IETF 102 - Montreal

Chairs:
Pascal Thubert
Thomas Watteyne

Etherpad: https://etherpad.tools.ietf.org/p/notes-ietf-102-6tisch

IPv6 over the TSCH mode of IEEE 802.15.4

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- **By participating in the IETF, you agree to follow IETF processes and policies.**
- **If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.**
- **As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.**
- **Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.**
- **As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.**

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

BCP 9 (Internet Standards Process)

BCP 25 (Working Group processes)

BCP 25 (Anti-Harassment Procedures)

BCP 54 (Code of Conduct)

BCP 78 (Copyright)

BCP 79 (Patents, Participation)

https://www.ietf.org/privacy-policy/ (Privacy Policy)

Reminder:

Minutes are taken *
This meeting is recorded **
Presence is logged ***

* Contribute online to the minutes at: https://etherpad.tools.ietf.org/p/notes-ietf-102-6tisch
** Recordings and Minutes are public and may be subject to discovery in the event of litigation
*** Sign the blue sheets!

Administrivia

- Minutes
  - Etherpad: https://etherpad.tools.ietf.org/p/notes-ietf-102-6tisch
- Remote participation
  - Meetecho: http://www.meetecho.com/ietf102/6tisch
  - Jabber: 6tisch@jabber.ietf.org
- Mailing list
  - 6tisch@ietf.org
  - To subscribe: https://www.ietf.org/mailman/listinfo/6tisch
- Meeting materials:
  - https://datatracker.ietf.org/meeting/102/materials.html/#6tisch
  - One set of slides per presentation

Agenda
[1/2]

```
Intro and Status
    * Note-Well, Blue Sheets, Scribes, Agenda Bashing
    * Status of the work, link with other WGs
    * 6TiSCH Interop event 26-27 of June in Paris                [10min]
      (chairs)

 Chartered items

    * draft-ietf-6tisch-6top-protocol-12                        [5min]
      (Xavi Vilajosana, remote)
      goal:  IESG LC status

    * draft-chang-6tisch-msf-02                                 [10min]
      (Tengfei Chang or Simon Duquennoy)
      goal: prepare for WG adoption

    * draft-ietf-6tisch-minimal-security-06                     [25min]
      (Malisa Vucinic, remote)
      goal: present changes in -06 and discuss WGLC comments

    * draft-ietf-6tisch-dtsecurity-zerotouch-join-02            [10min]
      (Michael Richardson)
      goal: progress status

    * draft-richardson-6tisch-enrollment-enhanced-beacon-00     [10min]
      (Michael Richardson)
      goal: call for adoption
```

Agenda
[2/2]

Unchartered items, time permitting

* draft-vilajosana-6tisch-globaltime-01 [5min]
  (Xavi Vilajosana)
  goal: discuss interaction with minimal security

* draft-munoz-6tisch-multiple-phys [5min]
  (Jonathan Munoz)
  goal: info

* retransmission algorithm IEEE 802.15.4-2015 [5min]
  (Yasuyuki Tanaka>)
  goal: information sharing

* status of the 6lo fragmentation design team (Thomas) [5min]

* AOB [QS]

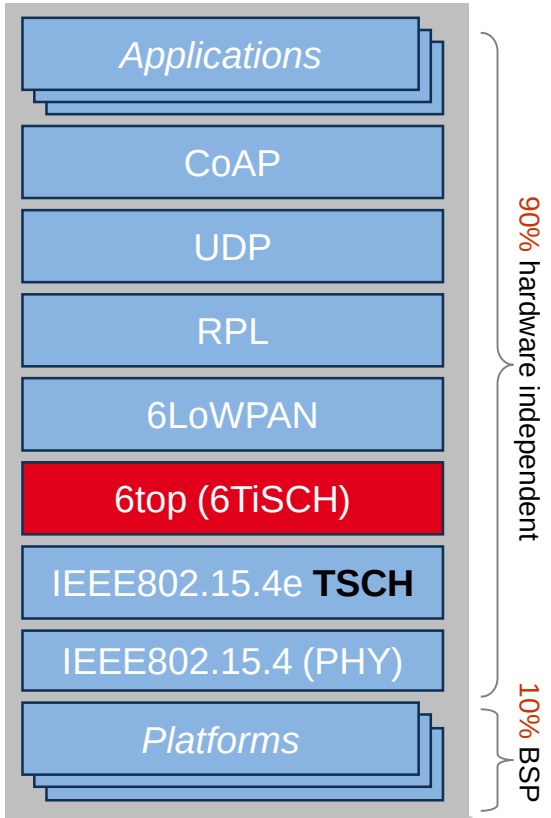
Total scheduled time 90/90min

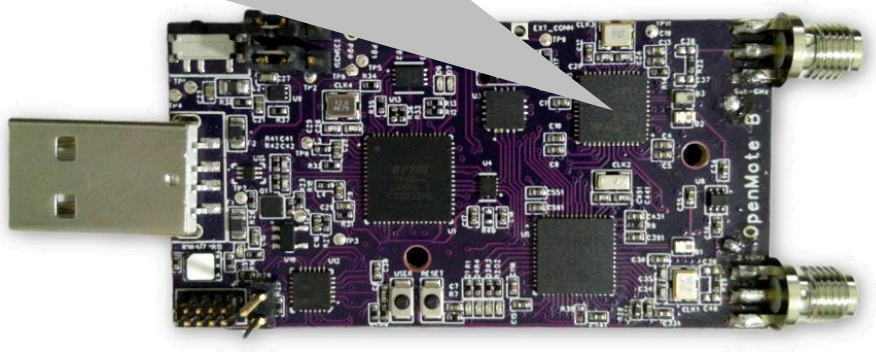
Links with other WGs

- 6lo
  - 6lo fragmentation DT
    - draft-watteyne-6lo-minimal-fragment
    - draft-thubert-6lo-fragment-recovery
  - 6LoWPAN ND
    - draft-ietf-6lo-rfc6775-update,
    - draft-ietf-6lo-ap-nd, draft-ietf-6lo-backbone-router
  - draft-ietf-6lo-deadline-time
    - *6TiSCH-specific ASN used as option for timestamp*
- ROLL
  - draft-ietf-roll-dao-projection
  - draft-thubert-roll-unaware-leaves
  - draft-richardson-6tisch-roll-enrollment-priority
    - *use RPL DIO to propagate configuration for draft-richardson-6tisch-enrollment-enhanced-beacon*
- CoRE
  - liaison issued about draft-ietf-6tisch-minimal-security
    - *defines "Stateless-Proxy CoAP Option"*

OpenWSN – release 1.14.0

- www.openwsn.org
- Open-source implementation of the 6TiSCH protocol stack. Full support of latest drafts:
  - IEEE802.15.4 TSCH (with link-layer security)
  - draft-ietf-6tisch-minimal-security
  - draft-ietf-6tisch-6top-protocol
  - draft-chang-6tisch-msf
- Running on 11 platforms, including the OpenMote B
- Over 60 direct contributors, catalyst for R&D around TSCH networks
- Open-source (BSD license)
- Reference implementation for ETSI 6TiSCH interop events
- Core team: Tengfei Chang, Xavi Vilajosana



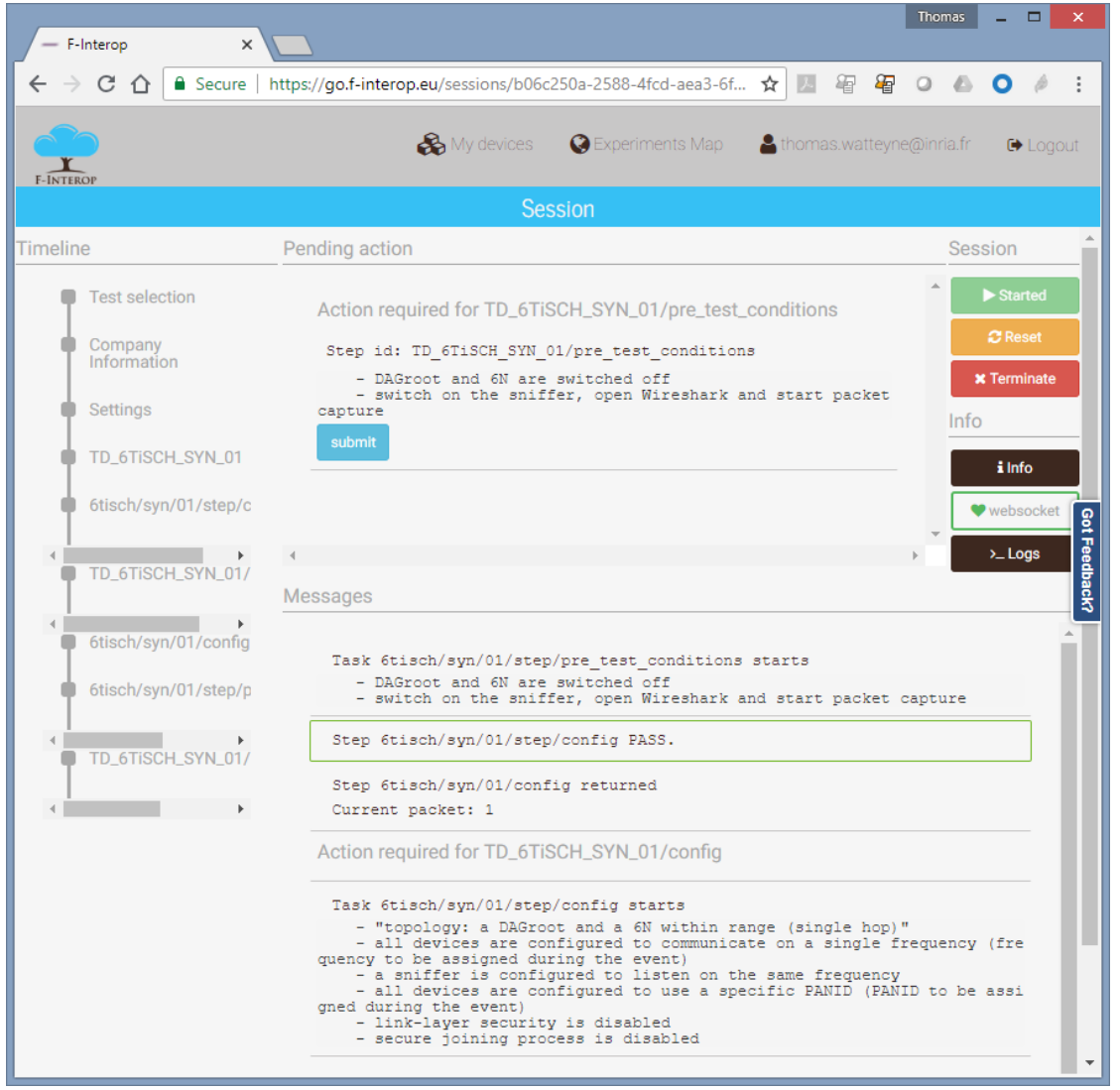


OpenMote B
www.openmote.com

F-Interop – 6TiSCH Test Suite release 1.0.0

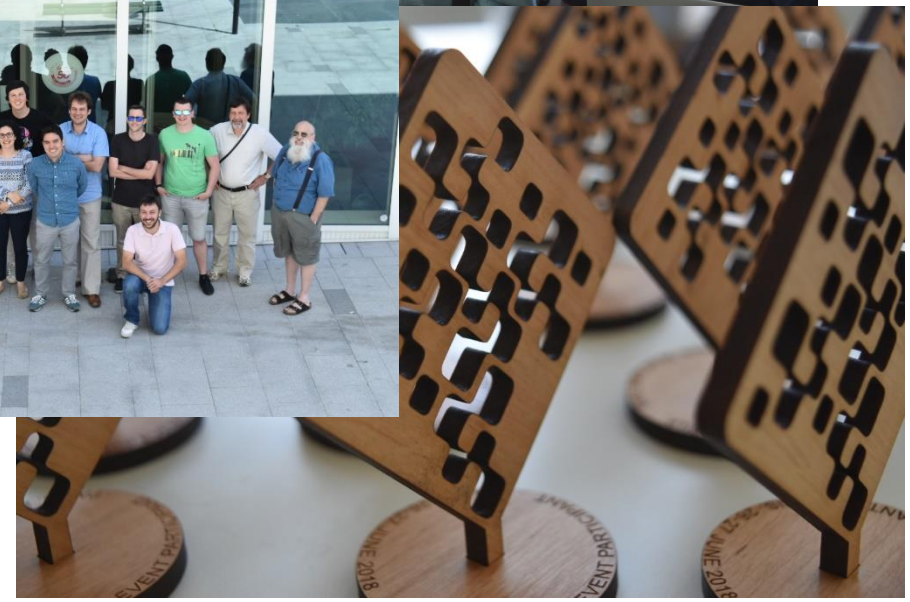
Running conformance and interop tests online.

https://www.f-interop.eu/



2nd F-Interop 6TiSCH Interoperability Event

- 26-27 June 2018, Paris
- Scope
  - RFC8180 (minimal draft)
  - draft-ietf-6tisch-6top-protocol (6P)
  - draft-ietf-6tisch-minimal-security (CoJP)
  - RFC8025 (6LoRH)



	Interoperability		Not Executed		Totals	
	OK	NO	NA	OT	Run	Results
6TiSCH	34 (97.1%)	1 (2.9%)	53 (60.2%)	0 (0.0%)	35 (39.8%)	88
CoAP	38 (88.4%)	5 (11.6%)	45 (51.1%)	0 (0.0%)	43 (48.9%)	88

draft-ietf-6tisch-6top-protocol

Authors: Qin Wang (Ed.)
Xavi Vilajosana
Thomas Watteyne

Status

- Status:
  - Published v12 consolidating responses to LC reviews
    - 20 June 2018
  - IESG Evaluation:: AD Followup
  - Telechat date: Has enough positions to pass.
  - IANA: Version changed – review needed.
- Side note:
  - Implementations exist and evaluated during F-Interop plugtest in June 2018
- Should move on?

Yes

Suresh Krishnan

No Objection

Ignas Bagdonas
Deborah Brungard
Ben Campbell
Alissa Cooper
Spencer Dawkins
Benjamin Kaduk
Warren Kumari
Mirja Kühlewind
Alexey Melnikov
Eric Rescorla
Alvaro Retana
Adam Roach
Martin Vigoureux

draft-chang-6tisch-msf-02

Authors: Malisa, Vucinic
Xavier, Vilajosana
Simon, Duquennoy
Diego, Dujovne
Tengfei, Chang (Ed)

Actions after IETF 101 London

- Merged ASF into MSF (lead by Simon)
- draft-chang-6tisch-msf-02 was published on 2018-07-02 :
  - Draft: https://tools.ietf.org/html/draft-chang-6tisch-msf-02
  - Diff: https://tools.ietf.org/rfcdiff?url2=draft-chang-6tisch-msf-02.txt

Updates on MSF-02

- MSF cells in a nutshell
  - Minimal cell: used for **broadcast** / rendez-vous (EB, DIO)
  - Autonomous cells: one **unicast** cell per neighbor, address is hash of MAC
  - “Dedicated” cells: additional **unicast** cells for parent<->child links

Updates on MSF-02

- Section 3: Autonomous Unicast Cells
  - When to add/remove cells (6P Clear can NOT erase autonomous cells)

    1. One cell to receive, at a [slotOffset,channelOffset] computed as a hash of the node's EUI64 (detailed next). The cell options for this cell are RX=1.
    2. For each neighbor in the IPv6 neighbor table, one cell to transmit, at a [slotOffset,channelOffset] computed as a hash of the neighbor's EUI64 (detailed next). The cell options for this cell are TX=1, SHARED=1.

  - Which cell to choose

```
slotOffset(MAC) = 1 + hash(EUI64) % (length(Slotframe_1) - 1)
channelOffset(MAC) = hash(EUI64) % 16
```

  - Hash collision handling

    1. The TX cell with the most packets in outgoing queue takes precedence.
    2. If all TX cells have empty outgoing queues, the RX cell takes precedence.

Updates on MSF-02

- Section 4: Node Behavior at Boot
  - Setting up autonomous Unicast cells
    - …
    - Step 2 - Receiving EBs
    - Step 3 - Setting up Autonomous Unicast Cells
    - Step 4 - Join Request/Response
    - …
  - No “dedicated” cell to preferred parent at boot
    - Step 5 - 6P ADD to Preferred Parent (**removed**)

Updates on MSF-02

- Section 5.1 : Handling transient traffic bursts
  - IEEE 802.15.4-2015 already defines pending bit behavior
  - Simply refer to it:

> In order to handle transient traffic bursts, MSF uses the [IEEE802154-2015] frame pending bit (page 152, Section 7.2.1.3). By setting the bit, a node can transmit a series of packets to a given neighbor in consecutive time offsets. The next paragraphs define how to handle longer-term fluctuations in traffic, using 6P.

  - Long-term changes in traffic handled with 6P

Issues on MSF-02

- https://github.com/twatteyne/draft-chang-6tisch-msf/issues
  - Terminology: “dedicated”
    - Dedicated means without “shared” OPTION. Name autonomous cell by “installed cell”, “managed cell” or “managed MSF cell”
  - List of packet that go on minimal cell
    - Currently minimal cell can only send EB/DIO, should also include RPL DIS, IPv6 NDP, application broadcast packet
  - Slotframe 0 vs Slotframe 1 length
  - Separating TX and RX counters
  - 6P timeout
    - Calculation depending on the PDR on Tx and Rx cells
    - Increasing Timeout value if previous 6P transaction failed
  - Change “NumCellsPassed” to “NumCellsElapsed”

Summary

- ASF has been merged into MSF
- Issues remaining will be fixed in next version
- Call for adoption
  - draft-ietf-6tisch-msf-00 ?

draft-ietf-6tisch-minimal-security

Authors: Mališa Vučinić (Ed.)
Jonathan Simon
Kris Pister
Michael Richardson

Status

- Published -06
  - Reviews by Xavier Vilajosana, Pascal Thubert
  - Extensive discussions during and after IETF101
- Status:
  - Interoperability of -06 achieved during 6TiSCH plugtest in June
    - OpenWSN and a Contiki-based implementation
  - WGLC over, 7 reviews received:
    - Göran Selander
    - Tero Kivinen
    - Xavier Vilajosana
    - Klaus Hartke
    - Jim Schaad
    - Tengfei Chang
    - William Vignat
- Goal of the presentation
  - Quick summary of updates since -05
  - Discuss WGLC comments

Change #1: Redefined CBOR structures

- Adding flexibility to top-level structs by using maps and registries

```
request_payload = [
    network_identifier : bstr,
]
```

-06

```
Join_Request = {
    ? 1 : uint              ; role
    ? 5 : bstr              ; network identifier
}
```

```
response_payload = [
    COSE_KeySet,
    short_address,
    ? JRC_address : bstr,
]
```

-06

```
Configuration = {
    ? 2 : [ +Link_Layer_Key ],    ; link-layer key set
    ? 3 : Short_Address,          ; link-layer short address
    ? 4 : bstr                    ; JRC address
    ? 5 : bstr                    ; network identifier
    ? 6 : bstr                    ; network prefix
}
```

- Inner structures optimized

```
COSE_Key = {
    1 => tstr / int,          ; kty
    ? 2 => bstr,              ; kid
    ? 3 => tstr / int,        ; alg
    ? 4 => [+ (tstr / int) ], ; key_ops
    ? 5 => bstr,              ; Base IV
    * label => values
}
```

-06

```
Link_Layer_Key = (
    key_index           : uint,
    ? key_usage         : uint / nint,
    key_value           : bstr,
)
```

e.g. K2 key from RFC8180

Change #2: Support for “6LBR pledge”

- Generalized Constrained Join Protocol to support the joining of 6LBR pledge
- New **role** parameter added to Join_Request
  - defaults to “non-6LBR pledge”
- For some parameters, different processing depending on the “role” the pledge is playing (6LBR vs non-6LBR)
- Terminology in the document:
  - “pledge” : non-6LBR pledge
  - “6LBR pledge”
  - “(6LBR) pledge”

Change #3: Rekeying and parameter update mechanism

- Once pledge completes the join, becomes a CoAP *server,* exposing */j*
- JRC can at any time send a Parameter Update Request message to implicitly derived node's global IP address
  - Payload of the request is a **Configuration** object with updated parameters, e.g. new key
- Mechanism used to implement rekeying
  - Node (ex pledge) receives a Configuration object
    - Installs the new key, keeps using the old key until it sees traffic encrypted with the new key
  - 6LBR (ex 6LBR pledge) receives a Configuration object
    - Installs the new key, immediately removes old keys, starts using the new key
- Mechanism used to update short addresses or any other parameter

Change #4: Misc

- Many editorial edits, clarifications
- Aligned the key derivation with OSCORE-13
- Defined IANA registries
  - CoJP Parameters: for CBOR labels
  - CoJP Key Usage: Values of key_usage parameter, e.g. K1 from RFC8180
- Cannot settle on the name:
  - Renamed “6TiSCH Join Protocol” to “Constrained Join Protocol”
  - Current abbreviation CoJP: cojeep

WGLC comments 1/10

What to do with Stateless-Proxy?

Göran Selander:

> Would it be possible/desirable to use the Token instead of this new option (Stateless-Proxy)? The allowed size of Tokens would need to be enlarged but besides that, are there any other limitations? The Tokens would be unique by construction and the overhead would be reduced.

Klaus Hartke:

> Not only are there are now two tokens in a message, which doesn't help with keeping the protocol (CoAP) simple and easy to understand; the new token is also not even always echoed back.

- CoAP Token has the same processing semantics as Stateless-Proxy
- It **is** possible to use existing 8-byte Token to carry Stateless-Proxy info in **some** cases, not in all
  - e.g. non default port numbers, multiple net interfaces

Proposed Resolution: Working together with CoRE on the best way forward. Presenting the option during CORE WG meeting on Thursday. Will keep WG posted with updates.

WGLC comments 2/10

Is the join process ongoing?

Tero Kivinen:

> In section 6 there is text saying:
>
> > *How the JP learns whether the join process is ongoing is out of scope of this specification.*
>
> This is very important part of the process, and I think it should be part of this document, and not out of scope for this document. Which document will specify this if not this?

- JP accepts unsecured frames at L2 for the duration of the join process
- Issue has been discussed extensively during IETF99 in Prague
- Conclusion: define extended version of join metric, present in EBs
  - draft-richardson-6tisch-enrollment-enhanced-beacon-01
  - currently called “proxy prio” (?)
  - *should* allow the diffusion by means of EB whether join process is ongoing (e.g. upon a button press on the 6LBR)

Option 1) Keep working on draft-richardson-6tisch-enrollment-enhanced-beacon
Option 2) (Ab)use one value of the Join Metric for a simple solution
Option 3) JRC sends a control message to each JP as part of Parameter Update Request

WGLC comments 3/10

L2 state at JP to accept unsecured frames from the pledge

Tero Kivinen (rephrased):

> Actually if you follow the 802.15.4 (security processing) and someone sends you unsecured frame, the security processing will reject it, upper layer is then supposed to add an entry in the table with *secExempt* set, so that the next transmission from the same node passes (if join process is ongoing). This means JP is not fully stateless, as claimed.

- JP -> Pledge communication: **OK**
  - Upon reception of Stateless-Proxy, JP adds an entry in the L2 table for pledge, removes it once it receives an L2 ack
  - Every packet from JRC to the pledge needs to have Stateless-Proxy option set (JP enforces this when forwarding)
- Pledge -> JP communication. Performance issue: Fully compliant 802.15.4 security processing:
  - JP rejects first transmission from Pledge, does **not** ACK it at L2
  - JP adds an entry in the table allowing the pledge's address to be exempt from security processing
  - L2 retransmission from the pledge now passes
  - JP removes this entry **once** it forwards the request to the JRC using Stateless-Proxy
  - JP needs to expire this entry after a configurable timeout in case of an attack, malformed request, etc

Many existing implementations of 802.15.4 security processing (Contiki, OpenWSN, Contiki-NG, RIOT) are able to pass the first Pledge->JP frame to upper layer of JP without rejecting it. No performance hit in practice.

Proposed Resolution: Continue ML discussions.

WGLC comments 4/10

When rekeying, add delay before removing old keys

Tero Kivinen:

> *Upon reception and successful security processing of a link-layer frame secured with a key from the new key set, a non-6LBR node MUST remove any old keys it has installed from the previous key set.*

I think it would be better to wait for a while before deleting the old set, but immediately move to use the new set for transmissions. I.e., we might have node B and C, which both have old and new keys, their parent A sends an EB with new keys out, but node C is not able to receive it correctly. Now if C wants to send frame to A or B, it will still be using old key as it has not yet seen any new frames. Both A and B will throw that frame out as it is using old key.
If this would be changed to say that "node MUST remove any old keys after delay of N seconds" (or delay of N slotframes or whatever).

Proposed Resolution: Add configurable delay before removing the key at non-6LBR nodes

WGLC comments 5/10

Error handling at the CBOR level of CoJP

Xavi Vilajosana:

> I miss some section describing how errors are handled at the cbor level. This is what if the received Configuration option is wrong, e.g there is an element in the map with an unsupported value.

- Error handling currently defined for OSCORE-related errors
  - Silent ignore to reduce DoS space
- Missing error handling on CoJP parameter *semantics*
  - e.g. unsupported parameter included in the Join_Request object, unexpected combination of values,…

Proposed Resolution: Add **error** CBOR parameter that can be returned in the Join Response or Parameter Update Response message with value explaining the error nature. Error goes over the secure channel.

Should we define specific error codes for potential cases in order to be able to act on the error programmatically?

WGLC comments 6/10

Handling of Parameter Update transmission failures

Xavi Vilajosana:

> The JRC is the origin of Parameter Update Requests which may contain for example rekeying material or a new short address. The draft needs to describe what happens if the destination 6N is not reachable.
> I understand that there will be a timeout and possibly will retry later or do not try anymore (this has to be stated).
> What if the node is no more in the network? when the JRC will stop sending the short address updates? When it will remove that node from its "database"?

- Parameter Update Request is a CoAP **CON**firmable message
  - Handling in case transmission fails does not seem to impact interoperability and seems more like a policy
  - Working group input?
- Could impact security in case of short-address (re)assignment
  - See comment from Tero Kivinen

Proposed Resolution: Explicit that this is an implementation decision. Extend short_address assignment text mandating uniqueness as per Tero's email.

WGLC comments 7/10

Nonce re-use when JRC2 takes over from JRC1

(and pledge is not re-provisioned with a new PSK)

Jim Schaad:

1. A pledge completes a join operation with JRC1.
2. JRC1 performs a number of parameter updates.
3. JRC1 disappears for some reason leaving no traces behind.
4. The pledge is then told to do a second join and it attaches to JRC2. → assumption of 6LBR going down with the JRC
5. JRC2 performs a parameter update. Since JRC2 does not know how many messages were sent from JRC1, **it does not know what to set the partial IV to and thus would reuse IV values.**

1. Use case corresponds to the change of ownership of the pledge without re-provisioning the pledge with a new PSK
2. JRC of company A goes “boom”, the same company deploys a new JRC

- Do we want to solve these use cases? First, second or both?

Proposed Resolution:

Use case (1) can be solved by mandating that JRC1 transfers partial IV values to JRC2 out of band

In (2), partial IV information is no longer available. Force everyone to rejoin, but how if JRC is in the Cloud?

WGLC comments 8/10

New CoJP parameters to fully bootstrap 6LBR

Tengfei Chang:

Table 2 listed the parameters in the configuration object. It's generally for non-6LBR pledge.
I made a pre-list for those parameters that are required by 6LBR pledge. They are from the information that EB should carry.

- time slot template
- channel hopping template
- number of slotframes
  - slotframe handler
    - slotframe length
    - number of links
    - link information (slotoffset, channeloffset, type)

anything else?

- Will enable full bootstrapping of the 6LBR using CoJP
- Disadvantage is spec readability: none of these parameters are relevant to non-6LBR pledges

Proposed Resolution: Add the new parameters in the draft but define **separate** CBOR structures that are sent to non-6LBR and 6LBR pledges. Allows developers to focus on the objects they care about.

WGLC comments 9/10

Message overhead optimizations

Extensive review and ensuing discussion with William Vignat at:
https://bitbucket.org/6tisch/draft-ietf-6tisch-minimal-security/issues/19/concerns-about-the-cojp-message-size-the

Optimization #1:

- In Join Requests, EUI-64 of the pledge is present twice: as OSCORE kid context, within Stateless-Proxy option.
- **Proposed Resolution:** Imply OSCORE kid context values from the value of Stateless-Proxy option at JRC. Saves 8 bytes.

Optimization #2:

- Short Address lease time is encoded in **seconds** from the instant the CoJP message was received
- **Proposed Resolution:** Round to minutes, hours or days? Working group input?

WGLC comments 10/10

Fragmentation and support for BLOCKWISE

William Vignat:

> The BLOCK-WISE (CoAP) option is being devised just for this, however it is not really meant to be used with non-confirmable messages for obvious reasons such as packet loss...
> I understand the reasoning behind making the request a NON-confirmable message to reduce the strain on the JP and the potential DoS, however maybe the answer(i mean the CoJP response) should at least be a CONfirmable message so that it can easily be fragmented using BLOCK-WISE ?

- With default CoJP values, no need for fragmentation with IEEE802.15.4 frames using 4-byte MICs
- In case of fully-blown CoJP messages and parameters, less optimal stack config, fragmentation can occur
  - JRC in the cloud
  - short address lease times, multiple L2 keys, etc
- **Implicit assumption on fragmentation being done at 6LoWPAN layer**

Proposed Resolution:
Is there interest in supporting fragmentation using BLOCKWISE? This would enable CoJP to be used in non-IP networks, but would complicate the current design where CoAP messages are NON confirmable for DoS reasons

Next steps

- Publish -07 implementing the issues raised
- Ship

Zero-touch join

Metrics and Values

draft-ietf-6tisch-dtsecurity-zerotouch-join

On behalf of
Michael Richardson
mcr+ietf@sandelman.ca

ANIMA

Notes

The BRSKI draft passed WGLC

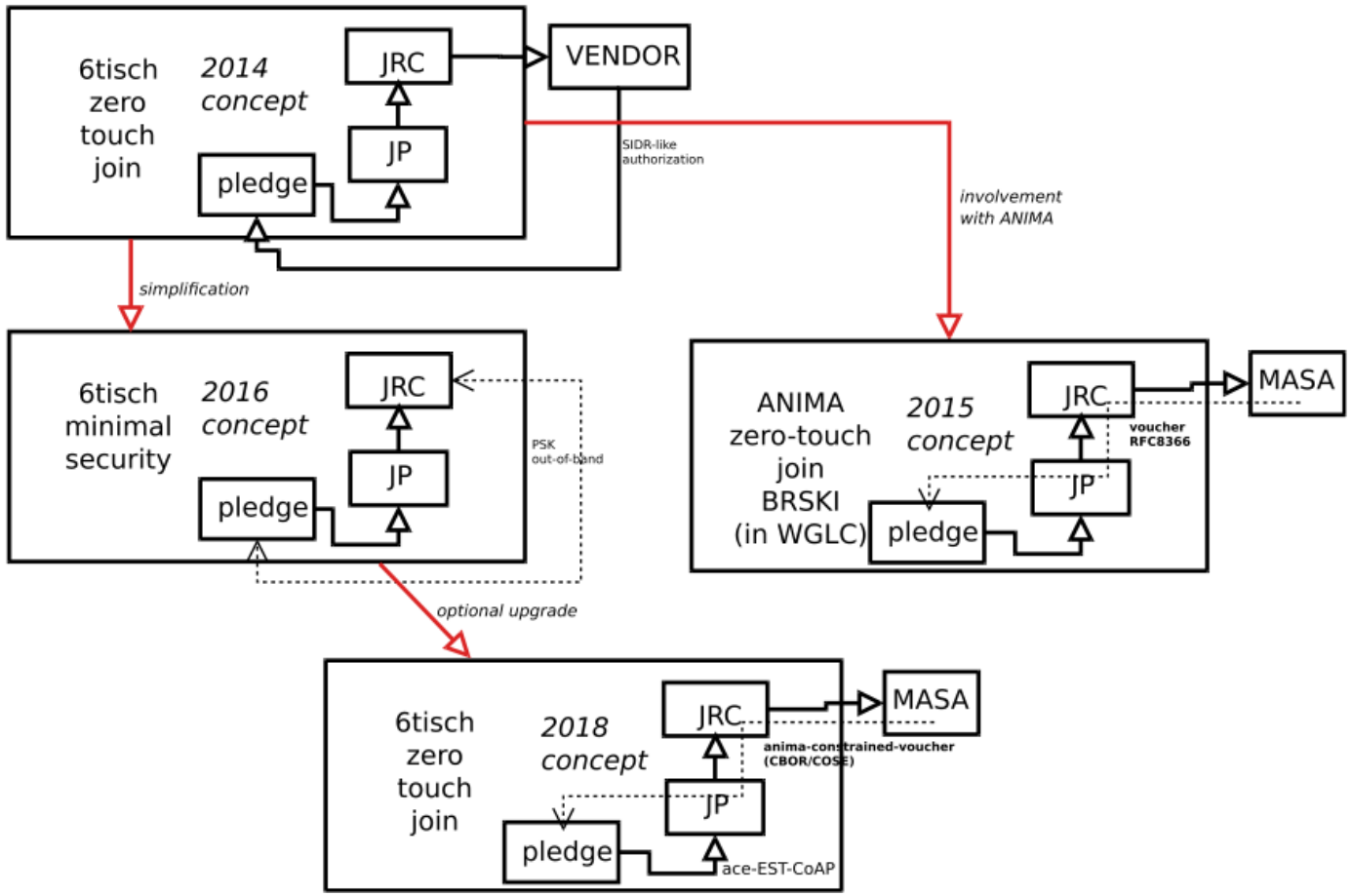
The constrained voucher document was adopted.

Hope WGLC by October 2018 on this document.

ietf-6tisch-dtsecurity-zerotouch-join

- Status
  - -02 published on April 30
  - Lost co-author.
- Many components broken out of this document:
  - Voucher Artifact is now RFC8366.
    - Constrained version is ietf-anima-constrained-voucher
  - Enrollment protocol is ietf-anima-bootstrapping-keyinfra-15 (“BRSKI”), WGLC ended June 14
    - Constrained version of EST is ietf-ace-est-coaps
  - Remaining constrained version of BRSKI in this document.
- Next steps
  - Today’s state: “WG Document”
  - Needs a co-author! **“Your name here”**
  - Requires draft-richardson-6tisch-enhanced-beacon.

6tisch constrained bootstrap evolution



Enhanced Beacon

Metrics and Values

draft-richardson-6tisch-enrollment-enhanced-beacon

On behalf of
Michael Richardson
mcr+ietf@sandelman.ca

What's the problem?
Network Selection

- A (new!) device (pledge!) will not know which network it should enroll in.
- A single network will be visible multiple times.

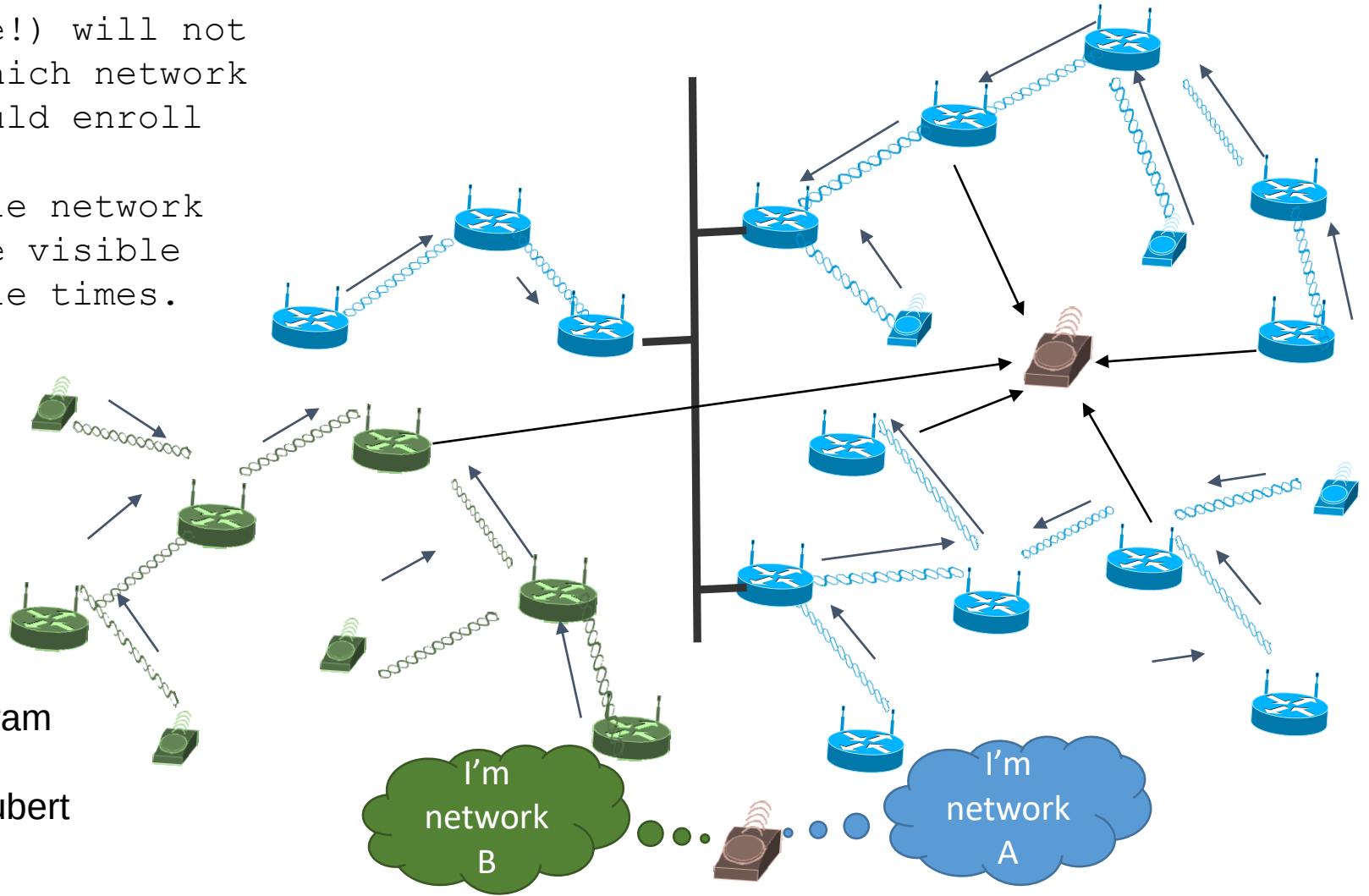


Diagram By P.Thubert

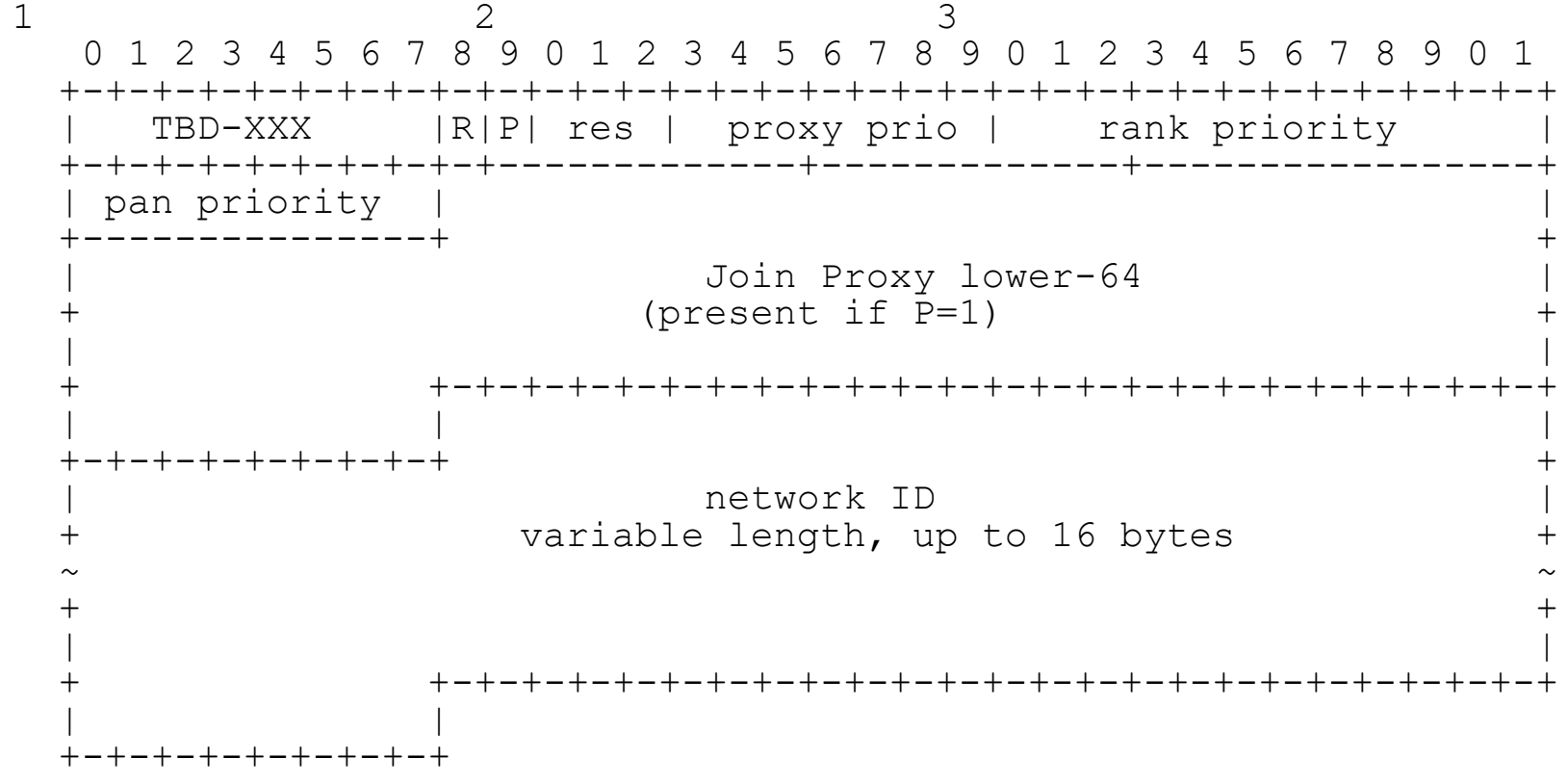
What do I mean by “JOIN”?

- Some confusion about JOINing an LLN → means getting the network keys/credentials
  - Calling this:
    - ENROLLMENT
- Vs JOINing a DODAG → which means selecting a Parent and sending a DAO to it.
  - Parent Selection

What's the 6tisch part?

[RFC8137] creates a registry for new IETF IE subtypes. This document allocates a new subtype TBD-XXX.

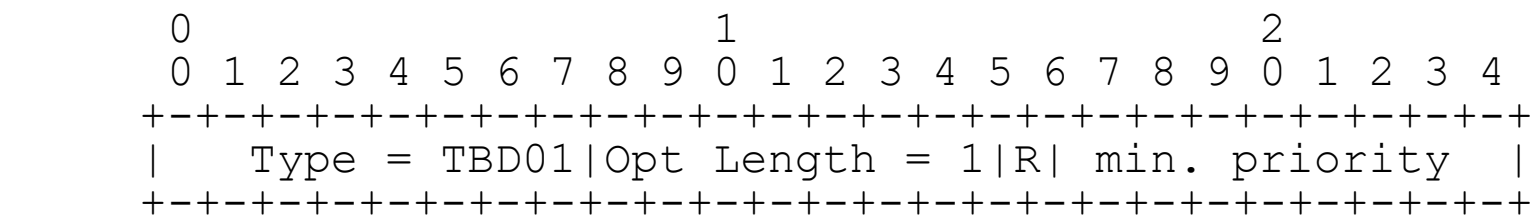
This document documents a new IE subtype structure is as follows. As explained in [RFC8137] the length of the Sub-Type Content can be calculated from the container, so no length information is necessary.



What's the ROLL part?

Enabling secure network join in RPL networks

draft-richardson-6tisch-roll-enrollment-priority defines a new DIO Option.



min.priority a 7 bit field which provides a base value for the Enhanced Beacon Join priority. A value of 0x7f (127) disables the Join Proxy function entirely.

R a reserved bit that SHOULD be set to 0 by senders, and MUST be ignored by receivers. The reserved bit SHOULD be copied to options created.

The Minimum Priority influences the Proxy Priority that is announced in the Enhanced Beacon. The local node will apply additional criteria (such as number of neighbor cache entries it can allocate for untrusted nodes).

What's the problem?

- There is some desire to base which network to ENROLL on, based upon the **Parent Selection** Criteria.
  - (RPL) DIOs can not be seen until node joins network, as they are encrypted.
  - Untrusted nodes can only see Enhanced Beacons.
- A long sleeping node needs the (signed) Enhanced Beacons in order to resynchronize. Such nodes will have ALREADY enrolled, so in fact, having the **Parent Selection** info in the Beacon is a great saving.

Goals in 6tisch

- Decide what set of things we want in the Enhanced Beacon.
  - Write this down somewhere, and ask ROLL to document how those numbers are derived, creating any new metrics or configuration containers needed.
- Document the security risk of exposure of these values.

Called for adoption on June 15th
Confirming now…

Goals in ROLL

- Determine how the newly exposed metrics interact with or are derived from DIO things.
  - A value in an enhanced beacon vs a value in a subsequent DIO.
- There are two additional things related to Enrollment Priority and also the Parent Selection:
  - Number of children
    - Multiple drafts about balancing children
      - Children require (priviledged) neighbour cache entries.
      - Enrollment requires unpriviledged neighbor cache entries
  - Availability of bandwidth for Enrollment
    - Turn off enrollment when there are issues.

Questions/Discussion

- ?

draft-vilajosana-6tisch-globaltime

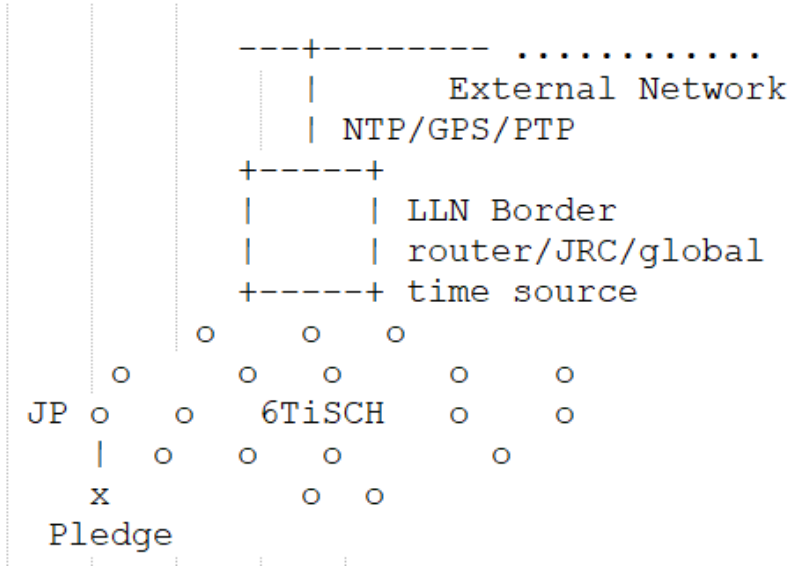
Authors: Xavier Vilajosana
Pere Tuset
Borja Martinez
Jonathan Muñoz

Status

- Updated draft to v01
- Published: 19th of June 2018
- Addressed comments received at ML to produce v1.
- Adjusted to new format of CoJP Join Request/Response using dictionaries.
  - Global time service is co-located with JRC.
    - No other options are possible now. Eliminates security issues.
    - Removed the gt_address from the option

Discussion

- Definition of the interaction model.
  - If the Global Time is served by the JRC. The JRC must know (map) ASN and Global time.
    - Is this in the scope of this draft? If so how?
  - Use of CoJP Parameter Update functionality to update global time lease or leap_second.
    - Reverse model initiated by the JRC instead of initiated by the 6N.
      - Analogous to short address refresh.
    - The \gt service then should be exposed by the 6N



Thanks!

Xavier Vilajosana

xvilajosana@uoc.edu

Problem Statement for Generalizing 6TiSCH to Multiple PHYs

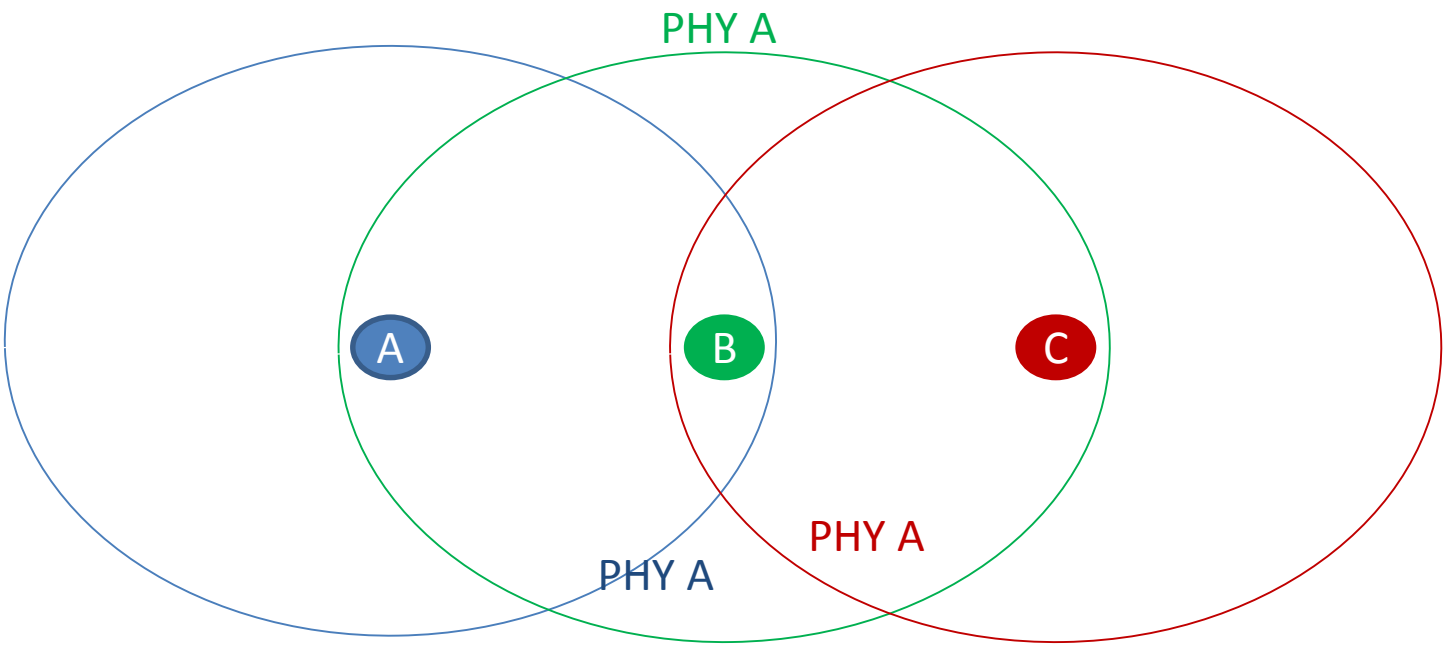
Jonathan Munoz
Tengfei Chang
Xavier Vilajosana

ToC

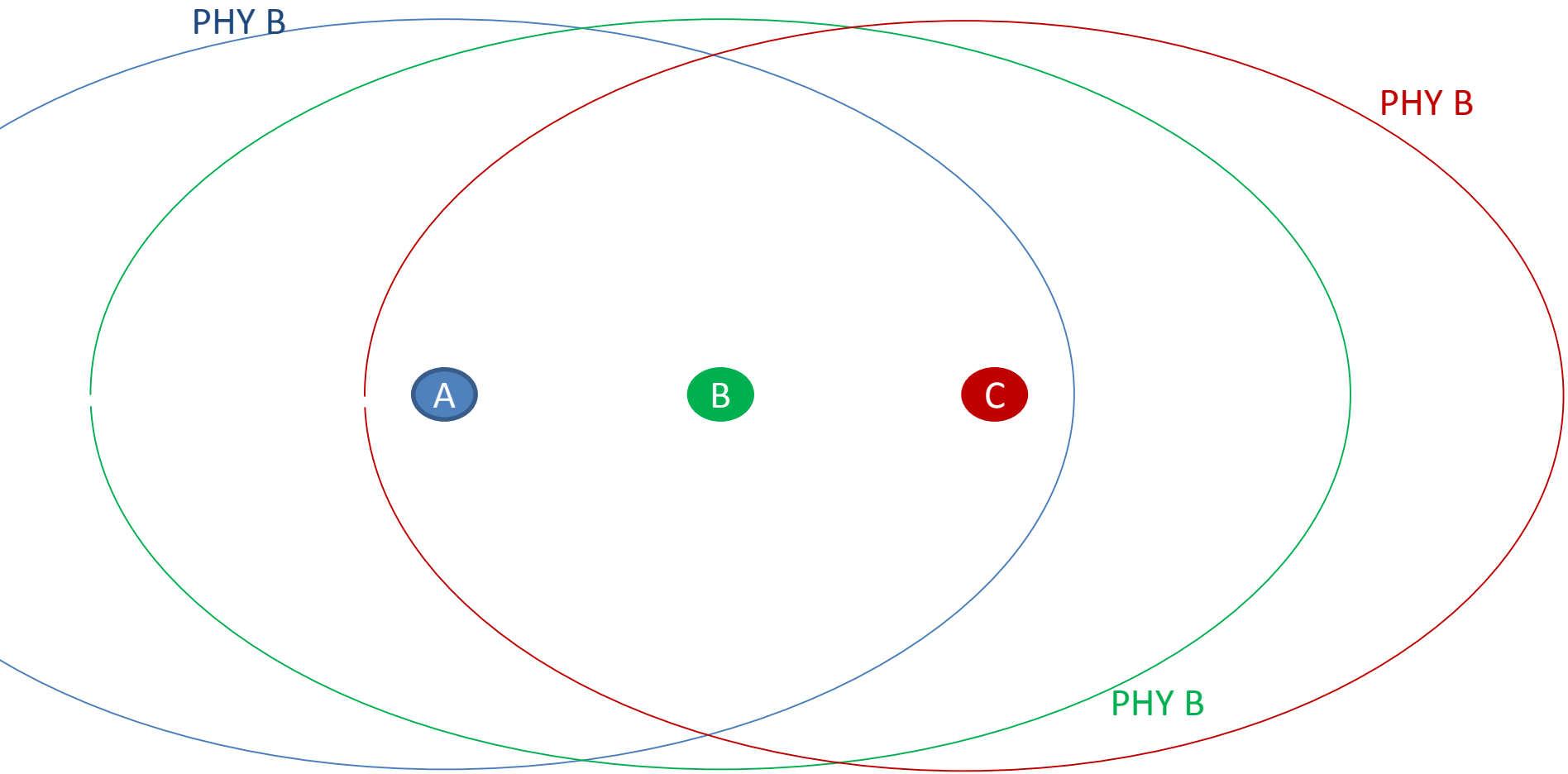
Context: 6TiSCH Protocol Stack

- 6TiSCH protocol stack sits on one PHY (*de facto* IEEE802.15.4-2006 O-QPSK, 250 kbps, 127 B).
- Amendments to the IEEE802.15.4 standard include more PHYs, with different size and data rates (6.25 kbps – 800 kbps, 2047 B).
- New radio chips implementing those PHYs are available.
- Possibility of having a 6TiSCH network over different PHYs.

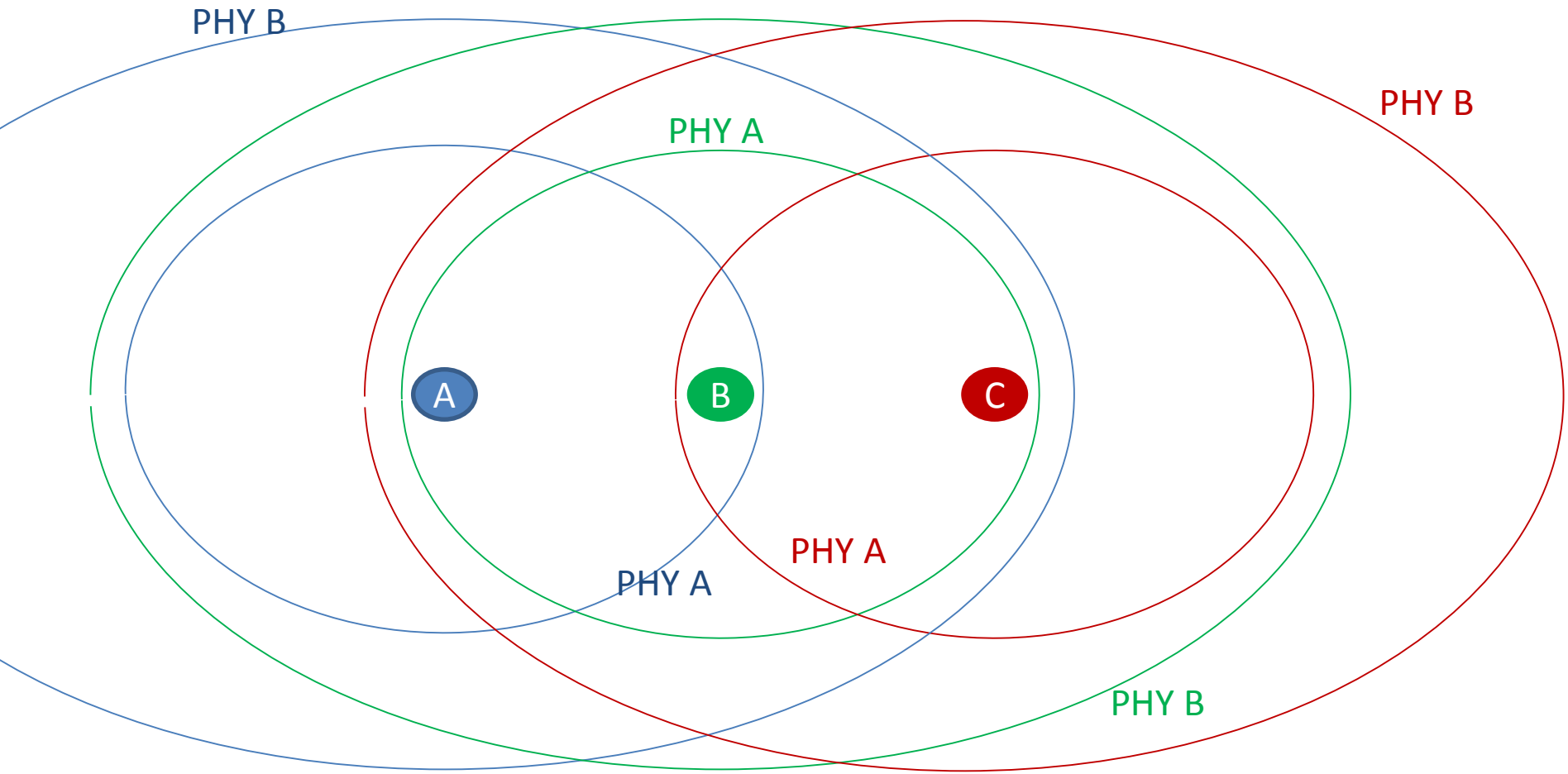
Neighbour Considerations



Neighbour Considerations



Neighbour Considerations



MAC Sub-Layer

- Network Formation

  A node to get synch'ed must listen for a EB

  – With one PHY (802.15.4 O-QPSK): round robin of 16 frequencies.
  – Multiple PHY: round robin of all frequencies of all PHYs implemented.

- Discovering neighbour nodes capabilities:
  – N.A. on networks using one PHY
  – For multiple PHYs:
    - Unicast solicitation
    - Listening for EBs

MAC Sub-Layer

- TSCH Configuration
  - Timeslot duration
  - Channelization over multiple PHYs: channels have different characteristics on each PHY.

6top Sub-Layer

- Resource Allocation
  - Measured in amount of cells allocated/slotframe. Depending on the PHY used, more of less data can fit in a timeslot.

- Duty cycle regulations
  - Frequency bands are subjected to comply with regional regulatory norms.

- 6LoWPAN Considerations
  - Designed with IEEE802.15.4 O-QPSK in mind.
  - In multi PHY environment, must consider fragments of more than 127 B.

- RPL Considerations
  - Rank of the nodes must consider more than one PHY.
  - New OFs, taking into account resource occupancy, different throughput and energy consumption of each PHY.

Retransmission Algorithm in IEEE 802.15.4-2015

6TiSCH WG, IETF 102

Yasuyuki Tanaka

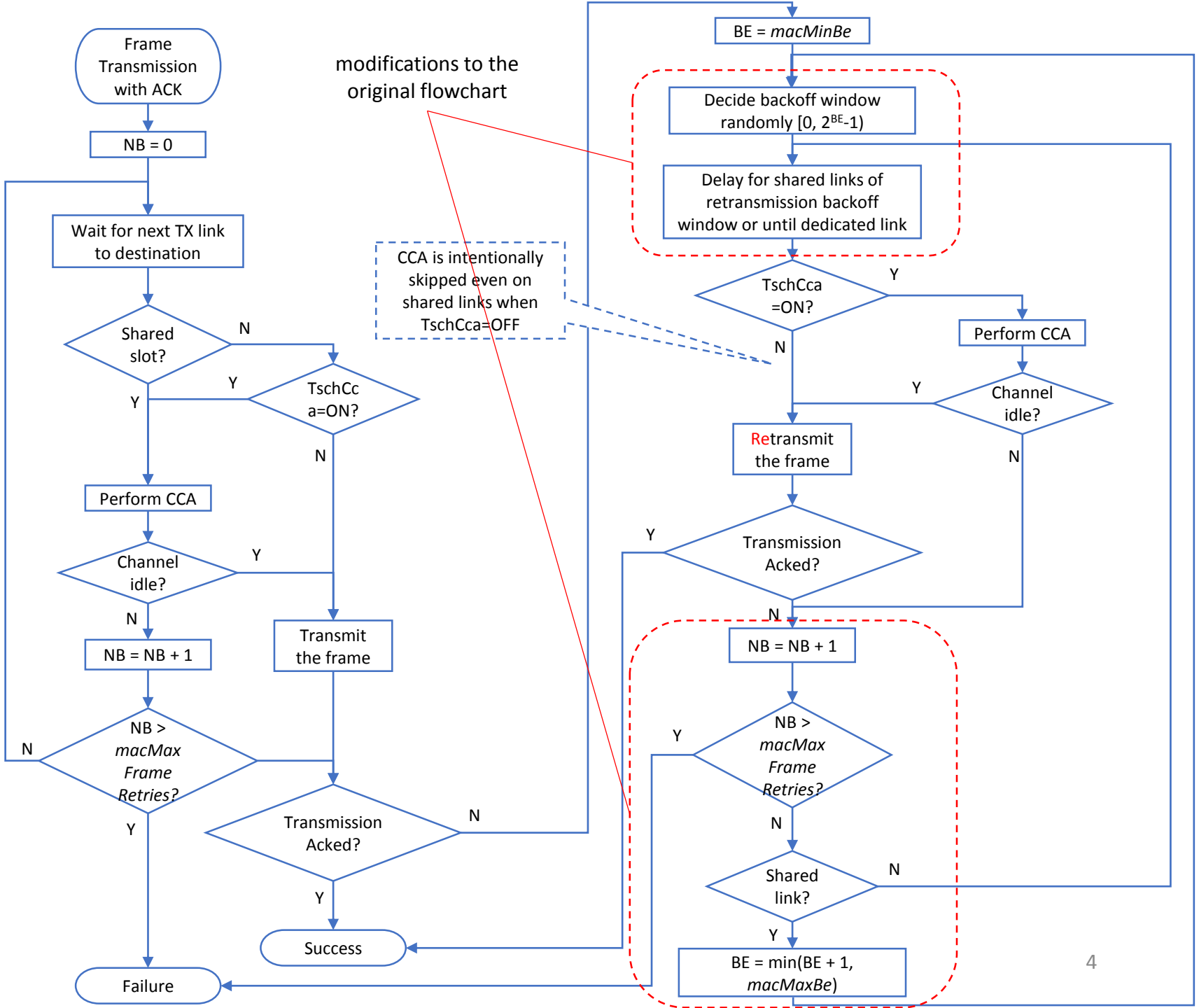
Preface

- This presentation gives some hints which could help you understand better TSCH CSMA-CA retransmission algorithm described in IEEE 802.15.4-2015
- See the email thread for the past discussions
  - “Questions on TSCH CSMA-CA retransmission algorithm in IEEE 802.15.4-2015”
  - https://mailarchive.ietf.org/arch/msg/6tisch/3ODRFDW8QqALyeL0HC3zX5Tjr7Y
- IEEE 802.15.4md is working on revising IEEE Standard 802.15.4
  - The future revision of IEEE 802.15.4 may have clearer descriptions on the algorithm ;-)
  - Thank Tero for this information!

keys for correct understandings

- Look at Figure 6-5 (CSMA-CA algorithm) carefully as well as Figure 6-6 (TSCH Retransmission backoff algorithm)
  - Why? they are closely related
    - For instance, *NB* used in Figure 6-6 is initialized in Figure 6-5
    - The rightmost branch in Figure 6-6 is dead part, which is covered by Figure 6-5
  - Erratum in Figure 6-6
    - "BE = min(BE-1, macMinBe)" should be
    - "BE = min(BE+1, macMaxBe)"
- You can ignore sentences in page-64 which tell conditions to reset the "backoff window"
  - These conditions are redundant as per Figure 6-6 and the text in Page-66.
  - The backoff windows is reset every time the retransmission algorithm starts, anyway.

A complete flowcahrt of TSCH Transmission for unicast frames without PCA



6lo Fragmentation DT

Thomas Watteyne (Chair)
Carsten Bormann
Rahul Jadhav
Gorry Fairhurst
Pascal Thubert
Gabriel Montenegro

6lo Fragmentation DT

- IETF101:
  - Problem Statement & Goal presented
- IETF102: 3 drafts
  1. draft-ietf-lwig-6lowpan-virtual-reassembly *(adopted)*
  2. draft-watteyne-6lo-minimal-fragment
  3. draft-thubert-6lo-fragment-recovery
- Goal:
  - Call for 6lo WG adoption of drafts 2 and 3
  - Close 6lo fragmentation DT