IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbe LB271 Security comment resolutions – Part 1 | | | | |
| Date: 2023-07-06 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Background

This contribution proposes comment resolutions to TGbe comments received in LB271 on Clause 12 of P802.11be D3.0. The resolutions will be shown relative to D3.0.

CIDs 18019, 15140, 16368, 15194, 15067, 15142, 15195, 15196, 15197, 15512, 18283

Rev 0. Initial submission

Rev 1. Updates based on offline comments.

Rev 2. Further updates based on offline comments

Rev 3. Updates based on TG review during the May interim

Rev 4. Removed approved comments and updates to comments that required additional work

Rev 5. Updates based on TG review prior and during the July adhoc.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Comment** | **Proposed Change** |
| 18019 | 12.7.2 | 415.23 | It's not clear what SA/DA value to use in the A3 of the EAPOL-Key frames in MLO case | Need to clarify. One option is to use the MLD MAC address and another option is to use the link MAC address that corresponds to the link for which the EAPOL-Key frame is transmitted. |
| 15140 | 35.3.2 | 480.12 | There has been discussions about what is the SA or DA in EAPOL key frame. | If needed, clarify with the following. For MLO, - EAPOL key data frame from AP MLD to non-AP MLD with To DS 0 and From DS 1 with SA field, then the value of the SA field is the AP MLD MAC address. - EAPOL key data frame from non-AP MLD to AP MLD with To DS 1 and From DS 0 with DA field, then the value of the DA field is the AP MLD MAC address. |
| 16368 | 12.2.4 | 395.28 | Need to clarify EAPOL PPDU behavior as well. The SA and DA for an EAPOL PPDU is set to the Supplicant and Authenticator address. In the case of MLO, the SA and DA are set to the respective MLD address. | Add the following at the end of the paragraph at 395.28. "The SA and DA address for EAPOL PPDUs shall be set to the applicable Supplicant and Authenticator MLD MAC address." |

### Discussion:

* The comments are asking for clarification on the addresses used in the header of EAPOL PDUs.
* For MLO, the Authenticator and Supplicant addresses are the respective MLD addresses, where the RA and TA are the affiliated STA addresses on the link that the frames are exchanged.
* That means that the SA and DA for EAPOL PDUs should be set to the respective MLD MAC Address.
* Also, 18019 suggests making a change in 12.7.2 which describes the EAPOL-Key frame, where 16368 suggests making the change in the RSNA establishment clause. The addressing would apply to all EAPOL PPDUs.
* It seems reasonable to add the text in 12.2.4 and add a note in 12.7.2.

### Proposed Resolution: (16368, 15140, 18019)

REVISED

Make the change in 12.2.4 proposed by the commenter and add a note in 12.7.2.

Append the following sentences to the end of the paragraph at 395.27:

“For MLO, when an EAPOL PDU is sent from a Supplicant to an Authenticator, the SA shall be the MLD MAC address of the Supplicant, and the DA shall be the MLD MAC address of the Authenticator. Conversely, when an EAPOL PDU is sent from an Authenticator to a Supplicant, the SA shall be the MLD MAC address of the Authenticator, and the DA shall be the MLD MAC address of the Supplicant.”

Relative to REVme D3.0, on p2898.31, insert the following note:

“NOTE – For MLO, the SA and DA of an MSDU carrying EAPOL-Key PDUs is set to the applicable MLD MAC address. See 12.2.4”

At 480.55, insert the following note after NOTE 2

“NOTE 3 – For MLO, the SA and DA of an MSDU carrying EAPOL-Key PDUs is set to the applicable MLD MAC address. See 12.2.4”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15194 | 12.4.1 | 396.58 | "SAE entity" is not defined anywhere. | Add a definition for "SAE entity" including what 802.11 architectural components can be an SAE entity. |
| 15067 | 12.4 | 0.00 | SAE changes are gratuitous and bad | Revert back the SAE changes. "SAE entity" is meaningless and distracts from the definition of the protocol. It's OK to mention that between 2 MLDs the MAC addresses are the MLD MACs but that doesn't justify the wholesale changes to this section. |

### Discussion:

* One commenter does not like the term SAE entity and requested that it be reverted.
* Another commenter mentions that SAE Entity is not defined. However it is defined in clause 3.2 (See D3.0 p61.1)
* The term “SAE entity” was originally introduced to reduce the usage of “STA or MLD” when describing the protocol.
* In the baseline, the term “SAE peer” is already used. It would be better to replace “SAE entity with “SAE peer”
* After checking the usage of “SAE entity” in all 19 locations in the P802.11beD3.0, as well as checking the “SAE entity” can be replaced by “SAE peer” in all locations.
* After review and discussion in the TGbe task group during the May interim the feedback from the TG was that the use of the term “SAE entity” was preferred.
* The current definition is:

**simultaneous authentication of equals (SAE) entity:** An entity that is a station (STA) or a multi-link device (MLD) that participates in SAE authentication (see 12.4 (Authentication using a password)).

### Proposed Resolution: (15067, 15194)

**(15194):**  REJECTED. The definition of SAE entity is already given in clause 3.2 (see D3.0 p61.1) and describes which architectural components can be an SAE entity (a STA or MLD)

**(15067):**  REJECTED. Theterm SAE entity has a definition in clause 3.2 (see D3.0 p61.1) and is used in clause 12.4 to describe a participant in SAE authentication without having to describe each type of entity that can perform the SAE authentication protocol.

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15142 | 12.2.10 | 0.00 | Expand privacy enhancement to MLD. Simply allow MLD to randomize MLD MAC address. | Allow non-AP MLD to randomize MLD MAC address by following the rule defined for non-AP STA under non-MLO. Simply allow the affiliated STA of an MLD to use random MAC address during authentication for the affiliated STA and use ranodm MAC address for affiliated STA during assocaition for the link that is not used to exchagne (re)assocaition request/response frame. The commenter is willing to submit the contribution. |

### Discussion:

* The clause does need to be extended to clarify requirements for an MLD.
* There are three high level things to add:
  + Clarify that the current requirements for a non-AP STA would apply to a non-AP MLD.
  + Describe the requirements for selecting a randomized MAC address for an affiliated STA.
  + Describe the requirements for an affiliated STA, which differ from a non-AP MLD and non-AP STA.

### Proposed Resolution: (15142)

REVISED. Clarify the requirements for a non-AP MLD for MAC Privacy Enhancements

Relative to REVme D3.0, at p2791.20 insert the following paragraphs.

"MAC privacy enhancements are enabled on a non-AP MLD when dot11MACPrivacyActivated is set to true. When enabled, the non-AP MLD shall adhere to the above requirements for a non-AP STA (that is not affiliated with an AP MLD) in selecting a MLD MAC address, including sequence number space and scrambler requirements.  The above requirements defined for a non-AP STA in managing its MAC address during association or establishing transaction state with an AP shall apply to the non-AP MLD in managing its MLD MAC address during association or establishing transaction state with an AP MLD.

When a non-AP MLD with MAC privacy enhancements enabled becomes a non-AP STA for the purpose of BSS transition to an AP, the non-AP STA shall adhere to the requirements above and 35.3.1 for managing and selecting the MLD MAC address. Similarly, when a non-AP STA becomes a non-AP MLD for the purpose of BSS transition to an AP MLD, the non-AP MLD shall adhere to the requirements above and 35.3.1 for managing the MLD MAC address.

NOTE – The non-AP STA MAC address is the MLD MAC address when a non-AP MLD transitions to an AP.  See 35.3.1.

When MAC privacy enhancements are enabled on a non-AP MLD, the SME of the non-AP MLD manages the MAC addresses for each of the affiliated non-AP STAs. The randomized MAC address for an affiliated non-AP STA shall be selected according to IEEE Std 802-2014 and IEEE Std 802c-2017.  Every time an affiliated STA MAC address is changed to a new random value, counters in all sequence number spaces used to identify each MMPDU shall be reset (see 10.3.2.14.2 (Transmitter requirements)) and the STA shall set the TXVECTOR parameter SCRAMBLER\_RESET to RESET\_SCRAMBLER on the next transmitted PPDU.

A non-AP MLD connecting to an AP MLD shall not change the affiliated non-AP STA MAC address(es) for the duration of its association to the AP MLD. An affiliated non-AP STA MAC address may be changed subject to the requirements above when performing BSS transition or ESS transition.”

Modify the description of the “Local MAC Address Policy” subfield in Table 9-190.

Add the “Local MAC Address Policy” extended capability field to the TGbe draft and append the following sentence to the description:

“All STAs affiliated with an MLD set the Local MAC Address Policy subfield to the same value.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15195 | 12.4.1 | 397.32 | Which two STA does "Between the two STAs," refer to? | Change to "Between two non-MLD STAs," |
| 15196 | 12.4.1 | 397.33 | "Peer" is not defined in the context of "begin the protocol when they discover a peer by receiving Beacon or Probe Response frame(s)". Initiation of the protocol should be conditioned on the STA deciding to connect to a specific "peer". | Add a definition for "candidate SAE peer: a remote SAE entity with which the local SAE entity wishes to authenticate" and "SAE peer: a remot4e SAE entity with whith the local STA has completed SAE authentication". (See e.g. peer mesh station and candidate peer mesh station.) Change "when they discover a peer" to "when they discover a candidate SAE peer" and "authentication from a peer" to "authentication from a candidate SAE peer". |
| 15197 | 12.4.1 | 397.34 | "Peer" is not defined in the context of "when they receive an Authentication frame indicating SAE authentication from a peer." Initiation of the protocol should be conditioned on the receiving STA choosing to accept the authentication request from the "peer". | Add a definition for "candidate SAE peer: a remote SAE entity with which the local STA entity wishes to authenticate" and "SAE peer: a remot4e SAE entity with whith the local STA has completed SAE authentication". (See e.g. peer mesh station and candidate peer mesh station.) Change "when they discover a peer" to "when they discover a candidate SAE peer" and "authentication from a peer" to "authentication from a candidate SAE peer". |

### Discussion:

* Cited text in context:

Text

Description automatically generated

* The text the commenter is pointing to is referring to the MAC address of the SAE peers. The paragraph indicates the MAC address of A-MAC and B-MAC.
* Also change SAE entity to SAE peer (See resolution to CID 15194 and CID 15067
* Upon TG review, the feedback from the group was not to replace SAE entity with another term, so the resolution has been adjusted.

### Proposed Resolution: (15195, 15196, 15197)

REVISED. Clarify the MAC address identities for the SAE.

At 397.30, Change

“The parties involved are called Entity-A and Entity-B. They are identified by their MAC addresses, denoted A-MAC and B-MAC. Between two MLDs, the MAC addresses of Entity-A and Entity-B are their MLD MAC addresses. Between the two STAs, the MAC addresses of Entity-A and Entity-B are their STA MAC addresses. Two SAE entities begin the protocol when they discover a peer by receiving Beacon or Probe Response frame(s), or when they receive an Authentication frame indicating SAE authentication from a peer.”

to

“The SAE entities involved in SAE authentication are identified by their MAC addresses, denoted as *A-MAC* and *B-MAC* in 12.4.4. Between two STAs, the SAE entities are identified by their STA MAC addresses. Between two MLDs, the SAE entities are identified by their MLD MAC addresses. An SAE entity begins the protocol when it discovers a candidate SAE entity by receiving a Beacon or Probe Response frame, or when it receives an Authentication frame indicating SAE authentication from a candidate SAE entity.”

### Comment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Comment** | **Proposed Change** |
| 15512 | 12.5.2.3.1 | 402.26 | The text is not true, since the MPDU is modified (e.g., TA) in MLO case. Same issue in P406L35. | Change to: For non-MLO, MPDUs are not modified when retransmitted. For MLO, MPDUs are not encapsulated with a new PN when retransmitted on another link. |
| 18283 | 12.5.2.3.1 | 402.26 | "NOTE 1--Retransmitted MPDUs are not modified on retransmission. For MLO, MPDUs are not encapsulated with a new PN when retransmitted on another link." Retransmitted MPDUs are modified on retransmission when it is retransmitted on a different link because the management frame is re-encrypted. | Fix this bug. |

### Discussion:

* Cited text in context:

Word

Description automatically generated with low confidence

* The baseline text has changed with REVme D3.0 and helps to address both of these comments: “NOTE 1—The frame body of the retransmitted MPDU is not modified on retransmission.”
* The 11be text can be fixed in the same manner with the resulting text: “NOTE 1—The frame body of the retransmitted MPDU is not modified on retransmission. For MLO, the frame bodies of MPDUs are not encapsulated with a new PN when retransmitted on another link.”
* Not all management frames can be transmitted on a different link
* As noted in 15512, this change needs to be made in the GCMP clause as well

### Proposed Resolution: (15512, 18283)

REVISED. At 402.26 and 406.35, change the text of the note to

“NOTE 1—The frame body of the retransmitted MPDU is not modified on retransmission. For MLO, this also applies for retransmission on another link.”

Note to commenter. The first sentence of the note was updated as part of REVme D3.0 at 2835.34