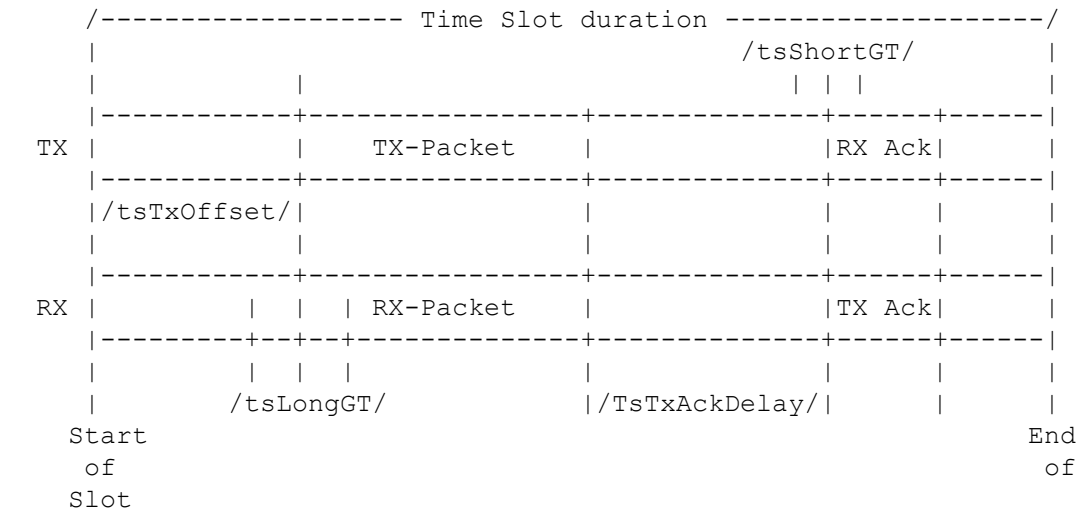
draft-ietf-6tisch-minimal-03

Xavier Vilajosana (Ed.)
Kris Pister

Status

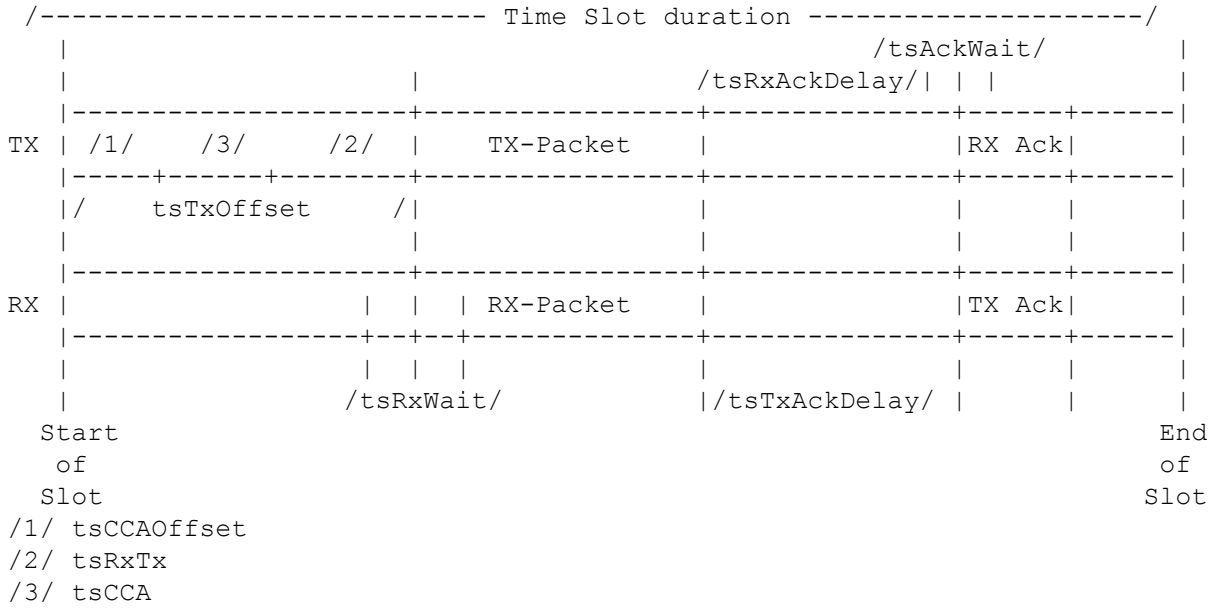
- Status:
  - Adopted at Vancouver IETF89
  - Latest version draft-ietf-6tisch-minimal-03 published on 26th of October 2014 https://datatracker.ietf.org/doc/draft-ietf-6tisch-minimal/
- Changes since IETF90
  - Homogenized default timing with IEEE802.15.4e
  - Added security requirements
  - Pointed out the need of HbH compression using 6lo approach

Time slot internal timing diagram



OLD

NEW



OLD

IEEE802.15.4e TSCH parameter	Value
TsTxOffset	2120us
TsLongGT	2000us
TsTxAckDelay	1000us
TsShortGT	400us
Time Slot duration	10000us

NEW

IEEE802.15.4e TSCH parameter	Value (us)
tsCCAOffset	1800
tsCCA	128
tsTxOffset	2120
tsRxOffset	1120
tsRxAckDelay	800
tsTxAckDelay	1000
tsRxWait	2200
tsAckWait	400
tsRxTx	192
tsMaxAck	2400
tsMaxTx	4256
Time Slot duration	10000

Security

A minimal security configuration inherits the security considerations defined in the Section 19 of [RFC6550]. Other specific security mechanisms described in Section 10 of [RFC6550] are OPTIONAL in this scope. As this document refers to the interaction between Layer 3 and Layer 2 protocols, this interaction MUST be secured by L2 security mechanisms which include a CCM* [RFC3610], [CCM] ,[CCM-Star], architecture. Yet, as RPL is a distributed routing protocol, a peer-wise security mechanism might be used, rather than a centralized one. Key distribution is out of scope of this document, but examples include pre-configured keys at the nodes, shared keys amongst peers or well-known keys. Refer to the 6TiSCH architecture document [I-D.ietf-6tisch-architecture] for further details on security aspects. This document RECOMMENDS the use of shared keys and a CCM* architecture. It also RECOMMENDS the strict application of RPL consideration introduced above.

Security -- Summary

- Inherits security considerations from RFC6550 (Section 19)
  - Be aware of low power requirements
  - Be aware of constrained nature of the nodes
  - Based on symmetric-key and public-key cryptography and use keys that are to be provided by higher-layer processes.
  - The mechanisms assume a secure implementation of cryptographic operations and secure and authentic storage of keying material.
  - Key can be shared by peers or by groups of peers.
- Optional specific security requirements defined by RFC 6550 (Section 10)
  - Three modes:
    - Unsecured
    - Pre-installed
    - Authenticated.
- Interaction between nodes must be secured at L2. Provided by L2 security mechanisms. (CCM*)
- Key distribution is out of scope. (refer to draft-ietf-6tisch-architecture)
- Recommends:
  - Shared keys
  - CCM*
  - Strict application of RPL considerations in point 1)

Open Questions

- HbH header compression. Indicate direction
  - 6lo approach used. We need a more clear visión to summarize it at the draft.
- Security
  - Link it to the security draft?
- Review of IEs in the EBs and other Frames. Is everything covered?
  - Need review and approval from 15.4e experts/implementors