



23 June 2017 Webex

IPv6 over the TSCCH  
mode of IEEE 802.15.4

Chairs:

**Pascal Thubert**

**Thomas Watteyne**

Etherpad for minutes:

<http://etherpad.tools.ietf.org:9000/p/6tisch?useMonospaceFont=true>

# Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- By participating with the IETF, you agree to follow IETF processes.
- If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.
- You understand that meetings might be recorded, broadcast, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:

- BCP 9 (on the Internet Standards Process)
- BCP 25 (on the Working Group processes)
- BCP 78 (on the IETF Trust)
- BCP 79 (on Intellectual Property Rights in the IETF)

# Reminder:

Minutes are taken \*

This meeting is recorded \*\*

Presence is logged \*\*\*

\* Scribe; please contribute online to the minutes at: <http://etherpad.tools.ietf.org:9000/p/6tisch?useMonospaceFont=true>

\*\* Recordings and Minutes are public and may be subject to discovery in the event of litigation.

\*\*\* From the Webex login

# Agenda

- Administrivia [10min]
  - Agenda bashing, approval minutes, past TODO's
  - Announcements (TEE webinar, Maria-Rita's non WG forming BoF)
  - IETF99, getting ready
- draft-ietf-6tisch-terminology-09 [5min] [Maria Rita]
- draft-ietf-6tisch-6top-protocol (Xavi, Qin) [10min]
- Security DT Update [10min]
  - draft-ietf-6tisch-minimal-security-03 [Malisa]
  - Other news [Michael]
- Plugtests Update [15min]
  - admin [Thomas]
  - update TD [Maria Rita]
  - update golden image [Tengfei]
  - update tools [Remy]
- AOB [10min]
  - hackathon: OpenWSN, ...?

# Last Interim Action Items

- Xavi and Qin to follow up review SF0
- Diego to continue the thread on time out computation between SF0 and 6P. Whether ASN of the time out should be indicated in the packet.
- Xavi and Qin to post 6p-06 addressing Jonathan's comments
- All to review the plugtest TD



# TEE Webinar [announcement]

I thought you may find it interesting that there are a few webinars scheduled in context of the IETF TEEP effort to increase awareness of Trusted Execution Environments (TEEs).

If you are interested to learn about that technology please add your name to the Doodle poll. The conference bridge details will be posted to the IETF TEEP mailing list:

<https://www.ietf.org/mail-archive/web/teep/current/maillist.html>

Here is the link: <http://doodle.com/poll/ynpkewhruwwin8fv>

Here is some additional info: <https://www.ietf.org/mail-archive/web/teep/current/msg00125.html>

Ciao

Hannes & Dapeng

# non-WG forming BoF at IETF99 - Prague

**Info session M2MSAT project**

# M2MSAT project

<https://artes.esa.int/projects/m2msat>

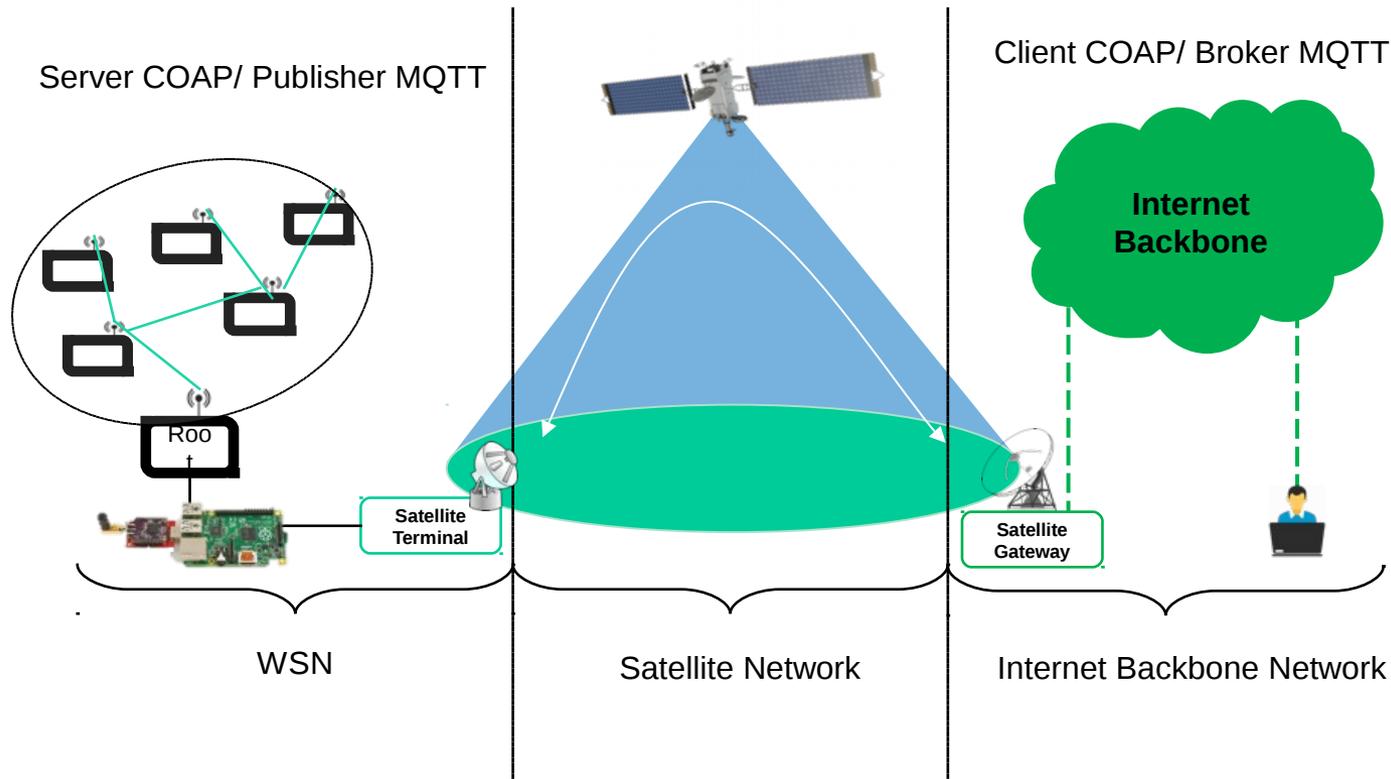


- Funded by ESA (ITT AO8550)
- “Light-Weight Application and Transport Protocols For Future M2M Applications”
- 15 months – started October 2016
- Partners:

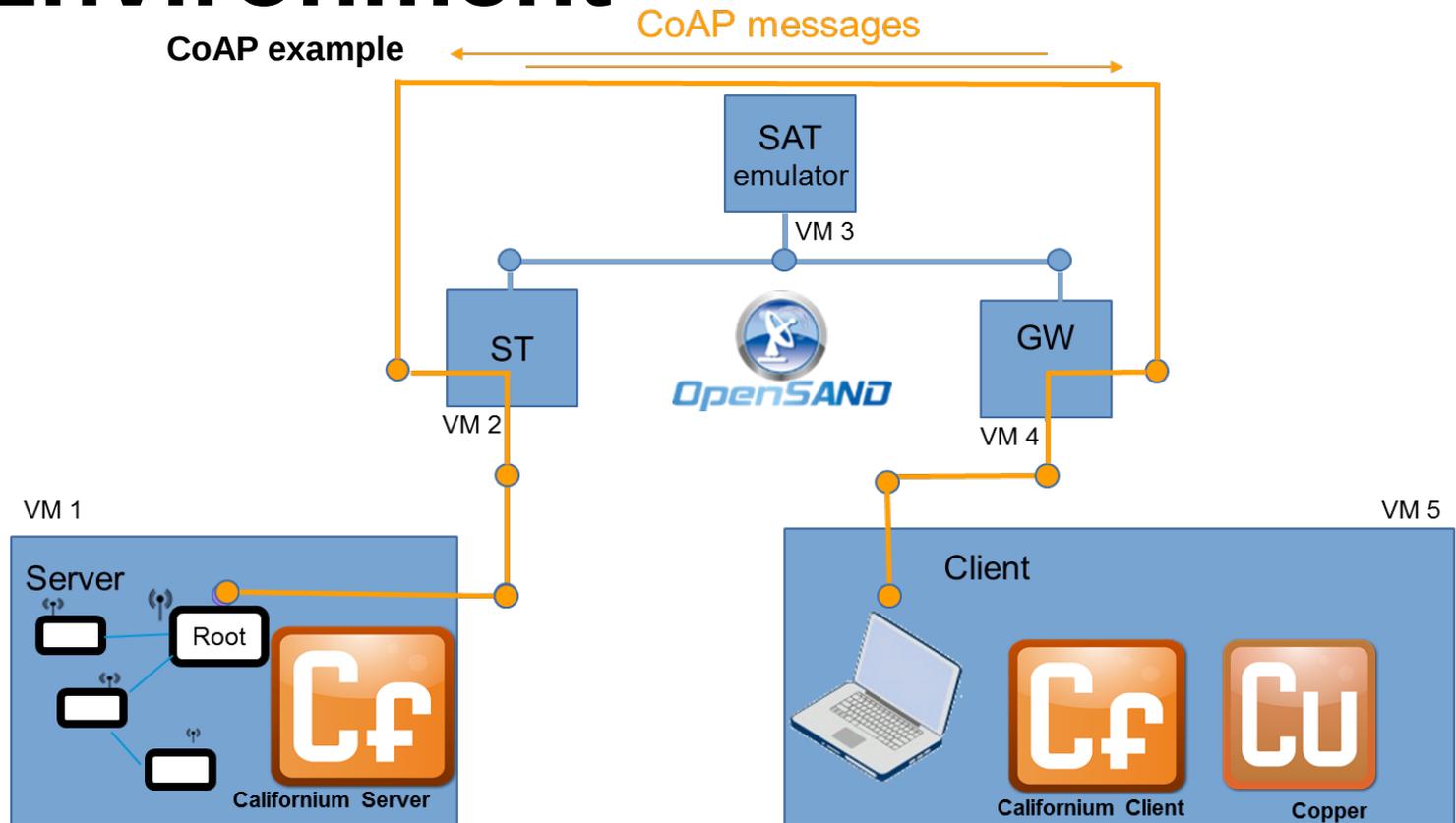


- **Objectives**
  - Identify M2M/IoT protocols suitable for future services
  - Define references M2M/IoT satellite network scenarios
  - Design protocols optimizations, and integrated network functions
  - Demonstrate, via implementations in a real testbed, the achievable enhanced performance

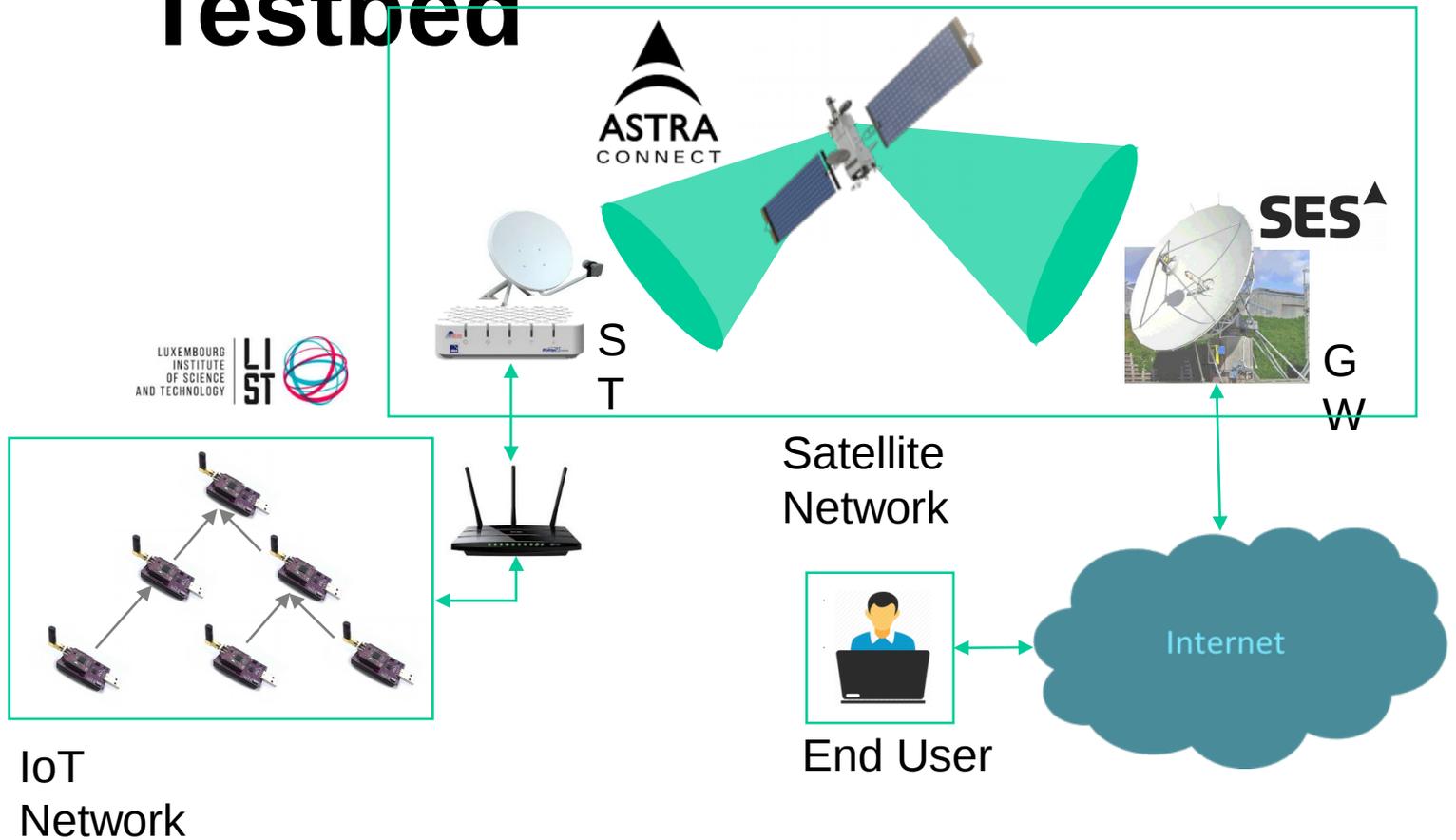
# System Architecture with GEO satellite



# Simulated Environment



# IoT - satellite Testbed





# About the Info Session

Where: IETF99 – Prague

When: schedule will be published on Monday

Preferable Monday July 17<sup>th</sup> 2017

Before or after 6TiSCH meeting – do you see any conflict??

Scope:

Disseminate about the M2MSAT project

Receive Feedback from SDOs

6TiSCH, CORE, 6lo, LPWAN, etc.

# IETF99 update

- 6TiSCH-related agenda
  - Fri 14 July: plugtest (afternoon only, starting 2pm!)
  - Sat 15 July: plugtest (all day)
  - Sun 16 July: hackathon (under name “OpenWSN”)
  - Mon 17 July: 6TiSCH WG meeting (1.30-3.30pm)
- 6TiSCH WG meeting
  - Call for agenda items opens today (see ML)
- Important dates
  - Fri 23 June: final agenda published
  - Mon 03 July: draft cut-off
  - Wed 05 July: draft WG agenda
  - Fri 07 July: early bird registration cut-off
  - Mon 10 July: revised WG agenda



# draft-ietf-6tisch-terminology-09

Maria Rita Palattella

# draft-ietf-6tisch-terminology-09



.v08 expired

.v09 published on 2017-06-19

Main difference compared to v8

- Updated references
  - draft-ietf-6tisch-minimal -> RFC8180
- updated security related terms
  - JN -> Pledge,
  - JCE -> Join Registrar/Coordinator (JRC)
  - JA -> Join Proxy (JP)



# draft-ietf-6tisch-6top-protocol

Xavi Vilajosana

Qin Wang

# 6P latest update

- Status: published v6
- Minor changes according to comments received by Jonathan and Lotte.
- Still needed: update references to RFC8180 and RFC8137 (ready in v7 but not published yet).
-



# 6p Comments from Jonathan

->Section 4.1: "If no dedicated cells are scheduled between nodes A and B, shared cells MAY be used. -> Is there another option? if not, shouldn't say MUST?"

[Qin] There may be another option. i.e. do nothing if no dedicate cells

[JM] Do nothing is always an option. If a 6p transaction is going to happen, either on a dedicated cell or a shared cell.

**[Resolution:]**"If no dedicated cells are scheduled between nodes A and B, shared cells **are** used'

->Section 4.3.2:

" All cells in the CellList MUST already be scheduled between the two nodes and must match the CellOptions field. If node A puts cells in its CellList that are not already scheduled between the two nodes and match the CellOptions field, node B replies with a RESET return code"

Section 4.3.3:

"Upon receiving the request, node B's SF verifies that all the cells in the Relocation CellList are indeed scheduled with node A, and are associate the options specified in the CellOptions field. If that check fails, node B MUST send a 6P Response to node A with return code CELLLIST\_ERR."

Both errors give a different response but it looks to me that they have the same source -mismatch in their schedule-. Is it ok?

[Qin] should change error code in 4.3.2 to CELLLIST\_ERR.

**[Resolution:]**RESET → CELLLIST\_ERR



# 6p Comments from Lotte

RETURN CODES →

Return code of ERR\_VER in section 4.4.1., but doesn't list it in the table of section 8.2.4. 6P Return Codes (the table does, however list VERSION).

RESOLUTION->Table fixed as VER\_ERR also return codes updated.

Also, the table in section 8.2.4 mentions a return code called SFID, while section 4.4.2. says to set a return code called ERR\_SFID. The same goes for other codes, such as ERR\_GEN, ERR\_EOL and ERR\_BUSY. Is this intentional?

Same here; errors have been updated to SFID\_ERR, GEN\_ERR, VER\_ERR, etc..



# draft-ietf-6tisch-minimal-security

Mališa Vučinić, Inria

Jonathan Simon, Linear Technology

Kris Pister, UC Berkeley

Michael Richardson, Sandelman Software Works

# Status

## News

draft-ietf-6tisch-minimal-security-03

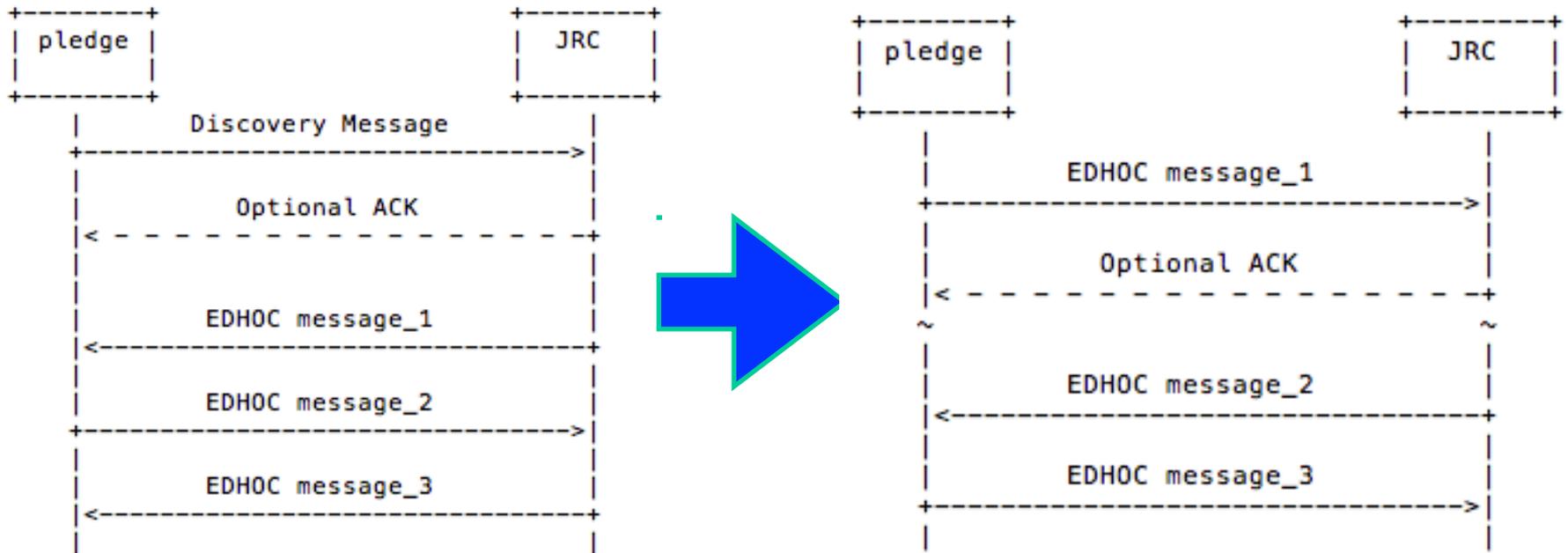
Published on June 15th 2017

Implementation under way

PSK variant will be tested during plugtest

Summary of updates in -03

# Update #1: Security Handshake



Optional with PSKs

Mandatory with asymmetric keys



# Update #2: How pledge learns JRC address

Pledge communicates at IP layer with JP  
JP statelessly forwards to JRC

How JP knows the address of JRC?

- Learns at join time when it acted as a pledge

- Join Response now contains the address

- Omitted if JRC is co-located with 6LBR root

- Assumption is that 6LBR is pre-configured with the address

# Update #3: Mandatory to Implement Algorithms

AEAD algorithm:

AES\_CCM\_16\_64\_128 from COSE

8 byte authentication tag

Corresponds to CCM\* in nonce length

Hash:

SHA-256

Asymmetric:

P-256 Elliptic Curve (secp256r1)

ECDSA with SHA-256 signature algorithm



# draft-ietf-6tisch-minimal-security-03

Malisa Vucinic



# other security DT news

Michael Richardson



# F-Interop 6TiSCH Plugtest

Maria Rita Palattella

Tengfei Chang

Remy Leone

Xavi Vilajosana

Thomas Watteyne

# Plugtest: Admin

- Schedule
  - Friday: afternoon only, starting at 2pm
    - Room will be open in the morning, you'll welcome to use it
  - Saturday: all day
- Sync'up calls with participants
  - Date TBD, proposal: Monday 3 July 4pm CEST
  - To be confirmed on ML
- But, most importantly
  - Food and drinks throughout the session (same as during 6TiSCH #1 plugtest!)
  - Dinner planned Friday event (free of charge for participants, thanks ETSI/LIST)

# Update Test Description

- Update by Thomas Watteyne
- Open questions:
  - Is RFC8138 mandatory?
  - status dissectors; revise draft-munoz-6tisch-examples

# Update Golden Image

- Overview by Tengfei Chang

# Update (F-interop) Tools

- Overview by Remy Leone



AOB



# OpenWSN hackathon

- Announcement: <https://www.ietf.org/mail-archive/web/6tisch/current/msg05384.html>
- Info: <https://www.ietf.org/registration/MeetingWiki/wiki/99hackathon>
- Core team present only on Sunday (conflict with plugtest)
- Current work:
  - RIOT support: enable OpenWSN on RIOT platform.
  - F-Interop: The traditional interoperability test need vendors to sit down in a same room and perform the test with varies of tools. With F-Interop, everything will be done at home.
  - 6TiSCH Wireshark Dissector.
  - TBA

# Packet Expiration Time in 6LoWPAN Routing Header

## draft-lijo-6lo-expiration-time-03

<https://www.ietf.org/id/draft-lijo-6lo-expiration-time-03.txt>

Lijo Thomas <[lijo@cdac.in](mailto:lijo@cdac.in)>

Akshay P.M <[akshaypm@ece.iisc.ernet.in](mailto:akshaypm@ece.iisc.ernet.in)>

Satish Anamalamudi <[satishnaidu80@gmail.com](mailto:satishnaidu80@gmail.com)>

S.V.R Anand <[anand@ece.iisc.ernet.in](mailto:anand@ece.iisc.ernet.in)>

Malati Hegde <[malati@ece.iisc.ernet.in](mailto:malati@ece.iisc.ernet.in)>

Charlie Perkins <[charlie.perkins@huawei.com](mailto:charlie.perkins@huawei.com)>

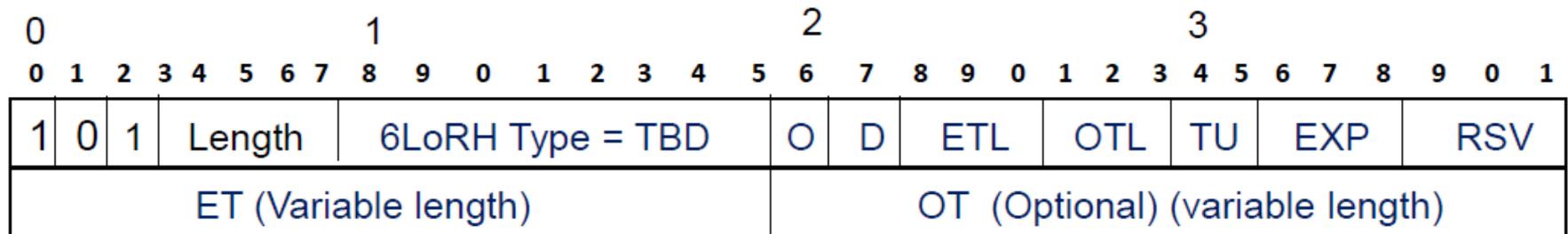
# Motivation and Background

- Delay sensitive industrial M2M IoT applications
- Packet expiration assists in meeting delay constraints in deterministic network
- Positive response from the 6TiSCH ML 😊
- Interest from in-band-oam draft authors to include packet expiration time in IPv6 Header
- Applicability : 6lo, 6tisch, roll, and detnet

## Quick updates

- Inclusion of "Network ASN" as one of the time units as the draft can be seamlessly integrated with 6tisch networks
- Implemented the draft on OpenWSN platform and happy to announce that it has been successfully merged and currently available with the main distribution.

# Deadline-6LoRH Elective Header for Packet Expiration Time



|                          |   |
|--------------------------|---|
| O flag<br>(1 bit)        | Origination Time field<br>1: Origination Time is present<br>0: Origination Time is absent                         |
| D flag<br>(1 bit)        | Drop flag<br>1: Drop<br>0: Ignore and forward   |
| ETL<br>(3 bits<br>[bbb]) | [bbb]+1 = Length of Expiration Time<br>000 : Length of ETL is "1 octet"<br>:<br>111 : Length of ETL is "8 octets" |
| OTL<br>(3 bits<br>[bbb]) | [bbb]+1 = Length of OriginationTime<br>000 : Length of OTL is "1 octet"<br>:<br>111 : Length of OTL is "8 octets" |

|                         |   |
|-------------------------|---|
| TU<br>(2 bits)          | Indicates time units for packet expiration and origination time fields<br>00 : Time in microseconds<br>01 : Time in seconds<br><b>10 : Network ASN</b><br>11 : User Defined |
| EXP<br>(3 bits)         | Multiplication factor (exponent of base 10)   |
| RSV<br>(3 bits)         | Reserved  |
| ET<br>(Variable length) | Expiration Time value<br>(8..64-bit)  |
| OT<br>(Variable length) | Origination Time value (Optional)<br>(8..64-bit)  |

# Way Forward

A scheduling function based on this draft to enable realization of applications with deadlines

## Comments and Questions

Happy to receive your comments on the draft ...

**Thanks !!!**



Thank you!