IEEE P802.15
Wireless Personal Area Networks

|  |
| --- |
| One-to-many CIDs 584, 590, 593 and 594 |
| Date: Jan 12, 2025 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jinjing Jiang | Apple Inc. |  |  | jinjing @ apple.com |
| Rojan Chitrakar | Huawei |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document discusses and proposes resolutions for the following CIDs: 584, 590, 593 and 594.

The discussion and proposed changes are based on P802.15.4ab™ D01 Draft Standard for Low-Rate Wireless Networks.

Revision history:

R0 – Initial version

R1 - minor editorial update

R2 - minor editorial update

R3 – revise the “proposed changes” for CIDs 584, 590, 593 and 594. Remove CID 1166.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Comment** | **Proposed Change** | **Proposed resolution** |
| 584 | 104 | 7 | The slot index fields are limited to 8-bits because of the security, but here they are sent as 16-bit fields.  | Change Start and End Slot Index fields to be one octet long. | Revised.  |
| 590 | 107 | 1 | The slot index fields are limited to 8-bits because of the security, but here they are sent as 16-bit fields.  | Change Start and End Slot Index fields to be one octet long. | Revised. |
| 593 | 108 | 1 | The slot index fields are limited to 8-bits because of the security, but here they are sent as 16-bit fields.  | Change Start Slot Index field to be one octet long. | Revised. |
| 594 | 108 | 5 | The slot index fields are limited to 8-bits because of the security, but here they are described as 16-bit fields.  | Change Start Slot Index field to be one octet long. | Revised. |

## CIDs 584, 590, 593, 594

After searching the draft, the following places use the Slot Index directly or indirectly.

* P30 L6 - Figure 3—Frame Counter field for Compact frame nonce in non-hyper block mode
* P30 L13 - Figure 4—Frame Counter field for Compact frame nonce in hyper block mode
* P48 L21 - Figure 11—Scheduling List field element format when Scheduling List Type is zero
* P49 L24 - Figure 14—Scheduling List field element format when Scheduling List Type is three
* P50 L9 - Figure 15—Scheduling List field element format when Scheduling List Type is four

**The first two from the above are related to frame counters in security. Let us discuss them first.**

**Background:**

The total Nonce length is limited to 13 octets as specified in Annex B, i.e., the Frame Counter field is limited to 5 octets, so the slot index can’t be simply increased to 16-bits for Fig 4:







Max value of Block Index, Hyper Block Index (16 bits) = 65,535

P43 L29:

Ranging Block Index = Current Hyper Block Index × the number of blocks in a hyper block + the relative block index

**Proposal:** Unify the nonce for block based mode and hyper block mode. For Hyper block mode, use the ranging block index as the Block Index field.

**Implication:** The Ranging Block Index for Hyper block mode is limited to 65,353 and this limit has to be specified in 4ab.

**Proposed changes for D0.1:**

**9.3.2.4 AEAD Nonce for Compact frames**

…

The Frame Counter field for Compact frame is formatted as illustrated in Figure 3 and the Slot Index field, the Round Index field and the Block Index field are set as the indices of the ranging slot, ranging round and ranging block, in which the Compact frame is transmitted or received, respectively. In hyper block mode, the ranging block index shall be calculated as specified in 10.32.3.5 Hyper block mode.

|  |  |  |
| --- | --- | --- |
| **Bits: 0-15** | **16-23** | **24-39** |
| Slot Index | Round Index | Block Index |

**Figure 3—Frame Counter field for Compact frame nonce**

**10.32.3.5 Hyper block mode**

…

Ranging Block Index = Current Hyper Block Index × the number of blocks in a hyper block + the relative block index

If secure Compact frames are used in Hyper Block mode, the Controller shall ensure that the values of Hyper Block Index and Relative Block Index does not cause the value of the Ranging Block Index to exceed 216 – 1.

NOTE - The maximum value of Ranging Block Index in this case is restricted by the size of the Block Index field of the Frame Counter field for Compact frame nonce as specified in 9.3.2.4 .

The hyper block index together with the ranging block index is used by devices to maintain synchronization

with the block structure.

**For Schedule IE design, we can directly changes the field to 2 octets without affecting other functionalities.**

**Proposed changes for D0.1:**

|  |  |
| --- | --- |
| **Octets:2** | **2/8** |
| Slot Index | Sender Address |

**Figure 11—Scheduling List field element format when Scheduling List Type is zero**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Bits: 0-1** | **2** | **3-7** | **Octets: variable** | **2/8** | **0** | **0/2** |
| Scheduling Bitmap Length | Bitmap OffsetPresent | Reserved | Scheduling Bitmap | SenderAddress | Receiver Address | Bitmap Offset |

**Figure 13—Scheduling List field element format when Scheduling List Type is two**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bits: 0-14** | **15-18** | **19-23** | **Octets:2/8** | **0/2/8** |
| Starting Slot Index | Scheduling Step | Scheduling Repetition | SenderAddress | ReceiverAddress |

**Figure 14—Scheduling List field element format when Scheduling List Type is three**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Bits: 0-14** | **15-18** | **19-23** | **Octets:2/8** | **0/2/8** | **1** | **1** | **1** |
| Starting Slot Index | Scheduling Step | Scheduling Repetition | SenderAddress | ReceiverAddress | SequenceIndex | Number of Gaps | Sequence Repetition |

**Figure 15—Scheduling List field element format when Scheduling List Type is four**