IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for Location | | | | |
| Date: 2020-10-14 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Bangalore India |  | [Girish.madpuwar@broadcom.com](mailto:Girish.madpuwar@broadcom.com) |
| Nehru Bhandaru | Broadcom | San Jose  CA, USA |  | [Nehru.bhandaru@broadcom.com](mailto:Nehru.bhandaru@broadcom.com) |
| Ali Raissinia | Qualcomm |  |  | alirezar@qti.qualcomm.com |

**Abstract**

This submission proposes resolutions of comments received from TGaz LB 249.

* CIDs:
  + - Total CID: 5
    - CIDs: 3123, 3124, 3450, 3754, 3775

The comments are based on TGaz Draft 2.4 and “IEEE P802.11-REVmd/D3.2, March 2020”

Revision 0: initial draft

Revision 1: minor corrections

Revision 2: revised resolution for CID 3450. Included CID 3775

### CID 3123 / 3124/ 3754 / 3775

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3124 | 11.22.6.4.6.2  Page 160 | Alireza Raissinia | Paragraphs (four of them) starting from line 20 and ending line 43) seem to describe a behavior when RSTA indicates the need for a new SAC for measurement is needed, which is missing from the text as it describes not to use TOD or TOA. | Add a phrase to highlight the condition when RSTA indicates the need for use of new SAC. | Revised.  The change is applicable for TB and non-TB mode of operation.  Modified section 11.22.6.4.6.1 & 11.22.6.4.6.2  TGaz editor, make the changes identified in submission 11-20-1649 |
| 3754 | 11.22.6.4.6.1  Page 154 | Mark RISON | This is confusing. In both cases the LTF\_SEQ is being set to "the Secure-LTF-bits-I2R", so there's no need for two bullets. Ditto R2I below | As it says in the comment | Revised.  TGaz editor, make the changes identified in submission 11-20-1649 |
| 3775 | 11.22.6.4.6.2  Page 160 | Mark RISON | "When an RSTA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE 20 to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any 21 secure HE-LTF or null (#1828, #1831)" -- a bit string or null are the only two things it can be set to, as far as I can tell | Delete the para at the referenced location, and the next 3 paras | Revised  TGaz editor, make the changes identified in submission 11-20-1649 |
| 3123 | 11.22.6.4.6.1  Page 153 | Alireza Raissinia | Delete " a new Secure LTF Counter" and add "LTF Generation Information corresponding to Secure LTF Counter" | As per comment | Revised  TGaz editor, make the changes identified in 11-20-1649 as below |
|  |  |  |  |  |  |

***TGaz Editor: Add following to section 3.2***

**3.2 Definitions specific to IEEE 802.11**

**Null-SAC-HE-LTF** : A HE LTF present in I2R NDP or R2I NDP in the Ranging frame exchange where SAC subfield in the STA Info field of Ranging NDP Announcement frame or SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame doesn’t match with value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA (#3124).

**11.21.6.4.5.2 TB Ranging Measurement Exchange with Secure LTF**

***TGaz Editor: modify following to section 11.22.6.4.5.2 Page 159 line 1***

When an RSTA has established a secure LTF measurement setup with an ISTA as specified in 11.21.6.3.4 (Negotiation for secure LTF in the TB and Non-TB measurement exchange), the RSTA that sends a Ranging Secure Sounding Trigger frame to the STA shall set: (#1260)

* The SAC subfield in the Trigger Dependent User Info field (#1129) corresponding to the ISTA in the Ranging Secure Sounding Trigger frame to the same value as in the LTF Generation SAC field in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA

The RSTA shall set the I2R Rep subfield of the STA Info field corresponding to the ISTA in the Ranging Secure Sounding Trigger frame equal to the RSTA Assigned I2R Rep corresponding to the ISTA.

* After transmission of the Ranging Secure Sounding Trigger frame to the ISTA, the RSTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set tothe Secure-LTF-bits-I2R based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA (see 11.21.6.4.5.4 (Secure LTF Generation)).

When the RSTA receives the HE TB Ranging NDP from the ISTA, the RSTA shall:

1. Send a Ranging NDP Announcement frame.
2. Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to
   * the Secure-LTF-bits-R2I based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA (see 11.21.6.4.5.4 (Secure LTF Generation)).
3. Send a Location Measurement Report frame that includes the Secure LTF Parameters field to the ISTA.

Otherwise, the RSTA shall follow the rules in 10.22.2.2 (EDCA backoff procedure) as the frame exchange is not successful.

:

:

***TGaz Editor: modify following to section 11.22.6.4.5.2 Page 160 line 24***

When an ISTA receives a Ranging Secure Sounding Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, the ISTA shall:

* Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-I2R based on (#1830, #1832) the Secure LTF Counter (#2289) and the corresponding SAC (#3123) in the Secure LTF Parameters field in the last Fine Timing Measurement frame received, or last Location Measurement Report frame received from the RSTA (see 11.21.6.4.5.4 (Secure LTF Generation));
* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to the Secure-LTF-bits-R2I based on (#1830, #1832) the Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last Fine Timing Measurement frame received, or last Location Measurement Report frame received from the RSTA see 11.21.6.4.5.4 (Secure LTF Generation));

When an ISTA receives a Ranging Secure Sounding Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, the ISTA shall:

1. Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to (#2289) the Secure-LTF-bits-I2R for generating any secure HE-LTF (#3124) (#1828, #1831);
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to (#2289) the Secure-LTF-bits-R2I for receiving any secure HE-LTF (#3124) (#1828, #1831);

When an ISTA receives a Ranging NDP Announcement frame from an RSTA in which the AID11/RSID11 subfield in the STA Info field contains the 11 least significant bits of the AID or RSID of the ISTA, the ISTA shall:

1. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_OFFSET that is set to the Offset subfield value in the STA Info field;
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_N\_STS that is set to the R2I N\_STS subfield value in the STA Info field;
3. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_REP that is set to the R2I Rep subfield value in the STA Info field;

When a Location Measurement Report frame contains range measurement results measured from an I2R NDP and a R2I NDP, an RSTA or ISTA that transmits the RSTA2ISTA or ISTA2RSTA Location Measurement Report frame shall include the Secure LTF Parameters field in the Location Measurement Report frame and the Range Measurement SAC subfield in the Secure LTF Parameters field in the Location Measurement Report frame to the same value as in the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame that solicited the I2R NDP and the R2I NDP. The Measurement Result LTF Offset field in the Secure LTF Parameter element in the Location Measurement Report frame shall set to the same value as in the Offset subfield of User Info field in the Ranging NDP Announcement frame that precedes the R2I NDP. When an ISTA or RSTA receives RSTA2ISTA or ISTA2RSTA Location Measurement Report frame, the ISTA or RSTA shall compare the value of Measurement Result LTF Offset field with the value of the Offset subfield in the corresponding User Info field of Ranging NDP Announcement frame, and if these two values don’t match, the ISTA or RSTA shall discard the measurement results carried in the Location Measurement Report frame. (#1580, #2283, #1163)

When frame exchange which consist of receiving HE TB Ranging NDP and transmitting HE Ranging NDP results into null-SAC-HE-LTF, the RSTA shall not use the TOA and TOD value of the HE TB Ranging NDP and HE Ranging NDP respectively and shall (#3842) set the Invalid Measurement Indication subfield to 1 in the TOA error field field in the Location Measurement Report carrying the TOA value of the I2R HE TB Ranging NDP (#3775).

When an ISTA receives a Ranging Secure Sounding Trigger frame from an RSTA in which the value of the SAC subfield in the Trigger Dependent User Info field is not equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA, the ISTA shall

* not use TOD value of the I2R HE TB Ranging NDP
* not use TOA value of the R2I HE Ranging NDP, and shall (#3842) set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the Location Measurement Report carrying the TOA value of the HE Ranging NDP if the Location Measurement Report transmission from the ISTA was negotiated.

STA shall discard SAC value used for frame exchange and shall not use the same SAC value in the current measurement exchange.

***TGaz Editor: Replace Figure 11-37p on Page 162 with following figure***

******

**11.21.6.4.5.3 Non-TB Ranging Measurement Exchange with Secure LTF.**

***TGaz Editor: modify following to section 11.22.6.4.5.3 Page 163 line 12***

When an ISTA has established a secure LTF measurement setup with an RSTA as specified in 11.21.6.3.4 (Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange), this ISTA shall set the following subfields in any Ranging NDP Announcement frame addressed to that RSTA as follows: (#1260)

* The SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame to the same value as in the LTF Generation SAC field in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA
* Otherwise the SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame set to a value of 0 to indicate that a new Secure LTF Counter (#2289) and the corresponding SAC (#3123) is needed.

The ISTA shall set the I2R Rep subfield and R2I Rep subfield of the STA Info field in the Ranging NDP Announcement frame to the RSTA Assigned I2R Rep and the RSTA Assigned R2I Rep values respectively, corresponding to the RSTA.

An ISTA that sends a Ranging NDP a SIFS after transmission of the Ranging NDP Announcement frame shall set the TXVECTOR parameter LTF\_SEQUENCE as follows:

* Either (#3754) null (#1828, #1831) if the SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame is set to a value of 0 (#3124);
* Or the Secure-LTF-bits-I2Rbased on (#1830, #1832) the Secure LTF Counter (#2289) and the corresponding SAC in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA (see 11.21.6.4.5.4 (Secure LTF Generation)) (#3123).

After transmission of the Ranging NDP Announcement frame to the RSTA, the ISTA’s MAC sublayer shall issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR

parameter that is set (#2289) as follows:

* Either (#3754) null (#1828, #1831) if the SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame is set to 0.
* Or the Secure-LTF-bits-R2I based on (#1830, #1832) the Secure LTF counter in the Secure LTF Parameters field in the last Fine Timing Measurement frame received or last Location Measurement Report frame received from the RSTA (see 11.21.6.4.5.4 (Secure LTF Generation)).

When an RSTA receives a Ranging NDP Announcement frame from an ISTA frame in which the SAC subfield in the STA Info field with AID equal to 2043 is neither equal to value 0 nor the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA, the RSTA shall:

* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that is set to the Secure-LTF-bits-I2R for receiving null-SAC HE-LTF (#1828, #1831);
* Send an HE Ranging NDP to ISTA with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-R2I for generating null-SAC-HE-LTF (#1828, #1831) to the ISTA, if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame;
* Send a Location Measurement Report frame that includes the Secure LTF Parameters field containing secure LTF counter and corresponding SAC to the ISTA, if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the value of the SAC subfield in the STA Info field with AID equal to 2043 is set equal to the value of the LTF Generation SAC subfield in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA, the RSTA shall:

* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that is set to the Secure-LTF-bits-I2Rbased on (#1830, #1832) the Secure LTF Counter and corresponding SAC (#2289) in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame, or last transmitted Location Measurement Report frame to the ISTA; see 11.21.6.4.5.4 (Secure LTF Generation))
* Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-R2I based on (#1830, #1832) the Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last transmitted Fine Timing Measurement frame, or last transmitted Location Measurement Report frame to the ISTA, if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame; see 11.21.6.4.5.3 (Secure LTF Generation))
* Send a Location Measurement Report frame that includes the Secure LTF Parameters field to the ISTA, if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame.

An RSTA transmitting a Location Measurement Report frame contains range measurement results measured from an I2R NDP and a R2I NDP, shall include the Secure LTF Parameters field in the Location Measurement Report frame and set the Range Measurement SAC subfield in the Secure LTF Parameters field in the Location Measurement Report frame to the same value as in the SAC subfield in the STA Info field with AID equal to 2043 in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP.

When a STA sends null-SAC-HE-LTF in HE Ranging NDP (#3124) (#1828, #1831), the STA shall not use the TOD value of HE Ranging NDP for the secure range measurement.

When a STA receives null-SAC-HE-LTF in HE Ranging NDP (#3124) (#1828, #1831), the STA shall not use the TOA value of the HE Ranging NDP and shall (#3842) set the Invalid Measurement Indication subfield to 1 in the TOA Error field in the Location Measurement Report carrying the TOA value of the HE Ranging NDP.

When there is a transmission failure within a secure measurement exchange sequence, the recovery procedure of the LTF Generation SAC (#2289) is illustrated in Figure 11-37r (Error recovery of Non-TB Ranging measurement exchange using Secure LTF). (#1129)

STA shall discard SAC value used for frame exchange and shall not use the same SAC value in the current measurement exchange.

***TGaz Editor: change as specified in the section below on page 130 line 9***

**11.21.6.3.4 Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange (#1817, #1818, #1824, #2321)**

:

:

**Suggested Change (p130.9)**

For each secure FTM negotiation, prior to transmission of IFTM, and for each measurement within an FTM session, an RSTA shall increment the Secure-LTF-Counter by 1. The Secure-LTF-Counter is included as part of Secure LTF Counter (#2289) conveyed to the ISTA. An ISTA determines the Secure-LTF-Counter to use for a measurement using the Secure LTF Counter and LTF Generation SAC received from the RSTA in a the most recent protected IFTM or LMR frame. The Secure-LTF-Counter shall be reset when a new KDK is derived as part of a new PTK derivation and it shall continue, and not be reset, for each secure FTM negotiation using a given KDK.

***TGaz Editor: change the title of section 11.21.6.4.54. to follwing***

**11.21.6.4.5.4 Secure LTF Generation**

### CID 3450

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3450 | 11.22.6.3.3 | 140 | The exact detail of timestamping NDP tx and rx at the antenna connector should be clarified, as it is for | Add figures like Figure 6-17 to 11.22.6.4.2.2 and 11.22.6.4.3.3 (perhaps as part of Figure 11-36F, for example), to show the snapshot of the timestamp at the Antenna (not at the MLME) in the NDP cases. | Revised.  Please refer submission 11-20-1437 resoultion of CID 3451.  1. figure 6-17b title changed to:  “Fine Timing Measurement primitives and timestamp reporting capture for Non-  TB Ranging measurement exchange”  2. figure 6-17c title changed to:  “Fine Timing Measurement primitives and timestamps reporting capture for TB  Ranging measurement exchange”  Thus figures represent timestamp reporting and not timestamp capture  TGaz editor, make the changes identified in submission 11-20-1437. No additional change proposed in this submission. |