**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title |  | |
| Date Submitted | [12 March 2015] | |
| Source | [] [] [address] | Voice: [ ] Fax: [ ] E-mail: [ ] |
| Re: | [Interest Group 6tisch Interim Meeting in Vancouver] | |
| Abstract | [Interest Group 6tisch Minutes.] | |
| Purpose | [Official minutes of the Task Group Session | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

**IEEE 802.15 Plenary Meeting – Session #96**

**Hyatt Regency, Vancouver, Canada**

**May 11-14, 2015**

Monday, 11 May 2015, 13:30 (PM1) 2

# Monday, 11 May 2015, 13:30 (PM1)

**13:30** IG 6tisch chair, Pat Kinney, called meeting to order.

Chair presented opening report 15-15-0350-01-ig6t:

Chair displayed the IEEE-SA slides #1 through #4 of the IEEE patent policy.

Chair asked if anyone in the meeting was personally aware of the holder of any patent claims that are potentially essential to implementation of the proposed standard(s) under consideration by this group and that are not already the subject of an Accepted Letter of Assurance? There were no responses.

**Agenda for Vancouver**

* + Chair presented the agenda 15-15-0349-00, objectives are to review issues such as RPL overhead, security, etc. Status of IETF 6TiSCH
* **Review and Status of IETF 6TISCH**
* Chair presented the IETF 6TiSCH status focusing on the minimal draft effort, the architecture draft effort
  + 6tisch Minimal issues discussion
    - Issues – References to 802.15.4
      * Issue as to how to reference IEEE 802.15.4
      * Initial text referred to subclause numbers of 802.15.4e and 802.15.4-2011
      * Comment made to not reference subclause numbers
      * Comment made to not call out 802.15.4e in the text, but put that information in the Normative Reference section
      * Comment made to just state 802.15.4 without specifying a specific document e.g. 2011
      * Significant push back from those who did not trust IEEE 802.15 as to backwards compatibility, i.e. what if IEEE 802.15 changed the revision and deleted critical portions of the text?
    - Issues – Security
      * This draft assumes the existence of two cryptographic keys, K1 and K2.  EBs SHOULD be authenticated with key K1.  DATA, ACKNOWLEDGEMENT, and MAC COMMAND frame types SHOULD be authenticated and encrypted with key K2.  For early interoperability, K1 MAY be set to "6TiSCH minimal15".  K2 SHOULD be a randomly generated high entropy cryptographic key.  Key distribution is out of scope.
  + 6tisch Architecture
    - Routing
      * Route Computation may be achieved in a centralized fashion by a Path Computation Element (PCE), in a distributed fashion using the Routing Protocol for Low Power and Lossy Networks (RPL) [RFC6550], or in a mixed mode.
      * The Backbone Routers may perform proxy IPv6 Neighbor Discovery (ND) [RFC4861] operations over the backbone on behalf of the wireless devices (also called motes), so they can share a same IPv6 subnet and appear to be connected to the same backbone as classical devices.
      * The Backbone Routers may alternatively redistribute the registration in a routing protocol such as OSPF [RFC5340] or BGP [RFC2545], or inject them in a mobility protocol such as MIPv6 [RFC6275], NEMO [RFC3963], or LISP
    - Schedule Management
      * The 6TiSCH architecture defines four ways a schedule can be managed and TimeSlots can be allocated:
      * Static Scheduling
      * Neighbor-to-Neighbor Scheduling
      * Remote monitoring and Scheduling management
      * Hop-by-hop scheduling.
    - Forwarding models
      * G-MPLS Track Forwarding, which switches a frame received at a particular TimeSlot into another TimeSlot at Layer-2
      * 6LoWPAN Fragment Forwarding, which allows to forward individual 6loWPAN fragments along the route set by the first fragment
      * Classical IPv6 Forwarding, where the node selects a feasible successor at Layer-3 on a per packet basis, based on its routing table.
  + 6tisch Security
    - Provisioning
      * A) nothing
      * B) PSK(s)
      * C) raw public/private key
      * D) certificate(s) from
      * i) manufacturer/distributor/installer
      * ii) consortium (e.g. Corner Grocers Alliance)
      * iii) end user/owner (e.g. Charlie's Market)
      * iv) desired network(s)
    - Operation
      * 1) L2 key(s) for MIC (and optionally encryption)
      * 2) DTLS session with JCE if present
      * 3) DTLS session with PCE if present
      * 4) L2 keys for 6top communication to neighbors
      * 5) locally-significant certificate for future joins
  + Next Meeting – IETF93, Prague; 20 – 25 July 2015

**14:30** Meeting adjourned