IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11[Resolutions to a few LB240 comments(relative to IEEE 802.11 REVmd D2.0 and P802.11az D1.0) |
| Date: 2019-06-03 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Ganesh Venkatesan | Intel Corporation | 2111 NE 25th Ave, Hillsboro, OR 97124 | 503 334 6720 | ganesh.venkatesan@intel.com |

**Abstract**

This submission proposes resolutions to the following LB240 CIDs 1026, 1099, 1235, 1883, 1923, 2223, 2235, 2253, 2335, 2339, 2451 and 1593.

History:

R0: Initial Version

R1: Incorporate feedback from the Apr 24th teleconferenceR2: enumerating management frames that are subject to protection using PTKSA derived from PASN seems to be tedious with the risk of being incomplete. Some of the comments in the discussion at the May 01-03, 2019, ad hoc lead to the recommendation to use option-A (incorporate text changes from 19/163r3).

R3: Updated with feedback during the May 29th, 2019 teleconference. (CID: 1026, 1099, 1235, 1883, 1923, 2223, 2235, 2253, 2335, 2339 and 2451)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1026 | Albert Petrick | 11.3.3 | 78.05 | Fix "TBD" in management frame - Disassociation and sentence structure | As commented | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 1099 | Alfred Asterjadhi | 11.3.3 | 86.04 | TBD. | Fix the TBD | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 1235 | Assaf Kasher | 11.3.3 | 78.04 | TBD in text - should be removed | replace "TBD (subset or all)" with "All" | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 1883 | Kazuyuki Sakoda | 11.3.3 | 78.04 | There is a TBD in 11.3.3 | Please resolve this tbd | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 1923 | Mark RISON | 11.3.3 | 86.04 | A document with a "TBD" is not suitable for letter ballot | As it says in the comment | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 2223 | Michael Montemurro | 11.3.3 | 78.04 | "TBD (Subset or all)". It sounds like more work is required here. Also, aren't all frames (regardless of security assocation) considered Class 2 frames? | Replace TBD with a description of the Claass 2 frame. | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 2235 | Minyoung Park | 11.3.3 | 78.04 | There is a TBD in the draft. | Please resolve the TBD. | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 2253 | Nehru Bhandaru | 11.3.3 | 78.04 | Text adopted from 19/163r3 related to TBD resolution of frame filtering related to pre-association missing. It should read "Unicast Protected Dual of Public Action frames (9.6.10) when PTKSA from PASN authentication exists" | Replace with text from document - see comment. | Revise, incorporate the changes identified in submission 11-19-466r3.  |
| 2335 | Stephen McCann | 11.3.3 | 78.04 | The "TBD" needs to be clarified. | Change "TBD" to "All" | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 2339 | Thomas Handte | 11.3.3 | 78.04 | There is a TBD | Please define the TBD | Revise, incorporate the changes identified in submission 11-19-466r3. |
| 2451 | Tomoko Adachi | 11.3.3 | 78.04 | Determine the TBD part. | As in comment. | Revise, incorporate the changes identified in submission 11-19-466r3. |

Discussion:

Option-A:

Submission 19/163r3 proposes the following:

(iv) Unicast Protected Dual of Public Action frames (9.6.10) when PTKSA from PASN authentication exists

Option-B:

Alternatively, an explicit enumeration of all PTKSA derived from PASN protected frames will resolve these comments as well.

enumerate all unicast robust management frames that .11az envisions to be protected by PTKSA derivred from PASN. The list currently includes, initial Fine Timing Measurement Request, initial Fine Timing Measurement and Location Measurement Reports. Note that the initial Fine Timing Measurement Request and initial Fine Timing Measurment frames as defined in IEEE802.11-2016 are not subject to this protection – these frames are subject to this protection if and only if they include (a) Ranging Parameters element or (b) Fine Timing Measurement Parameters element where Secure ToF Measurement is enabled.

Resolution: Revise

***TGaz Editor: Incorporate the change to clause 11.3.3 as shown below:***

i) Association Request/Response
ii) Reassociation Request/Response
iii) Disassociation

iv) Unicast Protected Dual of Public Action frames (9.6.10) and SA Query (9.6.9) when PTKSA from PASN authentication exists (#1026, #1099, #1235, #1883, #1923, #2223, #2235, #2253, #2335, #2339, #2451 and #1593):

***TGaz Editor: Modify Table 9-375 in Cl. 9.6.10 as shown below:***

|  |  |  |
| --- | --- | --- |
| **Public Action field value** | **Description** | **Defined in** |
| 32 | Protected Fine Timing Measurement Request (See 11.22.6.3. Fine Timing Measurement Procedure Negotiation). | 9.6.8.32 (Fine Timing Measurement Request frame format)NOTE- A protected Fine Timing Measurement Request frame can be used only in Non-TB and TB modes of the Fine timing measurement procedure or while used while negotiating a DMG/EDMG Session. |
| 33 | Protected Fine Timing Measurement (See 11.22.6.3 Fine timing measurement procedure negotiation, 11.22.6.4 Measurement Exchange) and 11.22.6.6 Fine timing measurement terminaton) | 9.6.8.33 (Fine Timing Measurement frame format)NOTE- A protected Fine Timing Measurement frame can be used only in Non-TB and TB modes of the Fine timing measurement procedure negotiation, while negotiating a DMG/EDMG FTM session or while performing the Measurement Exchange over DMG/EDMG bands (See 11.22.6.4 Measurement exchange) or while terminating a secure Fine Timing Measurement session (See 11.22.6.6 Fine timing measurement termination). |
| 34 | Protected Location Measurement Report | 9.6.8.37 (Location Measurement Report frame format) |
| 35-255 | Reserved |  |

***TGaz Editor: Add to the end of Cl. 11.22.6.3.1 as shown below:***

Prior to initiating a Fine Timing Measurement Procedure Negotiation, an ISTA may execute the Pre-Association Security Negotiation (PASN) with a RSTA and establish a security context to protect the initial Fine Timing Measurement Request and the corresponding initial Fine Timing Measurment exchange. Under these conditions the initial Fine Timing Measurement Request frame and the corresponding initial Fine Timing Measurement frame shall be transmitted using the Protected Dual of Public Action frames (see Cl. 9.6.10 Protect Dual of Public Action frames), if they include either

1. a Fine Timing Measurement Parameters element where the Fine Timing Parameters element field has the Format and Bandwidth subfield set to a value in the range 31-41, or
2. a Ranging Parameters element

If a Fine Timing Measurement session is successfully established as a result of the above exchange, the corresponding measurement exchange (Cl. 11.22.6.4 Measurement Exchange) is defined as a Secure Fine Timine Measurement Session.

***TGaz Editor: Add to the end of Cl. 11.22.6.4.2 as shown below (Note that 11.22.6.4.2 describes the legacy FTM Measurement Exchange which contains the content from the baseline 11.22.6.4 Measurement Exchange):***

When a Secure Fine Timing Measurement Session is established as described in 11.22.6.3.1, the Fine Timing Measurement frames transmitted during the execution of Measurement Exchange shall be Protected Dual of Public Action frames (See Cl. 9.6.10 Protected Dual of Public Action frames)

***TGaz Editor: Add to Cl. 11.22.6.4.3.4 as shown below:***

**11.22.6.4.3.4 TB Ranging Measurement Reporting Part**

The last part of each polling/sounding/reporting triplet is the measurement reporting part, which appears SIFS time after the measurement sounding part (see Figure 11-336c). The measurement results shall be carried in LMR frames (see subclause 9.6.7.37 Location Measurement Report frame format). LMR frames shall carry measurement results from the RSTA to the ISTA, and if negotiated also from the ISTA to the RSTA (see Figure 11-36g). If the Range Reporting is performed in the context of a Secure Fine Timing Measurement Session, the corresponding LMR frames shall be transmitted using the Protected Dual of Public Action frames (See 9.6.10 Protected Dual of Public Action frames). The feedback type of the ISTA-to-RSTA and RST-to-ISTA LMRs shall be either immediate (i.e., from the current availability window) or delayed (i.e., from the last availability window in which the ISTA responded to the TF Ranging Poll and the RSTA allocated resources to that ISTA during the measurement sounding part). The LMR feedback (immediate/delayed) is indicated by the RSTA during the negotiation phase (see subclause 11.22.6.3.1 Range Measurement Negotiation).

***TGaz Editor: Add to the start of Cl. 11.22.6.4.4.3 as shown below:***

**11.22.6.4.4.3 Non-TB Ranging Measurement Reporting Part**

If the Range Reporting is performed in the context of a Secure Fine Timing Measurement Session, the corresponding LMR frames shall be transmitted using the Protected Dual of Public Action frames (See 9.6.10 Protected Dual of Public Action frames).

***TGaz Editor: Change Cl. 11.22.6.6.1 and 11.22.6.6.2 as shown below. Note that the editor instructions to rename Cl. 11.22.6.6 in the baseline as 11.22.6.6.1 EDCA-based ranging session termination is missing in D1.0:***

***Editor: Rename 11.22.6.6 to Fine timing measurement session termination; create a new subclause 11.22.6.6.1 titled EDCA-based ranging session termination and move the contents of 11.22.6.6 to the new subclause.***

**11.22.6.6 Fine timing measurement session termination**

**11.22.6.6.1 EDCA-based ranging session termination**

***TGaz Editor: Add the following to the end of Cl. 11.22.6.6.1 as shown below.***

When the FTM session is a Secure Fine Timing Measurement Session, the Fine Timing Measurement frames transmitted shall be the Protected Dual of Public Action frames (See 9.6.10 Protected Dual of Public Action frames)

 **11.24.6.6.2 TB Ranging and non-TB Ranging session termination**

A TB Ranging or a NTB Ranging session may be terminated through one of the following. In all these cases if the ranging session is a Secure Fine Timing Measurement Session, the corresponding Fine Timing Measurement frames transmitted shall be protect dual of Public Action frames (See 9.6.10 Protected Dual of Public Action frames):

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1589 | Ganesh Venkatesan | 4.3.19.19 | 6 |  | "With the regular transfer of Fine Timing Measurement frames it is possible for the recipient STA to track changes in its relative location with other STAs in the environment." Not true if the measurement exchange is non-Trigger based or Trigger based | The statement in the baseline needs to be modified to include exchanges corresponding to nTB abd TB as means for estimating position/location. Replace with "With the regular transfer of Fine Timing Measurement frames or with regular execution of ranging sounding exchanges, it is possible for the recipient STA to track changes in its relative location with other STAs in the environment." | REVISE |  |

Discussion: The comment identifies a valid omission. However, the use of ‘ranging sounding’ is odd and needs better wording. Recommend using ‘range measurement exchanges’ instead of ‘ranging sounding exchanges’.

Alternatively, the following could be used:

With the regular execution of range measurement exchanges, it is possible for the recipient STA to track changes in its relative location with other STAs in the environment.

Proposed Resolution: REVISE

 Replace statement at P6L18-19 as follows:

With the regular transfer of Fine Timing Measurement frames or with regular execution of range measurement exchanges,it is possible for the recipient STA to track changes in its relative location with other STAs in the environment.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1593 | Ganesh Venkatesan | 6.3.5.3.3 | 10 |  | The description corresponding to Contents of the PASN Authentication Frame is incorrect. Note that .confirm is generated by the MAC layer and sent to the SME. So, the contents of the .confirm primitive are derived from a Authentication frame received from the peer. So, 'the set of elements and fields to be included in PASN authentication frames' is incorrect.This comment applies to .indication primitive as well. | Replace with "The set of elements and fields relevant to PASN authentication from the received Authentication frame from the peer", or something to that effect. The key here is that the parameters that make up the .confirm primitive are derived from the frame received from the peer (and not received from the SME to populate a frame to be sent to the peer). |  |  |

Discussion: This is an issue in the baseline as well. This specific comment addresses a new parameter introduced in .11az.