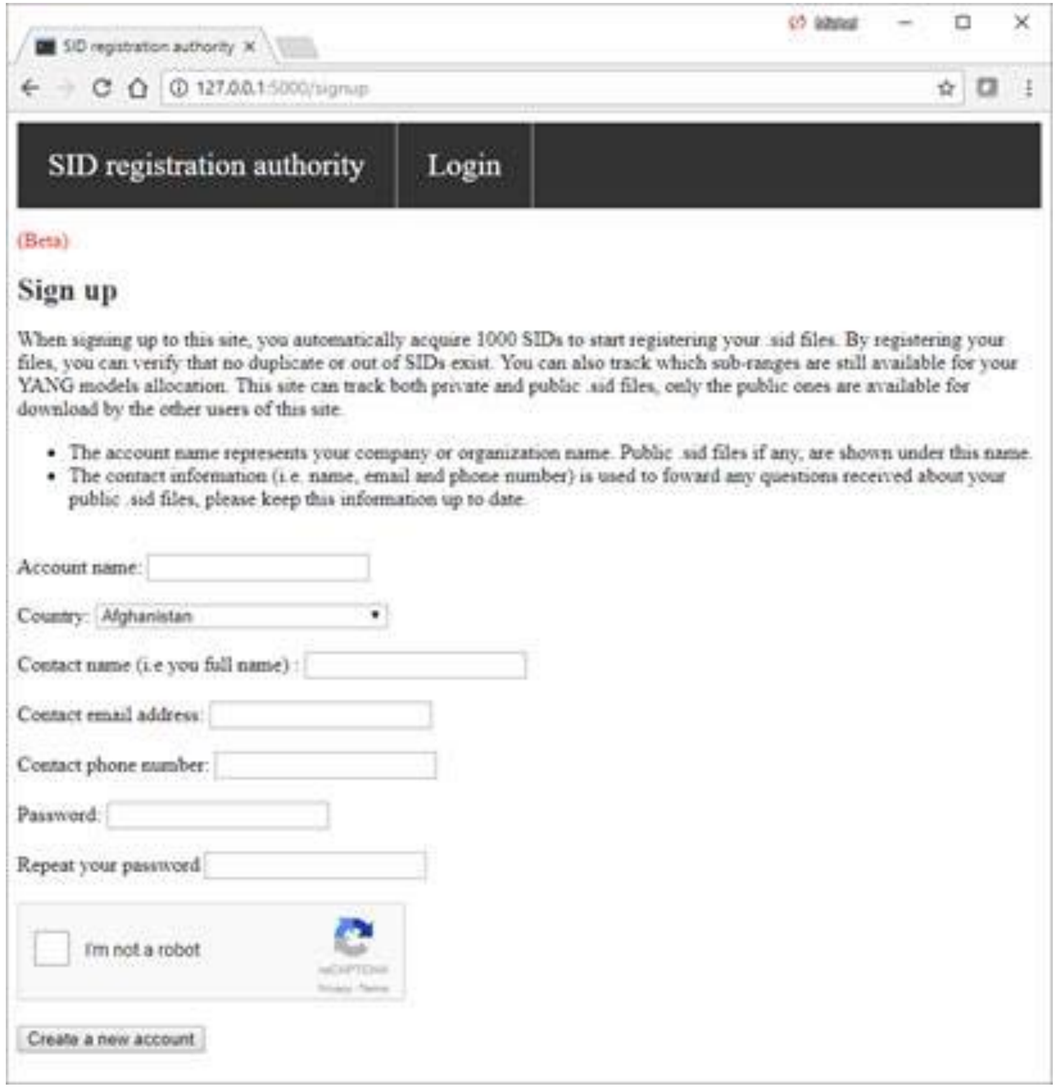
Four main topics

- SID definition (semantic)
  - 64 bit identifier assigned to all YANG identifiers
- SID file format (.sid)
  - YANG Schema -> JSON format
- SID file lifecycle
  - Range registration, .sid generation, .sid update
- Allocation policies
  - Two-tier allocation system
    - MegaRange (1M SIDs) and Range (~1000 SIDs flexible size)
  - Review allocation policy with IANA

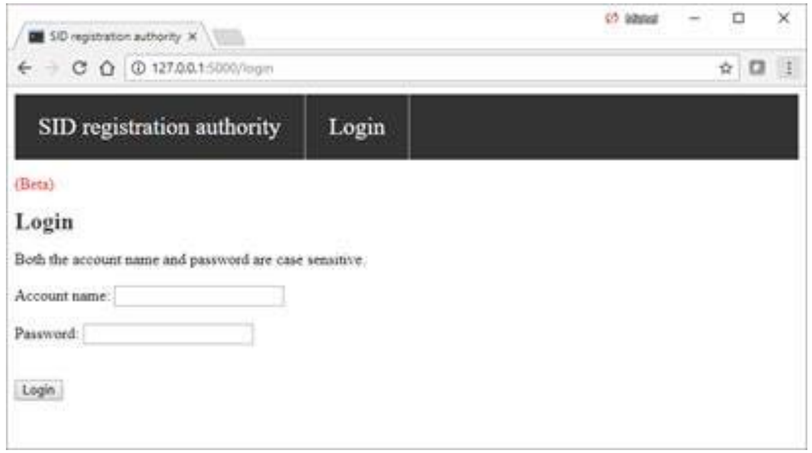
SID registry



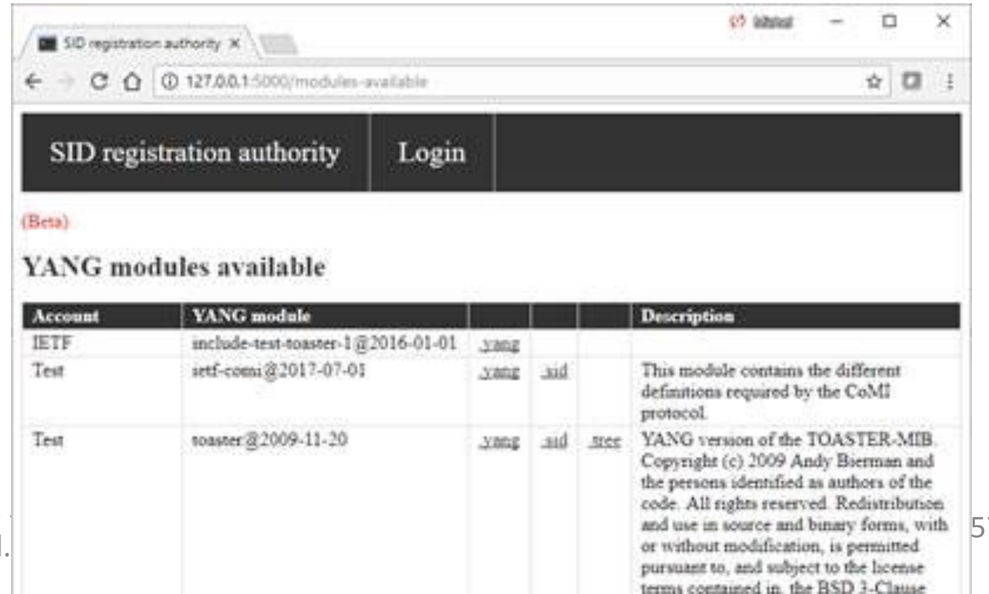
Sign-up



Login

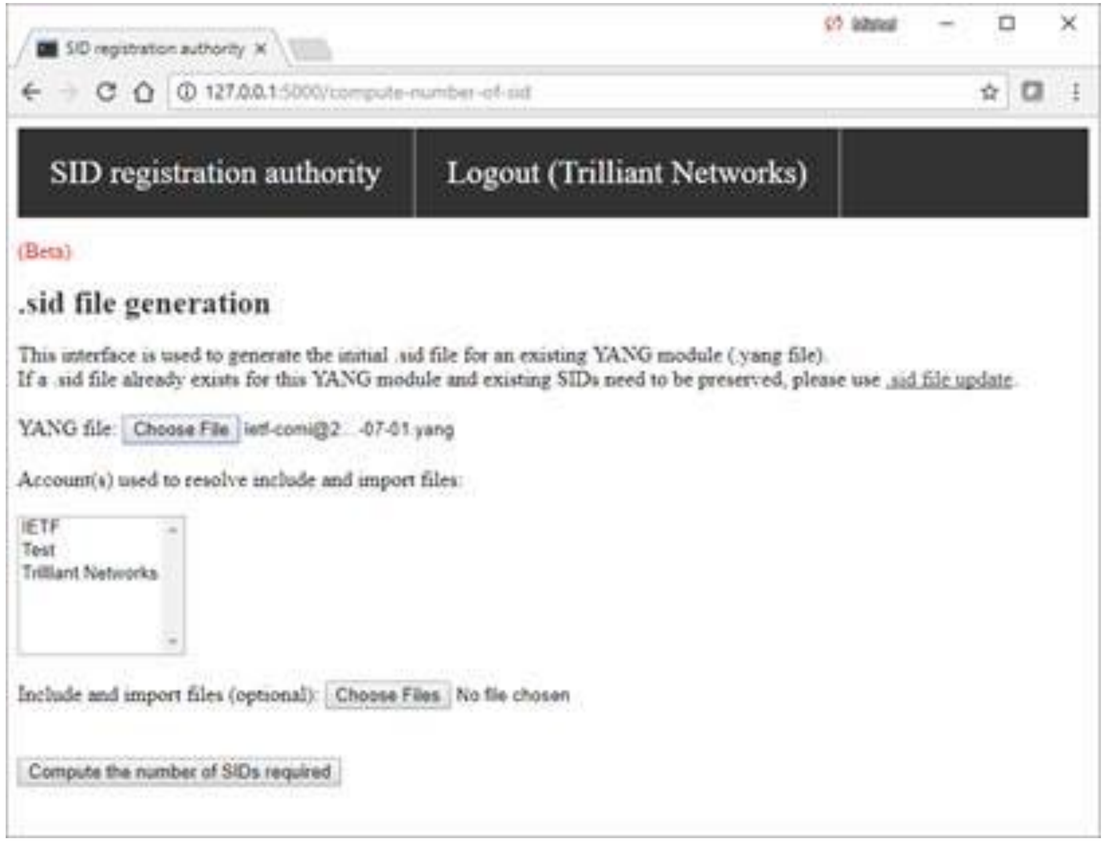


Available modules



SID Ranges

SID generation tool



+ SID file update

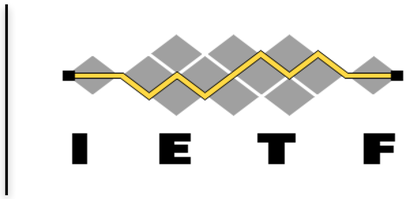
+ SID file consistency check

Next steps

- The SID registry* is online at:
  - http://sidreg.acklio.com:5000
  - Not (yet) a fully validated registry (as per IANA)
  - Start operating in 1M-2M range
    - Get feedback, clear out bugs
  - Behavior may (will) change in time as we get more feedback

    (Until now we have done the same with Github)

- WGLC on draft-core-sid ?
  - Cross-validation with NETMOD
  - It takes time to create an IANA registry (after it is published by the IESG)
    - And we need the Mega-Range Registry so that we can claim that this* is a valid registry



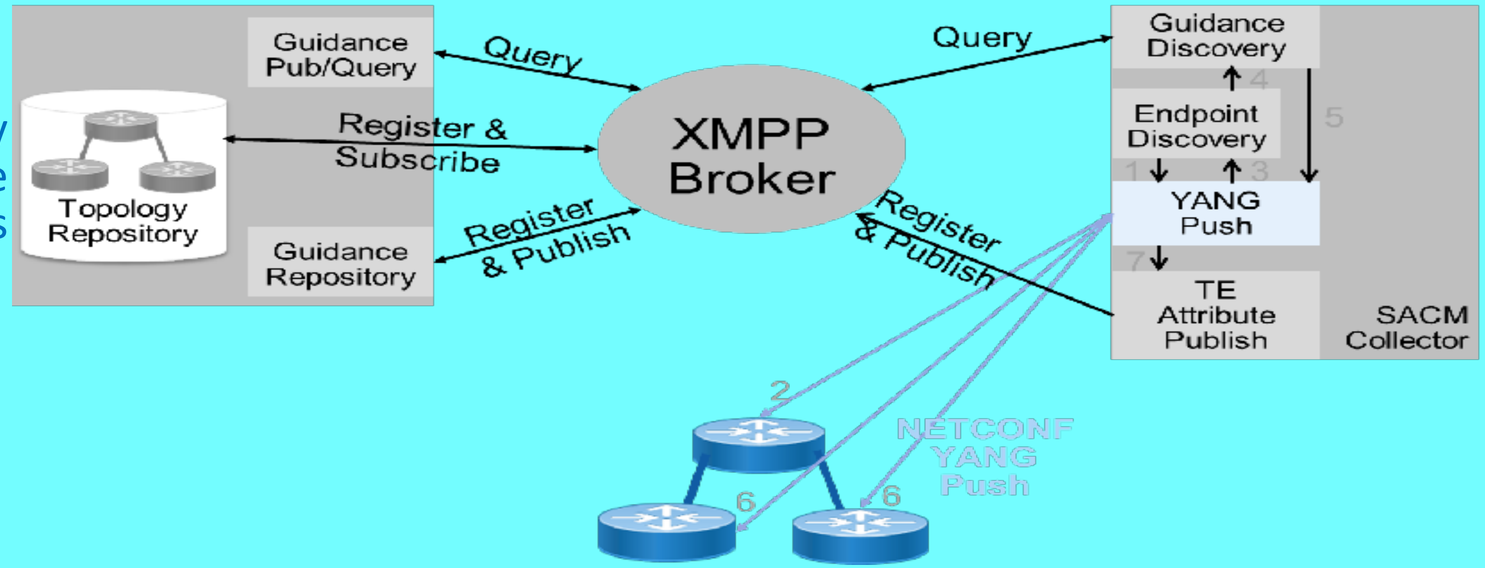
Thanks!

Hackathon 100 Results
SACM + Telemetry via YANG Push

Winner: Best Cross WG collaboration

- SACM
- NETCONF
- CORE

Device discovery
Topology maintenance
Security events



On Change subscription

- L2 link neighbors
- Hardware/software inventory

Telemetry
(and CoMI PUSH)

draft-birkholz-yang-push-coap-problemstatement

H. Birkholz <henk.birkholz@sit.fraunhofer.de>

Tianran Zhou <zhoutianran@huawei.com>

Xufeng Liu <Xufeng_Liu@jabil.com>

Eric Voit <evoit@cisco.com>

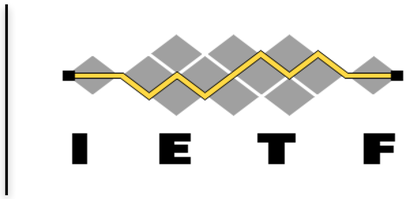
Motivation

- Telemetry
  - Changes to configuration and operational data (e.g. YANG datastores)
  - Streaming continuous changes happening on the device

- A feature called “YANG PUSH”
  - Remote extract of the datastore
    - Streaming delta of the data
  - In NETCONF / RESTCONF
    - Subscriptions are XPath expression

- Problem statement
  - Self-descriptiveness for data in motion for constrained devices and networks
  - Scalability – this is feasible (and may become crucial) for big routers

Next steps



- How to do it?
  - Use FETCH existing functionality to cover a huge percentage of the use-cases (multi-sub-tree extraction)
  - Represent XPath expressions in CBOR?
  - More?

- Next steps
  - Draft – extension on CoMI
  - Define new Content-Format for the XPath expressions
  - Work requires 43.7% CoMI, 56.7% YANG expertise

Thanks!

H. Birkholz <henk.birkholz@sit.fraunhofer.de>

Tianran Zhou <zhoutianran@huawei.com>

Xufeng Liu <Xufeng_Liu@jabil.com>

Eric Voit <evoit@cisco.com>

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

CoRE Pub/Sub

draft-ietf-core-coap-pubsub-02

Jaime Jimenez, Ari Keranen, Michael Koster

Status

- No substantial changes to the basic functionality since WG adoption
- Keeping the protocol simple
- Addressing a substantial set of comments in the next update

Roadmap

- Address all outstanding comments in the pending -03 draft
- Normative language to be reworked considering test cases generated from the requirements
- Security considerations section needs to contain more guidance
- Target WGLC for after revision -03 review

Early registration of 4.29 (too many requests)?

- 4.29 is useful for a number of design patterns that are similar to pubsub
- Should we register this now?

All times are in time-warped CEST

Monday (120 min)

- 13:30–13:40 Intro, Agenda, Status
- 13:40–13:55 Post-WGLC: CoAP-TCP (chairs)
- 13:55–14:05 Up for WGLC: CoCoA (CG)
- 14:05–14:45 Up for WGLC soon: RD (CA)
- 14:45–15:15 Up for WGLC soon: COMI (AP)
- 15:15–15:30 WG document: Pubsub (MK)
- If time permits: Payment over CoAP (AB)

HTTP (and CoAP) bindings for Payment Requests

W3C Web Payments WG

- Has defined a standard for requesting a payment
- Bindings defined for browser API
- WG being re-chartered to specify unbound data model in 2018

Proposal

- Define HTTP bindings for this data
- Headers in 402 (Payment Required) response
- Headers in paid requests/responses
- Also interest in CoAP bindings

Adrian Hope-Bailie
adrian@hopebailie.com

HTTP (and CoAP) bindings for Payment Requests

Support from Web Commerce IG, Web of Things WG and Automotive WG at W3C.

Soliciting interest from **HTTPbis** and **core**

Early proposal **draft-hope-bailie-http-payments**

Mailing list: **public-iotpay@w3.org**
Join via https://lists.w3.org/Archives/Public/public-iotpay/

Adrian Hope-Bailie
adrian@hopebailie.com

- **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 8179 and its updates**

üBlue sheets
üScribe(s)

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:

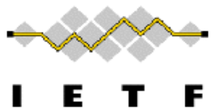
- **The IETF plenary session**
- **The IESG, or any member thereof on behalf of the IESG**
- **Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices**
- **Any IETF working group or portion thereof**
- **Any Birds 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 8179.

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 8179 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.



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

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

Media Types for Sensor Measurement Lists (SenML)

draft-ietf-core-senml-11

IETF 100, Singapore

Ari Keränen
ari.keranen@ericsson.com

Updates since -10

- Lots of editorial changes; thank you for all the reviews!
- Clarification: version field MUST appear in all resolved records if and only if different from default
- Removed link; to be done as extension
- Changed registry policy to Expert Review only
- Added SI-spec justification for Celsius unit

To Be Done

- Move security considerations from media type registrations to the security considerations section?
- More detailed IANA registry table?
- Final editorial tweaks

- Publish

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

Object Security ~~of CoAP~~ for Constrained RESTFUL Environments (~~OSCOAP~~) OSCORE

draft-ietf-core-object-security-06

Göran Selander, Ericsson
John Mattsson, Ericsson
Francesca Palombini, Ericsson
Ludwig Seitz, RISE SICS

IETF 100, CoRE WG, Singapore, Nov 14, 2017

Draft Status (v-06) (1/2)

- Protects the CoAP Code (now encrypted)
  - "dummy" Code for proxies: POST/FETCH for requests, 2.04 for responses
- OSCORE now describes cross-protocol translators (HTTP-to-CoAP, CoAP-to HTTP) (OCF request)→ Name change
  - Defines new HTTP header "Object-Security"
- Changed how the COSE compressed object is transported
  - CoAP payload → ciphertext
  - Object-Security option value → everything else

Draft Status (v-06) (2/2)

- Removed OSCON (from appendix)
- Simplified Observe processing
- Nonce construction
  - Sender ID is now part of the nonce
  - Partial IV does not need to be sent in (non-Observe) responses → Memory save

Interop Report

- Test specifications, reports, captures: https://github.com/EricssonResearch/OSCOAP

- 5 Interop (Feb, March, May, July, Nov)

- Last interop including latest changes: Hackathon IETF100
- Updated test spec, report to come
- 2 implementations tested (python, C#)
- 15 tests on succeeding and failing OSCORE processing

- Successful interoperation

Issues left

- Check the issue tracker!
  https://github.com/core-wg/oscoap/issues

- Observation renewal
- Minor issues as result of latest interop
- Privacy and traffic analysis considerations review
- RFC2119 compliance
- Test vectors

Next Steps

- WGLC

Multicast OSCORE

draft-tiloca-core-multicast-oscoap-04

Marco Tiloca, RISE SICS
Göran Selander, Ericsson
Francesca Palombini, Ericsson
Ji-Ye Park, Universitaet Duisburg-Essen

IETF 100, CoRE WG, Singapore, Nov 14, 2017

Multicast OSCORE

- Version -04 available: draft-tiloca-core-multicast-oscoap-04
- Aligned with latest version of OSCORE
- Addressed comments from IETF99, especially from Jim Schaad
- Improved readability, details are now in Appendices

Thank you!

Comments/questions?

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

Echo and Request-Tag

draft-ietf-core-echo-request-tag-00

Christian Amsüss, John Mattsson,
Göran Selander

Previously on this document

- IETF94: Echo option presented as "Repeat"
  (in core-coap-actuators)
- IETF98: Request-Tag option introduced
  (in core-request-tag)
- IETF99:
  - Pivoted to problem (core-coap-actuators) and solutions document (echo-request-tag)
  - Presented the relevant attacks
  - Asked for for reviews and alternative approaches

Current state

- Problem and solutions documents updated
- Fixed loudest complaint: "Repeat" → "Echo"
- Mechanisms fully established
- OSCORE uses both options
- Adopted by WG

Next steps

- Restructure the Echo part
- Editorial fixes

Issues tracked on
https://github.com/core-wg/echo-request-tag/issues

Questions

Thank you

Mitigating Delay Attacks on Constrained Application Protocol

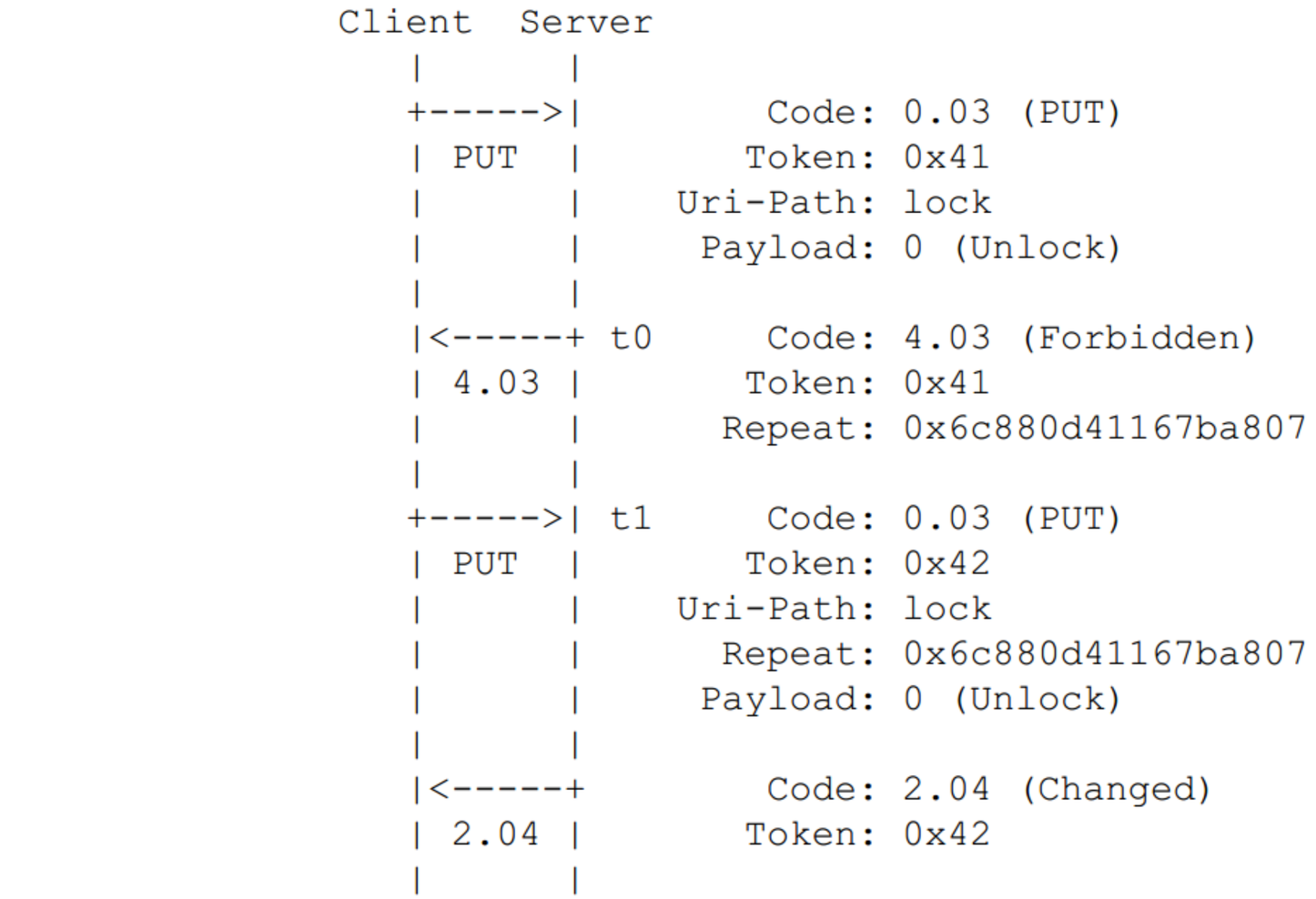
Scarlett Liu Julian Zhu
October 2017

(Scarlett.liuyan@huawei.com
Jintao.Zhu@huawei.com)

Background

- Delay attacks have become a topic in the CoAP, especially for the constrained nodes connecting and interacting the physical world.
- Draft-mattsson-core-coap-actuators proposes a challenge-response mechanism via a two round trips to mitigate delay attacks.

The mechanism specified in Draft-mattsson-core-coap-actuators

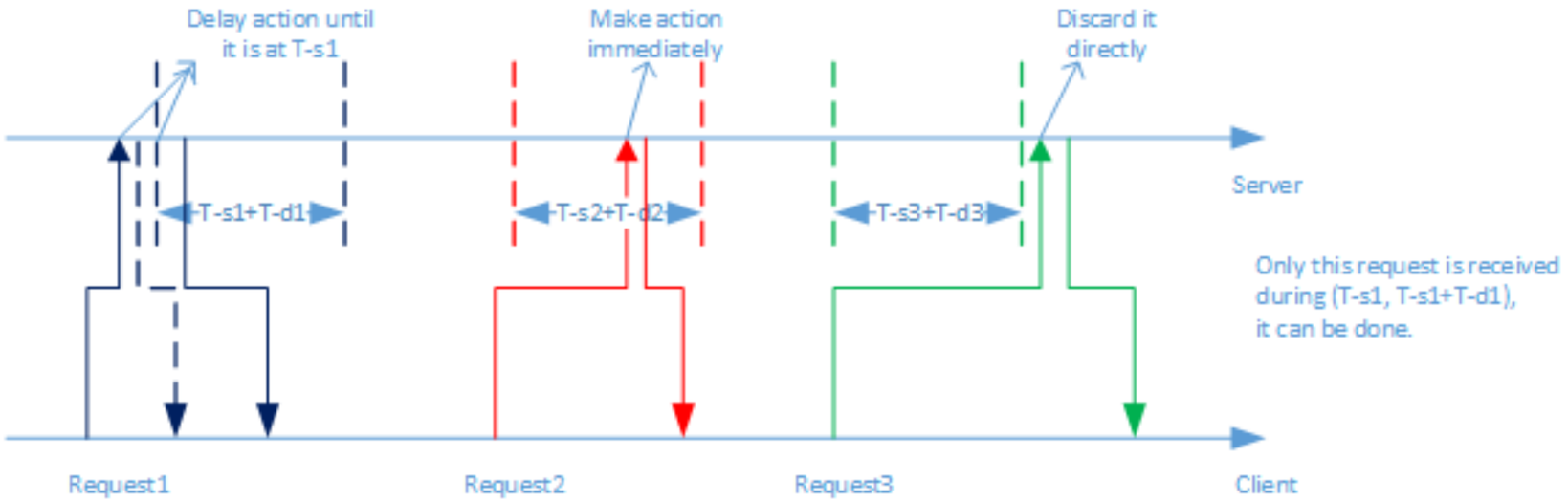


The Problem

- Regardless of the delay attacks, two round-trips increase the delay in processing of the original action.
- How to set the THRESHOLD on the server-side is confused and is hard to implement even in the some complicated situation where actions relevant for actuators are sensitive to time.

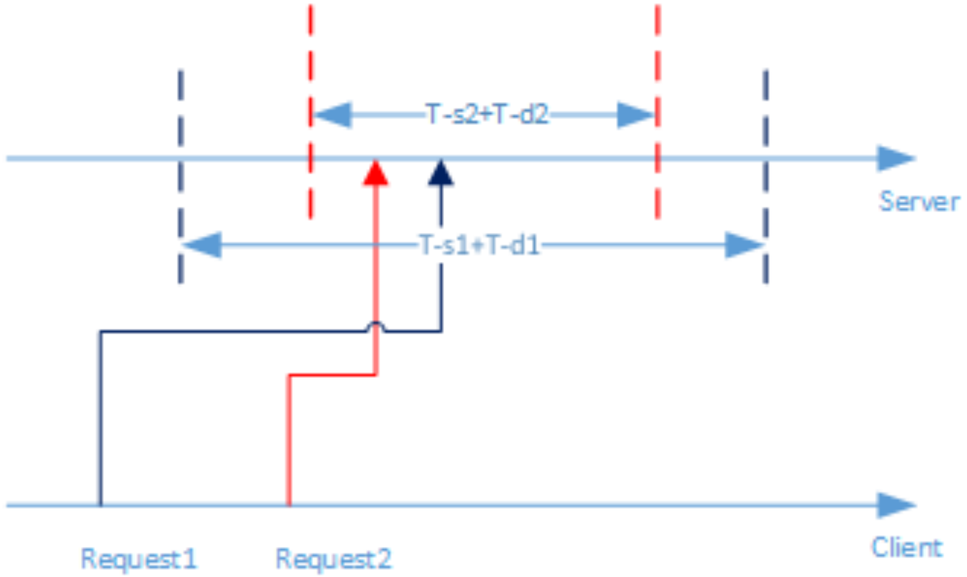
The Time Window Options(1)

- For simple single action actuators, the Time Window Option is introduced as a new CoAP option. The Time Window Option contains T-start and T-duration (as shown in Figure below).



The Time Window Options(2)

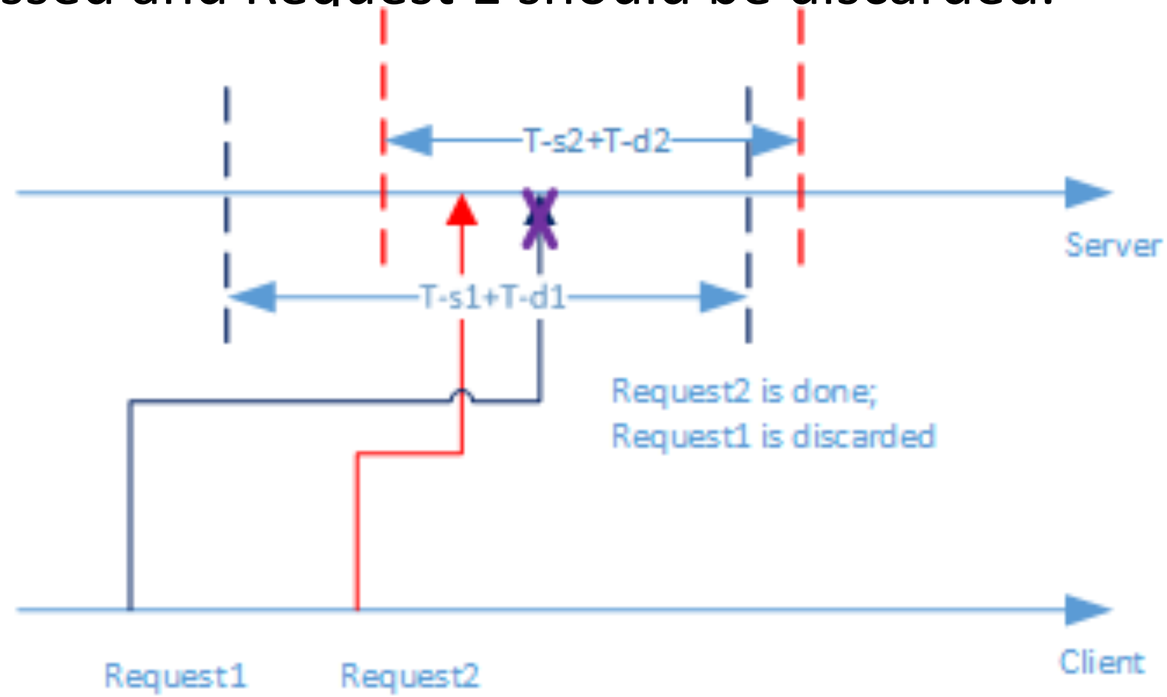
- For multi-interrelated action actuators, the Sequence Number Option and Response Policies are introduced. The Response Policies contains three modes to cope with the problem as shown in Figure below.



If Preemption Mode, Server will make action by request2 and discard requests which are later than request1.
If Sequence Mode, Server will always make action by the sequence numbers of the requests regardless of whoever first receives.
Else if Sequence and Discard mode, Server will refer to make action by the sequence numbers of the requests until the request2 who first receives almost expires, at that time Server must do by the request2. And if Server receives the request1 and must discard it.

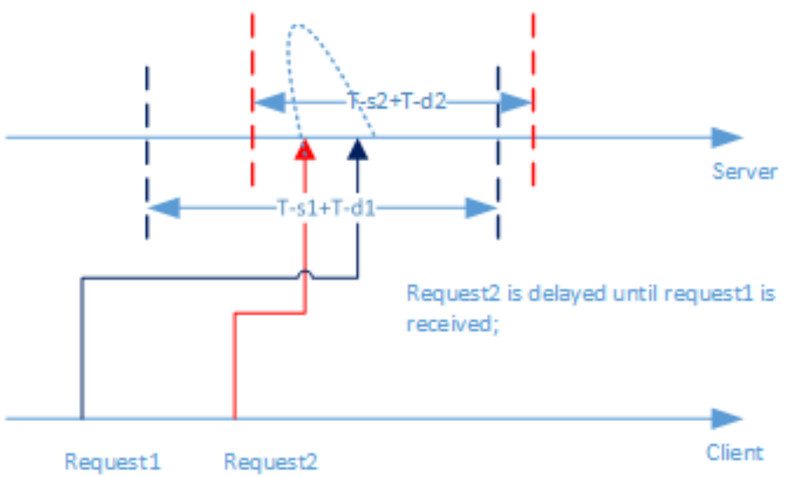
Response Polices(1)

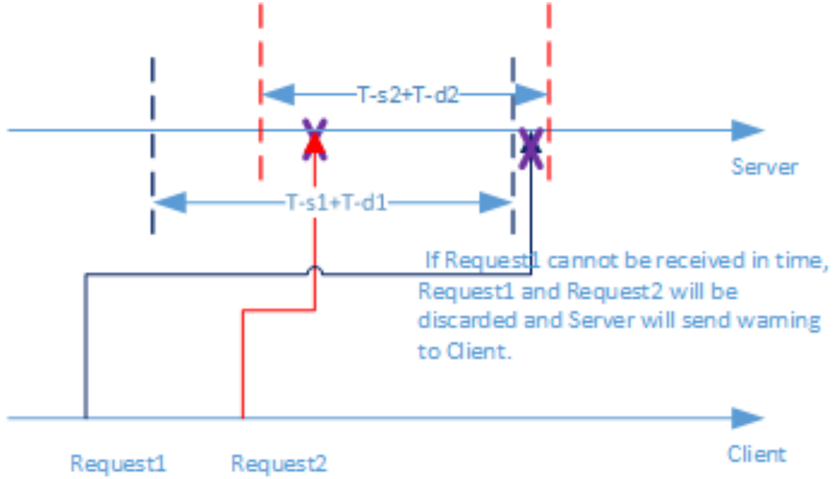
- Preemptive mode: if Request 2 comes earlier than Request 1 and Request 2 is in its valid time window, Request 2 should be processed and Request 1 should be discarded.



Response Polices(2)

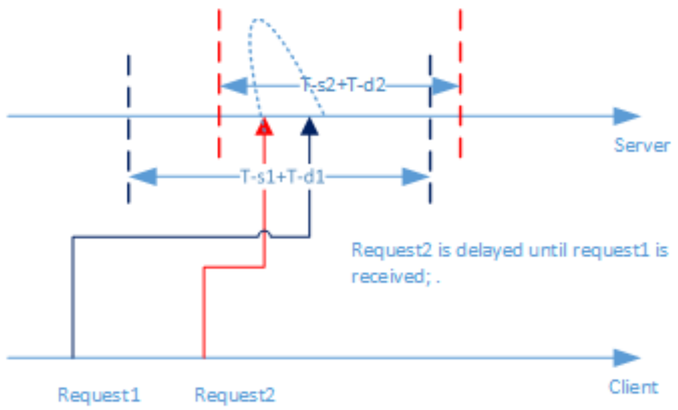
- Sequential mode: Although Request 2 comes earlier than Request 1 and Request 2 is in its valid time window, Request 2 cannot be processed until Request 1 is processed(as shown in the left Figure).
- If Request 1 cannot be processed due to delay, then Request 2 should be discarded (as shown in the right Figure).

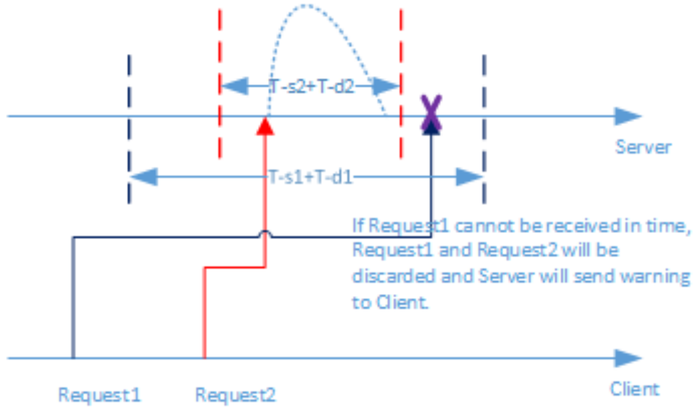




Response Polices(3)

- Sequential with conditional discard mode: Based on the Sequential mode, If Request 2 is about to expire but Request 1 has not come yet, Request 2 should be processed before it is expired as shown in the left Figure.
- Then, the Request 1 should be discarded when received as shown in the right Figure.





Thank you ☺️

Comments / Questions ?

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

‘Pending’ response code

Peter van der Stok, Klaus Hartke

IETF 100 - CoRE Working Group

Motivation

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

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

This draft specifies CoAP new response code x.xx for the same purpose.

Details

- Pending response indicates that target resource exists, but no representation is available yet.
- Location may be specified where result will become available.
- Allows multiple clients to have multiple concurrent requests open at the server.
- Client has to retry with GETrequest after Max-Age.
- Can be used in conjunction with “observe”
- Not covered by current CoAP response codes

- Interesting for this WG?

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

SMS

- draft-becker-core-coap-sms-gprs
- Recently got a new editor (Koojana Kuladinithi)

- Didn’t get enough support for adoption yet
- More support may be forthcoming
- Might want to do adoption call soon

draft-ietf-core-interfaces-10
&
draft-ietf-core-dynlink-04

draft-ietf-core-interfaces-10: status

- Overall, draft is in good shape
- 4 open issues to be resolved
  - 2 have been open since -09
  - 1 new one related to SenML explanations in the draft
  - 1 new one related to consistency with OCF interface design pattern for using “if” link target attribute

draft-ietf-core-dynlink-04: Status

- From -03 to -04: reverted “gth” and “lth” attributes to “gt” and “lt”
- Going forward: Needs some editorial work and clearer examples
- 4 open issues
  - 1 on error handling
  - 1 on adding a new link relation
  - 2 on absorbing work done in draft-groves-core-obsattr and draft-groves-core-bas

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

Draft-arkko-dev-urn-05

Arkko, Jennings & Shelby
(+ thanks to Ari's contributions)

A Uniform Resource Name (URN) namespace for hardware device identifiers.

Potentially useful in applications such as in sensor data streams and storage, or equipment inventories.

Complements other similar identifiers NIs (RFC 6920), UUIDs (RFC 4122), IMEIs (RFC 7254) etc. Supports, e.g., MAC and EUI-64, identifiers.

urn:dev:mac:0024befffe804ff1

Version -05

- Delimiter change to ensure easy carrying in SenML
  - urn:dev:ow:264437f5000000ed;humidity vs. urn:dev:ow:264437f5000000ed_humidity
- Introduced “local” or “organisation specific” device identifiers
  - urn:dev:org:32473:123456
- More text on privacy considerations
- Added text to IANA considerations to specify when new allocations under DEV URNs are appropriate

Next Steps

- Thoughts on the delimiter change? Breaks any existing usage?
- Thoughts on local device identifiers?
- Adding device IDs specified in OneM2M and LWM2M (urn:dev:os and urn:dev:ops)? And would BBF USP protocol identifiers be useful to add as well?
- Peter: Needs to use the new URN registration template
- Fix a mistake in ABNF (org: vs. dn:)
- Draft adoption?

All times are in time-warped CEST

Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

OPC UA Message Transmission Method over CoAP

draft-wang-core-opcua-transmission-02

Ping Wang< wangping@cqupt.edu.cn >,
Chenggen Pu< mentospcg@163.com >,
Heng Wang< wangheng@cqupt.edu.cn >,
Yi Yang<382991208@qq.com>,
Lun Shao<yjssslcqupt@163.com>,
Junrui Wu<wjr930914@gmail.com>
Chongqing University of Posts and Telecommunications, China

Jianqiang Hou<houjianqiang@huawei.com>
Huawei Technologies, China

Singapore, November 12, 2017

Motivations and Goals

- Motivations
  - OPC Unified Architecture (OPC UA) is a data exchange standard that provides interoperability in industrial automation.
  - Utilizing OPC UA transmitting over CoAP could meet the demand for industry 4.0 based on the exchange of semantic information.
- Goals
  - Implement the exchange of semantic information utilizing OPC UA transmitting in CoAP.
  - Enable the OPC UA packets transmission over CoAP.
  - Achieve different ways to transmit information from clients to servers based on OPC UA over CoAP.

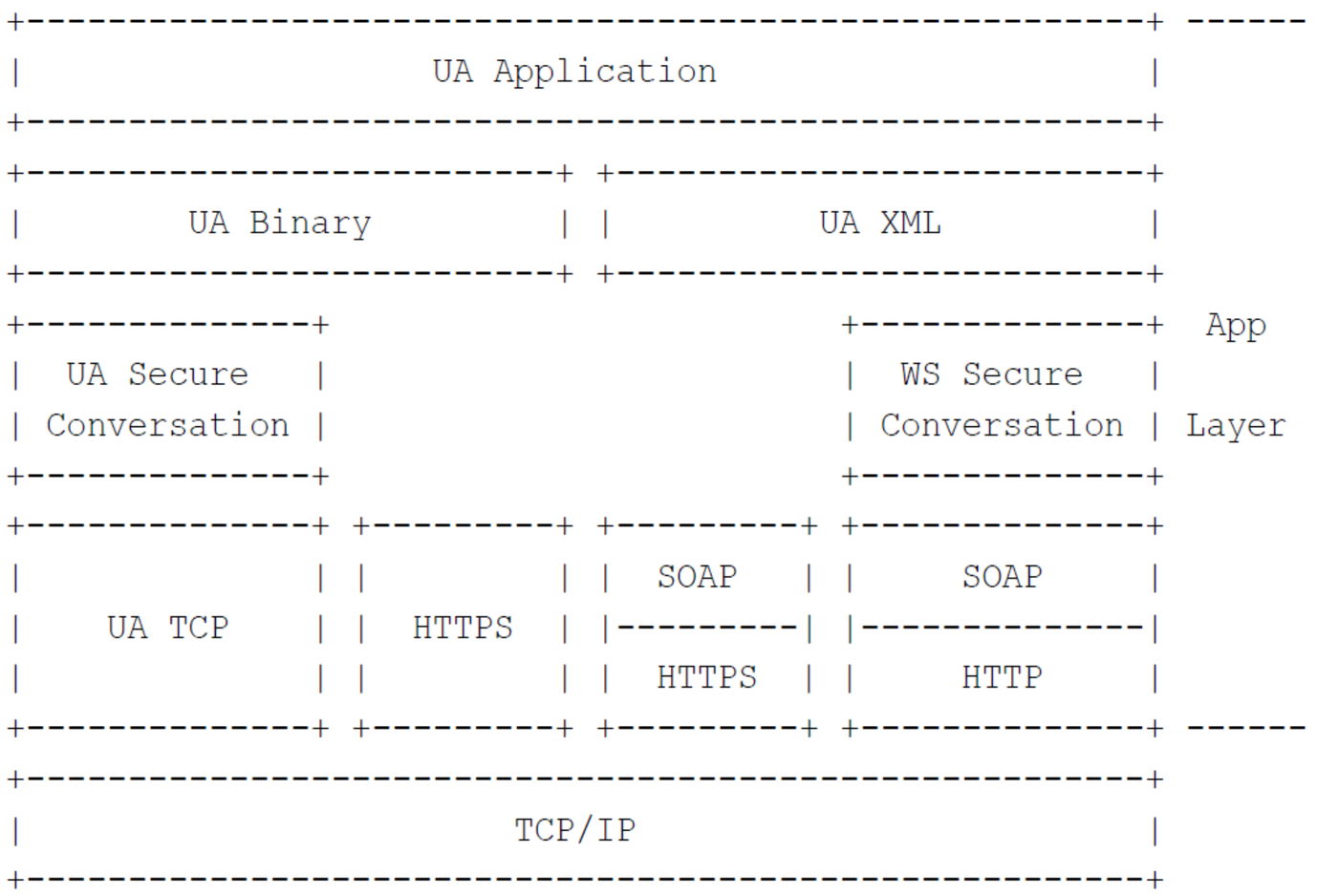
Overview

- What is OPC UA?
- Preliminary Work
- Architecture of OPC UA over CoAP
- Transmission scheme
- Next Steps

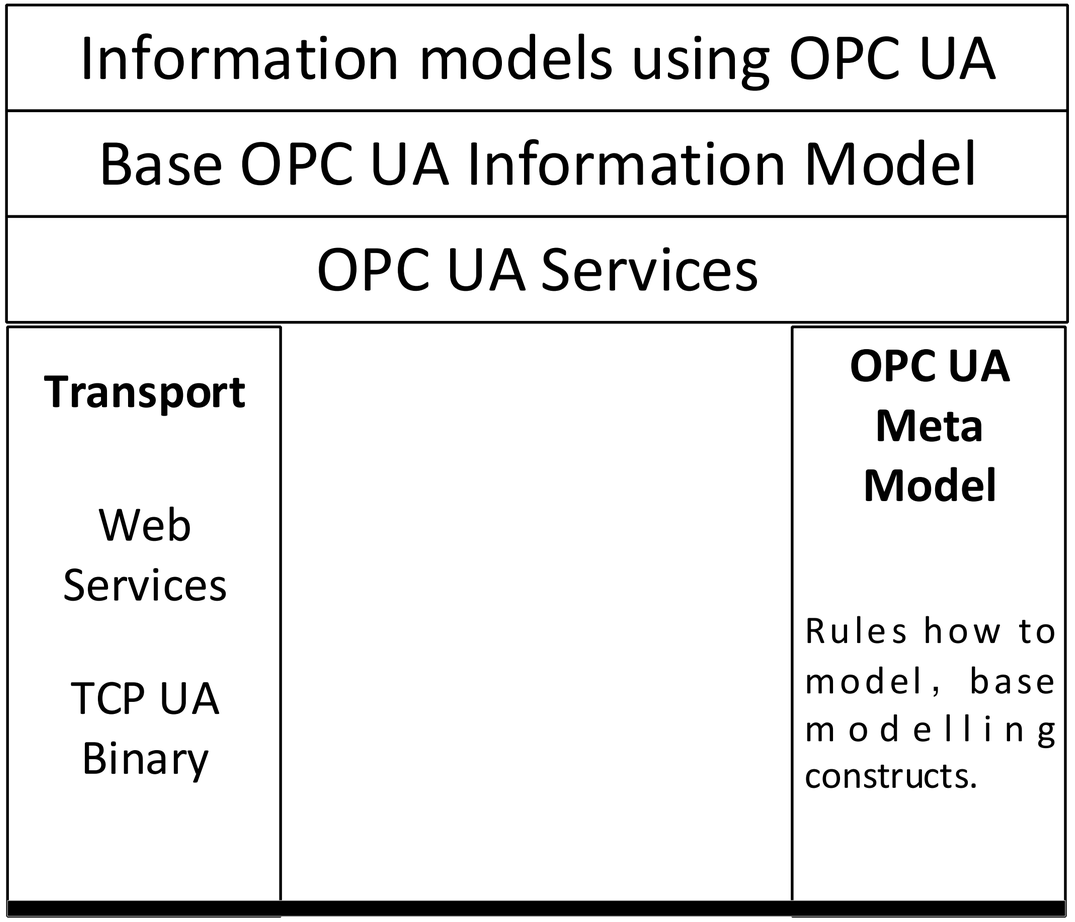
What is OPC UA?

- Overview of OPC UA
  - OPC Unified Architecture (OPC UA) is the data exchange standard for safe, reliable, manufacturer and platform-independent industrial communication. It enables data exchange between products from different manufacturers and across operating systems. It is the evolution product of OPC, the widely used standard process for automation technology, and combines the benefits of web services and integrated security with a consistent data model.
- Advantages of OPC UA
  - Functional equivalence: Building on the success of OPC Classic, OPC UA was designed to enhance and surpass the capabilities of the OPC Classic specifications.
  - Platform independence: From an embedded micro-controller to cloud-based infrastructure. all of them can use OPC UA, and whether it is WINDOWS, LINUX or MAC OS.
  - Secure: OPC UA is firewall-friendly while addressing security concerns by providing a suite of controls.
  - Comprehensive information modeling: The framework turns data into information. With complete object-oriented capabilities, even the most complex multi-level structures can be modeled and extended.

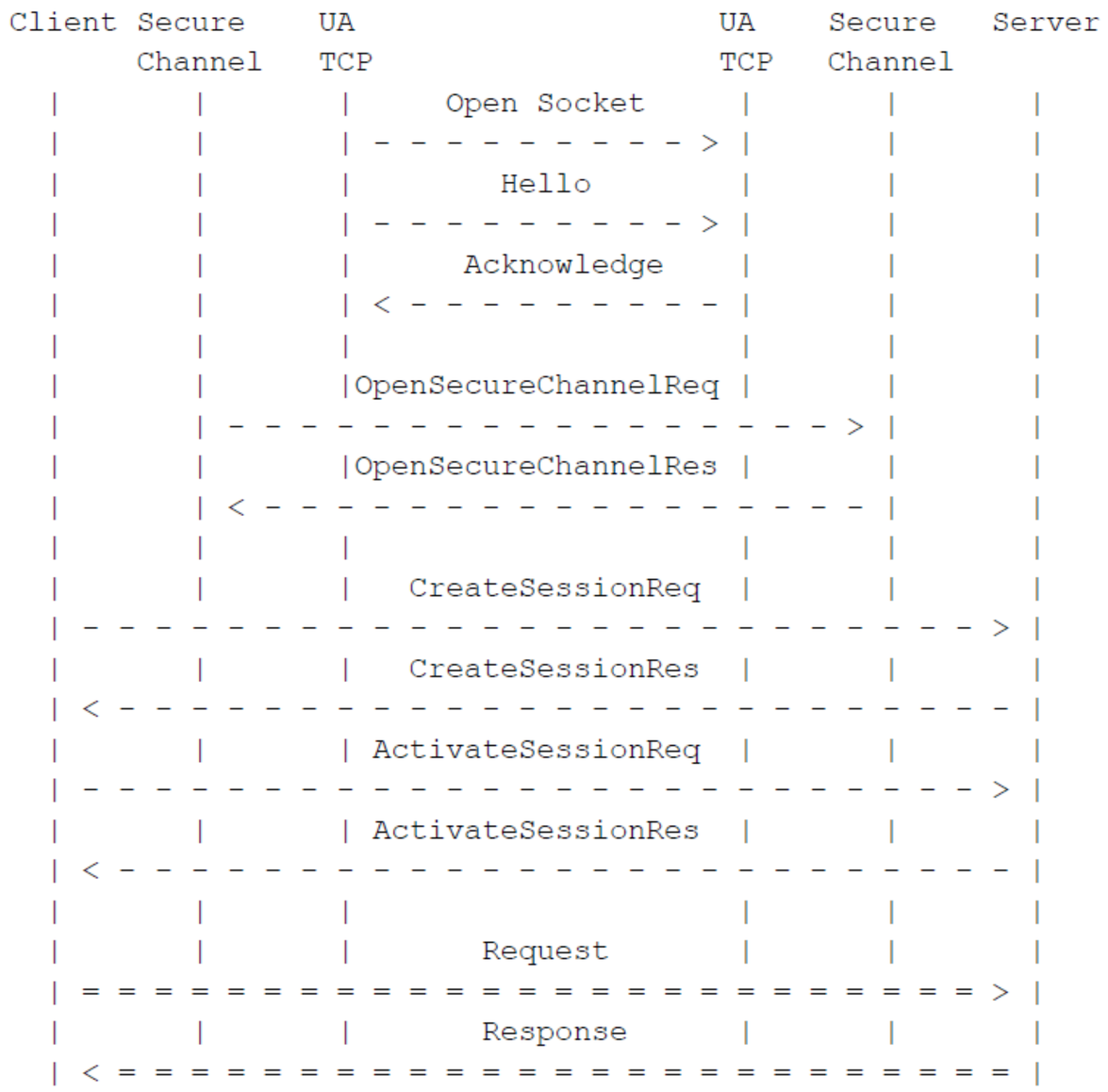
- Protocol Stack of OPC UA
  - Be built on existing protocols such as **TCP, TLS, HTTP.**
  - Consist of four sublayers: UA Application, Serialization Layer, Secure Channel Layer, Transport Layer.
  - Serialization layer includes two kinds of data encoding methods: **UA binary** and **UA XML**, which respectively has its advantages.
  - Set secure channel layer as none, and in transport layer, the options can be UA TCP, HTTPS, SOAP/HTTPS and SOAP/HTTP.



- The Foundation of OPC UA
  - The fundamental components of OPC UA are **transport mechanisms** and **data modeling**.
  - The transport defines different mechanisms optimized for different use cases.
  - Optimized for **speed and throughput** = UA TCP with UA Binary; **firewall-friendly** = HTTP + XML.



- Request/Response Model of OPC UA
  - The message exchange in UA binary mode.
  - Using “hello” (HEL) and “acknowledge” (ACK) messages for clients to connect with servers.
  - Using a pair of specific messages to open security channel and define the encryption property.
  - Using another two pairs of specific messages to create and activate a session.
  - After all of these steps, the connection is initiated and the client can send request messages for services.

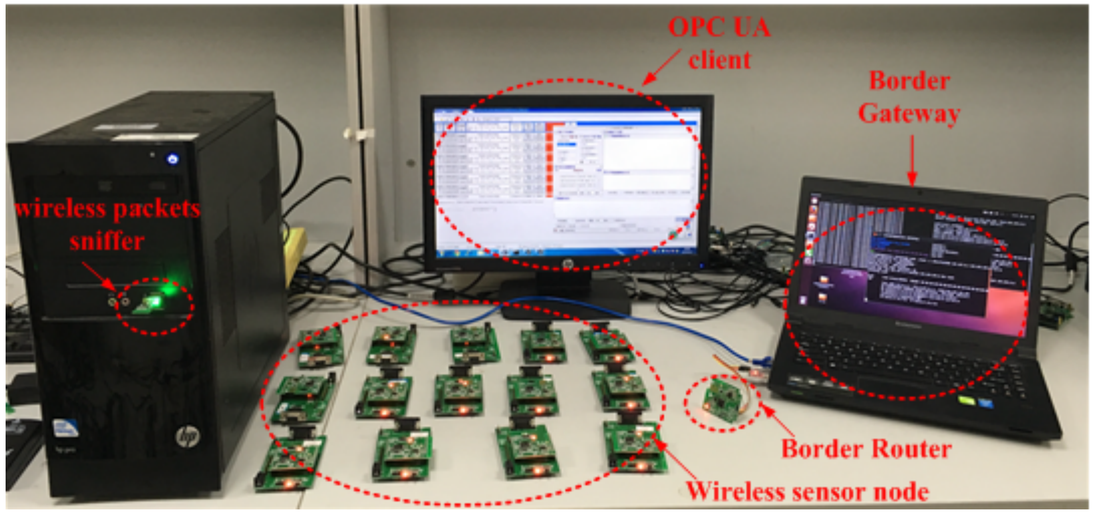


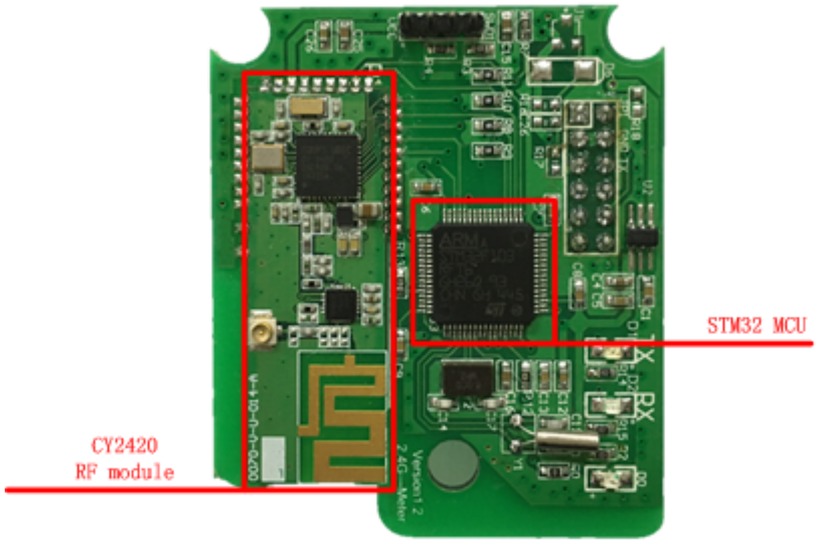
Preliminary Work

- Design an OPC UA compression and decompression mechanism for 6LoWPAN.
- Design a nano OPC UA server for Wireless field devices by using contiki3.0.
- Integrate IEEE 802.15.4 with OPC UA for Low-Power Wireless Sensor Networks.
- Design a dormant agent mechanism with OPC UA.

Layer	Protocol
Application	OPC UA(Based on open62541)
Transport	TCP
Network	IPv6/RPL
Adaptation	6LoWPAN
MAC	IEEE 802.15.4
Physical	IEEE 802.15.4

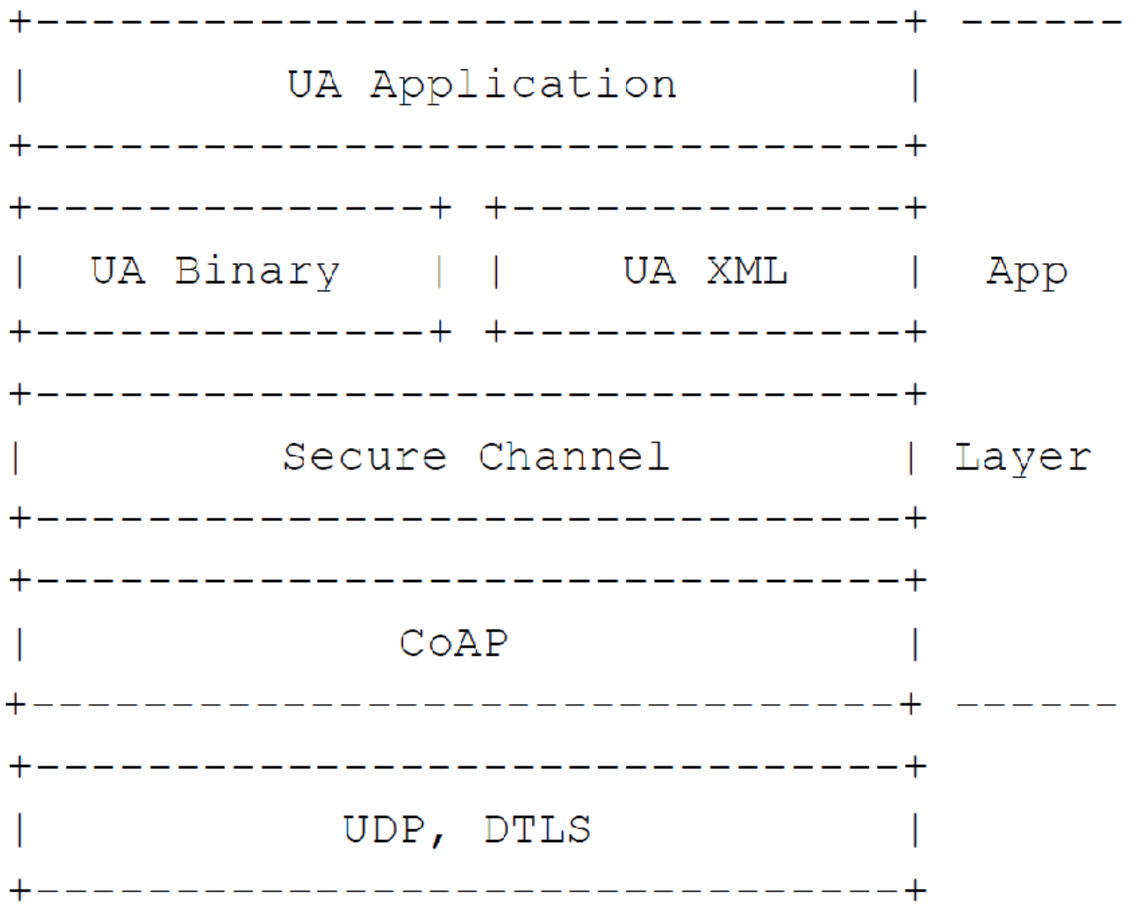
- Testing Platform
  - Nodes use STM32@72Mhz and CY2420 RF module.
  - Build a test network consisted of 15 nodes , a border router and an OPC UA client(UA EXPERT).
  - The purpose is applying OPC UA to WSNs based on 6LoWPAN.





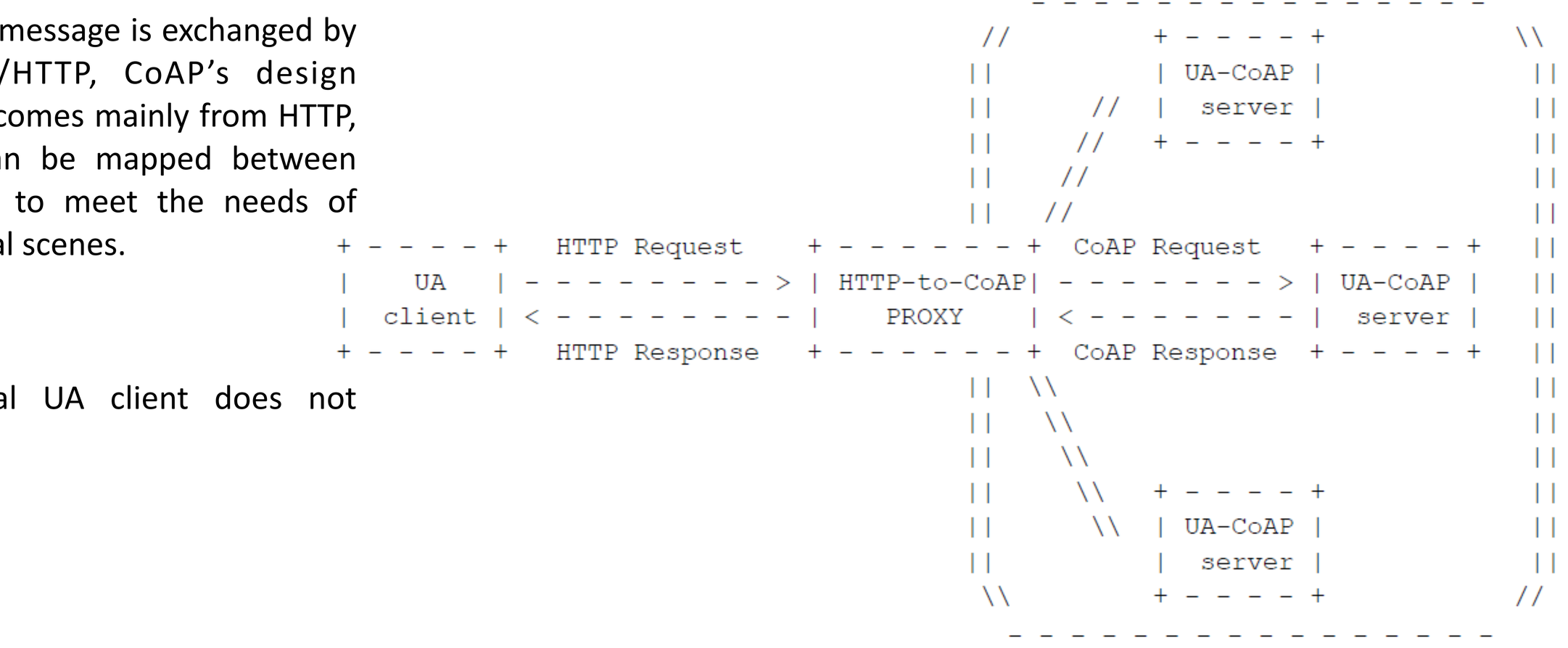
Architecture of OPC UA over CoAP

- Two options in Serialization Layer
  - OPC UA packets are encoded in either UA binary or XML format, and the option field in the CoAP header can specify parameters that support both formats.
- Security
  - DTLS runs on the top of UDP in transport layer to make sure the whole communications work in the security mode. HTTPS -> DTLS

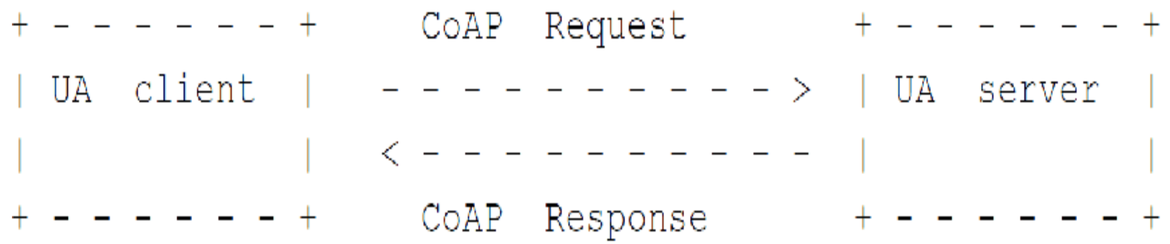


Transmission scheme

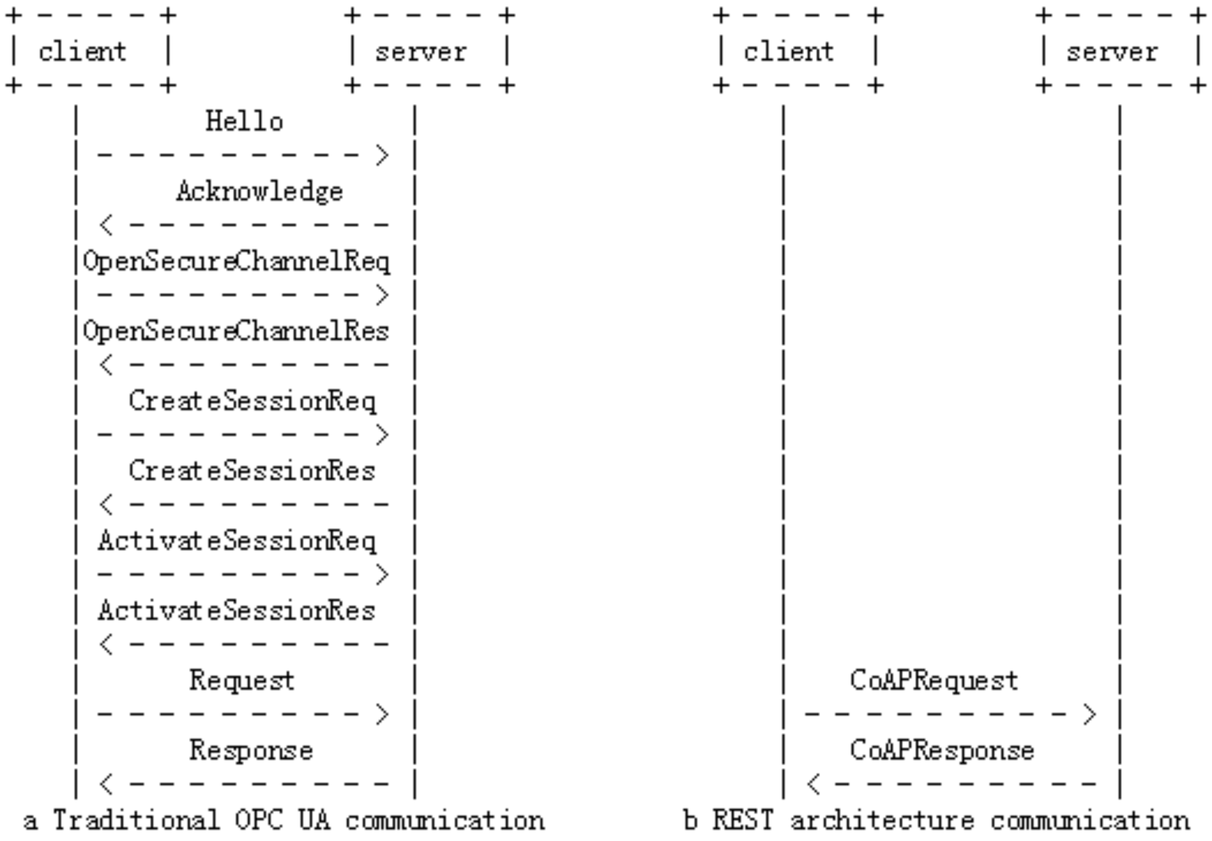
- Proxy for OPC UA-CoAP
  - In OPC UA, message is exchanged by using TCP/HTTP, CoAP's design inspiration comes mainly from HTTP, the two can be mapped between each other to meet the needs of some special scenes.
  - The original UA client does not change.



- Direct transmission
  - OPC UA packets are encoded in either binary or XML format, and the optional fields in the CoAP header specify parameters to support these two formats.
  - The entire packet of the OPC UA can be encapsulated in the payload of the CoAP message for direct transmission.
  - Noted that this method of transmission needs to be modified on the server side and the client side of the OPC UA according to CoAP.



- REST transmission for OPC UA
  - The traditional OPC UA requires a series of interactions between normal read and write operations.
  - Reduce the interactions process in OPC UA, CoAP request/response carries OPC UA information model to achieve communicating.
  - For the constrained scenes, it’s a good choice.



Next Steps

- Add some use cases of the draft and further improve the details of the draft.
- Implement the proposed architecture.
- Make some considerations about security.
- Optimize pub/sub of OPC UA and CoAP.

Thanks!

Ping Wang< wangping@cqupt.edu.cn >,
Chenggen Pu< mentospcg@163.com >,
Heng Wang< wangheng@cqupt.edu.cn >,
Yi Yang<382991208@qq.com>,
Lun Shao<yjssslcqupt@163.com>,
Junrui Wu<wjr930914@gmail.com>,
Chongqing University of Posts and Telecommunications, China

Jianqiang Hou<houjianqiang@huawei.com>
Huawei Technologies, China

Singapore, November 12, 2017

All times are in time-warped CEST

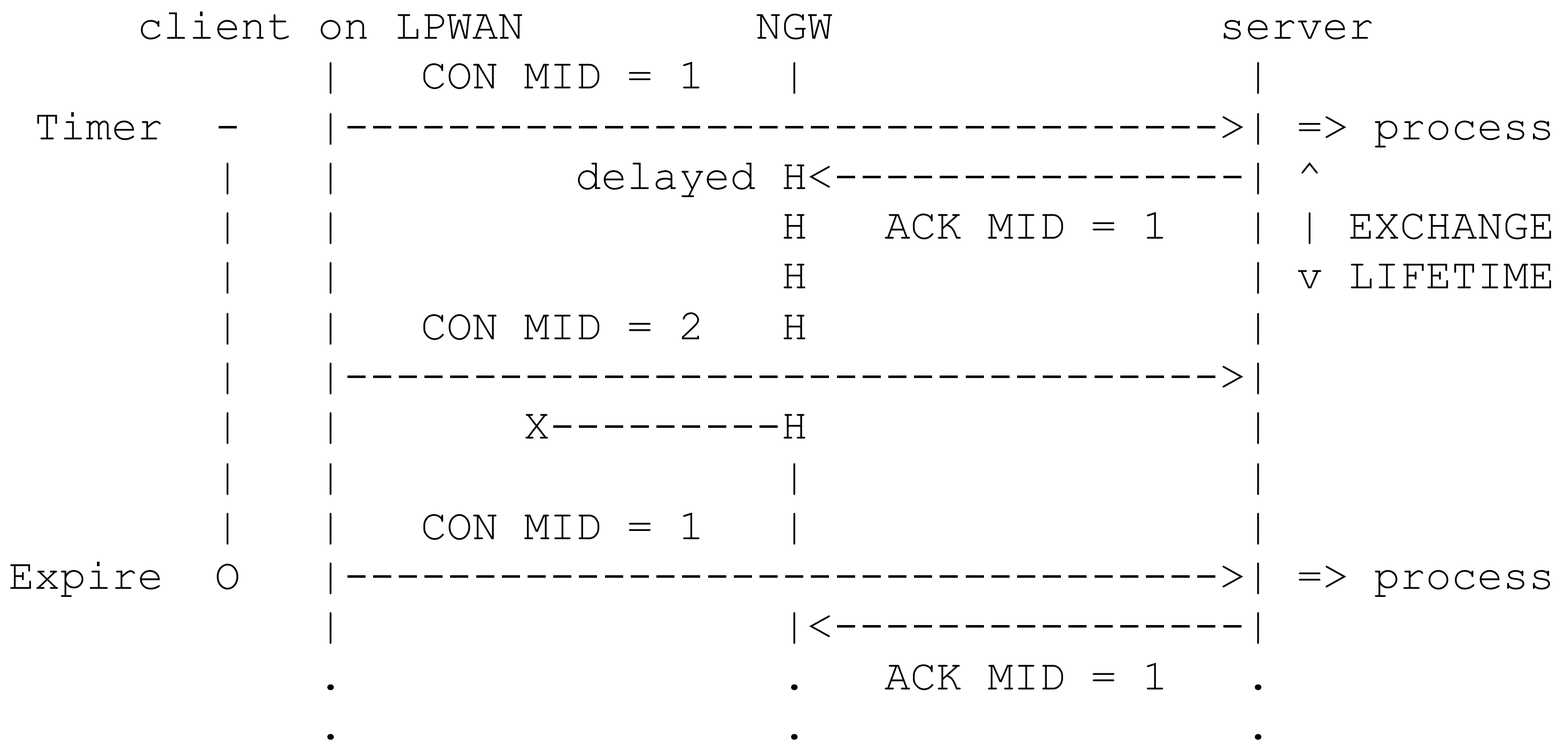
Tuesday (120 min)

- 13:30–13:35 Intro, Agenda
- 13:35–13:50 Post-WGLC: SenML (AK)
- 13:50–14:20 Up for WGLC: OSCORE (FP)
- 14:20–14:35 Newly adopted: ERT (?)
- 14:35–14:45 Pending for EST (PV)
- 14:45–15:00 SMS; Dynlink/Interfaces
- 15:00–15:10 dev URN (JA)
- 15:10–15:20 OPC/UA (CP)
- 15:20–15:30 Time scale (LT)

Draft-toutain-core-time-scale-00

Authors:
Laurent Toutain <laurent.toutain@imt-atlantique.fr>
Ana Minaburo <ana@ackl.io>

LPWAN Networks



CoAP Server

- Have to deal with clients sending at different periods:
  - Ack may be delayed by the downlink (sleeping nodes)
  - MID must be kept for a longer duration in server to detect duplicates

Time Scale option

Number	C	U	N	R	Name	Format	Length	Default
259	X				Time Scale	uint	1-4	3600

- Critical option: to inform client if the option is supported or not.
- No caching
- In all requests

DoS attack

- Too much MID in memory if hold duration is increased ?
  - Time Scale informs the server of the period
  - Server can still limit the number of MID per device.