IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for Location |
| Date: 2019-12-26 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Electronic City, Bangalore India |  | Girish.madpuwar@broadcom.com  |
| Nehru Bhandaru | Broadcom | San JoseCA, USA |  | Nehru.bhandaru@broadcom.com |
|  |  |  |  |  |

**Abstract**

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

* CIDs:
	+ - Total CID: 30
		- CIDs: 3066, 3450, 3123, 3754, 3760, 3842, 3843, 3912, 3913, 3914, 3771, 3124, 3777, 3778, 3779, 3780, 3782, 3783, 3625, 3768

The comments are based on TGaz Draft 2.0

Revision 0: initial draft

### CID 3066

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3066 | 11.22.6.4.1 | 128 | What is the "I." in line 21 page 128? | As per comment | Accpeted  |

11.22.6.4.1 FTM Measurement exchange overview

FTM measurement has three basic ranging mechanisms:

— EDCA based ranging described in 11.22.6.4.2 (EDCA based ranging measurement exchange)

— TB ranging described in 11.22.6.4.3 (TB ranging measurement exchange) and 11.22.6.4.8

(Measurement exchange in Passive TB ranging)

— non-TB ranging described in 11.22.6.4.4 (non-TB ranging measurement exchange)

### 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.Adding figure inclause 6.3.56.1 |

***TGaz Editor: replace “Figure 16-7b and 16-7c with following figures***



Figure 16-7b non-Trigger Based Sounding Exchange for Ranging



Figure 16-7c Trigger Based Sounding Exchange for Ranging

### CID 3123

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3123 | 11.22.6.4.6.1 | 153 | Delete " a new Secure LTF Counter" and add "LTF Generation Information corresponding to Secure LTF Counter" | As per comment | Revised |

***TGaz Editor: Modify the text as per following suggestion:***

**11.22.6.4.6.1 Secure Non-TB ranging mode**

When an ISTA has established the secure LTF measurement setup with a RSTA as specified in 11.22.6.3.4 (Secure LTF measurement setup), the ISTA that sends a Ranging NDP Announcement frame shall set (#1260):

— The SAC subfield in the STA Info SAC field 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 received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA, if the ISTA has not sent any Ranging NDP Announcement frame after the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;

— Otherwise the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame to 0 to indicate that a new Secure LTF Generation Information r (#2289) is needed.

**11.22.6.4.6.2 TB ranging measurement exchange for secure LTF**

When an RSTA has established the secure LTF measurement setup with an ISTA as specified in 11.22.6.3.4 (negotiation for secure LTF in the TB and NTB 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 AID/RSID of 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, if the RSTA has not sent any Ranging Secure Sounding Trigger frame to the ISTA after the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA;

— Otherwise the SAC subfield in the Trigger Dependent User Info field in the STA Info field corresponding to AID/RSID of the ISTA in the Ranging Secure Sounding Trigger frame to 0 to indicate that a new Secure LTF Generation Information (#2289) is needed.

### CID 3754

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3754 | 11.22.6.4.6.1 | 154 | 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 | Rejected |

Section 11.22.6.4.6.1 Secure Non-TB ranging mode stats the following:

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

*—Either the Secure-LTF-bits-I2R for generating* ***any secure HE-LTF*** *or* ***null*** *(#1828, #1831), if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to a value of 0;*

*— Otherwise the Secure-LTF-bits-I2R (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA.*

**Reason for rejection:**

If ISTA doesn’t have valid Secure-LTF-bits, it indicates by setting STA Info SAC field in Ranging NDP Announcement is set to value 0. Range measurement results from this sequence needs to be ignored. Hence it’s really doesn’t matter what value is used for Secure-LTF-bits-I2R. In first bullet use of word “any” in the first clause above indicates that ISTA can generate any secure HE-LTF using Secure-LTF-bits-I2R or “null”. Whereas bullet two indicates that valid Secure-LTF-bits-I2R bits are being used.

### CID 3760 / CID 3914 / CID 3912 / CID 3913

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3760 | 11.22.6.4.6.1 | 155 | "The LTF Generation SAC and its associated Secure LTF Counter (#2289) parameters are carried in an initial Fine Timing Measurement frame and a Location Measurement Report frame." but the figure doesn't show the counter | Show the counter in Figure 11-36n--Normal secure measurement exchange in Non-TB mode | Revised.Suggested change is done for both non-TB and TB mode |
| 3914 | 11.22.6.4.6.1 | 156 | Figure 11-36n, the term "LTF\_GEN\_INFO" is no longer used. Replace it with the correct term. Same errors occur in Figure 11-36o, Figure 11-36p, 11-36q, and should be corrected. | As in comment. | Revised.Suggested change is done for both non-TB and TB mode |
| 3912 | 11.22.6.4.6.1 | 156 | Figure 11-36n, the text "LTF Sequence of I2R NDP\_1 is derived from LTF\_GEN\_INFO1" is incorrect, and should be replaced with "LTF Sequence of I2R NDP\_1 is derived from LTF\_GEN\_INFO1 and LTF\_GEN\_SAC1". Same errors occur in Figure 11-36o, Figure 11-36p, 11-36q, and should be corrected. | As in comment. | Accepted.I2R bits are generated using LTF-counter and SAC. R2I bits are genated using LTF-counter  |
| 3913 | 11.22.6.4.6.1 | 156 | Figure 11-36n, the text "LTF Sequence of I2R NDP\_2 is derived from LTF\_GEN\_INFO2" is incorrect, and should be replaced with "LTF Sequence of I2R NDP\_2 is derived from LTF\_GEN\_INFO12 and LTF\_GEN\_SAC2". The same error occurs in Figure 11-36p, and should be corrected. | As in comment. | Revised.I2R bits are generated using LTF-counter and SAC. R2I bits are genated using LTF-counter |

***TGaz Editor: Update “Figure 11-36n as follow:***

Note: following changes are done to the figure

1. For Initiating STA (text to the right of vertical line)
	* LTF\_GEN\_INFO1 replaced with SEC\_LTF\_CNTR1 & LTF\_GEN\_SAC1
	* LTF\_GEN\_INFO2 replaced with SEC\_LTF\_CNTR2 & LTF\_GEN\_SAC2
2. For Responding STA ( text to left of vertical line)
	* LTF\_GEN\_INFO1 replaced with SEC\_LTF\_CNTR1
	* LTF\_GEN\_INFO2 replaced with SEC\_LTF\_CNTR2
3. Text on Arrow
	* LTF\_GEN\_INFO1 replaced with SEC\_LTF\_CNTR1
	* LTF\_GEN\_INFO2 replaced with SEC\_LTF\_CNTR2
	* LTF\_GEN\_INFO3 replaced with SEC\_LTF\_CNTR3

LTF\_GEN\_INFO is repleaced by SEC\_LTF\_CNTR)



***TGaz Editor: modify “Figure 11-36o as follows:***

1. For Initiating STA (text to the right of vertical line)
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1 & LTF\_GEN\_SAC1
2. For Responding STA ( text to left of vertical line)
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1
3. Text on Arrow
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1
	* Replace LTF\_GEN\_INFO2 with SEC\_LTF\_CNTR2
	* Replace LTF\_GEN\_INFO3 with SEC\_LTF\_CNTR3



***TGaz Editor: modify text in “Figure 11-36p as follows:***

* For Initiating STA (text to the right of vertical line)
	+ Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1 & LTF\_GEN\_SAC1
	+ Replace LTF\_GEN\_INFO2 with SEC\_LTF\_CNTR2 & LTF\_GEN\_SAC2
1. For Responding STA ( text to left of vertical line)
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1
	* Replace LTF\_GEN\_INFO2 with SEC\_LTF\_CNTR2
2. Text on Arrow
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1
	* Replace LTF\_GEN\_INFO2 with SEC\_LTF\_CNTR2
	* Replace LTF\_GEN\_INFO3 with SEC\_LTF\_CNTR3



***TGaz Editor: replace “Figure 11-36q do the following change***

* For Initiating STA (text to the right of vertical line)
	+ Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1 & LTF\_GEN\_SAC1
1. Text on Arrow
	* Replace LTF\_GEN\_INFO1 with SEC\_LTF\_CNTR1
	* Replace LTF\_GEN\_INFO3 with SEC\_LTF\_CNTR3



### CID 3842 / CID 3843

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3842 | 11.22.6.4.6.1 | 154 | "the STA shall not use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indication subfield to 1 in the TOA Error field" is ambiguous. It might mean "the STA shall not use the TOA value of the HE Ranging NDP and shall not set the Invalid Measurement Indication subfield to 1 in the TOA Error field", or it might mean "the STA shall not use the TOA value of the HE Ranging NDP and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field", or it might mean "the STA shall not both use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indication subfield to 1 in the TOA Error field" | Change "the STA shallnot use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indication subfield to 1 in the TOA Error field" to "the STA shall not use the TOA value of the HE Ranging NDP and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field" | Accepted.This change is related to 11.22.6.4.6.1 non-TB ranging mode |
| 3843 | 11.22.6.4.6.1 | 155 | "the STA shall not use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indication subfield to 1 in the TOA Error field" is ambiguous. It might mean "the STA shall not use the TOA value of the HE Ranging NDP and shall not set the Invalid Measurement Indication subfield to 1 in the TOA Error field", or it might mean "the STA shall not use the TOA value of the HE Ranging NDP and shall set the Invalid Measurement Indication subfield to 1 in the TOA Error field", or it might mean "the STA shall not both use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indication subfield to 1 in the TOA Error field" | Change "the STA shallnot use the TOA value of the HE Ranging NDP and set the Invalid Measurement Indicationsubfield to 1 in the TOA Error field" to "the STA shallnot use the TOA value of the HE Ranging NDP and shall set the Invalid Measurement Indicationsubfield to 1 in the TOA Error field". Make similar changes at 160.28 and 160.40 | Accepted.This change is related to 11.22.6.4.6.2 TB ranging mode |

***CID 3842***

***TGaz Editor: modify text in following paragraph on page 157 line 33 of section 11.22.6.4.6.1***

11.22.6.4.6.1 Secure Non-TB ranging mode

:

:

When a STA receiving an HE Ranging NDP sets the LTFVECTOR parameter in the PHY-RXLTFSEQUENCE.request primitive to either a bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#1828, #1831), the STA shall not use the TOA value of the HE Ranging NDP and shall 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.

:

:

***CID 3843***

***TGaz Editor: modify text in following paragraph on page 162 line 20 of section 11.22.6.4.6.2***

:

:

When an RSTA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#1828, #1831), the RSTA shall not use the TOD value of HE Ranging NDP for the range measurement.

When an RSTA receiving an HE TB Ranging NDP sets the LTFVECTOR parameter in the PHY-

RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#1828, #1831), the RSTA shall not use the TOA value of the HE Ranging NDP and shall 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 TB Ranging NDP.

When an ISTA sending an HE TB Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#1828, #1831), the ISTA shall not use the TOD value of HE TB Ranging NDP for the range measurement.

When an ISTA receiving an HE Ranging NDP sets the LTFVECTOR parameter in the PHY-

RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) for generating any secure HE-LTF or null (#1828, #1831), the ISTA shall not use the TOA value of the HE Ranging NDP, and shall 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.

:

:

### CID 3771

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3771 | 11.22.6.4.6.2 | 158 | "The RSTA that sends the Ranging NDP Announcement frame shall set the Offset subfield in the STA Info field corresponding to AID/RSID of the ISTA in the Ranging NDP Announcement frame to values meeting the Equation (11-aa)" -- there's only one field so only one value can be passed. Ah, is this because the equation has indices? The wording is odd anyway | Change to "A RSTA shall set the Offset subfields in theSTA Info fields in the Ranging NDP Announcementframe to values that satisfy Equation (11-aa)" | RevisedRepetation of Ranging NDP Announcement removed. Reference of AID/RSID in the description is required since it is acting as an index associated with multiple ISTA |

***TGaz Editor: modify text in following paragraph on page 160 line 37 of section 11.22.6.4.6.2***

**11.22.6.4.6.2 TB ranging measurement exchange for secure LTF**

:

:

The RSTA shall set the Offset subfield in the STA Info field corresponding to AID/RSID of the ISTA in the Ranging NDP Announcement frame to values that satisfy the Equation (11-aa):



:

:

### CID 3124

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3124 | 11.22.6.4.6.2 | 160 | 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: Add following to section 3.2***

**3.2 Definitions specific to IEEE 802.11**

**Non-SAC-HE-LTF** : The HE LTF in UL NDP or DL NDP sent by ISTA or RSTA in the Ranging frame exchange where SAC subfield in the STA Info SAC field of Ranging NDP Announcement frame is 0 or where SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame is 0 or when TXVECTOR parameter LTF\_SEQUENCE is set to null.

***TGaz Editor: modify following to section 11.22.6.4.6.1 Secure Non-TB ranging mode***

When an ISTA has established the secure LTF measurement setup with a RSTA as specified in 11.22.6.3.4 (Secure LTF measurement setup), the ISTA that sends a Ranging NDP Announcement frame shall set (#1260):

* The SAC subfield in the STA Info SAC field 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 received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA, if the ISTA has not sent any Ranging NDP Announcement frame after the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;
* Otherwise the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame to 0 to indicate that a new Secure LTF Counter (#2289) 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 Max I2R Rep subfield value and the Max R2I Rep subfield value in the Ranging Parameters field in the last received Fine Timing Measurement frame from the RSTA.

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

* Either the Secure-LTF-bits-I2R or null (#1828, #1831), if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to a value of 0 to geneate non-SAC-HE-LTF.
* Otherwise the Secure-LTF-bits-I2R (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA.
* 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 the Secure-LTF-bits-R2I or null (#1828, #1831), if the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement is set to zero to generate non-SAC-HE-LTF
* Otherwise the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, #1832) Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the SAC subfield in the STA Info SAC field is set to zero, the RSTA shall:

* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter that is set to either the Secure-LTF-bits-R2I or null (#1828, #1831) to generate non-SAC-HE-LTF;
* Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to either the Secure-LTF-bits-R2I or null (#1828, #1831) to send non-SAC-HE-LTF to the ISTA, if the RSTA receives an HE Ranging NDP from the ISTA a SIFS after the ranging NDP Announcement frame; Such arrangement results into generation of non-SAC-HE-LTF.
* 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.

When an RSTA receives a Ranging NDP Announcement frame from an ISTA in which the value of the SAC subfield in the STA Info SAC field is 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-I2R (see 11.22.6.4.6.3 (Secure LTF Generation Information)) 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;
* Send an HE Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) 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, 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 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 a value of the SAC subfield in the STA Info SAC field is neither equal to 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:

* Not issue a PHY-RXLTFSEQUENCE.request primitive;
* Not send an HE Ranging NDP to the ISTA;
* Not send a Location Measurement Report frame to the ISTA.

When a Location Measurement Report frame contains range measurement results measured from an I2R NDP and a R2I NDP, an RSTA 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 SAC field in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP.

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

When a STA receiving an HE Ranging NDP (#1828, #1831) receives non-SAC-HE-LTF, the STA shall not use the TOA value of the HE Ranging NDP and 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.

The LTF Generation SAC and its associated Secure LTF Counter (#2289) parameters are carried in an initial Fine Timing Measurement frame and a Location Measurement Report frame. The LTF Generation SAC is included in the Ranging NDP Announcement frame as illustrated in Figure 11-36n (Normal secure measurement exchange in Non-TB mode). (#1129)

***TGaz Editor: modify following to section 11.22.6.4.6.2 TB ranging measurement exchange for secure LTF***

**11.22.6.4.6.2 TB ranging measurement exchange for secure LTF**

When an RSTA has established the secure LTF measurement setup with an ISTA as specified in 11.22.6.3.4 (negotiation for secure LTF in the TB and NTB 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 AID/RSID of 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, if the RSTA has not sent any Ranging Secure Sounding Trigger frame to the ISTA after the last transmitted Fine Timing Measurement frame or last transmitted Location Measurement Report frame to the ISTA;
* Otherwise the SAC subfield in the Trigger Dependent User Info field in the STA Info field corresponding to AID/RSID of the ISTA in the Ranging Secure Sounding Trigger frame to 0 to indicate that a new Secure LTF Counter (#2289) is needed.

The RSTA shall set the I2R Rep subfield of the STA Info field corresponding to AID/RSID of the ISTA in the Ranging Secure Sounding Trigger frame to the Max I2R Rep subfield value in the Ranging Parameters field in the last transmitted Fine Timing Measurement frame from the RSTA 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 to as follows:

* Either the Secure-LTF-bits-I2R or null (#1828, #1831), if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame 0 to generate non-SAC-HE-LTF.
* Otherwise the Secure-LTF-bits-I2R (see 11.22.6.4.6.3 (Secure LTF Generation Information)) 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.

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 as follows:
	* Either the Secure-LTF-bits-R2I or null (#1828, #1831), if the SAC subfield in the Trigger Dependent User Info field in the Ranging Secure Sounding Trigger frame 0 to genernate non-SAC-HE-LTF.
	* Otherwise the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) 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.
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.

:

:

:

The RSTA shall set the R2I Rep subfield of the STA Info field corresponding to AID/RSID of the ISTA in the Ranging NDP Announcement frame to the Max R2I Rep subfield value in the Ranging Parameters field in the last transmitted Fine Timing Measurement frame from the RSTA to the ISTA.

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 received Fine Timing Measurement frame or last received Location Measurement Report frame 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 (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;
* Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to the Secure-LTF-bits-R2I (see 11.22.6.4.6.3 (Secure LTF Generation Information)) based on (#1830, #1832) Secure LTF Counter (#2289) in the Secure LTF Parameters field in the last received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA;

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 received Fine Timing Measurement frame or last received Location Measurement Report frame from the RSTA, the ISTA shall:

1. Send an HE TB Ranging NDP with the TXVECTOR parameter LTF\_SEQUENCE set to (#2289) either the Secure-LTF-bits-I2R or null (#1828, #1831) to generate non-SAC-HE-LTF;
2. Issue a PHY-RXLTFSEQUENCE.request primitive with a LTFVECTOR parameter LTF\_SEQUENCE that is set to (#2289) either the Secure-LTF-bits-R2I or null (#1828, #1831) to generate non-SAC-HE-LTF;

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;

(#1580, #2283, #1163) When a Location Measurement Report frame contains range measurement results measured from an I2R NDP and a R2I NDP, a 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 Offset subfield in the corresponding User Info field of Ranging NDP Announcement frame, and if these two values don’t match each other, the ISTA or RSTA shall discard the measurement results carried in the Location Measurement Report frame.

When an RSTA sending an HE Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) or null (#1828, #1831) to generate non-SAC-HE-LTF, the RSTA shall not use the TOD value of HE Ranging NDP for the range measurement.

When an RSTA receiving an HE TB Ranging NDP sets the LTFVECTOR parameter in the PHY-

RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) or null (#1828, #1831) to generate non-SAC-HE-LTF, the RSTA shall not use the TOA value of the HE Ranging NDP and 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 TB Ranging NDP.

When an ISTA sending an HE TB Ranging NDP sets the TXVECTOR parameter LTF\_SEQUENCE to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) or null (#1828, #1831) to generate non-SAC-HE-LTF, the ISTA shall not use the TOD value of HE TB Ranging NDP for the range measurement.

When an ISTA receiving an HE Ranging NDP sets the LTFVECTOR parameter in the PHY-

RXLTFSEQUENCE.request primitive to either the bit string (e.g., the Secure-LTF-bits-R2I or Secure-LTF-bits-I2R) or null (#1828, #1831) to generate non-SAC-HE-LTF, the ISTA shall not use the TOA value of the HE Ranging NDP, and 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.

The LTF Generation SAC and its associated Secure LTF Counter (#2289) parameters are carried in an initial Fine Timing Measurement frame, and a Location Measurement Report frame. The LTF Generation SAC is included in the Ranging Trigger frame Secure Sounding as illustrated in Figure 11-36p (Normal secure measurement exchange in TB mode). (#1129)

### CID 3777 / CID 3778

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3777 | 11.22.6.4.6.3 | 162 | KDF-Hash-Length -- Hash and Length are undefined | Copy from line 6 on next page | RevisedReference added to section 12.7.1.6.2 |
| 3778 | 11.22.6.4.6.3 | 162 | Having || on the left is confusing and risks misunderstandings | Express SAC and the other thing with separate equations using the L() operator (see baseline) | AcceptedText is Annex J also updated based on comment for section 11.22.6.4.6.3 |

***TGaz Editor: Modify following text in section 11.22.6.4.6.3***

**11.22.6.4.6.3 Secure LTF Generation Information**

For a given secure measurement frame (e.g. NDP), the SAC and secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the RSTA are derived as follows

R2I-bits = KDF-Hash-*Length*(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)

SAC = L (R2I-bits,0,16)

Secure-LTF-bits-R2I = L(R2I-bits,16,k-16)

When the derived SAC is equal to 0, the STA shall increment the Secure-LTF-Counter by 1 and perform the derivation again until a nonzero SAC value is obtained.

Similarly, for a given secure measurement frame (e.g. NDP), the secret (pseudo-random) bits to protect all of the LTFs in the frame originating from the ISTA for a given SAC are derived as follows

Secure-LTF-bits-I2R = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

where

KDF-Hash-*Length* is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors))

*Length* is the length in bits required for the SAC concatenated with the Secure-LTF-bits sequence generation input.

 k is obtained using equation 11-yy.

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the Secure-LTF-Counter input to the KDF as well as in the transmitted LTF sequence information. It shall be padded with leading (MSB) 0s to be exactly 6 octets. The SAC transmitted and used in deriving Secure-LTF-bits shall also be of exactly 2 octets in length.

NOTE—A 6 octet sequence counter is sufficient because a unicast protected management frame that uses a 6 octet packet number is used to convey the LTF sequence information that carries the counter.

With the preceding construction, an attacker not knowing Secure-LTF-Key-Seed, would not be able to predict the SAC that would be used for given measurement.

For each measurement, the number of bits required in Secure-LTF-bits-R2I and SAC shall be derived by equation 11-yy and number of bits required in Secure-LTF-bits-I2R shall be derived by Equations 11-zz.

 ( (4P’ + 3) x DL\_N’ HE-LTF x DL\_N’ REP + 16 + 7 ) & ~7), (11-yy)

 ( (4P’ + 3) x UL\_N’ HE-LTF x UL\_N’ REP + 7 ) & ~7), (11-zz)

***Note to TGaz Editor: Term k-16 in Secure-LTF-bits-R2I denotes minus and not hyphen***

***TGaz Editor: Modify following text in Annex J.14.1 on page 241***

**J.14 LTF Sequence Generation Test Vectors**

Downlink Secure LTF bits are derived as follows, 176 bits that comprise of 156 bits for 80 MHz Bandwidth, two symbols for repetition and two repetitions, plus 16 bits for SAC rounded to nearest multiple of 8 bits.

R2I-bits = KDF-Hash-*Length*(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)

SAC = L (R2I-bits,0,16)

Secure-LTF-bits-R2I = L(R2I-bits,16,160)

### CID 3779/ CID 3780

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3779 | 11.22.6.4.6.3 | 163 | Numbers are already exact | Change "exactly 6 octets" to "6 octets long" and "exactly 2 octets in length" to "2 octets long" | Accepted |
| 3780 | 11.22.6.4.6.3 | 163 | "Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the Secure-LTF-Counter input to the KDF as well as in the transmitted LTF sequence information. It shall be padded with leading (MSB) 0s to be exactly 6 octets." -- what is "It"? The Secure-LTF-Counter? The transmitted LTF sequence information? Something else | Replace "It" with what it actually refers to | Accepted |

***TGaz Editor: Modify following text in 11.22.6.4.6.3 Secure LTF Generation Information on page 165***

Integer to octet string conversion (MSB first) specified in 12.4.7.2.2 shall be used to encode the Secure-LTF-Counter input to the KDF as well as in the transmitted LTF sequence information. Secure-LTF-Counter shall be padded with leading (MSB) 0s to make it 6 octets long. The SAC transmitted and used in deriving Secure-LTF-bits shall also be of 2 octets in length.

### CID 3782

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3782 | 11.22.6.4.6.3 | 163 | "For each measurement, the maximal numbers of bits in Secure-LTF-bits-R2I and Secure-LTF-bits-I2R shall be derived by Equations (11-yy, shown including the SAC bits (underlined)) and (11-zz), respectively." -- I have absolutely no idea why I can't be told the number of bits rather than the "maximal" number of bits, nor what the significance of the underlined SAC bits is | As it says in the comment | Rejected |

**Resion of rejection:**

1. Underline just indicates that proposed addition which was accepted. This is how new text is indicated in the submission.
2. Number of bits depends on parametes P’, DL\_NHE-LTF and DL\_NREP . These pareameter will change based on use case. Equation is better way to indicate number of bits required then adding table for all possible values.

### CID 3783

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3783 | 11.22.6.4.6.3 | 164 | " bitwise 1's complement" is an odd way to say what I think it is | Change to " bitwise NOT operator" | Accepted |

***TGaz Editor: Modify following text in 11.22.6.4.6.3 Secure LTF Generation Information on page 166***

**11.22.6.4.6.3 Secure LTF Generation Information**

For a given secure measurement frame (e.g. NDP), the SAC and secret (pseudo-random) bits to

protect all of the LTFs in the frame originating from the RSTA are derived as follows

:

:

- is the assigned number of I2R repetitions equal to the value set in LTF\_REP within the TXVECTOR and the RXVECTOR for the uplink.

- & is the bitwise AND operator and ~ is the bitwise NOT operator

### CID 3625

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3625 | 11 |  | All the stuff on Secure-LTF-Key-Seed should be in Clause 12 | Move from 11.22.6.3.4 Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange, 11.22.6.4.6.3 Secure LTF Generation Information, | Rejected |

**Rason for rejection:**

The FTM section is build in a manner that intent to be readable to the uninitiated reader who is familiar with 802.11 but not with FTM.

As a result the structured mechanism is as follows:

1. Overview
2. Negotiation
3. Meas. exchange
4. Termination

Each of those section/subclause attempts to be structured on its own. And there the method is go from simplest to most complex operation.

The relevant functionality (modulation of PHY PPDUs)  is composed of several components:

1. A security negotiation and key derivation
2. Negotiation of intent to do MAC and/or PHY security for FTM
3. FTM MAC level signaling in support of PHY continuously changing waveforms
4. PHY waveform modulation

Item (a) is described completely within in section 12 (whether PASN or regular security association) – it is part of security negotiation

Item (b) is all embedded in the FTM negotiation, is specific signaling to FTM and separating that to section 12 makes it meaningless.

Item (c) could either appear as part of section 11 (MLME) or section 27 (PHY) as this is the signaling that have to do with modulation of waveforms.

Eventually it was decided to put them in the MLME because the FTM uses FTM MAC frame and not HE PPDU headers.

From the CID prespective, it cannot be part of section 12 security because that would mean that FTM signaling (message exchange) has to go to section 12 as well which is completely out of context/partial. The reader would need to have the standard open in two different sections and combing sentences from two clauses. And if that is the case than derivation of waveforms of section 27 (HE PHY) and 28 (EDMG PHY) needs to go in section 12 as well because only there it is fully understandable how the key is then used to encode the bits that goes to the NDP frame same as encoding an MPDU.

### CID 3768

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3768 | 11.22.6.4.6.2 |  | The technical comments on 11.22.6.4.6.1 also apply to 11.22.6.4.6.2 | As it says in the comment | Revised.Refer resolution of CID 3754, 3760, 3842, 3843 |