03 March 2017 Webex

IPv6 over the TSCH
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 [2min]
  - Agenda bashing
  - Approval minutes from last meeting
- Status of drafts (chairs) [5min]
- Update on security (Michael) [10min]
- Update on 6P (Xavi) [10min]
- Preparation for IETF 98 (Pascal) [25min]
- AOB [3min]

Draft status

draft-ietf-6tisch-minimal-21

OPSDIR Last Call Review (of -20): Ready

SECDIR Telechat Review (of -19): Has Issues

GENART Telechat Review (of -19): Ready

SECDIR Last Call Review (of -17): Serious Issues

GENART Last Call Review (of -17): Almost Ready

INTDIR Early Review (of -15): Ready with Nits

INTDIR Early Review (of -13): Ready

Update on security
Design team meetings

Meetings occurred:
2017-01-17, 2017-01-31, 2017-02-14,
2017-02-21 (extra), 2017-02-28.
next: 2017-03-14
Typically present:
Michael Richardson, Tero Kivinen, Pascal Thubert,
Thomas Watteyne, Mališa Vučinić, Göran Selander, Toerless Eckert, Peter van der Stok

Recent minutes so far: https://www.ietf.org/mail-archive/web/6tisch-security/current/msg00661.html

draft-ietf-6tisch-minimal-security

- This is the one-touch version
  - Rekey provisions removed from this to make it as minimal as possible.
  - Tracking updates from OSCOAP and EDHOC.
  - Some complications to proxy mechanism as a result of changes in EDHOC relating to SIGMA-I.
    - Considering to add a 6TiSCH-specific CoAP option for stateless proxying
    - Discussions on Core list with Klaus Hartke
  - Considering to add passive flow in the asymmetric key mode triggered by a CoAP message
  - General rewriting of the text to make it more explicit

draft-ietf-6tisch-dtsecurity-secure-join

- This is the zero-touch version
  - Removing text from this document to move it to minimal-security as appropriate.
  - Considering abandonning fully passive mode for hybrid
    - Pledge uses minimal EDHOC process to build secure relationship.
    - JRC drives enrollment, providing certificate via CoMI interface
    - Still some wiggle room as to whether ownership voucher is transfered during EDHOC process vs occurs in CoMI interface

draft-richardson-6tisch-minimal-rekey

- Moved rekey from minimal to new document.
  - Provides for CoMI managed access to keys.
  - Rekey is managed by slow process of JRC reaching out to all nodes and writing new keys.
    - Provision of new keys includes timeout on old key, after switch-over.
  - Nodes accept traffic from old keys and new keys, uses old keys for transmission until use of new key is seen.
    - Switch over from old to new keys triggers expiration of old keys based upon timers.
- Short addresses are also managed in this interface, short addresses timeout based upon ASN.
  - JRC can garbage collect short-addresses by initiate rekey.
- SEEKING WG adoption and co-authors.

draft-richardson-6tisch-join-enhanced-beacon

- Need for definition of extension to enhanced-beacon made clear by join process.
    - Uses IANA registry created by draft-kivinen-802-15-ie
- Includes some bits to help hosts (aka non-RPL leaf nodes) to find correct network, and give hint about using unicast Router Solitications.
- Network ID is based upon SHA256 of DODAGID to identify network.
- Notes that EB is not encrypted, so inappropriate to put much information in.
- Has bit to indicate if sender is available as a Join Proxy; L3 address is implied by SLAAC configuation of Link-Local address from EUI-64 of sender.

SEEKING WG adoption and co-authors.

Update on 6P

NumCells in DELETE request

```
4.2.9.  6P DELETE Request Format

                          1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |Version| T | R |      Code     |      SFID     | SeqNum|  GEN  |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |          Metadata             |  CellOptions  |   NumCells    |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | CellList ...
     +-+-+-+-+-+-+-+-+-

   [...]

   NumCells:  The number of cells from the specified CellList the sender
         wants to delete from the schedule of both sender and receiver.
   CellList:  A list of 0, 1 or multiple 6P Cells.  The CellList is an
         opaque set of bytes, sent unmodified to the SF.  The
         RECOMMENDED format of each 6P Cell is defined in Section 4.2.7.
         The SF MAY redefine the format of the CellList field.
```

Should be say that NumCells MUST be equal to the number of cells in the CellList?
Or just remove the NumCells field?

Reordering

```
4.2.  Message Format  . . . . . . . . . . . . .
  4.2.1.  6top Information Element  . . . . . .
  4.2.2.  General Message Format  . . . . . . .
  4.2.3.  6P Message Types  . . . . . . . . . .
  4.2.4.  6P Command Identifiers  . . . . . . .
  4.2.5.  6P Return Codes . . . . . . . . . . .
  4.2.6.  6P CellOptions  . . . . . . . . . . .
  4.2.7.  6P Cell Format  . . . . . . . . . . .
  4.2.8.  6P ADD Request Format . . . . . . . .
  4.2.9.  6P DELETE Request Format  . . . . . .
  4.2.10. 6P STATUS Request Format  . . . . . .
  4.2.11. 6P LIST Request Format  . . . . . . .
  4.2.12. 6P CLEAR Request Format . . . . . . .
  4.2.13. 6P RELOCATE Request Format  . . . . .
  4.2.14. 6P Response Format  . . . . . . . . .
  4.2.15. 6P Confirmation Format  . . . . . . .
4.3.  Protocol Behavior . . . . . . . . . . . .
  4.3.1.  Version Checking  . . . . . . . . . .
  4.3.2.  SFID Checking . . . . . . . . . . . .
  4.3.3.  Concurrent 6P Transactions  . . . . .
  4.3.4.  Timeout . . . . . . . . . . . . . . .
  4.3.5.  SeqNum Mismatch . . . . . . . . . . .
  4.3.6.  Clearing the Schedule . . . . . . . .
  4.3.7.  Adding Cells with 2-step Transaction
  4.3.8.  Aborting a 6P Transaction . . . . . .
  4.3.9.  Deleting Cells  . . . . . . . . . . .
  4.3.10. Listing Cells . . . . . . . . . . . .
  4.3.11. Cell Relocation . . . . . . . . . . .
  4.3.12. Cell Suggestion . . . . . . . . . . .
  4.3.13. Generation Management . . . . . . . .
  4.3.14. Handling error responses  . . . . . .
```

```
4.2.  Message Format  . . . . . . . . . . . . . . . . . . . . .
  4.2.1.  6top Information Element  . . . . . . . . . . . . . .
  4.2.2.  General Message Format  . . . . . . . . . . . . . . .
  4.2.3.  6P Message Types  . . . . . . . . . . . . . . . . . .
  4.2.4.  6P Command Identifiers  . . . . . . . . . . . . . . .
  4.2.5.  6P Return Codes . . . . . . . . . . . . . . . . . . .
  4.2.6.  6P CellOptions  . . . . . . . . . . . . . . . . . . .
  4.2.7.  6P Cell Format  . . . . . . . . . . . . . . . . . . .
  4.2.14. Generic 6P Request Format
  4.2.14. Generic 6P Response Format
  4.2.15. Generic 6P Confirmation Format
4.2. 6P Commands and Operations
  4.2.8.  Adding cells
  4.2.9.  Deleting cells
  4.2.10. Retrieving the status
  4.2.11. Listing cells
  4.2.12. Clearing the Schedule
  4.2.13. Relocating a cell
4.3.  Protocol Behavior . . . . . . . . . . . . . . . . . . . .
  4.3.1.  Version Checking  . . . . . . . . . . . . . . . . . .
  4.3.2.  SFID Checking . . . . . . . . . . . . . . . . . . . .
  4.3.3.  Concurrent 6P Transactions  . . . . . . . . . . . . .
  4.3.4.  Timeout . . . . . . . . . . . . . . . . . . . . . . .
  4.3.5.  SeqNum Mismatch . . . . . . . . . . . . . . . . . . .
  4.3.8.  Aborting a 6P Transaction . . . . . . . . . . . . . .
  4.3.9.  Deleting Cells  . . . . . . . . . . . . . . . . . . .
  4.3.10. Listing Cells . . . . . . . . . . . . . . . . . . . .
  4.3.11. Cell Relocation . . . . . . . . . . . . . . . . . . .
  4.3.12. Cell Suggestion . . . . . . . . . . . . . . . . . . .
  4.3.13. Generation Management . . . . . . . . . . . . . . . .
  4.3.14. Handling error responses  . . . . . . . . . . . . . .
```

renaming

- STATUS -> COUNT?

Preparation for IETF 98

Meeting

- Thomas remote, Michael sitting
- 6P: Xavi and Qin remote
- SFO: ?
- Security?

Meeting agenda

- 2h30
- News on minimal
- 6P?
- Security
- SF0?

draft-…-6tisch-…

Author1
Author2
Author3

Meeting

- STATUS -> COUNT?

AOB ?

Thank you!