IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11[LB249 CR for Various Comments without clause number](relative to P802.11az/D2.0) |
| Date: 2020-01-30 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Jonathan Segev | Intel Corporation | 3600 Juliette Ln, Santa Clara, CA 95054 |  | jonathan.segev@intel.com |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Abstract**

This submission contains proposals to resolve LB#249 CIDs 3829, 3511, 3855, 3630, 3708

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3829 | P.46L.2 | 9.3.1.22.10 | ", and the size of this fieldis one octet" is duplication, as is ", and the size of this field is two octets" at line 10. Also "The CFO parameter field is a signed value of length 2 octets." at 97.4 | Delete the cited text | Revised.TGaz editor make the changes identified by submission 11-20-0159 below.  |

**Discussion:**

This resolution was already presented, strawpolled and met threshold as is but the CID number had a typo showing 3892 instead of 3829 – without change to resolution.

802.11 style guide indicates that in the case of frame/element formats, which are given in a figure and thus normative, the size of the element can be provided in the figure and thus does needs not specifically identified in the immediate accompanying text. However this is not the case for the 2nd quoted parameter “CFO parameter field” which appears on a different page and for text readability purposes the size of the field is given.

**TGaz Editor: Modify the subclause 9.3.1.22.10 P.46 L.2 (D2.0) as follows:**

**9.3.1.22.10 Ranging Trigger variant** (#1707)

The Trigger Subtype field value in the Trigger Dependent Common Info field of the Ranging Trigger frame (Table 9-25k Ranging Trigger subtype field encoding) signals Ranging Trigger 22 frame subvariants (#1391, #1939). The format of the Trigger Dependent Common Info field of Ranging Trigger frame of subvariant Poll, Sounding, Secure Sounding and Report is shown in Figure 9-61d.x.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3511 | P.129L.44 | 11.22.6.4.2.1.2 | Expressions like " Ack frames with PACKET-TYPE equal to TRN-T-PACKET " should refer to this being a \*VECTOR parameter | As it says in the comment | Revised.The commenter is correct that the PACKET-TYPE is a RxVector parameter.TGaz editor make changes identified below in submission 11-20-256. |

**TGaz Editor make changes identified below to P802.11az D2.0 P.130 L.44:**

**11.22.6.4.2.1.2 PDMG/PEDGM AOA/AOD measurement exchange**

…If the RSTA has set the AOD Channel Measurement Feedback subfield to 1 in the DMG Direction Measurement Capabilities field, it shall also include a Channel Measurement Feedback Type field and a Channel Measurement Feedback field in the Fine Timing Measurement frames sent to the ISTA following the reception of the Ack frames that its RXVECTOR PACKET-TYPE parameter equal to TRN-T-PACKET.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause | Comment | Proposed change | Resolution |
| 3855 | P.79L.11 | 9.4.2.297 | "The Secure LTF Counter (#2289) field (#1129) is present in the RSTA2ISTA (#1664) Location 11Measurement Report frame and is reserved otherwise. " -- the field is always present, the only question is when it is reserved | Change to "The Secure LTF Counter (#2289) field (#1129) is reserved in frames other than the RSTA2ISTA (#1664) LocationMeasurement Report frame. ". At 79.17 change "This field is used in theLocation Measurement Report frame transmitted from an RSTA and is reserved otherwise. " to "This field is reserved in frames other than aLocation Measurement Report frame transmitted by an RSTA. " | RevisedSee discussion below. TGaz Editor: make changes as reflected in submission 11-20-0256 below.  |

**Discussion:**

The are two options for an unused set of bits as normal practice in IEEE 802.11:

1. 1st is the field exists but the value is invalid.
2. 2nd is the field does not exists.

11az selected the latter by that allowing the bits on ISTA2RSTA LMR to be used for other purposes.

Other cases of the same practice exists in REVmd (e.g. 160/80+80 BW field “In a TVHT STA, this field is reserved.” Operating mode field format”, User Position Array field “User Position subfield in the User Position Array field is reserved.”, Coverage Class field “The Coverage Class field is reserved”).

Recommendation was to reject the comment.

Jan 30 discussion:

During the previous presentation of the CID resolution, CRC members proposed removal of the Secure LTF Parameters from the ISTA2RSTA LMR as the parameters not needed in ISTA2RSTA LMR.

The parameters Secure LTF Parameters:

1. The Secure LTF parameters is an optional sub-element of the LMR frame.
2. It is mandated for a LTF secure



*“The Secure LTF Parameters field is present if an ISTA and RSTA have negotiated FTM session with secure LTF measurement exchange mode (see 11.22.6.3.4 Secure LTF measurement setup). If present, it contains a Secure LTF Parameters element as defined in 9.4.2.297 (Secure LTF 8 Parameters element).”*

Other consideration (post call):

A secure measurement requires to be able to indicate failure to estimate or risk to measurement estimate possibly due to intentional or unintentional interference. This is carried in the “Invalid Measurement” indication bit, however this bit is contained in the TOA Error field, so some security related functionality already outside of the Secure LTF Parameters field already.

Recap of the Secure LTF Parameters field:



1. SAC || Secure-LTF-bits-R2I = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)
2. Secure-LTF-bits-I2R = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

Secure LTF Counter – Generated by RSTA and sent to ISTA. used by the KDF at ISTA to generate R2I and I2R secure LTF bits (relevant in R2I LMR only).

Generated by the RSTA and sent to ISTA.

1. SAC || Secure-LTF-bits-R2I = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)
2. Secure-LTF-bits-I2R = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

LTF Generation SAC – used to generate the secure LTF bits I2R and R2I of the next sounding round.

Generated by the RSTA and sent to ISTA.

1. SAC || Secure-LTF-bits-R2I = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, Secure-LTF-Counter)
2. Secure-LTF-bits-I2R = KDF-Hash-Length(Secure-LTF-Key-Seed, “Secure LTF Expansion”, SAC || Secure-LTF-Counter)

Ranging Management SAC (should actually be be Range Measurement SAC) – used to associate the measurement results with the SAC used for their generation/measurement instance:

“**9.4.2.297 Secure LTF Parameters element**

**…**

*The Range Measurement SAC field is the same value as the SAC subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the I2R NDP and the R2I NDP….*

*This field is reserved in the initial Fine Timing Measurement frame.”*

*“***11.22.6.4.6.1 Secure Non-TB ranging mode**

**…**

*When a Location Measurement Report frame contains range measurement results measured from 19 an I2R NDP and a R2I NDP, an RSTA shall include the Secure LTF Parameters field in the 20 Location Measurement Report frame and set the Range Measurement SAC subfield in the Secure 21 LTF Parameters field in the Location Measurement Report frame to the same value as in the SAC 22 subfield in the STA Info SAC field in the Ranging NDP Announcement frame that solicited the I2R 23 NDP and the R2I NDP.”*

Dialog token:

Appears in the TF and NDPA in the clear, and in the LMR.

LMR section **9.6.7.48**

*“The Dialog Token field is used to link the location measurement report to the Measurement 5 Sounding Phase which was used for the reported measurement.”*

**11.22.6.4.3.4 TB Ranging measurement reporting phase**

*“The RSTA sets a value in the Sounding Dialog Token Number field in its transmitted Ranging NDP Announcement frame as part of each Measurement Sounding phase. Measurement instances 22 are associated with the Sounding Dialog Token Number field value.”*

*“The Dialog Token field in the LMR frame shall be identical to the Sounding Dialog Token field in the corresponding Ranging NDP Announcement frame in the Measurement Sounding phase from which the reported TOA and TOD values were measured (see 11.22.6.4.3.3 TB ranging measurement sounding phase (#****1474****)). “*

*“***11.22.6.4.4.2 Non-TB Measurement Sounding phase**

*The ISTA maintains a sounding dialog token counter modulo 64 for each RSTA corresponding to a Non-TB Ranging session. The value in the counter is filled in the Sounding Dialog Token Number subfield in its transmitted Ranging NDP Announcement frame. The sounding dialog token counter shall be increased by 1 after each new transmitted Ranging NDP Announcement frame. “*

Removal of the Range Measurement SAC:

It is correct that the Dialog Token and the Range Measurement SAC in the LMR serves similar purpose when Secured Measurement results is in place.

**Is it possible to get rid of the Range Measurement SAC?**

The SDT is only available in the NDPA and the TF and then post sounding in the LMR.

An attacker can send an NDPA or TF with incorrect SDT causing the ISTA/RSTA to go out of sync.

SAC cannot be “easily found” because the probability of a guess is 1/216 i.e. not great.

**Can the SAC not be included only in the ISTA2RSTA LMR?**

The I2R LMR Range Measurement SAC and the R2I LMR Range Measurement SAC of a single exchange instance should be aligned by out of sequence may still happen, i.e. by attacker.

Also would make the I2R LMR interpretation dependent on another message reception (not recommended).

Recommendation to leave the R2I LMR Range Measurement SAC as is.

**Resolution:**

**TGaz Editor: Modify the subclause 9.4.2.297 P.78 L.1 (D2.0) as follows:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | B0 – B7 | B8 – B15 | B16 – B23 | B24 – B71 | B72 – B87 | B88 – B103 | B104 – B111 |
|  | Element ID | Length | Element ID Extension | Secure LTF Counter  | LTF Generation SAC | Range Measurement SAC | Measurement Result LTF Offset |
| Octets | 1 | 1 | 1 | 6 | 2 | 2 | 1 |

1. Figure 9-1012—Secure LTF Parameters element format (#1580, #2283, #1163, #1129)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3489 |  | 4.3.19.19 | It is not clear what "device" means | Change to "STA" in 4.3.19.19 Fine timing measurement, 11.22.6.4.2.1.1 General , 11.22.6.4.3.4 TB Ranging measurement reporting phase | Revised.The commenter is correct, DMG device has 0 occurrences in REVmd and 11ay D5.0. TGaz editor make the changes identified in 11-20-0256 below.  |

**Resolution:**

**TGaz Editor: Modify the subclause 4.3.19.19 P.22 L.13 (D2.0) as follows:**

DMG and EDMG STAs can also estimate the direction of the transmission (Angle of 13 Departure) of frames transmitted to and reception (Angle of Arrival) of frames received from a 14 peer, allowing for estimating position using measurements obtained from frame exchanges with a 15 single peer (#1759, #1760, #1901, #2485, #2486, #2487, #2488).

**TGaz Editor: Modify the subclause 11.22.6.4.2.1.1 P.129 L.15 (D2.0) as follows:**

A PDMG/PEDMG ISTA/RSTA performs an FTM exchange that does not require AOA or AOD 9 measurements as defined in 11.22.6.4.1 (EDCA based ranging measurement exchange). To 10 perform an FTM exchange that does require AOD or AOD measurements, it follows the 11 procedure in 11.22.6.4.2.1.2 (PDMG/PEDMG AOA/AOD measurement exchange). In both 12 these cases, when the first path AWV setting is not used in the exchange, the trigger field shall be 13 set to 1 in the Fine timing Measurement Request that initiates the exchange. In both cases the 14 same AWV used for data transfer between the STAs shall be used for transmission and 15 reception of the preamble and data portion of the PPDUs. (#**1442**, #**2345**, #**2346**)

**TGaz Editor: Modify the subclause 11.22.6.4.3.4 P.144 L.10 (D2.0) as follows:**

In the secured mode of TB Ranging, a STA should discard ranging measurements when it 10 detects that the transmit center frequency offset (CFO) between the ISTA and the RSTA exceeds 11 the allowed tolerance from the values specified in 27.3.18.3 and 27.3.14.3.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3630 |  |  | If the thing being measured for legacy FTM is called "RTT" then so should what is measured for the new ToF-based mechanisms | Change "ToF" to "RTT" throughout | Revised.Agree with commenter the 11az draft uses the terms interchangeably.Refer to discussion depicted in submission11-20-0159 below.TGaz editor replace all occurances of TOF with RTT.  |

**Discussion:**

RTT is defined by eq. 11-5 which is limited to EDCA based FTM.

RTT has 13 occurrences in D2.0, 6 in REVmd D3 while TOF has 0 occurrences in REVmd D3.0 and 46 in 11az D2.0.

The use of TOF is made in sections dealing with TB, NTB and passive sections interchangeably with RTT.

It would be advisable to use a single term.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3708 |  |  | There are references to "Trigger Poll frame" but these are not defined | Delete the cited text in 6.3.56.1 General, 9.3.1.19 VHT/HE/Ranging NDP Announcement frame format (2x), 9.3.1.22.10 Ranging Trigger variant (#1707) (3x), 11.22.6.4.3.3 Measurement Sounding Phase of TB Ranging (#2158) (2x) | Revised.Agree in principal, refer to discussion below.TGaz editor, make changes identified below (total of 7 occurances). |

**Discussion:**

P802.11az defines a Trigger frame of variant ranging sub-variant poll in section 11.22.6.4.3.2

“The Ranging Trigger frame of subvariant Poll is called the TF Ranging Poll”

The Term Trigger Poll frame should be replaced with TF Ranging Poll.

**Resolution:**

**TGaz Editor replace all occurrences of ‘Trigger Poll frame’ with TF Ranging Poll (total of 7).**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3709 |  |  | There's a "Sounding Dialog Token Number" field and a "sounding dialog token counter" but neither of these actually get used on reception for anything | As it says in the comment | Reject.This is a field that is part of 802.11ac and 802.11ax NDPA frame, commenter should review those amendments for the full descriptive behavior of use of the field.For the benefit of the commenter refer also to discussion in submission 11-20-0159 below. |

**Discussion:**

The NDPA frame is a control frame used as part of the sounding mechanism of 11ac, 11ax and 11az.

The NDPA frame includes a field named Sounding Dialog Token which is used by 11ac VHT NDP Announcement frame and in 11ax HE NDP Announcement frame.

The ISTA use of the Sounding Dialog Token and matching of that to measurement is described in P.145 L28-30 of D2.0.

“The ISTA maintains a sounding dialog token counter modulo 64 for each RSTA corresponding to a Non-TB Ranging session. The value in the counter is filled in the Sounding Dialog Token 29 Number subfield in its transmitted Ranging NDP Announcement frame. 30”.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3716 |  |  | There's lots of talk of allocating resources, but it's not always clear what this really means | When it just means "schedule for UL MU", say that; when it just means "transmit to using DL MU", say that (see e.g. sentence at 143.19) | Reject.This is a field that is part of 802.11ac and 802.11ax NDPA frame, commenter should review those amendments for the full descriptive behavior of use of the field.For the benefit of the commenter refer also to discussion in submission 11-20-0159 below. |

**Discussion:**

The NDPA frame is a control frame used as part of the sounding mechanism of 11ac, 11ax and 11az.

The NDPA frame includes a field named Sounding Dialog Token which is used by 11ac VHT NDP Announcement frame and in 11ax HE NDP Announcement frame.

The ISTA use of the Sounding Dialog Token and matching of that to measurement is described in P.145 L28-30 of D2.0.

“The ISTA maintains a sounding dialog token counter modulo 64 for each RSTA corresponding to a Non-TB Ranging session. The value in the counter is filled in the Sounding Dialog Token 29 Number subfield in its transmitted Ranging NDP Announcement frame. 30”.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 3716 | P143L.16 |  |

|  |  |
| --- | --- |
| There's lots of talk of allocating resources, but it's not always clear what this really means | When it just means "schedule for UL MU", say that; when it just means "transmit to using DL MU", say that (see e.g. sentence at 143.19) |

 | When it just means "schedule for UL MU", say that; when it just means "transmit to using DL MU", say that (see e.g. sentence at 143.19) | Reject.This is an invalid comment, see further discussion below. |

**Discussion:**

This is an invalid comment, it fails to identify a specific problem in a meaningful way, it is not possible to understand what specific issue (page, line) is identified, the comment just requires the CRC to “do some work”.

The comment provides an example but this example seems to be reasonably understandable for those familiar with 802.11ax amendment.

**“**This TF shall allocate uplink resources to ISTAs that negotiated ISTA2RSTA LMR and were allocated resources in the preceding measurement 20 sounding phase. 21”