IEEE P802.11
Wireless LANs

|  |
| --- |
| TGbe LB266 Security comment resolutions |
| Date: 2022-10-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | montemurro.michael@gmail.com  |

Background

This contribution proposes comment resolutions to TGbe comments received in LB266 on Clause 12 of P802.11be D2.0. The resolutions will be shown relative to D2.0.

CIDs 13162, 12322, 13599

Rev 4. These are the remaining CIDs after TG review.

Rev 5. Based on reflector feedback

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page** | **Line** | **Comment** | **Proposed Change** |
| 13162 | 12.4.1 | 334 | 57 | This could be seen as a technical change to the baseline, as the definition of "SAE entity" does not refer to APs, while the original text makes it clear that two APs could use SAE between themselves (e.g. for AP PeerKey) | Change the definition at 53.63 to "simultaneous authentication of equals (SAE) entity: an entity that is a station (STA), access point (AP) or a multi-link device(MLD) that participates in SAE authentication (see 12.4 (Authentication using a password))." |

### Discussion:

* The cited text is:

### Graphical user interface, text, application  Description automatically generated

* The first two comments indicate that the cited text between 47 and 52 are duplicates of 12.1.
* The third comment notes that the SAE Entity should be updated to include a reference to AP peers that perform SAE in a mesh. In this it makes sense to include STA, AP, or MLD
* The definition would be changed as follows:

Change

“ an entity that is a station (STA) or a multi-link device (MLD)’

To

“an entity that is a station (STA), mesh STA, or a multi-link device
(MLD)."

* After TG review, it was commented that the term “STA” encompasses a STA or a mesh STA.

### Proposed Resolution:

**(13162)** REJECTED. The group reviewed and discussed the comment and the proposed resolution and concluded that the term STA in the definition encompasses a non-AP STA, mesh STA, or AP.

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 12322 | 12.5.3.3.1 | 339 | 53 | An unified framework should be defined for both individually addressed Data frame and Management frame. Please remove the word "Data" | Please remove the word "Data" |

### Discussion:

* The cited paragraph is:



* It’s clear from the cited text that individually addressed data frames use the MLD MAC address in the CCM Nonce construction (i.e. what some people call AAD swap). What is not clear is that individually addressed management frames, whether directed to the MLD or the affiliated STA use the affiliated STA MAC address on the link that they are transmitted.
* CID 12322 is requesting that individually addressed management frames use the same CCM Nonce construction as data frames.
* CID 12093 is citing the construction of the AAD, but is essentially the same comment as CID 12092
* **TO DISCUSS:** For MLO there are three options for AAD and CCM Nonce construction:
	+ Use a different AAD and CCM Nonce construction for individually addressed management and data frames (i.e. the current behavior documented in the draft)

* + Use the same AAD and CCM Nonce construction for data and MLD level management frames and a AAD and different CCM Nonce construction for link-specific management frames.
	+ Use the same AAD and CCM Nonce construction for all data and management frames for MLO
* Note: the resolution below is based on the current behavior in the draft.
* At a minimum, if the TG does not change the current behavior, a note needs to be added to clarify the behaviour for management frames with MLO
* Add a note at the end of item 3:

After 339.65, add the following note and renumber as necessary:

“NOTE 2 – For MLO, AAD and CCM Nonce construction for management frames follows 12.5.3.3.4 and uses the MPDU header fields to be transmitted over the affiliated STA link.”

* Also add a similar note in the GCM clause

After 343.64, add the following note and renumber as necessary:

“NOTE – For MLO, GCM Nonce construction for management frames uses the MPDU header fields to be transmitted over the affiliated STA link.”

* Quote from reflector discussion (reference to past minutes on the topic:

*“704r1 CR for ML Security for Individually addressed Management Frame*

*Discussion:*

*C: some concerns. link specific information should be used to protect the message. By using MLD address, the link specific information is missing. The change is too late.*

*A: link ID is used to indicate the intended link. There should be no security issue.*

*C: wth link ID in the frme body, there should be no issue. But the inclusion of link ID in the frame body is not mandatory.*

*C: the proposal is the good method*

*C: disagree with the comment. The discussion is wrong. The change is too late.*

*A: link ID will be always in the frame body.*

*C: this is not true.*

*SP: Do you support to accept the resolution in 11-22/704r1 for the following CIDs?*

*5181 and 5184*

*Result: 23Y, 51N, 30A”*

### Proposed Resolution: (12092, 12093)

(12322) REJECTED…. Technical reason

### Comment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Comment** | **Proposed Change** |
| 13599 | 12.5.3.4.4 | 342 | 6 | "The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA and priority value of the received MPDU."In the MLO, the replay counter is not associated with the TA. Please update this baseline rule.And, in Figure 12-23, the MLD MAC Address value should be provided into the Replay check box. | As in the comment. |

### Discussion:

* The comment refers to the mechanism for PN processing for replay detection when MLO is enabled.
* The cited text for CCMP in the baseline is at 3152.1 for REVme D1.0 in clause 12.5.3.4.4):



* The text for GCMP in the baseline at 3161.36 for REVme D1.0 in clause 12.5.5.4.4):



* The PN is associated with the PTKSA and the TA for replay detection for individually addressed data frames transmitted between MLDs should be the MLD Address of the transmitter, not the TA.
* Note that in the baseline block diagrams, the TA is not shown as an input into the “Replay check” box so unless the baseline figure is updated, the figure in the TGbe draft does not need to be updated.
* Similar to what was done for the AAD derivation, the following sentence could be added after the first sentence at the two cited locations:

“If the To DS or From DS subfields in the MAC header of the MPDU are not both equal to 0, and the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, for the purpose of replay detection, the TA is set to the MLD MAC address of the transmitting MLD.”

* After TG review of the proposed resolution, there was concern with the statement “the TA is set to the MLD MAC address”. The updated resolution is given below.

### Proposed Resolution: (13599)

REVISED. Incorporate the changes in <this> document under “Proposed Resolution: (13172)” to clarify the process for replay detection with MLO.

***Add the following baseline clause to the TGbe draft:***

**12.5.3.4.4 PN and replay detection**

***At 3152.1 relative to REVme D1.0, make the following changes:***

d) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA and priority value of the received MPDU. If the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, the receiver shall discard any Data frame that is received with a PN less than or equal to the value of the replay counter that is associated with the transmitter MLD MAC address and priority value of the received MPDU. The receiver shall discard MSDUs and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. (#199)If the receiver set the MFPC bit on a given link to 1, it shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA of that individually addressed Management frame.

***Add the following baseline clause to the TGbe draft:***

**12.5.5.4.4 PN and replay detection**

***At 3161.36 relative to REVme D1.0, make the following changes:***

d) The receiver shall discard any Data frame that is received with its PN less than or equal to the value of the replay counter that is associated with the TA and priority value of the received MPDU. If the MPDU is an individually addressed Data frame transmitted by a STA affiliated with an MLD, the receiver shall discard any Data frame that is received with a PN less than or equal to the value of the replay counter that is associated with the transmitter MLD MAC address and priority value of the received MPDU. The receiver shall discard MSDUs and MMPDUs whose constituent MPDU PN values are not incrementing in steps of 1. If the receiver set the MFPC bit on a given link to 1, it(#199) shall discard any individually addressed robust Management frame that is received with its PN less than or equal to the value of the replay counter associated with the TA of that individually addressed Management frame.