IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CR for Location | | | | |
| Date: 2020-10-06 | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | Email |
| Girish Madpuwar | Broadcom | Electronic City, 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) |
|  |  |  |  |  |

**Abstract**

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

* CIDs:
  + - Total CID: 16
    - CIDs: 3066, 3760, 3842, 3843, 3912, 3913, 3914, 3771, 3777, 3778, 3779, 3780, 3782, 3783, 3625, 3768

The comments are based on TGaz Draft 2.3 and “IEEE P802.11-REVmd/D2.4, August 2019”

Revision 0: initial draft

Revision 1: proof reading and minor amendments

Revision 2: minor amendments

Revision 3: comments using draft 2.3 as baseline

Revision 4: minor correction based on review feedback

Revision 5: corrected header information. Updated resolution of CID 3780

Revision 6: Ammendment base on feedback received in 11az call.

Revision 7: minor corrections

### CID 3066

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & Page** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 3066 | 11.22.6.4.1  Page 128 | Alecsander Eitan | What is the "I." in line 21 page 128? | As per comment.  Delete “I” | Accepted |

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

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 mode)

— Non-TB Ranging described in 11.22.6.4.4 (Non-TB Ranging measurement exchange)

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3760 | 11.22.6.4.6.1  Page 155 | Mark RISON | "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  Page 156 | Qi Wang | 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  Page 156 | Qi Wang | 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. | Revised.  I2R bits are generated using LTF-counter and SAC. R2I bits are genated using LTF-counter |
| 3913 | 11.22.6.4.6.1  Page 156 | Qi Wang | 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 of section “11.22.6.4.6.1 Secure Non-TB ranging mode” as follow:***



***TGaz Editor: modify “Figure 11-36o of section “11.22.6.4.6.1 Secure Non-TB ranging mode” as follows:***



***TGaz Editor: modify text in “Figure 11-36p of section “11.22.6.4.6.2 TB ranging measurement exchange for secure LTF” as follows:***



***TGaz Editor: modify text in “Figure 11-36q of section “11.22.6.4.6.2 TB ranging measurement exchange for secure LTF” as follows:***



### CID 3771

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3771 | 11.22.6.4.6.2  Page 158 | Mark RISON | "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 the  STA Info fields in the Ranging NDP Announcement  frame to values that satisfy Equation (11-aa)" | Revised  Repetation 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 make the changes identified in 11-20-0340 below |

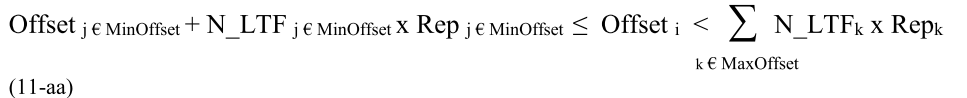
***TGaz Editor: modify text in following paragraph on page 164 line 36 of section 11.22.6.4.6.2***

**11.22.6.4.6.2 Secure TB ranging mode**

:

:

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



:

:

### CID 3842 / CID 3843

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Commenetr** | **Comment** | **Proposed Change** | **Resolution** |
| 3842 | 11.22.6.4.6.1  Page 154 | Mark RISON | "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 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" 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. |
| 3843 | 11.22.6.4.6.1  Page 155 | Mark RISON | "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 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" 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". Make similar changes at 160.28 and 160.40 | Accepted. |

### CID 3777 / CID 3778 / 3782

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Page** | **Comment** | **Proposed Change** | **Resolution** |
| 3777 | 11.22.6.4.6.3  Page 162 | Mark RISON | KDF-Hash-Length -- Hash and Length are undefined | Copy from line 6 on next page | Revised  Reference added to section 12.7.1.6.2  TGaz editor, make the changes identified in 11-20-0340 as below |
| 3778 | 11.22.6.4.6.3  Page 162 | Mark RISON | Having || on the left is confusing and risks misunderstandings | Express SAC and the other thing with separate equations using the L() operator (see baseline) | Accepted  Text is Annex J also updated based on comment for section 11.22.6.4.6.3  TGaz editor, make the changes identified in 11-20-0340 as below |
| 3782 | 11.22.6.4.6.3  Page 163 | Mark RISON | "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 | Revised  ”Underlined” is removed from text.  Please refer resolution of CID3777 / CID3778  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 than adding table for all possible values.  TGaz editor, make the changes identified in 11-20-0340 as below |

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

**11.22.6.4.6.3 Secure LTF Generation**

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

R2I-bits (#3778) = KDF-Hash-*Length*(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)

SAC = L (R2I-bits,0,16) (#3778)

Secure-LTF-bits-R2I = L(R2I-bits,16,Length-16) (#3778)

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)) (#3777)

*Length* is the length in bits required for the SAC concatenated with the Secure-LTF-bits sequence generation input. Length is obtained from equation 11-yy. (#3777)

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)) (#3777)

*Length* is the length in bits required for the SAC concatenated with the Secure-LTF-bits sequence generation input. Length is obtained using equation 11-zz. (#3777)

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 using equation 11-yy and Secure-LTF-bits-I2R shall be derived by Equations 11-zz . (#3782)

( (4Pʹ + 3) x DL\_Nʹ HE-LTF x DL\_Nʹ REP + 16 + 7 ) & ~7), (11-yy)

( (4Pʹ + 3) x UL\_Nʹ HE-LTF x UL\_Nʹ 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 254 line 22***

**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 (#3778)= KDF-Hash-*Length*(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)

SAC = L (R2I-bits,0,16) (#3778)

Secure-LTF-bits-R2I = L(R2I-bits,16,160) (#3778)

***Informative note to Editor:*** *L (S, F, N) is defined in section “1.5 Terminology for mathematical, logical, and bit operations” as follows*

* *L (S, F, N) is bits F to F+N–1 of the bit string S starting from the left, using the IEEE 802.11 bit conventions from 9.2.2*

***Informative note to Editor:***FunctionKDF-Hash-*Length*(K,A,B)

* K is a key;
* A is a unique label for each different purpose of the PRF, treated as an ASCII string
* B is a variable-length string

### CID 3779 / CID 3780

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 3779 | 11.22.6.4.6.3  Page 163 | Mark RISON | Numbers are already exact | Change "exactly 6 octets" to "6 octets long" and "exactly 2 octets in length" to "2 octets long" | Revised  Agree in principle  TGaz editor make change identified in 11-20-0340 |
| 3780 | 11.22.6.4.6.3  Page 163 | Mark RISON | "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 | Revised  Agree in principle  TGaz editor make change identified in 11-20-0340 |

***TGaz Editor: Modify following text in 11.22.6.4.6.3 Secure LTF Generation Information on page 169 line 9***

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 be of 2 octets in length.

### CID 3783

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number & page** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 3783 | 11.22.6.4.6.3  Page 164 | Mark RISON | " 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 169 line number 23***

**11.22.6.4.6.3 Secure LTF Generation**

:

:

where

* Pʹ is a bandwidth dependent parameter based on the assigned, maximum bandwidth for this session; see 27.3.18c (Generation of Randomized LTF Sequence). 𝑃 ′ shall be 7, 8, 9, and 10 for assigned, maximum bandwidths 20, 40, 80, and 160/80+80 MHz, respectively; see Table 9-280 (Format and Bandwidth field).

:

:

* UL\_Nʹ REP 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** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 3625 | 11 | Mark RISON | 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. Measurement 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 in section 11. It contains 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. For the reason mentioned above it’s kept in section 11.

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** | **Commenter** | **Comment** | **Proposed Change** | **Resolution** |
| 3768 | 11.22.6.4.6.2 | Mark RISON | 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.  Changes coming from the following CIDs resolutions address the comments. TGaz editor incorporate the changes appearing in 11-20-0340 for the following CIDs  CID 3760 – revised,  CID 3842 – Accepted  CID 3843 – Accepted  11.22.6.4.6.1 and 11.22.6.4.6.2 sections upated |