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: 2019-10-08 |
| 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 |
| Ali Raissinia | Qualcomm | 1700 Technology Dr, San Jose, CA 95110 | 408-652-1057 | alirezar@qti.qualcomm.com |

**Abstract**

This submission proposes resolutions to the following LB240 CIDs 1026, 1099, 1235, 1883, 1923, 2223, 2235, 2253, 2335, 2339, 2451, 2524 and 2523.

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)

R4: removed CIDs that are not resolved by this submission. Updated to address the case of FTM frames indicating Availability Window updates that are aggregated along with LMR, in which case while in the context of a Secure FTM session, these frames are Protected Dual of the corresponding Public Action frames. Expanded the description of negotiation to address all combinations of the Protection of Range Negotiation and Measurement Management Frames Required field in the Extended Capabilities element, setting up of security context and exchange of action frames in the Protected Dual of Public Action frame format. (CID: 1026, 1099, 1235, 1883, 1923, 2223, 2235, 2253, 2335, 2339, 2451, 2524 and 2523)

R5: Fixed text changes to Cl. 11.3.3 (edit to bullet numbered iv) and incorrect table reference 9-362 (and not 9-372).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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. |
| 2524 | Yunsong Yang | 9.6.10 | 75.01 | In all Protected Dual of Public Action frames, the Public Action field value must be kept the same as the corresponding unprotected Public Action frame. So, the Public Action field value for the Protected Location Measurement Report frame should be 46, assuming 46 is assigned to the unprotected Location Measurement Report frame. | Change the Public Action field value for the Protected Location Measurement Report frame to 46. Insert a new row above the Protected Location Measurement Report row, with the field value column being "34-45" and the Desription column being "Reserved". Change the field value column of the last row to "47-255". | REVISE. Since the Location Measurement Frame is not assigned an Action Field value by ANA, the editor needs to request an assignment and use the assigned value in both Table 9-372 and 9-375. In this submission both Tables 9-372 and 9-375 will use the <ANA> designation to indicate that the corresponding value is pending assignment by ANA. |
| 2523 | Yunsong Yang | 9.6.7.1 | 66.29 | In 9.6.7.1, Table 9-362 (Public Action field values) should be updated by adding the 4 new Public Action frames defined in this draft. | Add the 4 new Public Action frame defined in this draft to Table 9-362 (Public Action field values) in 9.6.7.1. | Accept |

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.

|  |  |  |  |
| --- | --- | --- | --- |
| **RSTA setting of** Protection of RangeNegotiation andMeasurement ManagementFrames Required field | **FTM Session** | **Ranging Parameters element or** **Fine Timing Parameters element with Format and Bandwidth subfield set to a value 31 through 41.** | **Notes** |
| 1 | Secure FTM Session | Y | ISTA shall set up PASN or PMF prior to Negotiation and use Protected Dual of Public Action frame format for IFTMR/IFTM/FTM/LMR |
| N | Not Permitted |
| 0 | Secure FTM Session | Y | ISTA shall set up PASN or PMF prior to negotiation and use Protected Dual of Public Action frame format for IFTMR/IFTM/FTM/LMR.  |
| N | Not Permitted |
| Non-secure FTM Session | Don’t Care | Regardless of any prior PASN or PMF set up, ISTA shall only use Public Action frame format for IFTMR/IFTM/FTM/LMR |

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):

***Editor: Add new entries (and adjust the reserved values) to Table 9-362 as shown below:***

***TGaz Editor: Request ANA for an assignment to the Action field value corresponding to the Location Measurement Report action frame (and others). Use the assigned value (labelled <ANA> in this submission) in Table 9-362 and 9-375.***

|  |  |
| --- | --- |
| **Public Action field value** | **Description** |
| 45 | On-channel Tunnel Request |
| <ANA> | Location Measurement Report |
| <ANA+1> | ISTA Passive Location Measurement Report |
| <ANA+2> | Primus RSTA Passive Location Measurement Report |
| <ANA+3> | Secondus RSTA Passive Location Measurement Report |
| <ANA+4>-255 | Reserved |

***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). |
| 34-45 | Reserved |  |
| <ANA> | Protected Location Measurement Report | 9.6.8.37 (Location Measurement Report frame format) |
| <ANA>-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 for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the Extended Capabilities element to 1, an ISTA shall establish a security context with the RSTA.

An ISTA initiating a Fine Timing Measurement Procedure Negotiation for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the Extended Capabilities element to 0 may establish a security context with the RSTA based on its operating policy setting.

The security context can either be established using the Pre-Association Security Negotiation mechanism (12.13 Pre-Association Security Negotiation), if the ISTA and the RSTA are not associated; or management frame protection mechanism (12.6.19 Protection of Robust Management Frames), if the ISTA and the RSTA are associated.

A Secure Fine Timing Measurement Session is established when an ISTA and a RSTA establish a security context and use it to exchange the initial Fine Timing Measurement Request frame and the corresponding initial Fine Timing Measurement frame in the Protected Dual of Public Action frame format (see Cl. 9.6.10 Protect Dual of Public Action frames) and the negotiation completes successfully.

An ISTA shall not initiate a Fine Timing Measurement Negotitation for a session that is not a Trigger-Based, non-Trigger-Based or Fine Timing Measurement session with a Format and Bandwidth not in the range 31 through 41 with Protected Dual of Fine Timing Measurement Request frame

***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 and FTM (See 11.22.6.5.1 Availability Window parameter modification) 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)

 **11.22.6.6.2 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)