IEEE P802.11
Wireless LANs

|  |
| --- |
| LB 240 CR MAC Miscellaneous  |
| Date: 2019-11-11 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Yongho Seok  | MediaTek |  |  | yongho.seok@mediatek.com  |
| ChaoChun Wang | MediaTek |  |  |  |
| James Yee | MediaTek |  |  |  |

**Abstract**

This submission proposes resolutions of comments received from TGaz LB240.

(The proposed change is based on TGaz Draft 1.5.)

* CIDs: 1015, 2025, 1188, 1454, 2259 (5 CIDs)

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGaz Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGaz Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGaz Editor: Editing instructions preceded by “TGaz Editor” are instructions to the TGaz editor to modify existing material in the TGaz draft. As a result of adopting the changes, the TGaz editor will execute the instructions rather than copy them to the TGaz Draft.***

| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** | **Resolution** |
| --- | --- | --- | --- | --- | --- |
| 1015 | 16.28 | 6.3.56.2.4 | States the MLME returns an error to the SME if there is no active FTM session. Clarify what type of "error" and details on what conditions | Clarify as commented | Revised- Since the SME maintains an FTM session, if there is no active FTM session, the SME does not issue the MLME-FINETIMINGMSMT.request primitive. So, remove the error condition. TGaz editor makes changes as specified in 11-19/1958r1 for CID 1015. |
| **TGaz Editor: Change as the following: (#1015)** **6.3.56.2.4 Effect of receipt** ***Change the following paragraph as follows):*** On receipt of this primitive. (#1766)~~— If there is no active FTM session with the specified peer entity, the MLME returns an error to the SME.~~ ~~— If there is an active FTM session where~~ the corresponding measurement exchange is  |
| 2025 |  |  | [Re-raising this comment from the comment collection, as it is not possible to determine from 18/1544r8 whether/how it was addressed. References are to the CC draft and hence may be wrong against D1.0.]PHY-RXLTFSEQUENCE needs to be added to Table 8-2 | As it says in the comment | Revised- Agree in principle. PHY-RXLTFSEQUENCE is added to Table 8-2.TGaz editor makes changes as specified in 11-19/1958r1 for CID 2025.  |
| **TGaz Editor: Change as the following: (#2025)** **8.3.4.2 PHY-SAP inter-(sub)layer service primitives*****Insert a new last row in Table 8-2 as follows:***

|  |
| --- |
| **Table 8-2 - PHY SAP inter-(sub)layer service primitives** |
| Primitive | Request | Indication | Confirm |
| PHY-RXLTFSEQUENCE | X |   |  |

 |
| 1188 | 21.03 | 8.3.5 | The is no PHY-SAP interface to indicate to the Receiver which sequences should be used in future secure EMDG TRN fields | Add a primitive to send those sequences to the PHY, or modify the PHY\_RTLTFSEQUENCES to enable usage in DMG | Revised- Agree in principle. Add a primitive to send the SECURE\_TRN\_SEQUENCES. TGaz editor makes changes as specified in 11-19/1958r1 for CID 1188. |
| **TGaz Editor: Change as the following: (#1188)** **8.3.4.2 PHY-SAP inter-(sub)layer service primitives*****Insert a new last row in Table 8-2 as follows:***

|  |
| --- |
| **Table 8-2 - PHY SAP inter-(sub)layer service primitives** |
| Primitive | Request | Indication | Confirm |
| PHY-RXTRNSEQUENCE | X |   |  |

8.3.4.4 Vector descriptions*Insert the following rows at the end of Table 8-4:* Table 8-4 —Vector description

|  |  |  |
| --- | --- | --- |
| Parameter | Associated vector | Value |
| TRN\_SEQUENCE | TRNVECTOR | Indicates the Secure TRN bit sequences used in the PEDMG secure ranging PPDU. The Secure TRN bit sequences generation is defiend in 12.2.11 (PEDMG Secure Ranging Sequences).  |

8.3.5.22 PHY-RXTRNSEQUENCE.request8.3.5.22.1 FunctionThis primitive is a request by the MAC sublayer to the local PHY entity to provide the Secure TRN bit sequences for the receipt of the PEDMG secure ranging PPDU. 8.3.5.22.2 Semantics of the service primitiveThis primitive provides the following parameter: PHY-RXTRNSEQUENCE.request(TRNVECTOR)The TRNVECTOR represents the Secure TRN bit sequences used in the PEDMG secure ranging PPDU. 8.3.5.22.3 When generatedThis primitive is issued by the MAC sublayer to the PHY entity before receiving the secure TRN subfield of the PEDMG secure ranging PPDU. 8.3.5.22.4 Effect of receiptThe effect of receipt of this primitive by the PHY entity is to make a secure ranging waveform based on the TRNVECTOR. 8.3.5.23 PHY-RXTRNSEQUENCE.confirm8.3.5.23.1 FunctionThis primitive is issued by the PHY to the local MAC entity to confirm that the PHY has applied the parameters provided by the PHY-RXTRNSEQUENCE.request primitive. 8.3.5.23.2 Semantics of the service primitiveThe semantics of the primitive are as follows:This primitive provides the following parameter: PHY-RXTRNSEQUENCE.confirm ()This primitive has no parameters.8.3.5.23.3 When generatedThis primitive is issued by the PHY to the MAC entity when the PHY has received and successfully applied the parameters in the PHY- RXTRNSEQUENCE.request primitive.8.3.5.23.4 Effect of receiptThe effect of the receipt of this primitive by the MAC is unspecified. |
| 1546 | 71.08 | 9.6.7.48 | The definition of the Time-Stamp Error subfield does not seem very efficient or appropriate. We should consider imprioving on this. | Revisit the definition of the Time-Stamp Error subfield and improve on it. | Rejected- The comment fails to identify a specific issue to be addressed. It fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined. |
| 2259 | 128.27 | 12.2.11 | "The first 32 octets of the Secret Key are used for encryption using AES-Counter Mode...of message exchanges between 28 the I-STA and R-STA" - how does this relate to keys established as part of RSNA negotiations that are used to protected data/management frames. If this applies to FTMR/FTM frames, nonce construction, aad construction may need to be specified (or could be the same as RSNA) | Clarify | Revised- Agree in principle. The first 32 octets of the secret key are removed. But, since the related chanes are applied on <https://mentor.ieee.org/802.11/dcn/19/11-19-1785-04-00az-lb240-secure-edmg-ftm-cids-v2.docx>, TGaz editor needs no changes on TGaz Draft for this CID.  |